Issues in Information Systems
Volume 25, Issue 3, pp. 62-80, 2024

DOI: https://doi.org/10.48009/3_iis_2024_106

The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector

Mustafa Farouk Abo El Rob, Middle Georgia State University, *mustafa.aboelrob@mga.edu,*
Mohammad Anwar Islam, Middle Georgia State University, *mohammad.islam@mga.edu,*
Sriteja Gondi, University of Texas at Dallas, *Sriteja.Gondi@UTDallas.edu,*
Oula Mansour, Colorado School of Mines, *omansour@mines.edu.*

Abstract

In recent years, the number of cyber attacks on digital enterprises have increased tremendously. In response to the escalation of these attacks, researchers and security professionals have enhanced several cybersecurity frameworks as mitigation mechanisms. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) and NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) are prominent frameworks utilized as the defense mechanisms in various sectors. This paper applies the techniques and tactics of the ATT&CK framework in the assessment of the SolarWinds compromise, illustrating how the security posture can be strengthened. The assessment further demonstrates how entities in the public sector can successfully create plans, methods, processes, and procedures against ATT&CK. This paper explores the practical application of the ATT&CK framework in real-world scenarios. It further aims to assist security leaders and professionals in adopting the ATT&CK framework within their organizations to improve their cyber defense capabilities. Through the implementation of the ATT&CK framework, organizations can create a more resilient and proactive security environment that effectively impedes cyber threats and protects critical digital assets.

Keywords: cybersecurity, frameworks, MITRE ATT&CK, tactics, NIST CSF, SolarWinds.

Introduction

Cybersecurity is a critical business function for today's enterprises. Cybercriminals use intrusion to attack networks, hosts, applications, and systems through various covert channels. These intrusions infiltrate enterprise networks and devices to steal or destroy data, applications, and systems. Mukkamala et al. (2002) defined intrusion as unauthorized access to information within a computer or network system to compromise its integrity and confidentiality. Nowadays, breaches into corporate networks are becoming all too common. A prime example is the Colonial Pipeline incident (Turton & Mehrotra, 2021), where a cyberattack led to the shutdown of a major pipeline. To mitigate the consequences of attacks (e.g., data loss and downtime to major disruptions), robust cyber defenses are essential for companies. In extreme cases like that of the Colonial Pipeline, shutting down systems preemptively is at times necessary to avert disaster.

Over the years, the evolution of cyber threats has necessitated the development of robust cybersecurity frameworks to bolster organizational defenses. Among these, the MITRE ATT&CK, Cyber Kill Chain, Diamond Model of Intrusion Analysis, and NIST Cybersecurity Framework stand out as pivotal in shaping security operations that intelligently combat cyberattacks. Although these frameworks vary in operation,

they collectively contribute to a refined understanding and mitigation of cyber threats. For instance, the MITRE ATT&CK for ICS exemplifies a mid-level framework offering detailed, actionable insights into adversary behaviors, which contrasts with the more abstracted, high-level perspective provided by the Cyber Kill Chain. This distinction highlights how detailed frameworks like MITRE ATT&CK are becoming increasingly preferred for their practical applicability in real-world scenarios, as they allow security professionals to both visualize organizational impacts and execute specific countermeasures against cyberattacks.

The widespread adoption of the MITRE ATT&CK framework, as evidenced by its integration into technologies from vendors like LogRhythm SIEM, Check Point, ServiceNow, Splunk, and F5, underscores its utility. The framework's detailed documentation and standard taxonomies facilitate its implementation across various industries, helping organizations build effective defenses against cyber threats. The Enterprise Matrix of the MITRE ATT&CK framework, accessible at MITRE ATT&CK Enterprise Matrix, serves as a comprehensive guide for organizations to identify potential attack techniques and develop robust counterstrategies.

The purpose of the study is to examine how the MITRE ATT&CK framework can be effectively integrated in the public sector to improve its security posture. In the paper, the framework was applied in the assessment of the SolarWinds compromise. The assessment identified a specific technique from each tactic within the Enterprise Matrix to mitigate adversarial activities. The application of the framework assesses a government organization's preparedness against cyberattacks by leveraging these techniques. Leveraging these specific techniques will enable governmental preparedness against cyberattacks by implementing measures to mitigate, detect and respond to security breaches.

Furthermore, the study explores the organization's confidence in its ability to adopt Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) comprehensively. The rest of the paper is organized as follows: Section 2 is the literature review. Section 3 presents the analysis of MITRE ATT&CK framework-based security controls the organization has implemented to fend-off cyberattacks. Section 4 is the discussion and results.

Literature Review

The MITRE ATT&CK framework has become a pivotal methodology in the cybersecurity domain, offering comprehensive matrices of tactics, techniques, and procedures (TTPs) that guide security experts and organizations in identifying, understanding, and defeating cyberattacks. The MITRE ATT&CK utilizes a holistic approach by incorporating PRE-ATT&CK and ATT&CK models. PRE-ATT&CK is a complementary model that focuses on encompassing the different phases of the organization's attack life cycle to aid in preventing cyberattacks (Georgiadou et al., 2021). Gonzales (2022) applied both MITRE ATT&CK and a different set of frameworks called the Cyber Kill Chain in the context of a small business environment. Although the frameworks were different, they resulted in the same conclusion. Both frameworks identified that user awareness has the biggest impact against ransomware attacks. Pérez-Sánchez & Palacios (2022) proposed a detection system based on analyzing events and matching the risk level with the MITRE ATT&CK matrix and Cyber Kill Chain. The author found that standard antivirus/antimalware software was not fully capable of detecting sophisticated malware.

Expanding on the foundational role of the MITRE ATT&CK framework in enhancing cybersecurity measures, its application and relevance become more evident when evaluating the adaptive challenges faced by various sectors during the COVID-19 pandemic (INTERPOL, 2020). This dramatic shift in the cybersecurity landscape set the stage for Executive Order 14028, issued on May 12, 2021, which mandated

federal agencies to implement the Zero Trust (ZT) Architecture-based security posture. This directive demonstrated a strategic dynamic towards the necessity for adaptive and robust frameworks like MITRE ATT&CK.

