MITRE ATT&CK and NIST Cybersecurity Framework

The lack of relationships between attack and control frameworks

Executive Master Cyber Security

Martijn Eikelenboom

Universiteit Leiden

MITRE ATT&CK and NIST Cybersecurity Framework

The lack of relationships between attack and control frameworks

by

Martijn Eikelenboom

to obtain the degree of Master of Science

at Leiden University,

to be defended on Thursday January 23, 2025 at 12:00.

Student number:	S3840174	
Project duration:	August, 2024 – January 1, 2025	
Thesis committee:	Prof. dr. B. van den Berg,	Leiden University, supervisor
	Dr. T. van Steen,	Leiden University

Cover: Image generated using OpenAI, depicting a hacker in a business suit

Style: TU Delft Report Style, with modifications by Daan Zwaneveld

Universiteit Leiden

Summary

This thesis explores the integration of two prominent cybersecurity frameworks, the NIST Cybersecurity Framework and MITRE ATT&CK with the aim to align cybersecurity control frameworks with adversarial behavior of attackers. As the former should defended against the tools, techniques and procedures described by the latter, it seems logical that there is a link between these frameworks.

MITRE ATT&CK and the NIST Cybersecurity Framework both serve different purposes, one is to describe adversarial threats in the real world and the other is to support organizations in managing cybersecurity risks. Both of these frameworks are not linked together; however, they do share links with another set of controls: NIST SP 800-53. As both MITRE ATT&CK and the NIST Cybersecurity Framework have mappings to NIST SP 800-53 an end-to-end mapping can be created. This mapping results in a direct linkage between adversarial behavior and a NIST Cybersecurity Framework subcategory, although with limitations in scope, as only technical preventative measures are scoped in the mapping between MITRE ATT&CK and NIST SP 800-53. By counting the number of occurrences of behaviors, NIST SP 800-53 controls and NIST Cybersecurity Framework subcategories, NIST Cybersecurity Framework subcategories can be prioritized based on their number of occurrences.

As adversarial behavior from ransomware actors is well documented, the tools, techniques and procedures from these groups can be used to apply the model towards real-world attacks, resulting in a list of prioritized NIST Cybersecurity Framework subcategories. An interesting result of this exercise is the priority given to the detection-related subcategories of the NIST Cybersecurity Framework. This is interesting as the mapping between MITRE ATT&CK and NIST SP 800-53 has put the detection measures specifically out of scope.

Comparing the prioritized list of subcategories from the model with expert advice on ransomware mitigations, shows the expert advice takes a more holistic approach by applying more functions from the NIST Cybersecurity Framework. This is expected considering the limitations in scope of the mapping between MITRE ATT&CK and NIST SP 800-53. However, expert recommendations do not directly link adversarial behavior with NIST Cybersecurity Framework subcategories, and a combination of both of these approaches could add value in prioritizing NIST Cybersecurity Framework subcategories when defending against attackers.

Contents

1 Introduction

Cybersecurity control frameworks such as the NIST Cyber Security Framework [20], when adopted by organizations, are intended to help organizations achieve a level of assurance in cybersecurity. Although these frameworks often encompass more than just protecting against malicious outside attackers, that protection should often (depending on the risk of an organization) be the bare minimum result of adopting such a framework (or at least identify that protection is insufficient).

In addition to a framework like the NIST Cybersecurity Framework, MITRE ATT&CK [32] is a widely adopted framework to document the behavior of attackers, with a detailed level of tools, techniques and procedures used by these attackers. Currently there is no relation between these two types of frameworks, whilst it would be logical when an organization aims for assurance from a compliance framework it could relate the measures from that compliance framework to the actions of attackers.

1.1. Problem description

Cybersecurity frameworks such as the NIST Cybersecurity Framework play an important role in guiding organizations on how to effectively manage cybersecurity risks and implement structured security practices. The NIST Cybersecurity Framework provides a framework for organizations to assess their cybersecurity posture, identify potential vulnerabilities, and establish a set of controls and processes to protect (critical) assets. On the other hand, the MITRE ATT&CK framework is a database of adversary behavior, observed from real-world attacks, offering a detailed understanding of how threats manifest.

Although the MITRE ATT&CK framework provides a lot of information, it is not intended to be a governance framework to manage cybersecurity in organizations. Its primary value lies in offering insight into the behavior of attackers. These attackers and their behavior create cybersecurity risks for organizations. Depending on the risk posture of these organizations, the NIST Cybersecurity Framework is intended to manage this risk, and the NIST Cybersecurity Framework would ideally provide protection against many of the attacks in the MITRE ATT&CK framework. This would imply that there is a relationship between these two frameworks: the controls within the NIST Cybersecurity Framework should help mitigate the risks posed by the threats documented in MITRE ATT&CK.

A challenge within the cybersecurity industry is the lack of direct alignment between the NIST Cybersecurity Framework and the MITRE ATT&CK framework. For organizations, it is not clear how the NIST Cybersecurity Framework controls relate to MITRE ATT&CK tools, techniques and procedures [11]. This leaves organizations uncertain about which controls in the NIST Cybersecurity Framework to implement or prioritize when defending against specific threats documented in the MITRE ATT&CK framework. Addressing this gap would help organizations better tailor their cybersecurity strategies to counter real-world attacks.

Where the NIST Cybersecurity Framework is a high level control framework, the National Institute of Standards and Technologies has many in-depth special publications on specific aspects of cybersecurity. One of these special publications: SP 800-53 documents cybersecurity and privacy controls to mitigate various threats [23]. The MITRE organization has released a mapping between the MITRE ATT&CK techniques and SP 800-53 controls [18]. The National Institute of Standards and Technologies themselves have published a mapping between the NIST Cybersecurity Framework and SP 800-53 [23]. A mapping putting it all together currently does not exist.

When this integration can be created, it is relevant to examine if this integration can be validated using real-world attacks. With the current wave of ransomware attacks, these attacks, their tools, techniques and procedures and recommendations on mitigating these attacks are well documented, making it an interesting candidate to validate the integration and would also add value to a challenge many organizations currently face.

1.2. Research objective

The objective of this exploratory research is to identify if a mapping between MITRE ATT&CK and the NIST Cybersecurity Framework makes sense and results in prioritizing the NIST Cybersecurity Framework controls when defending against specific type of attacks.

In order to achieve this, the following research question will be used:

”Can cybersecurity control frameworks, such as the NIST Cybersecurity Framework, be effectively aligned with MITRE ATT&CK to prioritize controls that mitigate adversarial threats in the real world?”

To support the research question, the following subquestions will be answered:

1. What does the MITRE ATT&CK framework entail and what is its purpose?
2. What does the NIST Cybersecurity Framework entail and what is its purpose?
3. Through which means can these frameworks be connected?
4. Plotting the tools, techniques and procedures of ransomware actors on this mapping, does it give a prioritized list of NIST Cybersecurity Framework controls?
5. Can the list of prioritized NIST Cybersecurity Framework controls be validated using ransomware tools, techniques and procedures and mitigations and recommendations?

1.3. Research design

To answer the research questions, the following research approach is chosen:

1. Study the literature and documentation on MITRE ATT&CK, NIST SP 800-53 and the NIST Cy-

bersecurity Framework to understand their background and purpose, answering subquestions 1 and 2.

2. Extend the existing mapping between MITRE ATT&CK and NIST SP 800-53 to the NIST Cybersecurity Framework answering subquestion 3.
3. Literature review and desk research to collect tools, techniques and procedures from Ransomware groups and feed them into the mapping to answer subquestion 4.
4. Literature review and desk research on ransomware mitigations, mapping these to the NIST Cybersecurity Framework and comparing the results of both exercises to answer subquestion 5.

1.4. Scope

For exploratory research, the scope is limited to well-known and widely used frameworks such as MITRE ATT&CK and the NIST Cybersecurity Framework. MITRE ATT&CK is a framework that is widely accepted. Frameworks like ISO 27001 could have also been chosen, but lack existing mappings to perform this research.

As for tools, techniques and procedures, ransomware groups are chosen to get tools, techniques and procedures from as the tools, techniques and procedures of these groups are well documented.

2

MITRE ATT&CK Analysis

2.1. Introduction

The MITRE ATT&CK framework is a framework that is used in the cybersecurity industry and by researchers to model cyber security attacks. This chapter describes the background of the MITRE ATT&CK frameworks, its purpose, and how it works.

2.2. MITRE and MITRE ATT&CK origins

The MITRE organization was founded in 1958 as a non-profit research organization to support government agencies, both military and civilian, as objective advisors [41]. MITRE has several focus areas, one of which is cybersecurity. Within that cybersecurity focus area, MITRE ATT&CK was developed as a method for red and blue teams to have a common understanding of the behaviors used by red teams and threat actors [55]. The MITRE ATT&CK framework was started in 2013 as an internal project and released to the public in 2015 [50].

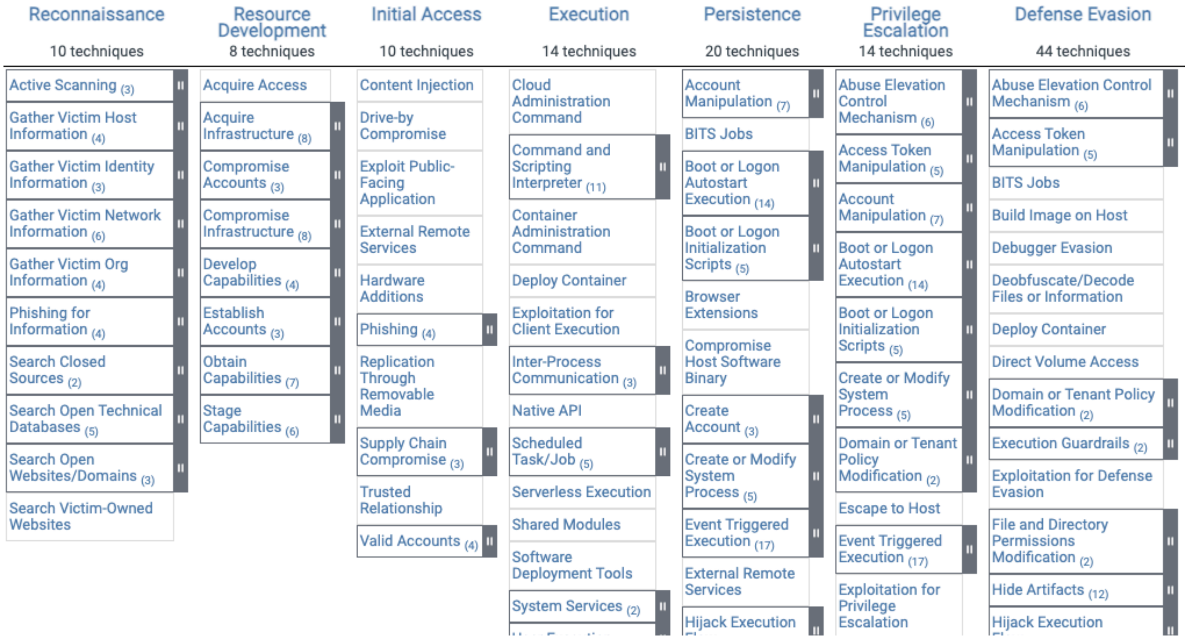
2.3. MITRE ATT&CK framework

According to their website, MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations [32]. The ATT&CK knowledge base is used as a basis for the development of specific threat models and methodologies in the private sector, in the government, and in the cybersecurity product and service community [32]. In addition to modeling attacks, the MITRE ATT&CK framework also has a database of procedures, detections, and mitigations available for most of the techniques.

The MITRE ATT&CK framework has three matrices, one for Industrial Control Systems [27], one for Mobile [28] and one for Enterprise [26]. The matrices follow the same classifications using tactics and techniques, but applied to different technology platforms. The Enterprise matrix is targeted at systems used in enterprise environments, like Windows, macOS, Linux, Office Suite etc. Mobile is targeted at the mobile operating systems Android and iOS and ICS is targeted at industrial control systems used to monitor and control industrial processes, machinery, and equipment in e.g. manufacturing and energy.

