jamk.fi

Threat Detection Gap Analysis Using MITRE ATT&CK Framework

Jarkko Kinnunen

Master's thesis
February 2022
Information and Communications Technology
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Kinnunen Jarkko	Master's thesis	February 2022
		Language of publication: English
	Number of pages 70 (79)	Permission for web publication: yes

Title of publication

Threat Detection Gap Analysis Using MITRE ATT&CK Framework

Degree program

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Saharinen Karo, Kokkonen Tero

Assigned by

Enfo Oyj

Abstract

The volume and impact of security incidents against organizations are increasing globally. Each organization needs to understand what assets they are defending and what detection tools they have in place to detect future cyber-attacks. One of the main challenges organizations face in the fight against cyber-attacks is the lack of visibility and understanding of how these attacks begin, spread, and evolve. In addition, organizations lack information on what threats can be identified with existing security solutions.

The thesis aimed to determine whether using the MITRE ATT&CK framework can improve the organization's knowledge of their security solutions threat detection capabilities. The research method used in the thesis was Design Science Research.

The research consisted of two different phases. The first step was to map threat detection capabilities from the selected security products to the MITRE ATT&CK framework. The thesis assigner uses the chosen security products to provide continuous security services to their clients. The security solutions detection capabilities were illustrated at a general level and mapped to the MITRE ATT&CK framework using public sources. In the second phase, a gap analysis of the threat detection capabilities of the security solutions was conducted. The results were compared to four different threat intelligence reports of adversaries' TTPs seen in the wild.

The research results were evaluated using a questionnaire within the organization that assigned the research. Based on the findings, threat detection gaps could be identified using the MITRE ATT&CK framework from the chosen security solutions. The research results can be used to develop the organization's defense capabilities.

Keywords/tags

Design science research, gap analysis, MITRE ATT&CK, threat detection

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kinnunen Jarkko	Opinnäytetyö, YAMK	helmikuu 2022
		Julkaisun kieli: englanti
	Sivumäärä: 70 (79)	Verkkojulkaisulupa myönnetty: kyllä

Työn nimi

Threat Detection Gap Analysis Using MITRE ATT&CK Framework

Tutkinto-ohjelma

Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Saharinen Karo, Kokkonen Tero

Toimeksiantaja(t)

Enfo Oyj

Tiivistelmä

Organisaatioihin kohdistuvien tietoturvapoikkeamien määrä ja vaikutus kasvavat maailmanlaajuisesti. Jokaisen organisaation on tärkeää ymmärtää, mitä he puolustavat ja mitä havaitsemistyökaluja heillä on käytössä tulevien kyberhyökkäysten havainnoimiseksi. Organisaatioiden suurimpia haasteita kyberhyökkäyksien torjunnassa ovat näkyvyyden ja ymmärryksen puute siitä, miten nämä hyökkäykset alkavat, leviävät ja kehittyvät. Lisäksi yrityksiltä puuttuu ymmärrystä nykyisien tietoturvatuotteiden kyvyistä havaita uhkia.

Opinnäytetyön tavoitteena oli selvittää, voiko MITRE ATT&CK-viitekehystä käyttää organisaation tietämyksen parantamiseen tietoturvatuotteiden uhkien havaitsemiskyvyistä. Opinnäytetyössä käytetty tutkimusmenetelmä on suunnittelututkimus.

Tutkimus koostui kahdesta eri vaiheesta. Ensimmäisessä vaiheessa mallinnettiin uhkien havainnointikyvykkyydet valituista tietoturvatuotteista käyttäen MITRE ATT&CK-viitekehystä. Valitut tietoturvatuotteet ovat samoja, joita opinnäytetyön toimeksiantaja käyttää tarjotessaan asiakkailleen jatkuvia tietoturvapalveluita. Tietoturvaratkaisujen tunnistusominaisuudet mallinnettiin yleisellä tasolla käyttäen julkisia lähteitä. Toisessa vaiheessa työkalujen kyvykkyyksistä laadittiin GAP-analyysit, joissa niitä verrattiin neljään eri uhkatietoraporttiin hyökkääjien eri hyökkäysvaiheista.

Tutkimustuloksia arvioitiin kyselytutkimuksella, johon osallistui valittu joukko työn toimeksiantajan henkilöstöstä. Tutkimustuloksien perustella MITRE ATT&CK-viitekehyksen avulla voitiin havaita aukkoja valittujen työkalujen uhkien havainnointikyvyistä. Tutkimustuloksia voidaan käyttää organisaation puolustuskyvykkyyksien kehittämisessä.

Avainsanat (asiasanat)

GAP-analyysi, MITRE ATT&CK, suunnittelututkimus, uhkien havaitseminen

Muut tiedot (Salassa pidettävät liitteet)

Contents

Figures

Tables

Terms and abbreviations

APT	Advanced persistent threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CASB	Cloud Access Security Broker
CISA	Cybersecurity and Infrastructure Security Agency
FFRDC	Federally funded research and development center
IBM	International Business Machines Corporation
IoC	Indicators of compromise
JSON	JavaScript Object Notation
LotL	Living off the Land
MAD	MITRE ATT&CK Defender
MD5	Message-digest 5 algorithm
MSSP	Managed Security Service Provider
PsExec	Windows tool to execute a command-line process on a remote machine
SaaS	Software as a Service
SHA-2	Secure Hash Algorithm 2
SIEM	Security Information and Event Management
SMB	Server Message Block
Tor	The Onion Router
TTPs	Tactics, techniques, and procedures
VPN	Virtual Private Network
WMI	Windows Management Interface

1 Introduction

Cyber incidents and their impact on organizations are growing on a global scale. According to IBM (2021), the average total cost of a data breach in Scandinavia is USD 2.67 million. Currently, all kinds of organizations are targeted by adversaries. Especially some of the trending cyber-attacks cost organizations more. According to F-Secure (2021), in August 2021, ransomware attacks have been trending 300% upwards every month since August 2020. In every organization, it is crucial to know what they are defending inside the company and what detection tools are in place to discover upcoming cyber-attacks (F-Secure, 2021).

Especially ransomware is trending, in VirusTotal report, around 130 different families associated with ransomware were active in 2020 and the first half of 2021. Different ransomware families were grouped by 30,000 clusters of malwares that looked and operated similarly. (Diaz, 2021) Coinciding cyber-attacks are getting more complex and harder to detect. New adversaries' tactics, techniques, and procedures (TTPs) constantly evolve (Microsoft, 2020). Adversaries use more complex TTPs when deploying Ransomware and related malware. This is due popularity of Ransomware kits. These kits are one of the many attack kits designed to enable low-skill attackers to perform more sophisticated attacks. Many of these tools can be purchased in the dark web markets. (Microsoft, 2021a)

One of the main challenges to organizations and defenders stopping ransomware attacks is the lack of visibility and knowledge of how these attacks start, spread, and grow (Diaz, 2021). There is no single security solution or tool that can protect organizations. There are too many attack methods available adversaries to use. (McGuiness, 2001) According to Hyppönen (2021), it is difficult to defend against an unknown enemy. If we want to protect our information systems, we need to know who we are fighting against and why they are attacking. If we do not know our enemies, protection is desperate. (Hyppönen, 2021, 35) The assigner of this thesis was Enfo Oyj, a Finnish Managed Security Service Provider (MSSP). The motivation of the thesis assigner was to increase understanding of their security solutions threat detection capabilities and a general understanding of the MITRE ATT&CK framework inside the company.

2 Research method

2.1 Objectives and structure of the thesis

This thesis aims to explore and cover how organizations can understand their current security solutions' threat detection capabilities and improve possible knowledge gaps. The thesis aim is to answer one main research question:

- Can gap analysis using the MITRE ATT&CK framework improve an organization's understanding of its threat detection capabilities?

Three sub-research questions are created to answer the main research question:

- Is the MITRE ATT&CK framework suitable for conducting the gap analysis?
- Are the identified gaps useful to improve the detection capabilities?
- Is it possible to identify and detect gaps from commercial security solutions?

The scope of this thesis is limited to evaluating the detection capabilities of the selected security solutions. The security solutions chosen are:

- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud (Windows machines)

The security solutions are chosen for this thesis because the company that assigned the work provides managed security services using these tools to its customers. As a result, the company should better understand its current threat detection capabilities. The company can use this information to improve existing services or create new services. In addition, the author has a long experience and history with the selected tools, and there is enough information publicly available to evaluate the tool's detection capabilities with the required accuracy for the thesis. The research goal is not to produce 100% pinpoint accuracy for the detection capabilities of the selected security solutions. The goal is to give the organization a better understanding of evaluating detection capabilities of different solutions for future use cases.

Another key point of the thesis is to define tools and processes to help organizations document and illustrate their threat detection capabilities. The MITRE ATT&CK

framework is selected as the tool that demonstrates and documents the threat detection capabilities of the chosen security solutions. According to CISA (2021), the ATT&CK framework can be used to: assess security tool capabilities, identify defensive gaps, organize detection, or threat hunting. Additionally, in Cybersecurity Insiders (2021) survey, 82% of the respondents knew the ATT&CK framework. The author wanted to use a known existing framework and contribute new knowledge. Security solutions and methods in the research can additionally be used in threat hunting and forensics capabilities, but they are not in the scope of this thesis.

The first part of the thesis introduces the reader to the topic and research problem. Chapter two gives more context about the research methods and research goals. The third chapter introduces the theory used based on this thesis. The theoretical background demonstrates why the used artifacts are created, and the fourth chapter illustrates how the artifacts are designed and implemented. The fifth chapter presents the practical use of the artifacts and how the gap analysis is conducted. Finally, the conclusions and discussion for future research are given.

2.2 Research methodology

This thesis uses Design Science Research Methodology for Information Systems Research method. According to Johannesson & Perjons (2014), "*Design science is the scientific study and creation of artefacts as they are developed and used by the people with the goal of solving practical problems of general interests*" (p. 7). The design science research model focuses on contributions to new and actual knowledge. The process of creating and evaluating the artifacts is illustrated in Figure 1, quoted from (Vaishnavi, 2019). The structure of the thesis is built based on this Figure.

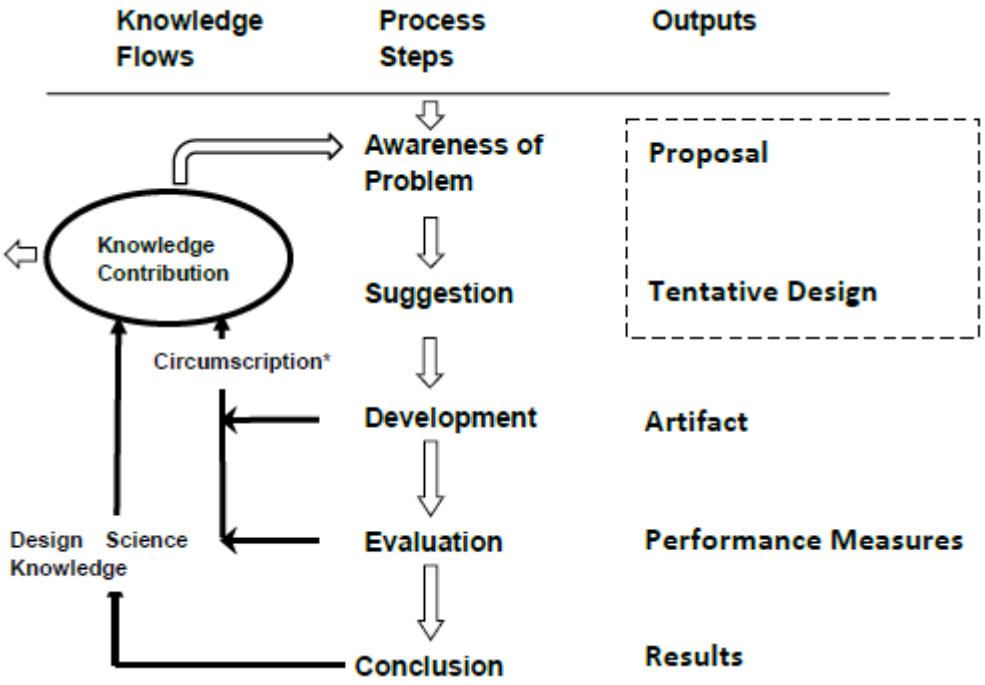


Figure 1. Design Science Research Process Model

In design science, research artifacts are objects made by individuals. Artifact's objective is to address or ideally mitigate or solve a practical problem. (Johannesson & Perjons, 2014, 7.) According to Vaishnavi (2019), "*Design means 'to invent and bring into being.' Thus, design deals with creating a new artifact that does not exist.*" To get answers to the research question, two new artifacts are developed:

1. Design and create defensive detection capabilities artifacts for commercial products using MITRE ATT&CK framework
2. Design and create adversaries TTPs artifacts from publicly available threat intelligence reports

The artifacts are created to contribute value and improvement to the Information Security community. More specifically, specialists and managers are responsible for defending organizations' cybersecurity. The created artifacts are objects to answer the research questions. The defensive artifacts are the documented detection capabilities of security solutions. The adversary artifacts are TTPs information from threat intelligence reports. According to Mavroeidis, Hohimer, Casey, & Jøsang (2021), threat intelligence information can provide organizations a better situational

awareness to prioritize and help organizations defend against the most relevant threats.

Contribution in this thesis is classified to Improvement research category in the design science research contribution framework. Figure 2 presents the matrix for four different design science research contribution areas.

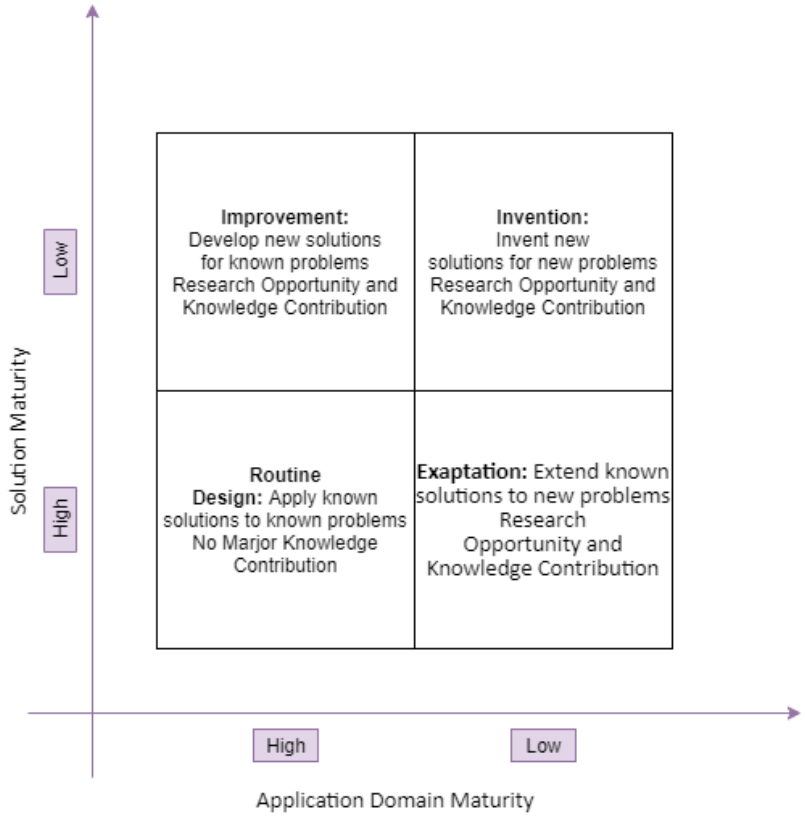


Figure 2. Design science research contribution framework adapted from Gregor & Hevner, 2013

Many organizations are struggling to defend their organizations against adversaries' attacks; there are no one-size-fits-all solutions to protecting all the assets. Almost all companies use more than one cybersecurity solution (Magowan, 2017). This research aims to contribute knowledge and improve organizations understanding of their defensive controls and identify gaps. According to Gregor & Hevner (2013), "*Improvement: New Solutions for Known Problems The goal of DSR in the improvement quadrant is to create better solutions in the form of more efficient and effective products, processes, services, technologies, or ideas*" (p. 339).

Improvements are possibly the most typical area to contribute to design science (Johannesson & Perjons, 2014). Many of the previous research related to Information Technology belongs to the Improvement research category. The critical challenge of the Improvement research category is to demonstrate the improved solution differences on prior knowledge. Concrete improvements in the research can be positive changes in process quality, productivity, visibility, or other quality measures, depending on the research goals. (Gregor & Hevner, 2013, 346) The contribution type suitability for the research is one of the reasons why the research method is chosen for the thesis.

The threat detection capabilities of the selected security solutions are evaluated by conducting a gap analysis between the finished artifacts. The research results are evaluated using a questionnaire within the organization that ordered the research. Respondents to the questionnaire were introduced to the author's thesis topic and research results in an online workshop before answering the questionnaire.

2.3 Research ethics

The thesis followed the ethical guidelines from the JAMK University of Applied Sciences (JAMK University of Applied Sciences, 2018). Commercial products have been used in the study. The author has not requested a separate research permit from the vendor, as all information used in the thesis has been obtained from public sources. The thesis does not infringe any copyrights or disclose any confidential information regarding the security solutions or by the company assigned the research. The security solutions detection capabilities are illustrated at a general level and do not represent any actual production environment. All the original information and sources are referred to in accordance with JAMK's reporting guidelines (JAMK, 2022). Evaluation of the thesis results has been conducted using an online questionnaire. Respondents' identities cannot be identified from the survey responses.

3 Theoretical-conceptual starting points

3.1 Adversaries

To understand what we need to protect, we need to know the adversaries' conducting attacks on our organization. The goals and objectives of an adversary can vary. Adversaries can conduct an attack on an organization to steal data, espionage, sabotage, or extort. (Trend Micro, 2015)

Adversaries are often rated by their skills or intent. In Figure 3, is seen the distribution between different adversary tiers. At the top of the pyramid, the number of attackers is the highest. At the top of the pyramid, adversaries do not usually use sophisticated attack techniques. The adversaries' experience, resources, and skills increase as you continue down the pyramid. At the top of the pyramid, script kiddies mainly use prebuild tools to conduct their attacks. Script kiddies and hacktivists often want to achieve a political or social impact. The bottom of the pyramid is organized crime and advanced persistent threats (APTs). These groups usually have some financial objective or motive. (Chapple & Seidl, 2019, 37-38)

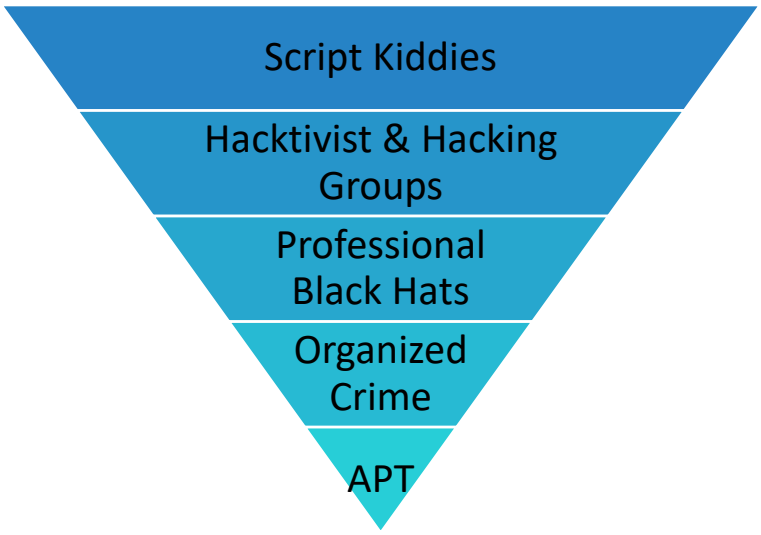


Figure 3. Adversary tiers adapted from Chapple & Seidl, 2019

Espionage or cyber-attacks are easy to disguise as being done by another country or group. For example, investigating an incident that involves a set of IP addresses, the attacker might have acquired attacking infrastructure from other organizations or

spoofed the IP addresses using a set of tools or software. Attribution of security incidents can be assessed based on the attack method used, tools used, and code analyzed from the found malware, or the benefit gained from the attack. (Järvinen, 2018, 18)

According to Bautista Jr. (2018), attribution is about validating a threat or adversary by recording their actions. Mavroeidis et al. (2021) pinpointed in their study that attribution can be a challenging task because it requires direct evidence and systematic analysis from multiple different internal and external data sources. The protocols used in Internet traffic adversaries can easily disguise their identities. It is relatively easy for malicious actors to spoof their attacking infrastructure. Spoofing the attacks is why attribution to cyber incidents is considered hard or nearly impossible. Attribution is even more challenging when the motivation of adversaries is considered. (Yannakogeorgos, 2016) Jaafar, Avellaneda, & Alikacem (2020) illustrated in their study that regulatory challenges complicate the data collecting process to conduct attribution. Due lack of international regulations and information privacy, collecting and exchanging data to perform attribution can be challenging.

