A Proposed Framework for Mitigating Software Supply Chain Attacks in Defense Organizations

Mohamad Nur Hidayat Zarkia @ Zakaria[1], Ganthan Narayana Samy[2], Abdul Ghafar Jaafar[3] Mahiswaran Selvananthan[4] Nurazean Maarop[5] Sundresan Perumal[6]

[1,2,3,5]*Faculty of Artificial Intelligence, Universiti Teknologi Malaysia*

[4]*Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia*

[6]*Faculty of Science and Technology, Universiti Sains Islam Malaysia*

[1]*mohamadnurhidayat@graduate.utm.my,* [2]*ganthan.kl@utm.my* [3]*abdulghafar@utm.my,* [4]*mahiswaran@utm.my,* [5]*nurazean.kl@utm.my,* [6]*sundresan.p@usim.edu.my*

Article history

Received:
13 November 2025

Received in revised form:
20 November 2025

Accepted:
1 December 2025

Published online:
26 December 2025

*Corresponding author:
mohamadnurhidayat@graduate.utm.my

Abstract

A software supply chain attack is a cyber-attack where the attack targets the supply chain to damage the security of the software and the target environment. Therefore, this research addresses the critical issue of software supply chain attacks, which exploit vulnerabilities in third-party vendors, leading to third-party compromise and software dependencies posing significant risks to national security, operational capabilities, and organizational trust in Defense organizations. The key importance of this research lies in proposing a framework to mitigate software supply chain attacks for the Defense organization, a high-value entity in the defense sector. The research employs a literature review, later conducting qualitative methodology through semi-structured interviews, and thematic analysis. Data collection will involve engaging participants from academia, industry, and military personnel in cybersecurity domains. The security framework is constructed by integrating insights from military-specific policies, global frameworks, and legal aspects in a few countries, followed by participant opinion and expert validation to ensure its comprehensiveness and relevance. The expected findings include identifying key components and vulnerabilities influencing software supply chain attacks, proposing a tailored framework for the Defense organization, and evaluating the proposed framework. The originality of this research lies in its focus on the Defense organization, adapting and integrating elements from global frameworks and military-specific policies to address unique challenges in a defense context. The practical significance of this research extends to scholars, industry professionals, and Defense organizations. The proposed framework will serve as a strategic tool for the Defense organization to enhance cybersecurity resilience, streamline decision-making processes, and foster trust in third-party engagements.

Keywords: *Software Supply Chain, Software Supply Chain Attacks, Supply Chain Security, Security Framework, Defense Organization*

1. Introduction

The emergence of the digital landscape is characterized by deeply interconnected and interdependent systems, where the creation and deployment of software rely on a global network of developers, suppliers, artificial intelligence (AI) - generated

* *Corresponding author. mohamadnurhidayat@graduate.utm.my*

source code, and open-source components. Adversaries can use vulnerabilities in supply chain attacks by targeting software dependencies, which is one of the attacks that target the weakest link, focusing on the third party as a vendor (Kulikov et al., 2022). This software supply chain attack occurs when an adversary aims to target software development, integration, or distributed processes to compromise the system through a trusted environment by manipulating components. This attack is dangerous because the adversary will use this entry point to exploit the vulnerabilities and weaknesses of third-party software, firmware, and services in less secure entities. Their motivation is to cause single damage that will affect all the organizations at risk, operational disruptions, data theft, financial gain, reputational damage, and leverage the interconnected nature of modern supply chains to amplify the attack's impact. Recently, studies by Tan et al. (2024) and Куликов et al. (2022) underscore that security concerns and complexity in the supply chain have been happening for many years. In addition, Ishgair et al. (2024) mentioned it is also required to understand more about AI-generated software's impact on security, as in the US, about 92% of developers rely on AI-based software. The evolving threat landscape necessitates a robust, practical, and up-to-date framework that enables organizations to mitigate these risks effectively**.** According to Nakano et al. (2021), implementing a security framework that validates conformance to predefined requirements can enhance the trustworthiness of supply chains, as this approach involves correlating with validation results to ensure the integrity of the entire supply chain.

