Master Thesis

Czech Technical University in Prague

F3

Faculty of Electrical Engineering
Department of Telecommunications

A security tool using the MITRE ATT&CK classification

Bc. Filip Harant

Supervisor: Ing. Jaroslav Burčík, Ph.D. LL.M
May 2024

MASTER'S THESIS ASSIGNMENT

I. Personal and study details

Student's name:	**Harant Filip**	Personal ID number:	**491863**
Faculty / Institute:	**Faculty of Electrical Engineering**		
Department / Institute:	**Department of Computer Science**		
Study program:	**Open Informatics**		
Specialisation:	**Cyber Security**		

II. Master's thesis details

Master's thesis title in English:

Security Tool Using Mitre ATT&CK Classification

Master's thesis title in Czech:

Bezpečnostní nástroj využívající klasifikaci Mitre ATT&CK

Guidelines:

Study the MITRE ATT&CK classification, which is used to describe and categorise attacks on computer systems and networks. Propose a tool that will be used to design and create threat models. This tool will be closely tied to the MITRE ATT&CK classification and will use an API to extract machine-readable data from the matrix and technical details of classified attacks.
Demonstrate the functionality of the tool using a sample threat model that takes into account the specifics of the organization for which it was created.

Bibliography / sources:

[1] Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 11 Strategies of a World-Class Cybersecurity Operations Center, 2022 The MITRE Corporation, ISBN: 979-8-9856450-7-1, dostupné z:
https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf [on-line]
[2] Ben Clark, Nick Downer, RTFM: Red Team Field Manual v2, 2022 Independently published, ISBN:978-1-07509-183-4.
[3] Blake E. Strom et.all, MITRE ATT&CK: Design and Philosophy, dostupné z
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf [on-line]

Name and workplace of master's thesis supervisor:

Ing. Jaroslav Burčík, Ph.D., LL.M. Department of Telecommunications Engineering FEE

Name and workplace of second master's thesis supervisor or consultant:

Date of master's thesis assignment: **13.02.2024** Deadline for master's thesis submission: **24.05.2024**

Assignment valid until: **21.09.2025**

Ing. Jaroslav Burčík, Ph.D., LL.M. Supervisor's signature	Head of department's signature	prof. Mgr. Petr Páta, Ph.D. Dean's signature

III. Assignment receipt

The student acknowledges that the master's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the master's thesis, the author must state the names of consultants and include a list of references.

.

Date of assignment receipt	Student's signature

Acknowledgements

I want to express my gratitude to Ing. Jaroslav Burčík, Ph.D., LL.M, for his help in crafting such an engaging topic in cyber security, like this tool. His willingness to always make time for me and consistently steer me in the right direction has been invaluable.

Declaration

I declare that I have independently prepared the submitted thesis and have cited all utilized information sources in accordance with the Methodological Guideline on Compliance with Ethical Principles in the Preparation of Higher Education Final Theses.

I acknowledge that my bachelor's thesis is subject to the rights and obligations stipulated by Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Czech Technical University in Prague has the right to conclude a license agreement for the use of this thesis as a school work pursuant to § 60 (1) of the cited law.

In Prague, on May 20, 2024. . . .

Abstract

This thesis focuses on creating a threat modeling tool utilizing the MITRE ATT&CK classification. The tool provides organizations with a comprehensive overview of techniques used by APT groups that may threaten the organization based on specifications entered into the tool and analysis of reports from MITRE TRAM, as well as potential mitigations and detection methods. Through conducting their own risk analysis, organizations can systematically and effectively respond to potential vulnerabilities by patching based on the output from this tool, followed by implementing recommended mitigations or possibly deploying methods to detect techniques threatening the organization.

Keywords: MITRE ATT&CK, MITRE Navigator, MITRE TRAM, MITRE Matrix, Cyberthread model

Supervisor: Ing. Jaroslav Burčík, Ph.D. LL.M
Praha, Technická 1902/2, A4-505a

Abstrakt

Tato diplomová práce se zaměřuje na vytvoření nástroje pro modelování hrozeb za pomoci klasifikace MITRE ATT&CK. Nástroj poskytuje organizaci ucelený přehled o technikách používaných APT skupinami, které mohou organizaci ohrožovat na základě specifikací zadaných do nástroje a analýzou reportů z MITRE TRAM, jejich možných mitigacích a detekčních metodách. Pomocí vlastní provedené analýzy rizik může organizace systematicky a efektivně reagovat na možné zranitelnosti záplatováním na základě výstupu z tohoto nástroje následováním doporučených mitigací či případně implementovat metody pro detekci technik, které organizaci ohrožují.

Klíčová slova: MITRE ATT&CK, MITRE Navigator, MITRE TRAM, MITRE Matrix, Cyberthread model

Překlad názvu: Bezpečnostní nástroj využívající klasifikaci MITRE ATT&CK

Contents

Figures

Tables

Chapter 1
Introduction

These days, we are up against a rising wave of complex online security threats. Attackers are getting better, creating new methods to circumvent safeguards. They aim to sneak into guarded info. Now, it is crucial in our fast-paced, digital world to make upgraded security tools. This aids companies in spotting threats, deciding wisely, reducing risks, and creating a digital shield for themselves.

1.1 Business protection

The evaluation of risks is a crucial element in safeguarding an organization's sensitive data against potential vulnerabilities. Through analysis, an organization can determine the best ways to defend against a range of cyber attacks, including the notorious Advanced Persistent Threat (APT). This vital process allows organizations to identify weaknesses and prioritize the most critical areas that require immediate attention.

Delving into the implementation of risk-based strategies, I discovered numerous tactics for minimizing potential harm. Information systems are intricate and determining which measures yield the most advantages can be challenging, especially when considering technical solutions outlined in the Cybersecurity Act. This becomes even more complex when facing APT threats. To tackle this issue, utilizing a knowledge base that outlines attack techniques and suggests effective methods to detect and mitigate these threats is highly recommended. While such databases already exist, it is still a daunting task to identify the exact actions to take to effectively decrease risk.

The renowned MITRE ATT&CK framework serves as a comprehensive classification system for cyber attacks, offering extensive insights into the methods, tactics, and other components utilized by malicious actors. To effectively safeguard against such threats, organizations must carefully and purposefully choose which information from this classification they address, taking into account risk analysis and vulnerability identification for optimal defense.

Navigating through a large classification can make it challenging to choose the most pertinent information. As such, it would benefit to create a new tool that enables effective filtering of techniques and safeguards. This tool would furnish the organization with a curated list of mitigations, based on risk analysis parameters. Armed with this list, the organization can confidently move forward with implementing robust security measures.

1.2 APT (Advanced Persistent Threads) attacks

Special attention was paid to APT attacks. These attacks are very sophisticated and persistent, posing a great threat to an organization. An APT attack is an event in which an intruder gains unauthorized access to a network and remains there for an extended period without being detected. The main aim of these attacks is usually data theft, disruption of operations, and/or causing damage to the targeted organization. Unlike other types of cyber-attacks, APT attacks are well thought out and specifically designed to take advantage of targeted infrastructure vulnerabilities.

These groups use different tactics, techniques, and procedures to achieve their objectives. The techniques may include a spear-phishing attack to get initial access, deployment of custom malware for establishing a stronghold, lateral movement for getting control within a network, and exfiltration of sensitive data. Due to the sophistication and persistence of these threats, organizations must use robust and integrated security measures.

It is important to mention that understanding and applying the ATT&CK framework provided by MITRE gives organizations the power to better prepare for and defend against APTs.

For example, within the MITRE ATT&CK framework, the Initial Access tactic contains techniques such as spear-phishing attachment, where an attacker sends an email with a malicious attachment to take advantage of a vulnerability in the recipient's system. Once this access has been achieved, the Execution tactic may use techniques like scripting or the exploitation of remote services to run malicious code. Tactics of Persistence ensure that the attacker has a foothold within the system; very often, it uses techniques such as creating new user accounts or modifying system processes.

The detection and response to APTs involve ongoing monitoring and advanced threat intelligence. SIEM systems and EDR solutions are of utmost importance in the identification of unusual activities that would indicate the presence of APTs. In addition, organizations must conduct threat-hunting practices on a regular basis, whereby security teams proactively search for signs of compromise, using the latest threat intelligence and attack patterns, as outlined in the MITRE ATT&CK framework.

Organizations should increase efforts to prevent APTs, which could have devastating implications for their operations, reputation, and bottom line. Prevention measures include strict network segmentation, regular patch management, thorough employee training on phishing and social engineering, and implementation of the principle of least privilege to reduce as much as possible the potential impact of compromised accounts.

In this work, I specifically refer to suggestions of appropriate steps, which are fine-tuned for an organization to perform adequate hardening and extricate itself from the threats posed by these groups based on publicly available information.

The MITRE ATT&CK framework can be used to plot possible attack vectors and form targeted defenses against such attacks. In this way, not only will immediate risks be alleviated that are associated with APTs, but the overall cybersecurity resiliency of an organization will be built to ensure long-term protection against evolving threats.

1.3 The goal of the project

When it comes to comprehending and dealing with online risks, an original perspective can help. MITRE ATT&CK fits the bill perfectly for this. It helps identify and explain the tactics, techniques, and procedures used by hackers during attacks. This model offers important glimpses into the hacker's mindset, aiding organizations in figuring out their weak spots.

There is a tool being created to help organizations build and manage their threat models based on MITRE ATT&CK. This tool will allow an organization to create a model using the parameters and reports ordered by the application interface and MITRE TRAM. This application will serve as a tool for security teams. It will help them easily detect threats, find weaknesses in their cyber defense, and assist with their mitigation.

In the thesis from M.Konečný [1] on page 91, the author shows a table with a risk analysis which he rates on a scale from 1 to 9, where 9 symbolizes the greatest degree of threat to the organization. On page 92, it then proposes measures to address the risks. The organization should be able to provide the same input as on page 92 based on the risk analysis and the tool I have proposed will be able to give the most narrowed down and effective suggestions for action.

1.4 Plans setting

The content of my thesis is extensive, so I have decided to structure it into several sub-points. This is how I plan to proceed in implementing the project and writing the final report.

- Description of terms related to my work and related work.
- Definition of the functional requirements of the application and how the application can be used in practice.
- My solution design and implementation.
- Description of what worked, what didn't work and what can be improved.

1.5 Introduction to the issue of corporate defender

In today's age of constant digital development and a growing cyber environment, the enterprise defender faces challenges that go beyond what an individual human could monitor and analyze. Millions of people around the world are working to create various cyber threats, creating a complex scenario. It is almost impossible for an individual to keep up with the volume of information and the speed at which threats evolve.

The enterprise defender, occupying a key position within the cybersecurity framework, needs a sophisticated tool that enables them to effectively respond to the dynamics of cyber threats. One of the key elements in this fight is the use of databases such as MITRE ATT&CK.

1.6 The company's key assets

Data centers, or modern business hubs, are an absolute necessity. They help companies thrive and stay relevant in a changing world. An integral part of any business, these centers add to the value of a company. They store important information about business operations, customer information, product development, documents on the development processes, and automation controls.

These centers help companies manage their tasks. They make work faster, with increased speed and output. There is a turnkey solution to effective data management that eventually helps a company increase its value. Especially in customer relations, data within these centers are important for providing personalized care and maintaining lasting business connections.

In organizations that have automated their manufacturing processes, all documents, such as technical documentation, are kept in data centers. In organizations mainly focused on development and innovation, the development documents in the data centers are also valuable. These create an irreplaceable base for the non-stop development and operation of the company. Data center security is thus becoming a key part of protection techniques since the corruption or loss of information could be disastrous in its consequences. That includes loss of business opportunities, clients, and business enterprise reputation. In this context, it would be important not only for the best safety but also for the effective management and use of data centers to maintain the stability, competitiveness, and long-term fulfillment of businesses in the trendy virtual generation.