Understanding the motivations that may drive the attackers can be beneficial to defending organizations in understanding the risks and impacts associated with the attacks (Mark, 2020). Understanding the attacker's motivation can be a more cost-effective way for the organization to apply appropriate defensive controls, as motivations for attacks often drive the attack method. Attacker motivation, in all its simplicity, can be divided into two different factors, intrinsic and extrinsic. Intrinsic motivation involves an adversary performing an attack's outcome is personally rewarding. Extrinsic motivations are those acts that result in external rewards. If the adversary gets paid for the attack or the attacker indirectly benefits from the attack, can be examples of extrinsically motivated behavior. (Mark, 2020)

When attackers compromise infrastructure, they might leave traces behind. These traces often are called Indicators of compromise (IoC). (Diogenes & Ozkaya, 2018, 221) IoC can be an example: IP address, domain names, URLs, SHA-256 and MD5 hashes, or changes in operating system configuration (Bautista Jr., 2018, 97). Not all indicators should be weighed equally. Some of the indicators can have more impact

and value than others. Figure 4 shows the relationship between the indicators an organization could use to detect an adversary's activities. (Bianco, 2014)

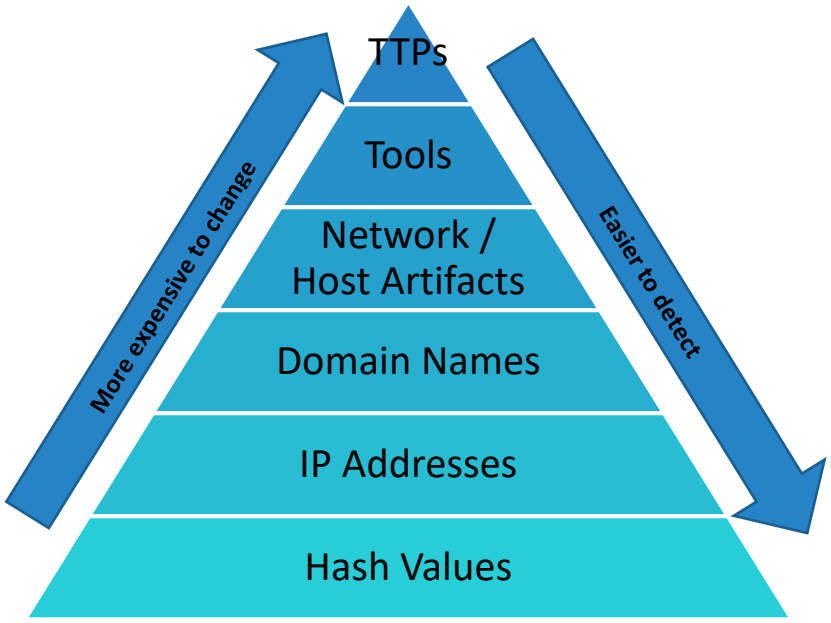


Figure 4. David Bianco's Pyramid of Pain adapted from Bianco, 2014

The bottom of the pyramid is hash values. Hash values are the most cost-effective to adversary change. Most hash generating algorithms calculate a message digest of the entire input and output to a unique hash value for the given input. If the adversary changes the file's content by one bit, the hash value is no longer the same. The hash value can be the most accurate indicator for defenders when detecting malicious activities. The probability of two different files having the same hash value is low. (Oriyano, 2016, 86-88)

The second step in the pyramid is IP addresses. IP addresses are relatively easy adversaries to change or spoof. An attacker can use the virtual private network (VPN), anonymous proxy service, The Onion Router (Tor), or other captured infrastructure to conduct the attack. That's why static IP blocklists are no longer effective defensive control for organizations to stop advanced adversaries. (Cyware, 2021)

Domain Names are above the IP address since creating new Domain Names is slightly more expensive for the adversary to change. Technically, generating new domains is not complicated, but it could require the adversary to invest more time in the attack.

The adversary needs to register and pay for the created domains to be hosted somewhere. Depending on the DNS provider, registering new domain names could take a few days to be visible through the Internet. (Bianco, 2014)

The fourth step on the pyramid is Network and Host Artifacts. When conducting an attack, most adversaries need to communicate with external entities through the network. The network artifact could be Command and Control data embedded in network protocols to exchange commands from the compromised host to the attacker. This behavior cannot be detected with all network solutions. So, the defender might need to invest in more intelligence products to detect these kinds of behavior. (Bianco, 2014; Cyware, 2021)

The top of the pyramid is Tools and Tactics, Techniques, and Procedures (TTPs). Berady, Jaume, Tong, & Guette's (2021) research paper indicated that the most valuable intelligence to defenders is to understand the adversary procedures that reside top of the pyramid. Adversaries can use multiple tools or malware to complete objectives in the target organization environment. According to Oriyano (2016), malware term comes from malicious software. Malware is a broader term for software families, including worms, viruses, trojans, adware, spyware, and logic bombs. Malware can have different functionalities, such as installing keyloggers to steal passwords, steal personal information or resources, and move laterally inside organizations. (Oriyano, 2016, 224-249)

If the defender can detect the usage of the adversary tool, this might have a more significant impact on the adversary and require them to change the tooling for the next attack. This would cost the adversary more time, depending on how broadly the defender can detect the usage of such tools. The adversary might not have the capability to create new tools. If the tools used by the adversary are purchased, they must obtain a new set of tools to conduct the next attack. (Bianco, 2014)

Sometimes attackers are not conducting the attack by using traditional malicious attacking tools. Adversaries can use so-called Living off the Land (LotL) attack methods. According to (Kaspersky IT Encyclopedia, n.d.), "*LotL attack describes a cyberattack in which intruders use legitimate software and functions available in the system to perform malicious actions on it*". Attackers using these tools can be harder

to detect inside an organization's environment. Commonly used tools used in LotL attacks are Powershell, Windows Management Interface (WMI), and PsExec. The organization's IT administrators regularly use these tools for their daily tasks. Essential for the defenders is to know what tools are used inside the organization and understand what is normal. (Cox, n.d.)

3.2 Defense in depth

Defensive security controls can be people, processes, and technologies that defend organizations' networks against intrusions (Diaz, 2021). Defense in depth is a strategy for protecting an organization's environment against cyber-attacks and slowing the adversary in the process. There should be more than one defensive security control to detect the adversary attack steps inside the organization's systems or networks (Chapple & Seidl, 2017, 294). If some defensive control fails, another control should stop or detect the attack in the next stage. There are many potential adversaries with a wide variety of attack methods available. There is no single method, tool, or solution to successfully detect or stop attacks on organizations. (McGuiness, 2001) The attacker might have compromised or gained access to different resources inside the organization. For example, mobile devices, on-premises services, cloud infrastructure. This means that organization needs to increase the adversaries cost for the attack in each possible resource. (Diogenes & Ozkaya, 2018, 201)

Defense in depth design describes three different control types that organizations can implement to prevent, detect, counteract, and limit the impact on security incidents. Different control types are: (1) Technical controls which include antivirus software, firewalls, network monitoring tools, and other systems that can technically provide security. This thesis is focused on analyzing technical controls. (2) Procedural controls, which can be company policies and guidelines on using company-provided devices and managing the organization's data. (3) Physical controls can be locked doors, fences, bollards, or any other physical control that can limit physical access to cause harm to the organization. (Chapple & Seidl, 2017, 298)

Different control types are classified into three schemes: (1) Detective controls give organizations visibility to security incidents. Detective technical controls can be

security tools detecting deviations in technical log data or when unwanted actions occur. A physical detective control example can be a security surveillance camera. This thesis concentrates, giving mainly contribution to technical detective controls. (2) Preventive controls can stop or prevent incidents from happening. Preventive physical control can be security guarding. Technical preventive controls can be intrusion prevention systems and other controls that can prevent security incidents. Detection rules and solutions used in this thesis can have preventive capabilities, but they are not in this research scope. (3) Corrective procedural controls can include implementing an incident response plan and business continuity plan to remediate or limit the security incidents' impact on the organization. (Chapple & Seidl, 2017, 298-299; Walkowski, 2019)

Figure 5 illustrates the layered security design in defense in depth. The organization needs to evaluate the most valuable assets and design the security principles according to conducted evaluation. In Figure 5, Data Security is the most important asset organization to protect, and it resides center of the circle. Keeping the Data Security safe should be the organization's top priority, and there should be most control types protecting it. (Chapple & Seidl, 2017, 295-299)

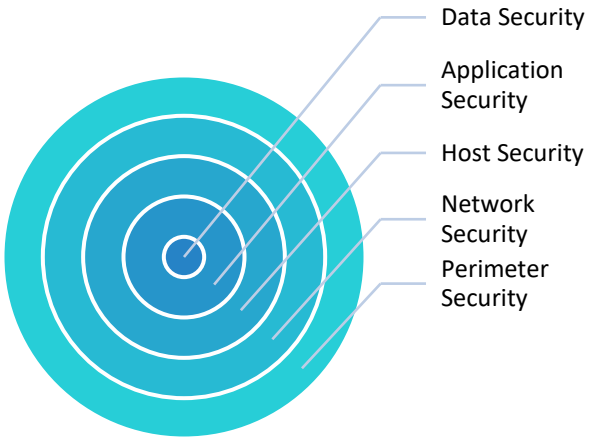


Figure 5. Layered security design adapted from Chapple & Seidl, 2017

According to Chapple & Seidl (2017, 306), layered security is efficient, and well-designed monitoring and detection centralized logging solution should be implemented. These solutions are called security information and event

management (SIEM) solutions. For monitoring to be effective, an organization needs to have a thorough understanding in its environment what to defend. (Turner, Toor, Smith, & Mcwhirt, 2022)

In their study, Khalid, Zainal, Maarof, & Ghaleb (2021) demonstrated that APT attack is a six-stage process. Most research is done to detect only a few stages of the attack. All these stages need to be detected and correlated for the detection to be effective. The study concluded that: "*Detecting all these stages and correlating them is still an open research problem."* (Khalid et al., 2021)

3.3 MITRE ATT&CK framework

Lockheed Martin developed the first Cyber Kill Chain model in 2011. The kill chain maps out an adversary's specific steps when targeting an organization. Lockheed Martin's model illustrates linear steps from reconnaissance to weapons deployment to command-and-control actions on the objective. By understanding the framework, defenders can better position their security controls and mitigations to an effective defense. After Lockheed Martin introduced the kill-chain methodology, MITRE Corporation researched adversaries and built a framework for the broader public. (Reiber & Wright, 2020) The MITRE Corporation is a not-for-profit organization. The corporation manages federally funded research and development centers (FFRDCs). These centers support various United States government agencies in aviation, defense, healthcare, homeland security, and cybersecurity. (The MITRE Corporation, 2021a)

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a knowledge base and framework to track cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle. The first version of the ATT&CK model was created in 2013. It included eight Tactics and around 70 Techniques. Since then, the model has grown to contain more sources and technologies. Version 10 of the matrix consists of 14 Tactics and over 500 combined Techniques and Sub-techniques. (Strom et al., 2020)

Compared to the Lockheed Martin Cyber Kill Chain model MITRE ATT&CK framework is more comprehensive and gives defenders more abstraction level to illustrate the

adversary behavior. The MITRE ATT&CK framework is constantly evolving due to high community support. (Chow, 2021)

The ATT&CK framework describes how adversaries gain initial access to organizations and then move laterally, escalate privileges, and generally evade your defenses. The framework can be used to determine what specific methods adversaries use when they conduct malicious activities to target the organization. The ATT&CK framework organizes adversary behaviors into a series of Tactics, Techniques, and Sub-techniques that adversaries may use within each Tactic category. The ATT&CK framework can be used both offensive and defensive points of view. (Strom et al., 2017) In his master's thesis, Hallberg has demonstrated a proof-of-concept implementation of how the MITRE ATT&CK framework is being used to visualize and detect intrusions. (Hallberg, 2020) The MITRE ATT&CK framework is suitable for supporting artifacts created in this thesis based on previous research.

Tactics

Tactics are the highest abstraction level of the ATT&CK matrix. Tactics describe why an attacker operates, Techniques and Sub-techniques explain how they do it. (Strom et al., 2017) MITRE ATT&CK Matrix for Enterprise Version 10 consists of 14 different Tactics. All Tactics have unique ID illustrated in Table 1. This ID helps when the framework is used programmatically. (The MITRE Corporation, 2021b)

For example, an adversary's strategic goal could be to profit from the organization using ransomware. This tactical end goal would reside in TA0040 - Impact. Usually, short-term tactical objectives must be completed for the adversary to achieve the initial tactical goal. Typically attacks begin when the adversary tries to gain access to the target organization (TA0001 - Initial Access). After gaining a foothold, the adversary must discover the path to the initial objective (TA0007 - Discovery). To move laterally, the adversary needs better privileges (TA0008 - Lateral Movement and TA0004 - Privilege Escalation). When moving laterally, the adversary needs to evade organization defense (TA0005 - Defense Evasion). To avoid detection adversary might run malicious code to bypass controls (TA002 - Execution). Like in the example adversary does not need to complete these short-term objectives in a particular order. (LogRhythm, n.d.)

Table 1. ATT&CK v10 Matrix Enterprise tactics

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather the information to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain its foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

When an adversary is conducting an attack against an organization, it does not have to go through all the Tactics to achieve its strategic goal (CISA, 2021).

Techniques

The MITRE ATT&CK Techniques describe how adversaries achieve tactical goals by performing an activity. ATT&CK Techniques address the “how” and, in some cases, the “what” an adversary gains by completing an action. There may be many ways, or methods, to achieve tactical objectives, so there are multiple Techniques in each Tactic category. (Strom et al., 2020) The MITRE ATT&CK Version 10 includes 188 Techniques, the differences between Tactics, Techniques, and Sub-techniques are illustrated with a partial presentation of the matrix in Figure 6 (The MITRE Corporation, 2021b).

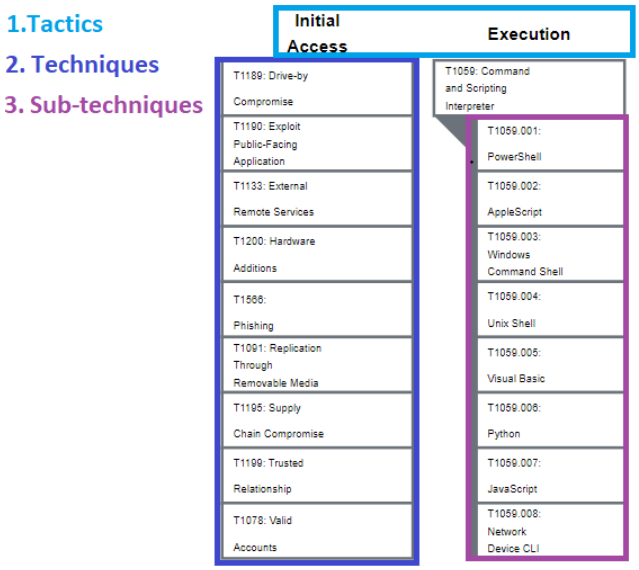


Figure 6. MITRE ATT&CK Tactics, Techniques and Sub-techniques

By design of the MITRE ATT&CK Enterprise framework, adversary actions can be mapped to multiple Techniques. For example, when an adversary uses malicious code to conduct a phase of an attack. The code can be obfuscated by VBA macros, including a command executed by cmd.exe that consists of a malicious PowerShell code. This single behavior can be mapped to multiple ATT&CK Techniques: (1) T1064 – Scripting and (2) T1059 - Command-Line Interface, and T1086 - PowerShell. (Picus Labs, 2020)

The single ATT&CK Technique can be part of many adversaries Tactics. Example Technique T1078 – Valid Accounts is part of four different Tactics: Defense Evasion, Persistence, Privilege Escalation, and Initial Access. (The Mitre Corporation, 2021c)

According to Mandiant (2022), adversaries prioritize identifying administrative accounts at the Initial Access phase. After successful identity compromise, adversaries use these accounts for lateral movement, persistence, and mission fulfillment. (Turner et al., 2022)

Sub-techniques

Sub-techniques explain the most specific ways adversaries achieve their tactical goals. Sub-techniques describe actions at a more thorough technical level than Techniques. Usually, Sub-techniques are targeted to a particular platform example, Linux or Windows environment. (Strom et al., 2020) ATT&CK Version 10 includes 379 sub-techniques (The MITRE Corporation, 2021b).

For example, Technique T1222 - File and Directory Permissions Modification is divided into two Sub-techniques illustrated in Figure 7. Sub-techniques can be identified with an added number after the Technique ID (.001). (The MITRE Corporation, 2021d)

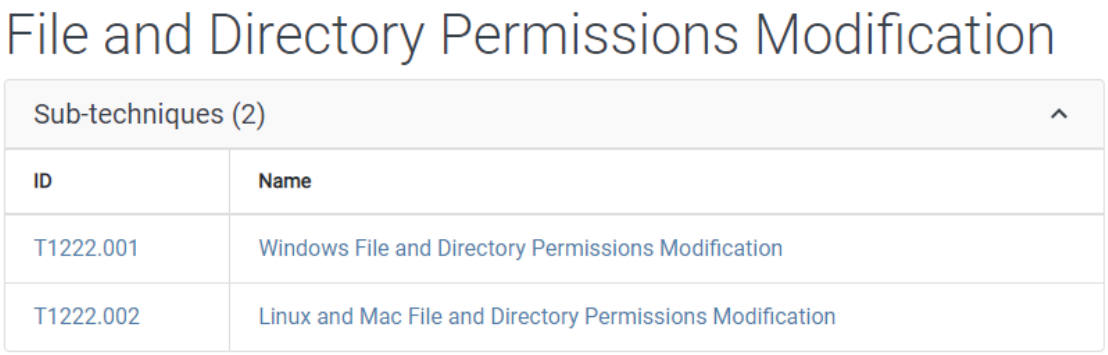


Figure 7. Technique T1222 - File and Directory Permissions Modification Sub-techniques

Procedures

Procedures describe the implementation of what the adversary uses for Techniques or Sub-techniques. Procedures are being used to describe in-the-wild use of Techniques or Sub-techniques while exhibiting several other behaviors in the way they are performed. Procedures may indicate the use of specific tools when adversaries achieve tactical goals. (Strom et al., 2020)

Data sources

The ATT&CK framework includes data sources. Data sources are tools and solutions that can provide information and logs to analyze a given ATT&CK Technique or Sub-technique. Currently, there are 38 different data sources provided by MITRE. Typical data sources are, an example, Active Directory, Firewall, and Windows Registry. (The MITRE Corporation, n.d.) The author has introduced a set of new data sources not included in the MITRE ATT&CK framework dataset in the next chapter.

4 Development of the artifact

4.1 Introduction to the developed artifacts

To know the gaps in our organization's defenses, we need to know our detection capabilities. This implementation demonstrates a case example using threat detection information publicly available on the Internet against the commercial detection tools selected in the study. Security solutions are chosen for this research:

- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud (Windows machines)

The coverage of the selected toolset was intriguing to the author. According to marmcimsft (2020), "*Microsoft Defender is a combined set of offerings, combining Microsoft 365 Defender and Azure Defender, protecting, and responding to threats across an attacker kill chain, from identities to endpoints, applications, email, infrastructure, and cloud. Thinking left to right, through an attacker lifecycle"*. Would it be enough to detect adversaries' attacks across the whole attack kill chain if an organization uses this toolset? Could we only rely on this toolset, or do we need additional detection tools to get better coverage? Starting process for the research is to examine the selected defensive tools. The chosen security solutions are illustrated in Figure 8 (marmcimsft, 2020), how Microsoft describes the solution's capabilities detecting threats in the attack kill chain.

