Journal of Emerging Technologies and Industrial Applications
Vol. 3 No. 1 (2024) pp. 1-7
e-ISSN: 2948-507X

Journal homepage: https://jetia.mbot.org.my/index.php/jetia/index

Effective SOC Response Strategies Using MITRE ATT&CK

Muhammad Irsyad Abdullah*[1], Aiman Ilyasa Abas[2,] Asif Iqbal Hajamydeen[3]

[1]Muhammad Irsyad Abdullah,
Centre of Cyber Security and Big Data Management & Sciences University, University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA

[2]Aiman Ilyasa Abas,
Faculty of Information Science and Engineering Management & Science University, University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA

[3]Asif Iqbal Hajamydeen
Centre of Cyber Security and Big Data Management & Science University, University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA

Email: [a]irsyad@msu.edu.my, [b]aimanilyasaabas@outlook.com, [c]asif@msu.edu.my

Abstract: In today's rapidly evolving cybersecurity landscape, the protection of critical digital assets demands proactive and robust response strategies. This paper introduces an investigation into achieving operational excellence in cybersecurity through the strategic integration of the MITRE ATT&CK framework within Security Operations Centres (SOCs). By leveraging the MITRE ATT&CK framework's comprehensive taxonomy of tactics, techniques, and procedures utilized by threat actors, this paper delves into the design and implementation of highly effective SOC response strategies. The paper presents real-world insights, practical applications, and case studies, shedding light on the transformative potential of fusing the MITRE ATT&CK framework with SOC operations. The findings underscore the importance of adaptive cybersecurity practices that not only detect threats but also enable swift and accurate responses for enhanced operational readiness.

Received 20 February 2024; Accepted 15 May 2024; Available online 26 June 2024

Keywords: Cybersecurity, MITRE ATT&CK framework, Security Operations Centre, threat detection, response strategies, operational excellence.

*Corresponding Author:

Muhammad Irsyad Abdullah,
Centre of Cyber Security and Big Data,
Management & Science University,
University Drive, Off Persiaran Olahraga, Shah Alam, 40100, MALAYSIA
Email : irsyad@msu.edu.my

1. Introduction

In the face of ever-evolving cyber threats, organizations are pressed to enhance their cybersecurity strategies to effectively safeguard critical assets. The MITRE ATT&CK framework, renowned for its detailed depiction of adversary behaviours, presents an invaluable tool for comprehending and countering cyber threats. However, operationalizing this framework within Security Operations Centres (SOCs) remains a critical challenge. This paper aims to bridge this gap by exploring how integrating the MITRE ATT&CK framework into SOC practices can lead to operational excellence. By aligning detection and response strategies with the ATT&CK framework's insights, SOC teams can elevate their abilities to detect and mitigate complex threats.

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that catalogues the tactics, techniques, and procedures (TTPs) commonly used by cyber adversaries during different stages of an attack. It provides a structured and detailed understanding of how cyber threats operate, making it a powerful resource for improving cybersecurity defence strategies.

In the context of security operations, the MITRE ATT&CK framework is highly relevant due to its ability to:

The ATT&CK framework significantly enhances cybersecurity capabilities in several key areas. First, it offers a comprehensive taxonomy of attack techniques, providing security teams with a profound understanding of adversary tactics, which is essential for more accurate threat detection [1]. Additionally, it aligns specific attack techniques with overarching tactics, a critical feature that aids security operations centre (SOC) teams in contextualizing threats, prioritizing alerts, and executing effective responses [2]. This alignment allows SOC teams to better structure incident response plans [3], leading to quicker and more effective mitigation, ultimately reducing the impact of cyber incidents [4].

Moreover, ATT&CK plays a pivotal role in the development of detection rules for various techniques [5]. These rules enable automated monitoring and real-time threat alerting, a key capability that empowers SOC analysts to catch threats as they occur [6]. By integrating with threat intelligence, ATT&CK enhances its value [7]. SOC teams can map threat actor behaviour to ATT&CK, resulting in more accurate and informed threat assessments [8].