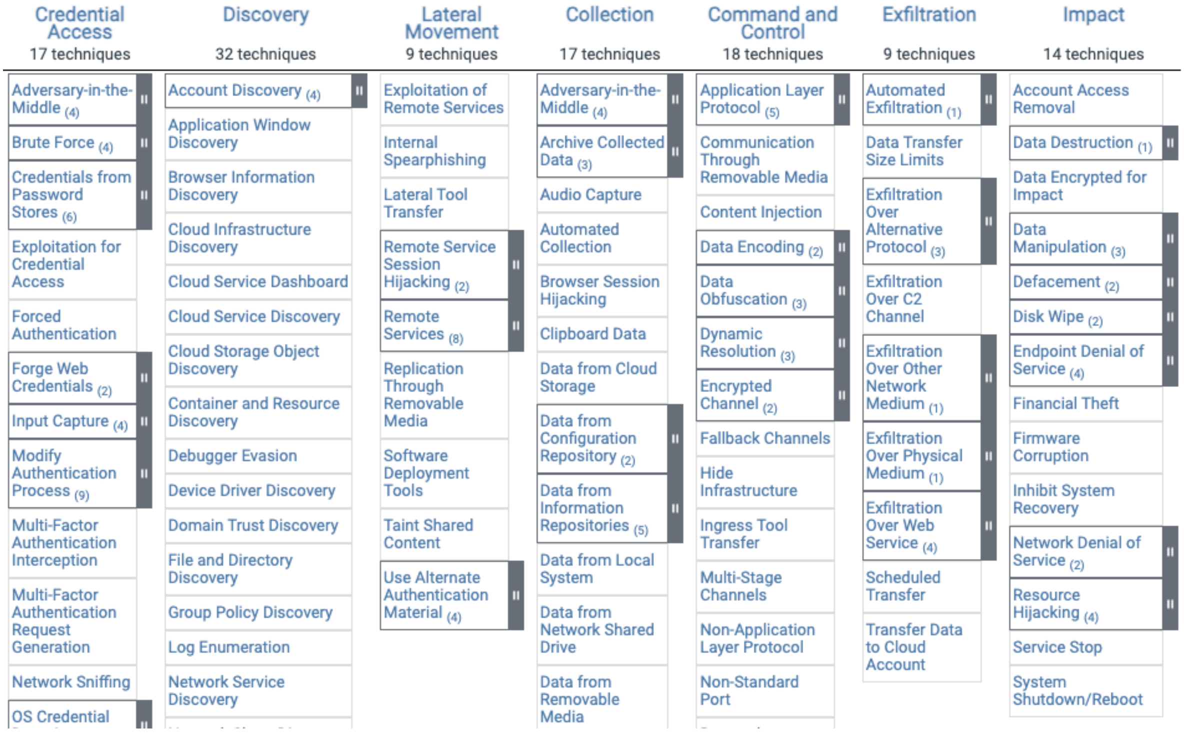
The context of this thesis is focused on organizations, and therefore the main framework to choose is Enterprise.

Figures 2.1 and 2.2 show an overview of 14 tactics and underlying techniques of the Enterprise matrix.



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Event Triggered Execution (17)	Domain or Tenant Policy Modification (2)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (2)
			Software Deployment Tools	Hijack Execution		Exploitation for Defense Evasion
			System Services (2)			File and Directory Permissions Modification (2)
						Hide Artifacts (12)
						Hijack Execution

Figure 2.1: MITRE ATT&CK Enterprise Matrix part 1 [26]



Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
OS Credential	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (4)
	Group Policy Discovery			Non-Standard Port		Service Stop
	Log Enumeration					System Shutdown/Reboot
	Network Service Discovery					

Figure 2.2: MITRE ATT&CK Enterprise Matrix part 2 [26]

2.3.1. Tactics

The MITRE ATT&CK framework is structured to have Tactics and Techniques. Tactics in the MITRE ATT&CK framework represent the goal of a technique which an adversary tries to achieve. The enterprise framework consists of 14 tactics, starting from tactics that describe the beginning of an attack path to one that describes the impact that an adversary tries to achieve. Every tactic has an unique identifying number and a description on what the tactic entails and a list of techniques and subtechniques linked tot that tactic [52].

Tactics can thus be viewed as a high-level logical grouping of techniques that could be seen as an attack path through which an attacker moves from the first step in reconnaissance to the end goals of exfiltration and impact.

2.3.2. Techniques

Techniques are categorized into tactics and describe how an adversary achieves his tactical goal by performing an action. MITRE ATT&CK has 202 techniques and 435 subtechniques [54]. Every technique has a unique number, and subtechniques get a .001-style addition to the number, uniquely identifying a subtechnique. A (sub)technique has a description and when available a paragraph with procedures, mitigations, and detections [4].

Where tactics are high-level logical groupings, techniques are what an attacker does to perform a specific action. Where subtechniques are listed, these techniques are more specific techniques with a more limited scope which an attacker performs [42].

Next to the description of the technique, a technique has sections for Procedures, Mitigations and Detections.

Procedures

Documentation of the specific use of a technique is provided as part of the technique documentation. These procedures represent the particular instance of the application of the technique by a specific group and are meant to give a better understanding of how the technique is used exactly in a specific scenario. Those specific scenarios can be used to improve detection [50].

Mitigations

Every technique has a section mitigations that describes security controls, concepts, and best practices to help protect and prevent against the execution of the related technique [32]. MITRE ATT&CK has 44 mitigations that are a high-level security control, concept, or best practice [31]. Mitigations are classified into a high-level category and sometimes have specific mitigation recommendations for different techniques [3].

Detection

Every technique is accompanied by a section detection that outlines potential data sources and indicators to identify the execution of a technique. Data sources provide guidance on what data sources in a network can be used to gain visibility into the given technique. Those data sources are often collected in central log repositories where rules can be created that trigger alerts on certain occurrences of technique execution [57].

2.4. MITRE ATT&CK usage

MITRE ATT&CK was started as a way to categorize common adversary behavior for adversary emulation and intrusion detection research [51][49]. This categorization and description of what techniques attackers use and how to detect and mitigate against these techniques has proved quite popular in the past decade.

MITRE has identified serveral use cases for their framework [49, P 3] and researchers have recently conducted an extensive review of the literature in which the MITRE ATT&CK framework has been used [47]. For this research, they reviewed 72 published articles and categorised the articles into four categories, only leaving out the SOC maturity proposed by Mitre. These four categories describe the way the MITRE ATT&CK framework is used in science.

The behavioral analytic category was considered by the researchers for all articles that addressed adversary behavior. According to the researchers MITRE ATT&CK is used as a source of information where MITRE ATT&CK is a database of techniques and where the techniques are correlated to model the adversary behind an attack. Another usage of the framework is as a support tool for various purposes, such as mapping behavior to data, abstracting technical detail to a higher level, and generalizing results [47].

Red teaming (a.k.a. pentesting) is a method to test the security of organizations and systems and to find vulnerabilities. The MITRE ATT&CK framework is used to support red-teaming activities. Research papers can be subcategorized in the modeling of real or simulated attacks and for the purpose of threat modeling. The latter involves the creation of a common language or framework to model and analyze attacks. In addition to research papers, the security industry and governments use the MITRE ATT&CK framework to model adversarial behavior, e.g. in incident reports describing a ransomware incident [10] or APT activity in the SolarWinds hack [5].

Cyber threat intelligence enrichment is combining information of APTs and their attack paths creates cyber threat intelligence that organizations can use and share knowledge amongst each other. The MITRE ATT&CK Framework helps to create a common language and enrich and combine available data from different sources [47]. Parties in the security industry use MITRE ATT&CK to describe the behavior of certain actors such as ALPHV Blackcat [1] or to describe generic and industry-specific threats [12, P 52].

Organizations that want to mitigate cyber attacks can use the MITRE ATT&CK Framework to asses gaps in their defensive measures in their IT infrastructure. Although articles on this topic are somewhat limited [47], the security industry has adopted the MITRE ATT&CK framework as a tool to show the detection coverage of cyber security monitoring products [56][7] or to map and assess detection coverage [40].

Another more commercial use case for the MITRE ATT&CK Framework is to perform product evaluations of cyber security vendors. MITRE uses the data they have collected on APTs to test the detection coverage of cyber security products against known attacks in a systematic way [45].

3
Control frameworks

As cybersecurity management becomes increasingly important within organizations due to increasing risks and the expansion of cybersecurity laws like NIS2, organizations need to mature their cybersecurity management. Cybersecurity frameworks have different goals, but share that they intend to secure information and IT assets against cybersecurity attacks and other hazards that threaten the confidentiality, integrity, or availability of information. These frameworks provide best practices and international standards to achieve organizational goals in cybersecurity [6].

3.1. Origins of control frameworks

Cybersecurity frameworks have been developed since the Trusted Computer System Evaluation Criteria (also known as The Orange Book) was published in 1983 by the Department of Defense of the United States. The Orange Book was intended to create a supply of secure high assurance systems that were formally evaluated against a set of criteria [24]. Although this framework focused on product security, information security management frameworks were introduced years later, with an important introduction of the NIST Cybersecurity Framework in 2014 [35].

3.2. The NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides guidance to industry, government agencies, and other organizations on how to manage cyber security risks [36].

According to the National Institute of Standards and Technologies, the Cybersecurity Framework must support identifying ”a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks” [9, P 1] .

The NIST Cybersecurity Framework consists of three parts: the framework core (figure 3.1), the implementation tiers, and the framework profiles. The core is organized in six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Each function is organized in categories and subcategories. The Cybersecurity Framework is not intended as a checklist of minimal requirements and needs to be tailored to the specific needs of organizations [36]. The recent update of the core introduced Govern as a separate function, whereas this was part of the other functions in the previous version of the Cybersecurity Framework [9].

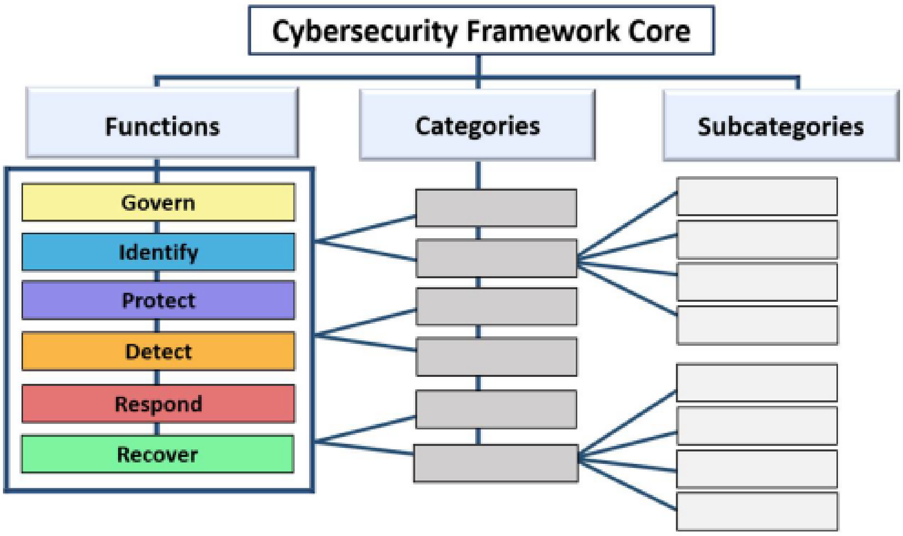


Figure 3.1: NIST Cybersecurity Framework core structure [36]

Tiers provide context on how an organization views cybersecurity risk. A higher tier reflects more rigor and sophistication in cybersecurity risk management practices. An organization could use this to select a tier to define their ambitions and meet their organizational goals. The NIST Cybersecurity Framework has four tiers, ranging from basic Tier 1 Partial, where cybersecurity risk management is not formalized, going to Tier 4 where cybersecurity risk management is integrated into the business process and is constantly adapted based on lessons learned. Framework profiles can be used to describe the current and/or the desired state of specific cybersecurity activities based on the current tier level and the desired tier level. These profiles can be used to identify gaps and address these gaps to achieve the desired profile state [9].