Chapter 2

Basic terms and research

In cybersecurity defense, the role of the defender is quite challenging due to the fact it requires a nuanced understanding of the threat landscape. As a defender, you should ask yourself: What types of challenges am I facing? I will break down key concepts.

In Addition, in conclusion to this chapter, I will focus on related works and try to explain each of the mentioned research in detail so you will be familiar with the main idea of each of them.

2.1 MITRE ATT&CK

MITRE ATT&CK (the term stands for Adversarial Tactics, Techniques, and Common Knowledge) [2] is an organized method for cataloging strategies and methods employed in cyber attacks.

It is considered a worldwide accessible database built from real-life insights. This design is a broad array of systems and strategies, known and utilized in sharing technology threat data.

With ATT&CK, a structured classification system is in place for various hostile behaviors, dividing into three "technological domains": "Enterprise", detailing behaviors on typical IT systems, like Linux or Windows. "Mobile," centered on mobile devices, for example, Android, and iOS. "ICS," is affiliated with industrial regulators and, to a wider extent, cyber-physical systems.

Aside from these areas, ATT&CK also records actions in reconnaissance and weaponization sectors under the PRE-ATT&CK label. This work focuses on the Enterprise ATT&CK map. The enterprise MITRE ATT&CK matrix is shown on the Figure below 2.1.

The Enterprise ATT&CK map is usually shown as a grid of tactics and techniques. Tactics point to potential attacker goals (like Initial Access, Privilege Escalation, etc.). Techniques highlight how an attacker may achieve a specific goal (like Access Token Manipulation, Accessibility Features, etc.).

The work here mostly revolves around tactics and techniques, which align with their designated categories. Each tactic is linked with one or more techniques. Moreover, the Enterprise ATT&CK framework gathers data about each used technique (like threat actors involved, infamous malware, and so on) and potential ways to counteract them.

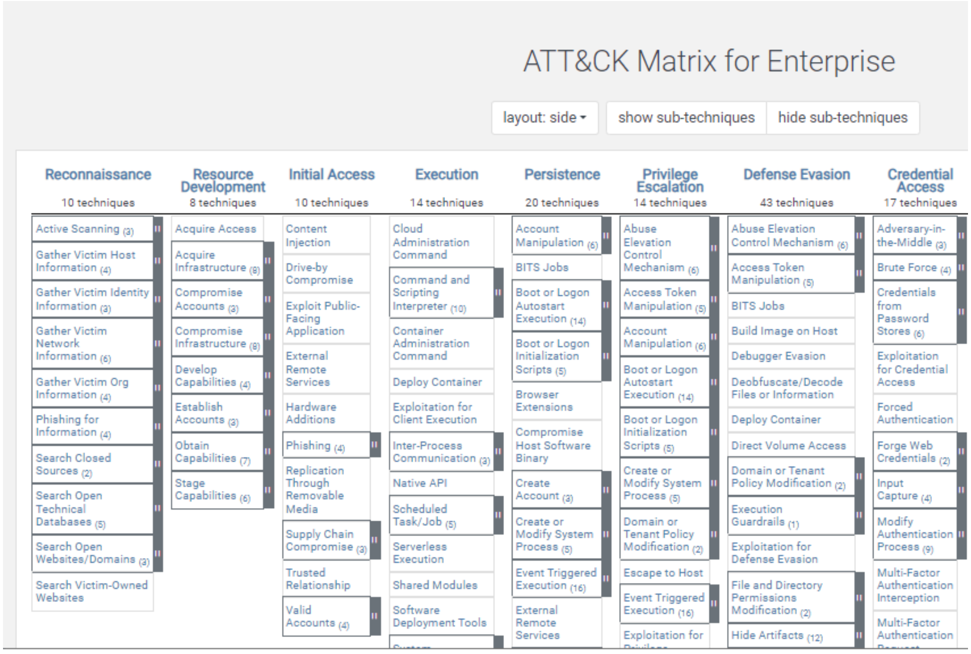


Figure 2.1: The MITRE ATT&CK matrix from the official MITRE ATT&CK web site showing available techniques for each phase - tactic.

2.2 STIX (Structured Threat Information eXpression)

STIX, or Structured Threat Information eXpression [3], is a standardized language for structuring and exchanging information about cyber threats. This standard was developed by the Organization for the Advancement of Structured Information Standards with the goal of enhancing the sharing of detailed threat information among different organizations and systems. STIX is a structured format for description, which includes identifiers, tactics, techniques, and procedures used by attackers in the context of cyber threats. The format can represent threats homogeneously, making them easier to analyze and share.

STIX was designed as a modular standard in that threat information is organized into separate modules or objects as follows:

- Details on specific indicators of a threat, such as IP addresses, file hash values, or domain names.

- Information on individuals or groups responsible for threats.
- Specific methods and procedures used by attackers to achieve their goals.
- Contextual information on coordinated activities or recurring attack patterns.

Since it is a standardized language, STIX allows for easy sharing of threat information across different tools and platforms. This means that information can be shared and interpreted with no loss of detail or meaning. STIX was designed to be extendable in that organizations can add their own definitions or extensions according to specific needs. This provides the standard the adaptability for multiple applications and use cases.

Some benefits of using STIX include:

- Organizations can effectively communicate about threats and share critical information with partners, allowing for better coordination of defensive measures.
- Standardized threat information allows for quicker identification and response to new and emerging threats.
- Its structured nature makes STIX ideal for use in automated systems for threat detection and response.
- Contextual information on coordinated activities or recurring attack patterns.

STIX is often used in conjunction with other standards, notably TAXII, which provides the means by which trusted systems can perform secure cyber threat indicator exchanges. Together, they enable the creation of robust and interoperable cybersecurity ecosystems.

In general, STIX is a crucial tool in modern cyber defense, enabling effective sharing and analysis of threat information to enhance organizations' capability to counter continuously emerging cyber threats.

2.3 TAXII (Trusted Automated eXchange of Indicator Information)

TAXII [4], or the Trusted Automated eXchange of Indicator Information, represents the state of the art in protocols for the exchange of cyber threat information. Such threats were designed to be shared in a loosely coupled way, based on the STIX language to represent structured and complete information. Using TAXII, organizations can securely and automatically share threat intelligence, enhancing their ability to detect, respond to, and mitigate cyber threats.

One of the key benefits of TAXII is that it shares detailed, substantial cyber threat information securely across a diversity of organizations, security communities, and products and services. It also works with standardized message exchanges, where the information shared is consistent and easily interpreted across different systems and organizations.

The protocol supports many modes of sharing, including hub-and-spoke, where information is sent to a central point and then redistributed, and peer-to-peer, where information is shared directly between organizations. This flexibility allows TAXII to fit the specific needs and preferences of different organizations and communities, which makes it a versatile tool for threat intelligence sharing.

TAXII plays a very important role in facilitating the collaboration and information sharing that occurs in cybersecurity. Sharing threat indicators, such as IP addresses, domain names, and malware signatures among other indicators of compromise (IOCs), in a standardized and automated manner is very fundamental to coordinated defense against cyber threats. Using TAXII, organizations can disseminate and receive threat intelligence quickly, thus enabling them to respond much faster to emerging threats.

More importantly, TAXII automates a lot of the work involved with sharing threat intelligence, making the process very fast and with reduced chances of human error in the process. The automation will further enhance continuous and real-time sharing of threat data, which is primary to the dynamics of the cyber threat environment.

TAXII is widely used in conjunction with STIX, which provides the structured format for the threat information being shared. In a combination of TAXII and STIX, it provides seamless and efficient flow, from threat intelligence creation to distribution and consumption. This integration of the standards into the ecosystem ensures a comprehensive and interoperable environment for cyber threat intelligence.

In general, TAXII is a very important tool when dealing with cybersecurity. It provides seamless and secure automation of exchange between organizations and platforms on threat intelligence, enhancing collaborative efforts in fighting cyber threats. By facilitating the sharing and receipt of critical threat intelligence by organizations, TAXII supports the establishment of a resilient, proactive cybersecurity environment where information sharing and collaboration of defense are on the front line.

2.4 MITRE ATT&CK Navigator

Mitre ATT&CK Navigator is an essential tool in the cybersecurity community, designed to enhance the functionality and visualization of the MITRE ATT&CK system.

The MITRE ATT&CK Navigator acts as an interactive and user-friendly interface that allows security personnel, inspectors, and guards to navigate many of the methods and techniques outlined in the ATT&CK System. The default MITRE ATT&CK Navigator matrix is shown on the figure below 2.2

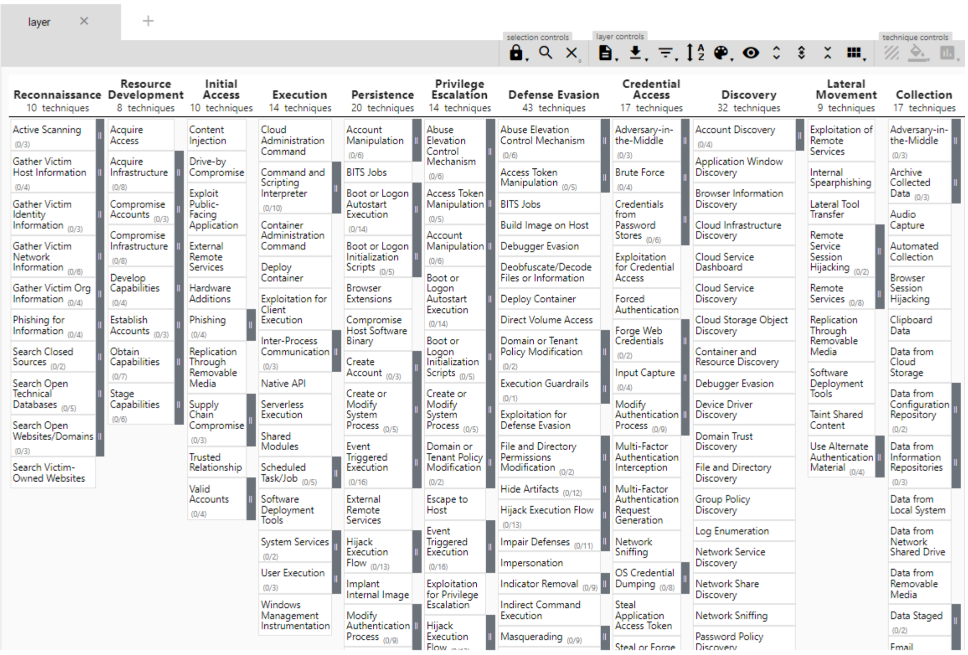


Figure 2.2: The MITRE ATT&CK Navigator matrix showing a new created layer of Enterprise ATT&CK.

2.5 MITRE TRAM

The MITRE Threat Report ATT&CK Mapping, or TRAM, is a sophisticated solution that helps cybersecurity professionals translate threat intelligence reports into structured formatting consistent with the MITRE ATT&CK framework. This tool foremost aims at streamlining what is otherwise a time-consuming process of mapping unstructured threat data into standardized ATT&CK technique mappings with better consistency and accuracy in analysis.

It is based on natural language processing, which identifies and extracts relevant ATT&CK techniques automatically from threat reports. This technological capability dramatically reduces the manual workload involved in analyzing and mapping these reports. The interactive user interface of TRAM offers analysts an opportunity to review and refine the automated mappings, which gains from the benefits of automation coupled with essential human oversight for the quality of the outputs.

