Improving Incident Management Processes with Feature Models

Karam Mustafa Ignaim[1,*] and João M. Fernandes[2]

[1]*Al-Balqa Applied University, Salt, Jordan*
[2]*Universidade do Minho, Centro ALGORITMI, Braga, Portugal*
E-mail: karam.ignaim@bau.edu.jo; jmf@di.uminho.pt
[*]*Corresponding Author*

Received 19 November 2023; Accepted 13 March 2024

Abstract

A cybersecurity incident is any event that directly or indirectly affects the confidentiality, availability, or integrity of a system or a service (or its data). The aim of a cyber-incident management process is to restore normal service levels as quickly as possible, by mitigating or eliminating the effects of system service disruptions. During the different phases of a cyber-incident management process, the documentation can be confusing and difficult to comprehend, making it ineffective. This paper aims to improve cyber-incident management processes that already exist by introducing feature models in order to handle incident documentation, classification, prioritisation, and mitigation. An example of an improved cyber-incident process is evaluated with respect to its efficiency and effectiveness, by conducting two case studies. The results of this work reveal that the improved process increases efficiency in addressing and repairing cyber-incidents by reducing the incident response time.

Keywords: Incident management process, cyberattack, incident response team, feature model.

Journal of Cyber Security and Mobility, Vol. 13_4, 701–724.
doi: 10.13052/jcsm2245-1439.1346

1 Introduction

In the ever-changing cybersecurity landscape of the present day, every organisation, regardless of its size, nature, or industry, is exposed to cyberattacks. Cyberattacks have become a major concern for many organisations, posing serious threats to the security and functionality of various systems and networks [1]. A cyber-incident can rapidly escalate into a business crisis, resulting in financial losses, legal consequences, operational disruption, and reputational harm [2]. Thus, organisations are increasingly investing in cyber-incident management processes to detect, respond to, and recover from these incidents [3]. A cyber-incident is defined as any unauthorised access, disclosure, disruption, or destruction of information or systems, whether intentional or accidental [4, 5].

Several approaches have been proposed to address cyber-incidents [6–9], but most of them do not guarantee complete prevention [10]. It is essential for organisations to adopt an approach that includes rigorous documentation of incident response procedures, regular training for the incident response team (IRT), and constant monitoring and updating of security measures [4]. This comprehensive approach ensures that the organisation is well-prepared to identify, control, and mitigate cyber-incidents in a timely manner.

There has been a significant amount of research conducted on the subject of improving cyber-incident processes [11–17]. A cyber-incident needs to be documented clearly to ensure that all relevant information is captured and can be analysed for future reference [4]. As the cyber-incident community continues to document incidents, there is a need for reflection on how information is captured and how taxonomies can either facilitate or impede meaningful analysis [18]. This documentation includes details such as the date and time of the incident, the actions taken by the IRT, and any vulnerabilities or weaknesses in the system that were exploited. By clearly documenting cyber-incidents, organisations can track patterns and trends, identify areas for improvement, and develop more effective strategies for preventing and mitigating future attacks. However, traditional cyber-incident management processes often lack the flexibility and efficiency necessary to handle the ever-evolving nature of cyberattacks. Therefore, this research proposes an improved cyber-incident management process that leverages feature models (FMs) [19] to address the limitations of existing approaches. The FMs are incorporated into the incident documentation, prioritisation, and mitigation phases.

The novelty of the proposed work lies in applying FMs to cyber-incidents management process, which, to our knowledge, has not been explored before. This approach can provide a systematic and flexible way to manage cyber-incidents, allowing organisations to effectively address and mitigate the impact of such incidents. By using FMs, one can identify the key features of cyber-incidents and use them to create customisable incident response plans tailored to their specific needs and requirements. This can lead to more efficient and effective incident response, reducing the overall impact of cyber-incidents on organisations.

The capacity of FMs to systematically categorise and prioritise features (of systems) justifies their use in this work [20–22]. FMs are known as one of the key models used in software product line engineering [19, 23]. They provide a systematic way to represent and manage the common and variable parts of a set of related software products [24]. In this study, FMs are used to capture, to analyse, and to improve the different aspects of the cyber-incident management process. By using FMs, one is able to identify the essential features that contribute to the efficiency of the IRT and to determine the necessary steps for improvement. This approach provides a valuable improvement to cyber-incident management capabilities. We conducted two case studies to evaluate the performance of the improved process and compare it with the existing one. The results reveal that the improved process significantly reduces the mean time to repair (MTTR) after an incident is handled and improves the overall incident resolution.

1.1 Contributions

Our study contributes to the existing body of knowledge on cyber-incidents from several perspectives.

Firstly, this study builds upon prior research by employing a systematic methodology to resolve cyber-incidents. Previous research has proposed similar concepts, (e.g., [11–14]). However, there is no comprehensive study that promotes the usage of feature modelling methods in the context of cyber-incident management processes.

Secondly, the majority of the research on cyber-incident management processes has been defined and applied to specific fields (e.g., [11, 25–27]). While the first case study in the evaluation of our work is drawn from the e-commerce sector, this paper includes a second case study that is focused on several sectors where cyber-incidents can occur.

Thirdly, our work sets up a foundation for the research community to conduct further research on feature-based incident responses by elaborating on or adapting the feature-based process. We also show that the feature modelling technique can be integrated within a traditional cyber-incident process through targeted refinements and improvements to the baseline incident response, while allowing for the flexibility of the response.