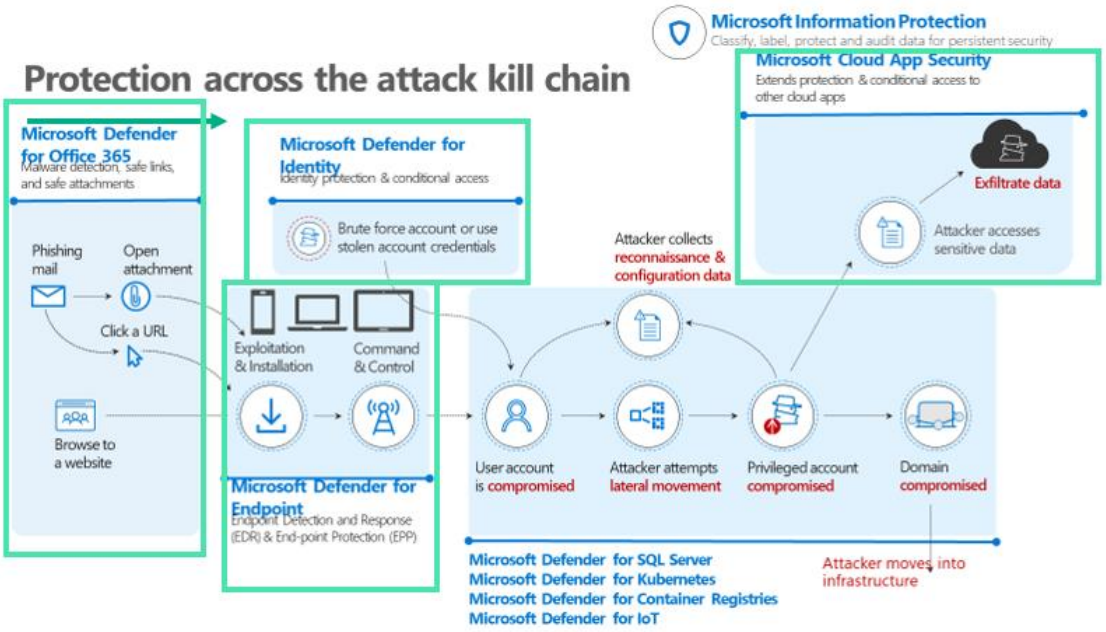


Figure 8. Illustration of Microsoft Defender protection across the attack kill chain

Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution. The solution handles on-premises Microsoft Active Directory signals to identify and detect threats. It can locate compromised identities and malicious insider actions. (Microsoft, Defender for Identity, 2021)

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) solution. Defender for Cloud Apps focuses on identifying, detecting, and responding to cyberthreats across Microsoft and third-party cloud services. (Microsoft, Cloud App Security, 2021)

Microsoft Defender for Office 365

Microsoft Defender for Office 365 is a cloud-based tool to safeguard organizations against malicious threats posed by email messages, links (URLs), and collaboration tools. Such as Microsoft SharePoint, OneDrive, and Teams (Microsoft, Defender for Office 365, 2021).

Microsoft Defender for Cloud (Windows machines)

Microsoft Defender for Cloud is a built-in Azure tool that provides threat protection on workloads running in Azure, on-premises, or other clouds. Microsoft Defender for Endpoint adds threat detection capabilities and respond features for Windows machines. Microsoft Defender for Cloud itself contains much more protection for different workloads. This research only focuses on using Azure Defender and only Windows OS. (Microsoft, Azure Defender, 2021)

4.2 Design and development of defensive artifacts

According to Vaishnavi (2019, 1), typically, research that uses the Design science research method to create artifacts has two contributions to the solution: (1) create new knowledge to the community with artifacts (things or processes) and (2) practical use and analysis of the created artifacts. The development process of design science research can be empirical (Vaishnavi, 2019, 20). The author has created a process for artifact creation to map the detection tools against the MITRE ATT&CK framework.

1. Identify the detection coverage of the selected security solutions (Data sources)
2. Map solutions detection rules to the MITRE ATT&CK framework (Create new knowledge)
    a. Analyze the publicly available information for the detection rules
    b. Analyze the MITRE ATT&CK Tactics used
    c. Analyze the MITRE ATT&CK Technique and possible Sub-technique used
    d. Score each detection rule to give a better quantitative value
3. Draw the MITRE ATT&CK layer for documented rules per solution
4. Compare all tools to data from adversaries' behavior (Gap analysis)
5. Evaluate findings

Identify the detection coverage of the selected security solutions (Data sources)

This process aims to contribute to creating new knowledge in the community and demonstrating the practical use of the artifacts. According to Cybersecurity Insiders' (2021) survey, 84% of the respondents do not have their threat detection capabilities

mapped to ATT&CK techniques. Information gathering was conducted on the security solution selected in the thesis to start the mapping process. The author identified 213 different detection rules within the chosen four security solutions. The count of detection rules is illustrated in Table 2. This thesis does not cover how the security solutions were configured since the data, and the detection capabilities are from publicly available information.

Table 2. Security solutions detection rules count

Tool	Source	Detection rules count
Microsoft Defender for Cloud Apps	(Microsoft, 2021b)	40
Microsoft Defender for Identity	(Microsoft, 2021c)	39
Microsoft Defender for Office 365	(Microsoft, 2021d)	34
Microsoft Defender for Cloud (Windows machines)	(Microsoft, 2021e)	100
Sum		**213**

Map solutions detection rules to MITRE ATT&CK framework (Create new knowledge)

Tactics Reconnaissance (TA0043) and Resource Development (TA0042) are excluded from the thesis since they are usually hard to detect using a set of tools. These tactics are part of the PRE matrix but are included in MITRE ATT&CK Enterprise version 10. (MITRE ATT&CK Defender™ (MAD), 2021)

Some of the selected security solutions detection rules were documented using the MITRE ATT&CK framework at the Tactics level by the product vendor. According to Picus Labs (2020), security solutions automatically map a malicious action only to a

single Tactic for technical reasons. More detailed mapping data was required to conduct the defensive gap analysis for the research.

Producing the mapping to the defensive artifacts is done by using hands-off Methodology illustrated in Table 3. According to MITRE ATT&CK Defender™ (MAD, 2021), the hands-off methodology is a good starting point for delineating and exposing the organization's defensive capabilities. The aim was not to produce 100% pinpoint accuracy for the selected security solutions, so hands-off methodology was logical for the mapping process.

Table 3. Defensive artifacts creation methodology adapted from MAD (2021)

Name	Methodology	Description
Hands-on	Penetration testing, red teaming, adversary emulation	Pinpoint Accuracy Time Consuming Invasive
Hands-off	No execution, document review & history with tools	Approximate Coverage Minimally invasive Variable time investment

The identified detection rules were mapped to cover the Technique and possible Sub- technique abstraction levels. Figure 9 illustrates the detection rules mapping process to the MITRE ATT&CK framework. The number left side of the boxes describes the process step number:

1. Selection of the detection rule for analysis
2. Analysis of the MITRE ATT&CK Tactics. The detection rule itself can contain visibility to multiple different Tactics.
3. Analysis of the MITRE ATT&CK Technique. The Tactics analysis result can include mapped to multiple MITRE Techniques.
4. Map the detection rule to the MITRE ATT&CK Sub-technique if it applies

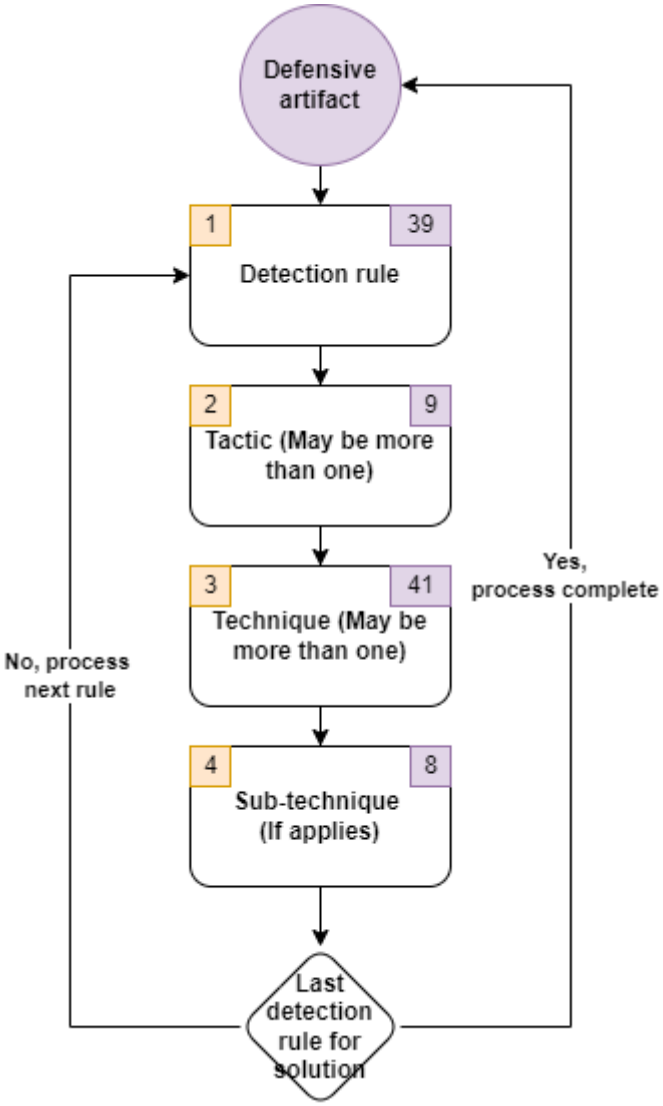


Figure 9. Defensive artifact mapping process to MITRE ATT&CK framework

The numbers on the right illustrated in Figure 9 shows how many different Tactics, Techniques, and Sub-techniques were identified on solution Microsoft Defender for Identity in the mapping process. The total count of analysis and mapping of all the selected tools are illustrated in Table 4. Below is an example of how the analysis and mapping process was conducted for one detection rule from solution Microsoft Defender for Identity.

Defensive artifact mapping process step one

Selection of the detection rule: "*Data exfiltration over SMB*". The detection rule short description is: "*A Defender for Identity Data exfiltration over SMB alert is triggered when suspicious transfers of data are observed from your monitored domain controllers*" (Microsoft, 2021c).

Defensive artifact mapping process step two

Map the detection rule to ATT&CK Tactic. The publicly available information from Microsoft provided documentation for the Tactics level but did not provide information for Techniques or Sub-technique level mapping. Provided Tactics were Command and control, Exfiltration, and Lateral Movement.

Defensive artifact mapping process step three

Map the detection rule to ATT&CK Techniques. The Techniques were identified:

- T1071 - Application Layer
- T1048 - Exfiltration Over Alternative Protocol.

Technique T1071 description illustrated in Figure 10 defines SMB as an application layer protocol (The MITRE Corporation, 2021d). Based on the Technique description, there is no suitable Sub-technique to map, so the rule has been mapped to the Technique level.

Technique T1048 describes adversaries stealing data using protocol not commonly used in Command & Control. In addition, the detection rule name was "*Data exfiltration over SMB"*, and SMB is one of the protocols listed in the description illustrated in Figure 10 screenshot taken from the MITRE website. (The MITRE Corporation, 2021d) The similar behavior described in the names gave more support for the interpretation for the mapping accuracy.

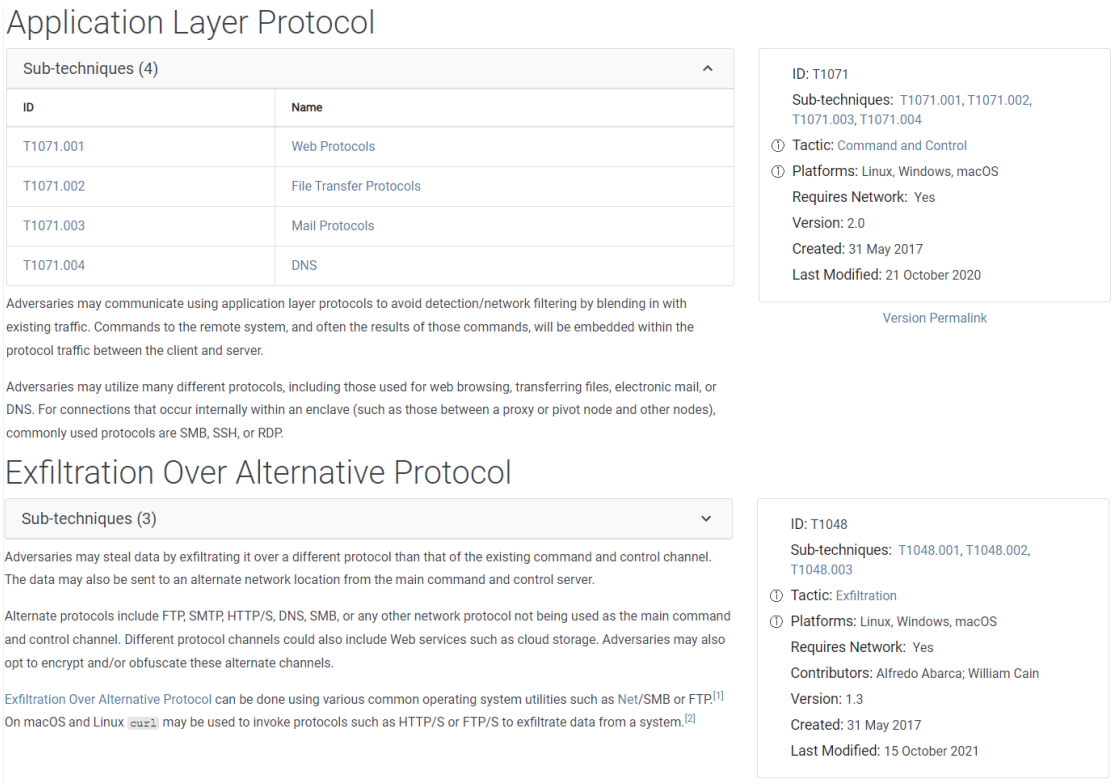


Figure 10. T1071 - Application Layer Protocol & T1048 - Exfiltration Over Alternative Protocol

Defensive artifact mapping process step four

Map the detection rule to ATT&CK Sub-technique if it applies. The Sub-technique has been identified to T1021.002 - Remote Services: SMB/Windows Admin Shares illustrated in Figure 11 screenshot taken from the MITRE website (The MITRE Corporation, 2021d).

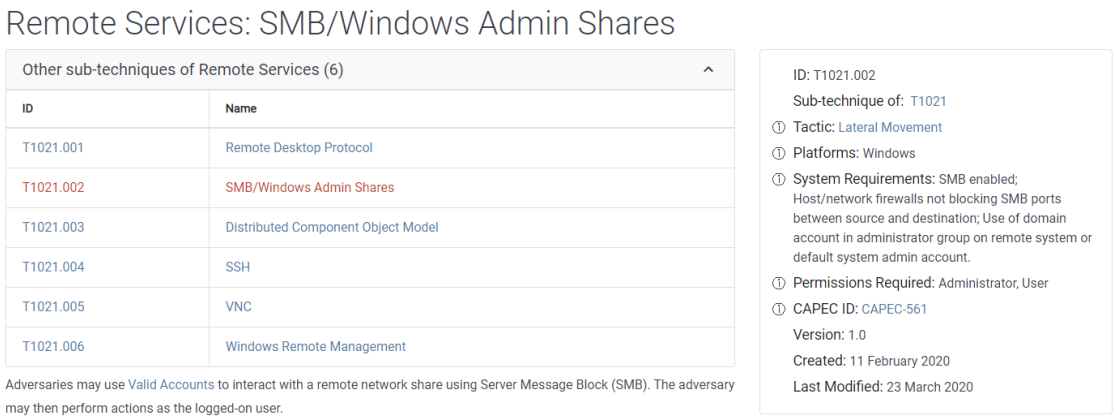


Figure 11. T1021.002 - Remote Services: SMB/Windows Admin Shares

The detection rule description defined that the detection rule could detect adversary lateral movement using SMB. Regarding ATT&CK TTPs, this Sub-technique was the best fit to describe the adversary behavior.

The analysis results of the previous steps were documented to a MITRE Enterprise Matrix provided structured JavaScript Object Notation (JSON) file format. The data format is easy for humans to read and write. JSON design is lightweight for computers to parse, generate and the text format is language independent. (Ecma International, 2017) Documented example mapping for the "*Data exfiltration over SMB*" rule is illustrated in Figure 12.


```
"techniques": [
    {
        "techniqueID": "T1071",
        "score": 10,
        "color": "",
        "comment": "Data exfiltration over SMB",
        "enabled": true,
        "metadata": [],
        "showSubtechniques": false
    },
    {
        "techniqueID": "T1048",
        "score": 20,
        "color": "",
        "comment": "Data exfiltration over SMB, Suspicious communication over DNS",
        "enabled": true,
        "metadata": [],
        "showSubtechniques": false
    },
    {
        "techniqueID": "T1021.002",
        "score": 20,
        "color": "",
        "comment": "Data exfiltration over SMB, Suspected SMB packet manipulation",
        "enabled": true,
        "metadata": [],
        "showSubtechniques": false
    }
],
```


Figure 12. Data exfiltration over SMB, JSON example

The analyzed rules were given a score value. The score describes how many different detection rules can detect the same Technique. The aim was to identify what Techniques and Sub-techniques had the best coverage. A score value of +10 was given for each successful Technique mapping for the detection rule. In addition, the detection rules names were documented in the "comment" field of the JSON file. Figure 13 illustrates the scoring chart to measure defensive artifacts' threat detection capabilities. In chart left, number ten indicates one detection rule is covering the

Technique, and right number 100 represents ten different detection rules that can detect this behavior. The max value of 100 does not mean we have 100% detection capabilities for the mapped Technique or Sub-technique. Still, it gives us a better quantitative value to examine how many different detection rules can detect the behavior.

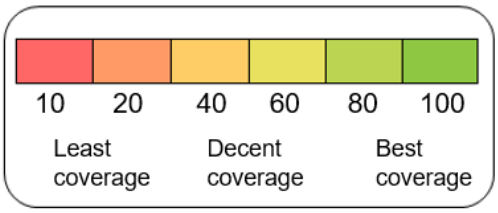


Figure 13. Defensive artifacts scoring

The distribution between solutions mapped to the ATT&CK framework is illustrated in Table 4. The summary value end of the table presents the total amount of the finding, not a distinct value. From the 14 Tactics in the MITRE ATT&CK Matrix for Enterprise, only 12 Tactics were used in this research. The whole list of Tactics is listed in Table 1. The summary value gives context to how many times the author needed to go through the Defensive artifact mapping and analysis process illustrated in Figure 9.

Table 4. Data collection table for defensive artifacts

Tool	Source	MITRE Tactics	MITRE Techniques	MITRE Sub-techniques
Microsoft Defender for Cloud Apps	(Microsoft, 2021b)	10	23	7
Microsoft Defender for Identity	(Microsoft, 2021c)	9	41	8
Microsoft Defender for Office 365	(Microsoft, 2021d)	8	9	3
Microsoft Defender for Cloud (Windows machines)	(Microsoft, 2021e)	11	26	34
Sum		38	99	52

4.2.1 Microsoft Defender for Identity – mapping results

The Defender for Identity documented 39 threat detection rules that were mapped against nine ATT&CK Tactics. Detection rules were mapped across 41 different Techniques and eight Sub-techniques illustrated in Figure 14. The most scored Technique was T1550 – Use Alternate Authentication Material scored “70”.

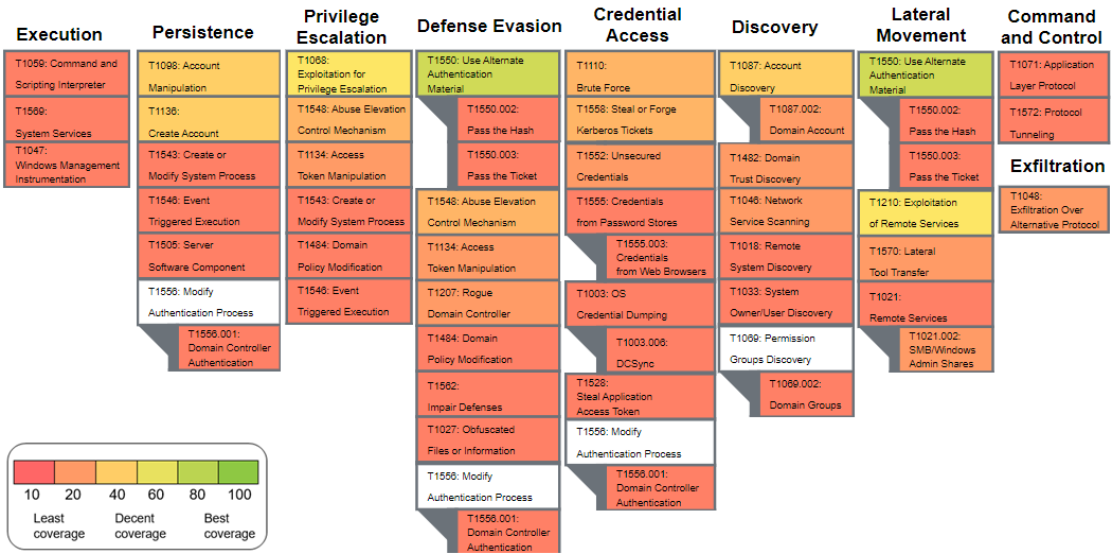


Figure 14. mitre-attack-defender-for-identity-v1.0.json

4.2.2 Microsoft Defender for Cloud Apps – mapping results

The Defender for Cloud Apps documented 40 threat detection rules that were mapped against 10 ATT&CK Tactics. Detection rules were mapped across 23 different Techniques and seven Sub-techniques illustrated in Figure 15. Most scored Techniques were T1078.004 - Valid Accounts: Cloud Accounts and T1537 - Transfer Data to Cloud Account. Both Techniques achieved a score of “50”.