Furthermore, ATT&CK fosters collaboration and communication across different cybersecurity teams and external partners by providing a common threat language [9]. This common language streamlines discussions about threats, ultimately improving the overall security posture of organizations [10]. ATT&CK remains agile and responsive to the evolving threat landscape [11]. New tactics and techniques are added over time, allowing SOC teams to stay current and adaptive in their defence strategies [12].

Lastly, ATT&CK aids in training security professionals [13]. By offering real-world scenarios and insights into attacker methodologies, it empowers analysts to better understand and respond to threats [14]. This educational aspect of ATT&CK contributes to building a skilled and vigilant cybersecurity workforce, a crucial element in defending against cyber threats [15].

In summary, the MITRE ATT&CK framework is a pivotal tool in the security operations landscape. It equips SOC teams with the knowledge needed to effectively detect, respond to, and mitigate cyber threats by providing a standardized and detailed understanding of adversary tactics and techniques. By incorporating ATT&CK into their strategies, organizations can bolster their security posture and enhance their overall cybersecurity resilience.

1.2 Tables

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base and framework that describes the actions and techniques that adversaries commonly use during different stages of a cyber-attack. The framework is organized into several categories, with "Tactics" being one of them. Tactics represent the high-level objectives that attackers aim to achieve. Each tactic consists of various "Techniques" that detail the specific methods used to accomplish the tactic's objective.

Table 1: Here's a table explaining each tactic in the MITRE ATT&CK framework.

Tactics	Attacker(s) Objective
Initial Access	Gain an initial foothold in the target environment.
Execution	Run malicious code or command on a victim's system.
Persistence	Maintain control over a compromised system for long-term access.
Privilege Escalation	Gain higher levels of access and control on a compromised system.
Defense Evasion	Avoid detection by security mechanisms.
Credential Access	Steal user or system credentials.
Discovery	Collect information about the target environment.
Lateral Movement	Move laterally within a network to access additional system.
Collection	Gather data of interest from compromised system.

Exfiltration	Steal and transfer data from the victim's environment.
Impact	Disrupt, alter, or destroy system, data, or operations of the target.
Resource Development	Established resources they can use to support operations.
Command and Control	Communicate with compromised system to control them.
Reconnaissance	Gather information they can use to plan future operations.

2 Related Work

Previous paper efforts have investigated the efficacy of the MITRE ATT&CK framework in various contexts, including threat modelling, red teaming, and vulnerability assessment. However, limited research exists on its direct application within SOC operations. This paper builds upon prior work by delving into the specific methodologies that enable SOC teams to extract maximum value from the ATT&CK framework. It also considers the nuances of real-world scenarios, showcasing how this integration can be implemented seamlessly to achieve operational excellence.

The field of cybersecurity has witnessed significant developments in recent years, driven by the growing sophistication of cyber threats and the need for more effective strategies to defend against them. This section reviews relevant literature and paper efforts that have contributed to the understanding and application of MITRE ATT&CK for enhancing Security Operations Centre (SOC) response strategies.

The MITRE ATT&CK Framework, standing as a cornerstone in the realm of cybersecurity, has evolved into a fundamental system for comprehending adversary tactics and behaviours. It offers a comprehensive taxonomy that classifies cyber threat tactics and techniques. This taxonomy serves as a guiding beacon for Security Operations Centre (SOC) analysts, allowing them to align their response strategies with a deep understanding of known adversary behaviours.

Numerous studies have delved into the integration of the MITRE ATT&CK framework into SOC response strategies. These studies have highlighted how this integration significantly augments threat detection and bolsters response capabilities. Additionally, investigations have been conducted into the application of cutting-edge machine learning techniques to automate SOC response actions. This development not only showcases the potential for heightened efficiency and effectiveness in responding to cyber threats but also underscores the adaptability of the framework in a rapidly evolving threat landscape.