1.2 Challenges of the Study

When a cyber-incident occurs, it is often unclear what information should be recorded about the incident. Currently, the data that are tracked are largely driven by compliance for reporting requirements and valuable information is not recorded, or information is not recorded in a way that makes analysis easy. For example, incidents are often documented in unstructured reports that require a manual analysis to identify trends. Explicitly recording certain data in a structured form makes analysis much more accurate and efficient.

1.3 Structure of the Paper

The rest of the paper is organised as follows. Section 2 provides an overview of previous works on cyber-incident management processes. Section 3 describes the major aspects of feature models. Section 4 presents the feature-based cyber-incident management process (FbCIMP), the central part of this paper. Section 5 illustrates the use of the FbCIMP with an example. The evaluation of the FbCIMP is discussed in Section 6. An analysis of the threats to the validity of the evaluation of the work is presented in Section 7. Section 8 concludes the paper and indicates some possible future work.

2 Related Work

There have been numerous prior studies conducted in field related to cyber-incident management processes. The majority of them appear to place significant reliance on standards, such as ITIL 4. The majority of research efforts in this domain can be categorised into two distinct fields: (1) theoretical approaches, which provide a series of principles to adhere to throughout the incident management life cycle, and (2) the availability of both free and commercial solutions for addressing incident management scenarios. Latrache et al. [10] tackle the challenges faced by existing incident management systems, by proposing a solution that uses the ITIL standard and

multi-agent technology. This ensures a streamlined and automated incident handling process, eliminating the complexities associated with current systems. Furthermore, the authors introduce a semantic matchmaking algorithm to improve the accuracy and efficiency of incident matching. Overall, their approach aims to provide a more effective and user-friendly incident management system.

Ruskojärvi [28] developed a security incident management process for a network operation centre and conducted testing of these processes in a controlled laboratory setting. Additionally, an action plan for ongoing improvement was devised. The objective of this study was to develop operational procedures and protocols that are effective and capable enough to effectively address security issues.

Kettunen [4] highlights the importance of communication and collaboration skills, for effective incident management. He also stresses the need for technical expertise in cybersecurity and the ability to quickly analyse and respond to security incidents. Additionally, the author recommends the development of leadership and decision-making skills to ensure efficient management of the virtual security IRT. By implementing these recommendations, the organisation can navigate the organisational changes successfully and establish a robust security incident management process.

Oriola et al. [7] implemented a collaborative-based national cybersecurity incident management system that brings together different stakeholders, such as government agencies, private companies, and cybersecurity experts. The system allows for real-time information sharing and coordination among these stakeholders, enabling a faster response to cyber-incidents. Additionally, the system incorporates advanced analytic and machine learning algorithms to identify and mitigate cyberthreats more effectively. Overall, the results demonstrate the effectiveness and reliability of the proposed collaborative approach in improving the cybersecurity posture of the information and communication technology ecosystem.

Kuhn [6] explored the importance of the Expanded Incident Life-cycle and its impact on the overall quality of IT services. By understanding and implementing this concept, IT professionals can effectively manage incidents and ensure timely resolution. The author also discussed how each stage of the lifecycle plays a crucial role in maintaining customer satisfaction and minimising downtime. Additionally, real-life examples and practical tips were provided to illustrate the practical application of the Expanded Incident Life cycle in different IT environments.

To our knowledge, there were no previous works on the use of FMs in cyber-incidents management. The works that utilise FMs tackle software engineering problems, such as software maintenance, emergence repair requests, and requirement engineering tasks [29].

With respect to previous work related to cyber-incident management process, this work also contributes to cyber-incident documentation and prioritisation by providing a structured approach to categorising and documenting incidents based on their features. This allows organisations to prioritise their response efforts based on the severity and potential impact of each incident. Additionally, the use of FMs enables organisations to continuously improve their incident response plans by identifying common features across incidents and implementing proactive measures to prevent future occurrences. Overall, this work continues and expands the previous scientific efforts in the field of cyber-incidents management by providing a structured framework that improves incident response capabilities. Furthermore, the use of FMs enables organisations to tailor their incident management strategies to their specific needs and requirements. This approach also facilitates the identification of potential gaps or weaknesses in the documentation and prioritisation of the incident response process, allowing for continuous improvement and refinement. Ultimately, the application of FMs in cyber-incidents management contributes to improving the overall cybersecurity process.

3 Feature Models

An FM depicts the common and variable features of concept instances, as well as their interdependencies [30]. Each FM depicts in a tree a set of features and their interrelationships. Relationships between a parent feature and its child features (or sub-features) are categorised as:

- **Mandatory features** are required in the concept instance.
- **Optional features** are optional in the concept instance.
- **Or features**, in which one or more must be selected if the parent feature is selected.
- **Alternative features**, where exactly one sub-feature must be selected if the parent feature is selected.

Figure 1 depicts some graphical elements, including relationships, that can be used in FMS. Besides these relationships, FMs allow propositional logic formulas about features (i.e., dependencies among the features) to be expressed. For instance, the formula “Camera requires High Resolution” states that if

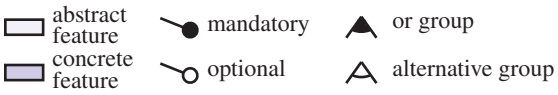

Figure 1 The notations of FMs.