Whilst many cybersecurity control frameworks exist, e.g. ISO27001, COBIT, PCI-DSS, the NIST Cybersecurity Framework is a widely adopted framework. The NIST Cybersecurity Framework is considered best practice by 70% of the respondents in a survey [44]. And more recently even the Dutch ”Algemene rekenkamer” used the NIST Cybersecurity Framework as their control framework, and the Dutch department of defense also uses the NIST Cybersecurity Framework [43].

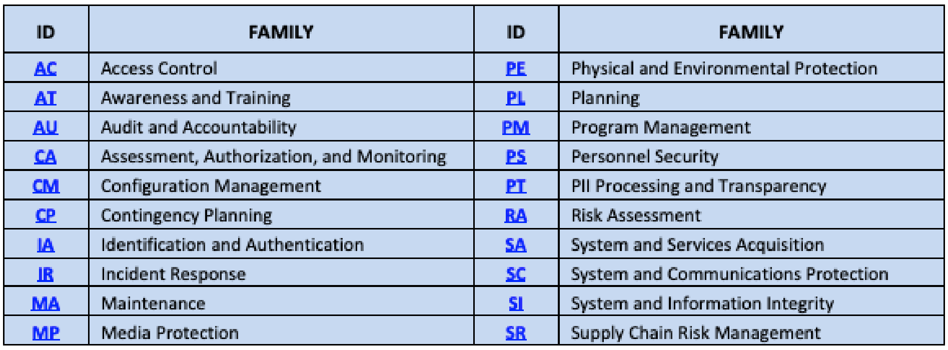
3.3. NIST SP 800-53

Whilst the NIST Cybersecurity Framework is an overarching cybersecurity framework, the National Institute of Standards and Technologies has published many Special Publications (SP) in its 800-series that present information that may be of interest to the cybersecurity community. The NIST Cybersecurity Framework is part of this series of publications. These publications are meant to address and support the privacy and security needs of the US Federal Government and have been created since the 1990s. Although some US governments need to adhere to some of these publications, they can be voluntarily adopted by organizations, and documents are not subject to copyright [39][53]. The National Institute of Standards and Technologies has published 212 publications in the SP-800 series [17].

Many special publications focus on a specific topics such as SP 800-30 on how to conduct risk assessments in cybersecurity [21] or various publications with recommendations on using the right encryption algorithms [48] and cipher suites [8].

The National Institute of Standards and Technologies has published SP 800-53 in 2005: Security and Privacy Controls for Information Systems and Organizations, which is a catalog of security and privacy controls [46]. These controls may be used to protect information systems and organizations against a diverse set of threats and risks. These controls and underlying measures are meant to safeguard (information) assets in an organization by making them resilient and reducing the impact when attacks occur [23]. The current version of SP 800-53 is revision number 5, which was published in 2020 [23].

NIST SP 800-53 is organized into 20 control families related to security and privacy (figure 3.2). Each family is identified with a two-character acronym. There are a total of 322 controls and another 867 control enhancements [23].



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Figure 3.2: NIST SP 800-53 Control Families [23, P8]

All controls in NIST SP 800-53 have the following parts to describe the control, with the base control, discussions on that base control, related controls and control enhancements with discussion on those enhancements [23, P 9]. As an example the SI-4 System monitoring control has 25 control enhancements next to the base control to address specific aspects of system monitoring [23, P 336-343].

4 Comparison and analysis

In chapter one and two MITRE ATT&CK, the NIST Cybersecurity Framework and NIST SP 800-53 have been discussed. These frameworks in itself cover different goals. MITRE ATT&CK is for modeling attacker behavior, the NIST Cybersecurity Framework provides a high-level set of controls to manage cybersecurity in organizations, and NIST SP 800-53 is a detailed list of controls and measures to protect organizations from a diverse set of threats. Although all these frameworks have value on their own, it is interesting to see if these frameworks can be aligned in such a way that attacker behavior can be aligned with controls from the NIST Cybersecurity Framework that mitigate this attacker behavior. Integrating these frameworks makes it possible to link the NIST Cybersecurity Framework controls to attacker behavior. With that integration organizations are able to choose and prioritize controls when defending against specific attacker behavior they see as a risk.

This chapter maps these frameworks on each other, using the existing mapping between MITRE ATT&CK and NIST SP 800-53 and the mapping between the NIST Cybersecurity Framework and NIST SP 800-53. For this research, these two mappings are combined to create an end-to-end integration from MITRE ATT&CK to the NIST Cybersecurity Framework that currently does not exist.

4.1. Threat Modeling with ATT&CK

The mapping of MITRE ATT&CK and NIST SP 800-53 has been done by MITRE Engenuity. MITRE Engenuity is a R&D organization part of the MITRE Corporation founded in 2019. The organization is focused on research and development in a non-competitive manner for the greater good [2]. The Center for Threat-Informed Defense is part of MITRE Engenuity and their goal is to advance the state of the art and the state of the practice in threat-informed defense globally [13].

The Center for Threat-Informed Defense developed the Mappings Explorer for cyber defenders to understand how security controls and capabilities protect against adversary techniques in the MITRE ATT&CK framework [25] and was announced in 2024. The goal of these mappings is to provide security teams with the knowledge to make threat informed decisions and increase the effectiveness of their defenses against threats that are most relevant to the organization and to make informed decisions about risk.

Part of the work is the creation of the mapping explorer. A tool in which multiple security control frameworks are mapped to adversary techniques in the MITRE ATT&CK framework. Currently, the mapping explorer has the following security frameworks:

- AWS for the Amazon Web Services cloud platform
- Azure for the Microsoft Azure cloud platform
- CVE for the Common Vulnerability and Exposure Program
- GCP for the Google Cloud platform
- M365 for the Microsoft 365 Cloud
- NIST SP 800-53 for the NIST SP 800-53 control framework
- VERIS for the Vocabulary for Event Recording and Incident Sharing common languague

Of this list, only NIST SP 800-53 is a platform agnostic framework that has a holistic cybersecurity control framework. Furthermore, NIST SP 800-53 is a list of controls that has a mapping to the NIST Cybersecurity Framework [18].

4.2. Mapping Methodology of MITRE Engenuity

MITRE Engenuity created a methodology to map security control frameworks to the MITRE ATT&CK framework. A mapping between a security control and an ATT&CK (sub)technique means that the security control may mitigate or prevent the successful execution of that (sub)technique. However, a mapping does not determine the extent of efficacy of security control.

The core of the mapping framework are ATT&CK mitigations. As discussed in chapter 2, mitigations represent security concepts and classes of technologies that can be used to prevent a (sub)technique from being successfully executed. In ATT&CK every mitigation is mapped to multiple (sub)techniques with a more detailed description of how that mitigation may be applied as a preventive measure against that (sub)technique (figure 4.1).

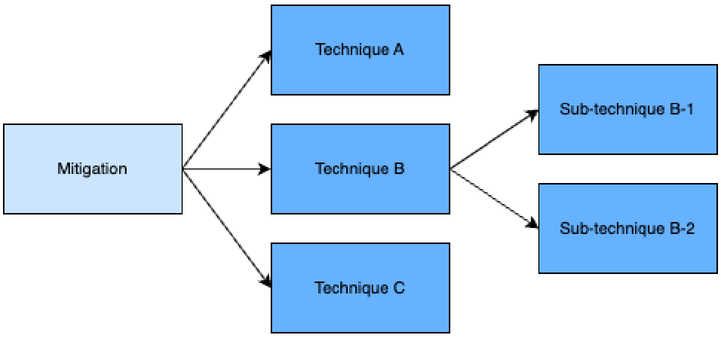


Figure 4.1: Mitigation to (sub)technique

Furthermore, every ATT&CK (sub)technique is reviewed to understand the adversaries goal (tactic) and how they achieve that goal (technique) as a basis for the relevant context with the mitigation to study relevant security controls (figure 4.2).

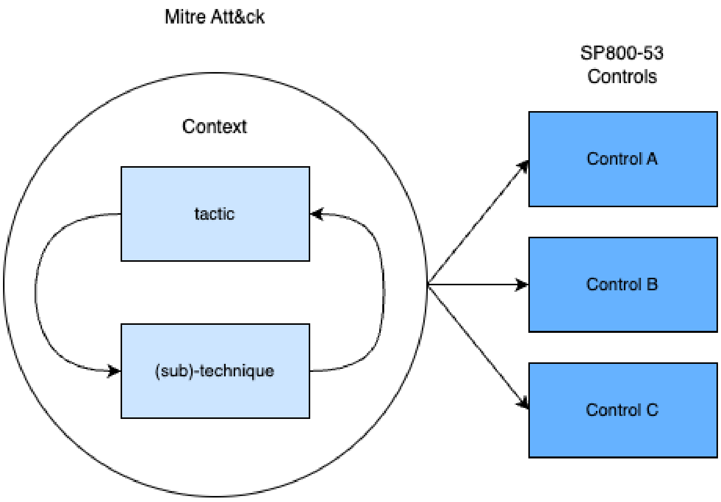


Figure 4.2: MITRE ATT&CK context to SP 800-53 controls

Next, each security control is reviewed in the context of those (sub)techniques and mitigation, and it is determined if the control is aligned with the mitigation and is relevant to the (sub)techniques (figure 4.3).

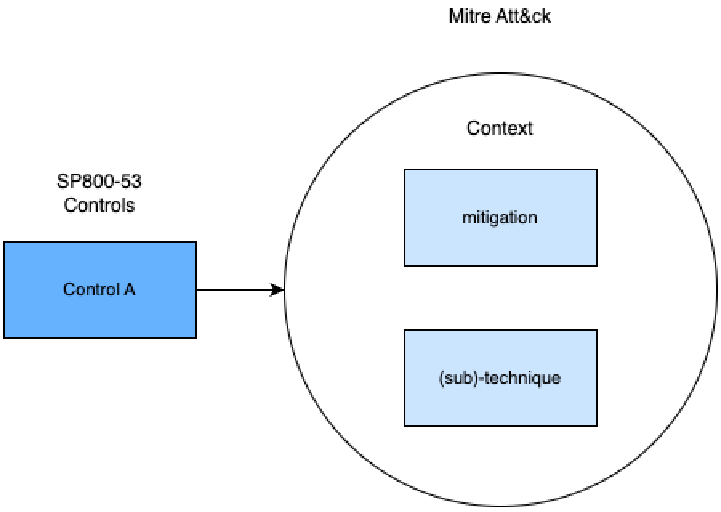


Figure 4.3: SP 800-53 controls to MITRE ATT&CK

When the previous steps have been executed and a control candidate is found, the mapping is created. This result is a (sub)technique that is mapped to one or more controls in the SP 800-53 control list [38].

Figure 4.4 represents the steps MITRE Engenuity took for the security control mapping methodology:

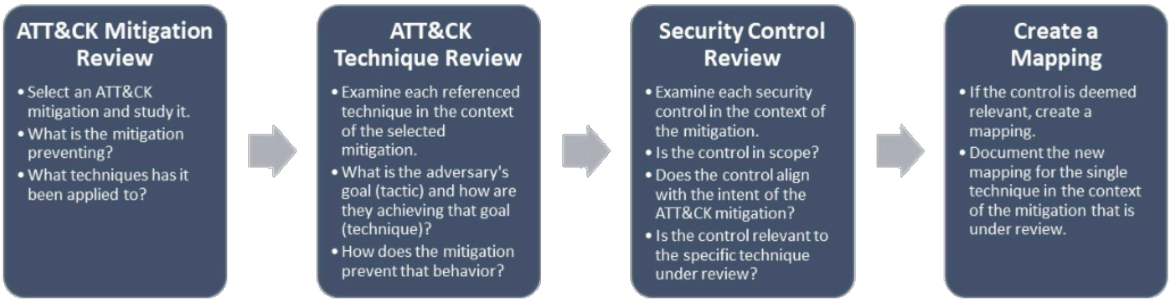

ATT&CK Mitigation Review
• Select an ATT&CK mitigation and study it.
• What is the mitigation preventing?
• What techniques has it been applied to?
ATT&CK Technique Review
• Examine each referenced technique in the context of the selected mitigation.
• What is the adversary's goal (tactic) and how are they achieving that goal (technique)?
• How does the mitigation prevent that behavior?
Security Control Review
• Examine each security control in the context of the mitigation.
• Is the control in scope?
• Does the control align with the intent of the ATT&CK mitigation?
• Is the control relevant to the specific technique under review?
Create a Mapping
• If the control is deemed relevant, create a mapping.
• Document the new mapping for the single technique in the context of the mitigation that is under review.