Seamless integration with the MITRE ATT&CK framework is another leading advantage allowing the tool to dynamically update when techniques and tactics are constantly added to the knowledge base. Additionally, TRAM can be trained on a specific dataset to provide improvements in accuracy for particular types of reports or in the organizational context. This offers a customization level that allows the user to fine-tune the tool toward a specific workflow requirement.

The advantages of using TRAM are many. It enables the reduction of time by a much greater degree than analysts need to spend in mapping, hence allowing them to have more detailed analysis and response strategies. Machine learning in the tool further enhances the precision of technique identification to mitigate the risk of human error. Additionally, the mapping done automatically brings a standardized approach to interpreting and applying ATT&CK techniques across a variety of reports and analysts.

From a practical point of view, organizations can use TRAM to quickly process and map threat reports, which provides for much faster detection and response to new threats. The tool is also good for training new analysts to efficiently map reports against ATT&CK techniques.

In all, MITRE TRAM is a powerful way to enhance the effectiveness and efficiency of cybersecurity threat intelligence analysis. It helps organizations to better understand and react to cybersecurity threats more effectively and to strengthen their defense.

2.6 Techniques, tactics, software, groups, and mitigations

The MITRE ATT&CK framework distinguishes between techniques, tactics, mitigations, software, and groups. There is an interconnection between these elements.

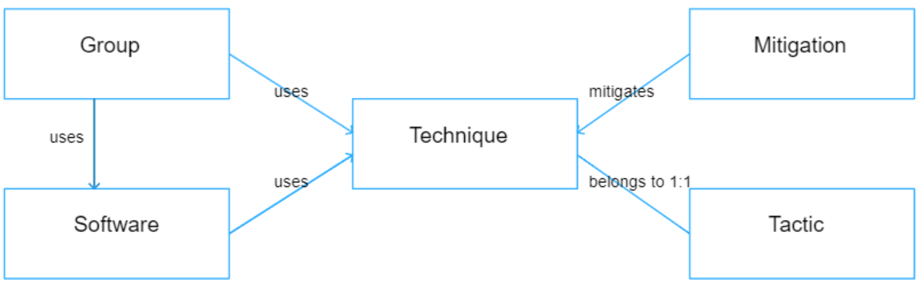


Figure 2.3: The relationship between techniques, tactics, mitigations, software, and groups

Tactics describe a kind of process that each attacker goes through if he intends to attack a victim and steal sensitive data. In general, each technique falls under a specific tactic, which allows for an understanding of the attackers' practices. We can think of it as a kind of higher-level strategy, where each technique serves as a specific step of a certain tactic.

Mitigations are closely related to techniques and they limit the impact of cyber threads. Each technique may require several mitigations, but even a single mitigation can partially eliminate multiple threats.

The software serves as a means to implement techniques and creates another layer of connectivity. This software can be used by groups along with the techniques listed in the database to implement attacks. Groups represent organized worldwide entities whose goals may vary depending on their preferences.

For standardized multi-platform recording of information, all this data is stored in STIX format. The relationships between the elements can be seen in the figure 2.3

2.7 Related studies

There are a huge number of studies, articles, and papers on MITRE ATT&CK, as it is indeed a very well-known tool that has active administrators and is constantly being synchronized over time. I have included some of them in this paper and will analyze them. The searches are varied to delve into different concepts of works that are different from each other, but accurate enough to relate to my work. Specifically, all of the studies work with and extend the MITRE ATT&CK framework in some way. However, upon closer examination, I concluded that most of the papers would not be ultimately useful to me, but I would still mention some selected papers. For example, the study Associations of MITRE ATT CK Adversarial Techniques [5] discusses the use of statistical machine learning analysis to infer technique clustering in the MITRE ATT&CK Framework, which provides information on adversarial tactics, techniques, and procedures. The goal is to predict unobserved attack techniques based on observed ones for attack diagnosis and mitigation. The study uses hierarchical clustering to identify 98 different technique associations for APT and Software attacks, with 78% of the techniques showing significant mutual information.

The Bayesian ATT&CK Network (BAN) that incorporates the MITRE ATT&CK framework was introduced [6]. It incorporates the MITRE ATT&CK framework by utilizing its Tactics, Techniques, and Procedures (TTPs) as nodes within the Bayesian network. BAN leverages the knowledge of cybersecurity experts and historical attack data to identify the fundamental relationships between ATT&CK techniques. It also uses publicly available APT reports to collect and extract the ATT&CK techniques noted in each report, which are then labeled in various ways. The structure of the BAN is trained through structure learning using dataset and expert knowledge, and the parameter learning is executed using the collected dataset to calculate the conditional probability table (CPT) of BAN. BAN thus utilizes the MITRE ATT&CK framework, expert knowledge, and historical attack data to construct a Bayesian network for predicting APT attacks.

Study Linking CVE's to MITRE ATT&CK Techniques [7] is about the importance of linking Common Vulnerabilities and Exposures (CVE) to MITRE ATT&CK Techniques to improve post-compromise detection of advanced intrusions. It also discusses the role of software vulnerabilities in cyber-intrusions and the need to understand how vulnerabilities enable attackers at each stage of the attack life cycle. The authors highlight the lack of methods to extract labels from threat reports and the sparse classification of CVE into the ATT&CK taxonomy. CVE2ATT&CK BERT-Based Mapping of CVEs to MITRE ATT&CK [8] discusses the importance of a standardized cyber-security knowledge database to combat cybercrime. It specifically focuses on the mapping of Common Vulnerabilities and Exposures (CVEs) to MITRE ATT&CK techniques using BERT-based algorithms. It discusses the need to link the Common Vulnerabilities and Exposures (CVE) list with the MITRE ATT&CK Enterprise Matrix to provide more context and valuable information for CVEs. The MITRE ATT&CK Enterprise Matrix links techniques to tangible configurations, tools, and processes that can be used to prevent a technique from having a malicious outcome. By associating an ATT&CK technique to a given CVE, more context and valuable information for the CVE can be extracted, enabling security analysts to discover and deploy the necessary measures and controls to monitor and avert the intrusions pointed out by the CVE.

Thesis from Chukwu [9] discusses the costs and consequences of cybercrime, as well as the limitations of current cybersecurity solutions. It proposes the integration of a data model for threat analytics and intelligence to enhance cyber threat detection through Security Information and Event Management (SIEM). The paper also emphasizes the importance of analyzing cyberattack patterns and tactics and proposes processes and procedures to enhance threat detection and response capabilities within organizations. It also discusses upgrading security mechanisms and integrating security procedures into existing business operations. The paper aims to provide insights into compliance, risk assessment, threat intelligence, and transitioning to suitable security controls. In addition to the MITRE ATT&CK framework and the ATT&CK Navigator, the document also mentions the use of other tools and procedures in alignment with the ATT&CK framework. These include Threat Intelligence Platforms, which aggregate and analyze threat intelligence data from various sources to provide insights into recognized adversary TTPs, and Security Information and Event Management (SIEM) Systems, which gather and scrutinize log data from an organization's IT infrastructure to detect specific techniques or indicators of compromise. Furthermore, the document discusses the use of the MITRE ATT&CK TRAM (Threat Report ATT&CK Mapping) to automatically map adversaries' procedures using trained machine learning algorithms or models.

An automatic method for generating attack sequences based on the tactics and techniques of MITRE ATT&CK for industrial control system security datasets was introduced in the study Design and Philosophy [10]. It also introduces an attack sequence executor for driving the attack sequence on the HAI (Human Augmented Intelligence) testbed. The approach is based on hidden Markov models and aims to provide a practical way to leverage datasets for cybersecurity research. The attack sequence executor works on the HAI testbed by utilizing the Purple Team ATT&CK Automation module. This module can automatically emulate MITRE ATT&CK tactics and techniques through Metasploit. The HAI testbed includes real ICSs (Industrial control systems) widely used in critical infrastructure, operating components such as engineering workstations (EWS) and human-machine interfaces (HMI), and a log server that collects data generated in the testbed. Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study [11] presents an analysis of the automatic mapping of Cyber Threat Intelligence (CTI) into attack techniques, focusing on the MITRE ATT&CK framework. It presents new datasets for CTI analysis and evaluates machine learning models, discussing classifier performance, classification errors, and challenges in CTI analysis. The study aims to support proactive security efforts by leveraging information about threat actors and their techniques.

Two studies [12],[13] propose new modeling languages. The first of them [12] proposes enterpriseLang which is a threat modeling language based on META Attack language (MAL) that enables attack simulations on system model instances. It supports the analysis of security settings and architectural changes to enhance system security. The language can model enterprise systems and provide probabilistic security measures. The future work includes enriching enterpriseLang with information from other databases and assigning probability distributions to attack steps/defenses for more realistic simulation results. The enterpriseLang is based on the MITRE Enterprise ATT&CK Matrix. The matrix serves as a knowledge base for the language and provides information on adversary behaviors, attack steps, and defenses. The enterpriseLang allows stakeholders to assess threats to their enterprise IT environment and analyze what security settings could be implemented to secure the system effectively.

Engla Rencelj Ling from KTH Royal Institute of Technology in Sweden presented a session on generating threat models and attack graphs based on the IEC 61850 System Configuration Language at the SAT-CPS '21 virtual event [13]. The study focused on the importance of securing power systems from cyber attacks and also the use of the Meta Attack Language (MAL) to develop threat modeling languages. The presentation also introduced the SCL-Lang, a MAL-based language created for creating threat models of substations based on their SCL files, enabling structured cyber security analysis for evaluating design scenarios before implementation.

In a study proposing a formal methodology for evaluating SD-IoT framework security through threat modeling [14] the researchers utilized the MITRE ATT&CK framework to map attack vectors of SDVN to the MITRE ATT&CK V13 framework. They employed both manual-based and tools-based methods, including the MITRE ATT&CK Navigator and the open-source TRAM tool, to suggest MITRE ATT&CK techniques for each phrase in threat reports.

MITRE TRAM [15], which was already mentioned in the previous chapter, is a system that uses a supervised Logistic Regression to label threat reports with MITRE ATT&CK techniques. It provides a user interface for administrators to define and refine labels. TRAM ingests unstructured data but is only trained from self-labeled examples and requires human intervention to correct misclassified labels. An advantage is all data from reports can be converted to json files and downloaded which makes it ideal for me to use it to get all techniques from that file.

The development and evaluation of a Pseudo-Active Transfer Learning (PATRL) process for improving the accuracy of predicting cybersecurity alerts is a main goal in the study that focuses on using unstructured text data [16], such as alert descriptions, to train a language model and then apply a Pseudo-Active Learning approach to iteratively improve the model's performance. The goal is to enhance the accuracy of predicting cybersecurity alerts, particularly for unknown or unclassified data, by leveraging transfer learning and active learning methodologies.

PATRL offers several advantages over TRAM. First, PATRL uses transfer learning, active learning, and pseudo-labeling to translate intrusion alert descriptions into action-intention stages (AIS) that are easy to interpret. This method overcomes the challenge of spurious minimal-label data and reveals the characteristics of unlabeled data. In addition, PATRL provides a Monte-Carlo Dropout Uncertainty and a Pseudo-Label Convergence Score for each forecast alert, providing analysts with insight into whether top-1 or top-3 forecasts should be trusted or whether new pseudo-labels are needed. In addition, PATRL significantly improves the unknown data accuracy in all pseudo-label selection methods, providing 85% top-1 accuracy and 99% top-3 accuracy. This high accuracy is especially useful in scenario-critical types in which misallocation can have a significant impact on the network. At first glance, PATRL may seem like a very promising tool. However, I could not find any code, and the authors of this study did not place their code anywhere.