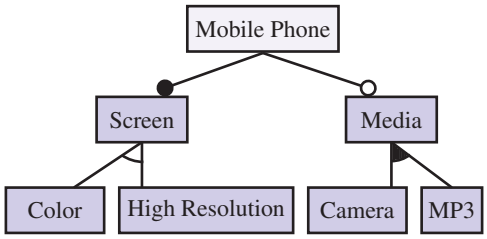

Figure 2 FM example from mobile phone domain.

the Camera feature is selected, the High Resolution feature must be selected (see Figure 2).

FM represent all the possible (valid) configurations of the model. For example, the configurations {Mobile Phone, Screen, Colour, Media, MP3} and {Mobile Phone, Screen, Colour, Media, Camera} are valid for the model in Figure 2. However, the configuration {Mobile Phone, Screen, Colour, Media} is invalid because the Or relationship among Media, Camera, and MP3 states that whenever Media is chosen, either Camera or MP3 must be selected.

4 Feature-based Cyber-incident Management Process

4.1 Problem Statement

The current cyber-incident management documentation can be confusing and hard to comprehend [4]. The cyber-incident process should be well-documented, yet straightforward enough for anyone to comprehend it. The cyber-incident management process should function in such a way that incidents can be prioritised and resolved swiftly, and that we can learn from previously resolved incidents. The cyber-incident management process needs to be continuously updated and developed in order to meet the demands of the future, just like any other process within an organisation. Moreover, the roles of participants in the security incident management process should be clear to the members of the IRT, who are responsible for mitigating the impact of incidents and assisting the business in resuming operations as quickly as

is feasible [31], and to those who need to report incidents. Without this, the cyber-incident management process does not function properly, resulting in standstills and potentially unreported incidents.

4.2 The Improved Process

In this section, we present a feature-based cyber-incident management process (FbCIMP). As the baseline, we use the cyber-incident management process (Figure 3), which is improved with feature modelling. The purpose of the improved process is to minimise the negative impact of incidents by restoring normal service operations as quickly as possible.

We propose the use of FMs to handle incident requests. This choice aims to benefit from the flexibility and adaptability provided by FMs. By using FMs, the incident management process can be improved, by allowing for easier customisation of incident requests based on the specific needs and requirements of the organisation. This results in a more efficient and effective incident management process, leading to a higher likelihood of incidents being reported and addressed in a timely manner. Additionally, FMs can also help in identifying and prioritising incident response actions, ensuring that resources are allocated appropriately to mitigate the potential impact of future security incidents. The steps of the cyber-incident process are as follows:

- **Identification:** This step involves detecting and recognising an incident, either through proactive monitoring or by receiving reports from users or an IRT.

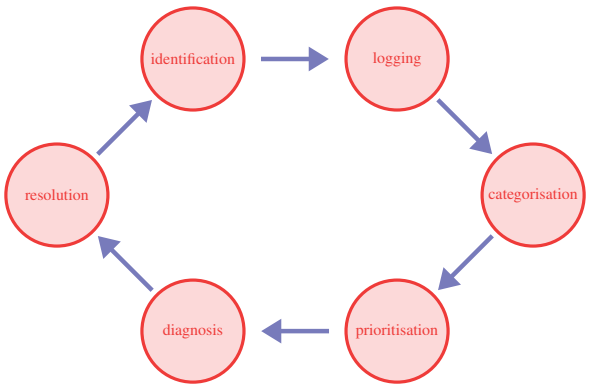

Figure 3 The cyber-incident management process.

- **Logging:** Once an incident is identified, it is important to record all relevant information about the incident, including its description, impact, and urgency.
- **Categorisation:** In this step, incidents are categorised based on their nature and impact, which helps prioritise their resolution. For this purpose, incidents are categorised by severity, impact, and service level agreement constraints.
- **Prioritisation:** Incidents are then prioritised based on their urgency and impact on the organisation, ensuring that the most critical ones are addressed first.
- **Diagnosis:** This step involves investigating the root cause of the incident to determine the relevant characteristics of the occurred incident and the underlying issue that needs to be resolved, and assigning the proper responsibilities for the IRT.
- **Resolution:** Once the root cause of the incident is identified and a solution is found, actions are taken to resolve the incident.

As shown in the top of Figure 4, the improved FbCIMP involves two main phases: (1) record and (2) manage. The record phase handles the identification and logging of incidents. Once the IRT identifies or gets notified about the incident, it captures enough information about it, including its type, time, and source. As depicted in Figure 4, during the logging step, the IRT models a cyber-incident FM that contains several features, like Incident ID, Source, and Time, that help to record and monitor incidents. The record phase becomes the basis for the management phase, which includes the categorisation, prioritisation, diagnosis, and resolution steps.

In the categorisation step, the IRT classifies and categorises the incident according to a specific scheme (i.e., set of criteria). As presented in Table 1, each incident criterion represents a parent feature (e.g., Incident Type is a parent feature) and the values of the criterion represent a sub-feature of the FM (e.g., cyberattack is a sub-feature). The IRT records the classification information of the cyber-incident in a sub-FM of the cyber-incident FM, which is designated, in this work, as the categorisation sub-FM (the part marked with a red line in Figure 6). The priority of an incident is typically determined in the prioritisation step by assessing its impact and urgency. It requires careful consideration of the unique circumstances surrounding each incident. The IRT records the prioritisation of incidents in the form of a sub-FM in the cyber-incident FM (Figure 7).