1.1 Research Background

In 2024, one of the incidents occurred where Maxis Berhad Malaysia claimed that the hacker group R00tk1t breached Maxis' infrastructure and threatened to expose sensitive customer data (Christopher Fam, 2024). According to Business Times by Bernama (2024), BlackBerry Ltd. has revealed that 79% of Malaysia's software supply chain was susceptible to cyberattacks. In 2024, Starbucks, one of the coffee shops, experienced significant operational disruption due to ransomware exploiting vulnerabilities through third-party software vendors, affecting the company worldwide (Davey Winder, 2024). Meanwhile, Nyonyoh (2025) emphasized that the previous incident related to the ASUS laptop was discovered in 2022 to have a pre-installed malicious backdoor in the ASUS Live Update Utility known as ShadowHammer. Subsequently, one of the cyber-attacks, on a managed service provider (MSP) called Kaseya Virtual System Administrator (VSA), a well-known software/remote monitoring and management (RMM) ("Computer Fraud and Security," 2021). Subsequently, one of the high-profile cases related to the attack on the software supply chain attacks targeting SolarWinds, which is a US IT management company (Martínez & Durán, 2021).

Based on a few significant incidents happened, we can see that the benefits from collaboration with third parties also introduce significant risk, especially software dependencies within supply chain processes and third-party compromise. The incident happen shows the vulnerability in supply change can be a primary challenges faced by Defense organization are due to a lack of visibility for security processes in a software supply chain, improper patch management, insufficient standardization, limited control mechanisms, difficulty of detection by Advance

Persistent Threat (APT) actors which can be concealed in a period of time, and the lack of tailored explicit frameworks to effectively mitigate cybersecurity risks inherent in software procurement and collaboration with local-international third-party vendors. With the advancement of technology and threats, the Defense organization was required to have its specific security framework to enhance the software supply chain security. The proposed security framework aims to simplify the procedural complexities and enhance the overall security effectiveness and improve visibility control, and resiliency in managing software dependency supply chain within Defense environments. The study presents a contribution on a novel approach, as it serves not as a strategic tool but can be a streamlining in complex decision making throughout the software lifecycle and foster a more secure relationship with third-party partners. Having this security framework will enable the organization to gain insight into implementing it in the future. This study aims to provide a clear understanding of the existence and emergence of threats, thereby ensuring the organization's cyber resilience. The security framework can provide significant findings, and the security framework can be implemented in the Defense environment due to the high level of security implementation. In addition, this research will assist scholars, industry, organizations, and researchers in producing a comprehensive and practical framework. The security framework will be more focused, precise, and concise in complying with the respective software supply chain attack. Researchers and scholars can clearly understand the proposed security framework to mitigate software supply chain attacks in a Defense organization, which requires filling the gap in the software supply chain security aspect in the industry.

2. Literature Review

The process in the software supply chain consists of a few processes, such as developing the software, maintaining a secure update, and securely distributing the software update to the user. The process includes stakeholders from the software developers, maintainers, and system administrators in the software application development environment. Fig. 1 illustrates the process flow in the software supply chain.

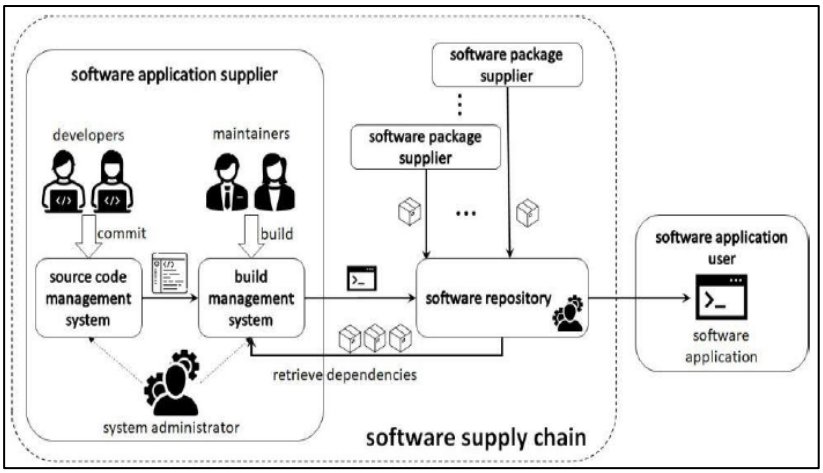

Figure 1. Software Supply Chain process (Source: Gokkaya et al., n.d.)

This software supply chain attack can also potentially occur when one of the third-party components or dependencies is compromised, caused by the adversary, which then impacts the entire software supply chain. There are two (2) types of supply chain attacks: direct attacks and indirect attacks. Direct attacks target specific nodes within the supply chain network, such as the software provider, retailer, or supplier. Dash et al. divide the indirect attack into two (2) types, which are:

a. One-Stage Risk Propagation attack is propagated from one node to another. For example, the attackers compromise software-building tools or update infrastructure.
b. Two-Stage Risk Propagation spreads further and affects additional nodes. For example, malware distribution through software updates within the trusted supply chain causes collateral damage to the whole ecosystem.