Furthermore, it is essential to emphasize the paramount importance of timely and accurate Cyber Threat Intelligence (CTI) in orchestrating an effective SOC response. Discussions have revolved around the significance of integrating the MITRE ATT&CK framework into CTI practices. Such integration provides SOC teams with a rich contextual understanding of adversary tactics and techniques. Armed with this intelligence, SOC teams are empowered to craft more informed, proactive, and ultimately effective threat responses.

In tandem with these developments, researchers have introduced frameworks and methodologies aimed at enhancing SOC capabilities. One notable example is the introduction of a SOC maturity model that seamlessly incorporates the MITRE ATT&CK framework. This model offers a structured and systematic approach for organizations to evaluate their current security posture and, subsequently, to develop targeted and robust response strategies. Such frameworks demonstrate the ongoing evolution of cybersecurity practices, aligning them with the dynamic threat landscape.

Lastly, real-world case studies have provided concrete evidence of the practical application of the MITRE ATT&CK framework within SOC response scenarios. These case studies illustrate how the framework has played pivotal roles in mitigating significant security incidents and, concurrently, in elevating the overall effectiveness of response efforts.

In conclusion, the MITRE ATT&CK Framework stands as a linchpin in the cybersecurity domain, facilitating comprehensive threat understanding, response enhancement, and the integration of cutting-edge technologies. Its role extends far beyond a mere reference guide, serving as a dynamic tool that adapts and evolves with the ever-changing threat landscape, ultimately fortifying organizations against cyber adversaries.

2.2 Background

In 2013, the MITRE ATT&CK framework was initiated to record and organize the methods used by attackers after breaching computer systems, with a focus on Microsoft Windows systems. Its goal was to enhance the ability to detect malicious actions [4,7]. Over time, ATT&CK expanded its scope to include a wider range of platforms and technologies, becoming a comprehensive knowledge source that documents cyber attackers' behaviour throughout their operations. It now serves as a guide for simulating adversary actions and identifying areas for analysis and defence improvement within targeted networks [6]. ATT&CK consists of several core components:

- **Tactics**: These represent the broader goals of adversaries during an attack, providing context by categorizing individual techniques into higher-level categories, such as data theft, privilege escalation, and evasion [5,6].
- **Techniques**: These describe how adversaries achieve tactical goals through specific actions,

addressing the "how" and sometimes the "what" gained from those actions [4,6].

- **Sub-techniques**: These offer more detailed methods for accomplishing tactical objectives, operating at a granular level compared to techniques [6,8].
- **Procedures**: These describe the specific ways in which adversaries apply techniques or sub-techniques, providing practical instances of their execution and potential additional behaviours [4,7].
- **Mitigations**: These specify defensive measures that can prevent adversaries from successfully executing their tactics with specific techniques, guiding responses to TTPs (Tactics, Techniques, and Procedures) [5].

ATT&CK has gained widespread adoption across various sectors, including government organizations, finance, healthcare, retail, and technology, thanks to active participation from the cybersecurity community [6]. It consists of three main models:
ATT&CK for Enterprise: Originally focused on Windows systems, it now includes Mac and Linux operating systems. The latest version, released in October 2020, encompasses 14 enterprise tactics, 177 techniques, 348 sub-techniques, and 42 mitigations.
ATT&CK for Mobile: Introduced in 2017, it focuses on mobile device threats, particularly on Android and iOS platforms. The October 2020 version includes 14 tactics, 86 techniques, and 13 mitigations.
ATT&CK for ICS: Released in January 2020, this model addresses cyber threats to Industrial Control Systems (ICS). It covers 11 tactics, 81 techniques, and 50 mitigations, aiming to understand adversary actions within ICS networks.
Recognizing the interconnected nature of cyber threats to IT and ICS networks, efforts have been made to combine the ATT&CK for ICS and Enterprise models. Mandiant Threat Intelligence, in collaboration with MITRE, initiated an integration project in late 2020 to improve communication of adversary behaviour across OT networks and address complex cybersecurity challenges [11].

