Journal of Cybersecurity and Privacy

MDPI

Article

Security Attack Behavioural Pattern Analysis for Critical Service Providers

Elias Seid *, Oliver Popov and Fredrik Blix

Department of Computer and Systems Sciences, Stockholm University, Borgarfjordsgatan 12, 164 55 Stockholm, Sweden
* Correspondence: elias.seid@dsv.su.se

Abstract: Identifying potential system attacks that define security requirements is crucial to building secure cyber systems. Moreover, the attack frequency makes their subsequent analysis challenging and arduous in cyber–physical systems (CPS). Since CPS include people, organisations, software, and infrastructure, a thorough security attack analysis must consider both strategic (social and organisational) aspects and technical (software and physical infrastructure) aspects. Studying cyberattacks and their potential impact on internal and external assets in cyberspace is essential for maintaining cyber security. The importance is reflected in the work of the Swedish Civil Contingencies Agency (MSB), which receives IT incident reports from essential service providers mandated by the NIS directive of the European Union and Swedish government agencies. To tackle this problem, a multi-realm security attack event monitoring framework was proposed to monitor, model, and analyse security events in social(business process), cyber, and physical infrastructure components of cyber–physical systems. This paper scrutinises security attack patterns and the corresponding security solutions for Swedish government agencies and organisations within the EU's NIS directive. A pattern analysis was conducted on 254 security incident reports submitted by critical service providers. A total of five critical security attacks, seven vulnerabilities (commonly known as threats), ten attack patterns, and ten parallel attack patterns were identified. Moreover, we employed standard mitigation techniques obtained from recognised repositories of cyberattack knowledge, namely, CAPEC and Mitre, in order to conduct an analysis of the behavioural patterns

Keywords: security pattern; IT-incidents; societal safety; cyber–physical systems; essential services; NIS-directive; socio-technical system; cyberattack

Citation: Seid, E.; Popov, O.; Blix, F. Security Attack Behavioural Pattern Analysis for Critical Service Providers. *J. Cybersecur. Priv.* **2024**, *4*, 55–75. https://doi.org/10.3390/jcp4010004

Academic Editor: Carlo Blundo

Received: 1 November 2023
Revised: 15 December 2023
Accepted: 20 December 2023
Published: 10 January 2024

1. Introduction

Over the past decade, various sectors within society have experienced a rapid process of digitalisation. One significant trend involves the migration of crucial information resources and organisational procedures from physical to digital platforms. The implementation of novel socio-technical solutions has brought about numerous advantages by significantly enhancing operational efficiency in both corporate and governmental organisations, thereby altering the landscape of information and process management. However, it has also presented novel challenges. The increasing reliance on systems and networks has led to a greater vulnerability in essential service providers, such as government agencies and healthcare organisations, to incidents that disrupt their operations [1]. Cybersecurity incidents that affect the cyberinfrastructure, which includes the network and system resources of important service providers, can cause major impacts to essential digital operations. Consequently, this disruption indirectly hampers the organisation's capacity to effectively deliver services to its stakeholders. In addition to the general public, various other organisations are also involved. This prompts inquiries into the extent to which cyberattacks can inflict damage on organisational systems and networks, as well as indirectly impacts organisational functions and society as a whole

(https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed on 19 December 2023).

Cyber–physical systems(CPS) security breaches have cost large organisations multi-million dollar losses, and this cost is rising [2]. These breaches are caused by CPS's complexity and heterogeneity in people, processes, technology, and infrastructure. These heterogeneous components raise many security concerns and increase the attack surface compared to homogeneous software systems. These breaches are caused by trusted insiders (inadvertent or malicious), malware, SQL injections, hijacked devices, etc. Due to the increased number of attacks, CPS are the ideal target for multistage attacks, as attackers can combine atomic attack actions with different components to launch more dangerous attacks [3].

Failing to consider diverse attacks when designing CPS can make them vulnerable. This trend is attributed to the relatively low risks involved and the potential for significant gains. In the present era, the advent of state-of-the-art technological developments in areas including cloud computing, artificial intelligence, and the Internet of Things has introduced new vulnerability and, as a result, presented considerable cybersecurity obstacles. The advancements have increased the importance of addressing the cyber threat landscape faced by vital service providers and the potential repercussions of attacks targeting them. (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed on 19 December 2023)

Targeted security analysis requires identifying likely attack strategies. The lack of knowledge about impending attacks makes operationalisation analysis difficult because analysts cannot realistically identify how attackers might attack a system, resulting in false positives or negatives during security analysis. As the security community has summarised practical attack knowledge in 559 attack patterns, i.e., common attack pattern enumeration and classification (CAPEC), we plan to remedy the knowledge gap. Shostack et al. argue that the formidable magnitude and span of CAPEC might deter individuals from participating [4], thus, analysts exhibit reluctance in employing such patterns. Although a number of studies have been performed to deal with the scalability problem of CAPEC [3,5,6], they all require manual practise, assessment of the applicability of cyber attack patterns, and cannot efficiently incorporate CAPEC behavioural patterns into security attack analysis.

Analysing potential attacks plays an important role in the design of secure CPS. This process facilitates the detection of attacks, which ultimately guides the formulation of essential security requirements. Furthermore, it provides insight into the necessity and rationale behind the implementation of specific security mechanisms. In our previous study, we have presented a comprehensive framework for monitoring security attack events across multiple realms [7]. The framework consists of the following elements: vulnerability model (VM), attack-mechanism model (AM), behavioural model (BM), and event model (EM). Each component of the framework is described below.

Vulnerability Model (VM): This model captures the type of attack pattern, as well as potential threats and asset types. An asset is anything that has value to an organisation. Assets can be tangible (physical) or intangible (non-physical). Security concerns, such as confidentiality, integrity, availability, and accountability of an asset, can be associated with the business, application, or infrastructure context.

Attack-Mechanism Model (AM): This model captures goal models, domain assumptions, attack mechanisms, and task operationalisations that are used in cyber attacks by taking advantage of CPS weaknesses with the intent of achieving negative social and technical impacts. The lack of adversaries during the design of a secure system creates a challenge for security development and engineering [8]. Adversaries are anti-stakeholders that compromise the system. For example, threats are indirectly discovered because of adversaries, whose goals, potentials, and behaviours define the threats to a system.

Behavioural Model (BM): This represents and captures the runtime behaviour of an attack strategy, providing the runtime attack behaviour of security attacks. In this model, the attack-mechanism Model(AM) was employed to generate attack behaviours.

Event Model (EM): This model captures events derived from the attack-mechanism and behavioural models (BM and AM). **Runtime Attack Model**: The BM provides annotations of fundamental system behaviour and derives runtime attack models from design-time attack models to support attack-event monitoring.

Addressing multi-stage attacks on CPS has proven to be challenging due to the vulnerability of their components to cyber-attacks. Addressing these attacks continues to be a challenging unresolved issue, as each component bears its own complexities and vulnerabilities, requiring an integrated security solution [9]. Designing a security solution for CPS is more challenging compared to software systems due to the additional consideration of the interaction between CPS components (such as sensing, communication, and computing components) and the physical environment [10]. CPS components that are exposed to increased risk and vulnerability to attack can be exploited by malicious actors. This vulnerability arises from the fact that these components, such as sensors, operate within an open and inherently insecure environment. Consequently, security threats such as unauthorised information disclosure, transmission of falsified data, and violations of authentication and/or authorisation protocols must be carefully considered.

The research in the area of security patterns has made significant advancements in the collection and organisation of these patterns. However, their practicality and usefulness in real-world scenarios is limited. In their study, ref. [11] proposed the concept of attack patterns as a means to consolidate and utilise the attack knowledge derived from multiple instances of attacks. The primary objective of this approach is to facilitate the analysis of security requirements. These proposals outline steps that can be taken to investigate the methods employed by attackers during an attack. Within the existing collection of the literature, various proposals have been put forth with the aim of presenting methods for representing attack scenarios. For instance, researchers have utilised attack trees [12] and graphs [13] as viable approaches to capture attack scenarios. In contrast to our approach, these efforts exhibit certain limitations in terms of providing explicit details regarding the execution of attack strategies.

Further study has also been carried out to analyse and model threats like STRIDE [4], but these efforts are somewhat limited in their ability to handle multi-stage attacks and fail to account for the intentions of the attacker. Several proposals, such as [14], have been explicitly addressed to capture the reasoning behind attacker actions using anti-goals, in contrast to this work. An attacker's perspective and the adversary's malicious intentions have been proposed for security analysis in similar ways to [14,15]. Our approach aligns with these approaches in terms of attack models, anti-goal refinement, and the construction of attack scenarios. However, our approach goes beyond this by analysing behavioural models of security attack scenarios and using them to generate runtime attack models.

This study has the potential to provide valuable insights into the patterns and advancements within the field of cybersecurity and is crucial for developing a comprehensive and evidence-based understanding of the potential threats. However, there is a lack of research investigating the impacts of cyberattacks on significant service providers. Furthermore, there is a lack of sufficient investigation into the nature of the impact that these attacks have had on the cyberinfrastructure of organisations, as well as the frequency with which incidents lead to adverse consequences beyond the digital realm. This trend can be partially attributed to the inherent challenges associated with the collection of data associated with the incidents that take place.