Figure 4.4: Security control mapping methodology [38]

4.3. Mapping NIST CSF to NIST SP 800-53

The mapping between the NIST Cybersecurity Framework and NIST SP 800-53 is provided by the National Institute of Standards and Technologies themselves. The mapping is on the level of subcategories in the NIST Cybersecurity Framework and the NIST SP 800-53 that support the achievement of the subcategories. There should be no assumption that there is a one-to-one mapping between controls and subcategories, meaning that controls do not necessarily cover all that needs to be done for a subcategory or may do more than is needed for that subcategory [25].

4.4. Mapping model

After covering the existing mappings, I have created a new integration between these existing mappings. This new integration is relevant because it creates an end-to-end integration between the attackers behavior and the NIST Cybersecurity Framework subcategories, which is not available at this point in time. The NIST SP 800-53 controls are the key part in this, as both the MITRE ATT&CK framework maps to NIST SP 800-53 and the NIST Cybersecurity Framework maps to NIST SP 800-53. Using this as the centralized control framework enables end-to-end integration. To do so, the existing methodologies for both the National Institute of Standards and Technologies for the NIST Cybersecurity Framework to NIST SP 800-53 mapping [23] and the MITRE Engenuity mapping for the MITRE ATT&CK to SP 800-53 are used [18]. Both are done by industry experts and are well documented and MITRE Engenuity has also documented their approach in creating this mapping (paragraph: 4.2).

Figure 4.5 shows this end-to-end integration, where the left part (red) is the existing mapping of MITRE ATT&CK to NIST SP 800-53 and the right part (blue) is the mapping of the NIST Cybersecurity Framework to NIST SP 800-53.

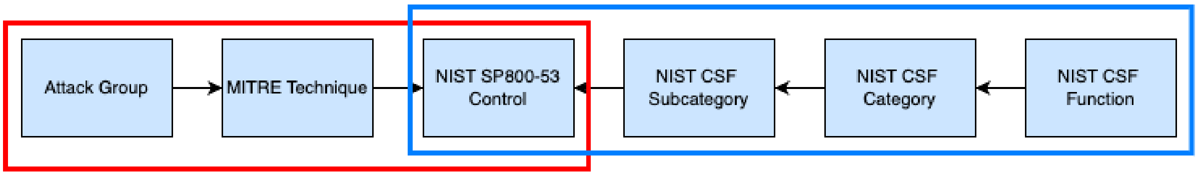


Figure 4.5: High level mapping model

Bringing everything together in a more detailed level gives the following model, visualized in figure 4.6. The starting point of the model are groups of attackers (Attacker column). The techniques these attackers use are mapped to the MITRE ATT&CK techniques (Technique column). For example, multiple groups might use technique B, some might use technique A and only one uses technique D.

Using the existing mapping from MITRE Engenuity these techniques are mapped to NIST SP 800-53 controls. And the existing mapping of the National Institute of Standards and Technologies is used to map the NIST Cybersecurity Framework subcategories to the NIST SP 800-53 controls. This gives an end-to-end mapping from the techniques being used by attack groups and a NIST Cybersecurity Framework subcategory.

Only mapping these to each other results in list op subcategories applicable to defending against these groups. It does not give any priority on which subcategory is more relevant for defending against attacks, and there is a risk, given enough techniques used, that in the end, many, if not all, subcategories in scope will be listed. A solution to this challenge could be to count the number of occurrences for every technique, control, and subcategory. The working assumption is that the more often a technique, control, or subcategory occurs, the more priority it should receive.

When all attack groups use a specific technique (technique B), defending against this technique should receive more priority over a technique that only one group uses (technique D). Continuing this logic, when NIST SP 800-53 control C defends against most commonly used techniques B and C, it should be given more priority than NIST SP 800-53 control F, which only defends against technique D which is only used by one attack group. And finally, when NIST Cybersecurity Framework subcategory B is mapped to the most prioritized NIST SP 800-53 controls, this subcategory should be most prioritized.

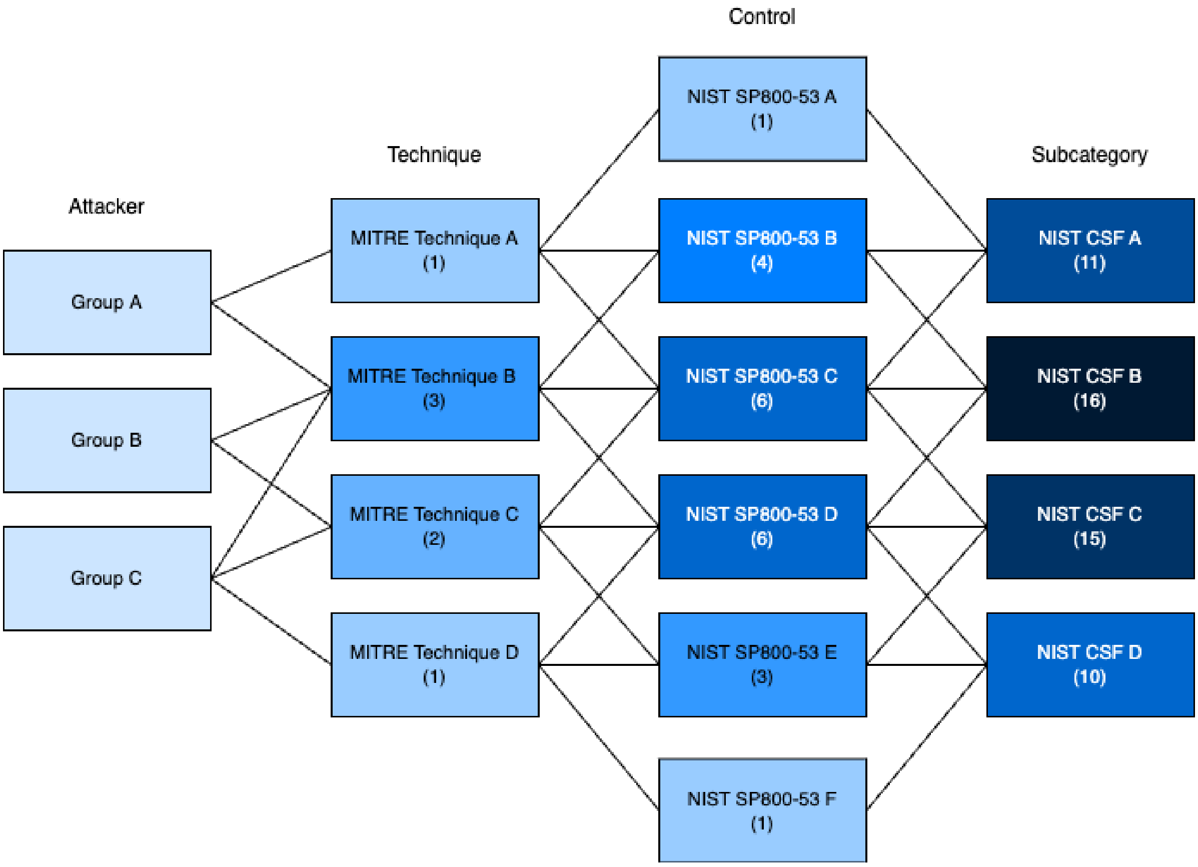


Figure 4.6: Mapping model

Applying this logic by counting the occurrences results in the following:

- Group A uses techniques A and B, Group B uses techniques B and C, and Group C uses techniques B, C, and D. Counting reveals that technique B is used three times, making it the most frequently used technique. Technique C is used twice, and Techniques A and B are used only once.
- NIST SP 800-53 control A only defends against technique A and technique A is only used once. Therefore, the count of NIST SP 800-53 control A is one. NIST SP 800-53 control C defends against technique A, B and C. Adding the counts of technique A, B and C results in a count of 6 for NIST SP 800-53 control C.
- This method of counting continues for the NIST Cybersecurity Framework controls. NIST Cybersecurity Framework control D applies to NIST SP 800-53 control D, E and F. Adding these counts together, NIST CSF control D gets a total count of 10.

Applying this logic of counting to every technique, control, and subcategory gives a total count for each of them. Performing the count for figure 4.6 results in the following priorities:

- Techniques:
  1. Technique B: count of 3
  2. Technique C: count of 2
  3. Technique A &D: count of 1
- Controls:
  1. Control C &D: count of 6
  2. Control B: count of 4
  3. Control E: count of 3
  4. Control A &F: count of 1
- Subcategories:
  1. Subcategory B: count of 16
  2. Subcategory C: count of 15
  3. Subcategory A: count of 11
  4. Subcategory D: count of 10

Following the model in figure 4.6, the model gives the NIST Cybersecurity Framework subcategory B the highest priority when defending against these attack groups.

5

Pratical application

By combining two existing mappings, MITRE ATT&CK to NIST SP 800-53 and NIST SP 800-53 and the NIST Cybersecurity Framework, an novel end-to-end mapping has been developed. This mapping establishes a connection between adversarial behaviors, as categorized by MITRE ATT&CK, and the subcategories within the NIST Cybersecurity Framework. The resulting model (figure 4.6) shows the potential to prioritize NIST Cybersecurity Framework subcategories based on adversarial behavior.

To validate this model and assess its practical ability, it is valuable to test it against real-world scenarios. Therefore, the behavior of real world attackers needs to be mapped against the MITRE ATT&CK framework to get a prioritized list of NIST Cybersecurity Framework subcategories. A group of attackers with well-documented adversarial behavior is that of ransomware attacks.

5.1. Ransomware

Before we can test this model against real-world attacks, we need to understand ransomware attacks and the techniques these groups use to carry out their attacks. Ransomware is one of the most impactful cybersecurity threats. This category became infamous with the Wannacry attack, crippling thousands of computers and organizations in more than 150 countries by encrypting data on every system it ran on [15]. The ransomware threat evolved from the Wannacry self-propagating malware attack to an endemic of ransomware groups that encrypt and exfiltrate organizations' data. The rise in ransomware attacks has caused a great deal of interest from academia [30] and from the security industry and governments.

That interest resulted in many publications detailing the modus operandi of these attackers. Ransomware groups either develop, buy, or make use of a service to attain encryption software. The next step for ransomware attackers is to gain access to their victim's network by using phishing techniques or exploiting vulnerabilities. Attackers then move throughout their victims' network, tacking various steps to create persistence and elevate their privileges. They try to delete backups, exfiltrate data, and encrypt as much data as possible, making it impossible for their victim to access their data. And even when they can still access the data, ransomware groups extort their victims by threatening to publicly release the exfiltrated data [29].

As incidents are often forensically investigated, the security industry gathers much data on the techniques ransomware actors use as part of their attacks. This data is shared with the community and with governments [14]. The American Cyber Defense Agency has created many advisories on ransomware groups, detailing the modus operandi of these attackers and using the MITRE ATT&CK framework to categorize these techniques [19].