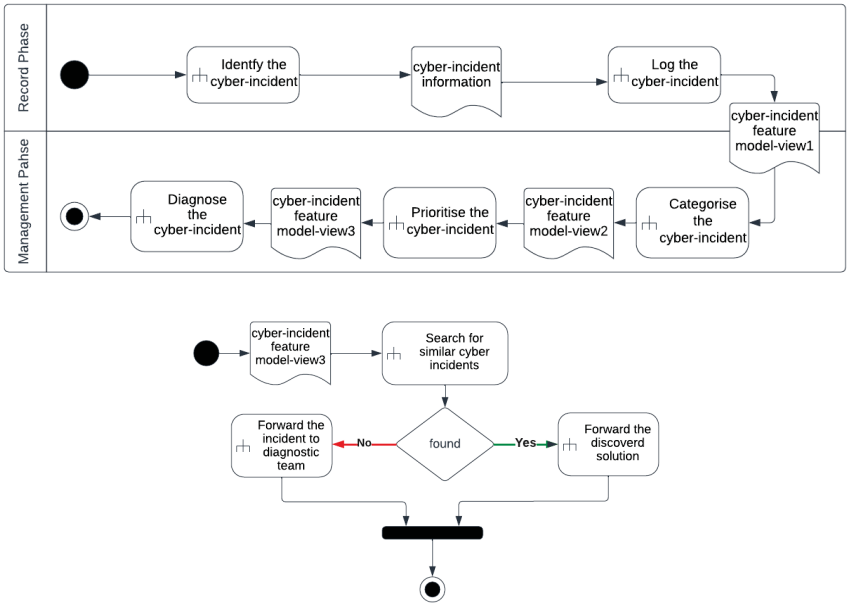

Figure 4 (top) The FbCIMP for a single cyber-incident; (bottom) the steps of the diagnosis activity.

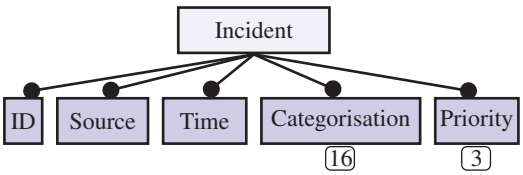

Figure 5 Abstract FM of a cyber-incident: view 1. The number inside a rounded rectangle represents the number of features in the subtree of a collapsed feature. Collapsing a feature hides its subtree to ease the visualisation.

Table 1 Classification of cyber-incidents

Feature	Incident Type	Incident Severity	Affected Service
	cyberattack	low	avionics
	system compromise	medium	communication systems
sub-feature	malware infection	high	flight control
	inside threat	critical	
	website defacement		

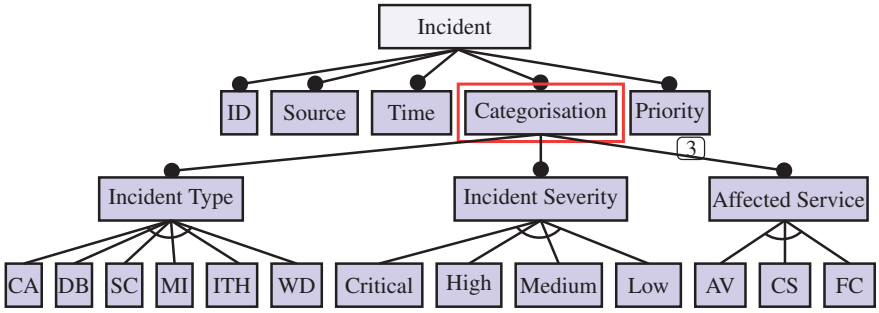

Figure 6 Abstract sub-FM of a cyber-incident: view 2. CA: cyberattack, DB: data breach, SC: system compromise, MI: malware infection, ITH: insider threat, WD: website defacement, AV: avionics CS: communication systems, FC: flight control.

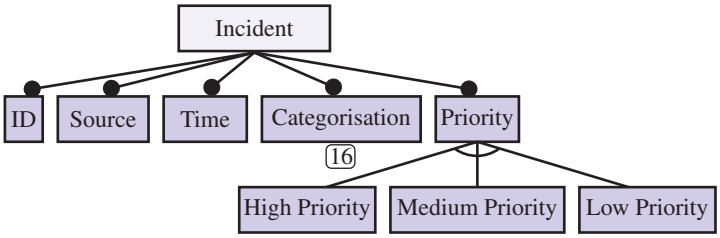

Figure 7 Abstract FM of a cyber-incident: view 3.

After recording the information related to the cyber-incident in the FM, in the diagnosis step, the IRT starts to search in the FM for similar incidents previously solved in order to minimise the response time and the resources consumed. Based on the result of the feature-based incident matching process, one of the following activities is performed:

- If the presented incident has already occurred and was resolved, the IRT forwards the discovered solution in the FM to the requester and calculates the productivity rate.
- If the provided occurrence occurs for the first time, the IRT forwards the gathered information to the diagnosis team.