A significant amount of the research on cyberattacks relies on sources such as media reports, open-source intelligence, and interviews with professionals [2–4,16,17]. At the same time, it has been determined by entities such as the European Union Agency of Cybersecurity (ENISA) that publicly reported incidents represent only a fraction of the total, implying that a significant number of incidents remain undetected or unreported (ENISA, 2022, Rue de la Loi 107, 1049 Brussels, Belgium).

The absence of research focused on the characterisation and consequences of malicious activity directed at significant service providers can be considered problematic from various

viewpoints. According to [9,18], it was argued that this trend may have implications for the organisations' capacity to effectively assess risk. This is due to a limited understanding of the probability and characteristics of potential attacks [9,18]. The lack of research into the adverse effects of cyber attacks hinders the researchers' ability to understand the organizational and societal implications of these malicious activities [19,20].

Objectives of this study: (1) Analyse the specific characteristics of cyber security threats that specifically target prominent service providers in Sweden. (2) Analyse cyber attack patterns and their corresponding cyber security solutions using Asfalia [7]. This study analyses cyber security incident reports submitted to MSB to enhance the understanding of cyberattacks on critical service providers in Sweden. The study aims to address the following research questions (RQs).

- Research Question (RQ1:) What is the impact of multi-stage attacks on the cyberinfrastructure of critical service providers?
- Research Question (RQ2): How do critical service providers analyse multi-stage cybersecurity attacks in order to defend against them?

The remaining parts of this paper are structured as follows. Section 2 presents the research baseline for our work, while Section 3 presents our approach and provides a case study. In Section 4, we provide cyber attack classification. In Section 5, we present the experiment and results, while Section 6 deals with the discussion. Section 7 presents the related work, and Section 8 concludes and discusses the future work.

2. Research Baseline

2.1. Digitising Critical Service Providers

The convergence of physical and digital dimensions through digitalisation has led to increased speed and connectivity for society. The integration of technology has increased volatility, uncertainty, complexity, and ambiguity in social contexts [1]. Modern society has transformed into a risk society as a result of increased complexity, forcing the adoption of comprehensive risk management [21]. Drawn from the influence of Beck and motivated by the consequences of digitalisation on societies' capacity to manage incidents, it was proposed that the convergence of digitalisation and globalisation has played a role in the emergence of transboundary crises [22].

A crisis can have cascading effects across spatial, temporal, and social boundaries [22]. Modern socio-technical developments, such as greater reliance on heterogeneous systems and software, as well as complex supply chains, contribute to escalating incidents [21]. According to the theory of transboundary crisis, modern society is more susceptible to disruptions in vital infrastructures and must adapt to minimise the associated risks [22].

Protecting vital information systems and networks from destruction and disruption has been a policy goal since the early 21st century to prevent incident escalation. Strategic goals such as societal resilience and robustness, which describe the ability to quickly recover and withstand incidents, have been established to ensure the continuity and integrity of IT-dependent services. The need for specific measures has evolved as more information assets and processes transition to technology [23]. This development coincides with the securitisation of cyberspace, emphasising cyber threats as a matter of internal and national security [24].

The growing impact of cyber threats to societal services and infrastructures has resulted in the emergence of more complex and uncertain risks. Thus, there is a need for interdisciplinary solutions to address these challenges. In academia, the fields of societal safety and societal security have combined, advocating for an "all-hazards" strategy [25]. Sweden has long used an all-hazards approach in policy, and MSB includes antagonistic hazards in national risk assessments [26]. As the EU emphasises cyber threats to internal market stability, the merger becomes more apparent [16]. According to [27], the EU's cyber governance understanding is influenced by real situations more than other authorities.

There are a total of 12 events that were identified as having the potential to impact social and economic stability [27]. The EU Cyber Security Act, as stated in [8], provides

a definition of cybersecurity that encompasses the protection of both IT resources and individuals impacted by incidents. The EU is implementing regulations to improve cybersecurity standards for key actors as digital integration blurs the lines between service providers. The EU directives NIS (EU 2016/1148, replaced by EU 2022/2555) and CER (2022/2557) have the objective of preventing IT incidents among important entities and reducing the impact of such incidents on critical functions and services.

2.2. Organisational and Societal Impact

Cyberspace incidents have had major effects on the real world due to digital convergence. The study [28] distinguishes between the direct and indirect impacts of cyber incidents. The direct impact on cyberinfrastructure describes how various activities can allow unauthorised access, modification, or removal of digital resources. The direct impact resembles operational and informational impact classifiers [24]. The indirect impact is caused by an event outside of the digital space [28]. Furthermore, the study in [29] investigated both primary and secondary cyber effects. Data fraud, destruction, or compromise can have detrimental effects on the organisation, stakeholders, government, and society. When evaluating cyberattacks on critical service providers, it is important to take into account these impacts [30]. The most prevalent indirect consequences on an organisation are typically related to financial impacts. Organisational risk assessments employ anticipated financial and economic losses to evaluate the probability and consequences of different scenarios. The economic and financial consequences are significant in cases where there is a loss of competitive advantage resulting from the disclosure of sensitive information or a disruption. A comprehensive analysis was undertaken to determine the mean expenses associated with cyber incidents across diverse industry domains, with a specific emphasis on identifying the most severe categories. Financial loss is incorporated as a factor in their cyber risk model [31,32].

Although it is the best way to calculate indirect impact from an incident, other variables should be considered. This is especially important when discussing how incidents affect organisations providing vital services to diverse stakeholders. The field of cybersecurity has advanced, and the authors argue that the study of cyber harm includes both the physical and psychological damage inflicted upon individuals and communities [33]. In order to achieve this, Agrafiotis et al. [20] identified five distinct categories: physical (digital), economic, psychological, reputational, and social. Physical or digital harm involves both harm to individuals and damage to cyberinfrastructure. Furthermore, the impacts on society involve disruptions in daily life, damage to the nation, and decreased employee morale. Agrafiotis et al. [20] also discuss negative effects like public perception changes, daily life disruptions, and national impact. ENISA, the EU cybersecurity agency, defines societal impact as effects on the public or widespread disruptions (e.g., national health system disruption) in their Cyber Threat Landscape reports (ENISA, 2022 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed on 19 December 2023)). If critical services are interrupted, system and network incidents can affect society.

2.3. Cyber–Physical Systems

The rapid pace of cyber developments has resulted in a lack of consensus regarding the understanding of cyberattacks and their consequences [34]. The present study adopts the definition of a cyberattack provided by [35], which encompasses a wide range of "offensive actions" that have an impact on the cyber infrastructure of an organisation. Offensive action includes both active attacks, such as DDoS attacks, and passive attacks, such as cyber-exploitation, which involves unauthorised information gathering [29].

Cyberattacks on the cyberinfrastructure may target processes, hardware, and users. There are various cyberattack techniques, such as syntax attacks (using malware) and semantic attacks (using social engineering techniques) to gain access to targeted cyber

infrastructure [29,34]. The definition of "offensive action" encompasses both social and non-digital actions, such as the physical targeting of hardware components [35].

Cyberattacks have multiple components and are understood at different levels of abstraction, leading to ambiguity in academia and organisation practises [36]. Numerous taxonomies have been developed to classify various aspects of attacks in recent decades [29]. According to [37], cyberattack frameworks typically include five components: goal, attack-source, target, attack vector, impact. The authors identify three dimensions of these components: adversarial, methodological, and operational, to differentiate their qualities better.

In this context, adversarial refers to the threat actor and their strategic and operational objectives for the attack. Methodological refers to the techniques used by threat actors to achieve their goals. Finally, the operational dimension refers to the impact of the cyberattack on the targeted infrastructure. The operational dimension of cyberinfrastructure includes two types of impact: impact on the targeted system networks or impact on information assets [37]. According to [22], a cybersecurity incident involves compromising the confidentiality, integrity, and availability of systems, networks, and other IT resources.

The AVOIDIT cyberattack taxonomy [38] is a well-known and often-used framework in the academic literature. It can be argued that this framework primarily emphasises the operational dimension of cyberattacks. A classification framework was introduced in [38], consisting of four classifiers designed to classify attacks. The following are the classifiers:

- Attack Vector: An attack vector constitutes the type of vulnerability that the attacker might use to obtain access to the cyber infrastructure
- Operational Impact: Operational impact can be defined as the activities undertaken by an attacker having gained access to the targeted organisation's cyberinfrastructure
- Informational Impact: Can be defined as the effect cyberattacks have had on sensitive and otherwise protected systems and information assets
- Target: High-level understanding of the concept and, thus, classifies incidents based on components like network and software or software system

Moreover, a classifier was added to categorise incidents based on preferred defensive measures. An attack vector refers to the specific path that is used to gain access to the targeted component. This definition aligns with MITRE's concept of "initial access" [39] (https://attack.mitre.org/, accessed on 6 June 2023). In contrast to MITRE, Simmons et al. emphasise a broad understanding of exploited vulnerabilities rather than attacker tactics and techniques in cyberattacks. The impact is described using operational and informational impact classifiers [38].

Operational impact encompasses compromised system or network functionality, including "web compromise", "installed malware", and "denial of service". An additional classifier, informational impact, describes how the attack impacts the informational resources within the cyber infrastructure. The classifier includes categories like "distortion" and "disclosure" of information. These categories can classify both active and passive attacks, with "installed malware" and "disclosure" describing cyberattacks attempting unauthorised information gathering through spyware and other means. The attack target classifier identifies the targeted cyberinfrastructure, such as "network" and "user" [39].