5.2. Scoping limitations

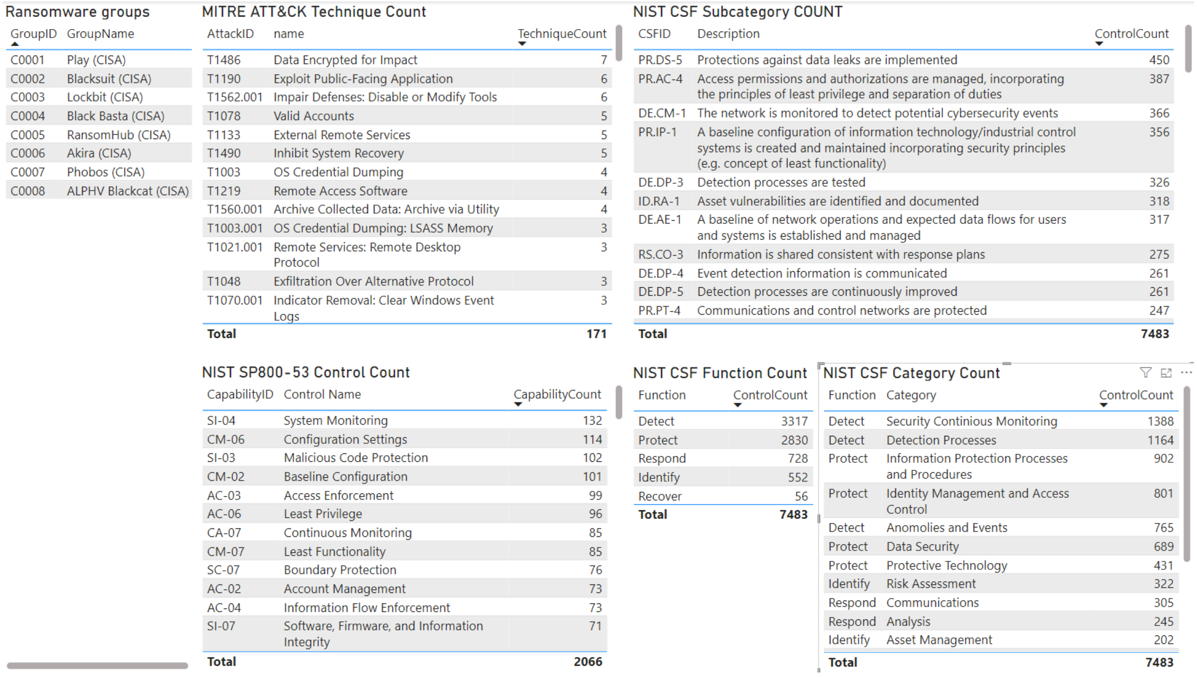
Before the mapping is put in practice, it is relevant to note that there some scoping limitations in the existing mappings. For the mapping, MITRE Engenuity took some scoping decisions that define how the mapping is performed. The limitations in the scoping are the focus on technical and operational elements of NIST SP 800-53 and not on management elements. Another scoping decision was that mitigations were chosen from the MITRE ATT&CK framework and controls that only monitor adversary behavior were discarded. And finally, pre-compromise mitigations were also put out of scope [38].

These scoping limitations will likely result in some categories from the NIST Cybersecurity Framework being ignored as they are part of functions that are not related to preventing attacks, but are focused on the management, detection, response, and recovery aspects.

5.3. Applying the model in practice

To demonstrate the practical application of this newly developed model, the eight most recent ransomware advisories from the United States National Coordinator for Critical Infrastructure Security and Resilience (CISA) [19] were analyzed. These advisories, containing the latest information, were selected as they approximately encompass a full year of CISA's guidance, providing a representative sample of common adversarial behaviors employed by ransomware attack groups. The techniques described in these advisories were systematically extracted and integrated into the novel mapping model, as depicted in Figure 4.6. The United States National Coordinator for Critical Infrastructure Security and Resilience were chosen as they are a non-commercial organization aimed at protecting the infrastructure of the United States.

The results of this application are presented in figure 5.1, offering a high-level overview that is further detailed in the accompanying tables within the figure. This approach not only validates the model's ability to connect current ransomware techniques to actionable cybersecurity framework elements, but also underscores its potential to enhance the understanding and prioritization of defensive measures against ransomware threats.



Ransomware groups

GroupID	GroupName
C0001	Play (CISA)
C0002	Blacksuit (CISA)
C0003	Lockbit (CISA)
C0004	Black Basta (CISA)
C0005	RansomHub (CISA)
C0006	Akira (CISA)
C0007	Phobos (CISA)
C0008	ALPHV Blackcat (CISA)

MITRE ATT&CK Technique Count

AttackID	name	TechniqueCount
T1486	Data Encrypted for Impact	7
T1190	Exploit Public-Facing Application	6
T1562.001	Impair Defenses: Disable or Modify Tools	6
T1078	Valid Accounts	5
T1133	External Remote Services	5
T1490	Inhibit System Recovery	5
T1003	OS Credential Dumping	4
T1219	Remote Access Software	4
T1560.001	Archive Collected Data: Archive via Utility	4
T1003.001	OS Credential Dumping: LSASS Memory	3
T1021.001	Remote Services: Remote Desktop Protocol	3
T1048	Exfiltration Over Alternative Protocol	3
T1070.001	Indicator Removal: Clear Windows Event Logs	3
Total		**171**

NIST CSF Subcategory COUNT

CSFID	Description	ControlCount
PR.DS-5	Protections against data leaks are implemented	450
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	387
DE.CM-1	The network is monitored to detect potential cybersecurity events	366
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	356
DE.DP-3	Detection processes are tested	326
ID.RA-1	Asset vulnerabilities are identified and documented	318
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	317
RS.CO-3	Information is shared consistent with response plans	275
DE.DP-4	Event detection information is communicated	261
DE.DP-5	Detection processes are continuously improved	261
PR.PT-4	Communications and control networks are protected	247
Total		**7483**

NIST SP800-53 Control Count

CapabilityID	Control Name	CapabilityCount
SI-04	System Monitoring	132
CM-06	Configuration Settings	114
SI-03	Malicious Code Protection	102
CM-02	Baseline Configuration	101
AC-03	Access Enforcement	99
AC-06	Least Privilege	96
CA-07	Continuous Monitoring	85
CM-07	Least Functionality	85
SC-07	Boundary Protection	76
AC-02	Account Management	73
AC-04	Information Flow Enforcement	73
SI-07	Software, Firmware, and Information Integrity	71
Total		**2066**

NIST CSF Function Count

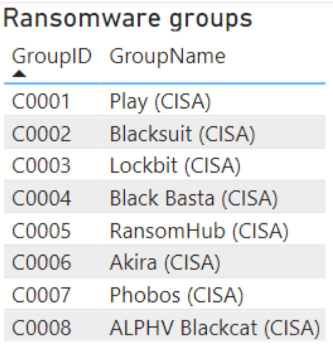
Function	ControlCount
Detect	3317
Protect	2830
Respond	728
Identify	552
Recover	56
Total	**7483**

NIST CSF Category Count

Function	Category	ControlCount
Detect	Security Continious Monitoring	1388
Detect	Detection Processes	1164
Protect	Information Protection Processes and Procedures	902
Protect	Identity Management and Access Control	801
Detect	Anomolies and Events	765
Protect	Data Security	689
Protect	Protective Technology	431
Identify	Risk Assessment	322
Respond	Communications	305
Respond	Analysis	245
Identify	Asset Management	202
Total		**7483**

Figure 5.1: Overview of the model in practice

Figure 5.2 shows the eight ransomware groups selected from the CISA advisories [19].

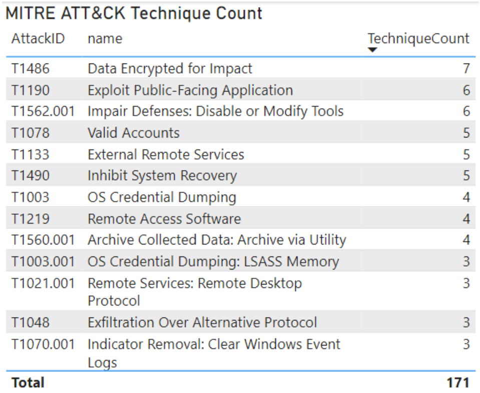


Ransomware groups

GroupID	GroupName
C0001	Play (CISA)
C0002	Blacksuit (CISA)
C0003	Lockbit (CISA)
C0004	Black Basta (CISA)
C0005	RansomHub (CISA)
C0006	Akira (CISA)
C0007	Phobos (CISA)
C0008	ALPHV Blackcat (CISA)

Figure 5.2: Ransomware groups

Figure 5.3 shows the techniques these ransomware groups use and counts how many times these techniques are used by the ransomware groups. The model has all techniques, but figure 5.3 shows the top 13 techniques by count. On top of the list, we see T1486 - Data Encrypted for Impact with a count of seven, meaning that seven out of eight ransomware groups use this technique as part of their modus operandi. T1190 - Exploit Public-Facing Application is used by six of the eight ransomware groups.

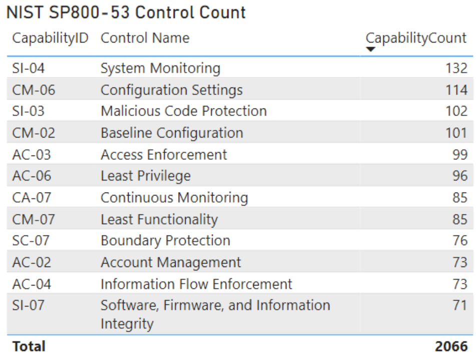


MITRE ATT&CK Technique Count

AttackID	name	TechniqueCount
T1486	Data Encrypted for Impact	7
T1190	Exploit Public-Facing Application	6
T1562.001	Impair Defenses: Disable or Modify Tools	6
T1078	Valid Accounts	5
T1133	External Remote Services	5
T1490	Inhibit System Recovery	5
T1003	OS Credential Dumping	4
T1219	Remote Access Software	4
T1560.001	Archive Collected Data: Archive via Utility	4
T1003.001	OS Credential Dumping: LSASS Memory	3
T1021.001	Remote Services: Remote Desktop Protocol	3
T1048	Exfiltration Over Alternative Protocol	3
T1070.001	Indicator Removal: Clear Windows Event Logs	3
Total		**171**

Figure 5.3: MITRE ATT&CK Technique Count

Figure 5.4 shows the number of times a NIST SP 800-53 control is mapped to a MITRE ATT&CK technique. Technique T1486 - Data Encrypted for Impact is (among other mappings) mapped to SI-04 System Monitoring. As this technique is used seven times, the SI-04 System Monitoring has a count of seven from this technique. As Technique T1190 - Exploit Public-Facing Application is also mapped to control SI-04 System Monitoring, another count of six is added to the total count of this control. This continues for every technique making a total count for SI-04 System Monitoring of 132.

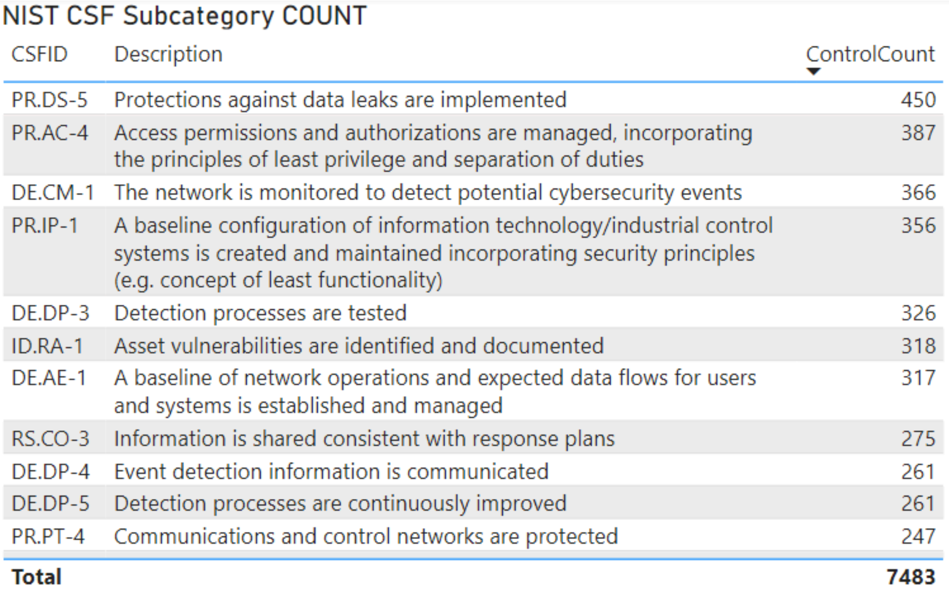


NIST SP800-53 Control Count

CapabilityID	Control Name	CapabilityCount
SI-04	System Monitoring	132
CM-06	Configuration Settings	114
SI-03	Malicious Code Protection	102
CM-02	Baseline Configuration	101
AC-03	Access Enforcement	99
AC-06	Least Privilege	96
CA-07	Continuous Monitoring	85
CM-07	Least Functionality	85
SC-07	Boundary Protection	76
AC-02	Account Management	73
AC-04	Information Flow Enforcement	73
SI-07	Software, Firmware, and Information Integrity	71
Total		**2066**

Figure 5.4: NIST SP 800-53 Control Count

Continuing this logic brings us to the figure 5.5 showing the number of counts per NIST Cybersecurity Framework subcategory. The subcategory PR.DS-5 Protections against data leaks is implemented, is (among other mappings) mapped to NIST SP 800-53 control SI-04 System Monitoring, making the count for this subcategory 132. As the control AC-06 Least Privilege is also mapped to subcategory PR.DS-5 another count of 96 is added to this subcategory. This is done for all controls making the total count for PR.DS-5 Protections against data leaks are implemented 450. And this is repeated for all mapping of the NIST Cybersecurity Framework to NIST SP 800-53 controls.