Karabacak & Whittaker (2022) analyzed whether the data breach of 2020 could have been prevented if the federal government had implemented zero-trust architecture on the attacked networks. The authors employed the MITRE ATT&CK framework to elucidate how the techniques and methodologies used by threat groups, such as APT29, can be effectively mitigated to prevent initial access attempts into federal networks. Kern et al. (2022) tested their D3TECT process model for tracing attacks on data sources using the MITRE ATT&CK framework. Bautista and Parada (2021) proposed the evaluation of web application software through the utilization of various frameworks recognized as industry best practices, including but not limited to, the MITRE ATT&CK, ISO/IEC standards, and the Software Assurance Maturity Model. Furthermore, Hwang et al. (2021) utilized real-world EDR event logs and incorporated MITRE ATT&CK knowledge with autoencoder-based anomaly detection techniques. This integration facilitated anomaly identification, resulting in more effective analysis and target selection from a security management perspective. Subsequent observations revealed indications of anomalous attacks, which prompted alerts to security managers and enabled the linkage of log information to legacy systems. Williams (2020) outlined the MITRE ATT&CK framework's potential in assessing an organization's competency in identifying, detecting, preventing, and recovering from cyberattacks. Shin et al. (2022) analyzed historical phishing endeavors by APT groups, applying the MITRE ATT&CK framework and TTPs to scrutinize various campaigns and devise counterstrategies against these threats.

With greater investigation into anomaly detection methodologies and the application of the MITRE ATT&CK framework in evaluating cybersecurity efficacy, there is a transition shift towards the innovative implementation of in-network deception technology within developed substation infrastructure systems. This technological innovation, which aims to strengthen the defenses of critical power grid components, represents a significant advancement in the field of cybersecurity. By integrating deceptive elements directly into the network infrastructure, a new, complex cybersecurity landscape is created, confounding potential attackers. For instance, decoy assets, intelligently designed to mimic authentic infrastructure components, act as bait, thereby increasing the prospect of early threat detection and neutralization by diverting attackers from critical assets (Mashima, 2022). Corresponding to the decoy assets, the incorporation of deterrent mechanisms, such as warning banners or simulated security measures, further discourages cyber-attacks.

Aligned with established frameworks such as the MITRE ATT&CK, in-network deception employs well-documented adversary tactics to provide a proactive and dynamic defense strategy against evolving cyber threats that target crucial electrical infrastructure. This method emphasizes a robust transition towards more resilient and adaptive cybersecurity measures, symbolizing a holistic approach in protecting critical national infrastructure from cyber-attacks (Mashima, 2022).

Expanding on these dynamic defense mechanisms, Kwon et al. (2020) developed the innovative Cyber Threat Dictionary (CTD) which is a pioneering framework designed to harmonize the detailed catalog of adversary behaviors outlined in the MITRE ATT&CK matrix—encompassing tactics, techniques, and procedures (TTPs)—with the strategic principles of the NIST Cybersecurity Framework, which aims to enhance organizational cyber defense postures. By integrating these two pivotal cybersecurity standards, the CTD provides professionals with a comprehensive toolkit for better identification, understanding, and mitigation of cyber threats.

Conforming to the MITRE ATT&CK architecture, in-network deception employs recognized adversarial tactics to establish a proactive and dynamic defense against the continuously evolving cyber threats that target critical electrical infrastructure (Mashima, 2022). This approach marks a significant shift towards more resilient and adaptive cybersecurity practices, demonstrating a holistic strategy in protecting vital national infrastructure from advanced cyber-attacks. Expanding on the capabilities of in-network deception technology, the discussion also introduces the innovative Cyber Threat Dictionary (CTD) developed by Kwon et al. (2020). This new framework seeks to integrate the detailed adversarial tactics, techniques, and procedures cataloged in the MITRE ATT&CK matrix with the strategic principles outlined in the NIST Cybersecurity Framework. This integration aims to enhance an organization's cyber defense capabilities. By merging these two fundamental cybersecurity standards, the CTD provides cybersecurity professionals with a comprehensive toolkit for better identifying, understanding, and addressing cyber threats.

This integration fosters a more structured and effective approach to managing cyber threats by utilizing detailed insights into adversary behaviors from the MITRE ATT&CK framework alongside the strategic guidance provided by the NIST Framework. As a result, the Cyber Threat Dictionary (CTD) enhances the understanding of the threat landscape and supports the implementation of timely and impactful countermeasures against cyber-attacks. Kwon et al. (2020) work through the CTD marks a crucial enhancement in cybersecurity practices, underscoring the importance of integrating and mapping established frameworks to develop comprehensive, actionable strategies for cyber defense. As cyber threats grow in complexity and sophistication, such innovations are crucial in strengthening digital infrastructures against new vulnerabilities.

In the broader discussion of cybersecurity innovations and the need to augment cyber defense mechanisms, it is essential to consider real-life incidents that highlight the complexity of contemporary cyber threats. A notable example is the SolarWinds Compromise, a sophisticated supply chain attack orchestrated by APT29 that emerged in mid-December 2020. This breach involved the introduction of malicious code into the SolarWinds Orion software build process, disseminated through a standard software update. The tactics employed by APT29 included password spraying, token theft, API abuse, and spear phishing, targeting a wide range of entities across government, consulting, technology, telecom, and other sectors worldwide. Roy et al. (2023) presents a pivotal systematization of knowledge (SoK) that highlights the convergence of the ATT&CK framework's practical applications within industry settings and its scholarly research implications. This framework is recognized for its comprehensive catalog of adversarial tactics and techniques, derived from empirical observations, with broad applications across various cybersecurity domains including threat intelligence, detection, and incident response. Despite its broad utilization, the academic and practical discourse has lacked a systematic review that amalgamates its varied applications and assesses its effectiveness.

Roy et al. (2023) addresses this gap by conducting a taxonomic review of the academic literature pertaining to the ATT&CK framework. They evaluate its application efficacy across diverse contexts and identify areas necessitating further scholarly inquiry. Their literature review highlights the framework's adaptability, noting its deployment in scenarios ranging from automated threat detection systems to the enrichment of cybersecurity educational curricula. The ATT&CK framework not only facilitates the categorization and comprehension of adversary behaviors but also supports the formulation of defensive strategies informed by a detailed understanding of potential attack methodologies. In professional circles, it has been pivotal in standardizing terminologies related to cyber threats, thus enhancing communication and collaborative efforts across different organizations.