2.1. Taxonomy of Threats and Vulnerabilities

To construct an effective cyber defense, we must identify the adversary's methods and vulnerabilities that they can exploit. The STRIDE threat modeling methodology was developed by Microsoft, offers a useful lens through which to classify adversarial goals. Within the supply chain context, these threat models manifest in specific ways, as one of the tools that can be described as follows:

a. Spoofing: Adversaries propagated from one node to another. For example, steal code signing certificates or sign malicious applications from a trusted source (Khalil et al., 2024).
b. Tampering**:** Unauthorized modification of software artifacts. It included physical and data tampering attacks on ICT components (Syed et al., 2022).
c. Repudiation: Attackers attempt to conceal their actions. For example, the adversary deletes the log to hide unauthorized activity in modifying the security update (Khalil et al., 2024).
d. Information Disclosure: This is the unauthorized access to and exfiltration of sensitive data. Other threats include hidden backdoor channels, malware distribution to steal intellectual property or operational plans, and counterfeit products (Nygård & Katsikas, 2022). It can be achieved by exploiting vulnerabilities in the software supply chain.
e. Denial of Service: These attacks aim to make systems or services unavailable to legitimate users. The system is targeting to deny the availability of the system and services using ransomware and DDoS attacks (Syed et al., 2022; Hammi et al., 2023). In a software supply chain context, this could involve a ransomware attack on a critical third-party vendor, disrupting services essential for military operations, as seen in the disruption of management software at companies like Starbucks.
f. Elevation of Privileges: Attackers seek to gain higher-level permissions than they were initially granted. For example, unauthorized users are accessing the system and performing lateral movement without permission (Syed et al., 2022).

The vulnerabilities in the software supply chain exist when the software is not patched and users do not conduct security updates, and sometimes the vulnerability has not been identified yet (zero-day vulnerability). It is also known as flaws and bugs that are not addressed yet by system administrators. One of the vulnerabilities that is probably going to happen on the supplier side is that the supplier is part of a phishing attack or credential theft, resulting in massive data loss for a factory (Mullet et al., 2021). Sundararajan et al. (2022), also mention that vulnerability can exist within insider threats, man-in-the-middle attacks, malware, and unauthorized access through unnecessary applications or programs. In Australian Army logistics, vulnerabilities exist because of a lack of skilled risk practitioners in cyber vulnerabilities, centralized data and architecture vulnerabilities can affect single point of failure (SPOF), education and research lacking in supply chain expertise, limited data availability for detailed analysis and risk management, obsolete systems and challenges in patch management, and vulnerabilities in IT supply chains such as software lifecycle and supply chain design vulnerabilities (Br Benjamin Turnbull, 2018). There are also vulnerabilities that are listed in the Open Web Application Security Project (OWASP) Top 10 - Web Application (2021) and OWASP Mobile Top 10 (2023). Top 6: In the OWASP Top 10 - Web application vulnerability, the vulnerability can include vulnerable and outdated software components, as one of the Critical Weaknesses Exposure (CWE), which involves using unmaintained third-party components and being unsupported. Top 8: Software and data integrity failure, which describes a lack of verification on any platform and insecure Continuous Integration and Continuous Delivery /Deployment (CI/CD) pipelines. Top 9: Security logging and monitoring failures due to improper log configuration and insufficient logs. Meanwhile, in OWASP Mobile Top 10 - Mobile Application 2024, the Top 2 are: Inadequate supply chain security, including lack of security in third-party components, malicious insider threat, inadequate testing and validation, and lack of security awareness.

Common Vulnerabilities and Exposures (CVEs) also provide documentation on known software exploited by attackers, directly or indirectly, through dependencies embedded in the supply chain. The CVE database was funded by the USA Cybersecurity and Infrastructure Security Agency (CISA) and is maintained and managed by the MITRE organization. The example of CVE related to the software supply chain, CVE 2025-3066 exploits the CI/CD pipelines of GitHub platforms, CVE 2024-3094, the danger of open-source platforms using Backdoor XZ Utils, and CVE 2023-34362 MOVEit Data Transfer, which is vulnerable to SQL injection, leading to unauthorized access and data breaches.