2.3 The Cyber-Security Culture Framework

The Cyber-Security Culture Framework, introduced in 2020 [11], provides a technique for analyzing and measuring people's and organizations' security culture readiness. It is based on a thorough examination of organizational and individual security concerns, which are organized into dimensions and domains as shown in Figure 1. These parts are generated from detailed reviews of the literature and research analyses of the present cyber-security scene.

The framework was initially intended to assess not only organizational security architecture, policies, and procedures, but also individual employee characteristics, behaviours, attitudes, and abilities. This holistic approach bridges the gap between the professional and scientific perspectives, considering both external and internal indicators related to cyber-security culture. Moreover, it addresses the complex interactions among these security facets within the intricate fabric of modern businesses.

Figure 1 shows the proposed framework's classification of security culture indicators into two tiers: organizational and individual. The first level includes six dimensions.

- Assets
- Continuity
- Access and Trust
- Operations
- Boundary Defence
- Security Governance

Each dimension corresponds to a specific security problem that organisations must handle through a combination of IT solutions and security measures. In turn, the second level breaks down into four dimensions:

- Attitude
- Awareness
- Behaviour
- Competence

The dimensions are further subdivided into domains, which examine different aspects of each security component. For example, the "Assets" dimension includes security rules that impose controls on an organization's assets (including personnel, infrastructure, machinery, systems, and information assets) in terms of confidentiality, availability, and integrity [11]. These controls are organized into various asset types and associated security management features by the domains within this dimension. As a result, domains within this dimension include "Hardware Assets Management" and "Hardware Configuration Management," "Network Infrastructure Management" and "Network Configuration Management," "Software Assets Management" and "Information Resources Management," and "Network Configuration Management," among others. Similarly, each security component inside this framework methodically displays an organization's specialised security application areas, down to quantitative indicators [11].
Each domain is associated with a set of metrics that may be examined and measured effectively using a variety of assessment approaches ranging from simple surveys and

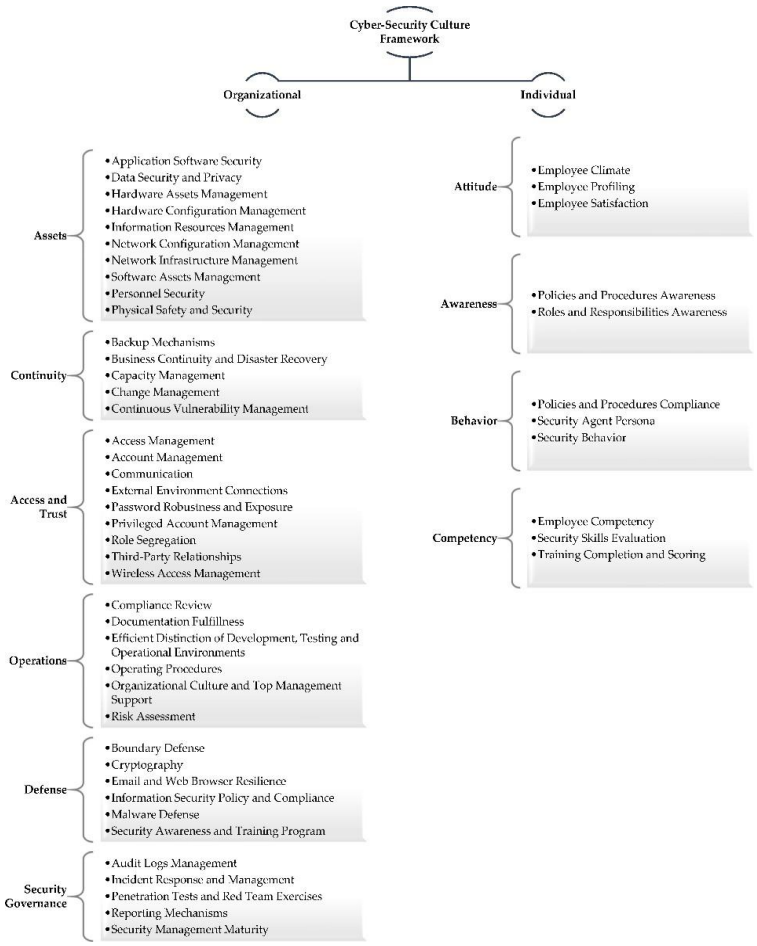

Figure 1. Cyber-Security Culture Framework.