A significant revelation from Roy et al.'s review is the identification of research gaps, particularly in the practical deployment and evaluation of the framework. Although the ATT&CK framework offers a solid

foundation for understanding adversarial behaviors, there exists a pronounced need for empirical studies to corroborate its efficacy in real-world settings. Moreover, the authors suggest the framework's potential expansion into emerging cybersecurity domains like predictive threat intelligence and automated defense systems. By delineating its current research applications, industry utilization, and potential areas for future research, Roy et al. enhance our understanding of the framework's capabilities in advancing organizational cybersecurity postures. As the landscape of cybersecurity threats evolves, the MITRE ATT&CK framework remains an indispensable resource in the ongoing endeavor to protect digital environments and infrastructure.

During the COVID-19 pandemic, the cybersecurity landscape saw a dramatic transformation, with an increase in cyber threats exploiting the situation. Supply chain disruptions became a focal point for cybercriminals, taking advantage of weakened infrastructures due to increased demand and reduced workforce capabilities. E-commerce and retail sectors, propelled by a surge in online shopping, faced heightened risks, including compromised payment credentials and cloud storage breaches. The travel industry, already vulnerable, encountered additional challenges as pandemic-related restrictions presented new opportunities for cybercriminals to exploit. INTERPOL (2020) reported a significant shift in cybercriminal targets from individuals and small businesses to major corporations, governments, and critical infrastructure, underscoring the increased security vulnerabilities as organizations rapidly deployed remote systems and networks to support staff working from home. Among the prevalent threats were COVID-19 themed phishing and online frauds, disruptive malware attacks against critical infrastructure and healthcare institutions, data harvesting malware, and a surge in malicious domain registrations related to COVID-19.

Moreover, the shift to remote work highlighted several cybersecurity issues, such as the increased risk of phishing attacks targeting remote workers and the vulnerabilities of organizations relying on legacy security architectures like VPNs. Budget constraints further complicated the cybersecurity landscape, with many organizations facing difficulties in adequately protecting against digital threats (INTERPOL, 2020). This period underscored the critical need for enhanced cybersecurity measures, including the adoption of "zero-trust" architectures, consolidated security solutions, and heightened security for the healthcare and financial sectors. The rapid expansion into AI and cloud technologies also highlighted the importance of adapting cybersecurity solutions to protect against new and evolving threats.

Analysis

The fourteen tactics in the Enterprise MITRE ATT&CK and one associated technique from each tactic are outlined below to demonstrate how organizations in the public sector can utilize the MITRE ATT&CK framework to address cyberattacks based on adversarial behaviors and activities in real-world scenarios. The techniques of each tactic have been carefully selected to best meet the specific needs of the organization within the public sector.

Tactic: ID: TA0001 - Initial Access *Technique ID: T1566 – Phishing*

Through Initial Access, competitors can control the cyber dynamics of the enterprise systems (Xiong et al., 2021). Adversaries may send phishing messages to gain access to the victim's machine. Many phishing attacks are conducted through social engineering, posing as a valid message from a trusted source. Phishing can be targeted at individuals, called spear phishing. The phishing message can send an attachment or link, and once the victim clicks the link or downloads the infected malware file, it executes the malicious code onto the victim's machine. Phishing can be conducted through social media sites as well. Organizations

implement firewalls to protect the network from malicious activities and equip all departments with additional security measures through secure web browsers making the agency fully prepared to fend off phishing attacks.

Policy and Process: There are clear policy guidelines for the workforce about phishing attacks, including how not to fall victim to attacks. Also, every month, employees will get at least one reminder of phishing attacks and associated dangerous consequences.

People: The organization has a comprehensive cybersecurity awareness and training program. Every member of the workforce must comply with security policies, including employee roles and responsibilities, the use of government-furnished equipment, social media use, etc. Furthermore, employees must take yearly compliance training, and each employee must pass the knowledge test with a minimum score of 80%.

Technology: Organizations have automated email filtering software to block malicious content. There is an allowed list for the trusted domain. Furthermore, the organization has a rigorous program in simulated phishing exercises run every month to identify vulnerabilities. The phishing exercises help the organization understand deficiencies in the workforce and improve training materials to beef up security posture.

- M1049- Antivirus/Antimalware: Anti-virus tools automatically quarantine suspicious files.
- M1031 - Network Intrusion Prevention: The network-based intrusion detection and prevention systems are in place.
- M1021 - Restrict Web-Based Content: The reverse web proxies have been implemented, preventing communication through unauthorized services.

Tactic: ID: TA002 – Execution *Technique ID: T1053 – Scheduled Task/Job*

During Execution, almost every organization can schedule information technology tasks in a fixed interval of time to perform some routine function like processing of data, workflows, etc. Therefore, adversaries may try to gain access to scheduled jobs and gain privileged access and execute malicious code. According to cybersecurity researchers, one can predict malicious activity by examining the behavior of the systems (Ajmal et al., 2021). This is significant to note as part of the active scanning and monitoring for the company.

Policy and Process: The agency security policy outlines user account management, including privilege account management and auditing of user activities, especially for privilege accounts.

People: All users must sign the rules of behavior and abide by the rules.

Technology: The Agency has deployed several mitigations and controls to defend the enterprise:

- M1047- Audit: The Agency uses the software toolkit to explore systems for permission weaknesses that could elevate privileges.
- M1026 – Privileged Account Management: The Agency only allows Admin group members to schedule the priority process.
- M1018 – User Account Management: The principle of least privileges is in place for all user accounts, and no privilege escalation is allowed.

Tactic: ID: TA0003 – Persistence *Technique ID: T1098 – Account Manipulation*

In Persistence, adversaries may penetrate and create unauthorized accounts to victim systems with higher privileges. Additionally, the attacker takes account manipulation action to preserve access to the compromised account. Manipulation activities may include subverting security policies like performing password updates, password reset policies, etc. Some controls are in place to mitigate the risk of this account manipulation technique.

Policy and Process: Security policy for privileged accounts describes account management, account life cycle, multi-factor authentication, etc.

People: Privilege account holders must sign and abide by privilege account rules of behavior throughout the life of the account.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1032 – Multi-factor Authentication (MFA): MFA is in place for all users and privileged accounts.
- M1030 – Network Segmentation: Access controls and firewalls for critical systems and domain controllers. The Agency uses a virtual private cloud to segment its resources.
- M1026 – Privilege Account Management: Privilege account holders must use their regular user account for day-to-day operational activities (not privilege account).