On the other hand, the tool I found the code for, and tested, was introduced in the study [17] that introduced a tool called rcATT, which is similar to the tool MITRE TRAM, however, gives better results. Also, this tool seems handy to me, as it only involves a small installation and can be done by typing a one-line command. However, the main drawback of this tool is that the libraries it uses are outdated in newer versions of Python and STIX. The user needs to install two versions of Python, where newer versions of Python are not supported, and does not want to make his life more difficult by trying to handle all the mistakes before installing the program thus, this is the reason why I, in the end, used MITRE TRAM as it is a well documented and supported tool.

Chapter 3

Specification of requirements for an interactive application

Every application under development should meet some prerequisites that make it usable, especially in a working environment. Such assumptions define how an application should look and give us the functionality. In addition to the functional requirements, it is important, among other things, whether the application or tool will have real-world usage or if it ends up like many other often not-so-good prototypes.

3.1 Functional requirements

The resulting application should ideally be based on a risk analysis. For this purpose, the organization must carry out an internal analysis to give the application-specific parameters that characterize it as much as possible. The input to the application should be the "industry" parameter, specifying in which sector the organization operates, the "geolocation" parameter, specifying the location of the organization, and the organization's risk analysis. The application retrieves the specified parameters and gets the most up-to-date information from MITRE MATRIX from the TAXII server using STIX from the MITRE ATT&CK framework. Based on the parameters, it finds out the groups that could be a hazard for the organization and gets a list of techniques the groups use.

If an organization wants more reliable results, it needs to download the MITRE TRAM tool, which is publicly available in the Github repository, and run the application. Collect reports from public sources, upload them to MITRE TRAM, and from there provide the data to the application. The application appropriately grabs this data and adds all relevant techniques extracted from the MITRE TRAM application to the existing techniques.

The user should be able to interact with the application through the user interface and spend as little effort as possible to get it working. The results of the techniques obtained should be displayed in the graphical interface of the application and the user should be able to download and upload the techniques to Mitre ATT&CK Navigator for analysis and good visibility. From the techniques, the user should be able to select the mitigations and detections that belong to the technique and that the user chooses to implement. Finally, the user should be able to download the results of techniques, mitigations, and detections into an Excel spreadsheet.

3.2 Practical utilization of the developed application

If an organization opts to align its patching strategy with the MITRE ATT&CK matrix, the cybersecurity officer would likely face significant time investment due to the extensive data contained within the matrix. My tool is designed with the main goal of simplifying the tasks of the security specialist, making it easier to interpret results. The specialist has the option to download these results for flexible manipulation, such as implementing individual patches using an Excel spreadsheet or visualizing the outcomes for a more comprehensive perspective within the MITRE ATT&CK Navigator.

Chapter 4
Implementation

In the process of developing my program, a primary focus was placed on seamless interaction with the MITRE ATT&CK framework. To achieve this, I leveraged the TAXII server, which provided access to essential information. Python was the natural choice of programming language, aligning with the preferences of the MITRE ATT&CK team and its existing Python examples for data parsing from the TAXII server.

While the MITRE ATT&CK team is contemplating the implementation of a traditional REST API in the coming year, this information has been verified through email correspondence with the team. Throughout my work, it became evident that direct interaction with JSON data would be advantageous for my specific requirements. Consequently, I manually downloaded data from the MITRE ATT&CK GitHub repository, such as the 'Enterprise-Attack.json' file, and stored it within my application directory. Experiments indicated that manual downloading and loading of data from a file significantly outpaced querying the server.

After discovering this, I decided on a plan that incorporated both direct file loading and server access for collecting the necessary data. By implementing this method, I was able to effectively utilize the full potential of the MITRE ATT&CK framework, perfectly aligning with the requirements of my master's thesis.

4.1 Working with MITRE kill chain

In my work, I often discuss various techniques, each of which typically falls under a specific tactic. To be more precise, an attacker generally follows several fundamental phases to reach their target. A comprehensive overview of these phases is provided by frameworks such as the Cyber Kill Chain, which refers to them as stages. The Cyber Kill Chain addresses cyberattacks against organizations from a high-level perspective, summarizing the attack process into seven stages.

However, in comparison to the Cyber Kill Chain, the MITRE ATT&CK framework offers a more detailed and extensive view of the cyberattack process, breaking it down into multiple phases called "tactics." These tactics cover a broader spectrum of attacker behavior and provide deeper insights into the various methods used throughout an attack. The difference between the two frameworks can be seen in the following image: ??.

Given that my work involves all these tactics, I will describe each one in detail.

Tactics outline the stages an attacker goes through from the initial access to the final impact. To achieve their goal, an attacker must navigate through these stages sequentially; failing to do so would hinder their ability to progress to the next phase. Here are the tactics as defined by the MITRE ATT&CK framework:

Figure 4.1: Comparing stages from Cyber Kill Chain and tactics from MITRE ATT&CK. Image source: https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-attack-vs-cyber-kill-chain.

1. Reconnaissance

   - **Description:** The initial phase where information about the target systems or organizations is gathered. This may involve searching for publicly available data, conducting phishing campaigns, or scanning for vulnerabilities.

2. Resource Development

   - **Description:** Developing, purchasing, or compromising resources that will be utilized in subsequent stages of the attack. Activities might include creating malware, registering domains, or setting up command and control infrastructure.

3. Initial Access

   - **Description:** Gaining an initial foothold in the network through methods such as spear-phishing, exploiting software vulnerabilities, or deploying malicious code on publicly accessible websites.

4. Execution

   - **Description:** Once access is gained, malicious code is executed on the target system. This phase might involve running scripts or programs that facilitate further infiltration or persistence.

5. Persistence

   - **Description:** Ensuring continued access to the system even after reboots or credential changes. Techniques include installing malicious services, modifying system configurations, or other methods to maintain access.

6. Privilege Escalation

   - **Description:** Attempting to gain higher-level permissions on the system to perform additional malicious activities. This could involve exploiting vulnerabilities or misconfigurations to elevate privileges.

7. Defense Evasion

   - **Description:** Employing various techniques to avoid detection by security systems such as antivirus software, firewalls, or intrusion detection systems. This can include obfuscating code, modifying logs, or using legitimate tools for malicious purposes.

8. Credential Access

   - **Description:** Obtaining credentials like passwords, keys, or tokens that provide access to additional systems or data. Techniques may include keylogging, memory dumping, or extracting password hashes.

9. Discovery

   - **Description:** Gathering information about the network and systems to understand the environment and identify further targets. This can involve network scanning, gathering user lists, or mapping infrastructure.

10. Lateral Movement

   - **Description:** Moving through the network to access other systems and expand the attacker's foothold. Methods include using shared folders, remote desktop protocols, or exploiting vulnerabilities.

11. Collection

   - **Description:** Gathering data from compromised systems that can be useful for the attacker's objectives. This can include documents, databases, emails, or other sensitive information.

12. Command and Control

   - **Description:** Establishing a communication channel with compromised systems to control them and carry out further operations. This can involve using reverse shells, web servers, or social media platforms for command and communication.

13. Exfiltration

   - **Description:** Transferring collected data from compromised systems to the attacker's infrastructure. Methods include using encrypted communication channels, hiding data within legitimate traffic, or uploading files to external servers.

14. Impact

   - **Description:** Performing actions that have a direct impact on compromised systems or organizations. This can involve encrypting data, deleting files, or sabotaging operations, leading to significant disruptions.

It is important to mention that each tactic takes a significantly different amount of time. In Figure 4.2, all these stages are divided into three color-coded sections. Each phase within an individual section lasts for a different duration. For example, the stages of reconnaissance and weaponization in the cyber kill chain, which can be mapped to the tactics of reconnaissance and resource development in MITRE ATT&CK, can take anywhere from hours to even months. In the figure, the description of these possibilities is highlighted in blue and labeled as the preparation phase. This phase takes a long time because the attacker must prepare for the attack in detail. If the attacker starts unprepared, the subsequent steps would take longer, and the defender might be able to thwart the attack during this time.

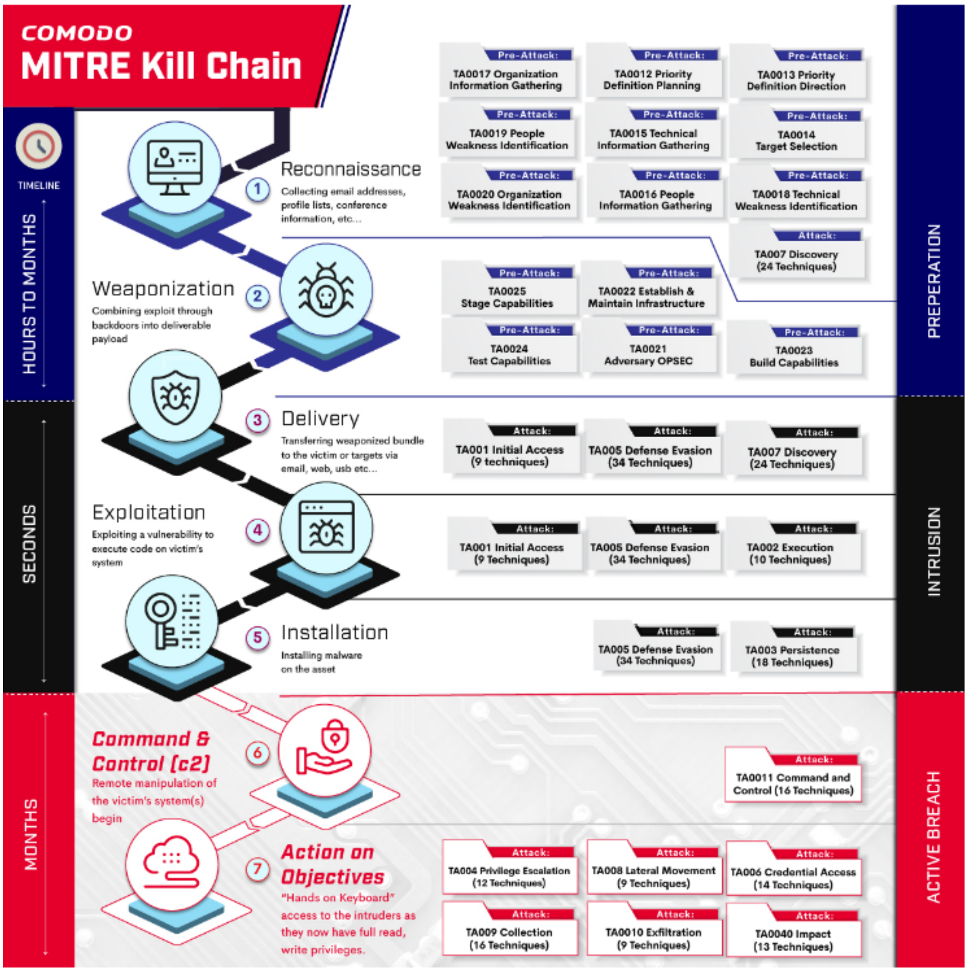


Figure 4.2: MITRE ATT&CK tactics and how long each phase takes. Not all techniques in this image are up to date, especially the Pre Attack techniques that do not exist now. However, for demonstration purposes, it is still a very good example. Image reference: https://techtalk.comodo.com/2020/08/27/comodo-mitre-kill-chain/

The second phase on this page is labeled as intrusion. Typically, this phase lasts only seconds. In the cyber kill chain, this phase includes delivery, exploitation, and installation, while in MITRE ATT&CK, it covers tactics from initial access to discovery, except for gaining persistence, which takes more time and falls into the active breach category. Progress through this phase is very rapid because the attacker usually has everything prepared, and it is almost an automated process requiring minimal to no human intervention.