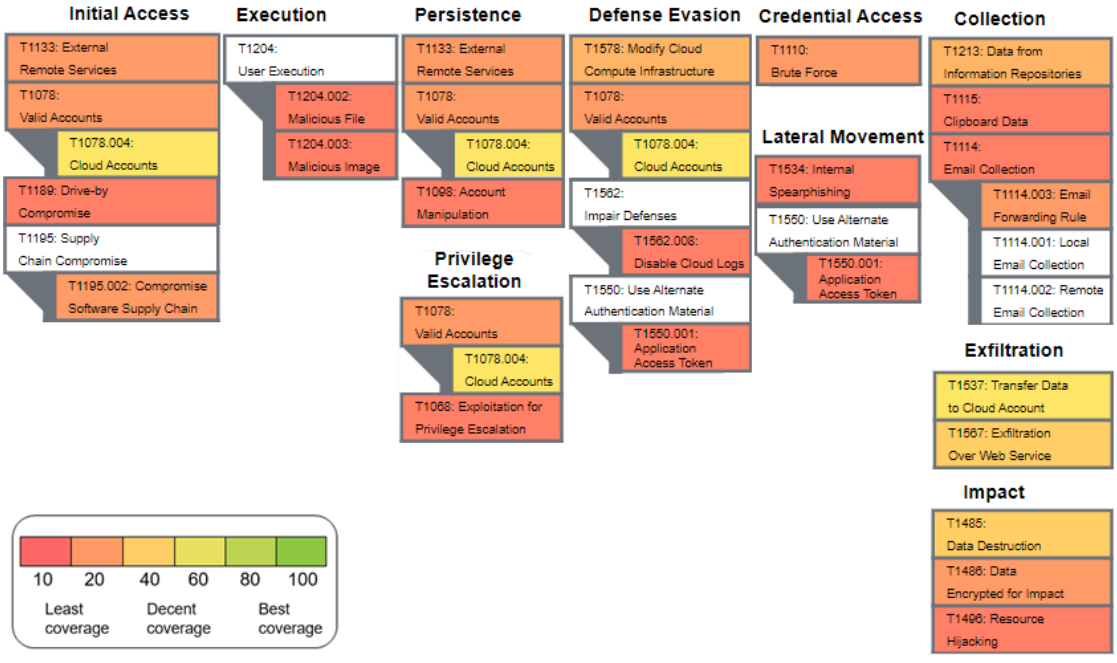


Figure 15. mitre-attack-defender-for-cloud-apps-v1.0.json

4.2.3 Microsoft Defender for Office 365 – mapping results

The Defender for Office 365 documented 34 threat detection rules that were mapped against eight ATT&CK Tactics. Detection rules were mapped across nine different Techniques and three Sub-techniques illustrated in Figure 16. The most scored Technique was T1566 – Phishing scored “120”.

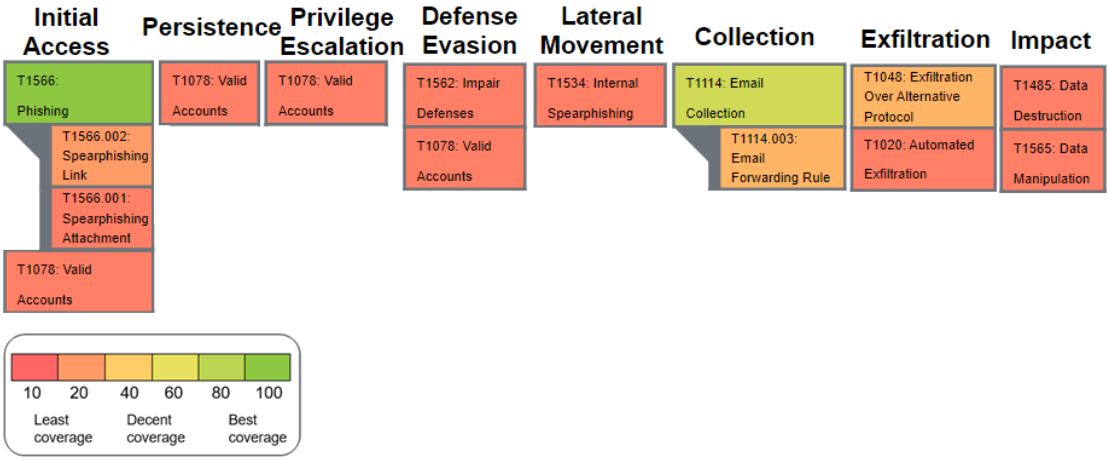


Figure 16. mitre-attack-defender-for-office-v1.0.json

4.2.4 Microsoft Defender for Cloud (Windows machines) – mapping results

Microsoft Defender for Cloud Windows machines documented 100 threat detection rules that were mapped against 11 ATT&CK Tactics. Detection rules were mapped across 26 different Techniques and 34 Sub-techniques illustrated in Figure 17. The most scored Technique was T1059 – Command and Scripting Interpreter scored “120”. A more prominent figure can be seen in Appendix 5.

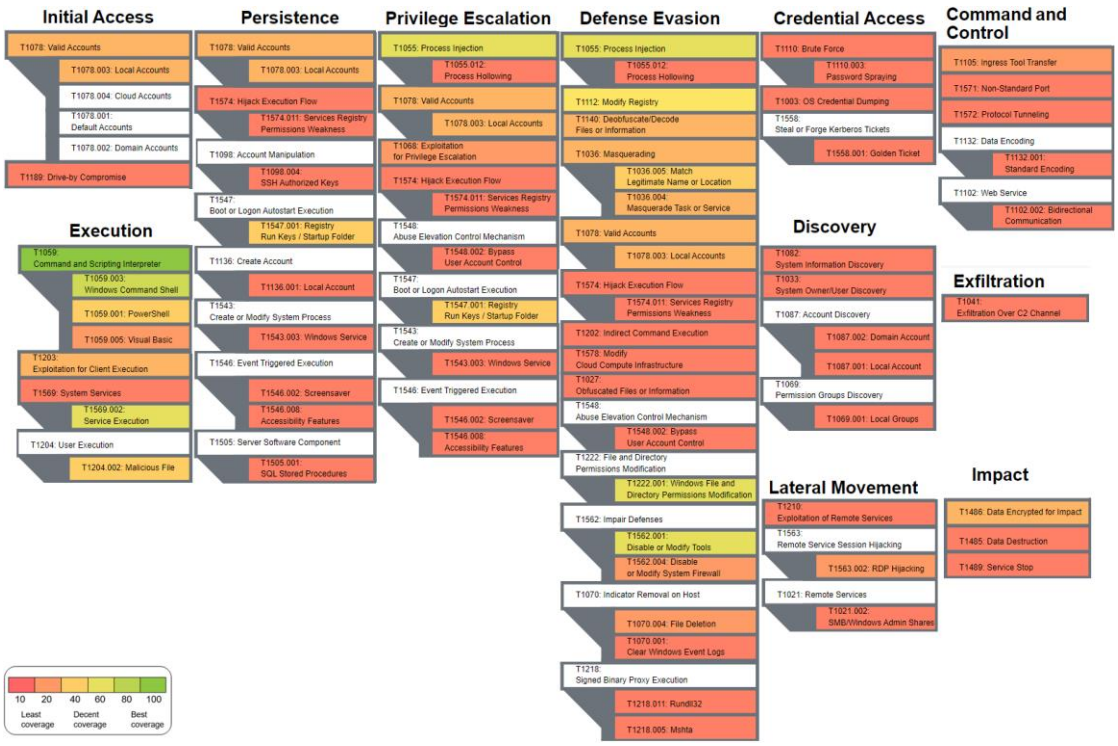


Figure 17. mitre-attack-azure-defender-v1.0.json

4.2.5 Summary of all security solutions – mapping results

All the security solutions' defensive capabilities are combined into a single ATT&CK layer. The artifacts detection capabilities are combined into a single layer illustrated in Figure 18. The combined ATT&CK layer is being used in the gap analysis examples in the following chapters. A larger figure can be seen in Appendix 6.

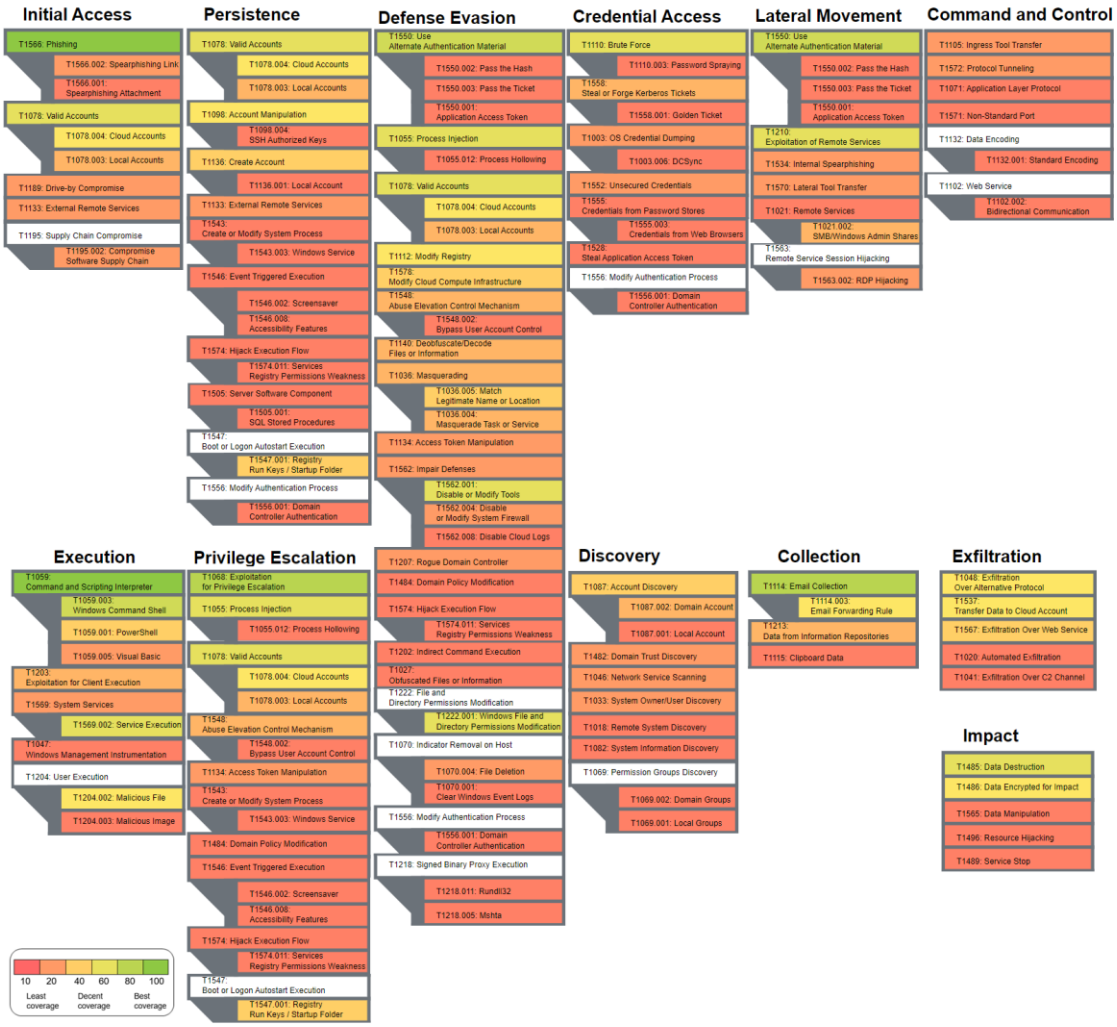


Figure 18. mitre-attack-all-tools-v1.0.json

All the identified 213 threat detection rules were mapped against 12 ATT&CK Tactics. Detection rules were mapped to 61 distinct Techniques and 48 distinct Sub-techniques. The most scored Technique was T1566 – Phishing scored “130”. Totally 51 distinct Techniques or Sub-techniques were mapped to a single detection rule with a score of “10”.

5 Implementation of the artifacts

5.1 Introduction to gap analysis

The gap analysis process was used to measure current defensive solutions coverage against adversary capabilities. This analysis method gives an organization a way to determine what part of its environment lacks defenses or threat detection visibility. These gaps can represent blind spots in organizations' defensive controls. The identified gaps can be valuable information for the organization to prioritize investments for security solutions. Same gap analysis can spot similarities and deviations for different solutions. (Strom et al., 2020)

The MITRE ATT&CK framework is being used as a tool for conducting the defensive gap analysis. The suitability of the framework has been studied previously. In their study, Pell, Emmanouil, Sotiris, & Ryan (2021) demonstrated that the ATT&CK framework is suitable for threat modeling 5G networks. The author performs the gap analysis comparing the defensive artifacts created in chapter 4.1 and adversary artifacts illustrated in Table 5.

92% of the attack.mitre.org data comes from Security Vendors, 5% from press reports, and 3% from publicly available government reports. Most of the reports are from actual incident reports. (MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training, 2021) The author did not want to use the adversary data provided by the MITRE. Instead, he wanted to explore and create the adversary artifacts from publicly available reports by himself.

Table 5 lists adversary behavior from different threat intelligence reports from various sources. These reports were analyzed and mapped to the MITRE ATT&CK framework by the author. The threat intelligence reports selected in this research had some ATT&CK TTPs documented that helped the artifact creation process.

Table 5. Adversary artifacts

Report Name	Source	MITRE Tactics	MITRE Techniques	MITRE Sub-techniques
BeyondTrust Labs - Analysis of Ransomware and Phishing Trends and How to Mitigate Them	(BeyondTrust, 2021)	8	11	6
Sophos - The Active Adversary Playbook 2021	(Shier, Gangwer, Iddon, & Mackenzie, 2021)	12	40	13
AdvIntel - Ransomware Advisory: Log4Shell Exploitation for Initial Access and Lateral Movement	(Kremez & Boguslavskiy, 2021)	11	16	12
Mandiant - Suspected Russian Activity Targeting Government and Business Entities Around the Globe	(Jenkins, Hawley, Najafi, & Bienstock, 2021)	12	43	29
Sum		**43**	**110**	**60**

Every threat report analyzed by the author had some inaccurate ATT&CK information. The Technique and Sub-technique codes were many times wrong. This might be due to negligence error, or the reports TTPs were mapped using older versions of the Matrix used in this thesis.

When conducting the gap analysis, the author tried to answer these questions:

- Can we detect this adversary behavior using our detection tools?
- Can we identify gaps in our detection capabilities?

For the first question author decided to create a scoring scale. Detection was good when the detection coverage was between 75-100%. Detection was decent when coverage was between 50%-75% and bad under 50%. Answers to the first questions are presented in the following chapters. The second question is analyzed in chapter 6.

5.2 Gap analysis 1 – Human operated ransomware

The BeyondTrust Labs Threat report is based on actual threats detected and analyzed attacks between Q1 2020 and Q1 2021 discovered by the BeyondTrust Labs team, collaborating with customers and incident response teams using Beyond Trust's products (BeyondTrust, 2021). Report analysis was divided into two different attack scenarios: (1) Human operated ransomware TTPs and (2) Most Common Techniques used after initial malware execution. The TTPs from the BeyondTrust Labs report is illustrated in Figure 19, quoted from (BeyondTrust, 2021).

Human Operated Attack Chain

Attack Chain Phase	MITRE Framework	Example
Access Environment	T1566 Phishing	**Initial Access** Trickbot via phishing email
	T1548.002 UAC Bypass	**Execution & Local Elevation** Cobalt Strike or PowerShell Empire
Persist, Recon, Traverse and Spread	T1134 Access Token Manipulation T1003 & T1003.001 Credential Dumping	**Credential Access** Using LaZange, Mimikatz or other tools
	T1055 Process Injection	**Privilege Escalation** Control over Valid Admin Accounts
	T1053 Scheduled Task/Job T1078 Valid Accounts: Domain Accounts	**Persistence** New Domain Admin (DA) Accounts
	T1087 Account Discovery T1033 System Owner/User Discovery	**Discovery** Recon and enumeration using Bloodhound
	T1035 Service Execution	**Lateral Movement** PsExec or other tools
	T1562 Impair Defenses	**Defense Evasion** Tampering with A/V & security services
Execute Objective	T1086 Data Encrypt for Impact	**Impact** Invoke Ryuk ransomware payload

Most Common Techniques After Initial Malware Execution

35% T1047
Using Windows Management Instrumentation calls to launch a process out of the process hierarchy, typically PowerShell or Window Command Shell (CMD)

22% T1204.002
User Execution: Malicious File is opened, which then downloads and directly launches a malware executable

17% T1059.001
Launch PowerShell initially

15% T1059.003
Launch the Window Command Shell (CMD), used for initial execution

1% Other
Use other exploitable native applications, such as Rundll32, WScript, or Mshta

Figure 19. BeyondTrust Labs TTPs

The analysis identified eight ATT&CK Tactics, 11 distinct Techniques, and six Sub-techniques in the BeyondTrust Labs threat report. The BeyondTrust Labs Threat report TTPs mapped to ATT&CK TTPs illustrated in Figure 20. The purple color is given to layers that represent adversary behavior. In the first attack scenario, adversaries try to get initial access to the organization using Technique T1566 – Phishing and Sub-technique T1548.002 UAC Bypass. After the initial access, adversaries use nine different Techniques and one Sub-technique for lateral movement, recon, and persistent phases illustrated in Figure 20. The adversary end objective was to Invoke the Ryuk ransomware payload, T1086 – Data Encrypt for Impact. In the second attack scenario, were identified one Technique and four Sub-techniques that adversaries use after initial malware execution:

- T1047 - Windows Management Instrumentation
- T1204.002 - User Execution: Malicious File
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1569.002 - System Services: Service Execution

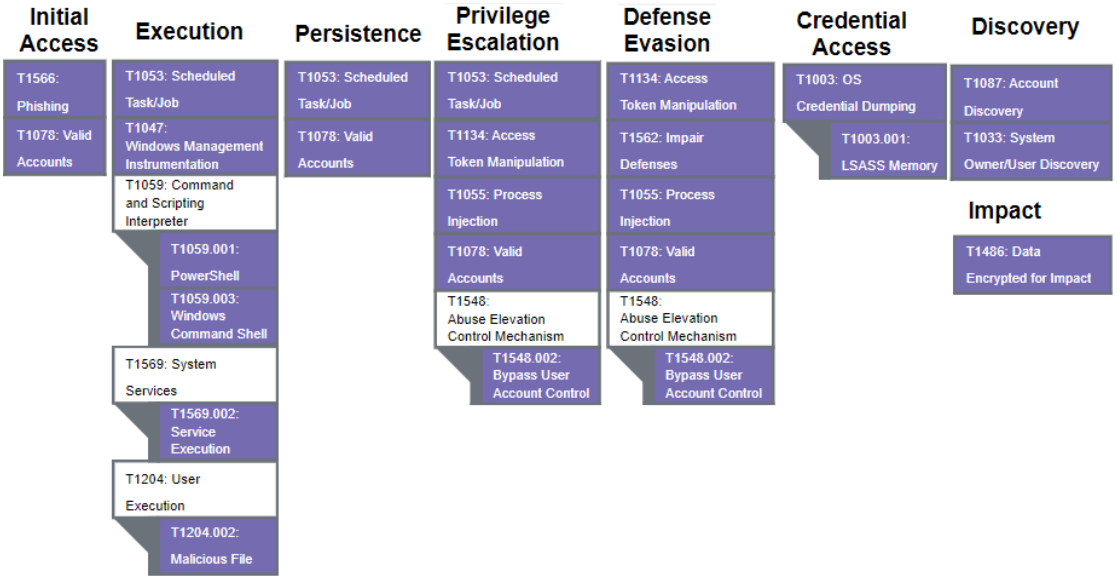


Figure 20. beyondtrust-malware-threat-report-2021-human-operated-attack-chain.json

Figure 21 illustrates an example of how the author conducted the gap analysis process in this study. The gap analysis process is demonstrated with one selected ATT&CK Tactic. On the left of Figure 21, we have the defensive artifacts covered. The

data is from all the defensive security solutions chosen in the thesis; the complete layer is illustrated in Appendix 6. Threat detection capabilities were compared to the threat detection capabilities to the adversary artifact ATT&CK layer shown in Figure 20. The outcome of this gap analysis is illustrated in Figure 21. Techniques and Sub-Techniques that have detection capabilities are marked as green, and with no detection are marked as red, shown in Figure 21.