2.4. Asfalia Framework

This section presents the Asfalia framework that supports the monitoring of security attack events for CPS, and the framework spans the three realms of a CPS. Moreover, the framework supports cross-realm analysis and monitoring, which spins off security events across realms. Our models focus on realm-specific adversaries, meaning that they span the three realms of a CPS (cyber, physical infrastructure, and social). We also analysed the interdependent relationships among realm-specific attack models. The AM depends on the VM model in revealing realm-specific vulnerabilities, and the vulnerabilities captured by (the VM) spin off and provide inputs to the next realm (AM). Thus, a suitable attack mechanism is selected by taking advantage of the weaknesses of the VM. More detailed information can be found in [7]. The Asfalia analysis process consists of the following steps.

Vulnerability Model (VM): This model captures the attack patterns, potential threats, and type of asset, in which an asset is a potential target for cyber attacks. The VM consists of the following sub-elements.

Threat: This is the potential for abuse of an asset that will cause harm in the context of the problem.

Vulnerability: This is a weakness in the system that an attack exploits.

Asset: This is anything that has value to an organisation, and it can be tangible (physical) or intangible (non-physical) with respect to the target of the attack.

Attack pattern: This is defined as a generic description of a deliberate, malicious adversary that frequently occurs in a specific context [40]. It describes the common elements and techniques used in attacks against vulnerable CPS components. These patterns generalise reusable attack knowledge from frequent adversaries to facilitate security requirements analysis for the system-to-be. An attack pattern consists of the general goal of the attack, the antecedent, the steps to carry out the attack, and the consequent.

Attack-Mechanism Model (AM): This model captures design strategies for different attack pattern mechanisms. More importantly, it builds attack mechanisms by employing goal models, domain assumptions, attack mechanisms, and task operationalisation artefacts. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, providing the adversary's perspective on the problem and the solution and guidance for mitigating the attack's effectiveness. The AM depends on the VM since it prepares its attacking mechanism based on the threat explored in the VM. However, threats can be refined not only linearly but also iteratively.

Behavioural Model (BM): Building a complete behavioural model for very complicated systems such as CPS, with many complex and heterogeneous states, is often challenging [7]. To understand how attackers fulfill their target by compromising security concerns such as confidentiality, integrity, availability, and accountability, one has to analyse how the threat environment behaves within the system, how adversaries can compromise the system, and how the system behaves under multi-stage attacks, as well as recognise system behaviours to facilitate such analysis. This model captures fundamental system behaviours such as **sequential**, **interleaving**, **multiplicity**, and **alternative** instances of attack goal models, sub-goals, domain assumptions, and tasks.

Event Model (EM): This model captures events derived from behavioural models (BM). These events could be grouped into observable and non-observable events from an event-log perspective. We focus mainly on observable events.

3. Data Collection Method

The data source used in this study consists of IT-incident reports that were submitted to MSB. Thus, it can be considered an unconventional study of the written data, primarily relying on sources that are document-based. Furthermore, the research was conducted using a secondary dataset consisting of written IT-incident reports that were submitted to MSB by different Swedish government agencies and organisations, following the guidelines specified in the European Union's NIS-directive. In Sweden and other countries, organisations have the choice to retain information. The Swedish legislation on public access to information and confidentiality, specifically the Public Access to Information and Secrecy Act (SFS 2009:400) and the Protective Security Act (SFS 2018:585), place limitations on the dissemination of information within public administration, including government agencies. Private companies have the option to withhold information about attacks and their consequences in order to protect their valuable assets or maintain positive relationships with stakeholders [3].

One potential limitation of this approach is that the secondary data used as the data source were not specifically collected for the purpose of this study. The analysis is constrained by this limitation. The conclusions that can be derived are dependent upon the characteristics and quality of the data obtained from the particular format of MSB's IT-incident reports. Another constraint involves relying on reported incidents as the basis

for analysing the cyber threat landscape, which fundamentally leads to conclusions that are dependent upon the reporting choices and methods of the organisations.

4. Cyber Attacks

4.1. Classification of Security Events

The data treatment process was carried out in four stages. During the first stage, all IT-incidents reported between 1 April 2019 and 1 April 2023 were gathered, and the incidents describing malicious events were singled out. The remainder were excluded from the dataset. During the second stage, the IT-incident reports were categorised according to **vulnerability**, **attack-mechanism** and **security events**, and **attack target**, and the results transformed into a similar, quantifiable format. The incidents that did not provide enough information for the incident to be classified in accordance with each classifier were categorised as **unknown**. The third stage of the data treatment process included summarising the quantities found within each category to be able to compare the frequencies.

During the period from April 2019 to 2023, (MSB) received a total of 1332 IT-incident reports from major service providers. Out of the total reports, 256 were submitted by organisations in the (NIS) sector, while the remaining 1076 were submitted by government agencies. Among the entire dataset, 254 reports contained detailed accounts of incidents that were ascribed to intentional and malicious acts. The remaining incidents were ascribed to a range of causes, including technician and user errors, system malfunctions, natural occurrences, and unidentified variables. Moreover, the frequency of the reported cyberattacks from April 2019 to 2023 has consistently maintained a stable level. During the period spanning from 1 April 2019 to 2020, there was a substantial increase in reported cyberattacks, reaching a total of 73 incidents. Afterwards, in the time period of 2022–2023, a total of 67 cyberattacks were reported. During the period from 2020 to 2021, there was a significant rise in cyberattacks, with a total of 61 reported cases. From April 2021 to 2022, there was a limited occurrence of cyber attacks that specifically focused on important service providers. The number of reported incidents totaled only 53 occurrences.

4.2. Vulnerability

The classifier of attack vector was used to categorise cyberattacks according to the abstract vulnerability exploited, or that the threat actor attempted to exploit, to compromise the perimeter of the organisation's cyber infrastructure. Among the total number of cyberattacks reported, the most common category, based on the analysis, was concluded to be **social engineering**. In total, 32 percent of the IT-incident reports that described cyberattacks, or a total of 81 cases, were categorised as having utilised social engineering techniques to gain initial access. This category includes cases of **phishing**, **spear phishing**, and other forms of manipulation attempts utilised with the aim of trying to deceive the recipient into responding or performing certain actions. The prevalence of social engineering incidents suggests that various deceptive tactics are commonly employed to gain unauthorised access to critical service providers. The second most prevalent method of attack was **insufficient capacity**, which was found to be responsible for 28 percent of all reported cyberattacks, totaling 72 cases. This category refers to incidents in which the attacker attempted to take advantage of the limitations in the capacity of cyber infrastructure resources, as illustrated by distributed denial of service attacks. Afterwards, the insufficient category accounts for a low percentage of cyberattacks.

Insufficient authentication involves techniques for bypassing authentication procedures, such as employing brute-force attacks. Meanwhile, the term "unknown" refers to incidents in which the reporting organisations did not provide sufficient details in their description of the event to determine the specific attack method used. This was later accompanied by **inadequate input validation** and **misconfiguration** at 9%, 5%, and 5%, respectively. The other category covers reports that described an attack vector that did not align with any other specified categories. These primarily describe common vulnerabilities in systems and code. Based on attack vector usage, social engineering cases increased in

April 2019–2020 and April 2020–2021. Social engineering techniques were used in 44% and 49% of reported malicious incidents during these periods. After that, social engineering decreased in frequency, accounting for only 15% of reported cyberattacks in 2022–2023.

This could indicate that threat actors are increasingly making use of other types of attack vectors. Alternatively, the organisations targeted are becoming better at protecting themselves against these types of attacks and, therefore, do not report them to the same extent. Meanwhile, using capacity limits as an attack vector saw a sharp increase in the April 2022–2023 period, going from representing approximately 20 percent of cyberattacks in April 2019–2022 to 52 percent.

4.3. Attack-Mechanism and Security Events

The classifiers of operational and informational impact have in this study previously been described as forms of direct impact within the cyber infrastructure. Based on the reports, the most common direct impact generated by an attack, looking at both operational and informational consequences, is **the disruption in access to information resources and systems**. As seen in Figure 1, cyberattacks resulting in the operational impact of denial of service have been concluded to account for 43 percent, or 109 cases in total, of the reported malicious incidents.

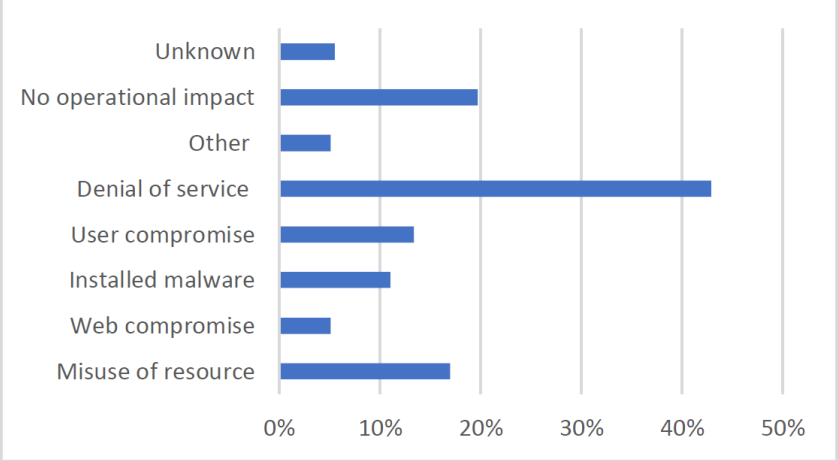

Figure 1. Attack-Mechanism and Security Events.