The COVID-19 pandemic prompted a targeted survey to assess the cyber-security readiness of vital infrastructures [12]. This survey was meticulously constructed, calibrated, verified, and administered to collect relevant data [12]. The examination of this data highlighted the complexities and importance of evaluating the cyber-security culture within organizations [14].

The assessment results provide valuable insights to decision-makers, enhancing the organization's security culture and

identifying potential cyber-security risks to the business ecosystem. Adversary behaviour and threats vary based on their source, whether internal or external. The framework has been used to identify potential insider threats [4]. This paper focuses on assessing the risks associated with ATT&CK TTPs (Tactics, Techniques, and Procedures) by evaluating the presence and utilization of recommended mitigation techniques from MITRE ATT&CK [11]. By analysing the effectiveness of these techniques, we aim to understand the risks associated with ATT&CK TTPs and develop mitigation strategies. [11][12][13][14]

3 Methodology

The paper methodology encompasses a multi-phased approach. Firstly, an in-depth analysis of the MITRE ATT&CK framework is conducted to identify relevant tactics, techniques, and procedures (TTPs) for modern cyber threats [7,8]. This initial phase involves an exhaustive review of the MITRE ATT&CK framework, considering its continuous updates and revisions to ensure the most current threat intelligence is incorporated into the analysis. Subsequently, the paper delves into the adaptation of SOC processes to align with the framework's insights. The existing SOC procedures and workflows within the organization are rigorously assessed and compared against the MITRE ATT&CK framework's recommended best practices [7,8]. This phase involves collaboration with SOC teams, cyber threat analysts, and incident responders to seamlessly integrate MITRE ATT&CK-informed strategies into day-to-day operations.

The paper goes beyond theory by presenting real-world case studies [3,4]. These case studies demonstrate how integrating MITRE ATT&CK enhances SOC response strategies in actual threat scenarios. They provide concrete examples of how the framework's tactics and techniques mapping, along with timely and precise responses, minimize potential damage and loss. Through meticulous analysis, key takeaways are revealed, including improved detection rates, reduced incident resolution times, and more effective mitigation of cyber threats [3-5]. These practical demonstrations of the paper findings offer actionable insights for SOC practitioners.

In the ever-changing field of cybersecurity, it is crucial for Security Operations Centers (SOCs) to understand adversary tactics and techniques in order to develop effective response strategies. The MITRE ATT&CK framework serves as a valuable resource for comprehending adversary behavior and enhancing SOC capabilities. This section provides a curated list of pertinent MITRE ATT&CK techniques, including their title, unique ID, and their use or purpose in cyberattacks.

Table 2: MITRE ATT&CK Techniques

Techniques	ID	Use
Phishing: Spear phishing Attachment	T1566.001	Deploying malware via malicious email attachments.
Phishing: Spear phishing Link	T1566.002	Delivering malware through malicious links in phishing emails.
Scheduled Task/Job: Scheduled Task	T1053.005	Creating scheduled tasks for persistence.
Command and Scripting Interpreter: Windows Command	T1059.003	Using Excel macros to download and deploy malware.

Command and Scripting Interpreter: JavaScript/JScript	T1059.007	Using malicious JavaScript files to communicate with C2 servers and download malware.
Native API	T1106	Managing execution flow using Windows API calls (CreateProcessW()).
User Execution: Malicious Link	T1204.001	Sending spearphishing emails to entice users to click on malicious links.
User Execution: Malicious File	T1204.002	Encouraging users to launch malicious documents to deliver malware.
Create or Modify System Process: Windows Service	T1543.003	Establishing persistence through AutoStart services.