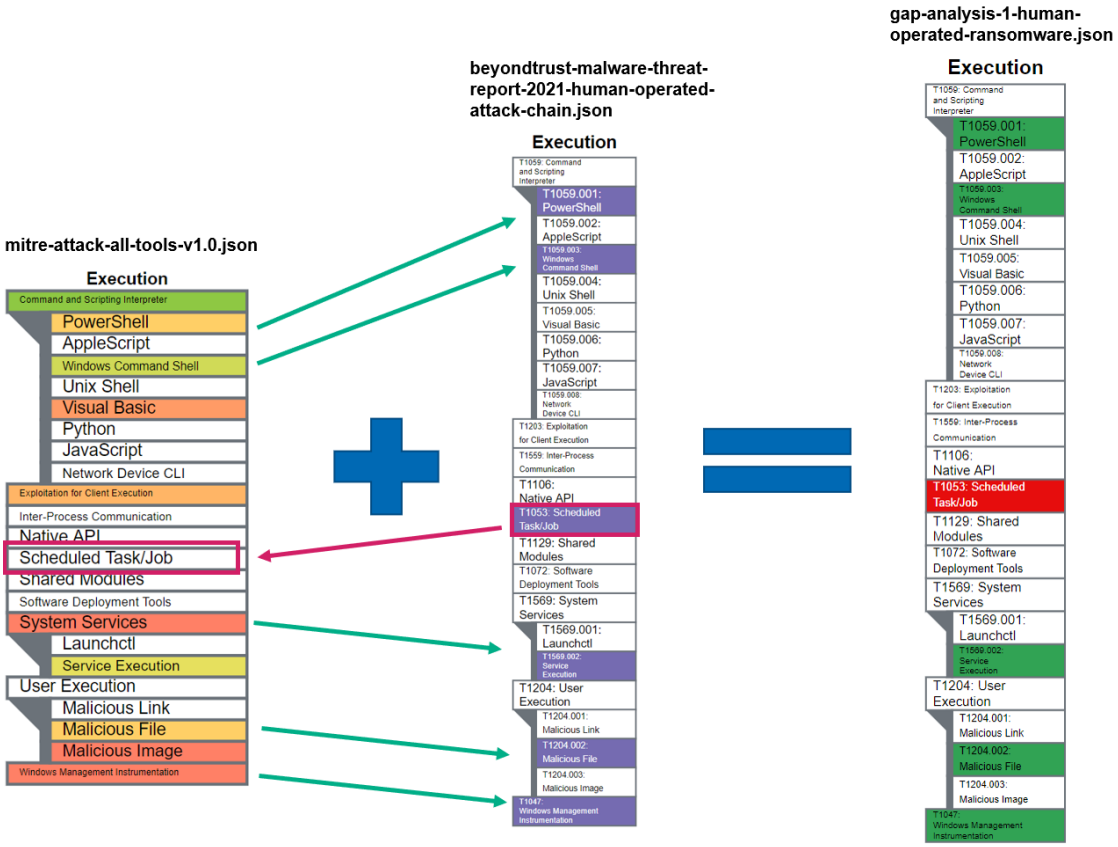


Figure 21. Gap analysis example with one MITRE Tactic

The gap analysis example identifies the lack of security solutions detection rules capabilities detecting ATT&CK Technique T1053 – Scheduled Task/Job since there are no detection rules to cover detection in these activities. In the final layer on the right side of the example, detected techniques are marked as green and undetected techniques are marked as red.

The same process was conducted to analyze all the Tactics from the threat intelligence report. The result of the complete gap analysis results is illustrated in Figure 22.

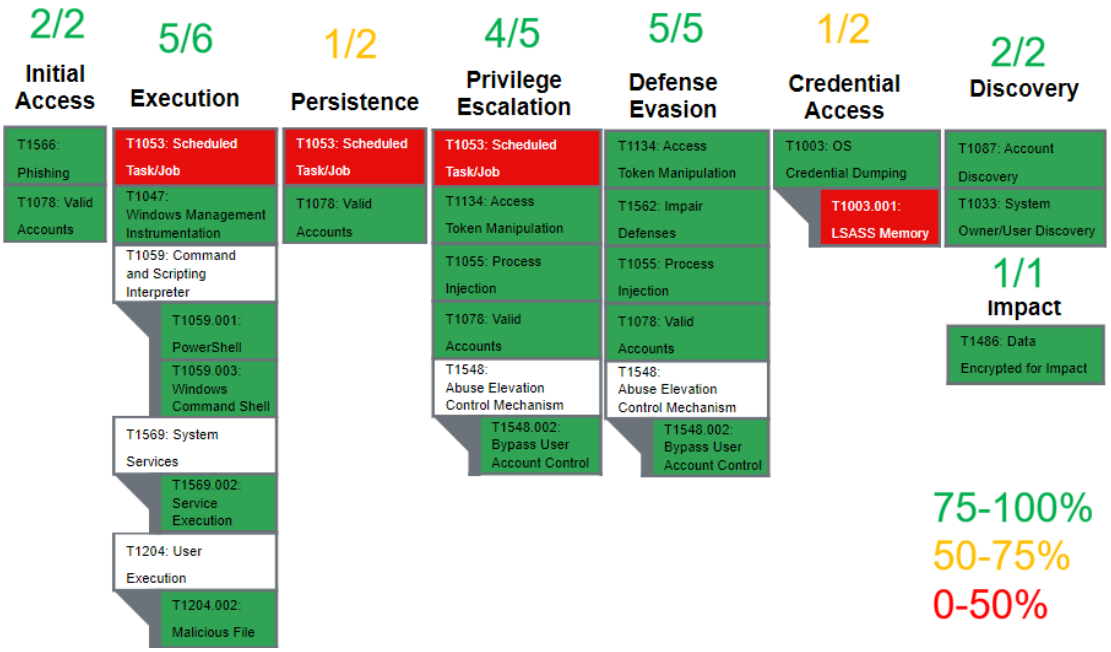


Figure 22. gap-analysis-1-human-operated-ransomware

Detected coverage by different ATT&CK abstraction levels:

- Tactics level: good coverage detected Tactics 8/8 Tactics used by the adversary
- Technique level: good coverage detected 10/11 Techniques used by the adversary
- Sub-technique level: good coverage detected 5/6 Sub-techniques used by the adversary

The gap analysis identified two gaps in the threat detection tools. One adversary Tactic: T1053 – Scheduled Task / Job and one Sub-technique: T1003.001 - LSASS Memory. The lack of detection rules identifying T1053 – Scheduled Task / Job impacts three different ATT&CK Tactics. The adversary can use this Technique to achieve multiple tactical goals.

5.3 Gap analysis 2 – Sophos - The Active Adversary Playbook 2021

The Sophos Active Adversary Playbook 2021 threat report illustrates Sophos telemetry, security incident reports, and the Sophos threat intelligence team's findings in 2020 and early 2021. The report includes TTPs that are categorized to the MITRE ATT&CK framework. Sophos aims for this report to help security teams understand what techniques adversaries use during attacks. (Shier, Gangwer, Iddon, & Mackenzie, 2021)

The analyzed Sophos report data differed from the previous adversary data used in the first gap analysis. The first report had clear TTPs to map specific adversary operations, but the Sophos report provided more overall statistics from every ATT&CK Tactics. Figure 23 illustrates the TTPs found in the Sophos threat intelligence report quoted from (Shier et al., 2021).

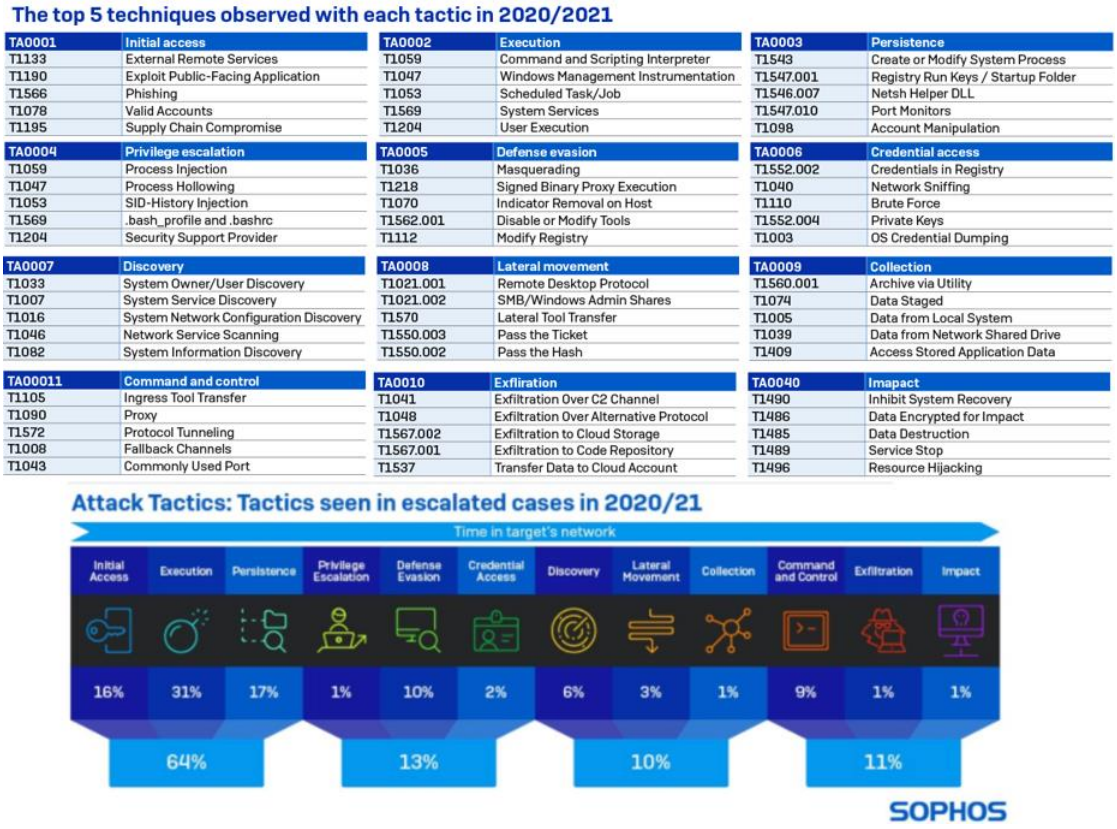


Figure 23. Sophos - The Active Adversary Playbook 2021 TTPs

The analysis identified adversary behavior in 12 Tactics, 40 different Techniques, and 13 Sub-techniques in the Sophos threat report. Results are illustrated in Figure 24.

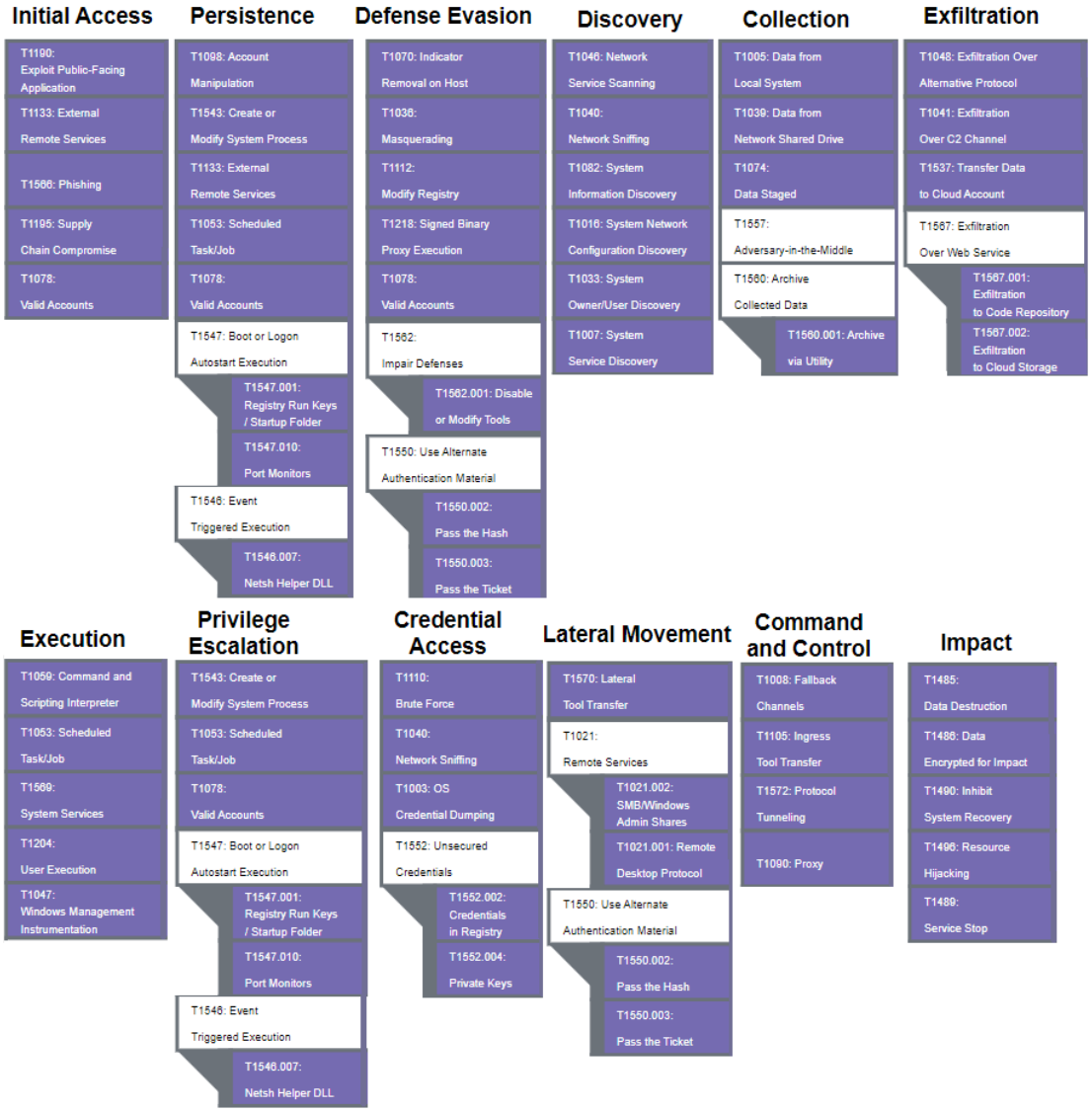


Figure 24. Sophos-secops-the-active-adversary-playbook-2021.json

Results of gap analysis two are illustrated in Figure 25. Detected coverage by different ATT&CK abstraction levels:

- Tactics level: good coverage detected Tactics 11/12 Tactics used by the adversary
- Technique level: decent coverage detected 25/40 Techniques used by the adversary
- Sub-technique level: bad coverage detected 5/13 Sub-techniques used by the adversary

Figure 25. gap-analysis-2–sophos-SecOps-the-active-adversary-playbook-2021.json

The security solutions' worst detection coverage were in Tactics: Credential Access and Collection. The best detection coverage in Tactics:

- Defense Evasion
- Lateral Movement
- Impact

5.4 Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access and Lateral Movement

According to Kremez & Boguslavskiy (2021), Conti was the first adversary group to weaponize the Log4j2 vulnerability. The threat actor did not use the Log4j2 vulnerability to gain initial access to an organization. Instead, use it in the lateral movement phase to exploit vulnerable VMware vCenter's from the pre-existent Cobalt Strike sessions. The main goal of Conti is to deploy ransomware to target organizations to make a profit. (Kremez & Boguslavskiy, 2021)

The analysis identified adversary behavior in 11 Tactics, 16 distinct Techniques, and 12 Sub-techniques in the Sophos threat report. Results are illustrated in Figure 26.

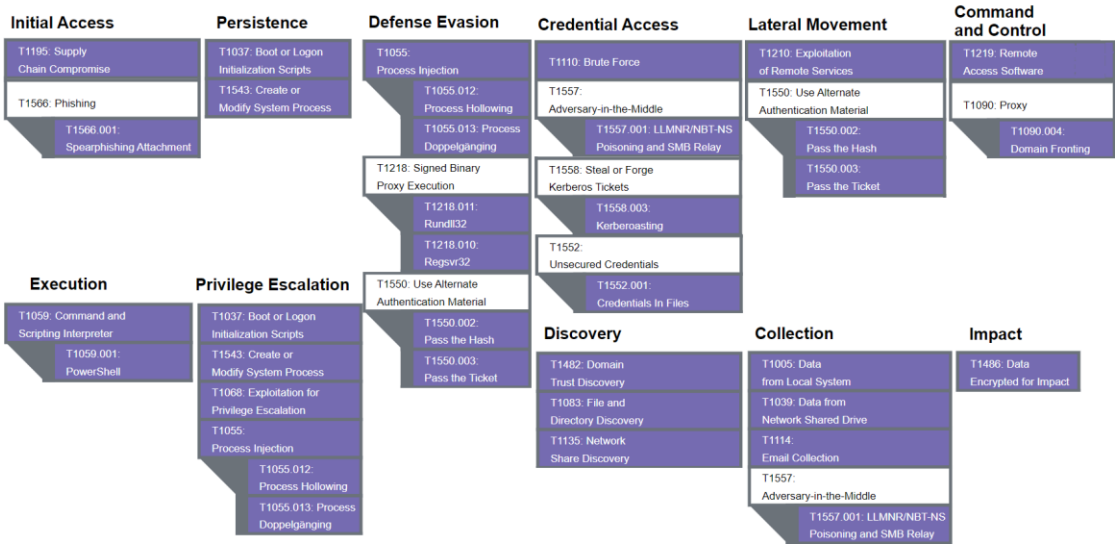


Figure 26. advintel-ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement.json

Results of gap analysis three are illustrated in Figure 27. Detected coverage by different ATT&CK abstraction levels:

- Tactics level: good coverage detected Tactics 11/11 Tactics used by the adversary
- Technique level: decent coverage detected 9/16 Techniques used by an adversary
- Sub-technique level: decent coverage detected 6/12 Sub-techniques used by the adversary

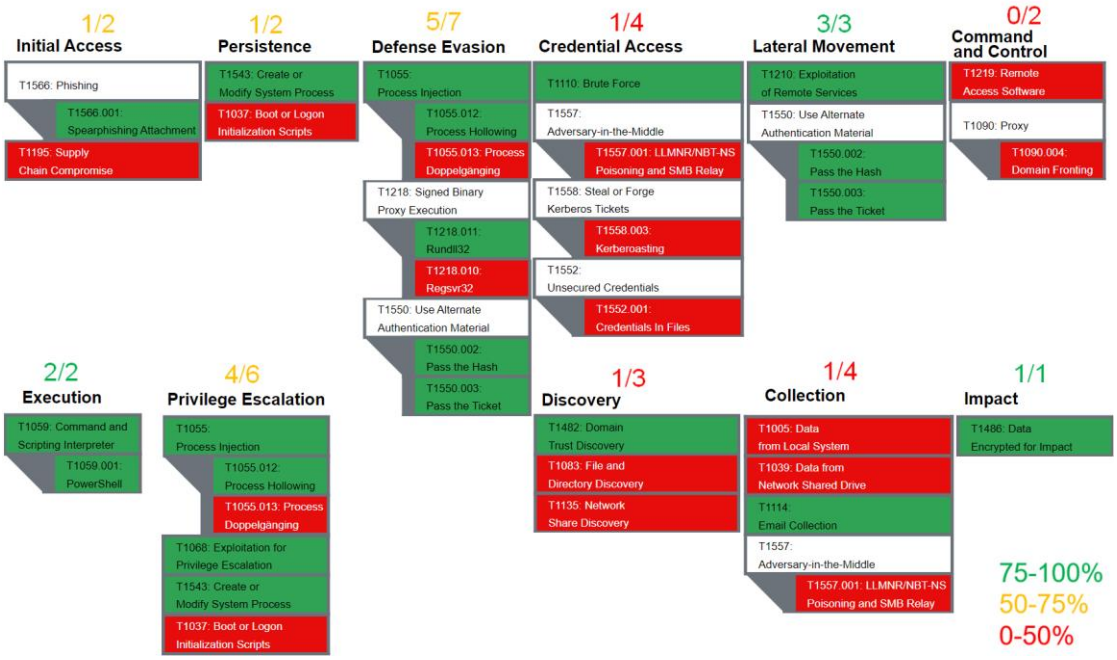


Figure 27. gap-analysis-3-ransomware-advisory-log4shell-exploitation-for-initial-access-&-lateral-movement.json

The security solutions did not have any detections in Command and Control Tactic. Additionally, Collection, Credential Access, and Discovery Tactics had only one Technique detected. The best detection coverage were in Tactics:

- Impact
- Lateral movement
- Execution

5.5 Gap analysis 4 - Nobelium Activity Targeting Government and Business Entities Around the Globe

This gap analysis is conducted using threat actor data from Mandiant. Mandiant claims that this threat actor is one of the most formidable actors they have encountered. Mandiant has given this threat actor APT naming: UNC2452. Microsoft refers to this actor as Nobelium. This threat intelligence report is based on TTPs what Mandiant has identified this threat actor's behavior in multiple different attacks across the globe. (Jenkins, Hawley, Najafi, & Bienstock, 2021) The analysis identified 12 Tactics, 43 distinct Techniques, and 29 Sub-techniques in the Mandiant threat report. Results are illustrated in Figure 28.