Tactic: ID: TA0004 – Privilege Escalation - *Technique ID: T1548 – Abuse Elevation Control Mechanism*

Through Privilege Escalation, and the corresponding technique being "Abuse Elevation Control Mechanism", organizations apply this technique to further block users from accessing system files (who do not have appropriate security clearance) and monitor service calls that may lead to system variable change.

Through this tactic, adversaries try to gain higher-level permissions on a system or network.
Some controls are in place to mitigate the risk of abuse elevation escalation technique. Adversaries can perform several methods to use the control mechanism to elevate privileges. In the Agency, several controls are in place to mitigate this risk.

Policy and Process: Security policy for privilege elevation describes who, how, and under what authority a person can perform elevation activities.

People: Privilege account administrators must sign and abide by rules of behavior before setting up the account.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1047 – Audit: Software tools to audit system admin and privilege accounts.
- M1026 – Privilege Account Management: Privilege account holders must only use their user account for day-to-day operational activities (not privilege account).
- M1052 – User Account Control: This control ensures that the highest level of enforcement is in place to prevent authorized elevation.

Tactic: ID: TA0005 – Defense Evasion *Technique ID: T1562 – Impair defenses*

In Defense Evasion, adversaries try to disable controls to do logging and audit verifications.
These are some controls to mitigate the risk of impairing the technique of the defense. There are several rules in place in the Agency to minimize this risk.

Policy and Process: The security policy for logging and auditing describes the mandatory defense mechanism and its resiliency to prevent impairment.

People: Administrator-level professionals have been trained to monitor all cyber defense controls.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1022 – Restrict File and Directory Permissions: Robust software tools are in place to restrict file and directory permissions.
- M1024 – Restrict Registry Permissions: Software tools are in place to restrict registry permissions.
- M1018 – User Account Management: Account management is in place to prevent the user activity logging mechanism from disabling.

Tactic: ID: TA0006 – Credential Access *Technique ID: T1556 – Modify Authentication Process*

Through Credential Access, and the corresponding technique "Modify Authentication Process", adversaries try to alter authentication processes and methods to access user credentials through this tactic. The criminals may modify the authentication process by either stealing the valid credentials or bypassing the authentication mechanism. Once successful in changing the process, adversaries can utilize stolen credentials to access the system. If adversaries know how to avoid the authentication mechanism, they will access various systems within the network.

Policy and Process: The security policy elaborated on credential access and associated risks.

People: The system administrators and administrators of identity and access management have been trained on vulnerabilities of authentication processes and best practices to safeguard the authentication mechanisms.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1032 – Multi-factor Authentication (MFA): MFA is in place for all users and privileged accounts.
- M1026 – Privilege Account Management: Privilege account holders must only use their user account for day-to-day operational activities (not privilege account).
- M1022 – Restrict File and Directory Permissions: Software tools are in place to restrict file and directory permissions.

Tactic: ID: TA0007 – Discovery *Technique ID: T1040 – Network Sniffing*

In Discovery, the technique is Network Sniffing, and these are fulfilled as the organizations implement multi-factor authentication at the enterprise level and apply network encryption. Adversaries may sniff the network to acquire information about the environment, including authentication tokens passed over the networks. The hackers may place a network interface to collect data in transit over the network passively. The Agency has implemented controls to defend against attacks using network sniffing.

Policy and Process: The security policy describes security controls to prevent network sniffing attacks.

People: Administrator-level professionals have been trained in detecting and preventing sniffing attacks

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1041 - Encrypt Sensitive Information: All traffic is encrypted using TLS/SSL and authentication through encrypted protocols like Kerberos.
- M1032 – Multi-factor Authentication (MFA): MFA is in place for all users and privileged accounts.

Tactic: ID: TA0008 – Lateral Movement *Technique ID: T1210 – Exploitation of Remote Services*

Through Lateral Movement, adversaries use the Exploitation of Remote Services. This tactic and technique are significant as organizations have carried out network scans and segregated incoming traffic appropriately. Adversaries may exploit remote services to gain unauthorized access to the internal networks. Adversaries can discover vulnerabilities like unpatched software through discovery methods like network scanning. The attackers also try to find defensive security software for detecting remote exploitation. The Agency has implemented the proper controls and mitigation strategies to avoid attacks by exploiting remote services.

Policy and Process: The security policy describes security controls for preventing cyberattacks by exploiting remote services.

People: Network engineers, system administrators, software engineers, and other IT support professionals have been trained to detect and prevent attacks through remote services.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1030 - Network Segmentation: Network segmentation isolates systems so that attackers cannot move all around the network.
- M1026 – Privilege Account Management: Privilege account holders must only use their user account for day-to-day operational activities (not privilege account).
- M1019 -Threat Intelligence Program: The Agency has a dedicated team for threat intelligence to gather information about advanced persistent threats (APT) and threat actors and proactively put controls to defend the Agency.
- M1051- Update Software: Agency has comprehensive patch management and software updates to ensure that unsupported software and tools are removed from all endpoints and servers.
- M1016 - Vulnerability Scanning: The Agency implemented a vulnerability platform that automatically scans networks and servers to detect vulnerabilities.

Tactic: ID: TA0009 – Collection *Technique ID: T1557 –Adversary-in-the-Middle*

In the Collection tactic, there are techniques that adversaries may use to gather data and sources of the data to use for malicious purposes. Using the Adversary-in-the-Middle technique, threat actors may force a device to communicate through an adversary-controlled system so that they can collect information or take some action. Through this tactic, adversaries steal or illegally exfiltrate data outside the organization. There are several rules to detect and prevent adversary-in-the-middle attacks and minimize credential access risks.

Policy and Process: The security policy elaborated details about adversary-in-the-middle attacks.

People: The Agency has provided training to its workforce about adversarial data collection techniques and methods to detect and prevent collection tactic attacks.

Technology: These controls and mitigation mechanisms are in place in the organization:

- M1041 - Encrypt Sensitive Information: All traffic is encrypted using TLS/SSL and authentication through encrypted protocols like Kerberos.
- M1037 - Filter Network Traffic: Network appliances filter and block suspicious traffic.
- M1031 - Network Intrusion Prevention: The network-based intrusion detection and prevention systems are in place.
- M1030 - Network Segmentation: Network segmentation isolates systems so that attackers cannot move all around the network.