4 Consideration And Limitation.

The cyber-security culture framework was designed to be universally applicable, suitable for organizations of all sizes, types, industries, technological levels, and security preparedness [12]. Its adaptation to the Electric Power and Energy Systems (EPES) sector involved enhancing controls and security indicators tailored to the power supply chain's operational lifecycle.

In contrast, MITRE ATT&CK is a comprehensive categorization of offensive operations used by adversaries against specific platforms [7]. It focuses on how attackers interact with systems during attacks, providing specialized data. Security specialists must evaluate and analyze the framework's recommended Tactics, Techniques, and Procedures (TTPs), considering insights from the MITRE ATT&CK knowledge base.

Adversary behavior constantly adapts to economic, societal, political, and technological aspects, exploiting vulnerabilities in digital infrastructures and human operations. Therefore, information security must evolve alongside these changes. The MITRE ATT&CK knowledge base and the cyber-security culture framework are dynamic systems that mature and adapt to the evolving cybercrime landscape [17]. Consequently, the efforts described in this article require regular revision and improvement to effectively connect these two evolving models.

4.1 Consideration

In this subsection, several critical considerations arise when using MITRE ATT&CK for SOC response strategies. Firstly, it's important to acknowledge the variability of adversary behaviour in real-world instances. This highlights the need to address threat actor adaptability and the ever-evolving landscape of cyber threats when implementing ATT&CK-based strategies (1). Secondly, specialized training for SOC analysts is crucial, emphasizing the importance of skill development and resource allocation for training (2). Additionally, finding the right balance in resource allocation, including time and personnel, is essential to effectively implement and sustain ATT&CK-based strategies while managing other SOC responsibilities (3). Moreover, exploring the integration of MITRE ATT&CK with existing security tools and technologies is imperative, requiring discussions on potential integration challenges and viable solutions (4). Lastly, integrating threat intelligence sources with MITRE ATT&CK data is significant, as it enhances the contextual understanding of adversary behaviour and strengthens the effectiveness of SOC response strategies (5). These considerations together create a comprehensive framework for successfully utilizing MITRE ATT&CK in SOC responses.

4.2 Limitations

This subsection explores the limitations and challenges of integrating MITRE ATT&CK into SOC response strategies. Firstly, it's important to recognize the evolving nature of MITRE ATT&CK and its incompleteness in capturing all adversary behaviours and emerging threats, leading to discussions about potential knowledge gaps [1]. Secondly, adopting ATT&CK-based detection strategies can increase false positives and alert fatigue, necessitating the exploration of mitigation strategies [2]. Additionally, the effectiveness of MITRE ATT&CK can vary based on SOC maturity and available resources, with smaller organizations facing distinct challenges compared to larger enterprises [3]. Privacy and compliance implications of using ATT&CK-based techniques, particularly in scenarios involving sensitive data or regulated industries, should be carefully examined [4]. Lastly, accurately attributing attacks to specific threat actors solely based on ATT&CK data is challenging, highlighting the attribution challenges within this framework [5]. These considerations emphasize the need for a nuanced approach to implementing MITRE ATT&CK in SOC response strategies, addressing these limitations and challenges [1][2][3][4][5].

4.3 Mitigation and Practice

In conclusion, this section suggests outlining potential mitigations for the identified limitations and discussing best practices to maximize the benefits of MITRE ATT&CK in SOC response strategies. This can involve ongoing research and initiatives within the cybersecurity community to continuously update and expand the framework. To address challenges such as false positives and alert fatigue, implementing advanced analytics, automation, and optimizing alert management processes can be effective. Tailoring the implementation of MITRE ATT&CK based on SOC maturity and available

resources, as well as considering privacy and compliance implications, are crucial. By providing practical guidance and highlighting collaborative efforts, organizations can navigate these limitations and leverage the full potential of MITRE ATT&CK in their SOC response strategies.