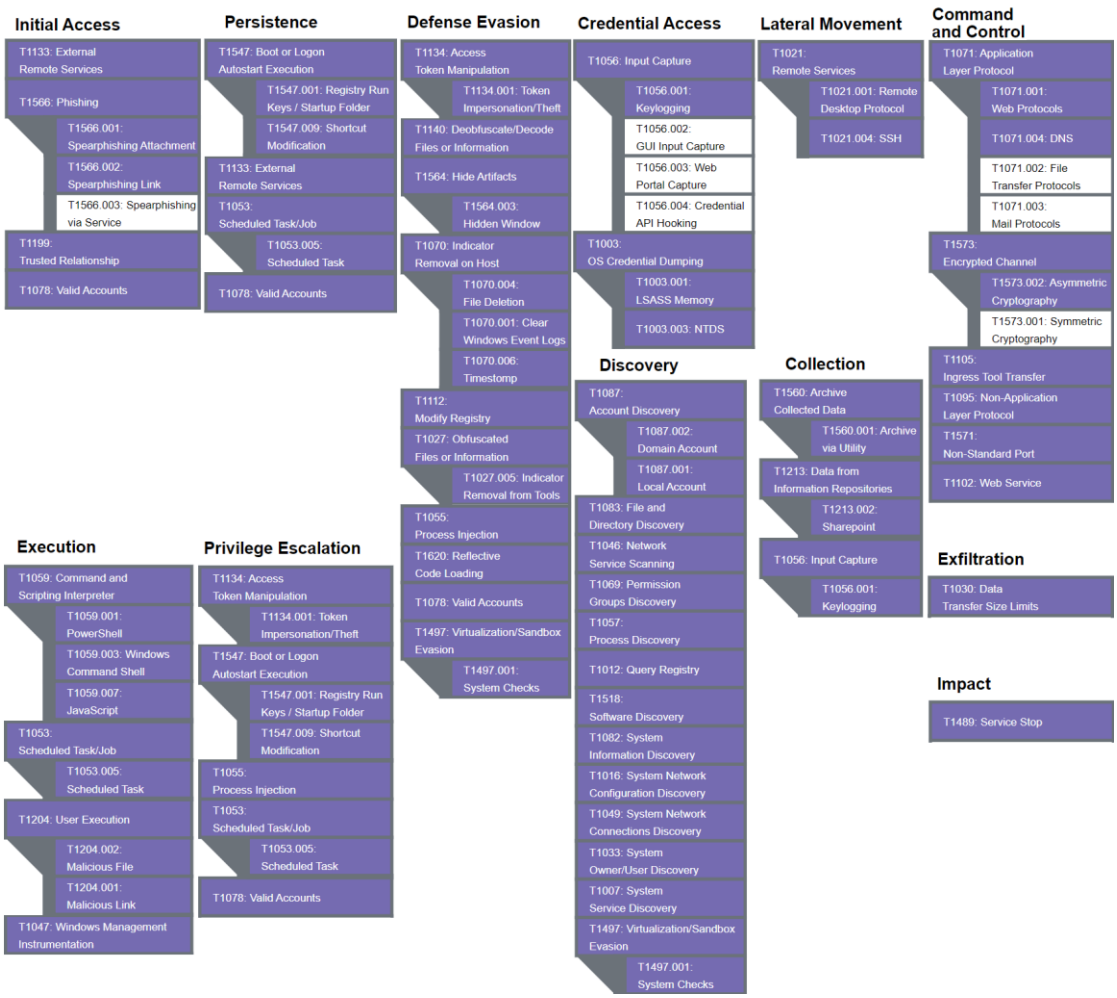


Figure 28. nobelium-activity-targeting-government-and-business-entities-around-the-globe.json

Results of gap analysis four are illustrated in Figure 29. Detected coverage by different ATT&CK abstraction levels:

- Tactics level: good coverage detected Tactics 11/12 Tactics used by the adversary
- Technique level: bad coverage detected 21/43 Techniques used by an adversary
- Sub-technique level: bad coverage detected 10/29 Sub-techniques used by the adversary

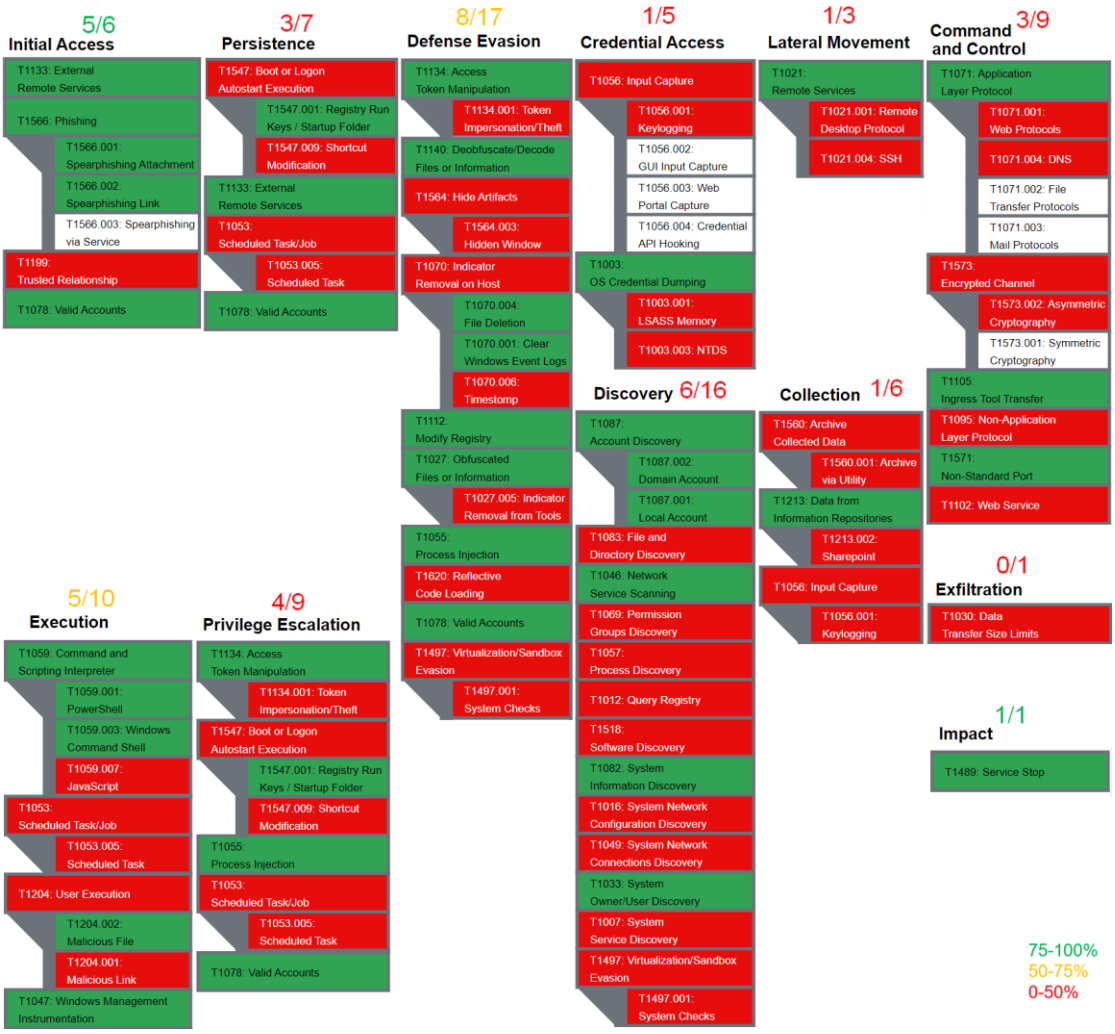


Figure 29. gap-analysis-4-nobelium-activity-targeting-government-and-business-entities-around-the-globe.json

The security solutions did not have any detections in Tactic: Exfiltration. Credential Access, Collection, and Lateral Movement Tactics had only one Technique detected, and the best detection coverage were in Tactics: Initial Access and Impact.

6 Results

6.1 Evaluation of the artifacts

In design science, research evaluating the artifacts should address how well the created artifacts solve the explicated research problem and fulfill the defined requirements. The evaluation process's goal can also be to spot new opportunities for further research. (Johannesson & Perjons, 2014) According to Gregor & Hevner (2013, 352), research evaluation should provide convincing evidence of how the study contributes to the subject.

Table 6 summarizes all the gap analyses conducted in this thesis. Based on these four gap analysis security solutions summaries, threat detection capabilities were worst against ATT&CK Tactic – Collection; only two of the 14 TTPs were detected. The best detection coverage Tactic was Impact, with seven of the eight TTPs detected. Based on the analysis of the selected security solutions, only three of the total 43 Tactics lacked any detection rules.

Table 6. Gap analysis summary

	Initial Access	Execution	Persistence	Privilege Escalation	Defensive Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gap analysis 1	2/2	5/6	1/2	4/5	5/5	1/2	2/2					1/1
Gap analysis 2	3/5	3/5	5/8	3/6	6/8	2/5	3/6	4/5	0/4	2/4	3/5	4/5
Gap analysis 3	1/2	2/2	1/2	4/6	5/7	1/4	1/3	3/3	1/4	0/2		1/1
Gap analysis 4	5/6	5/10	3/7	4/9	8/17	1/5	6/16	1/3	1/6	3/9	0/1	1/1
Sum	**11/15**	**15/23**	**10/19**	**15/26**	**24/37**	**5/16**	**12/27**	**8/11**	**2/14**	**5/15**	**3/6**	**7/8**

Figure 30 and Figure 31 illustrate the summary of all the gap analyses when presented at the MITRE ATT&CK framework layer. A combined larger figure can be seen in Appendix 7. The results are different from Table 6 since these are presented as distinct values.

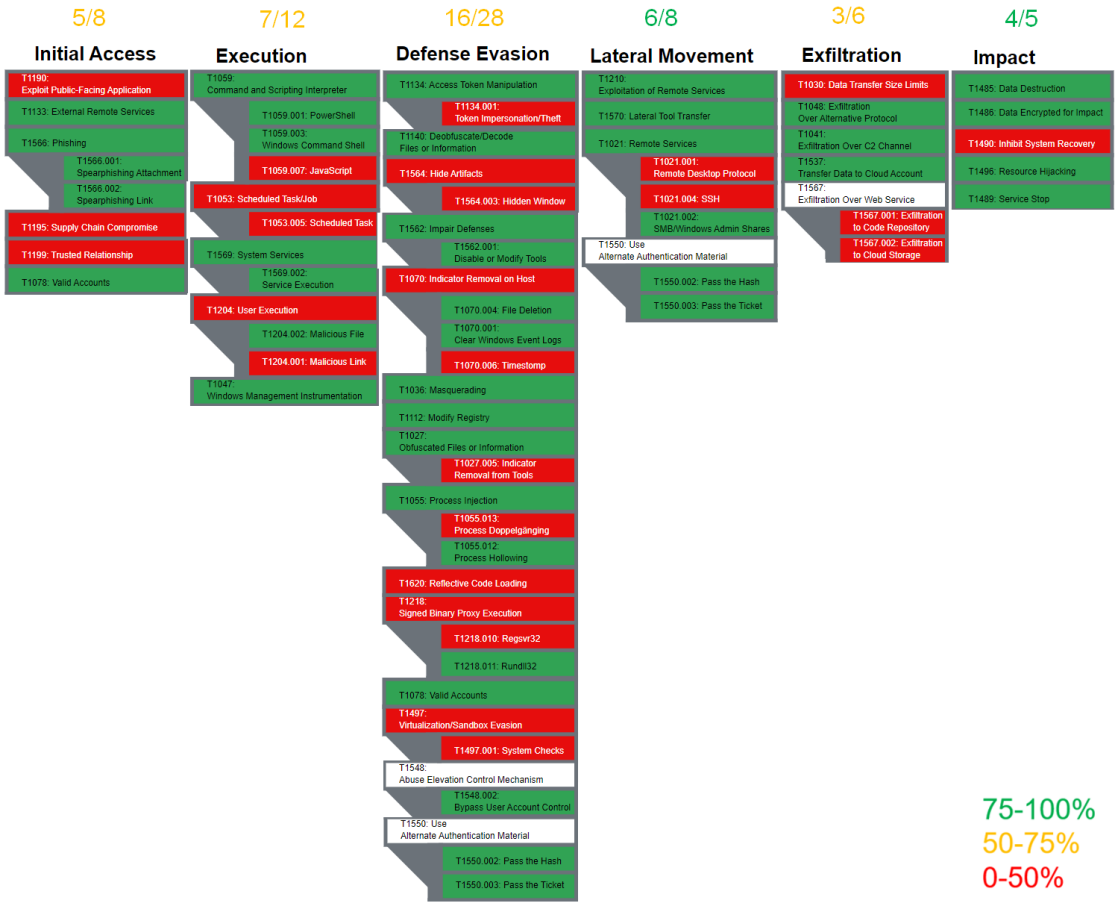


Figure 30. gap-analysis-summary-1.json

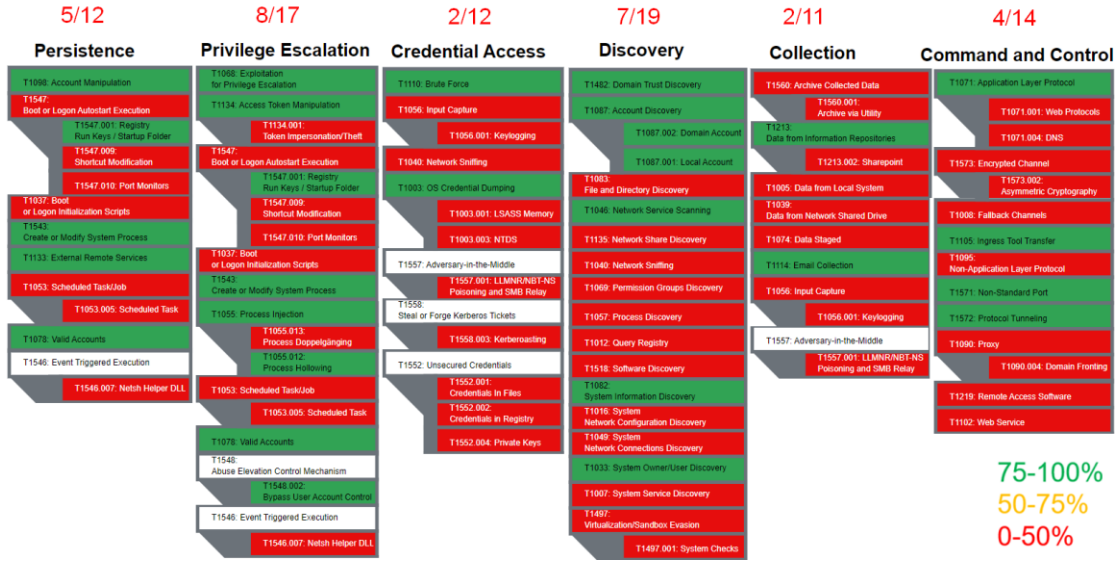


Figure 31. gap-analysis-summary-2.json

The author expressed a few open questions in chapter 4.1:

- Would it be enough to detect adversaries' attacks across the whole attack kill chain if an organization uses this toolset?
- Could we only rely on this toolset, or do we need additional detection tools to get better coverage?

Based on these findings, the security solutions have the decent capability to detect the adversaries' TTPs illustrated in the threat intelligence reports. The Impact was the most detected Tactic. Unfortunately, this is the adversary goal that causes the most damage to the organization.

Techniques in Tactic categories Credential Access and Collection were the least detected in the gap analyses. Illustrated in Figure 23, 1% of the total adversaries' TTPs seen in Sophos report were identified to Collection and 2% to Credential Access (Shier et al., 2021). Even when these Tactics were the worst, should the organization invest in new detection capabilities because the overall volume of the Tactics is so low. According to Shier et al. (2021), *"Early-stage tactics are the highest value detections for defenders because if they are blocked, they can neutralize and contain an attack before it has the chance to fully unfold and cause damage or disruption".*

In addition, the security solutions had a low success rate of detecting the TTPs in Tactics Command & Control and Exfiltration. Typically, these types of TTPs are detected with network devices. For example, firewalls, intrusion detection systems, and intrusion prevention systems. (The MITRE Corporation, n.d.) The selected security solutions did not include any data sources in this area.

The mapped security solutions had detection coverage to 23 Techniques and 30 Sub-techniques that were not seen in any of the adversaries' threat intelligence reports in Table 5. Figure 32 illustrates the coverage between different Tactics.

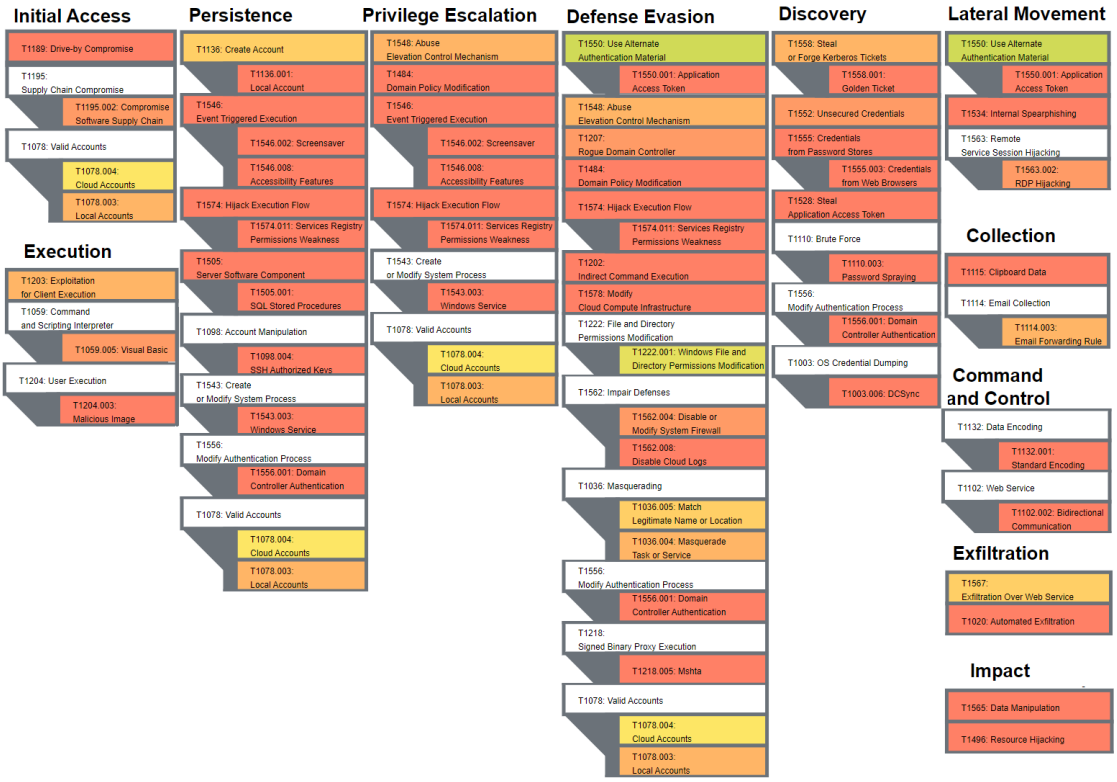


Figure 32. detection-but-not-in-adversary-reports.json

This analysis indicates that the security solutions have additional threat detection capabilities not introduced in this thesis. To answer one of the sub-research questions, it is possible to identify gaps in commercial security solutions. Additionally, the data used to conduct the gap analysis is not peer-reviewed, so the analyzed results may not be reliable or accurate.