4.3 Feature-based Incident Matching Process

Once an incident has been recorded and categorised, the IRT examines past incidents (represented in this work by cyber-incident FMs) for similar incidents that have already been detected and resolved. As shown in Figure 8, one form of incident information is captured using a specified XML

```
<and abstract="true" mandatory="true" name="Categorization">
    <graphics key="collapsed" value="false"/>
    <alt mandatory="true" name="Incident Type">
        <graphics key="collapsed" value="false"/>
        <feature name="cyberattack"/>
        <feature name="data breach"/>
        <feature name="system compromise"/>
        <feature name="malware infection"/>
        <feature name="insider threat"/>
        <feature name="website defacement"/>
    </alt>
    <alt mandatory="true" name="Incident Severity">
        <graphics key="collapsed" value="false"/>
        <feature name="Critical"/>
        <feature name="High"/>
        <feature name="Medium"/>
        <feature name="Low"/>
    </alt>
    <alt mandatory="true" name="Affected Service">
        <feature name="avionics"/>
        <feature name="communication systems"/>
        <feature name="flight control"/>
    </alt>
</and>
```

Figure 8 The XML format of the categorisation sub-FMs.

```
<alt name="Incident Type">
<feature name="Value"/>
<alt name="Incident Severity">
<feature name="Value"/>
<alt name="Affected Service">
<feature name="Value"/>
```

Figure 9 The XML matching tags.

representation (*ID*, *Time, Source*, *Incident Type*, *Incident Severity*, *Affected Service*). The proposed feature-based incident matching algorithm follows the work presented in [10]. In the matching process, we are just interested in the information included in the matching tags, as shown in Figure 9.

The matching between incidents is based on comparing the current incident with the past incidents to find any similarities, including *Source*, *Incident Type*, *Incident Severity*, and *Affected Service* tags. To accomplish this task, the matching algorithm employs semantic matching techniques, which means that the matching between incidents is not syntactic but rather based on their relationship. Based on previously recorded incident information, this matching represents the shared vocabulary for incidents. On the other hand,

because it is based on semantic principles, the key advantage of this process is that it improves the accuracy of the matching process.

The matching algorithm employed for incident representations recognises four distinct degrees: (i) *exact matching* refers to the scenario where two incidents are identical in all aspects (i.e., the current incident matches one of the past incidents); (ii) *includeIn matching* occurs when the current incident includes one of the past incidents; (iii) *subsume matching* is similar to includeIn but the current incident is more generic than all of the past incidents; and (iv) *fail matching* is when incidents are different, i.e., the current incident does not match any one of the past incidents. When an incident matching request is made, the IRT performs a calculation to determine the similarity degree (SD) between the current incident and the past incidents regarding the matching tags, according the following alternatives:

- SD $= 3$, if the current incident matches the past incident.
- SD $= 2$, if the current incident includes the past incident.
- SD $= 1$, if the current incident is more generic than the past incident.
- SD $= 0$, if the current incident does not match the past incident.

The final SD is calculated by the IRT based on the average of the SDs. If the SD is higher than the threshold (SD > 2), the current incident and the past incident are similar. In this case, the past incident has a high possibility of containing a solution that satisfies the current incident. When the final SD is between one and the threshold ($1 \leq$ SD ≤ 2), the past incident is a possible candidate to satisfy the current incident (i.e., *includeIn* and *subsume matching*). In another case, where there is no match between the current incident and past incident, the IRT needs to find a solution to resolve the incident. This process ensures that incidents are handled efficiently and effectively, minimising any impact on the system or services.

5 Running Example

This section presents an illustrative example of the use of the FbCIMP. To explain the steps of the proposed process, the running example illustrates a scenario in which a software development team is responsible for creating a new e-commerce website. A relevant feature of this website is the inclusion of a "Shopping Cart" functionality. In the record phase, customers report an incident—a problem with the Shopping Cart feature. They state that *when they try to add items to the cart, the system adds multiple expensive items to their shopping cart without their knowledge*. As shown in Figure 10, in the

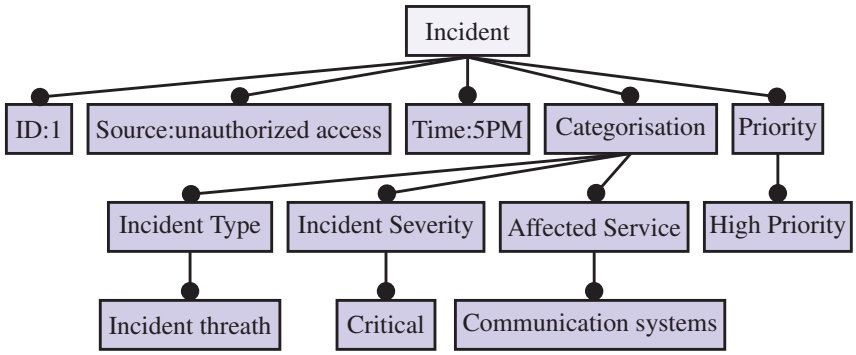

Figure 10 The FM of the recorded cyber-incident.

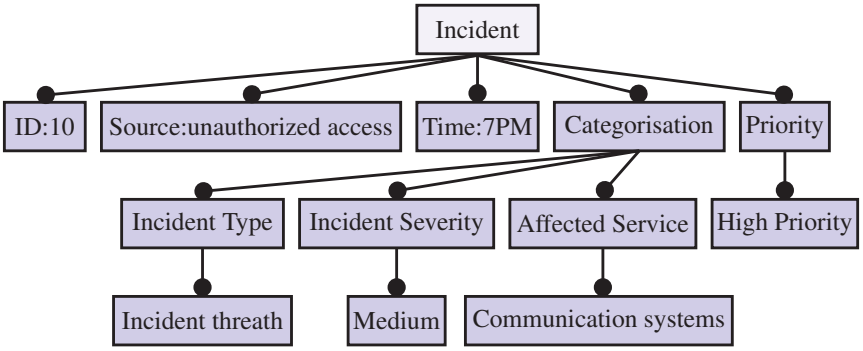

Figure 11 The FM of the past cyber-incident.

logging step, the IRT records the incident information in an FM with respect to the following features: ID, Source, Time, Incident Type (shopping cart error), Incident Severity, Affected Service, and Priority.