Tactic: ID: TA0010 – Exfiltration *Technique ID: T1041 –Exfiltration Over C2 Channel*

Exfiltration is where adversaries and criminals steal data from the network. Adversaries usually package data using compression and encryption to avoid detection. Command-and-control (C2) and similar other channels are used to transfer data. The organization adopted security controls to defend against command-and-control attacks.

Policy and Process: The security policy elaborated on data loss prevention (DLP) and mechanisms to prevent data exfiltration.

People: The Agency has provided cybersecurity and network professionals training about data loss prevention techniques and tools to defend against this type of attack.

Technology: These controls and mitigation mechanisms are in place in the organization:

- M1031 - Network Intrusion Prevention: The network-based intrusion detection and prevention systems are in place.
- M1057 - Data Loss Prevention: The Agency has implemented comprehensive tools for data loss prevention.

Tactic: ID: TA0011 – Command and Control *Technique ID: T1102 – Web Service*

In Command-and-Control, researchers have this tactic as one that utilizes remote interfaces to conduct hostile operations within the organization (Xiong et al., 2021). This represents an inter-organization attack. Cybercriminals install malware on a device within the victim's network. Once malware gets installed, it starts communicating with the adversary-controlled external server. Adversaries may use an existing and legitimate web service as a conduit to transfer data to/from the compromised system. Since the web service uses TLS encryption, it is difficult for the victim to detect data exfiltration. The organization adopted security controls to defend against command-and-control attacks.

Policy and Process: The security policy elaborated mechanisms and controls to defend against command-and-control attacks.

People: The Agency has provided cybersecurity and network professionals training about command-and-control techniques and tools to defend against this type of attack.

Technology: These technology controls and mitigation mechanisms are in place in the organization:

- M1031 - Network Intrusion Prevention: The network-based intrusion detection and prevention systems are in place.
- M1021 - Restrict Web-Based Content: The reverse web proxies have been implemented, preventing communication through unauthorized services.

Tactic: ID: TA0040 – Impact *Technique ID: T1565 – Data Manipulation*

Through the Impact tactic and corresponding Data Manipulation Technique, organizations maintain regular data backups as part of a disaster management plan and restricted file modification permissions. The adversaries are trying to interrupt business operations or destroy data and systems. Cybercriminals may alter or delete data to manipulate outcomes, create havoc in the victim organization's business processes, and even disrupt some operations. The Agency has taken a holistic approach to preventing criminals and adversaries from disrupting business operations.

Policy and Process: The security policy focused on disaster recovery (DR) and continuity of operations (COOP).

People: The Agency has provided cybersecurity and system operations professionals training on the continuity of operations and disaster recovery.

Technology: These controls and mitigation mechanisms are in place in the organization:

- M1041 - Encrypt Sensitive Information: All traffic is encrypted using TLS/SSL and authentication through encrypted protocols like Kerberos.
- M1030 – Network Segmentation: Access controls and firewalls for critical systems and domain controllers. The Agency uses a virtual private cloud to segment its resources.
- M1029 - Remote Data Storage: The Agency has implemented disaster recovery locations and different availability zones of cloud infrastructure to ensure disaster recovery.
- M1022 – Restrict File and Directory Permissions: Software tools are in place to restrict file and directory permissions.

Tactic: ID: TT0042 Resource Development *Technique ID: T1584 – Compromise Infrastructure*

In Resource Development, and the corresponding Compromise Infrastructure technique, organizations leverage this technique to protect their overall systems' infrastructure by executing vulnerability scans and continued monitoring the companies' environments.

Policy and Process: The security policy focused on minimizing amount and sensitivity of data.

People: Security Configuration Managers and Policy Analysts.

Technology: These controls and mitigation mechanisms are in place in the organization:

- (M1056) - Pre-compromise: Although this technique is challenging to mitigate, organizations can limit the amount and sensitivity of data that is available to external users by monitoring domain name system (DNS) data that can compromise third-party infrastructure.

Tactic: ID: TT0043 Reconnaissance *Technique ID: T1590 – Gather Victim Network Information*

During Reconnaissance and its subsequent technique "Gather Victim Network Information", organizations utilize this technique to implement active phishing defenses and eliminate interfaces with third parties in order to protect the network and infrastructure information from malicious activities. These defenses can be tested and refined by having designated users attempting certain phishing emails.

Policy and Process: The security policy focused on minimizing amount and sensitivity of data.

People: Threat Intelligence Analysts and Security Awareness Trainers.

Technology: These controls and mitigation mechanisms are in place in the organization:

- (M1056) - Pre-compromise: Although this technique is challenging to mitigate, organizations can limit the amount and sensitivity of data that is available to external users.

Case Study of MITRE ATT&CK Implementation in the Public Sector

A case study was executed to evaluate the thorough analysis of the MITRE ATT&CK implementation. The government agency utilized for the study has established an overarching security policy to safeguard its data, systems, and infrastructure. To achieve robust defense against adversarial attacks, the agency has implemented a comprehensive portfolio of security technologies, including both hardware and software resolutions. Integral to this strategy are several established security architectures and frameworks, notably the NIST Cybersecurity Framework and the MITRE ATT&CK framework. By adhering to industry best practices, the agency has meticulously architected, designed, and implemented its security posture, utilizing technologies that align with the NIST and MITRE standards. These frameworks have been pivotal in defining the agency's security architecture, capabilities, and functionalities to detect, protect, and remediate adversarial threats.

The SolarWinds Compromise underscores the complex nature of modern cyber espionage and the formidable challenges in securing supply chains from advanced adversaries. The attribution of this campaign to Russia's Foreign Intelligence Service (SVR), as confirmed by the US and UK governments in April 2021, highlights the state-supported dimensions of these operations. Affecting approximately 18,000 public and private sector entities, with a smaller subset experiencing system compromises due to subsequent APT29 activities—serves as a stark reminder of the intensifying cyber threat landscape. The MITRE ATT&CK framework, by providing a structured analysis of known adversary tactics and techniques, enables organizations to anticipate, prepare for, and effectively neutralize sophisticated cyber-attacks. Thus, the agency's adoption of these frameworks is crucial in maintaining a resilient and proactive security posture amidst an increasingly hostile cyber environment.