6.2 Evaluation of the research

The artifacts' gap analysis and creation process were evaluated inside the organization, which assigned the author's research. The evaluation was conducted by organizing an online workshop where the author presented the research and gap analysis results. After the workshop, attendees filled out an online questionnaire using Microsoft Forms to evaluate the research. Respondents' identities cannot be identified from the survey responses. The workshop was two hours long, and the workshop's agenda is illustrated in Appendix 1. The workshop was conducted online using Microsoft Teams. Workshop attendees were chosen by their expertise and role

in the organization. A total of nine persons attended the workshop and evaluated the research. Workshop participants came from two different groups: Security Operations and Security Governance. The workshop was recorded for educational purposes. Permission to record the workshop was asked from the participants.

According to Brace (2018), the questionnaire must collect the mandatory data in the most precise way possible. A badly written questionnaire will result in data provided in the questionary being inaccurate thus not usable in the evaluation. A good questionnaire should answer the study's objectives, and the quality of the questionnaire can affect the remaining processes of the study. (Brace, 2018, 9-10.) The critical aim of the author was to build the questionnaire to give accurate data to the research that can be efficiently processed later and give value to answering the research questions. The printed form of the questionnaire can be found in Appendix 2.

The questionnaire was sectioned into three different sections:

- Objectives and theory of the thesis
- Implementation of the thesis
- Conclusions and future work

According to Brace (2018, 45), sectioning the questionnaire is an excellent way to flow logically from one subject area to the next in the questionnaire. The questionnaire sections were planned according to the table of contents of the study, moving from more straightforward questions to more challenging in the last section. There was an additional question about what gap analysis was the most interesting to workshop participants.

The questions in each section were asked using Likert scales. Likert scales are typically used in online questionnaires. Likert scales are a series of questions where responders are asked to answer whether, and how strongly they agree or disagree, the answer to the question. (Brace, 2018, 95) Each section included 4-5 short questions around the section topic. According to Brace (2018, 16), short questions give researchers better and more accurate answers than long and complicated questions. There was a free feedback text at the end of every section so that responders could leave optional feedback or comments about the questions selected

in the questionnaire. Giving respondents free feedback questions in the questionnaire can provide much richer data to the research (Brace, 2018, 65). All answers to free feedback questions can be seen in Appendix 4.

Objectives and theory of the thesis

The first section's goal was to measure participants' learning and understanding of the research topic who attended the workshop. Did they get enough information in the workshop to understand the research scope? Did they understand how the scope of the research was limited, and did they understand the research goals? The results of the evaluation section are illustrated in Figure 33.

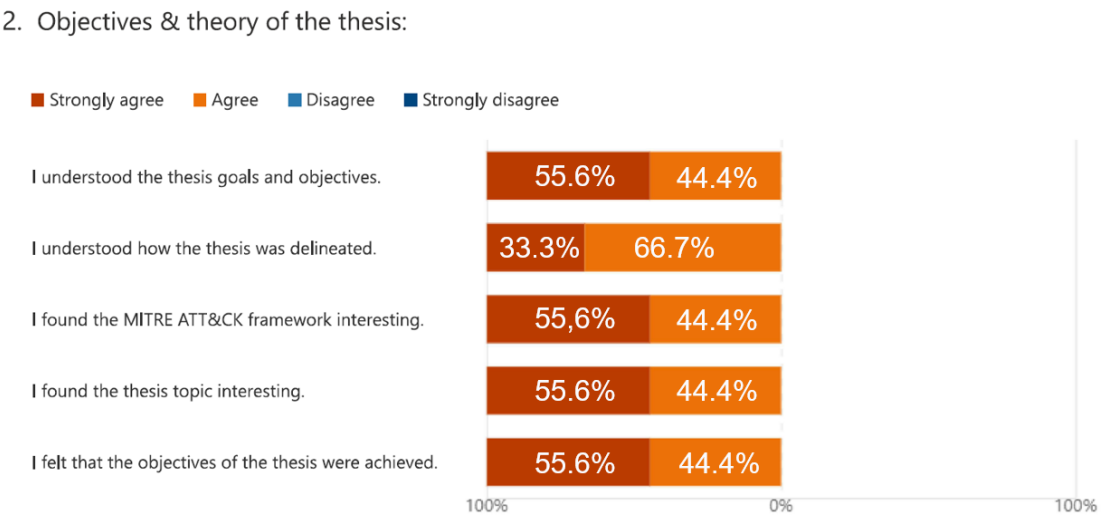


Figure 33. Evaluation of objectives and theory

These questions gave a good understanding of the participants' knowledge. If they had not understood the topic and the goal, the answers from the last questions would have less value because of a knowledge gap. There was no single negative answer to any of the Likert questions in this section. One respondent provided free feedback, *"A bit better explanation of why MITRE was chosen instead of something else and why it's relevant today would have been good."* The framework's relevance should be described more accurately in future workshops.

Implementation of the thesis

The second part of the questionnaire's aim was to evaluate the actual implementation of the research. How did the attendees think about the research outcomes, and did they find the study interesting in the first place? Did they believe that the selected security solutions and threat intelligence reports for adversary behavior chosen for the research were relevant to them? In addition, the MITRE ATT&CK framework's suitability as a tool to perform the gap analysis was evaluated. The second part evaluation results are illustrated in Figure 34.

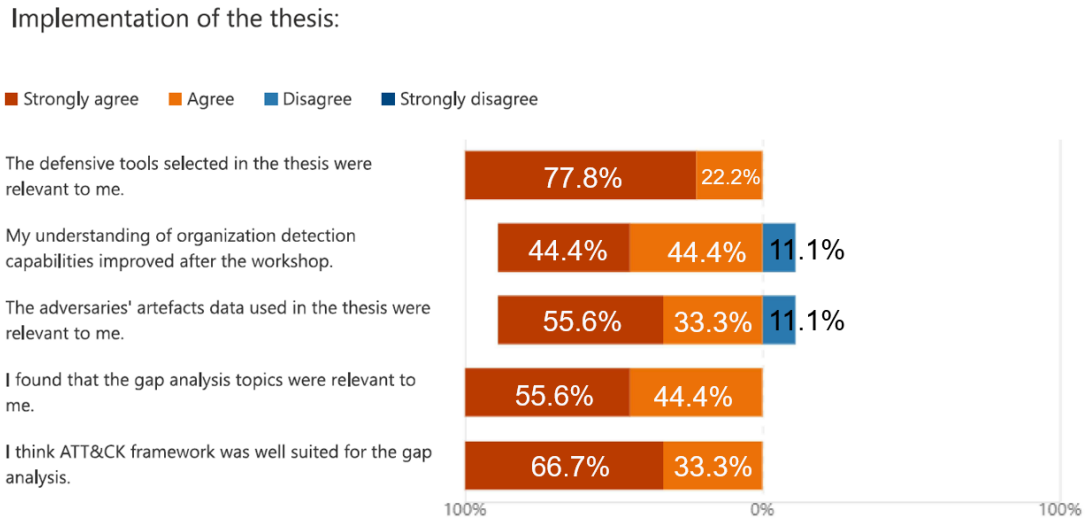


Figure 34. Evaluation of the research implementation

One of the Security Government participants felt that the threat intelligence data used in this thesis was not relevant. This might result from the author not presenting the results in an exciting way in the conducted workshop, or the selected reports did not have enough congregation for the participant. Additionally, one Security Operations participant did not feel that the thesis brings any additional understanding of the detection capabilities of the selected security solutions. This might be due to the high level of maturity of the specialist, or the author did not describe the solution's capabilities detailed enough in the workshop.

Part of the implementation section was a question of what gap analysis example was the most interesting to workshop participants. For this question author tried to

assess what kind of workshop topics would be the most interesting in the future. The results are illustrated in Figure 35.

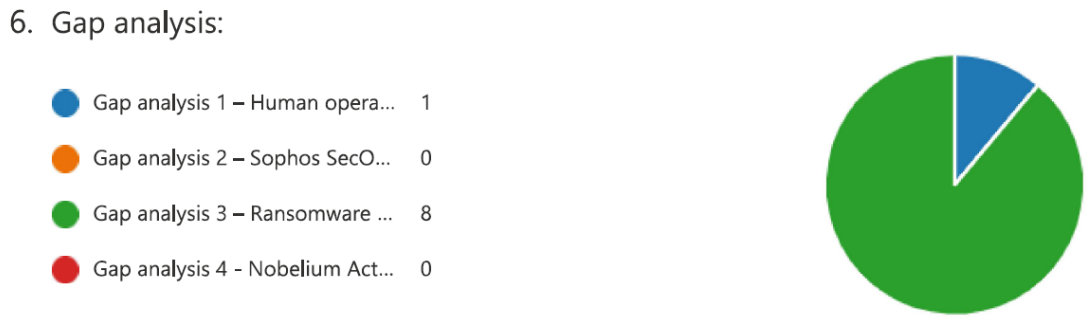


Figure 35. Most interesting gap analysis in a workshop

Eight of the nine participants found that the report using Log4j vulnerability to conduct an attack was the most interesting analysis. This result was a bit surprising to the author, but due to the timing and the media visibility of the case, it might not be so surprising. One of the participants gave free feedback: *"Gap analysis 3 highlighted the various stages of the attack in the most extensive way, and because this is the latest vulnerability globally, it clarified the picture of how advanced attacks are conducted today."* This indicates that recent events are often typically interesting to most people.

Conclusions and future work

In the conclusion and future work section, one of the research goals was to improve the organization's understanding of the research topic. These questions were used to measure the learning of the workshop participants and did they get enough perspective of the research. Did the participants get any new ideas about using the knowledge? Either improve the organization's security posture or create new business ideas. Answers for this section are illustrated in Figure 36.

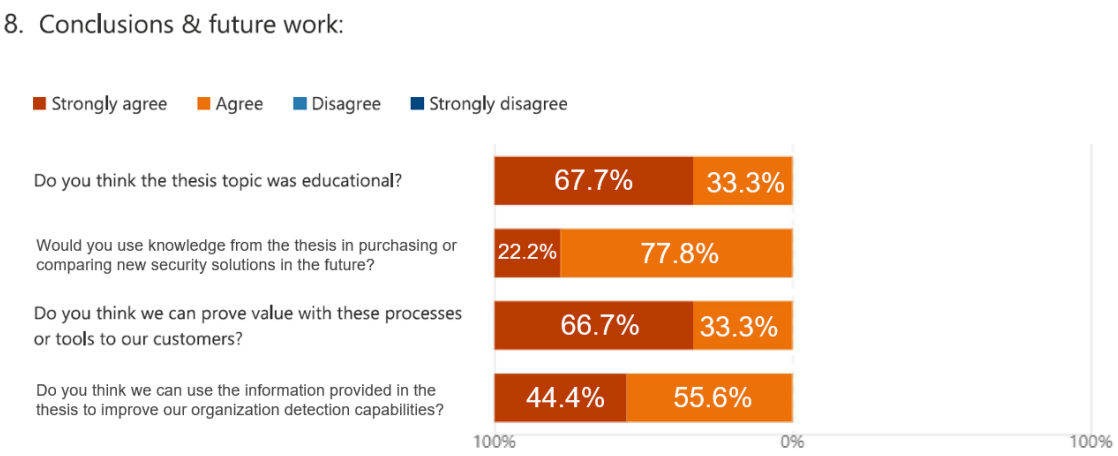


Figure 36. Evaluation of conclusions and future work

All the answers to the conclusions and future work section were positive. One of the participants gave free feedback: "*Future work could be that what is the most 'cost effective' way to improve organization detection capabilities.*" This could be a suitable research topic for the future.

6.3 Research objectives results

The thesis aimed to answer one main research question:

- Can gap analysis using the MITRE ATT&CK framework improve an organization's understanding of its threat detection capabilities?

Three sub-research questions were created to answer the main research question:

- Is the MITRE ATT&CK framework suitable for conducting the gap analysis?
- Are the identified gaps useful to improve the detection capabilities?
- Is it possible to identify and detect gaps from commercial security solutions?

The author used the Design Science Research method to create artifacts to help answer the research questions. The created artifacts provide new knowledge to the security community, and the author demonstrated the practical use of the created artifacts in the thesis. The selected research method provided a good backrest and frame for implementing the research. Based on the gap analysis where the artifacts were used, the author managed to find detection gaps between the threat intelligence reports and the security solutions. The hands-off method selected to

map the detection coverage was suitable based on the author's opinion. Conducting complete adversary enumeration to such a broad set of tools would have probably been too big a research scope for the individual researcher.

Based on the questionnaire result, 100% of the respondents agreed or strongly agreed that the research objectives were achieved. Additionally, 100% of the respondents agreed or strongly agreed that the MITRE ATT&CK was suitable for the gap analysis. 89% of the respondents felt that their understanding of the detection capabilities grew. As an answer to the research question conducting gap analysis improved the organization's understanding of the threat detection capabilities. In addition, the MITRE ATT&CK framework was found suitable for performing the gap analysis.

The results of the survey are a bit controversial to the author. The author has worked with most of the respondents in the past. This may have had a positive effect on the responses to the survey and the reliability of research results. For future research and more accurate results, this same workshop and questionnaire could be conducted to a broader set of audiences to get more reliable results.

7 Discussion

Many commercial tools have different licensing models. Usually, not all the organization assets, identities, and data are protected with the same security solutions. Organizations must know what solutions are protecting what assets and where. For example, do we use the same detection tools in our workstations, servers, or mobile devices? What about the tools protecting organization workloads in the cloud or on-premises? In addition, information regarding asset inventory is crucial. Organizations cannot defend something that they do not know.

While the accuracy of the produced artifacts was not a measure or goal of the research, the MITRE ATT&CK mappings were done purely on the hands-off method. The author believes that the created artifacts provide new information and contribution for future research. Future research could validate the accuracy of the artifact's threat detection capabilities. An adversary emulation or peer review could be used to validate the security solutions' threat detection capabilities. The defensive

forged artifacts represent commercial products, and the security solutions are Software as a Service (SaaS) solutions, so they evolve and change rapidly. In addition, every production environment is different and can contain customization regarding the security solutions configurations that could affect the mapping accuracy. The MITRE ATT&CK Techniques are not static either threat landscape is constantly evolving, and new TTPs and vulnerabilities are introduced continuously. The layers should be updated regularly to get actionable information.

This research gives a good foundation for the assigner organization to improve visibility and documentation for threat detection capabilities. Future research and improvements could expand the artifact coverage to all organization data sources and detection capabilities—for example, Security Information and Event Management (SIEM) tools threat detection rules. Security solutions used in this research can provide raw data and telemetry to the SIEM system where the defenders can make custom rulesets to detect specific adversary techniques. These custom rules might give better coverage to identified gaps in this research.

The outcome can differ depending on the metrics used to illustrate the research results. When conducting the gap analysis based on maturity, organizations can choose different abstraction levels in the MITRE ATT&CK framework. The mapping process is complex and requires lots of knowledge for the MITRE ATT&CK framework and the selected toolset's abilities and capabilities. Detecting all the TTPs in the ATT&CK matrix is unnecessary to detect and stop the adversary attack. The technology only serves one part of the detection process. A trained defender can identify relations and chain the indicators to the attack kill chain. This thesis did not provide any input to mitigate the actual threat detections. This could be a fit for future research.

When analyzing information from threat intelligence reports from security vendors researcher needs to keep in mind what kind of solution has detected the adversary behavior. If a firewall vendor publishes a threat report, it may not contain accurate results for threats found on workstations. Additionally, vendors publish reports for the found TTPs. The unseen ones are not detected and reported. The gap analysis data should be scoped per organization rather than generic data. The adversary information could be useless if it does not possess a threat or motivation. In the

defensive gap analysis, both artifacts should be functional and targeted to the organization when conducted.

References

Bautista Jr., W. (2018). *Practical Cyber Intelligence.* Packt Publishing Ltd.

Berady, A., Jaume, M., Tong, V. V., & Guette, G. (2021, June). From TTP to IoC: Advanced Persistent Graphs for Threat Hunting. *18*(2). doi:10.1109/TNSM.2021.3056999

BeyondTrust. (2021). *Malware Threat Report 2021.* Retrieved November 21, 2021, from beyondtrust.com: https://www.beyondtrust.com/resources/whitepapers/malware-threat-report-2021

Bianco, D. J. (2014, January 1). *The Pyramid of Pain*. Retrieved October 16, 2021, from http://detect-respond.blogspot.com/: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Brace, I. (2018). *Questionnaire design* (Fourth edition 2018 ed.). Kogan Page Limited.

Chapple, M., & Seidl, D. (2017). *CompTIA Cybersecurity Analyst (CySA+) Study Guide Exam CS0-001.* Indianapolis, Indiana: Wiley & Sons, Inc.

Chapple, M., & Seidl, D. (2019). *CompTIA PenTest+ Study Guide.* Indianapolis, Indiana: John Wiley & Sons, Inc. Retrieved January 13, 2022

Chow, E. (2021, June 27). *Lockheed Martin Cyber Kill Chain vs. MITRE ATTACK Framework*. Retrieved January 29, 2022, from eric-chow.medium.com: https://eric-chow.medium.com/lockheed-martin-cyber-kill-chain-vs-mitre-attack-framework-64f8f3bf1e58

CISA. (2021, June). *us-cert.cisa.gov.* Retrieved October 17, 2021, from Best Practices for MITRE ATT&CK® Mapping: https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisa-releases-best-practices-mapping-mitre-attckr

Cox, O. (n.d.). *Darktrace Blog*. Retrieved January 13, 2022, from darktrace.com: https://www.darktrace.com/en/blog/living-off-the-land-how-hackers-blend-into-your-environment/

Cybersecurity Insiders. (2021). *Industry Report: The State of MITRE ATT&CK® Threat-Informed Defense in 2021.* Retrieved January 29, 2022, from mitre-engenuity.org: https://mitre-engenuity.org/mad/state_of_attack_report_2021/

Cyware. (2021, August 12). *The Concept of Pyramid of Pain*. Retrieved February 11, 2022, from cyware.com: https://cyware.com/educational-guides/cyber-threat-intelligence/the-concept-of-pyramid-of-pain-f358

Diaz, V. (2021, October). *We analyzed 80 million ransomware samples – here's what we learned*. Retrieved October 15, 2021, from blog.google: https://blog.google/technology/safety-security/we-analyzed-80-million-ransomware-samples-heres-what-we-learned/

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity – Attack and Defense Strategies.* Packt Publishing Ltd.

Ecma International. (2017, December). *The JSON data interchange syntax.* Retrieved January 16, 2022, from ecma-international.org: https://www.json.org/json-en.html

F-Secure. (2021, September). *F-Secure Threat Highlights Report August 2021.* Retrieved September 5, 2021, from F-secure.com: https://www.f-secure.com/content/dam/f-secure/en/business/g/f-secure-threat-highlights-report-2021-08.pdf

Gregor, S., & Hevner, A. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *Vol 7 No. 2.* MIS Quarterly.

Hallberg, J. (2020, May). *Event-driven Analysis of Cyber Kill Chain.* Master's thesis. Retrieved January 27, 2022, from https://urn.fi/URN:NBN:fi:amk-2020060416949

Hyppönen, M. (2021). *Internet.* WSOY.