The management phase starts with the categorisation of the incident. As shown in Figure 10, the IRT builds the categorisation sub-FM. Additionally, in the prioritisation step, the team assigns a prioritisation degree (i.e., High Priority) to the incident. In the diagnosis step, the IRT starts to search in the past incidents/FMs for similar incidents previously solved. The matching process produces a matching between the current incident (Figure 10) and one of the past incidents (Figure 11) with SD $= 2$. The SD is between one and the threshold. This implies that the past incident contains a possible candidate solution to satisfy the current incident. At this time, the incident is assigned to a developer responsible for the Shopping Cart feature. He is tasked with

fixing the problem based on the candidate solution (diagnosis and resolution steps).

6 Evaluation

To illustrate the usefulness of the proposed process and its potential to improve the traditional cyber-incident management process, two case studies were conducted.[1] While the first case study was undertaken in the setting of e-commerce, the second one was implemented among the most sensitive industries to cyberattacks.

In both cases, the MTTR metric is used, since it is critical to measure the efficiency of incident management processes. MTTR is the average time that it takes to repair a system, after an incident has occurred. In the evaluation of the proposed process, MTTR is useful in tracking how fast the IRT was able to repair the systems under consideration. Thus, the metric measures how swiftly the IRT can repair the system. The goal is to keep the number as low as possible by increasing efficiency.

6.1 Case Study #1

The first case study was conducted at one company that is related to the e-commerce domain. We aimed to obtain initial feedback on the usability of the proposed process in order to decide if it was worthwhile to continue with a formal case study. We compared the proposed process with a similar cyber-incident management process (baseline process, Figure 3) according to the MTTR metric. We collected data for the MTTR of both processes over a one-month period (while the IRT responded to e-commerce incidents) and analysed the results. The incidents are related to the Shopping Cart feature presented in Section 5. A cyber-incident involving the shopping cart of an e-commerce website typically refers to a security breach or issue that affects the functionality, integrity, or privacy of the online shopping cart system. Table 2 presents the cyber-incidents related to e-commerce shopping carts. To evaluate the proposed process, we asked the IRT[2] of the company to resolve incidents (Table 2) using both the cyber-incident management process (CIMP) and the FbCIMP. Thus, we formulate the following hypotheses:

[1] They are presented at https://github.com/karamignaim/CICS.

[2] Due to confidentiality issues, the name of the company is not disclosed.

Table 2 The cyber-incidents involved in the e-commerce website

ID	Incident
1	**Data breach**: Hackers gain unauthorised access to the platform database.
2	**Payment gateway**: Hackers breach the payment gateway integrated with the shopping cart.
3	**Phishing campaigns**: Hackers send phishing emails or create fraudulent websites that mimic the e-commerce site shopping cart.
4	**Software update vulnerabilities**: Failure to apply security patches and updates to the shopping cart software can leave it vulnerable to known exploits.

- H_0: FbCIMP is **less** efficient in resolving and preventing incidents compared to CIMP.
- H_1: FbCIMP is **more** efficient in resolving and preventing incidents compared to CIMP.

As shown in Table 3, the analysis of the results show that our process has a significantly lower MTTR records compared to the baseline process over the weeks under evaluation. This indicates that the proposed process is effective in reducing downtime and resolving incidents more efficiently. Further, it means that our process is more efficient in reducing the MTTR compared to the baseline process. The lower MTTR records indicate that our process can resolve issues and restore normal operations faster, leading to reduced downtime and improved productivity. These findings validate the effectiveness of our process and highlight its potential to improve operational efficiency in the long run. Table 3 presents a comparison of the MTTR metric for both the CIMP and the FbCIMP, with respect to the cyber-incidents involved in the shopping cart of an e-commerce website. Overall, the results of the evaluation allow the null hypothesis (H_0) to be rejected and the alternative one (H_1) to be accepted.

The results of Table 3 reveal that the FbCIMP reduces MTTR by 31% ($\frac{30.5-21.0}{30.5}$), which gives a positive indicator that it is more efficient when compared to the CIMP.

The values in Table 3 are related to specific real-world incidents. MTTR can vary significantly based on organisation size, maturity of incident response processes, incident complexity, and other factors. Additionally, the effect of particular fundamental causes on MTTR may vary between organisations. Measuring and analysing MTTR metrics regularly is essential for identifying opportunities to improve incident response processes. Organisations can use these statistics to set targets, allocate resources, and optimise their incident management strategies.

Table 3 Weekly MTTR values (in hours) for CIMP and FbCIMP

Process Management	Week 1	Week 2	Week 3	Week 4	Mean MTTR
CIMP	20	48	18	36	30.5
FbCIMP	18	36	12	18	21.0

6.2 Case Study #2

The second case study assesses the effectiveness of the FbCIMP, with a focus on MTTR, in five different companies from various sectors. This case study has been defined and applied to the top industries at risk for cyberattacks, namely finance, healthcare, and education. The study evaluates how the use of the proposed process impacts the ability of the IRT of each company to respond swiftly to cyber-incidents and mitigate potential damages. High-risk industries are continuously exposed to cyberthreats, so a rapid response is essential in minimising risks. Thus, to apply this case study, we asked companies to adopt FbCIMP to improve their incident response capabilities. The primary objectives of this case study are (i) to evaluate how the FbCIMP impacts MTTR in high-risk industries, (ii) to identify unique factors influencing MTTR within different cyberattacks, and (iii) to provide insights and recommendations based on the evaluation findings.