Results and Discussion

Based on a thorough evaluation of the current security posture in relation to the tactics and techniques outlined by the MITRE ATT&CK framework, the organization has implemented a series of mitigation measures, procedures, and industry best practices. This comprehensive security approach has effectively shielded the government agency from significant cyberattacks. The agency boasts a dedicated cybersecurity organization led by a Chief Information Security Officer (CISO) and staffed with highly skilled cybersecurity professionals. This team has fully embraced the ATT&CK framework, ensuring a structured and proactive defense strategy. The cybersecurity unit has established a formal mechanism for continuous threat intelligence monitoring, allowing them to swiftly identify emerging threats and techniques.

Consequently, the security team can promptly implement appropriate mitigation measures in response to the nature and severity of new threats, as well as the capabilities of adversaries. Therefore, the author is confident in the agency's ability to adequately anticipate and counter adversarial tactics, techniques, and common knowledge, ensuring robust cybersecurity preparedness and resilience.

The SolarWinds compromise highlights three key aspects that underscore the need for advanced cybersecurity measures. First, the malicious code remained undetected for several months, allowing attackers to conduct reconnaissance and selectively target valuable assets, demonstrating the difficulty of detecting and mitigating such campaigns without significant resources and expertise. Second, the attackers' high level of sophistication enabled them to bypass traditional security measures by modifying legitimate software updates to distribute malware, indicating the necessity for organizations to adopt advanced cybersecurity measures to defend against well-resourced adversaries. Finally, the compromise emphasizes how vulnerabilities within supply chains can lead to widespread security breaches, where a single compromised vendor can have far-reaching consequences. As seen with the uncertainty of the last few years with the COVID-19 pandemic, the dynamics of cybersecurity have shifted in organizations across all industries. The workforce model has been virtualized, with employees working primarily from home. Companies have transformed their business models and interactions with clients to adapt to this new normal. Given the increased reliance on virtual interactions, persistent adversaries have expanded their target environments and evaded cyber defenses, as seen in the MITRE ATT&CK framework. The final takeaways from the Enterprise MITRE ATT&CK matrix emphasize that companies should adopt robust cybersecurity measures, apply best practices in systems development, proactively update security software with recent malware information, and provide security awareness training programs for all employees. By implementing these concepts and takeaways, organizations can achieve a robust approach and mature security capabilities, ensuring enterprise-wide cybersecurity success.

The mitigation strategies used during the SolarWinds Compromise are identified below, highlighting each key technique with its respective mitigation strategy to provide comprehensive protective measures. Additionally, insights from the paper "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping" are integrated to enhance the understanding and application of these mitigation strategies. In regular patching, one must ensure all systems and applications are regularly patched to fix known vulnerabilities, reducing the risk of exploitation, as covered by PR. IP-12. Organizations must develop and maintain an incident response plan to ensure quick addressal and mitigation of security incidents, supported by RS.RP-1. Security professionals must conduct regular security awareness training for all employees to reduce the risk of social engineering attacks, aligned with PR.AT-2.

1. Account Discovery (T1087)

- Access Controls: Implementing strict access control and least privilege principles can significantly reduce the number of accounts with elevated permissions, minimizing the attack surface. According to the Cyber Threat Dictionary, mapping these principles to the NIST Cybersecurity Framework's (CSF) Identity Management and Access Control (PR.AC) helps standardize and enhance security posture.
- Behavioral Analytics: Monitoring user behavior for unusual activities can help detect reconnaissance attempts early. The use of the MITRE ATT&CK Matrix in conjunction with the NIST CSF Detect function (DE.CM) provides a structured approach to identifying abnormal behavior.
- Auditing and Monitoring: Regularly auditing account permissions and utilizing automated tools to detect abnormal account enumeration activities can enhance security. This aligns with the CSF's Continuous Security Monitoring (DE.CM) category.

2. Account Manipulation (T1098)

- Multi-Factor Authentication (MFA): Requiring MFA for all accounts helps prevent unauthorized access even if credentials are compromised. The CSF's Identity Management (PR.AC-7) recommends MFA as a key control.
- Privileged Access Management (PAM): PAM solutions are essential for managing and monitoring privileged accounts and their activities. This is mapped to PR.AC-4 in the NIST CSF.
- Frequent Reviews: Regularly reviewing OAuth applications and service principles ensures no unauthorized changes have occurred, supporting PR.DS-6.

3. Infrastructure Acquisition (T1583)

- Domain Monitoring: Keeping an eye on domain registration and acquisition activities, along with using threat intelligence services, helps identify malicious domains. This corresponds to DE.CM-8 in the NIST CSF.
- Network Segmentation: Implementing network segmentation limits the spread of malicious activities from compromised infrastructure. This aligns with PR.AC-5.
- Threat Intelligence: Leveraging threat intelligence feeds keeps organizations informed about new and emerging threats related to infrastructure acquisition. This practice is supported by the NIST CSF's Information Sharing (ID.RA-2).

4. Application Layer Protocol (T1071)

- Encrypted Traffic Inspection: Inspecting SSL/TLS traffic can reveal malicious activity within encrypted communications. This technique maps to PR.DS-2 in the CSF.
- Web Application Firewalls (WAF): Deploying WAFs helps filter and monitor HTTP traffic for signs of command and control (C2) and data exfiltration activities. The relevant CSF category is PR.DS-1.
- Anomaly Detection: Implementing network anomaly detection systems identifies unusual patterns in web traffic. This is covered under DE.AE-3.

5. Command and Scripting Interpreter (T1059)

- Application Whitelisting: Restricting script and command-line interpreter execution to trusted applications and users prevents unauthorized script execution. This is aligned with PR.IP-1.
- PowerShell Constrained Language Mode: Using constrained language mode in PowerShell limits the execution of potentially harmful scripts. This technique is supported by PR.PT-1.
- Logging and Monitoring: Enabling detailed logging of script executions and monitoring for suspicious activities enhances detection capabilities, aligning with DE.CM-1.

6. Credentials from Password Stores (T1555)

- Password Policies: Implementing strong password policies, including regular changes and complexity requirements, secures credentials. This is aligned with PR.AC-1.
- Credential Guard: Solutions like Microsoft Credential Guard protect credentials stored on endpoints, supported by PR.DS-5.
- Secure Storage: Ensuring credentials are stored securely using modern cryptographic techniques prevents unauthorized access, as recommended in PR.DS-1.