IBM Security. (2021, June). *Cost of a Data Breach Report 2021 explores ways to help mitigate risk.* Retrieved November 25, 2021, from ibm.com: https://www.ibm.com/security/data-breach

Jaafar, F., Avellaneda, F., & Alikacem, E.-H. (2020). Demystifying the Cyber Attribution: An Exploratory Study. (pp. 35-40). IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). doi:10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00022

JAMK. (2022, January 25). *Opinnäytetyön raportointi.* Retrieved February 10, 2022, from oppimateriaalit.jamk.fi: https://oppimateriaalit.jamk.fi/raportointiohje/5-lahteiden-kaytto/5-2-tekstiviitteiden-merkinta/

JAMK University of Applied Sciences. (2018, December 11). *Ethical Principles for JAMK University of Applied Sciences.* Retrieved February 10, 2022, from jamk.fi: https://www.jamk.fi/sites/default/files/2021-12/Ethical%20Principles%2011122018.pdf

Järvinen, P. (2018). *Kyberuhkia ja somesotaa.* Docenco.

Jenkins, L., Hawley, S., Najafi, P., & Bienstock, D. (2021, December 6). *Suspected Russian Activity Targeting Government and Business Entities Around the Globe*. Retrieved December 27, 2021, from mandiant.com: https://www.mandiant.com/resources/russian-targeting-gov-business

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science.* Springer International Publishing Switzerland.

Kaspersky IT Encyclopedia. (n.d.). *Living off the Land (LotL) attack*. Retrieved January 13, 2022, from encyclopedia.kaspersky.com: https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/

Khalid, A., Zainal, A., Maarof, M. A., & Ghaleb, F. (2021). Advanced Persistent Threat Detection: A Survey. *3rd International Cyber Resilience Conference (CRC)* (pp. 1-6). IEEE. doi:10.1109/CRC50527.2021.9392626

Kremez, V., & Boguslavskiy, Y. (2021, December 17). *Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement*. Retrieved December 27,

2021, from advintel.io: https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement

LogRhythm. (n.d.). *Using MITRE ATT&CK™ in Threat Hunting and Detection.* Retrieved January 29, 2022, from logrhythm.com: https://logrhythm.com/uws-using-mitre-attack-in-threat-hunting-and-detection-white-paper/

Magowan, K. (2017, January). *Organizations Continue to Struggle with Cyber Security*. Retrieved December 12, 2021, from itchronicles.com: https://itchronicles.com/news/organizations-continue-struggle-cyber-security/

Mark, C. (2020, February 19). *Understanding cyber attacker motivations to best apply controls*. Retrieved January 13, 2022, from AT&T Cybersecurity: https://cybersecurity.att.com/blogs/security-essentials/understanding-cyber-attacker-motivations-to-best-apply-controls

marmcimsft. (2020, October). *Microsoft's End-to-End Security Commitments to Our Customers*. Retrieved October 15, 2021, from techcommunity.microsoft.com: https://techcommunity.microsoft.com/t5/public-sector-blog/microsoft-s-end-to-end-security-commitments-to-our-customers/ba-p/1784105

Mavroeidis, V., Hohimer, R., Casey, T., & Jøsang, A. (2021). Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. *13th International Conference on Cyber Conflict (CyCon)* (pp. 327-352). IEEE. doi:10.23919/CyCon51939.2021.9468305

McGuiness, T. (2001, November). *Defense In Depth.* Retrieved November 25, 2021, from sans.org: https://www.sans.org/white-papers/525/

Microsoft. (2020, September). *Microsoft Digital Defense Report 2020.* Retrieved September 5, 2021, from Microsoft.com: https://www.microsoft.com/en-us/security/business/security-intelligence-report

Microsoft. (2021a, October). *Microsoft Digital Defense Report OCTOBER 2021.* Retrieved October 11, 2021, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Microsoft. (2021b, October 11). *How to investigate anomaly detection alerts*. Retrieved October 30, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts

Microsoft. (2021c, June 30). *Microsoft Defender for Identity Security Alerts*. Retrieved June 11, 2021, from docs.microsoft.com/: https://docs.microsoft.com/en-us/defender-for-identity/suspicious-activity-guide

Microsoft. (2021d, October 15). *Alert policies in Microsoft 365*. Retrieved October 30, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Microsoft. (2021e, October). *Security alerts - a reference guide*. Retrieved October 30, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

Microsoft, Azure Defender. (2021, October). *Introduction to Azure Defender for servers*. Retrieved October 31, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction

Microsoft, Cloud App Security. (2021, October). *Microsoft Cloud App Security overview*. Retrieved October 31, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Microsoft, Defender for Identity. (2021, September). *What is Microsoft Defender for Identity?* Retrieved October 31, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/defender-for-identity/what-is

Microsoft, Defender for Office 365. (2021, October). *Microsoft Defender for Office 365*. Retrieved October 31, 2021, from docs.microsoft.com: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365

MITRE ATT&CK Defender™ (MAD). (2021). ATT&CK® SOC Assessments Certification Training. Retrieved October 16, 2021, from

https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-soc-assessments/

MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training (2021). [Motion Picture]. Retrieved October 15, 2021, from https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence/

Oriyano, S.-P. (2016). *Certified Ethical Hacker Version 9 - Study Guide.* John Wiley & Sons, Inc.

Pell, R., Emmanouil, P., Sotiris, M., & Ryan, H. (2021, October 14). Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK. *v4*, 13. Retrieved from https://arxiv.org/abs/2108.11206

Picus Labs. (2020, May). *The Top Ten MITRE ATT&CK Techniques*. Retrieved October 24, 2021, from picussecurity.com: https://www.picussecurity.com/resource/the-top-ten-mitre-attck-techniques

Reiber, J., & Wright, C. (2020, November). *https://attackiq.com/lp/mitre-attack-for-dummies/.* Retrieved October 16, 2021, from attackiq.com: https://attackiq.com/lp/mitre-attack-for-dummies/

Shier, J., Gangwer, M., Iddon, G., & Mackenzie, P. (2021, May 14). *The Active Adversary Playbook 2021.* Retrieved November 10, 2021, from news.sophos.com: https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., . . . Wolf, R. D. (2017, June). *Finding Cyber Threats with ATT&CK™-Based Analytics.* Retrieved October 9, 2021, from https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2020, March). *MITRE ATT&CKÒ: Design and Philosophy.* Retrieved October 9, 2021, from attack.mitre.org:

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

The MITRE Corporation. (2021a). *Corporate Overview*. Retrieved October 9, 2021, from https://www.mitre.org/about/corporate-overview

The MITRE Corporation. (2021b, October). Retrieved October 9, 2021, from Enterprise tactics: https://attack.mitre.org/tactics/enterprise/

The Mitre Corporation. (2021c, October). *Valid Accounts*. Retrieved January 19, 2022, from attack.mitre.org: https://attack.mitre.org/techniques/T1078/

The MITRE Corporation. (2021d, September 13). *Enterprise Techniques*. Retrieved January 19, 2022, from attack.mitre.org: https://attack.mitre.org/techniques/enterprise/

The MITRE Corporation. (n.d.). *Data Sources*. Retrieved January 13, 2022, from attack.mitre.org: https://attack.mitre.org/datasources/

Trend Micro. (2015, October). *Understanding Targeted Attacks: Goals and Motives*. Retrieved December 4, 2021, from trendmicro.com: https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives

Turner, B., Toor, O., Smith, D., & Mcwhirt, M. (2022, January 14). *Proactive Preparation and Hardening to Protect Against Destructive Attacks.* Retrieved January 19, 2022, from mandiant.com: https://www.mandiant.com/resources/protect-against-destructive-attacks

Vaishnavi, V. K. (2019, June 30). Design Science Research in Information Systems. Retrieved October 3, 2021, from http://www.desrist.org/design-research-in-information-systems/

Walkowski, D. (2019, August 22). *What Are Security Controls?* Retrieved from f5.com: https://www.f5.com/labs/articles/education/what-are-security-controls

Yannakogeorgos, P. A. (2016, May). *Strategies for Resolving the Cyber Attribution Challenge.* Retrieved December 4, 2021, from media.defense.gov:

https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF

Appendices

Appendix 1. Workshop agenda

Introduction to the research and introduction to the research method

- Research method - Research-based development
- Research goals and objectives
- Research questions that are answered
- How is the research delineated?
- Define tool and process to help the organization document and understand detection capabilities
- Assumptions of the results of the thesis

The theory around the MITER ATT&CK framework and solutions & processes used in research

- MITRE ATT&CK Enterprise Matrix overview
- Ideology behind thread detection
- Design and development of defensive artifacts
- Presenting the process and methodology of mapping the artifacts
- Introduction of the defensive tools used in research:
    - Microsoft Defender for Identity
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Office 365
    - Microsoft Defender for Cloud (Windows Machines)
- Defensive artifact mapping example – Microsoft Defender for Identity

Presentation of the results of the research through gap analysis:

- Definition of gap analysis
- Gap analysis 1 – Human operated ransomware
- Gap analysis 2 – Sophos SecOps - The Active Adversary Playbook 2021
- Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement
- Gap analysis 4 - Nobelium Activity Targeting Government and Business Entities Around the Globe

Gathering feedback and evaluation of the research through MS forms

Appendix 2. Evaluation questionnaire

* Required

1. Choose your role in the organization *

- ◯ Security Operations
- ◯ Security Government

Objectives & theory of the thesis

2. Objectives & theory of the thesis: *

	Strongly agree	Agree	Disagree	Strongly disagree
I understood the thesis goals and objectives.	◯	◯	◯	◯
I understood how the thesis was delineated.	◯	◯	◯	◯
I found the MITRE ATT&CK framework interesting.	◯	◯	◯	◯
I found the thesis topic interesting.	◯	◯	◯	◯
I felt that the objectives of the thesis were achieved.	◯	◯	◯	◯

3. Free feedback for the objectives & theory of the thesis or previous questions. (Optional)

Implementation of the thesis

4. Implementation of the thesis: *

	Strongly agree	Agree	Disagree	Strongly disagree
The defensive tools selected in the thesis were relevant to me.	○	○	○	○
My understanding of organization detection capabilities improved after the workshop.	○	○	○	○
The adversaries' artefacts data used in the thesis were relevant to me.	○	○	○	○
I found that the gap analysis topics were relevant to me.	○	○	○	○
I think ATT&CK framework was well suited for the gap analysis.	○	○	○	○

5. Free feedback for the implementation of the thesis or previous questions. (Optional)

Gap analysis

Witch of the gap analysis scenarios were the most interesting in the workshop?

6. Gap analysis: *

- ◯ Gap analysis 1 – Human operated ransomware
- ◯ Gap analysis 2 – Sophos SecOps - The Active Adversary Playbook 2021
- ◯ Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement
- ◯ Gap analysis 4 - Nobelium Activity Targeting Government and Business Entities Around the Globe

7. Why it was interesting? *

Conclusions & future work

8. Conclusions & future work: *

	Strongly agree	Agree	Disagree	Strongly disagree
Do you think the thesis topic was educational?	◯	◯	◯	◯
Would you use knowledge from the thesis in purchasing or comparing new security solutions in the future?	◯	◯	◯	◯
Do you think we can prove value with these processes or tools to our customers?	◯	◯	◯	◯
Do you think we can use the information provided in the thesis to improve our organization detection capabilities?	◯	◯	◯	◯

9. Free feedback for the future work or previous questions. (Optional)

Appendix 3. Questionnaire raw answers

Objectives & theory of the thesis

Choose your role in the organization	I understood the thesis goals and objectives.	I understood how the thesis was delineated.	I found the MITRE ATT&CK framework interesting.	I found the thesis topic interesting.	I felt that the objectives of the thesis were achieved.
Security Government	Strongly agree	Agree	Strongly agree	Agree	Strongly agree
Security Government	Strongly agree	Agree	Agree	Agree	Strongly agree
Security Operations	Agree	Agree	Strongly agree	Strongly agree	Agree
Security Operations	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
Security Government	Agree	Strongly agree	Agree	Strongly agree	Agree
Security Operations	Strongly agree	Strongly agree	Agree	Agree	Strongly agree
Security Operations	Agree	Agree	Strongly agree	Strongly agree	Agree
Security Operations	Strongly agree	Agree	Strongly agree	Strongly agree	Strongly agree
Security Operations	Agree	Agree	Agree	Agree	Agree

Implemantation of the thesis

Choose your role in the organization	The defensive tools selected in the thesis were relevant to me.	My understanding of organization detection capabilities improved after the workshop.	The adversaries' artefacts data used in the thesis were relevant to me.	I found that the gap analysis topics were relevant to me.	I think ATT&CK framework was well suited for the gap analysis.
Security Government	Strongly agree	Strongly agree	Agree	Agree	Strongly agree
Security Government	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Agree
Security Operations	Strongly agree	Agree	Agree	Strongly agree	Strongly agree
Security Operations	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
Security Government	Agree	Agree	Disagree	Agree	Agree
Security Operations	Strongly agree	Agree	Strongly agree	Strongly agree	Strongly agree
Security Operations	Strongly agree	Agree	Strongly agree	Agree	Strongly agree
Security Operations	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
Security Operations	Agree	Disagree	Agree	Agree	Agree

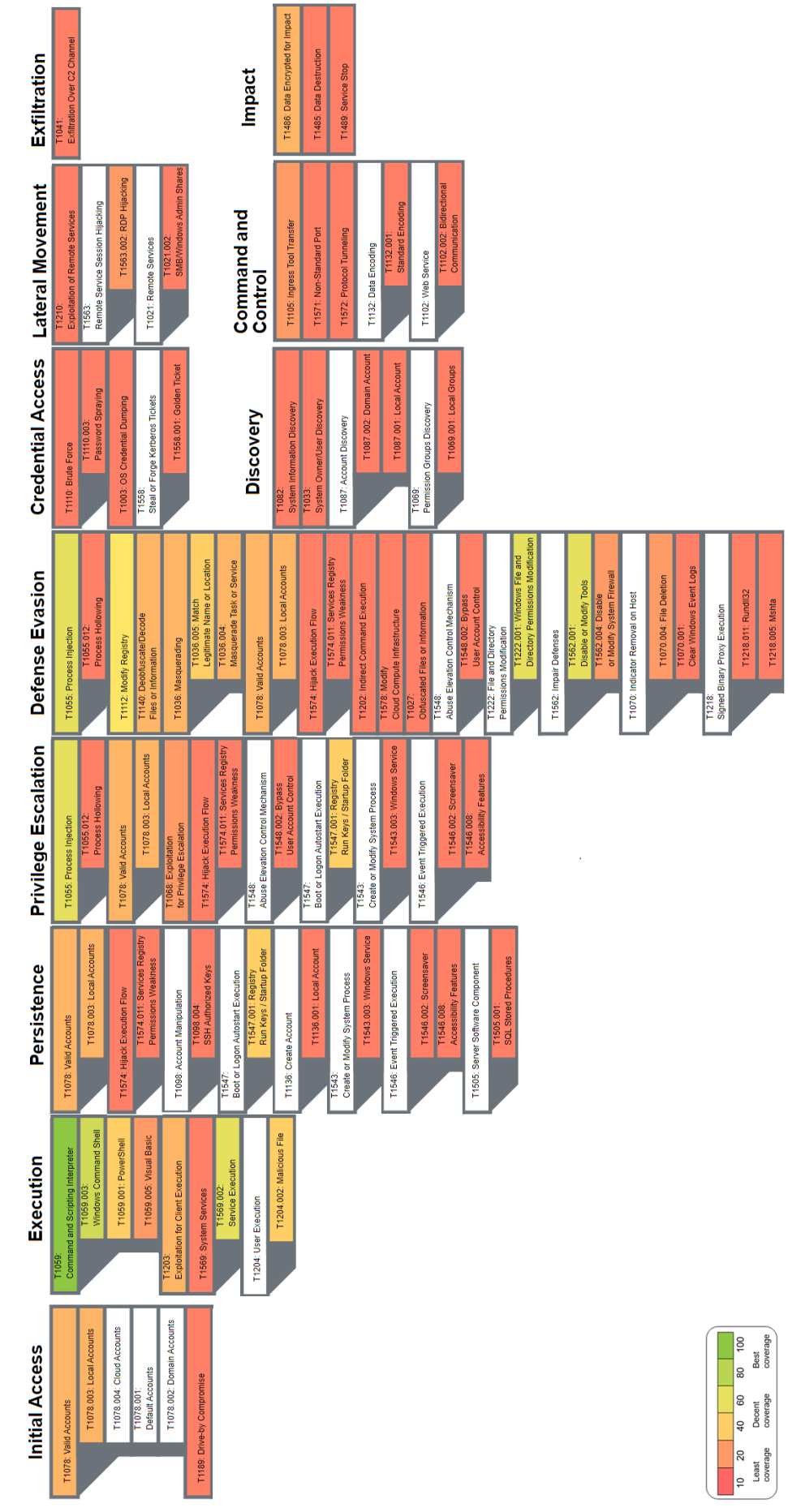
Conclusion & future work

Choose your role in the organization	Do you think the thesis topic was educational?	Would you use knowledge from the thesis in purchasing or comparing new security solutions in the future?	Do you think we can prove value with these processes or tools to our customers?	Do you think we can use the information provided in the thesis to improve our organization detection capabilities?
Security Government	Strongly agree	Strongly agree	Strongly agree	Agree
Security Government	Strongly agree	Agree	Agree	Agree
Security Operations	Agree	Agree	Strongly agree	Strongly agree
Security Operations	Strongly agree	Agree	Strongly agree	Strongly agree
Security Government	Agree	Agree	Agree	Agree
Security Operations	Strongly agree	Agree	Strongly agree	Strongly agree
Security Operations	Strongly agree	Agree	Strongly agree	Agree
Security Operations	Strongly agree	Strongly agree	Strongly agree	Strongly agree
Security Operations	Agree	Agree	Agree	Agree

Appendix 4. Questionnaire answers to free questions

Choose your role in the organization	Free feedback for the objectives & theory of the thesis or previous questions. (Optional)	Free feedback for the implementation of the thesis or previous questions. (Optional)	Free feedback for the future work or previous questions. (Optional)	Gap analysis:	Why it was interesting?
Security Government	A bit better explanation of why MITRE was chosen instead of something else and why it's relevant today would have been good. Otherwise well though out Objective and Theory part	Connecting the GAP analysis a bit more to real cases would have been preferred. Though an explanation was given why this was not done. Would make for a great followup	Good work!	Gap analysis 1 – Human operated ransomware	Think it's one of the most relevant currently
Security Government			Acquisition of new security solutions requires more detailed analysis of the threat landscape to obtain more relevant tools. Value can be provided for the customer but to provide best value, another framework should be used to analyze the current level of information security in the customers organization.	Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Log4j has gained lots of visibility and is interesting vulnerability.
Security Operations			Good topic and gap analysis looked very good with real world data. Based on this information, it is understood that while the tools are good, almost no single tool makes the environment fully protected.	Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Currently a hot topic in the world.
Security Operations				Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Most relevant
Security Government			Future work could be that what is the most "coast effective" way to improve organization detection capabilities. We could use this analysis to determine, what tools are best for our purpose.	Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Log4Shell is now on the frame and therefore the most interesting.
Security Operations	In my opinion, the presentation was very well defined and provided clear results from the research of this work, so the goals of the research were achieved.	I use the tools almost daily at work and this gave insight into their observation through clear gap analysis. Of course, be aware that the ability to detect all products has not been documented accurately enough, but this was also highlighted in the work and presentation.	Especially if this were simple to do with some automation chain / tool in post-breach analysis, it would be a good tool to detect gaps in detection and develop more detection coverage around existing tools. Also, for the customer, this can be a slightly simplified way to compare products and guide you in product selection and even in competitive situations.	Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Gap analysis 3 highlighted the various stages of the attack in the most extensive way, and because this is the latest vulnerability globally, it clarified the picture of how advanced the attacks are conducted today. Also, how attacks can progress even possibly without anyone noticing them.
Security Operations				Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Current relevant case affecting most of the ICT organizations in the world. The vulnerabilities because of Log4Shell are also already complex to determine in the environment so gap analysis for this is needed.
Security Operations				Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	Scope and ideology behind lateral movement is personally interesting and subject was current/relevant
Security Operations				Gap analysis 3 – Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement	New, very current topic and vulnerability with lots of risks, but also very difficult to detect and migitate

Appendix 5. mitre-attack-azure-defender-v1.0.json



Appendix 6. mitre-attack-all-tools-v1.0.json

Appendix 7. Gap-analysis-summary.json