The third phase, marked as an active breach, encompasses the command and control and action on objectives stages in the cyber kill chain. In MITRE ATT&CK, it includes all tactics from lateral movement to impact, as well as gaining persistence. This phase typically lasts for months since the attacker has already penetrated the network or system, and it takes a long time before they are detected.

4.2 The brief description of mitigations and detections

Another concept I frequently mention in my work is mitigation and detection, which I briefly discussed at the beginning of this paper. However, since these concepts are also outcomes of this work, I believe it is essential to delve into them in more detail.

The outcome of this work is a list of techniques along with their corresponding mitigations and detections for each technique. Based on this output, an organization can decide to follow this list and gradually implement protective measures that either detect an attacker using a specific attack technique or mitigate the risk of that attack being successfully carried out.

Detection involves implementing tools and methods within the organization's network, systems, or physical premises that can identify a particular technique and alert the organization to any malicious activity. By using such measures, the organization can quickly and effectively respond to ongoing attacks and prevent them from progressing further. Here is an example of five detections from the MITRE ATT&CK framework:

1. Command-Line Interface Monitoring

   - **Description:** Monitoring the use of command-line interfaces for unusual or unauthorized commands, which can indicate malicious activities such as script execution or system manipulation.

2. File Integrity Monitoring

   - **Description:** Tracking changes to critical system files and configurations to detect unauthorized modifications that may indicate tampering or persistence mechanisms.

3. Network Traffic Analysis
   - **Description:** Analyzing network traffic patterns to identify anomalous behavior, such as unexpected outbound connections or data exfiltration attempts.
4. User Behavior Analytics
   - **Description:** Leveraging machine learning and statistical models to establish a baseline of normal user activity and detect deviations that may signify compromised accounts or insider threats.
5. Endpoint Detection and Response (EDR)
   - **Description:** Deploying advanced EDR solutions to continuously monitor endpoint activities and detect suspicious behaviors, such as malware execution or lateral movement within the network.

Detection alone does not prevent an attack; it merely alerts us to its occurrence. Mitigation, on the other hand, reduces the risk of an attacker breaching our defenses. It involves patching vulnerabilities within the organization, strengthening security protocols, and employing measures that make it significantly harder for an attacker to succeed.

Mitigation strategies are comprehensive and include various approaches such as:

1. Patch Management
   - **Description:** Regularly updating and patching software and systems to fix known vulnerabilities.
2. Network Segmentation
   - **Description:** Dividing the network into segments to contain potential breaches and limit an attacker's movement.
3. Access Controls
   - **Description:** Implementing strict access controls to ensure that only authorized personnel have access to critical systems and data.
4. User Training
   - **Description:** Educating employees about security best practices and how to recognize potential threats.

5. Incident Response Planning

   - **Description:** Developing and regularly updating an incident response plan to quickly address and mitigate the impact of any security breaches.

By integrating both detection and mitigation strategies, an organization can create a robust security posture that not only identifies potential threats but also actively works to prevent successful attacks, ensuring a more resilient defense against cyber threats.

4.3 Parameters as an input

To ensure the proper functionality of the program, the user is required to input two different parameters. The first parameter specifies the geolocation where the organization is located. This is necessary because certain advanced persistent threat (APT) groups target specific geolocations. For instance, some APT groups based in Russia might primarily focus their attacks on European countries, making other parts of the world less of a target for them. Consequently, an organization would be interested only in the techniques used by groups that threaten its specific location.

The second parameter specifies the industry sector in which the organization operates. Similarly, some APT groups target specific industries based on their interests. Certain APTs might focus on sectors they perceive as most lucrative or likely to pay ransoms if an attack is successful. Examples of such sectors include government or finance.

After the user inputs these parameters on a user-friendly interface, which could be run locally on localhost, and clicks the "scan" button, the program queries the MITRE TAXII server for current data. At this stage, the program filters the current MITRE ATT&CK database to identify relevant groups. It selects groups whose descriptions mention targeting the geolocation specified by the user. From these filtered groups, it further selects those that also target the specified industry sector. This method effectively reduces the number of groups that pose a potential threat to the organization. In the subsequent phase, the individual techniques utilized by the filtered groups are obtained and processed in other parts of the program. Specifically, the corresponding mitigations and detections for these techniques are retrieved.

In these sections, I also modified the program's functionality to avoid querying the TAXII server every time. Instead, the program now retrieves data from the "enterprise-attack.json" file, which must be placed in the same directory from which the application is run. This file can be downloaded from the official MITRE ATT&CK GitHub, which is continually updated with the latest version. This change was primarily implemented to save time during the program's execution, as querying the TAXII server is very time-consuming, with each query taking up to four seconds. Accumulating such queries significantly extends the runtime, potentially reaching tens of minutes.

4.4 Reports as an input

In the event that an organization seeks to optimize the efficiency of identifying techniques that pose a threat, my program has the capability to process the outputs of analyzed reports from the MITRE TRAM tool in JSON format. An illustration of this tool is shown in the figure below 4.3. The user interaction required is minimal: the user needs to install the official MITRE TRAM tool, follow the official guide on GitHub, run the tool locally, and obtain a report from the detection or prevention tools they trust. The user should then upload these reports into MITRE TRAM and analyze them using this tool. The resulting output must be downloaded in JSON format and placed in the "TRAM_reports" folder of my program. During its execution, the program analyzes all files in this directory and selects techniques mapped by MITRE TRAM with a confidence level of at least 90%. These selected techniques are then added to the techniques used by groups that were previously filtered based on the specified parameters.

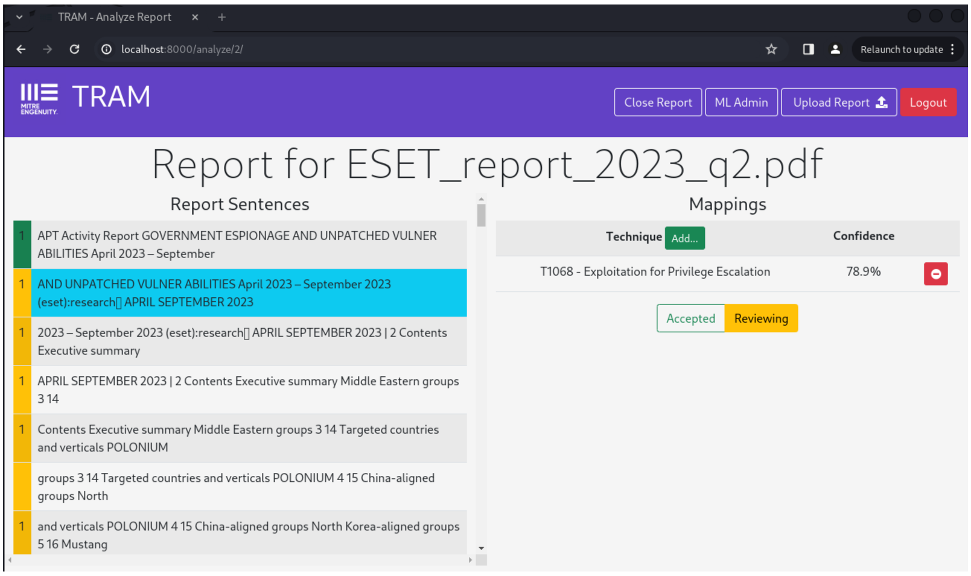


Figure 4.3: This image shows the analyzed report uploaded to MITRE TRAM. Notice the MITRE TRAM chunks the report into sentences that map with some probability to MITRE ATT&CK techniques.

4.5 The web application

During the implementation of my program, I concurrently developed a version that could be executed conventionally through the terminal. Subsequently, I initiated the development of a graphical interface version. However, recognizing the imperative of user-friendliness as a requirement, I opted to prioritize the continued development exclusively through the graphical interface.

The current operational model of the application entails the user depositing

MITRE TRAM reports in the designated TRAM_reports folder. Upon execution of the application, it selectively identifies techniques from the reports, specifically those flagged by MITRE TRAM with a probability of 90% or higher, employing a command-based mechanism.

```
python app.py
```

```
http://localhost:8080
```

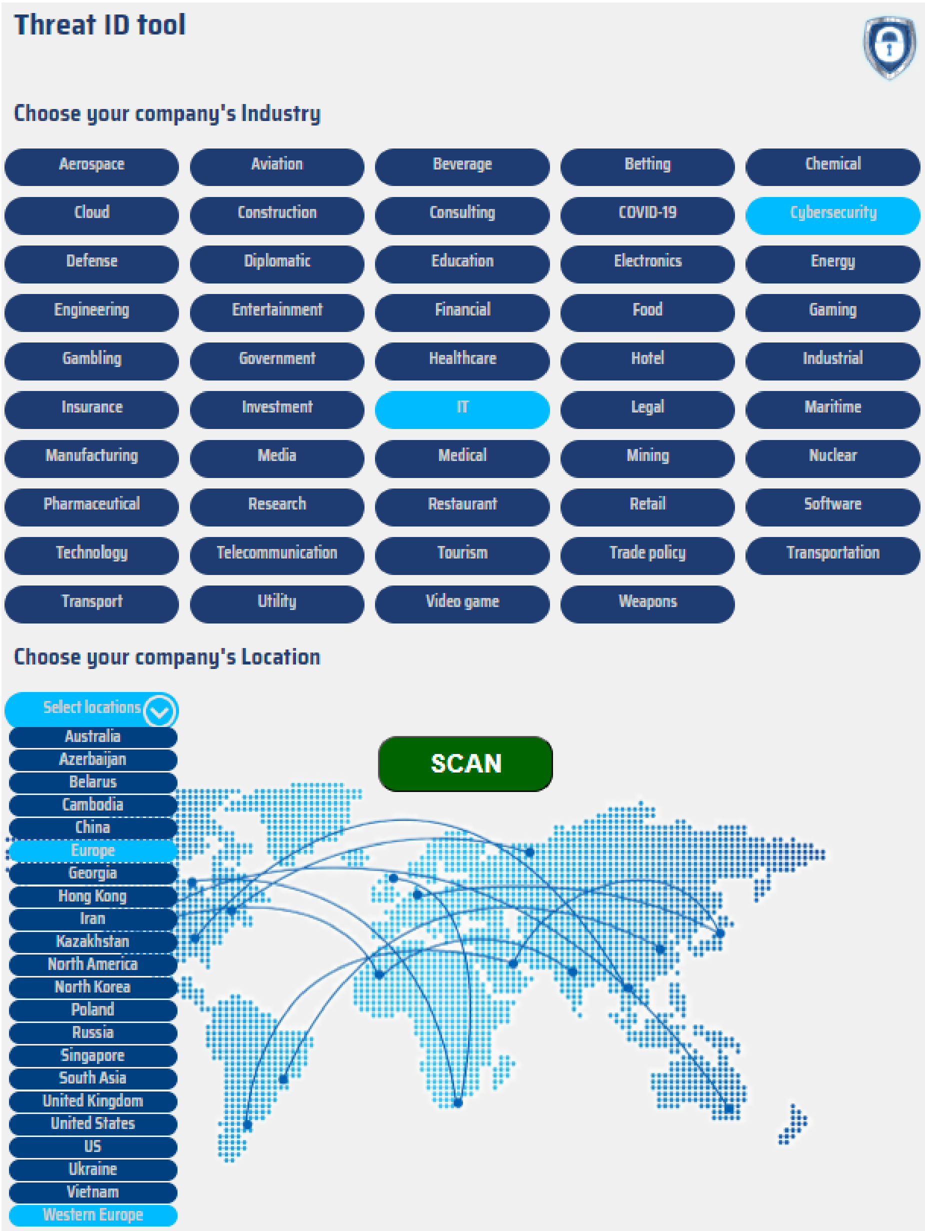


Figure 4.4: The web page is presented after the user enters localhost, showcasing the capability to select parameters through buttons and the option to execute the program using the "SCAN" button.