As pointed out by Parker et al. (2023), a cyberattack on the supply chain can potentially remain undetected for a long time and persistently exploit your infrastructure. The adversary can access the data and network of the software supply chain, which makes them vulnerable, as well as makes you vulnerable. In addition, if there are unresolved vulnerabilities, the bad actors are most likely to exploit them, as it is part of the adversary's playground. Supply chain attack techniques, including implementing a hidden backdoor, social engineering, DoS/DDoS attack, malware insertion in internal development environment (IDE), exploit misconfiguration, and outdated software/firmware vulnerabilities, Open-Source Intelligence (OSINT),

tampering, and counterfeit software, can be used to exploit and cause offense within the software supply chain process.

MITRE ATT&CK Techniques describes how the adversary can implement the techniques of supply chain compromise, including sub-techniques such as compromising software dependencies and development tools. Adversaries may manipulate the environment, such as using tools, source files, and counterfeit products. In the first sub-technique, compromising software dependencies and development tools by manipulating them, usually targeting popular open-source tools that are used by specific victims and distributed to a broad set of consumers. Meanwhile, the second sub-technique compromises the software supply chain by manipulating the source code, updating the distribution mechanism, and replacing the compiled release version. Another sub-technique related to the compromised hardware supply chain is the intention to modify hardware or firmware in the supply chain. Adversaries may insert a hidden backdoor into consumer networks that may be difficult to detect, giving access with a high degree of control over the system. Hardware backdoors can also be inserted through endpoints, network infrastructure, and servers. The other techniques that are also used, such as a trusted relationship by compromising third-party accounts, can put the organization at risk. Besides that, hardware addition is conducted by adding unauthorized hardware during installation or transit by a third party, such as hardware keyloggers or malicious USB devices.

MITRE Supply Chain Attack Framework and Attack Patterns provide a comprehensive framework and catalog for understanding and mitigating supply chain attacks targeting hardware, software, firmware, and system information/data in the US Department of Defense (DoD) acquisition lifecycle. In this document, we are focusing on the software supply chain attack, which can occur through ICT infrastructure at all levels. Fig. 2 shows the supply chain process where the attack can occur at all levels of the supply chain, especially ICT (software production), through hardware, software, firmware, and system data/information.

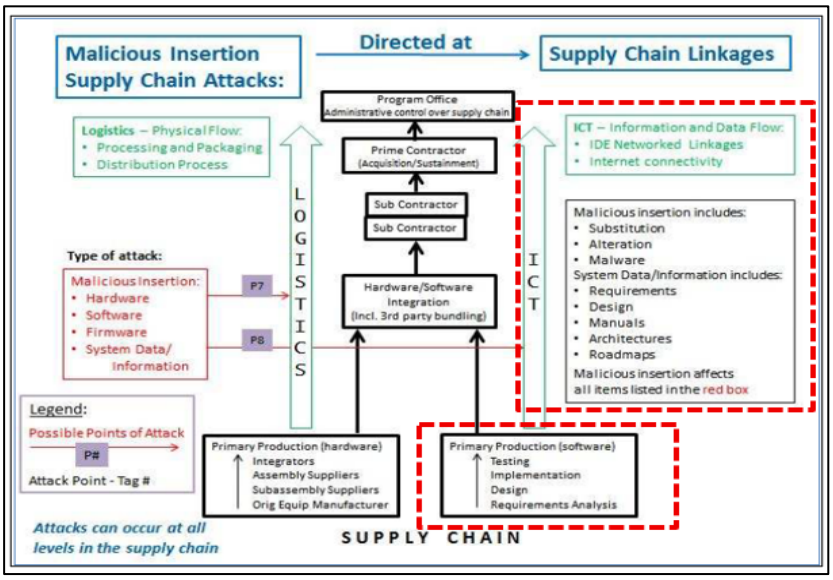

Figure 2. Points of Attack in Supply Chain (Source: Heinbockel et al., 2017)

2.2. Analysis of Lessons from Military and Civilian Incidents

The Earth Ammit cyber-espionage campaign (2023-2024) was reported by Ravie Lakshmanan, (2025b) a campaign specifically targeted at military, satellite, and drone manufacturing entities in Taiwan and South Korea. The attackers demonstrated sophisticated attack techniques in the supply chain, compromising Enterprise Resource Planning (ERP) software at an upstream software service provider to gain access to their ultimate targets. They then used trusted channels, such as remote monitoring and IT management tools, to deploy custom malware, exfiltrate data, and conduct espionage. This case highlights the adversary's willingness to execute multi-stage, patient attacks, infiltrating a softer commercial target to pivot into a hardened defense industry.