To conduct the case study, in the first phase, we selected five companies[3] from high-risk industries (Table 4). These industries were chosen due to their vulnerability to cyberattacks and the potential impact on critical systems and their data. In the second phase, we asked the companies to adopt our process to respond to cyber-incidents during one month, and we gathered data through interviews with company representatives, including IT personnel and cybersecurity experts. The primary metric for evaluation is MTTR. In the next phase, we conducted a comparative analysis of MTTR across the selected companies to identify differences and similarities between the proposed process and the baseline one adopted by each company (Table 4). By evaluating the effectiveness of both processes, we aimed to determine the impact of the proposed process on the MTTR.

As shown in Table 4, Company A scores an average MTTR of three hours, driven by a proactive approach to threat detection and well-defined response protocols. Company B has an average MTTR of five hours, influenced by strict regulatory requirements, resource constraints, and the need for

[3]Due to confidentiality issues, the names of the companies are not disclosed.

Table 4 Evaluation of the MTTR for five different companies in high-risk sectors

Company	Industry	MTTR (Hours)	
		FbCIMP	CIMP (Baseline)
A	finance	3	4
B	healthcare	5	7
C	education	7	9
D	finance	4	6
E	healthcare	6	9

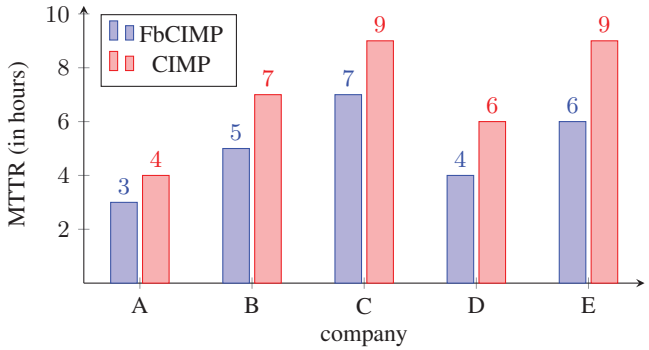

Figure 12 Comparison of FbCIMP and CIMP in high-risk sectors.

specialised healthcare data protection. Company C is concerned with infrastructure registers with an average MTTR of seven hours due to the complexity of securing critical infrastructure systems and coordination with regulatory bodies. Company D has an average MTTR of four hours and has benefited from advanced threat detection tools and efficient communication channels. Finally, company E has on average an MTTR of six hours, challenged by regulatory compliance requirements and resource allocation issues.

In each company, we divided the participants in the case study into two groups. The first group responded to cyber-incidents using the FbCIMP, and the second group using the baseline process (CIMP). At this time, an analysis was conducted to assess the average of the MTTR values among various companies over the course of one month. The assessment comprised contrasting the utilisation of the FbCIMP with the CIMP throughout the same time frame. In the final phase, as part of the case study, we calculated the MTTR values for both teams over the different sectors (Table 4 and Figure 12).

The comparative analysis between both processes shows that the MTTRs for all companies with the FbCIMP are lower when compared with the CIMP.

The use of FbCIMP consistently leads to shorter response times compared to the baseline process in health care, finance, and education sectors. This indicates that incorporating FMs into the cyber-incident process is effective in improving response times across different high-risk sectors. The data suggests that companies could consider the FbCIMP to improve their incident response capabilities and minimise downtime in critical situations.

7 Threats to Validity

When evaluating the FbCIMP, there are several potential threats to validity that one should be aware of. They are next presented.

Construct Validity: This threat relates to how the measures used to evaluate the proposed process accurately reflect the underlying constructs of interest. To mitigate this risk, we made efforts to ensure that the selected metrics and evaluation criteria align with the objectives of the FbCIMP.

Internal Validity: This pertains to the degree to which the observed effects (MTTR) can be related to the performance of the proposed process and not other factors. To improve internal validity, we attempted to use a controlled experimental design whenever possible and to account for variables that may have influenced the results.

External Validity: External validity refers to the generalisability of the findings beyond the proposed process to various types of organisations and cyber-incidents. If the participants do not accurately represent the target user population or if the evaluation setting is not reflective of real-world conditions, external validity may be threatened.

Maturation and Time Effects: Over time, participants may become more familiar with the proposed process, which could result in fluctuations to their evaluation. To control this threat to validity, we asked participants in the evaluation to work with various types of incidents, and we tried to conduct the evaluation at intermittent intervals.

8 Conclusion and Future Work

This paper provides a process for incorporating feature modelling into cyber-incident management processes. Having a clear incident response strategy is critical for organisations to manage cyber-incidents efficiently. The proposed process uses FMs to identify, classify, prioritise, and resolve potential

cyber-incidents based on their source, type, and severity. The improved process shows promising improvements in this aspect, indicating a positive step towards better cyber-incident response. This allows organisations to allocate resources more effectively and focus on the most critical incidents first.

Overall, the FbCIMP process improves the ability of organisations to respond to and recover from cyber-incidents. The evaluation of the proposed process, with two case studies, proves that the use of FMs significantly improves the efficiency of the cyber-incident management process. It also reduces MTTR, allowing organisations to quickly identify and address cyberthreats before they cause significant damage. In future work, we plan to use the attributed FM, as described in [32], in incident management, which offers a structured and customisable approach to capturing incident information and leads to better reporting, decision-making, and overall incident response effectiveness.