Subsequently, the user utilizes the web browser to access the localhost page where the corresponding webpage is actively hosted.

Upon navigating to the page, the user encounters a user-friendly interface (refer to the image 4.4) designed to evoke a sense of defensive purpose. I selected a color scheme of light gray and dark blue, with a shield logo in the top right corner to reinforce the defensive nature of the tool.

I considered including a fingerprint image and a pattern of ones and zeros to add a touch of mystery, but these elements did not integrate as well.

At the top of the page, the user can choose from various industry sectors that their organization might belong to. It is important to note that an organization can belong to multiple sectors, such as IT and cybersecurity, and the user can select multiple sectors without any limitation. Sector selection is achieved by clicking on the corresponding dark blue button, which then changes to light blue to clearly indicate that the sector is active.

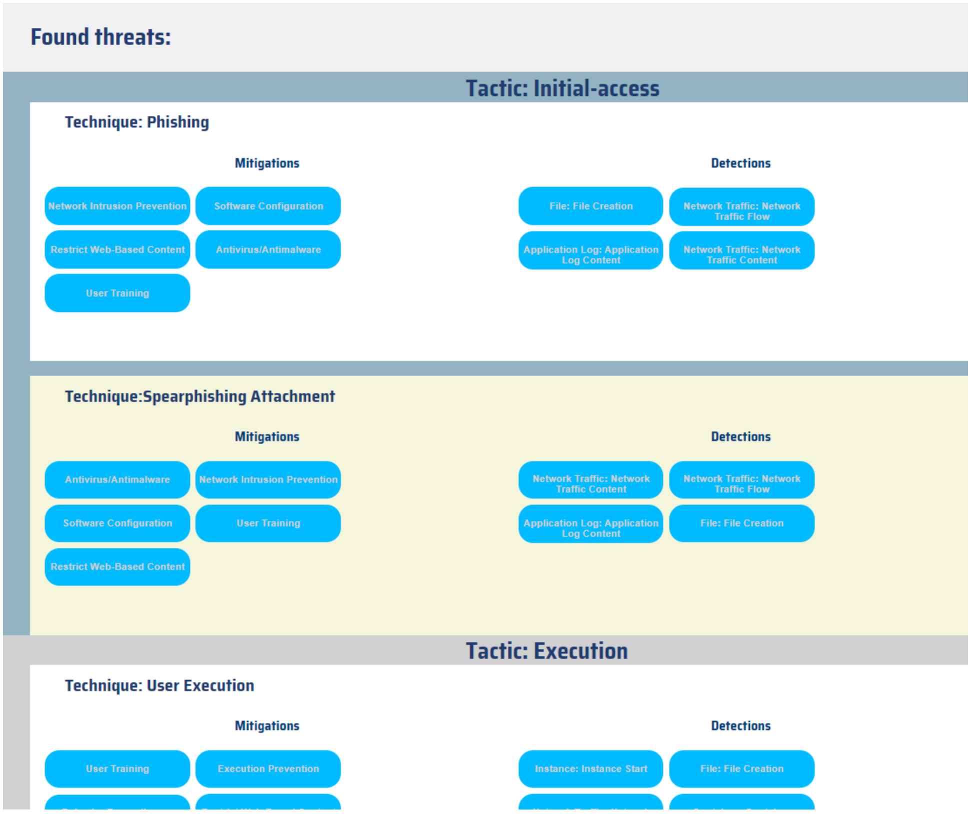


Figure 4.5: The second page is loaded after the completion of processes in the background. The user is given a user-friendly GUI with all relevant techniques, its possible mitigations, detections, and tactics they fall under.

The second part of the parameter selection is located further down the page next to a blue map of the world, symbolizing the choice of geolocations. The user selects geolocations using a scrollable button, which, when clicked, expands to display a list of geolocations. The user can then select the ones that apply to their organization. The chosen geolocations are highlighted in light blue, the same as for the industry selection.

After entering all the necessary information, the user can start the program by clicking a green button labeled "SCAN" (refer to Figure 4.4) at the bottom of the page. At this point, the program begins its operation, executing the main functions written in Python. The runtime can vary depending on the selected parameters, the number of parameters, and the volume of analyzed reports, potentially extending to several tens of minutes. Therefore, users should be prepared for a potentially lengthy process.

After the user waits for several minutes while the program processes the request, a blank page with a clock icon and the word "Loading" is displayed. Then, the second page with the techniques is loaded (Figure 4.5). This user-friendly page color-codes each technique based on its corresponding tactic, using a combination of blue-gray and light gray colors. Techniques are visually separated by alternating white and beige backgrounds, making it easier for the user to navigate the output provided.

The purpose of this design is to illustrate that each technique belongs to a specific phase or tactic.

Figure 4.6: The bottom of the web page shows two green buttons to download the techniques in JSON format and download all the selected mitigations and detections for each technique.

Once the user feels that the appropriate mitigations and detections for the selected techniques and tactics have been chosen, they will find two green buttons at the bottom of the page: "Download mitigations and detections" and "Download techniques.json", as shown in Figure 4.6.

Both buttons provide a comprehensive output of techniques but each interprets the results slightly differently. Clicking the "Download techniques.json" button downloads all the techniques listed on the page into a JSON file named "Techniques_to_mitigate.json", which can be imported into the MITRE ATT&CK Navigator. Upon downloading the file, the original MITRE ATT&CK Navigator page automatically opens, as shown in Figure 4.7.

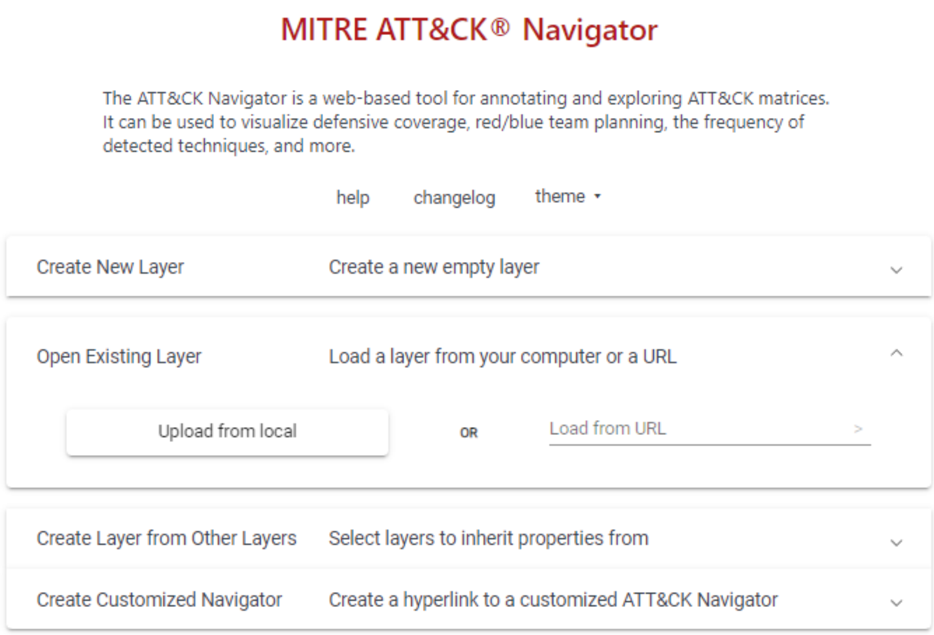


Figure 4.7: The Landing page of the MITRE ATT&CK Navigator. The user is able to upload a downloaded JSON file with techniques simple by clicking the "Upload from local" button and selecting the desired file he wants to check.

Here, the user can click on "Open existing layer", then "Upload from local", and upload the downloaded file. This tool visualizes each retrieved technique in red, allowing the user to easily see which tactic each technique belongs to and how they are organized sequentially. An example of this tool and the visualization of all filtered techniques is shown in Figure 4.8.

In contrast, the "Download mitigations and detections" button downloads an Excel file that includes only the techniques for which the user has selected some mitigations and detections at this stage. Unlike the previous button, which downloads all techniques, this button provides a download of only the selected techniques based on the chosen mitigations and detections. If no mitigations or detections are selected for a particular technique, that technique will not be included in the output. An example of such an output is shown in Figure 4.9.

Having this file downloaded, the user has full control over how they utilize it.

They can use it to guide their patching efforts, selectively delete or highlight specific techniques, or employ it in other ways to enhance their security posture.

One significant advantage of this approach is that each mitigation and detection in the Excel file is hyperlinked to the official MITRE ATT&CK website. This feature allows the user to quickly and easily access detailed information about any mitigation or detection they may be unfamiliar with.

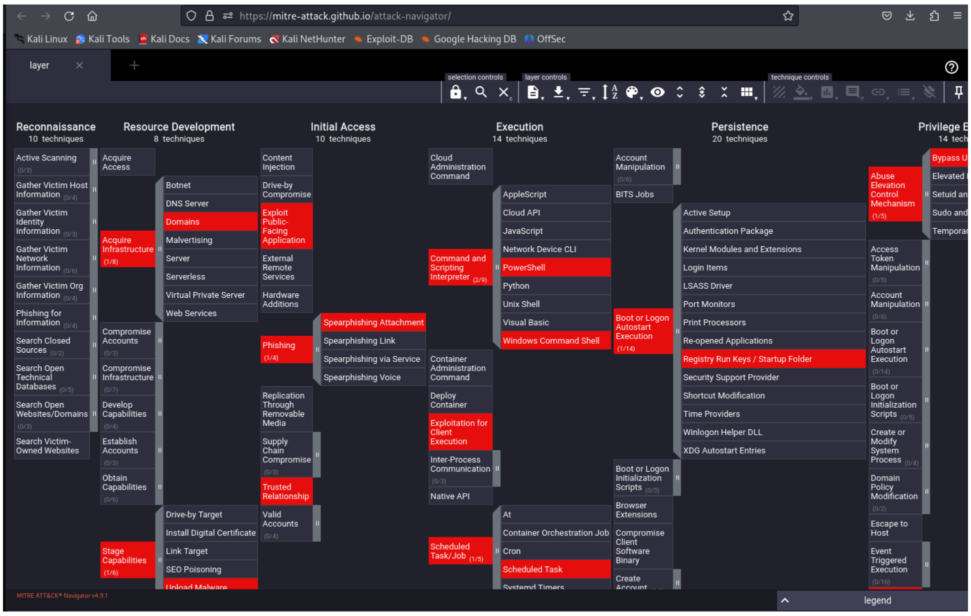


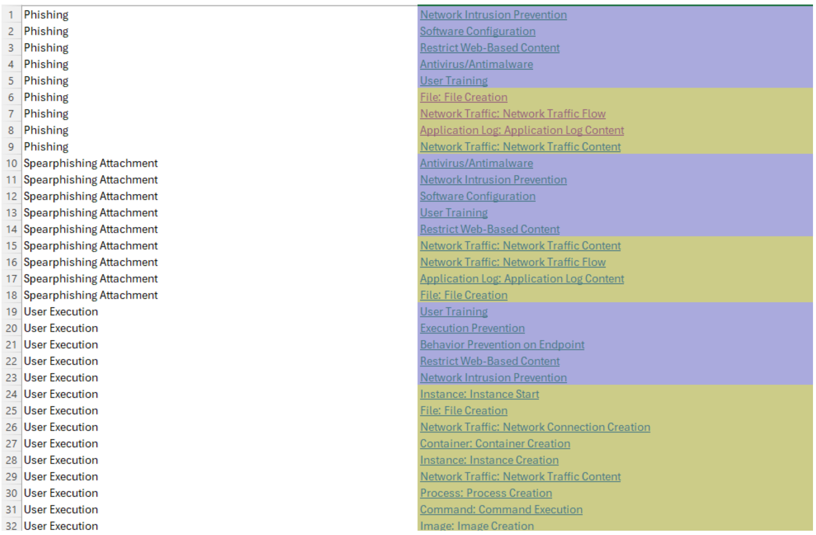
Figure 4.8: Sample uploaded JSON file containing techniques visualized in MITRE Navigator.