In 17% of incident reports, the misuse of resources was reported, followed by account hijacks in 13%. Threat actors installing malware in an organisation's cyber infrastructure accounts for 11% of cyberattacks, totaling 28 cases. Website resource compromise incidents account for approximately 5% of incidents. Unknown and other comprised 6% and 5% of the reported cyberattacks. Note that the other category primarily refers to fraud cases. The main impact of these attacks is on human behaviour and economic loss.

In 44 cases, or 17%, the attacker's operational impact was classified into multiple categories. Malware installation occurs in 39% of cases when a system user is compromised. Malware infection occurred in 32% of compromised user accounts. Approximately 20% of attacks resulting in a denial of service also involved other operational compromises, with the most common being the misuse of resources (11 cases). The distribution of informational impact is shown in Figure 2. One of the most common informational impacts described in incident reports is disruption in availability. Approximately half of malicious-activity-related incidents disrupt access to information resources and system functionality. In 16% of cases, disruption led to the disclosure of information, as determined by reading reports. The information was distorted in approximately 8% of cases.

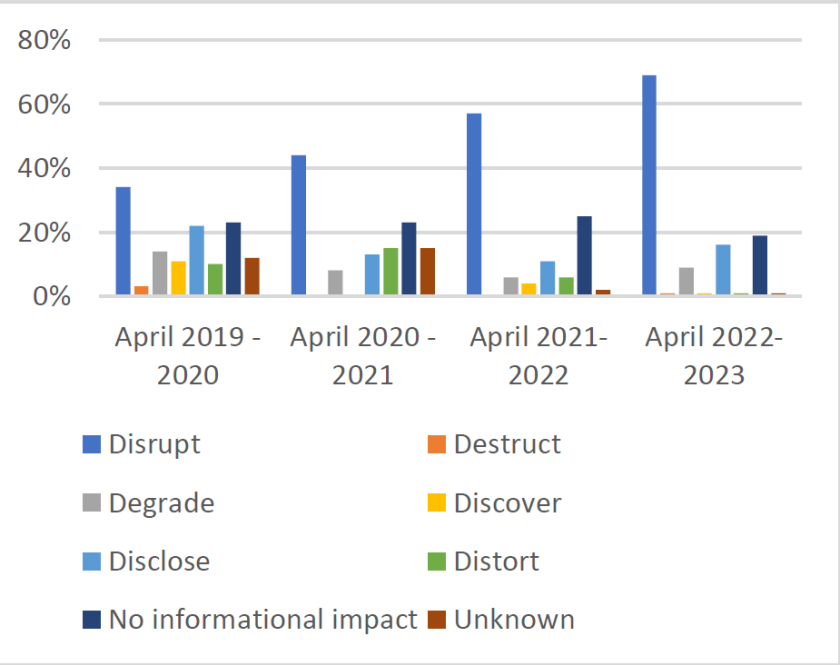

Figure 2. Informational Impact.

Approximately 4% of cases involved mapping and discovering the structure of the targeted organisation's network and systems. Only approximately 1% of cyberattack reports describe the permanent loss of information assets, making information destruction a rare impact. This may be due to organisations implementing measures to prevent permanent information loss. In contrast to the CIA-triad, most of the observed cyberattacks compromise availability, while fewer compromise confidentiality and integrity. The IT incident reports may be biassed due to the requirement for NIS organisations to report incidents that disrupt or degrade their operations.

The analysis revealed that many incidents had no significant operational or informational consequences. The analysis of reported malicious activity indicated that more than 20% of instances did not cause any operational consequences to the organisation's cyber infrastructure. Furthermore, 22% of attacks were reported to have had no impact on the organisations' data. Figure 2 illustrates the proportion of cyber-attacks that do not have a direct impact on operations or information. Approximately 15–21% of cyberattacks occurring from April 2019 to 2023 were related to IT incidents that seemed to have no effect on the targeted cyber infrastructure. According to the study's definition, in the period of April 2022–2023, only 12% of incidents were categorised as having no direct impact.

The primary methods of attack exploited in cases without immediate consequences were social engineering and insufficient authentication, although they ultimately proved unsuccessful. Leveraging vulnerabilities in authentication mechanisms and cognitive biases may increase the probability of failure. The findings of this study rely on incident reports, and organisations may have an increased understanding of unsuccessful attacks using these methods. In contrast, 94% of the identified denial of service attacks, specifically 103 out of 109, have resulted in disruptions to availability. Among the malware cases, only one reported no discernible informational impact, whereas three reported an indeterminate impact. This suggests that the organisation reported a malware infection but did not specify its consequences.

Of the entirety of the malware that was installed, 67% resulted in disruption, while 29% and 25% resulted in distortion and disclosure, respectively. This study is unable to evaluate the efficacy of these attacks beyond their impact on organisations and society, as it does not assign a value to the severity of the informational impact. A higher percentage of IT incident reports depict attacks as having an informational impact rather than an operational

impact. This could be attributed to the implementation of cybersecurity measures, which also have a significant informational influence. Figure 3 illustrates an upward trend in denial of service attacks over time. In the period from April 2019 to 2021, denial of service attacks constituted 26% of all attacks, whereas in the period from April 2022 to 2023, they accounted for 72% of all cyberattacks.

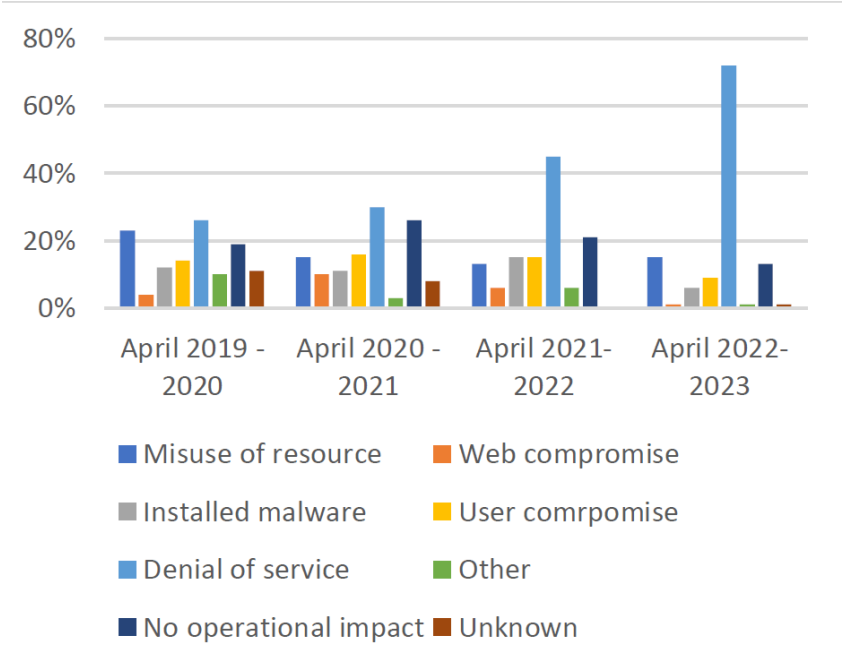

Figure 3. Operational Impact.

According to the analysis results, the share has shown growth both in relative and real terms since April 2020. Other operational impacts might lack the same level of visibility as a trend. Over the past few years, there has been a substantial increase in the number of incidents that have caused disruption to information assets and systems. Specifically, the percentage of such incidents has risen from 34% in April 2019–2020 to 69% in April 2022–2023. Contrary to what was stated earlier, not all denial of service attacks result in disruptions. Approximately 3% of the reports indicated that a denial of service attack did not result in any form of disruption. Organisations could have implemented defensive strategies to ensure continued access to specific information.

4.4. Attack Target

The study found that the fourth classifier specifically recognised cyber infrastructure components as potential targets for malicious activity, which also included incidents occurring within the supply chain of the reporting organisation. The predominant category of attacks reported involved the deliberate targeting of software or software systems. This phenomenon was observed in 47% of cases out of a total of 120 reported incidents. Out of the 96 reports, 38% of them documented cases where users were specifically targeted in attacks. Afterwards, there were 26 reported cases of assaults on network infrastructure. In seven instances, the specific cyber infrastructure that was targeted was categorised as "Unknown" due to a lack of adequate information in the IT incident report. According to Figure 3, websites were the target of 47% of reported cyberattacks, while emails and databases were targeted by 10% and 8% of the attacks, respectively.

A further analysis revealed that 70% of attacks causing denial of service targeted software systems, while 39% targeted websites. Many incidents have not affected internal cyber infrastructure but had the potential to disrupt external access to website resources. Additionally, 64% were attributed to threat actors targeting processing or network ca-

pacity, resulting in DDoS attacks. Approximately 16% of attacks, or 41 cases, involved organisations indirectly affected by the cyberattack via supply chain links. The organisations were affected due to a supply chain organisation being compromised. In 59% of cases, the incident targeted the organisation's software system, while 22% affected a network supplier.