In 2024, the discovery of pre-installed malware on low-cost Chinese Android phones, which mimicked a popular model, illustrates how compromise can occur at the point of manufacture (Ravie Lakshmanan, 2025a). Malicious applications containing cryptocurrency-stealing functionality were embedded in the device firmware before it was ever sold to the consumer. Another incident which explored in an even kinetic example is the 2024 Hezbollah pager incident which the pagers were believed to be a secure communication medium and were allegedly tampered the software/firmware with during the manufacturing or distribution process, to include small explosive charges that could be remotely detonated (Sarah Shamim, 2024). This incident demonstrates the extreme form of supply chain compromise, where the integrity of a physical device is subverted to produce a direct physical effect, blurring the line between cyber and conventional warfare.

According to Hacker News, reported by Ravie Lakshmanan (2021), one of the significant supply chain attacks related to the SolarWinds attack took place, where malicious code was injected into Orion software updates. An estimated eighteen thousand (18,000) customers, including various US federal agencies and Fortune, and five hundred (500) companies, were affected by this attack that distributed backdoors called SUNBURST or Solorigate. They prove that the software and hardware supply chain attack surface is not theoretical, but it is an active and contested domain. The threat had affected the entire product lifecycle, from initial design and manufacturing (firmware backdoors), through development (code repository compromise), to post-deployment maintenance (hijacked updates). Therefore, effective defense cannot be a single-point solution but must come with a comprehensive strategy that addresses security at every stage.

2.3. Related Work

In this section, there are a few frameworks that are considered for developing a framework for mitigating software supply chain attacks in a Defense organization. Defense Federal Acquisitions and Regulations Supplement (DFARS) Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting is a mandatory contractual requirement imposed by the US DoD contractors, subcontractors, and other third parties who handle Covered Defense Information (CDI) or Controlled Unclassified Information (CUI). This requirement is part of the Federal Acquisition Regulations System (FARS), which is one of the policies implemented in information security. The focus related to the supply chain

includes cyber incident management and data handling to safeguard data related to CDI and CUI.

The Cybersecurity Maturity Model Certification (CMMC) framework was developed by the CMMC (2024) is to secure its US Defense Industrial Base (DIB). It is developed based on the DFARS 252.204-7012, FAR Clause 52.204-21, and NIST 800-171 controls to recommend the security approach (CMMC, 2021). It consists of three (3) layers (pass from the first layer to the third layer) that are required to be implemented by the US DoD supplier.

UK Ministry of Defense - Defense Standard 05-138 Cybersecurity for Defense Suppliers, established by the Defense Cyber Protection Partnership (DCPP), is a joint entity between the MoD and industry formed as part of a forum to improve the protection of the supply chain from cyber threats. This document acts as a defense standard that defines the MoD requirement with the Cyber Security Model under the risk assessment that generates a Cyber Risk Profile (CRP) (DefStan, 2024).

NIST Special Publication (NIST 800-161r1) for Cyber Supply Chain Risk Management (C-SCRM) through this publication is a multidisciplinary approach by Boyens (2024) to managing cyber risks in the product and supply chain services. The enterprise should foster an overall culture of security that includes C-SCRM as an integral part of the whole security framework. C-SCRM involves supply chain stakeholders and interactions, which are crucial for mitigating risk in a complex ecosystem (Nygård & Katsikas, 2022). Craiger et al. (2021) also, adopt this framework in the Special Operations Forces (SOF) for DoD, USA. NIST introduced C-SCRM and continued research and publication efforts on best practices. By having this practice, the National Defense Authorization Act authorizes the Secretary of Defense, including the Army, Navy, and Air Force, to exclude vendors of their product if they pose a supply chain risk that is unacceptable (Hammi et al., 2023).

NIST Special Publication for Defending against Software Supply Chain Attacks was published by CISA, is a document that provides practical guidelines and standards for managing supply chain risk. The document highlights key attack techniques, including hijacking updates, undermining code signing, software vulnerability, frequent updates leading to vulnerability, and compromising source code. The document required the organization to implement C-SCRM and NIST Special Publication for Secure Software Development Framework (SSDF) (NIST 800-218). In this document, it is highlighted that the organization can have access to evaluate and communicate with vendors, configure the software based on the vendor instructions and document vulnerability management program, register software license, harden existing infrastructure, remove unauthorized software monitoring, and have network segmentation to isolate from the enterprise

ISO 27001 Information Security Management System (ISMS) is a systematic framework to manage and protect sensitive information through policies, processes, and controls (ISO, 2022). ISMS aims to ensure the confidentiality, integrity, and availability of information assets across an organization. Application of ISMS in supply chain security can be applicable in implementing risk analysis, Service Level Agreement (SLA) implementation, contract management, governance, extending to

procurement, Software Development Lifecycle (SDLC) practices, and requiring integration of suppliers into incident response and notification procedures.