By simply clicking on a specific mitigation or detection, which includes a hyperlink, the user is promptly redirected to the corresponding page on the official MITRE ATT&CK website. There, they can delve into detailed descriptions, examples, and additional resources, which makes it easier to understand and effectively apply the techniques. This streamlined access to information facilitates efficient navigation and exploration of the entire MITRE ATT&CK knowledge base.

Moreover, the Excel file provides users with the flexibility to tailor their cybersecurity strategies to their specific needs and preferences. Users can utilize the comprehensive data in the file to develop customized approaches to mitigating threats and detecting potential intrusions. For instance, users can modify or add to the existing mitigation strategies to address unique organizational requirements or emerging threats.

An illustration of the loaded page after clicking on a mitigation named "User Training" is shown in Figure 4.10. This example demonstrates how users can access detailed information on mitigations and detections directly from the MITRE ATT&CK website, enhancing their ability to make informed decisions about their cybersecurity practices.

Another advantage is that the user can choose to work exclusively with the second page and the Excel file. If they find it unnecessary or do not prefer to use it, they can simply disregard it.



1	Phishing	Network Intrusion Prevention
2	Phishing	Software Configuration
3	Phishing	Restrict Web-Based Content
4	Phishing	Antivirus/Antimalware
5	Phishing	User Training
6	Phishing	File: File Creation
7	Phishing	Network Traffic: Network Traffic Flow
8	Phishing	Application Log: Application Log Content
9	Phishing	Network Traffic: Network Traffic Content
10	Spearphishing Attachment	Antivirus/Antimalware
11	Spearphishing Attachment	Network Intrusion Prevention
12	Spearphishing Attachment	Software Configuration
13	Spearphishing Attachment	User Training
14	Spearphishing Attachment	Restrict Web-Based Content
15	Spearphishing Attachment	Network Traffic: Network Traffic Content
16	Spearphishing Attachment	Network Traffic: Network Traffic Flow
17	Spearphishing Attachment	Application Log: Application Log Content
18	Spearphishing Attachment	File: File Creation
19	User Execution	User Training
20	User Execution	Execution Prevention
21	User Execution	Behavior Prevention on Endpoint
22	User Execution	Restrict Web-Based Content
23	User Execution	Network Intrusion Prevention
24	User Execution	Instance: Instance Start
25	User Execution	File: File Creation
26	User Execution	Network Traffic: Network Connection Creation
27	User Execution	Container: Container Creation
28	User Execution	Instance: Instance Creation
29	User Execution	Network Traffic: Network Traffic Content
30	User Execution	Process: Process Creation
31	User Execution	Command: Command Execution
32	User Execution	Image: Image Creation

Figure 4.9: The Illustration of opened Excel output with all the listed selected techniques and their corresponding mitigations colored with blue and detections colored green inside.

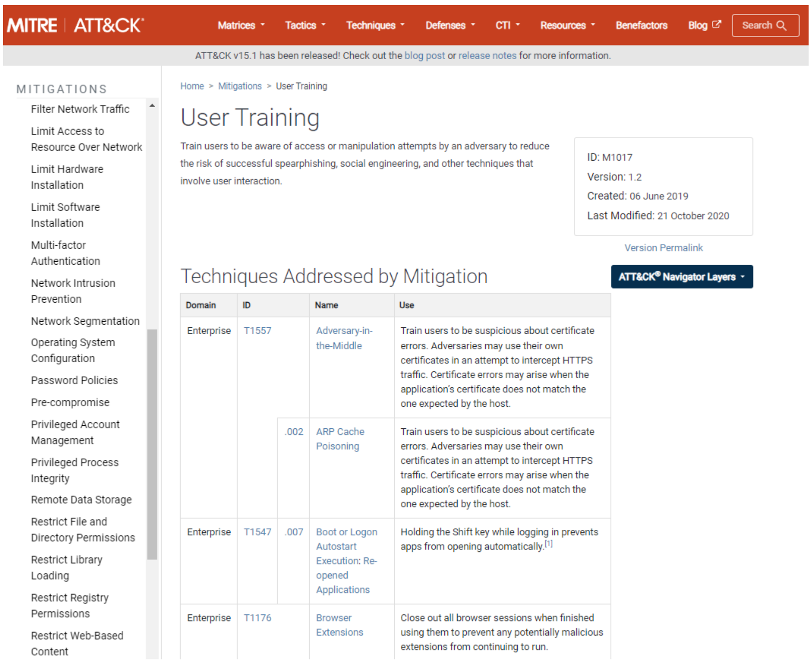


Figure 4.10: This image shows the page that is opened after clicking on the link in Excel under the "User training" technique. The user can then study in detail whatever he wants to know about this mitigation.

The program operates deterministically in its current state, ensuring that it consistently produces the same result for every unique input. For example, if the user accidentally deletes a table or closes the page due to negligence, they can easily restart the program with the same parameters and input reports to achieve identical results.

This deterministic behavior eliminates the need to save the application's current state to a file and manage the reading and writing of results. The user can rely on the program's ability to reproduce results without the need for complex data storage or management strategies.

This feature provides significant reassurance to users, as they can confidently work with the program knowing that any unintended actions or disruptions can be quickly resolved by restarting the program with the same inputs.

4.6 Working with the output

Furthermore, it is possible to work with the output of the tool or with an Excel spreadsheet that lists all the obtained techniques along with their mitigations and detections. At this point, it is up to the user, typically a cybersecurity specialist, to start implementing those mitigations and detections that appear most critical based on their organization's risk analysis.

Hrozba	Aktivum	Zdroj	Úroveň rizika
Krádež médií nebo dokumentů	Data o zákaznících	*e-shop*	7
	Nahrávky hovorů	*server*	7
Krádež zařízení	Firewall	*server*	7
	Aktivní síťové prvky	*router*	7
	Mobilní zařízení		7
Vyzrazení	Cenové nabídky	*e-shop*	8
	Dokumentace	*server*	8
	Interní postupy	*server*	8
	Data o zákaznících	*e-shop*	8
	Data o zaměstnancích	*server*	8
	Obchodní tajemství	*server*	8
Data pocházející z nedůvěryhodných zdrojů	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
Chybné fungování aplikačního prog. vybavení	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
Chyba používání	Pasivní síťové prvky	*rozvaděč*	7
	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
	Antivir		7
Zneužití oprávnění	Zálohy dat	*server*	7
	Data o zákaznících	*e-shop*	7
	Data o zaměstnancích	*server*	7
	Nahrávky hovorů	*server*	7
	Firewall	*server*	7
	Aktivní síťové prvky	*router*	7
	IP kamery		7
	IBM server		8
	Operační systémy	*server, PC*	7
	MS SQL Databáze	*server*	8
	MS Dynamics CRM	*server*	8
	Antivir		7
	MS Exchange server	*server*	7
Nedostatek personálu	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7

Figure 4.11: This figure illustrates a completed visual representation of risk analysis, akin to the output that an organization utilizing my tool might achieve. The image demonstrates how each identified threat is assigned a level of criticality, which the organization can then follow and adhere to when implementing mitigations and detections. Image reference: [1].

The specialist will select techniques that closely align with the critical issues identified in the risk analysis. Based on the level of criticality, they can prioritize what to address first, decide which tasks to allocate more time to, or determine if certain implementations can be entirely skipped if deemed non-essential for the organization.

In the figure 4.11 is an example of what an organization's risk analysis might look like. This image is taken from the thesis of a student [1], which focuses on the creation of risk analyses and proposes subsequent necessary steps leading to the implementation of an information security management system. For the purposes of this thesis, this figure is illustrative and demonstrates the potential output of an organization's risk analysis.

The first column in the figure lists the threats to the organization, the second column lists the assets, the third column lists the sources, and the fourth column provides the risk level, typically rated from 1 to 9. The figure shows a specific example. Consider the first threat, named "Theft of media or documents", which has a risk level of 7, and the third threat, "Disclosure", which has a risk level of 8. The organization should initially focus on mitigations and detections related to the technique most associated with disclosure, such as user Phishing for information. In this manner, the organization can proceed with patching or implementing detection systems and methods to cover its vulnerabilities as efficiently and swiftly as possible.

4.7 The program in the background: HTML, CSS and Python in the backend

When the "SCAN" button is clicked, a JavaScript function is triggered. This function collects the selected parameters (industries and locations) and sends them as a POST request in JSON format to the Flask server's main function endpoint.

Upon receiving the POST request at the main function endpoint, the Flask application extracts the selected industries and locations from the request's JSON payload and begins processing the data. Initially, it fetches relevant groups by calling the getGroupsByParams.relevant_groups_for_indu stries function, which retrieves groups pertinent to the selected industries and locations.

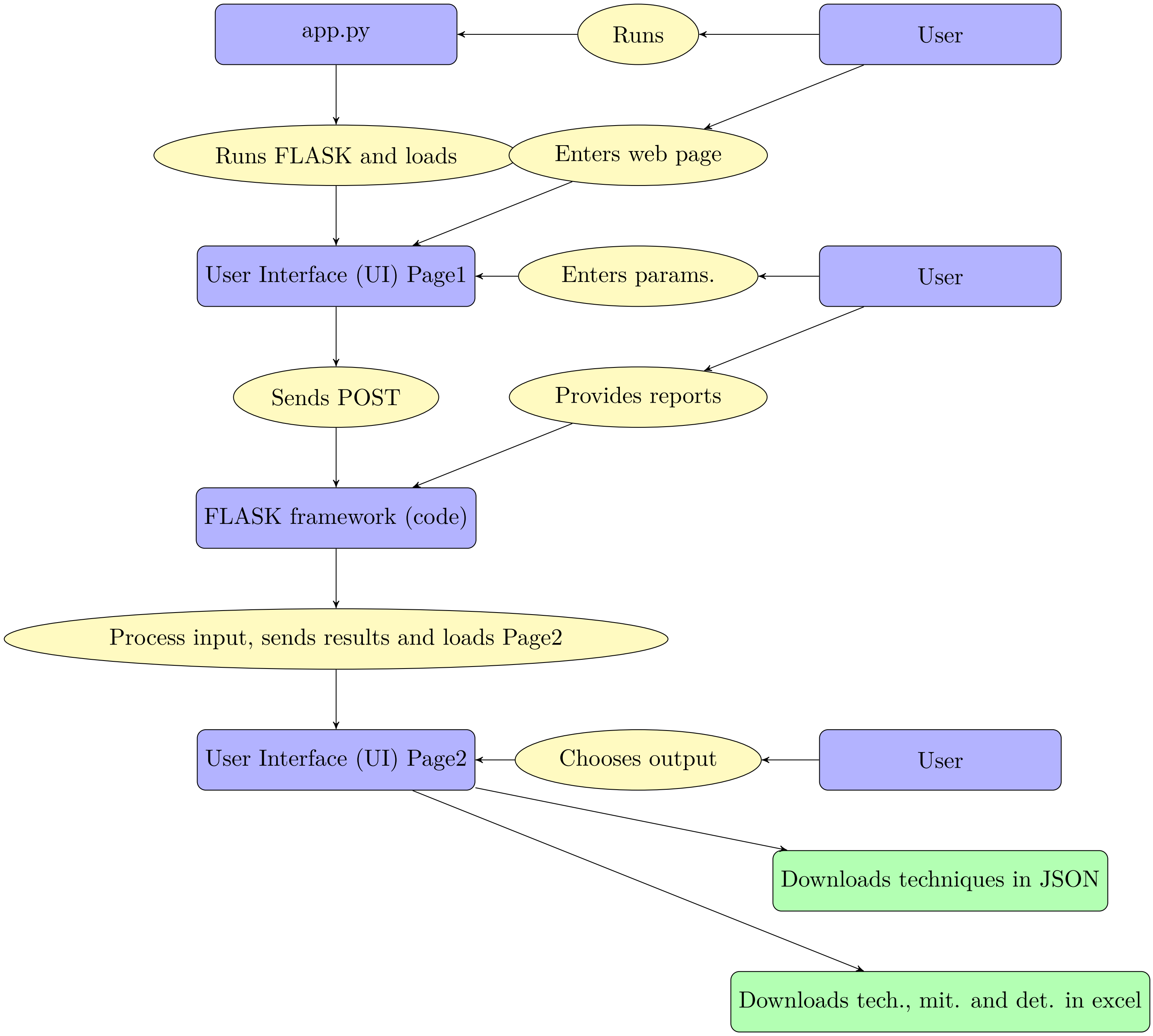
Next, the application fetches techniques used by these groups from the MITRE ATT&CK database using the getTechniquesByGroups.techniques _used_by_group2 function. Additionally, techniques are retrieved from MITRE TRAM's reports via the getTechniquesFromReports.getTechniques FromReports function. These techniques from both the database and the reports are combined into a single list. Detailed information about these techniques is then obtained using the getTechniquesByGroups.getTechniquesInfo function. This comprehensive list of techniques is saved to a JSON file using the js.createAndSaveJsonFile function.