7. Data from Information Repositories (T1213)

- Access Controls: Implementing strict access controls on internal knowledge repositories and sensitive information limits unauthorized access, aligned with PR.AC-3.

- Data Encryption: Encrypting sensitive data both at rest and in transit protects it from unauthorized access, as covered by PR.DS-1.
- Regular Audits: Conducting regular audits of access to information repositories helps detect and respond to unauthorized access, aligning with PR.PT-1.

8. Deobfuscate/Decode Files or Information (T1140)

- Anti-Malware Solutions: Deploying advanced anti-malware solutions capable of detecting and blocking deobfuscation attempts protects against malware, supported by PR.PT-3.
- File Integrity Monitoring: Using file integrity monitoring tools detects changes to critical files and binaries, aligning with DE.CM-8.
- Security Training: Training employees to recognize and respond to phishing and social engineering attacks reduces the risk of executing deobfuscated malware, as recommended by PR.AT-1.

9. Dynamic Resolution (T1568)

- DNS Security: Implementing DNS security measures such as DNSSEC and monitoring for suspicious DNS queries enhance protection, aligned with PR.DS-1.
- Blacklist Malicious Domains: Maintaining and updating a blacklist of known malicious domains and blocking them at the DNS level prevents communication with C2 servers, covered by DE.CM-8.
- Network Monitoring: Using network monitoring tools to detect and respond to abnormal DNS resolution patterns improves threat detection, supported by DE.CM-1.

10. Email Collection (T1114)

- Email Encryption: Encrypting email communications protects sensitive information, aligned with PR.DS-2.
- DLP Solutions: Deploying Data Loss Prevention (DLP) solutions monitors and controls the flow of sensitive information via email, supported by PR.DS-8.
- Access Restrictions: Restricting access to email export tools and monitoring their usage prevents unauthorized email collection, aligning with PR.AC-4.

Conclusion

Integrating policy, people, processes, and technology with the tactics and techniques from the ATT&CK framework effectively cultivates to an innovative approach in mitigating cybersecurity threats. By leveraging the MITRE ATT&CK framework, public sector organizations can enhance their cybersecurity capabilities, improve their resilience against cyber threats, and ensure they are better prepared to protect sensitive information and critical infrastructure. Adopting the ATT&CK framework provides the public sector with a standardized language and approach to cybersecurity, promotes interoperability and collaboration across various government agencies and international partners. This standardization is a novel strategy for addressing cyber threats at both national and global levels. The framework's continuous evolution and adaptation within the public sector context allow government organizations to stay ahead of adversaries by regularly updating their defenses based on the latest threat intelligence and attack patterns.

Integrating the MITRE ATT&CK Matrix with the NIST Cybersecurity Framework (CSF) offers a comprehensive approach to enhancing an organization's cybersecurity posture. By combining the detailed insights from the MITRE ATT&CK Matrix with the strategic guidance of the NIST CSF, organizations can develop a robust and multifaceted security strategy. This integration, as demonstrated by Kwon et al. (2020), enhances threat detection and response capabilities by providing detailed information on adversary tactics, techniques, and procedures (TTPs), ensuring comprehensive and aligned security measures. The

NIST CSF's broad coverage across identification, protection, detection, response, and recovery, when combined with the MITRE ATT&CK Matrix, ensures that no aspect of security is neglected. Leveraging detailed attack scenarios from the MITRE ATT&CK Matrix alongside the NIST CSF's risk management principles enables informed decision-making and prioritization of security efforts. The iterative nature of both frameworks promotes continuous monitoring and improvement, enabling organizations to regularly update their defenses based on the latest threat intelligence and security best practices.

The SolarWinds Compromise was a significant cyberattack that exploited the SolarWinds Orion platform to gain unauthorized access to multiple organizations. By examining the key techniques used in this attack, we identified specific mitigation strategies such as strict access controls, multi-factor authentication, network segmentation, and advanced threat detection measures. Integrating these mitigation techniques with the guidance provided by the MITRE ATT&CK Matrix and the NIST CSF can significantly reduce the risk of similar attacks. Our analysis highlighted the importance of continuous monitoring, regular updates to security protocols, and comprehensive threat intelligence to stay ahead of evolving cyber threats. In conclusion, the combined use of the MITRE ATT&CK Matrix and the NIST CSF offers a powerful approach to enhancing cybersecurity.

Limitations and Future Research

A significant limitation of this study is the lack of access to comprehensive and high-quality historical data in the public sector. Government organizations face challenges related to data confidentiality, integrity, and availability. A systematic review published in the Journal of Cybersecurity highlights the critical issue of data scarcity in cyber risk research. The review emphasizes how the development of effective cyber risk models is negatively impacted due to the lack of historical data (Elm & Eckenrode, 2023). This shortage is particularly problematic in the public sector, where data is often restricted due to confidentiality concerns. The review calls for improved data sharing practices to enhance cybersecurity research and policy making. Due to strict data protection regulations and the sensitive nature of governmental information, detailed and historical cybersecurity incident data is often restricted. This limitation hinders the ability to conduct thorough analyses and develop robust AI and ML models that could enhance the MITRE ATT&CK framework. Future research should focus on establishing secure data-sharing agreements to enable the collection and utilization of high-quality data while safeguarding confidentiality.

Another key issue is the lack of standardized metrics and benchmarks in the public sector, which disrupts the objectivity of the MITRE ATT&CK framework. Without established benchmarks, evaluating the impact of integrating the framework on cybersecurity postures is challenging. The absence of clear metrics leads to reliance on qualitative assessments and subjective judgments, which may not accurately reflect the framework's performance. The White House’s Federal Cybersecurity R&D Strategic Plan of 2023 highlights this problem and calls for improved metrics to better understand cybersecurity measures' impact and guide future research (The White House, 2024).

Despite the benefits, there are notable challenges in integrating these frameworks. The complexity and resource-intensive nature of combining the detailed TTPs from the MITRE ATT&CK Matrix with the broader categories of the NIST CSF can be demanding, requiring significant expertise and effort. Kwon et al. (2020) acknowledges these challenges but also highlights the potential benefits of overcoming them. Smaller organizations with limited resources may find it difficult to implement and maintain both frameworks effectively, as the detailed analysis and continuous monitoring required can be resource intensive. Tailored approaches may help mitigate these challenges. Additionally, there is a risk of over-reliance on these frameworks, which might lead to neglecting other crucial aspects of cybersecurity. It is

essential to maintain a balanced approach, incorporating insights from various sources and adapting to specific organizational contexts.