5 Conclusion

This paper highlights the significant impact of integrating the MITRE ATT&CK framework into Security Operations Centres (SOCs). By incorporating ATT&CK-based detection and response strategies, organizations can improve their operational excellence and reduce the time it takes to address threats. The findings emphasize the importance of proactively adapting to evolving threat landscapes and demonstrate the potential of the ATT&CK framework to provide SOC teams with the necessary insights for effective response actions. In today's digital world, where threats are becoming more sophisticated, the combination of MITRE ATT&CK and SOC operations is crucial for achieving cybersecurity operational excellence. This paper serves as evidence of the value of integrating the MITRE ATT&CK framework into SOC practices, leading to enhanced capabilities in detecting and mitigating cyber threats. To conclude, the fusion of MITRE ATT&CK with SOC operations not only improves the efficiency of threat detection and response but also strengthens organizations' resilience against the ever-growing digital threat landscape.

References

[1] What is the mitre ATT&CK framework? (no date) Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-mitreattack-framework (Accessed: 18 August 2023).

[2] M. Parmar and A. Domingo, “On the use of cyber threat intelligence (cti) in support of developing the commander’s understanding of the adversary,” in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019, pp. 1–6.

[3] Kwon, R.; Ashley, T.; Castleberry, J.; Mckenzie, P.; Gourisetti, S.N.G. Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 19– 23 October 2020.

[4] Cho, S.; Han, I.; Jeong, H.; Kim, J.; Koo, S.; Oh, H.; Park, M. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture. In Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, 11–12 June 2018

[5] Xiong, W.; Hacks, S. Threat Modeling and Attack Simulations for Enterprise and ICS. In Proceedings of the CS3STHLM,

[6] Security_Culture_Framework (Accessed: 24 August 2023).

[7] Georgiadou, A.; Mouzakitis, S.; Askounis, D. Detecting Insider Threat via a Cyber-Security Culture Framework. J. Comput. Inf. Syst. 2021. [Google Scholar] [CrossRef]

[8] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework,” Sensors, vol. 21, no. 9, p. 3267, May 2021, doi: 10.3390/s21093267.

[9] Avignon, France, 29 June–1 July 2020. [Google Scholar]

[10] Strom, B. “ATT&CK 101”, Medium. 2018. Available online: https://medium.com/mitre-attack/att-ck-101-17074d3bc62 (accessed on 3 January 2021).

[11] Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. MITRE ATT&CK®: Design and Philosophy; The MITRE Corporation: Bedford, MA, USA, 2018. [Google Scholar].

[12] Alkawaz, Mohammed Hazim, Stephanie Joanne Steven, Asif Iqbal Hajamydeen, and Rusyaizila Ramli. A Comprehensive Survey on Identification and Analysis of Phishing Website based on Machine Learning Methods. 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), pp. 82- 87. IEEE, 2021

[13] Alkawaz, Mohammed Hazim, Stephanie Joanne Steven, and Asif Iqbal Hajamydeen. 2020. Detecting Phishing Website Using Machine Learning. 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA). IEEE, 2020.

[14] Asif Iqbal Hajamydeen and Nur Izura Udzir. 2019. A Detailed Description on Unsupervised Heterogeneous Anomaly Based Intrusion Detection Framework. Scalable Computing: Practice and Experience, 20(1): 113-160

[15] Asif Iqbal Hajamydeen and Nur Izura Udzir. 2016. A Refined Filter for UHAD to Improve Anomaly Detection. Security and Communication Networks. John Wiley & Sons, 9(14), 2434 – 2447, DOI: 10.1002/sec.1514.

[16] Kamal, Ayesha, Asif Iqbal Hajamydeen, and Adam Amril Jaharadak. "Log Necropsy: Web-Based Log Analysis Tool." In 2022 IEEE 10th Conference on Systems, Process & Control (ICSPC), pp. 176-179. IEEE, 2022