Subsequently, the application reads the saved JSON file (Techniques_to _mitigate.json) and loads its content. For each technique in the file, additional information such as mitigations and detections is retrieved using the get_mitigations_for _technique and get_detections_for_technique functions. This collected information is structured into a list of dictionaries containing the technique name, mitigations, detections, and tactic.

The final list of techniques and their mitigations and detections is returned as a JSON response to the front-end. The front-end JavaScript receives this

JSON response and dynamically updates the user interface to display the techniques along with their mitigations and detections.

This process involves creating and inserting HTML elements into the DOM to present the data in a readable and interactive format, such as buttons and links for mitigations and detections. The process is shown on the diagram below.



Additionally, the user can download the techniques information as a JSON file by clicking a dynamically created button labeled "Download techniques.json." The interface also provides functionality for downloading the mitigations and detections as an Excel file, enhancing the usability and accessibility of the information for the user.

Chapter 5
Conclusion

The goals I had at the beginning of this project were rather clear: improve the efficiency of data processing, make user-friendly outputs, and make the outputs from Excel capable of visualizing and easily manipulating the output data. Additionally, and most importantly, simplify the lives of organizations that could be targets of APT groups. In fact, the effort went hand in hand with simplifying the complex threat analysis and mitigation of Advanced Persistent Threat groups, especially in view of simplifying the task. Protection against such threats is very important but not trivial, so the tool had to be made to reduce the complexity and focus on the most important aspects.

Special attention was paid to APT attacks. Advanced Persistent Threats are complicated and persistent threats to the organization. APTs are a type of cyber threat where a highly skilled and well-funded adversary gains unauthorized access to a network and stays there, mostly undetected, for a long time. More often, their primary goal is usually to steal sensitive data, disrupt operations, or cause damage to the target organization. Unlike other opportunistic cyber-attacks, APTs are planned and tailored to exploit specific vulnerabilities within the target infrastructure.

APTs make use of a range of tactics, techniques, and procedures to achieve their objectives. This could include spear phishing for gaining initial access, custom malware deployment to establish a foothold, lateral movement to expand control inside the network, and exfiltration of sensitive data. These threats require organizations to implement robust and comprehensive security measures because they are very complex and persistent.

APTs are really clever and use a lot of techniques. To make life easier for an organization, I can will MITRE ATT&CK. There, I can find out what the groups are doing and how they behave. Moreover, it is continuously updated. I explored what MITRE is about, the philosophy behind it, and how it can be used and found out that it can be used programmatically.

The MITRE ATT&CK is a detailed knowledge base of adversarial tactics and techniques seen in real-world cyber incidents. Within the MITRE ATT&CK framework, tactics represent the adversary's technical goals during an attack, such as initial access or maintaining persistence, while techniques are specific ways adversaries complete these objectives. Understanding and using the MITRE ATT&CK framework enables organizations to better prepare for and defend against APTs.

Detection and response to APTs involve continuous monitoring and advanced threat intelligence. Detecting unusual activities indicative of APT presence relies on security information and event management systems and endpoint detection and response tools. Threat hunting, an activity security teams engage in to look for indicators of compromise based on the latest threat intelligence and attack patterns outlined in the MITRE ATT&CK framework, should become part of standard practices.

APTs are much more serious and present a catastrophic impact on the organization's operations, reputation, and bottom line; organizations must make increased efforts to thwart these threats. Preventive measures include rigorous network segmentation, regular patch management, comprehensive employee training on phishing and social engineering, and implementing a principle of least privilege to minimize the impact of compromised accounts.

In this work, I specifically consider suggesting appropriate steps that an organization has to take to perform adequate hardening and extricate itself from the threats from these groups based on publicly available information. During my research, I identified that APT groups do not attack all industries indiscriminately but specialize in the attack against selected areas or segments of industries. This crucial finding means that organizations can significantly enhance their security posture by focusing on mitigating threats specific to their industry and geographical location.

Analyzing the data from the MITRE ATT&CK framework, I identified patterns indicating that these threat actors concentrate their efforts on particular sectors, such as finance, healthcare, or critical infrastructure, depending on their goals and capabilities. This targeted approach allows APT groups to exploit industry-specific vulnerabilities more effectively, thus requiring tailored defense strategies for each sector.

Given this insight, I propose a methodology that begins with a thorough internal risk analysis being conducted by the organization to understand its unique threat landscape. The application I developed retrieves industry-specific and geolocation-specific parameters to retrieve the most relevant and current data from the MITRE MATRIX via the TAXII server using STIX. It then identifies the groups that offer the most significant threats and lists the techniques these groups frequently utilize.

Many ideas were developed and considered with a view to attaining these goals. Of critical importance was the idea of the use of MITRE TRAM and Navigator to improve the analysis process. MITRE TRAM offered an organized form of data analysis capability, while Navigator offered data visualization and mapping, both of which were critical for the interpretation and reaction to threat intelligence.

The implementation of these tools required developing the best ways to process the input data and produce user-friendly outputs. There was a need to develop strong processes that could handle parameters and reports, along with a user interface that could display results clearly. I have also been in tricky situations where many options came at once, such as the proper tools and methods to use for analysis such as MITRE TRAM or rcATT, which had to be taken with care to ensure that there were good results.

This project met the initial goals through the integration of MITRE TRAM, Navigator, and MITRE Matrix as the building blocks and getting data from the MITRE database using Python. Data processing parameters and report generation functions have been implemented effectively. Outputs were not only user-friendly but also suitable for data visualization and Excel manipulation, though complex by their nature and long to process.

Other areas that the tool could further be enhanced on are smarter filters to enhance the selection of parameters and thus make the tool more flexible for use in different organizations. Additionally, increasing report processing based on various confidence intervals, such as excluding data below a 90% confidence level, will increase the precision of threat assessments.

Further optimization efforts are also necessary to increase the speed, accuracy, and general efficiency of the tool. This refinement process shall ensure that the tool remains capable of answering the changing needs that organizations face from APTs and will be in a position to provide highly effective capabilities for mitigation and intrusion detection.

This project has been very successful, as per its objectives, to provide a user-friendly and efficient tool for data analysis and assessment of threats. However, there is a need for continuous improvements; therefore, future iterations shall focus on enhancing filtering capabilities, optimizing report processing, and generally improving efficiency to serve organizational security needs.

Bibliography

[1] M. Konečný *GAP ANALÝZA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ.* Vysoké učení technické v Brně, 2018.

[2] *MITRE, "Mitre att&ck," https://attack.mitre.org/, 2018,* [Online; accessed 20-January-2024].

[3] S. Barnum *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* The MITRE Corporation.

[4] *TAXII: An Overview* `https://taxii.mitre.org/about/documents/TAXII_Overview_briefing_July_2013.pdf`. The MITRE Corporation, 2013, Accessed on May 24, 2024.

[5] R. AI-Shaer, J. M. Spring, E. Christou, *Learning the Associations of MITRE ATT&CK Adversarial Techniques.* Institute of Electrical and Electronics, 2020.

[6] Y. Kim, I. Lee, H. Kwon, K. Lee and J. Yoon, *BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework.* Institute of Electrical and Electronics Engineers, November 2023.

[7] A. Kuppa, L. Aouad and N.-An_le_Khac *Linking CVE's to MITRE ATT&CK Techniques* Association for Computing Machinery New York, NY, United States, August 2021.

[8] O. Grigorescu, A. Nica, M. Dascalu and R. Rughinis *CVE2ATT&CK BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques.* MDPI, August 2022.

[9] Chukwu, Ch. Jeremiah *Leveraging the MITRE ATT&CK Framework to Enhance Organizations Cyberthreat Detection Procedures.* Carleton University, 2023.

[10] B. E. Strom, Doug P. Miller, A. Applebaum, K. C Nickels, Adam G. Pennington, Cody B. Thomas *MITRE ATT&CKr: Design and Philosophy.* The MITRE Corporation July 2018.

[11] V. Orbinato, M. Barbaraci, R. Natella, and D. Cotroneo *Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study.* Institute of Electrical and Electronics Engineers, December 2022.

[12] W. Xiong, E. Legrand, O. Åberg and R. Lagerström *Cyber security thread modeling based on the MITRE Enterprise ATT&CK Matrix.* Softw Syst Model 21, 157–177 (2022). https://doi.org/10.1007/s10270-021-00898-7, June 2021.

[13] E. R. Ling and M. Ekstedr *Generating Thread Models and Attack Graphs based on the EIC 61850 System Configuration description Language.* KTH Royal Institute of Technology, 28 April 2021.

[14] S. Choi, J. Yun and B. Min *Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets.* CSET @ USENIX Security Symposium, August 2021.

[15] S. Yoder, *"Automating mapping to att&ck: The threat report att&ck mapper (tram) tool," https://medium.com/mitre-attack/automating-mappingto-attack-tram-1bb1b44bda76,* 2019.

[16] S. Moskal, S.J.Yang *Translating Intrusion Alerts to Cyberattack Stages using Pseudo-Active Transfer Learning (PATRL).* Institute of Electrical and Electronic Engineers, 2017.

[17] V, Legoy, M. Caselli, Ch. Seifert, A. Peter *Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports.* M.S. thesis, Dept. Elect. Eng., Math., Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2019.

Appendix A

Obsah přiloženého média

```
readme.txt ................................installation manual
├─ src .....................................source directory
│  ├─ static ................................directory for the web application
│  ├─ templates ..............................directory with images
│  ├─ TRAM_REPORTS.............directory for uploading analyzed reports from MITRE T
│  ├─ app.py .....................................main program
│  ├─ latex ..................directory for LaTeX source codes
│  ├─ enterprise-attack.json ...........current downloaded file from MITRE GitHub (t
│  └─ *.py .................. other necessary program files
└─ generated
   └─ thesis.pdf ...................PDF version of the thesis
```