C2-Eye: Framework for Detecting Command and Control (C2) connection of supply chain attacks, as a supply chain attack exploits trusted software mechanisms to distribute malware, making detection challenging. This framework detects the supply chain attack over the threat intelligence capability. C2-Eye addresses this by correlating host-based behavioral indicators with network activity, DNS metadata, semantic analysis, and real-time threat intelligence to identify malicious DNS queries and potential data exfiltration.

AsTRA Model by Ishgair et al. (2024) proposed framework that is utilized for representing software supply chain management and its causal relationships to identify security objectives and security techniques that are required to mitigate software supply chain attacks. The model recommended the approach, such as preventative and detection approaches. The methodology consists of defending principals, defending software artifacts, defending resources, defending steps, and defending supply chain topology.

Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) Software Supply Chain Security Framework, prepared by OIC-Cert (2024), initiates a framework that provides guidelines for securing software supply chains in the digital era. It addresses challenges posed by the complexity of modern software systems, globalization, and the increasing reliance on open source and third-party components. The framework is intended for regulatory authorities of member countries to assist in policy formulation for manufacturers and service providers.

In Malaysia, under the Malaysia Cyber Security Law Act, any cybersecurity incident notification must be reported to the government with a detailed report, such as the authorized person who reported, the NCII affected, and a comprehensive description within six (6) hours. After the incident, NCII needs to provide additional information within fourteen (14) days of the initial incident report. In the supply chain aspect cybersecurity third-party provider is required to have a license and report every incident promptly. Another cybersecurity act studied by Ludvigsen et al. (2022) and OIC-Cert (2024), such as the European Union (EU), Denmark, the United Kingdom (UK), and Ireland, implemented the Network and Information System (NIS) (Directive 2016/1148), which sets broad security requirements. As the EU, Denmark, and the UK are quite strict in enforcement with fines and potential for company closure as key measures. EU Act requires cybersecurity to be integrated into the design and development of products with digital elements. The AI Act mandates risk management and governance activities for high-risk AI systems. While Ireland focuses on the fines and investigation, it is more on compliance and administrative measures rather than forceful closures or criminal sanctions. In addition, the Canadian Act implements the Canadian Center for Cyber Security (CCCS) principles for "Security by Design and Default," highlighting secure software development practices. Based on the law and act highlighted, we can consider that the requirements vary by country, where best practices in the security domain can be applied, as they will help researchers gain a comprehensive understanding of developing the framework.

3. Methodology

The study utilizes a qualitative approach to validate an initial proposed framework derived from a literature review. Data will be collected through semi-structured interviews using a purposive sampling strategy with participants from academia, industry, and the military. The number of participants will be determined by data saturation. Data analysis will involve thematic and coding analysis using NVivo software. Finally, the proposed framework will be further evaluated by two (2) to three (3) experts for its practicality and comprehensiveness.

4. Proposed Framework

It is built upon a set of three (3) foundational principles and structured into five (5) interconnected domains that cover the entire security governance and software in the Defense organization. Fig. 3 shows the proposed framework for this study:

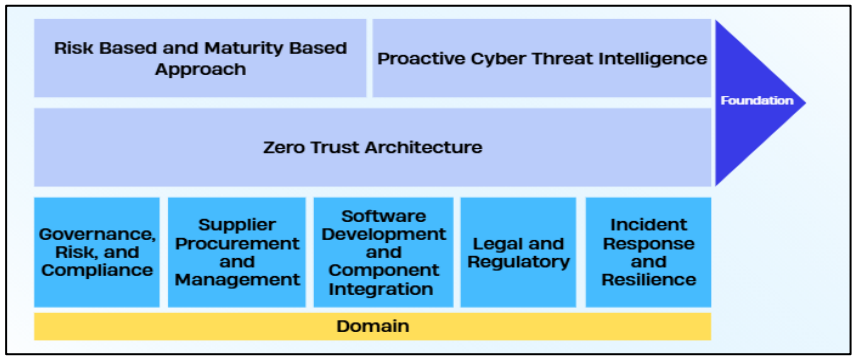

Figure 3. Proposed Framework to Mitigate Software Supply Chain Attacks

The first foundation principle describes risk-based and maturity approaches that are adopted from the maturity level concept from the NIST C-SCRM, CMMC, and risk profiling approach, taking from the UK Defense Standard, which software and suppliers will be classified based on risk to determine the required level of security. Secondly, Proactive Threat Intelligence is a second foundation principle required as intelligence is required to enhance the future visibility of the threat. The platform can use cyber threat intelligence (CTI) and threat detection in an organization by improving the detection and collaborating threat feeds from various sources, supply chain sources, and using ML. The component of the C2-Eye framework can be adapted and adopted, as it can enhance threat detection capability. In addition, according to CMMC (2024) The third foundation principle emphasizes the Zero Trust Architecture by using the principle "Never trust, always verify" principle, where the user or supplier should verify in all stages. This framework can be in line with the SolarWinds incident, where the attack comes from a trusted update and persists inside the environment.