The future of cybersecurity frameworks like the MITRE ATT&CK Matrix and the NIST CSF is promising, with ongoing enhancements expected to improve their integration capabilities. Efforts to streamline the integration process will make it easier for organizations to implement both frameworks together, improving their accessibility and effectiveness. Both frameworks will continue to expand and update their content to address emerging threats, ensuring they remain relevant and effective. The MITRE ATT&CK Matrix will incorporate new TTPs, while the NIST CSF will update its guidelines to reflect the latest security practices and technologies. As these frameworks evolve, their adoption will become more widespread, driving further standardization and refinement of security practices across various sectors. Kwon et al. (2020) predicts that these frameworks will become standard practice in cybersecurity management, significantly enhancing organizational resilience against evolving threats.

Integrating AI and ML with the MITRE ATT&CK framework and NIST CSF represents a significant advancement in cybersecurity, enhancing threat detection and mitigation by leveraging advanced algorithms. However, this integration presents challenges, including complexity and resource demands, particularly for smaller organizations. The combination of detailed TTPs from the MITRE ATT&CK Matrix with the broader categories of the NIST CSF requires significant expertise and effort. Despite these challenges, the evolving nature of these frameworks promises improved accessibility and effectiveness, driving further standardization and nuance in cybersecurity practices.

While there are challenges and limitations to consider, the benefits of improved threat detection, comprehensive coverage, and continuous improvement make this integration highly valuable. Organizations that effectively integrate these frameworks will be better equipped to anticipate, respond to, and recover from cyberthreats. This proactive approach not only enhances security but also builds trust with stakeholders, demonstrating a commitment to safeguarding critical assets and information. As these frameworks evolve, their role in shaping resilient and adaptive cybersecurity strategies will become even more pivotal, helping organizations stay ahead of the ever-changing threat landscape.

References

Ajmal, A., Shah, M., Maple, C., Asghar, M., & Islam, S. (2021). Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. *IEEE Access*, 9, 126023–126033. https://doi.org/10.1109/ACCESS.2021.3104260

Alexander, O., Belisle, M., & Steele, J. (2020). *MITRE ATT&CK® for industrial control systems: Design and philosophy*. MITRE. Retrieved January 20, 2023, from https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf

Bautista, E.C.R., & Parada, H.D.J. (2021). Guide of principles and good practices for software security testing in web applications for a private sector company. *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, 1-7. https://doi.org/10.1109/CONIITI53815.2021.9619664

Exec. Order No. 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 12, 2021).

Elm, F., & Eckenrode, J. (2023). Cyber risk and cybersecurity: A systematic review of data availability. *Journal of Cybersecurity*, *12*(1). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267

Gonzales, Sergio (2022). *Cyber Frameworks Small Business Application*. Electronic Theses, Projects, and Dissertations. 1500. https://scholarworks.lib.csusb.edu/etd/1500

Hwang, C.-W., Bae, S.-H., & Lee, T.-J. (2021, September 30). MITRE ATT&CK and Anomaly detection based on abnormal attack detection technology research. *Journal of Information and Security. Korea Convergence Security Association*. https://doi.org/10.33778/kcsa.2021.21.3.013

INTERPOL. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. INTERPOL. Retrieved October 20, 2023, from https://www.interpol.int/en/News-andEvents/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Karabacak, B., & Whittaker, T. (2022, March). Zero trust and advanced persistent threats: Who will win the war?. *Proceedings of the 17th International Conference on Cyber Warfare and Security*, USA, 17(1), 92-101. https://doi.org/10.34190/iccws.17.1.10

Kern, M., Skopik, F., Landauer, M., & Weippl, E. (2022). Strategic selection of data sources for cyberattack detection in enterprise networks: a survey and approach. *In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing (SAC '22)*. Association for Computing Machinery, New York, NY, USA, 1656–1665. https://doi.org/10.1145/3477314.3507022

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gupta Gourisetti, S. N. (2020). Cyber threat dictionary using MITRE ATT&CK Matrix and NIST Cybersecurity Framework mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE. https://doi.org/10.1109/RWS50334.2020.9241271

Mashima, D. (2022). MITRE ATT&CK based evaluation on in-network deception technology for modernized electrical substation systems. Sustainability, 14(3), 1256. https://doi.org/10.3390/su14031256

MITRE ATT&CK. Retrieved January 23, 2024, from https://attack.mitre.org/techniques/enterprise/

MITRE ATT&CK Navigator, Retrieved January 23, 2024, from https://mitre-attack.github.io/attack-navigator/

MITRE ATT&CK. SolarWinds Compromise. Retrieved September 7, 2023, from https://attack.mitre.org/campaigns/C0024/

Mukkamala S, Janoski G, Sung A. (2002). Intrusion detection using neural networks and support vector machines. *Proceedings of the 2002 International Joint Conference on Neural Networks*, IJCNN'02 (Cat. No. 02CH37290). Honolulu, HI, USA. 2, 1702-1707.

Pérez-Sánchez A., & Palacios R. (2022). Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences*, 12(3),1076 -https://doi.org/10.3390/app12031076

Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., & Loukas, G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. arXiv. https://doi.org/10.48550/arXiv.2304.07411

Shin, Y., Kim, K., Lee J.J., & Lee, K. (2022). Focusing on the weakest link: A similarity analysis on phishing campaigns based on the ATT&CK matrix. *Security & Communication Networks*, 1-12. doi:10.1155/2022/1699657

The White House. (2024). *Federal cybersecurity R&D strategic plan 2023*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

Turton, W. and Mehrotra, K. (2021, June 4). Hackers breached Colonial Pipeline using compromised password. *Bloomberg*. Retrieved December 15, 2022, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Williams, D. (2020). The MITRE ATT&CK Framework: Where do you start? *ISSA Journal*, *18(*9), 17-21.

Xiong, W., Legrand, E., Åberg, O., & Lagerstrom, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*. https://doi.org/10.1007/s10270-021-00898-7