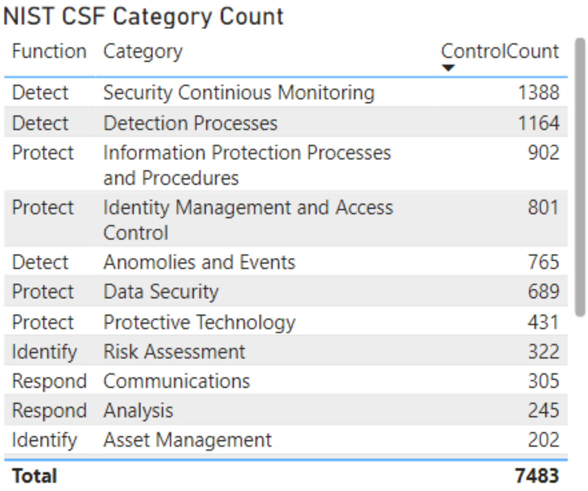
NIST CSF Subcategory COUNT

CSFID	Description	ControlCount
PR.DS-5	Protections against data leaks are implemented	450
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	387
DE.CM-1	The network is monitored to detect potential cybersecurity events	366
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	356
DE.DP-3	Detection processes are tested	326
ID.RA-1	Asset vulnerabilities are identified and documented	318
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	317
RS.CO-3	Information is shared consistent with response plans	275
DE.DP-4	Event detection information is communicated	261
DE.DP-5	Detection processes are continuously improved	261
PR.PT-4	Communications and control networks are protected	247
Total		**7483**

Figure 5.5: NIST Cybersecurity Framework Subcategory Count

Mapping the adversarial behavior of these eight ransomware groups to the NIST Cybersecurity Framework subcategory and counting the number of occurrences results in a prioritized list of NIST Cybersecurity Framework subcategories. Figure 5.5 shows the eleven main subcategories according to the number of occurrences and ordered from the most to the least. Based on this mapping of the number of occurrences these are the top subcategories one should prioritize when defending against the adversarial behavior of these eight ransomware groups.

The NIST Cybersecurity Framework subcategories are part of a NIST Cybersecurity Framework category. Figure 5.6 shows the sum of all subcategory counts at the category level. The category level shows what category of the NIST Cybersecurity Framework should be given priority to defend against the behavior of these eight ransomware groups.

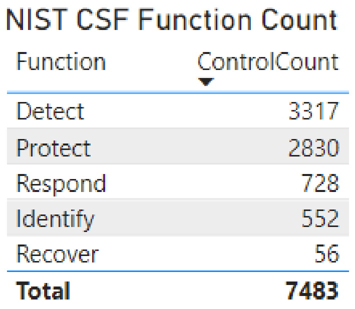


NIST CSF Category Count

Function	Category	ControlCount
Detect	Security Continious Monitoring	1388
Detect	Detection Processes	1164
Protect	Information Protection Processes and Procedures	902
Protect	Identity Management and Access Control	801
Detect	Anomolies and Events	765
Protect	Data Security	689
Protect	Protective Technology	431
Identify	Risk Assessment	322
Respond	Communications	305
Respond	Analysis	245
Identify	Asset Management	202
Total		**7483**

Figure 5.6: NIST Cybersecurity Framework Category Count

The NIST Cybersecurity Framework Functions are the highest level of the NIST Cybersecurity Framework Framework. Figure 5.7) shows the count per function and this is a sum of all the counts of categories in that function.



NIST CSF Function Count

Function	ControlCount
Detect	3317
Protect	2830
Respond	728
Identify	552
Recover	56
Total	**7483**

Figure 5.7: NIST Cybersecurity Framework Function Count

5.4. Findings from applying the model in practice

By applying this model in practice, we see a prioritized list of (sub)categories and functions based on the count. Evaluating the model at the function level (figure 5.7), clearly shows that the functions Detect (44%) and Protect (38%) are the most prominent functions totaling 82% of the total count at the function level. At the category level (figure 5.6) we observe some categories with a high count number. The top five represents 67% of the total count and the top 10 represents 93% of the total count, while the NIST Cybersecurity Framework has a total of 23 subcategories. At the subcategory level, the top ten account for 44% of the total count and the top 20 account for 74% of the total count of the 108 subcategories.

The scope limitations in paragraph 5.2 showed that the mapping of MITRE ATT&CK to NIST SP 800-53 was limited to only protective measures and the detective measures are specifically not part of the mapping. However, evaluating the model shows that the detection category is the category with the highest priority. At the category level, out of the top five categories, three are from the detect category and two are from the protect category. And finally, at the subcategory level, six are from the detect category and only two are from the protect category.

This manner of prioritizing combined with the limitations in scope clearly shows that detection is a NIST Cybersecurity Framework function that should be prioritized when defending against adversarial behavior of ransomware attackers.

6
Expert recommendations

Chapter 5 showed the NIST Cybersecurity Framework priorities from applying the model (figure 4.6) in practice using adversarial behavior of ransomware groups. It is interesting to explore whether these priorities align with the recommendations of experts on mitigating ransomware. The Center for Internet Security (CIS) has published this recommendation based on the NIST Cybersecurity Framework [22]. This comparison will give insight into the alignment and difference between the model and recommendations by experts.

6.1. Center for Internet Security

The Center for Internet Security is a non-profit organization that ”makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation” [2]. Center for Internet Security is responsible for the CIS Controls, which ”are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture” [16] and for the CIS benchmarks which ”are prescriptive configuration recommendations for more than 25+ vendor product families” [16]. Both are community-driven projects with support from experts around the globe.

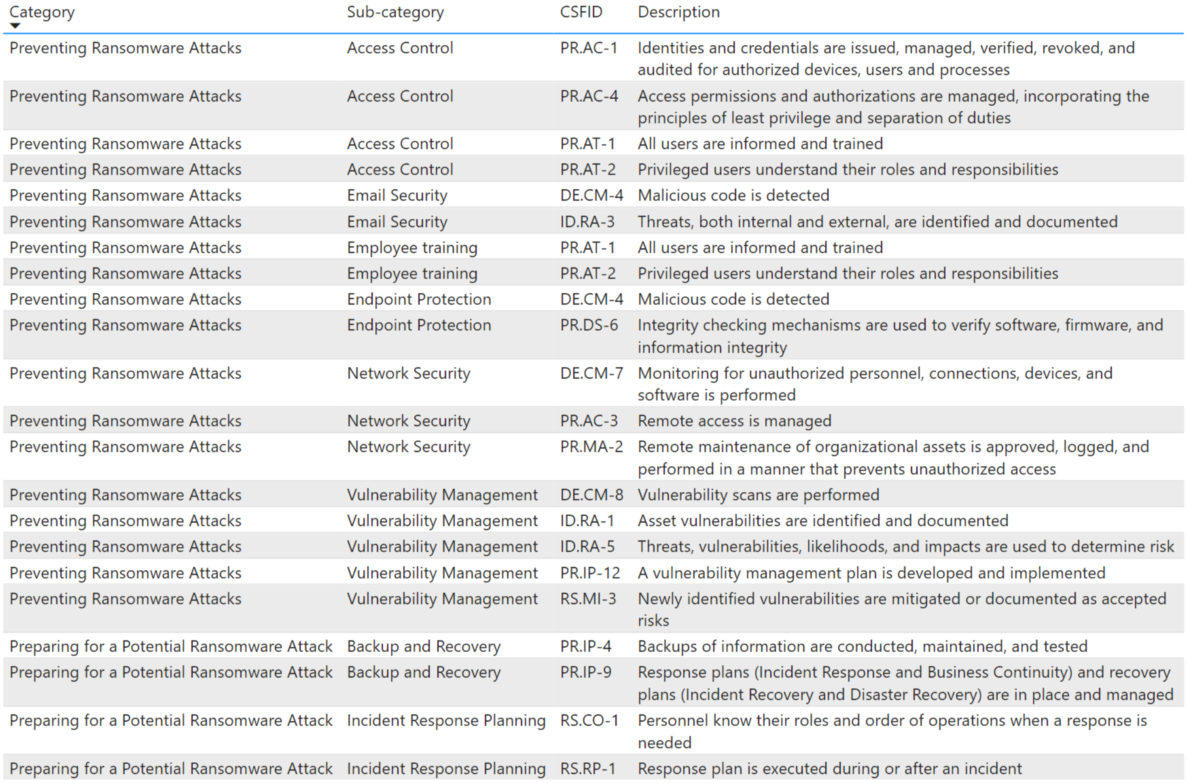
The Center for Internet Security is also the home of the Multi-State Information Sharing and Analysis Center (MS-ISAC) with a mission to improve cyber security for US government organizations, among other things, by sharing information, incident response and remediation support [34].

6.2. The Center for Internet Security Combatting Ransomware

This Center for Internet Security has published a document ’Combatting Ransomware’ [22] based on recommendations from the MS-ISAC Metrics Working Group [33] which advises the Nationwide Cybersecurity Review. The latter is a self-assessment of cyber security for government organizations in the United States that provides benchmarking among peers and guidance on maturing cyber security in organizations, using, among others, NIST SP800-53 controls [37].

The ’Combatting Ransomware’ document is structured in two main categories and eight subcategories.

The main categories are: Preventing Ransomware Attacks and Preparing for a Potential Ransomware Attack [22]. The first has six subcategories and the latter has two. For every subcategory the NIST Cybersecurity Framework subcategories are listed to mitigate part of the ransomware threat. Figure 6.1 shows an overview of all categories, subcategories and linked the NIST Cybersecurity Framework subcategories. A total of 19 unique NIST Cybersecurity Framework subcategories are recommended as effective controls to combat the ransomware threat. Some NIST Cybersecurity Framework subcategories are mentioned twice: DE.CM-4, PR.AT-1 and PR.AT-2 under different categories of the 'Combatting Ransomware' document.