Figure 3 shows that attacks on various cyber infrastructure components have had a direct impact on various degrees. Out of the attacks targeting users, predominantly using social engineering, 39% have not had any direct impact. Approximately 4% of attacks on software systems directly have not had any direct impact. All the reported attacks on network infrastructure components have effectively caused direct impact.

Implication: The prevalence of social engineering incidents suggests that various deceptive tactics are commonly employed to gain unauthorised access to critical service providers. Figure 3 demonstrates that there was an increase in social engineering cases during the periods of April 2019–2020 and April 2020–2021, based on the use of attack vectors. During these periods, social engineering techniques were employed in 44% and 49% of the reported malicious incidents. In the meantime, the occurrence of social engineering declined, representing a mere 15% of the reported cyberattacks during the period of 2022–2023. This suggests that malicious actors are progressively employing alternative methods of attack.

On the other hand, the targeted organisations are improving their ability to defend against these attacks, resulting in fewer reported incidents. During the period from April 2022 to April 2023, there was a significant rise in the use of capacity limits as a method of attack. This method went from accounting for around 20 percent of cyberattacks in the period from April 2019 to April 2022, to representing 52 percent of cyberattacks. As shown in Figure 2 there has been a relative increase in attacks targeting software systems as well as relative decrease in attacks targeting users' accounts more specifically.

5. Experiment and Result

Once the security events are classified, we proceed to conduct an experiment on attack pattern behavioural analysis. This experiment is based on the findings of the attack classification presented in Section 4.

5.1. Security Attack Behavioural Pattern Analysis Using Asfalia Framework

This section provides an analysis of the behavioural patterns of security attacks in CPSs using the Asfalia framework. The framework enables the monitoring of security attack events and covers all three realms of a CPS. In addition, the framework facilitates cross-realm analysis and monitoring, allowing for the detection of security events that occur across different realms. Our models specifically target adversaries that exist within specific realms, encompassing the three realms of a CPS (cyber, physical infrastructure, and social) as shown in Figure 4.

Attack patterns are grouped into two categories: The first category of cyberattack is domain-based attack, which involves targeting specific domains or networks. The other category is mechanism-based attack, which focuses on exploiting vulnerabilities in various systems or mechanisms. For example, 'social engineering' is a type of cyberattack categorised under the domain-based attack category, while 'collect and analyse' is a type of cyberattack categorised under the mechanism-based attack. There have been a total of 18 cyber security incidents classified as cyber attacks, based on the method of attack, and seven incidents classified as domain-based cyber attacks. The reports were categorised into two distinct classifications pertaining to cyber security and cyberattacks. An analysis of cyber security attack patterns was performed on five significant cyber incidents. The events were classified and categorised according to a domain-based attack. Out of the total of 254 cyber security incidents that have been reported, Asfalia has identified 7 vulnerabilities and 5 critical cyber security incidents. Moreover, the six targets that were targeted to cyberattacks were captured.

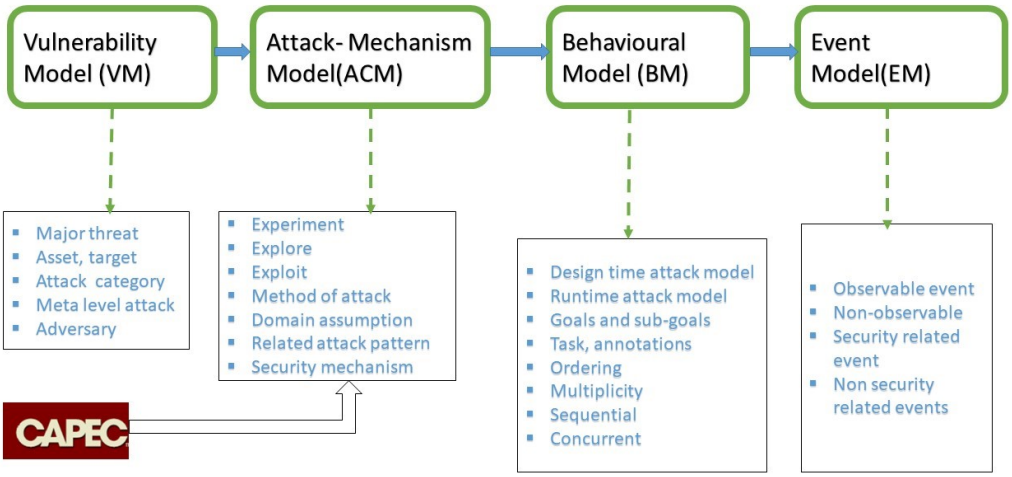

Figure 4. Meta-level attack and Design-time attack model.

5.2. Security Attack Behaviour Analysis of DDoS

Vulnerability Model (VM): This model captures type of attack patterns, potential threats, and type of asset in which an asset is a potential target for cyber attacks. VM consists of the following sub-elements: **threat**, **vulnerability**, **asset**, **attack pattern**, **antecedent**, **consequent**. **(1) threat**: An adversary exploits a deadlock condition in the target software in order to induce a denial of service. This attack can be categorised as a forced deadlock attack pattern. Additionally, the adversary may employ a parallel-attack pattern by manipulating timing and state. The specific target of this attack is the software itself. **Attack-Mechanism Model (AM)**: This model captures design strategies, different attack pattern mechanisms. More importantly, it builds attack mechanisms by employing goal models, domain assumptions, attack mechanisms, and task operationalisation artifacts. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, providing the adversary's perspective on the problem and the solution, and gives guidance on ways to mitigate the attack's effectiveness. AM model depends on VM model since it prepares its attacking mechanism based on the threat explored in VM model as shown in Figure 5. However, threats can be refined not only linearly but also iteratively. The second sub-attack mechanism consists of three sequential steps. Prior to initiating an attack, the attacker must acquire a comprehensive understanding of the targeted system. After that, they launch a specific operation within the system. Finally, they investigate whether the target condition reveals a deadlock condition.

Assumption within the domain: Assuming that the target host has an application programming interface (API) that allows attacker access, and the target programme is currently in a deadlock state. In the fourth task or activity, the attacker must begin the exploratory phase by initiating the first action and then proceeding to initiate a second action. The objective of this task is to verify if the programme is in a state of deadlock.

Behavioural Model (BM): To understand how attackers fulfill their target by compromising security concerns such as confidentiality, integrity, availability, and accountability, one has to analyse how the threat environment is behaving within the system, how the adversaries can compromise, and how the system behaves under multi-stage attacks, as well as recognise system behaviours to facilitate such analysis. This model captures fundamental system behaviours such as sequential, interleaving, multiplicity, alternative instances of attack goal models, sub-goals, domain assumptions and tasks (mechanisms).

Runtime Attack Model. The BM model provides annotations of fundamental system behaviour, derives runtime attack models from design-time attack models in order to support attack event monitoring. Alternative system behavior expresses that the system needs to satisfy a goal, and depending on the type of obstacle faced, a change in behaviour is

expected to happen, and multiple instance annotates running system behaviours that could have more than one instance, and the instances can be ordered in sequence (sequential) or they can occur concurrently (interleaved).

Sequential: The attack pattern known as "Forced Deadlock" can be annotated with the following behavioural annotations: (G2, G3#, and G4#). These annotations indicate that the sub-attack mechanism "Get familiar with system" must be achieved first, followed by the instances of "Trigger an action" and "Explore if the target condition has a deadlock condition". **Interleaving**: The formal behavioural annotation for the action of (triggering an action) is denoted as (T2#DA1), which represents the interleaved fulfilment of the (target host exposing an API to the user) and the triggering of the first action followed by the initiation of a second action. The formal behavioural annotation for the sub-attack, which involves exploring whether the target condition has a deadlock condition, is represented as (T3#DA2). This annotation signifies the sequential execution of two actions: first, checking the programme for a deadlock condition, and second, assuming that the target programme indeed has a deadlock condition.

Event Model (EM): This model captures events that are derived from behavioural models (BM). From the perspective of the event log, these events can be categorised into observable and non-observable events. Specifically, our focus is directed towards events that can be directly perceived or witnessed. Security events are generated from the behavioural model, also referred to as the BM model. For instance, the occurrence of distributed denial of service (DDoS) attacks has been captured, with one specific event identified as E1: the initiation of the exploratory phase. E2: "An action was triggered and initiated", and E3: "A denial of service occurred".