Domain One (1) focuses on Governance, Risk, and Compliance; established strategic leadership and policies are required to manage this type of attack. Risk and asset management are important to classify the asset information, especially the classification data and personally identifiable information (PII). In these stages,

Cyber Risk Profiles can be implemented for suppliers and projects like the NIST C-SCRM and UK MoD Defense Standard Cybersecurity for Defense Suppliers. As people and processes are the most critical in the organization, awareness programs should be organized regularly for the stakeholders, such as procurement and technical staff. Subsequently, the second domain is the supplier procurement and management domain, which can be described by looking into existing procurement requirements and maintenance processes. The supplier and dependencies must be continuously audited and monitored by the Defense organization when required to improve the visibility within the supply chain. Contractual documents required the customer to fulfill such ISO 27001:2022 and other related security requirements. Next, Domain Three (3), which explained Software Development and Component Integration, emphasized secure software development, transparency, and verification from the SBOM provided by the supplier. In another component security aspect, such as Open-Source Software Management, they should be implemented in a safe and trusted platform. Legal and regulatory is also part of the proposed framework under Domain Four (4) needs to ensure the user and supply chain fulfill the national compliance requirements and follow international standards. Enforcement can be done by having clear legal and contractual penalties for supplier non-compliance and strong enforcement models that can be seen in other international laws. Lastly, in the incident response and resilience domain are important in detection and reporting using advanced detection tools. DFARS also emphasizes the strict incident response for the US DoD supply chain, forensics investigation, recovery, and resilience to ensure operation during and after attacks. It can be achieved by monitoring and conducting regular security assessments and vulnerability management to ensure system and information integrity.

5. Future Direction

Data collection and analysis through a qualitative approach will be conducted to ensure all the framework components are validated, considering that it has a proposed comprehensive framework. This proposed framework can also be adapted and adopted to other NCII sectors tailored to a unique operational environment, such as energy, finance, or telecommunication. By pursuing these studies, the academic and defense community can continue to advance the state of the art in software supply chain security, ensure that the organization remains resilient and secure against cyber threats.

6. Conclusion

The software supply chain attack has exposed critical vulnerabilities to most organizations. As national security is the main concern, a comprehensive framework is required to protect Defense organizations that rely on the globalized and complex ecosystem of software suppliers. This article presents a novel framework for mitigating software supply chain attacks in a Defense organization. It's originally taken from many aspects, adapting and integrating a global framework, legal aspect, and military-specific policies to address unique challenges and to ensure security assurance.

Acknowledgement

The authors acknowledge Universiti Teknologi Malaysia (UTM), Kuala Lumpur campus, for providing guidance, support, and facilities to complete this paper.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

References

[1] Bernama. (2024, August 13). 79% of Malaysian companies have been cyber-attacked over the last 12 months - Survey. Business Times.

[2] Boyens, J. M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[3] Br Benjamin Turnbull. (2018). Cyber-Resilient Supply Chains - Mission Assurance in the Future Operating Environment.

[4] Christopher Fam. (2024, February 5). Maxis says its system is unaffected after R00tk1t hacker group threatens to expose 'treasure trove of customer data' . *The Star*.

[5] CMMC. (2024). Cybersecurity Maturity Model Certification (CMMC).

[6] Computer Fraud and Security. (2021). *MA Business*.

[7] Craiger, J. Philip., Lindamood-Craiger, Laurie., & Zorri, D. M. . (2021). *Cyber Supply Chain Risk Management : Implications for the SOF Future Operating Environment*. Joint Special Operations University Press.

[8] Dash, A., Sarmah, S. P., Tiwari, M. K., Jena, S. K., & Glock, C. H. (2024). Cybersecurity investments in supply chains with two-stage risk propagation. *Computers and Industrial Engineering*, *197*. https://doi.org/10.1016/j.cie.2024.110519

[9] Davey Winder. (2024, November 27). Wake Up And Smell The Ransomware - Starbucks Impacted By Cyber Attack. Forbes.