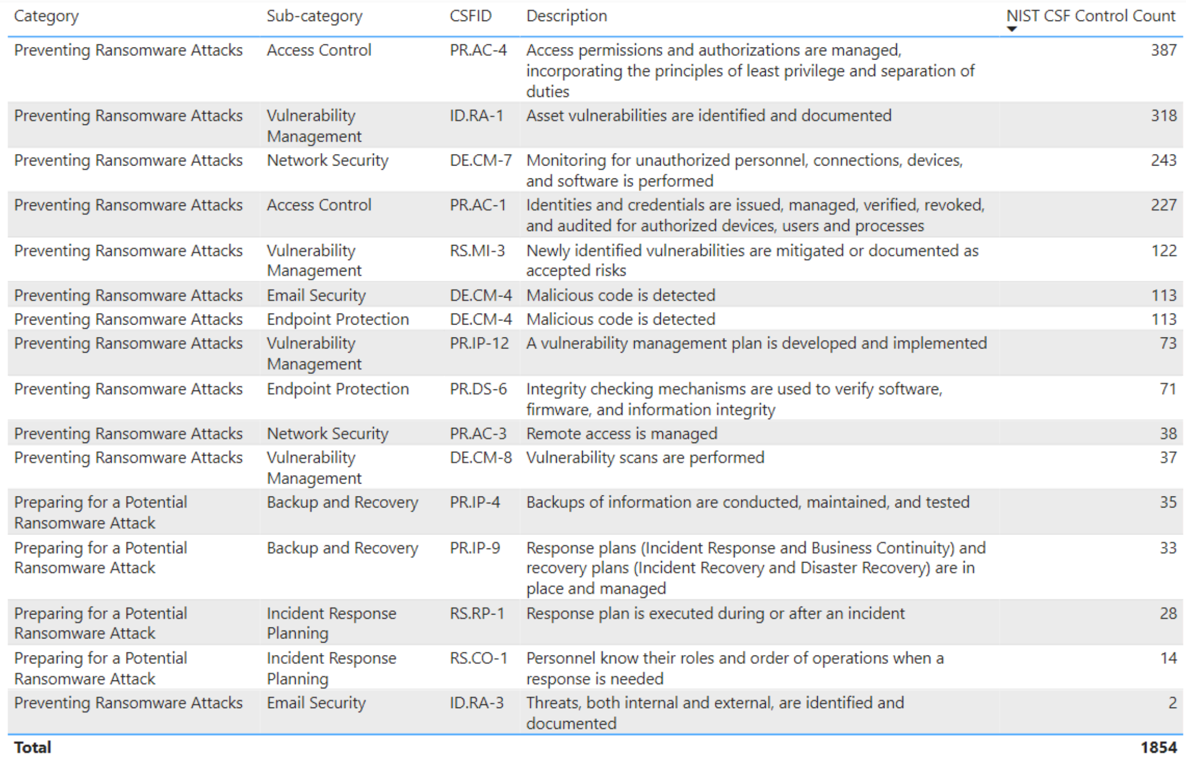


Category	Sub-category	CSFID	Description
Preventing Ransomware Attacks	Access Control	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Preventing Ransomware Attacks	Access Control	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Preventing Ransomware Attacks	Access Control	PR.AT-1	All users are informed and trained
Preventing Ransomware Attacks	Access Control	PR.AT-2	Privileged users understand their roles and responsibilities
Preventing Ransomware Attacks	Email Security	DE.CM-4	Malicious code is detected
Preventing Ransomware Attacks	Email Security	ID.RA-3	Threats, both internal and external, are identified and documented
Preventing Ransomware Attacks	Employee training	PR.AT-1	All users are informed and trained
Preventing Ransomware Attacks	Employee training	PR.AT-2	Privileged users understand their roles and responsibilities
Preventing Ransomware Attacks	Endpoint Protection	DE.CM-4	Malicious code is detected
Preventing Ransomware Attacks	Endpoint Protection	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
Preventing Ransomware Attacks	Network Security	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Preventing Ransomware Attacks	Network Security	PR.AC-3	Remote access is managed
Preventing Ransomware Attacks	Network Security	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Preventing Ransomware Attacks	Vulnerability Management	DE.CM-8	Vulnerability scans are performed
Preventing Ransomware Attacks	Vulnerability Management	ID.RA-1	Asset vulnerabilities are identified and documented
Preventing Ransomware Attacks	Vulnerability Management	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
Preventing Ransomware Attacks	Vulnerability Management	PR.IP-12	A vulnerability management plan is developed and implemented
Preventing Ransomware Attacks	Vulnerability Management	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks
Preparing for a Potential Ransomware Attack	Backup and Recovery	PR.IP-4	Backups of information are conducted, maintained, and tested
Preparing for a Potential Ransomware Attack	Backup and Recovery	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Preparing for a Potential Ransomware Attack	Incident Response Planning	RS.CO-1	Personnel know their roles and order of operations when a response is needed
Preparing for a Potential Ransomware Attack	Incident Response Planning	RS.RP-1	Response plan is executed during or after an incident

Figure 6.1: Combatting Ransomware recommendations overview [22]

6.3. Comparing recommendations to findings

Comparing the recommendations from the 'Combatting Ransomware' document to the prioritized list in Chapter 5 results in the shared NIST Cybersecurity Framework subcategories in figure 6.2.



Category	Sub-category	CSFID	Description	NIST CSF Control Count
Preventing Ransomware Attacks	Access Control	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	387
Preventing Ransomware Attacks	Vulnerability Management	ID.RA-1	Asset vulnerabilities are identified and documented	318
Preventing Ransomware Attacks	Network Security	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	243
Preventing Ransomware Attacks	Access Control	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	227
Preventing Ransomware Attacks	Vulnerability Management	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	122
Preventing Ransomware Attacks	Email Security	DE.CM-4	Malicious code is detected	113
Preventing Ransomware Attacks	Endpoint Protection	DE.CM-4	Malicious code is detected	113
Preventing Ransomware Attacks	Vulnerability Management	PR.IP-12	A vulnerability management plan is developed and implemented	73
Preventing Ransomware Attacks	Endpoint Protection	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	71
Preventing Ransomware Attacks	Network Security	PR.AC-3	Remote access is managed	38
Preventing Ransomware Attacks	Vulnerability Management	DE.CM-8	Vulnerability scans are performed	37
Preparing for a Potential Ransomware Attack	Backup and Recovery	PR.IP-4	Backups of information are conducted, maintained, and tested	35
Preparing for a Potential Ransomware Attack	Backup and Recovery	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	33
Preparing for a Potential Ransomware Attack	Incident Response Planning	RS.RP-1	Response plan is executed during or after an incident	28
Preparing for a Potential Ransomware Attack	Incident Response Planning	RS.CO-1	Personnel know their roles and order of operations when a response is needed	14
Preventing Ransomware Attacks	Email Security	ID.RA-3	Threats, both internal and external, are identified and documented	2
Total				**1854**

Figure 6.2: Shared recommendations

Out of the 19 unique NIST Cybersecurity Framework subcategory recommendations from ’Combatting Ransomware’ 15 unique recommendations are shared with the model. The ones that are not shared are:

1. ID.RA-5 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
2. PR.AT-1 All users are informed and trained
3. PR.AT-2 Privileged users understand their roles and responsibilities
4. PR.MA-2 Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Considering the scope of the mapping (paragraph 5.2) it seems logical that the first three of the four above items are not part of the shared recommendations. ID.RA-5 relates to cyber security management and PR.AT-1 and PR.AT-2 relates to training of employees and privileged users. For PR.MA-2 it is less clear why this is not a shared recommendation, as the intention of this subcategory seems to be to limit remote access to organizational assets.

Comparing the control count of the findings to these recommendations, it can also be noted that only six recommendations have a control count of more than 100 and only two have a control count of more than 250, whilst the top ten list in the findings have a control count higher than 250. Although recommendations are shared, they are usually not prioritized in the model. Some of these differences can be explained by the fact that the recommendations from ’Combatting Ransomware’ are part of the category ’Preparing for a Potential Ransomware Attack’. As the focus of the exising mapping (paragraph 5.2) lies on preventative measures, controls from the NIST Cybersecurity Framework functions Response and Recovery are probably not much prioritized.

6.4. Comparing findings to recommendations

When comparing the prioritized list from chapter 5 only two of the top ten items are shared recommendations. Eight items from the top ten are not in the recommendations of the 'Combatting Ransomware' document:

- PR.DS-5 Protections against data leaks are implemented
- DE.CM-1 The network is monitored to detect potential cybersecurity events
- PR.IP-1 A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- DE.DP-3 Detection processes are tested
- DE.AE-1 A baseline of network operations and expected data flows for users and systems is established and managed
- RS.CO-3 Information is shared consistent with response plans
- DE.DP-4 Event detection information is communicated
- DE.DP-5 Detection processes are continuously improved

Of these eight items, five come from the NIST Cybersecurity Framework Detection function, which makes the Detection function a notable difference between the recommendation and the prioritized subcategories of the model. Therefore, it seems that there is a difference in the way experts view the importance of detection subcategories of the NIST Cybersecurity Framework compared to when there is a direct link between adversarial behavior and the NIST Cybersecurity Framework subcategories.

6.5. Mapping model considerations

Comparing the mapping model with the expert recommendations, there is some overlap, but there are also some notable differences. The main advantage of the mapping model is that it is based on an integration where controls in the NIST Cybersecurity Framework are directly linked to adversarial behavior, whereas the experts recommendations are based on expertise and no such direct link. Another difference is the priority given to controls in the mapping model. By simply counting the number of occurrences of behavior, controls, and subcategories, priorities are given to the most important controls. And although the experts give priority by selecting a limited number of controls there, are still 19 subcategories remaining that have no priority among themselves.

A downside of the mapping model is that it is limited to mainly technical aspects as part of the scope (paragraph 5.2). Therefore, the mapping model prioritizes technological categories over others.

7 Conclusion

National Institute of Standards and Technologies provides organizations through the NIST Cybersecurity Framework and NIST-SP 800-53 with controls to protect organizations against cyber security threats, and MITRE ATT&CK provides insights into real-world adversarial tools, techniques and procedures. It only seems logical that there is a direct link between a control of NIST Cybersecurity Framework and MITRE ATT&CK since the first should defend against the adversarial threat of the latter.

These mappings have limitations, as the scope of the existing mapping is limited to mitigations of the MITRE ATT&CK framework and detections in MITRE ATT&CK are not part of the mapping. Extending the mapping with real-world adversarial behavior of ransomware groups and counting the occurrences of techniques and controls gives a prioritized list of NIST Cybersecurity Framework subcategories. Although MITRE ATT&CK detections are outside the scope of the mapping, the NIST Cybersecurity Framework Detection function is the most prioritized function and has many prioritized items in the subcategories. According to this mapping, detection should be prioritized in combating ransomware.

Although the mapping has limitations in its scope, it adds value by directly linking adversarial behavior with NIST Cybersecurity Framework. Taking into account these limitations, the prioritized NIST Cybersecurity Framework subcategories neglect that there are other important aspects of cybersecurity. For example, the priorities from these mappings lie in prevention and detection; however, when something goes wrong, Response and Recover are important functions. Detecting a cybersecurity event is one thing, for mitigation, one needs to respond to that event and take action, and depending on the impact of the event, recovery is essential to minimize the impact of said cybersecurity event. This limitation gives a one-sided view of cybersecurity that focuses on only prevention and detection. And Identify as a function is important to at least identify the threats an organization wants to defend against. Integration of these functions and their (sub)categories could give the mapping a more holistic view of cybersecurity. The mapping model would be more relevant if these subcategories could also be mapped. The mapping between the NIST Cybersecurity Framework and NIST SP 800-53 exists. The challenge lies in mapping these non-technical aspects from MITRE ATT&CK to NIST SP 800-53.

Comparing real-world advice from experts on the ransomware threat with the prioritized subcategories shows that there are overlapping subcategories in both. However, evaluating the top ten prioritized subcategories shows that eight are not in the recommendations of experts, and half of that top ten that is not aligned is regarding the Detection function of the NIST Cybersecurity Framework. Part of this difference is the emphasis on technical prevention in the model, while experts take a more balanced approach to all NIST Cybersecurity Framework functions. The value in the mapping model lies in the prioritization and direct link between adversarial behavior, something the experts did not provide.

Where the model, with its limitations in scope, lacks a holistic approach, it does directly link adversarial behavior with NIST Cybersecurity Framework. And where the expert takes that holistic approach, it seems to lack such a direct connection between adversarial behavior and the NIST Cybersecurity Framework. Combining both would likely give a more balanced approach on what NIST Cybersecurity Framework subcategories to prioritize and address defending against a ransomware threat.

Further research

Further research can be conducted on mapping the detection category of MITRE ATT&CK to NIST SP 800-53. As this will likely result in more prioritization of the detection function of the NIST Cybersecurity Framework, research on the mapping of the NIST Cybersecurity Framework to SP 800-53 may be relevant, especially research on the efficacy of a control with regard to protecting against adversarial behavior. This would give the possibility to add weight to the counting of controls, making the prioritization more relevant and balanced.

Further research can also be conducted on the integration of the other functions of the NIST Cybersecurity Framework to the model. For example, although the response does not prevent or mitigate adversarial behavior, it does intend to minimize the impact of said behavior, which is quite relevant for organizations. Integration on this level would further optimize the model.