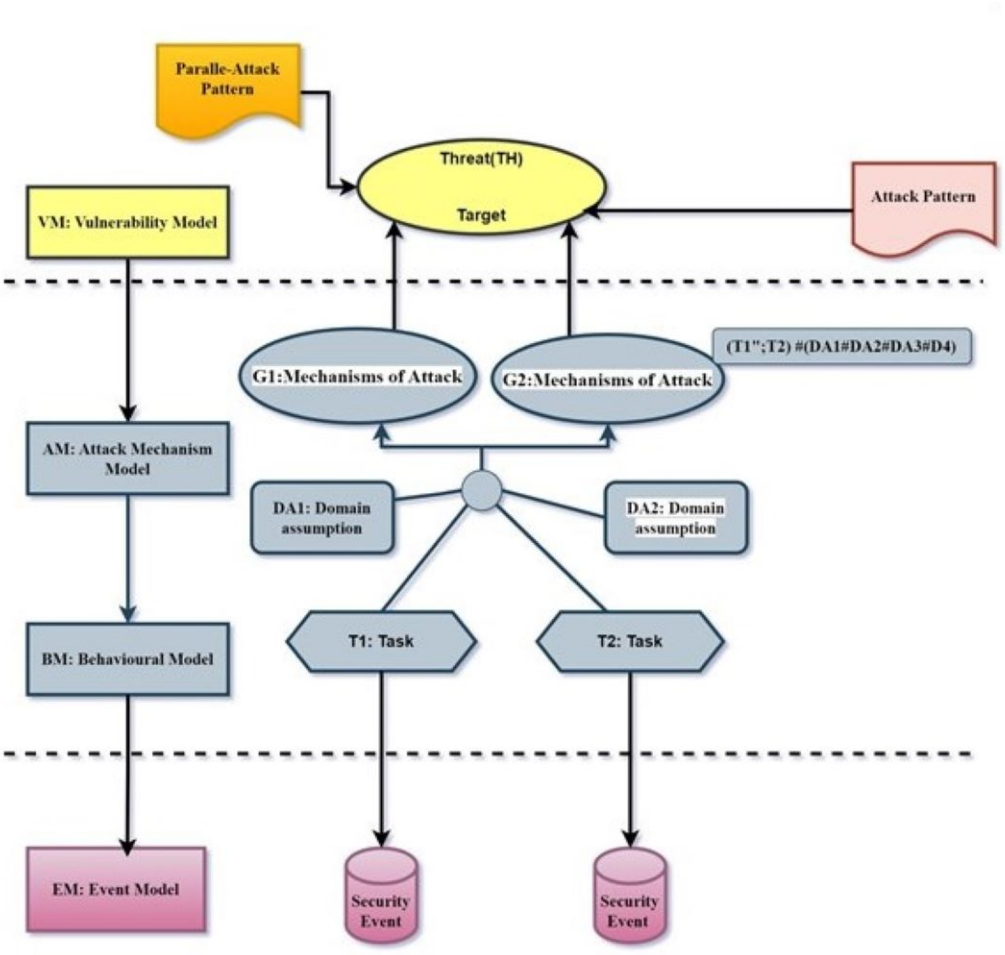

Figure 5. Graphical Representation of the Component of the Framework.

5.3. Security Attack Behaviour Analysis of Installed Malware

Vulnerability Model (VM) (1) Threat: Cause a victim to load content into their web browser that bypasses security zone controls and gains access to privileges, **target**: software, **attack pattern:** (cross zone scripting), and **parallel attack:** privilege escalation)

Attack-Mechanism Model (AM): (1) Cross zone scripting, (2) exploit systems susceptible to the attack, (3) find the insertion point for the payload, and (4) craft and inject the payload.

Tasks: (1) Leverage knowledge of common local zone functionality, (2) find weakness in the functionality used by both privileged and unprivileged users, (3) make the maliciously vulnerable functionality to be used by the victim, (4) leverage cross-site scripting vulnerability to inject payload, and **domain assumption:** insufficient input validation by the system.

Behavioural Model (BM): The formal behavioural annotation for the sub-attack Cross Zone Scripting can be represented as (Try (G2) U Succeed (G2)); G3; G4); that is, "Try (Exploit systems susceptible to the attack) U Succeed (Exploit systems susceptible to the attack)" is followed by "Find the insertion point for the payloadG:" and "Craft and inject the payload", and the formal behavioural annotation for the sub-attack "Craft and inject the payload": can be represented as (T2; DA1; T3); that is, (Make the maliciously vulnerable functionality to be used by the victim) has to be achieved first followed by (insufficient input validation by the system) and (leverage cross-site scripting vulnerability to inject payload).

Event Model (EM): This model captures the security events E1: Internet and local zone enabled, E2: enable functionality failed, E3: internet and local zone disabled, E4: weakness found, E5: weakness failed, E6: victim-injected payload, and E7: payload injected.

5.4. Security Attack Behaviour Analysis of Installed Web Compromise (XSS through HTTP Query String)

Vulnerability Model (VM): **(1) Threat**: An adversary convinces a victim to submit a malicious HTTP query string into a vulnerable web application, **Target**: software (web browser), **attack pattern:** XSS Through HTTP query strings, and **parallel attack:** DOM-based XSS.

Attack-Mechanism Model (AM): seven attack mechanisms were captured, namely, (1) XSS through HTTP query string; (2) use a browser or an automated tool; (3) attempt variations in input parameters; (4) exploit vulnerabilities; (5) steal session IDs, credentials, page contents; (6) content spoofing; and (7) forceful browsing. **Tasks**: 10 specific tasks have been captured, namely: (1) use spidering tool to follow and record all links, (2) use a proxy tool to record all links visited, (3) use a browser to manually explore and analyse the website, (4) use a list of XSS probe strings to inject in the parameter of known URLs; (5) use a proxy tool to record the results of the manual input of XSS probes in known URls, (6) develop malicious JavaScript that is injected through vectors and send information to the attacker, (7) develop malicious JavaScript that is injected through vectors and take and cause the browser to execute it, (8) develop malicious JavaScript that is injected through vectors and perform actions on the same website, (9) develop malicious JavaScript that is injected through vectors, and (10) cause the browser to execute requests to other websites .

Behavioural Model (BM): A formal behavioural annotation for the sub-attack "XSS through HTTP query String" is (G1; (G2 # G3)) #. That is, first, use a browser or automated tool, then repeatedly attempt input parameter variations and exploit vulnerabilities. A formal behavioural annotation for the sub-attack G2 (**Use a browser or an automated tool)** is T1; (T2 # T3); that is, the sub-attack G2 (use a browser or automated tool) has a formal behavioural annotation. T1 (use spidering tool to record links) should be completed first, followed by T2 (use proxy toll to record links), and T3 (use browser to manually explore and analyse website). Formal behaviour annotation for G3 sub-attack (**attempt variations on input parameters)** is (T4 # T5), which involves interleaved fulfilment (T4: inject XSS probe strings into known URL parameters) and (T5: record manual XSS probe input results in known URLs) using a proxy tool. Formal behaviour annotation for G5 sub-attack (**steal**

session IDs, credentials, page content) is (T6; T7), which involves developing malicious JavaScript that is injected through vectors and sending information to the attacker first, followed by taking and causing the browser to execute. Formal behaviour annotation for (**exploit vulnerabilities)** (G5; G6 # G7) suggests stealing session IDs, credentials, and page content first, followed by forced browsing and content spoofing.

Event Model (EM): This model captures the security events E1: links recorded, E2: website explored, E3: visited links recorded, E4: known URLs injected, E5: results of manual input of XSS probes recorded: E6: information sent, E7: attacker's command executed by the browser, E8: action performed on the same website, E9: request executed to other website, and E8: invalid information exposed to the user. The two remaining analyses for user compromise and misconfiguration (phishing) utilise the same steps as previously explained. The framework has effectively described one attack pattern for user compromise attacks, one attack pattern for parallel attacks, four sub-attack mechanisms, and three domain assumptions. In addition, a grand total of eight tasks and eight security events have been captured following the enhancement of sub attacks and a behavioural annotation was performed. Two attack patterns, one primary and one parallel, have been identified for the type of attack referred to as misuse of resources (relative path traversal). In addition, one primary attack mechanism and three supplementary attack mechanisms were identified. Seven tasks were recorded in addition to three domain assumptions. Furthermore, an overall total of nine security incidents were recorded.

6. Discussion

6.1. Implications within the Realm of Cyber Physical-Systems

Research question (RQ1): upon analysing classifiers, it is clear that the primary direct impacts on the cyberinfrastructure of major service providers are denial-of-service and disruption. The incidence of these attacks has escalated during the surveyed timeframe. Many recorded cases of denial-of-service attacks explicitly attribute the cause to distributed denial-of-service (DDoS) attacks. Furthermore, a multitude of documented attacks suggest that the objective was to intentionally disrupt the resources of the website. Some denial-of-service attacks and disruptions have been associated with cyberinfrastructure intrusions, misuse of resources, and installation of malicious software. When evaluating the efficacy of denial of service attacks, 94% of them resulted in different levels of disruption.

A prior analysis suggests that a substantial proportion of denial-of-service attacks consist of distributed attacks targeting the resources of websites. Website disruptions may only affect external access, while internal informational resources for employees remain unaffected. Furthermore, attacks have the potential to result in denial-of-service. Although there is a declining pattern, social engineering attacks continue to be reported frequently. When compared to other types of attacks, social engineering and attacks that take advantage of insufficient authentication did not have a significant impact on the cyberinfrastructure of major service providers.

The trend may be due to the organisations' increased awareness of initial access attempts, as previously discussed. While the use of social engineering to illegally access user accounts has decreased, it still remains a significant part of reported malicious incidents for major service providers. Intrusions resulting in improper resource utilisation and denial-of-service attacks were common, while web compromise was less common. Nevertheless, this study fails to specify the exact length of time or the specific services that are most profoundly affected by these disruptions. Disruption was the top reported impact, followed by disclosure, with 16% citing a malicious event. More often than breaches of integrity or confidentiality, service disruptions or degradation occurred. Criticism of this study may point to bias in the criteria for reporting incidents by organisations.