[10] DefStan. (2021). UK Cyber Security for Defence Suppliers.

[11] Gokkaya, B., Aniello, L., & Halak, B. (n.d.). *Software supply chain: review of attacks, risk assessment strategies and security controls*. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

[12] Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security Threats, Countermeasures, and Challenges of Digital Supply Chains. *ACM Computing Surveys*, *55*(14 S). https://doi.org/10.1145/3588999

[13] Heinbockel, W. J., Laderman, E. R., & Serrao, G. J. (2017). MITRE Supply Chain Attacks and Resiliency Mitigations Guidance for System Security Engineers.

[14] Ishgair, E. A., Melara, M. S., & Torres-Arias, S. (2024). *SoK: A Defense-Oriented Evaluation of Software Supply Chain Security*. http://arxiv.org/abs/2405.14993

[15] ISO. (2022). ISO/IEC 27001:2022 ISMS.

[16] Khalil, S. M., Bahsi, H., & Korõtko, T. (2024). Threat modeling of industrial control systems: A systematic literature review. *Computers and Security*, *136*. https://doi.org/10.1016/j.cose.2023.103543

[17] Kulikov, S. S., Belonozhkin, V. I., & Yuyukin, N. A. (2022). Analysis of Information Security Threats, Associated with Supply Chain Attacks. *Information and Security*, *1(-)*, 135–140. https://doi.org/10.36622/VSTU.2022.25.1.011

[18] Ludvigsen, K. R., Nagaraja, S., & Daly, A. (2022). *Preventing or Mitigating Adversarial Supply Chain Attacks; A Legal Analysis*. http://arxiv.org/abs/2208.03466

[19] Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering*, *11*(5), 537–545. https://doi.org/10.18280/IJSSE.110505

[20] Mullet, V., Sondi, P., & Ramat, E. (2021). A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. In *IEEE Access* (Vol. 9, pp. 23235–23263). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3056650

[21] Nakano, Y., Nakamura, T., Kobayashi, Y., Ozu, T., Ishizaka, M., Hashimoto, M., Yokoyama, H., Miyake, Y., & Kiyomoto, S. (2021). Automatic Security Inspection Framework for Trustworthy Supply Chain. *2021 IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications (SERA)*, 45–50. https://doi.org/10.1109/SERA51205.2021.9509040

[22] Nygård, A. R., & Katsikas, S. (2022, August 23). SoK: Combating threats in the digital supply chain. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3544421

[23] Nyonyoh, R. (2025). The Strategic Threat of Supply Chain Attacks: A National Security and Economic Perspective. *Asian Journal of Economics, Business and Accounting*, *25*(4), 483–491. https://doi.org/10.9734/ajeba/2025/v25i41765

[24] OIC-Cert. (2024). OIC-CERT Software Supply Chain Security Framework Version 2.0. www.oic-cert.org

[25] Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. In *Computers and Chemical Engineering* (Vol. 171). Elsevier Ltd. https://doi.org/10.1016/j.compchemeng.2023.108169

[26] Ravie Lakshmanan. (2021, January 21). Here's How SolarWinds Hackers Stayed Undetected for Long Enough. *The Hacker News*.

[27] Ravie Lakshmanan. (2025a, April 16). Chinese Android Phones Shipped with Fake WhatsApp, Telegram Apps Targeting Crypto Users. *The Hacker News*.

[28] Ravie Lakshmanan. (2025b, May 14). Earth Ammit Breached Drone Supply Chains via ERP in VENOM, TIDRONE Campaigns. *The Hacker News*.

[29] Sarah Shamim. (2024, September 18). How did Hezbollah get the pagers that exploded in Lebanon? Aljazeera.

[30] Sundararajan, V., Ghodousi, A., & Dietz, J. E. (2022). The Most Common Control Deficiencies in CMMC non-compliant DoD contractors. *2022 IEEE International Symposium on Technologies for Homeland Security, HST 2022*. https://doi.org/10.1109/HST56032.2022.10025445

[31] Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. In *Computers and Security* (Vol. 112). Elsevier Ltd. https://doi.org/10.1016/j.cose.2021.102536

[32] Tan, Z., Marnerides, A. K., Anagnostopoulos, C., Parambath, S. P., & Singer, J. (2024). *Advanced Persistent Threats based on Supply Chain Vulnerabilities: Challenges, Solutions and Future Directions*. https://doi.org/10.36227/techrxiv.170594149.97651781/v1