References

[1] *#StopRansomware: ALPHV Blackcat | CISA*. Feb. 27, 2024. URL: `https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a` (visited on 09/27/2024).

[2] *About us - CIS®*. CIS. URL: `https://www.cisecurity.org/about-us/` (visited on 01/03/2025).

[3] *Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®*. URL: `https://attack.mitre.org/mitigations/M1036/` (visited on 12/18/2024).

[4] *Active Directory, Data Source DS0026 | MITRE ATT&CK®*. URL: `https://attack.mitre.org/datasources/DS0026/` (visited on 09/07/2024).

[5] *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | CISA*. Apr. 15, 2021. URL: `https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a` (visited on 09/27/2024).

[6] Marwan Alshar'e. "CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001". In: *Applied computing Journal* (Feb. 9, 2023), pp. 245–255. ISSN: 2788-9688. DOI: `10.52098/acj.202364`. URL: `https://acaa-p.com/index.php/acj/article/view/64` (visited on 10/06/2024).

[7] *Assessing and expanding MITRE ATT&CK coverage in Splunk Enterprise Security*. Splunk Lantern. Feb. 7, 2023. URL: `https://lantern.splunk.com/Security/UCE/Guided_Insights/Cyber_frameworks/Assessing_and_expanding_MITRE_coverage_in_Splunk_Enterprise_Security` (visited on 10/03/2024).

[8] Elaine Barker and William C Barker. "Recommendation for Key Establishment Using Symmetric Block Ciphers". In: ().

[9] Matthew Barrett. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, Apr. 16, 2018, NIST CSWP 04162018. DOI: `10.6028/NIST.CSWP.04162018`. URL: `http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf` (visited on 11/17/2024).

[10] *BlackSuit Ransomware*. The DFIR Report. Aug. 26, 2024. URL: `https://thedfirreport.com/2024/08/26/blacksuit-ransomware/` (visited on 09/27/2024).

[11] Danny Bradbury. *How to map MITRE ATT&CK against security controls | Infosec*. Sept. 27, 2021. URL: `https://www.infosecinstitute.com/resources/industry-insights/how-to-map-mitre-attck-against-security-controls/` (visited on 01/16/2025).

[12] Red Canary. *2024 Threat Detection Report*. URL: `https://resource.redcanary.com/rs/003-YRU-314/images/2024ThreatDetectionReport_RedCanary.pdf?version=0`.

[13] *Center for Threat-Informed Defense*. MITRE Engenuity. URL: `https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/` (visited on 11/23/2024).

[14] Nationaal Cyber Security Centrum. *Melissa: samenwerkingsverband ransomwarebestrijding - Nieuwsbericht - Nationaal Cyber Security Centrum*. Last Modified: 2024-02-22T14:02 Publisher: Nationaal Cyber Security Centrum. Oct. 3, 2023. URL: `https://www.ncsc.nl/actueel/nieuws/2023/oktober/3/melissa-samenwerkingsverband-ransomwarebestrijding` (visited on 11/30/2024).

[15] Qian Chen and Robert A. Bridges. *Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware*. Sept. 25, 2017. DOI: `10.48550/arXiv.1709.08753`. arXiv: `1709.08753[cs]`. URL: `http://arxiv.org/abs/1709.08753` (visited on 11/29/2024).

[16] *CIS Benchmarks™*. CIS. URL: `https://www.cisecurity.org/cis-benchmarks/` (visited on 01/03/2025).

[17] *Computer Security Resource Center*. URL: `https://csrc.nist.gov/publications/sp800` (visited on 11/18/2024).

[18] Mike Cunningham. *Unite ATT&CK and Security Controls with Mappings Explorer*. MITRE-Engenuity. Mar. 27, 2024. URL: `https://medium.com/mitre-engenuity/unite-att-ck-and-security-controls-with-mappings-explorer-48509e4b8793` (visited on 11/24/2024).

[19] *Cybersecurity Alerts & Advisories | CISA*. Aug. 29, 2024. URL: `https://www.cisa.gov/news-events/cybersecurity-advisories` (visited on 11/30/2024).

[20] *Cybersecurity Framework*. Nov. 12, 2013. URL: `https://www.nist.gov/cyberframework` (visited on 01/16/2025).

[21] Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments*. NIST Special Publication (SP) 800-30 Rev. 1. National Institute of Standards and Technology, Sept. 17, 2012. DOI: `10.6028/NIST.SP.800-30r1`. URL: `https://csrc.nist.gov/pubs/sp/800/30/r1/final` (visited on 11/18/2024).

[22] Center for Internet Security. *Combatting Ransomware*. Oct. 2024. URL: `https://learn.cisecurity.org/combatting-ransomware-guide`.

[23] Joint Task Force Interagency Working Group. *Security and Privacy Controls for Information Systems and Organizations*. Edition: Revision 5. National Institute of Standards and Technology, Sept. 23, 2020. DOI: `10.6028/NIST.SP.800-53r5`. URL: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf` (visited on 12/22/2024).

[24] Steven B. Lipner. “The Birth and Death of the Orange Book”. In: *IEEE Annals of the History of Computing* 37.2 (Apr. 2015), pp. 19–31. ISSN: 1058-6180. DOI: `10.1109/MAHC.2015.27`. URL: `http://ieeexplore.ieee.org/document/7116444/` (visited on 10/10/2024).

[25] *Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5 (xlsx)*. URL: `https://csrc.nist.gov/files/pubs/sp/800/53/r5/upd1/final/docs/csf-pf-to-sp800-53r5-mappings.xlsx`.

[26] *Matrix - Enterprise | MITRE ATT&CK®*. URL: `https://attack.mitre.org/matrices/enterprise/` (visited on 12/18/2024).

[27] *Matrix - ICS | MITRE ATT&CK®*. URL: `https://attack.mitre.org/matrices/ics/` (visited on 09/07/2024).

[28] *Matrix - Mobile | MITRE ATT&CK®*. URL: `https://attack.mitre.org/matrices/mobile/` (visited on 09/07/2024).

[29] Sifra R. Matthijsse, M. Susanne Van ‘T Hoff-de Goede, and E. Rutger Leukfeldt. “Your files have been encrypted: a crime script analysis of ransomware attacks”. In: *Trends in Organized Crime* (Apr. 27, 2023). ISSN: 1084-4791, 1936-4830. DOI: 10.1007/s12117-023-09496-z. URL: https://link.springer.com/10.1007/s12117-023-09496-z (visited on 11/30/2024).

[30] Timothy McIntosh et al. “Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration”. In: *ACM Computing Surveys* 57.1 (Jan. 31, 2024), pp. 1–40. ISSN: 0360-0300, 1557-7341. DOI: 10.1145/3691340. URL: https://dl.acm.org/doi/10.1145/3691340.

[31] *Mitigations - Enterprise | MITRE ATT&CK®*. URL: https://attack.mitre.org/mitigations/enterprise/ (visited on 12/18/2024).

[32] *MITRE ATT&CK®*. URL: https://attack.mitre.org/ (visited on 01/16/2025).

[33] *MS-ISAC Working Groups*. CIS. URL: https://www.cisecurity.org/ms-isac/services/working-groups/ (visited on 01/03/2025).

[34] *Multi-State Information Sharing and Analysis Center*. CIS. URL: https://www.cisecurity.org/ms-isac/ (visited on 01/03/2025).

[35] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, Apr. 16, 2018, NIST CSWP 04162018. DOI: 10.6028/NIST.CSWP.04162018. URL: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (visited on 12/22/2024).

[36] National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology, Feb. 26, 2024, NIST CSWP 29. DOI: 10.6028/NIST.CSWP.29. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (visited on 01/02/2025).

[37] *Nationwide Cybersecurity Review (NCSR)*. CIS. URL: https://www.cisecurity.org/ms-isac/services/ncsr/ (visited on 01/03/2025).

[38] *NIST 800-53 Mapping Scope – Mappings Explorer*. URL: https://center-for-threat-informed-defense.github.io/mappings-explorer/about/methodology/nist-scope/ (visited on 12/04/2024).

[39] “NIST Special Publication 800-series General Information”. In: *NIST* (May 21, 2018). Last Modified: 2024-06-24T11:04-04:00. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (visited on 11/18/2024).

[40] NVISIO. *DeTT&CT : Mapping detection to MITRE ATT&CK*. NVISO Labs. Mar. 9, 2022. URL: https://blog.nviso.eu/2022/03/09/dettct-mapping-detection-to-mitre-attck/ (visited on 10/03/2024).

[41] *Our Story | MITRE*. URL: https://www.mitre.org/who-we-are/our-story (visited on 09/07/2024).

[42] Adam Pennington. *“ATT&CK with Sub-Techniques” is Now Just ATT&CK*. MITRE ATT&CK®. July 14, 2020. URL: https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de (visited on 12/18/2024).

[43] Algemene Rekenkamer. *De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN*. 2024.

[44] Dimensional Research. *Trends in security framework adoption*. 2016.

[45] Amy L. Robertson. *Adversary Emulation: Why We Do It*. MITRE-Engenuity. Aug. 17, 2023. URL: `https://medium.com/mitre-engenuity/adversary-emulation-why-we-do-it-629c7e27e566` (visited on 10/04/2024).

[46] R Ross et al. *Recommended security controls for federal information systems and organizations*. NIST SP 800-53r1. Edition: 0. Gaithersburg, MD: National Institute of Standards and Technology, 2005, NIST SP 800–53r1. DOI: `10.6028/NIST.SP.800-53r1`. URL: `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r1.pdf` (visited on 12/22/2024).

[47] Bader Al-Sada, Alireza Sadighian, and Gabriele Oligeri. "MITRE ATT&CK: State of the Art and Way Forward". In: *ACM Computing Surveys* (Aug. 8, 2024), p. 3687300. ISSN: 0360-0300, 1557-7341. DOI: `10.1145/3687300`. URL: `https://dl.acm.org/doi/10.1145/3687300` (visited on 09/07/2024).

[48] K A Scarfone, M P Souppaya, and M Sexton. *Guide to storage encryption technologies for end user devices*. NIST SP 800-111. Edition: 0. Gaithersburg, MD: National Institute of Standards and Technology, 2007, NIST SP 800–111. DOI: `10.6028/NIST.SP.800-111`. URL: `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf` (visited on 12/22/2024).

[49] Blake Storm et al. *MITRE ATT&CK®: Design and Philosophy*. 2018.

[50] Blake Strom. *ATT&CK 101*. MITRE ATT&CK®. Sept. 21, 2018. URL: `https://medium.com/mitre-attack/att-ck-101-17074d3bc62` (visited on 09/07/2024).

[51] Blake Strom. *The Philosophy of ATT&CK*. MITRE ATT&CK®. Nov. 7, 2018. URL: `https://medium.com/mitre-attack/the-philosophy-of-att-ck-9e8f81aba119` (visited on 09/15/2024).

[52] *Tactics - Enterprise | MITRE ATT&CK®*. URL: `https://attack.mitre.org/tactics/enterprise/` (visited on 09/07/2024).

[53] Hamed Taherdoost. "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview". In: *Electronics* 11.14 (July 12, 2022), p. 2181. ISSN: 2079-9292. DOI: `10.3390/electronics11142181`. URL: `https://www.mdpi.com/2079-9292/11/14/2181` (visited on 10/06/2024).

[54] *Techniques - Enterprise | MITRE ATT&CK®*. URL: `https://attack.mitre.org/techniques/enterprise/` (visited on 09/07/2024).

[55] *Threat-Informed Defense | MITRE*. Sept. 6, 2024. URL: `https://www.mitre.org/focus-areas/cybersecurity/threat-informed-defense` (visited on 09/07/2024).

[56] *View MITRE coverage for your organization from Microsoft Sentinel*. Apr. 17, 2023. URL: `https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage` (visited on 10/03/2024).

[57] John Wunder. *Getting Started with ATT&CK: Detection and Analytics*. MITRE ATT&CK®. Sept. 18, 2019. URL: `https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0` (visited on 12/18/2024).