Despite the assumption that service providers are vulnerable, this study demonstrates that many cyber incidents targeting an organisation's infrastructure do not have any reported impacts on the organisation or its stakeholders. There are multiple factors that can contribute to this situation. Major service providers show the necessary abilities to

minimise both the direct and indirect impacts of an attack. Furthermore, strong services or institutions within society have the capability to effectively alleviate the negative effects of numerous reported incidents. The analysis uncovered a small number of incidents that led to the destruction of information assets, suggesting that threat actors do not specifically focus on targeting them. This implies that critical service providers hold the capability to effectively avert such occurrences. While these findings do not definitively prove the futility of cyberattacks, they substantially challenge the idea that critical service providers and society in general are overly vulnerable to malicious attacks.

6.2. Behavioural Attack Pattern Analysis

Research Question 2: identifying potential attacks on a system is a vital aspect in developing secure systems, as it allows for determining the necessary security requirements. Analysing attacks in CPS provides a substantial challenge due to their ubiquitous occurrence. These systems contain individuals, entities, software systems, and tangible infrastructures. The Asfalia framework facilitates the analysis of attack patterns for critical service providers, covering the three realms of CPS. In addition, the framework facilitates cross-realm analysis and monitoring, allowing for the detection of security events that occur across different realms. Our models specifically target adversaries that are specific to each realm, encompassing the three realms of a CPS (cyber, physical infrastructure, and social).

We conducted an analysis of the interconnected relationships between attack models specific to different domains. The (AM) relies on the (VM) to reveal vulnerabilities that are specific to a particular realm. The vulnerabilities identified by the VM are then transferred to the next realm, which is the AM, and serve as inputs. Therefore, an appropriate attack strategy is chosen by exploiting the vulnerabilities of the VM.

Attack pattern: This refers to a broad description of an intentional and malicious opponent that often arises within a particular setting. This paper discusses the typical elements and techniques employed in cyberattacks targeting vulnerable components of (CPS). These patterns extrapolate reusable knowledge about common adversaries to aid in the analysis of security requirements for the system under consideration. An attack pattern comprises the overarching objective of the attack, the initial phase, the sequential actions to execute the attack, and the consequent outcome. Every attack pattern incorporates information regarding the design and execution of specific attack components, offering insights into the adversary's viewpoint on the issue, as well as guidance on how to minimise the impact of the attack. The (AM) relies on the (VM) as it formulates its offensive strategy by analysing the vulnerabilities discovered within the VM. Nevertheless, threats can be enhanced not only in a linear manner but also through iterative processes.

Hence, a thorough analysis of an attack requires an assessment of the strategic components related to the individuals and organisations involved, encompassing social and organisational factors. Furthermore, it is essential to consider the technical factors that affect software systems and physical infrastructure. This endeavour requires a significant level of expertise in security, which presents difficulties in terms of obtaining it. We initially concentrated on analysing the process of identifying an assailant's tactics by conducting a methodical analysis of their malicious intentions. Each attack strategy includes one or more anti-goals that define the malicious intentions of attackers, offering understanding into what and when they might intend to initiate an attack.

Although both the AVOIDIT and cyber harm taxonomy use advanced classifiers to classify attacks, it is possible that the categories they use are too abstract, which can lead to a lack of effective differentiation of attack characteristics. The gap was leveraged by utilising the Asfalia framework to analyse the attack characteristics and behaviours. Identifying attack strategies that are likely to be put into action is highly important in the context of targeted security analysis. However, a limited understanding of the future attacks presents a significant barrier to the analysis and implementation process. Analysts cannot precisely determine the techniques that potential attackers might use to attack a system, leading to the presence of either incorrect indications of attacks or missed indications of attacks

during the security analysis. The security community has curated an extensive repository of practical attack knowledge, encompassing 700 attack patterns, referred to as CAPEC. We aim to tackle the problem of knowledge deficiency by employing the attack patterns.

6.3. Threats to Validity

Access to major service provider cyber threat landscape data improved the study's validity, generalisability, and credibility. Although not all critical service providers must report incidents to MSB, the study's findings may be questioned. Different incident reporting and information inclusion criteria between government agencies and NIS organisations affect results. NIS organisations, unlike government agencies, do not need to report incidents that do not disrupt or degrade services, making a higher reporting threshold problematic.

Factors affecting subject performance were important in this study. We believe that the skills of the subjects involved in the experiment were appropriate for the objective of the preliminary evaluation. Moreover, regarding the security background of the analysts in this case study, it is important to note that all the authors have significant experience in the field of cyber security research. The participants were engaged in the development and analysis of security event models. Due to the absence of empirical evidence, it remains uncertain whether individuals without expertise in security can effectively utilise our approach. Nevertheless, our approach offers security patterns that facilitate the reuse of security knowledge by analysts.

7. Related Work

Altuhhova et al. use BPMN constructs to represent security-related concepts and model secure business process models [41], whereas Rodrguez et al. suggest an extension of the UML activity diagram to model security requirements as part of the business process model [42]. A rigorous procedure is suggested by [43] for the purpose of extracting and examining security requirements from business process models. The vast majority of effort is devoted to analysing software security requirements using techniques like attack tree [12], misuse case [44], and obstacle analysis [14]. Moreover, several proposals have been proposed to analyse and model attack scenarios, outlining steps to investigate how attackers execute an attack. Within the domain of the literature, there are numerous past studies that have focused mainly on devising techniques for simulating attack scenarios.

For instance, researchers used attack trees [12] and graphs [13] as a means to capture and represent attack scenarios. Unlike our approach, these efforts are somewhat constrained in their ability to precisely define the methods used in attack strategies. Security patterns have been acknowledged as an effective approach to designing system security. As a result, more than dozen security methodologies have been suggested, all of which are based on security patterns [45]. Uzunov et al. introduce a comprehensive pattern-driven security approach [30] that is specifically designed for general distributed systems. This approach is based on a substantial collection of well-documented security patterns [33].

This methodology encompasses both the stage of gathering and analysing requirements and the stage of designing in the software development lifecycle. During the requirement analysis stage, the first step is to gather secure use cases by identifying activities that involve misuse. In order to fulfil these secure scenarios, they next identify appropriate security solutions by employing security patterns. Once the security solutions have been selected for the design phase, they implement security solution frameworks. These frameworks include high-level security patterns and micro process patterns, which are used to create the design of the security system. A further study has been conducted to analyse and conceptualise threats, such as STRIDE [3]. However, STRIDE falls short in capturing the intentions of attackers and has certain limitations when it comes to addressing multi-stage attacks. Unlike this work, there have been several explicit proposals aimed at understanding the underlying motives of attackers by using anti-goals, as suggested by [14]. Alternative methodologies, surpassing the works of [14,15], have been suggested

for analysing security analysis by considering the perspective of an attacker and thoroughly analysing the malicious intentions of adversaries.

Our approach exhibits resemblances to these approaches in terms of attack models, anti-goal refinement, and the construction of attack scenarios. However, our approach improves this by examining behavioural models of security attack scenarios and applying them to construct runtime attack models. Furthermore, our approach simplifies the building of runtime behavioural models and the identification of security events for the purpose of monitoring security attacks.

8. Conclusions

The analysis of IT incident reports from Swedish service providers to MSB indicates that denial-of-service attacks and disruptions have the most significant effect on operations and information. Among the 254 cyberattacks analysed, a significant number did not result in any apparent direct or indirect impacts. In many cases, social engineering attacks had minimal immediate impacts. While the occurrence of social engineering for initial access and user attacks is declining, it still remains widespread. Instances of malware infection are minimal. The IT incident reports revealed a limited number of malicious incidents that compromised the information resources of significant service providers.

The experiment has categorised the attack patterns according to the domain and method of attack.

Mechanism-Based Attack: The attack patterns are structured hierarchically, taking into account the commonly utilised mechanisms for exploiting vulnerabilities. The attack patterns encompassed within this category exemplify the diverse methodologies employed in targeting a system. Nevertheless, the aforementioned attacks do not adequately depict the resultant ramifications or objectives.

Domain-Based Attack: The attack patterns are organised in a hierarchical manner, taking into consideration the attack domain. Attacks encompassing various techniques, including social engineering, supply chain, communication, physical security, and others, are classified within this category. We performed a behavioural attack pattern analysis using the Asfalia framework, specifically developed for monitoring and analysing security events in CPS. The analysis was performed using IT incident reports obtained from critical service providers to MSB. The use of the framework was essential in order to make the analysis and documentation of security events, behavioural models, and their annotations possible, given the significant scale of the scenario.

The analysis of attack patterns resulted in the identification of five security attacks, seven vulnerabilities (also known as threats), ten attack patterns, and ten parallel attack patterns. Furthermore, the framework effectively specified a comprehensive set of 24 attack mechanisms, 32 specific tasks, 23 behavioural annotations, 10 domain assumptions, and 35 security events. The analysis indicates that the security incidents used in the experiment can be categorised into specific attack patterns based on their behaviours, such as password recovery exploitation, authentication abuse, buffer overflows, cross-site scripting, phishing, and brute force attacks. Our framework offers the benefit of assisting security analysts in their analysis of security events and the creation of security solutions for essential service providers. More precisely, the VM captures the malicious individuals and weaknesses and then analyses the target of the attack using a specialised approach specific to the domain. The AM constructs an attack model by exploiting the adversaries specified in the VM. The behavioural model (BM) provides annotations for the (VM) and (AM). In (EM), events are derived from behavioural models.

There is a need for research on incident severity using indirect impact indicators. The incidents were categorised based on the type of component. Studying how DDoS attacks contribute to the prolonged duration of critical service downtime would be noteworthy. The experimental results indicate that the primary limitation of the current framework is the requirement for users to have a high level of proficiency in both modelling and security. Further experiments will include different combinations of users, including individuals

with proficiency in modelling but little knowledge in security, as well as those with expertise in security but limited knowledge in modelling. Hence, it is important to enhance Asfalia prior to undertaking a further evaluation.

Author Contributions: Conceptualization, E.S., O.P. and F.B.; Methodology, E.S.; Formal analysis, E.S.; Validation, E.S. and O.P.; Supervision, O.P. and F.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We extend our appreciation to Josefin Andersson, a student at Stockholm University, for her diligent work in collecting and classifying the report. In addition, we would like to extend our appreciation to MSB for their cooperation.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Urbach, N.; Roeglinger, M. *Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age*; Springer: Berlin/Heidelberg, Germany, 2019
2. Ponemon, L. *Cost of Data Breach Study: Global Analysis*; Technical Report; Poneomon Institute: Traverse City, MI, USA, 2015.
3. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA , 2014.
4. Markopoulou, D.; Papakonstantinou, V. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Comput. Law Secur. Rev.* **2021**, *41*, 105502. [CrossRef]
5. Engebretson, P.H.; Pauli, J.J. Leveraging parent mitigations and threats for capec-driven hierarchies. In Proceedings of the Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 26–29 April 2009; pp. 344–349.
6. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
7. Seid, E.; Popov, O.; Blix, F. Security Attack Event Monitoring for Cyber Physical-Systems. In Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, 22–24 February 2023; Mori, P., Lenzini, G., Furnell, S., Eds.; SciTePress: Setubal, Portugal, 2023; pp. 722–732.
8. Panda, A.; Bower, A. Cyber security and the disaster resilience framework. *Int. J. Disaster Resil. Built Environ.* **2020**, *11*, 507–518. [CrossRef]
9. Papakonstantinou, V. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Comput. Law Secur. Rev.* **2022**, *44*, 105653. [CrossRef]
10. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proc. IEEE* **2012**, *100*, 283–299. [CrossRef]
11. Moore, A.P.; Ellison, R.J.; Linger, R.C. *Attack Modeling for Information Security and Survivability*; Technical Report; Carnegie-Mellon University in Pittsburgh: Pittsburgh, PA, USA, 2001.
12. Schneier, B. Attack trees. *Dr. Dobb J.* **1999**, *24*, 21–29.
13. Phillips, C.; Swiler, L.P. A graph-based system for network-vulnerability analysis. In Proceedings of the 1998 Workshop on New Security Paradigms, Charlottesville, VA, USA, 22–25 September 1998.
14. Van Lamsweerde, A. Elaborating security requirements by construction of intentional anti-models. In Proceedings of the 26th International Conference on Software Engineering, Edinburgh, UK, 23–28 May 2004; IEEE Computer Society: Washington, DC, USA; pp. 148–157.
15. Li, T.; Horkoff, J.; Paja, E.; Beckers, K.; Mylopoulos, J. Analyzing attack strategies through anti-goal refinement. In *IFIP Working Conference on The Practice of Enterprise Modeling*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 75–90.
16. Calderaro, A.; Blumfelde, S. Artificial intelligence and EU security: The false promise of digital sovereignty. *Eur. Secur.* **2022**, *31*, 415–434. . [CrossRef]
17. Hsieh, H.F.; Shannon, S.E. Three approaches to qualitative content analysis. *Qual. Health Res.* **2005**, *15*, 1277–1288. [CrossRef]
18. Osei-Kyei, R.; Tam, V.; Ma, M.; Mashiri, F. Critical review of the threats affecting the building of critical infrastructure resilience. *Int. J. Disaster Risk Reduct.* **2021**, *60*, 102316. [CrossRef]
19. Caldarulo, M.; Welch, E.W.; Feeney, M.K. Determinants of cyber-incidents among small and medium US cities. *Gov. Inf. Q.* **2022**, *39*, 101703. [CrossRef]
20. Agrafiotis, I.; Nurse, J.R.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J. Cybersecur.* **2018**, *4*, tyy006. [CrossRef]
21. Kaiya, H.; Kono, S.; Ogata, S.; Okubo, T.; Yoshioka, N.; Washizaki, H.; Kaijiri, K. Security requirements analysis using knowledge in capec. In *Advanced Information Systems Engineering Workshops*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 343–348.
22. Boin, A. The transboundary crisis: Why we are unprepared and the road ahead. *J. Contingencies Crisis Manag.* **2019**, *27*, 94–99. [CrossRef]

23. Harry, C.; Gallagher, N. Classifying cyber events. *J. Inf. Warf.* **2018**, *17*, 17–31.
24. Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making? *Int. J. Disaster Risk Reduct.* **2018**, *27*, 632–641. [CrossRef]
25. Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 1–12.
26. Mitnick, K.D.; Simon, W.L. *The Art of Deception: Controlling the Human Element of Security*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
27. Shevchenko, P.V.; Jang, J.; Malavasi, M.; Peters, G.W.; Sofronov, G.; Trück, S. The nature of losses from cyber-related events: Risk categories and business sectors. *J. Cyberse-Curity* **2023**, *9*, tyac016. [CrossRef]
28. Van den Berg, B.; Kuipers, S. Vulnerabilities and Cyberspace: A New Kind of Crises. In *Oxford Research Encyclopedia of Politics*; Universiteit Leiden—LUMC: Leiden, The Netherlands, 2022.
29. Wang, E.K.; Ye, Y.; Xu, X.; Yiu, S.-M.; Hui, L.C.K.; Chow, K.-P. Security issues and challenges for cyber physical system. In Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, Hangzhou, China, 18–20 December 2010; pp. 733–738.
30. Uzunov, A.V.; Ferncez, E.B.; Falkner, K. Engineering security into distributed systems: A survey of methodologies. *J. UCS* **2012**, *18*, 2920–3006.
31. Gopstein, A.; Gopstein, A.; Nguyen, C.; Byrnett, D.S.; Worthington, K.; Villarreal, C. *Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
32. Mancuso, V.F.; Strang, A.J.; Funke, G.J. ; Finomore, V.S. Human factors of cyber attacks: A framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Chicago, IL, USA, 27–31 October 2014; SAGE Publications: Los Angeles, CA, USA, 2014; Volume 58, pp. 437–441.
33. Uzunov, A.V.; Fernandez, E.B.; Falkner, K. Ase: A comprehensive pattern-driven security methodology for distributed systems. *Comput. Stand. Interfaces* **2015**, *41*, 112–137. [CrossRef]
34. Simmons, C.; Ellis, C.; Shiva, S.; Dasgupta, D.; Wu, Q. AVOIDIT: A Cyber Attack Taxonomy. In Proceedings of the 9th Annual Symposium on Information Assurance, Kyoto, Japan, 4–6 June 2014; pp. 12–22.
35. Derbyshire, R.; Green, B.; Prince, D.; Mauthe, A.; Hutchison, D. An analysis of cyber security attack taxonomies. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 24–26 April 2018; pp. 153–161.
36. Whyte, C. European Union: Policy, cohesion, and supranational experiences with cybersecurity. In *Routledge Companion to Global Cyber-Security Strategy*; Routledge: London, UK, 2021; pp. 201–210.
37. Yuan, X.; Nuakoh, E.B.; Beal, J.S.; Yu, H. Retrieving relevant capec attack patterns for secure software development. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 8–10 April 2014; pp. 33–36.
38. Simmons, C.; Ellis, C.; Shiva, S.; Dasgupta, D.; Wu, Q. *AVOIDIT: A Cyber Attack Taxonomy*; Technical Report CS-09-003; University of Memphis: Memphis, TN, USA, 2009.
39. Rashid, S.Z.U.; Haq, A.; Hasan, S.T.; Furhad, M.H.; Ahmed, M.; Barkat Ullah, A.S. Faking Smart Industry: A Honeypot-Driven Approach for Exploring Cyber Security Threat Landscape. In Proceedings of the International Conference on Cognitive Radio Oriented Wireless Network and Wireless Internets, Virtual Event, 11 December 2021; Springer International Publishing: Cham, Switzerland, 2021; Volume 427, pp. 307–324.
40. Fernandez-Buglioni, E. *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
41. Altuhhova, O.; Matulevičius, R.; Ahmed, N. Towards definition of secure business processes. In *Advanced Information Systems Engineering Workshops*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 1–15.
42. Rodríguez, A.; Fernández-Medina, E.; Trujillo, J.; Piattini, M. Secure business process model specification through a uml 2.0 activity diagram profile. *Decis. Support.* **2011**, *51*, 446–465. [CrossRef]
43. Herrmann, P.; Herrmann, G. Security requirement analysis of business processes. *Electron. Commer. Res.* **2006**, *6*, 305–335. [CrossRef]
44. Sindre, G.; Opdahl, A.L. Eliciting security requirements with misuse cases. *Requir. Eng.* **2005**, *10*, 34–44. [CrossRef]
45. Høyland, S.A. Exploring and modeling the societal safety and societal security concepts—A systematic review, empirical study and key implications. *Saf. Sci.* **2018**, *110*, 7–22. [CrossRef]