Acknowledgments

We express our gratitude to Dr. Ali Shoker for his guidance and first evaluation of this manuscript. We thank the teams of the companies for taking part in the evaluation process. The case studies would not be completed without their continuous support and cooperation. This work was supported by FCT—Fundação para a Ciência e Tecnologia within the R&D Units Project Scope UIDB/00319/2020.

References

[1] Patrick Taylor Smith. "Cyberattacks as casus belli: A sovereignty-based account". In: *Journal of Applied Philosophy* 35.2 (2018), pp. 222–241.

[2] Lena Y Connolly and David S Wall. "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures". In: *Computers & Security* 87 (2019), p. 101568.

[3] Rishi Vaidya. *Cyber security breaches survey 2019*. University of Portsmouth, 2019.

[4] Eetu Kettunen. *Enhancing incident management process*. Master's thesis. Jyväskylä, Finland: JAMK University of Applied Sciences, 2023.

[5] Jeetendra Pande. "Introduction to cyber security". In: *Technology* 7.1 (2017), pp. 11–26.

[6] Janet Kuhn. "Expanding the expanded incident lifecycle". In: *Do-IT Yourself* 5.7 (2009).

[7] Oluwafemi Oriola et al. “A collaborative approach for national cybersecurity incident management”. In: *Information & Computer Security* 29.3 (2021), pp. 457–484.

[8] Martin Gilje Jaatun and Rainer Koelle. “Cyber security incident management in the aviation domain”. In: *11th International Conference on Availability, Reliability and Security (ARES 2016)*. 2016, pp. 510–516.

[9] Nivedita Shinde and Priti Kulkarni. “Cyber incident response and planning: a flexible approach”. In: *Computer Fraud & Security* 2021.1 (2021), pp. 14–19.

[10] Amal Latrache, El Habib Nfaoui, and Jaouad Boumhidi. “Multi agent based incident management system according to ITIL”. In: *Intelligent Systems and Computer Vision (ISCV 2015)*. 2015, pp. 1–7.

[11] Maria Bartnes, Nils Brede Moe, and Poul E Heegaard. “The future of information security incident management training: A case study of electrical power companies”. In: *Computers & Security* 61 (2016), pp. 32–45.

[12] Martin Sarnovsky and Juraj Surma. “Predictive models for support of incident management process in IT service management”. In: *Acta Electrotechnica et Informatica* 18.1 (2018), pp. 57–62.

[13] Claudio Bartolini, Cesare Stefanelli, and Mauro Tortonesi. “SYMIAN: Analysis and performance improvement of the IT incident management process”. In: *IEEE Transactions on Network and Service Management* 7.3 (2010), pp. 132–144.

[14] George Grispos, William Bradley Glisson, and Tim Storer. “Enhancing security incident response follow-up efforts with lightweight agile retrospectives”. In: *Digital Investigation* 22 (2017), pp. 62–73.

[15] Olaolu Kayode-Ajala. “Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption”. In: *Applied Research in Artificial Intelligence and Cloud Computing* 6.8 (2023), pp. 1–21.

[16] Florian Menges and Günther Pernul. “A comparative analysis of incident reporting formats”. In: *Computers & Security* 73 (2018), pp. 87–101.

[17] Rajeev Gupta, K Hima Prasad, and Mukesh Mohania. “Automating ITSM incident management process”. In: *International Conference on Autonomic Computing (ICAC 2008)*. 2008, pp. 141–150.

[18] Marshall A Kuypers, Thomas Maillart, and Elisabeth Paté-Cornell. *An empirical analysis of cyber security incidents at a large organization*.

Department of Management Science and Engineering, School of Information, Stanford University, 2016.
[19] Kyo C Kang, Jaejoon Lee, and Patrick Donohoe. "Feature-oriented product line engineering". In: *IEEE Software* 19.4 (2002), pp. 58–65.
[20] Ebrahim Bagheri and Dragan Gasevic. "Assessing the maintainability of software product line feature models using structural metrics". In: *Software Quality Journal* 19 (2011), pp. 579–612.
[21] Guoheng Zhang, Huilin Ye, and Yuqing Lin. "An approach for validating feature models in software product lines". In: *Journal of Software Engineering* 7.1 (2013), pp. 1–29.
[22] Karam Ignaim et al. "A concrete product derivation in software product line engineering: A practical approach". In: *International Journal of Computer Applications in Technology* 70.3–4 (2022), pp. 225–232.
[23] Karam Ignaim. "EvoSPL: An evolutionary approach for adopting software product lines in the automotive industry". PhD thesis, Braga, Portugal: Universidade do Minho, 2021.
[24] R Al-Msie'deen. "Reverse engineering feature models from software variants to build software product lines: REVPLINE approach". PhD thesis, Montpellier, France: Universitè Montpellier II, 2014.
[25] George Stergiopoulos, Dimitris A Gritzalis, and Evangelos Limnaios. "Cyber-attacks on the Oil & Gas Sector: A survey on incident assessment and attack patterns". In: *IEEE Access* 8 (2020), pp. 128440–128475.
[26] Robert J Turk. *Cyber incidents involving control systems*. Tech. rep. Idaho National Laboratory, Idaho, United States, 2005.
[27] Richard Smith et al. "The agile incident response for industrial control systems (AIR4ICS) framework". In: *Computers & Security* 109 (2021), p. 102398.
[28] Tanja Ruskojärvi. *Cyber security incident management process in NOC/SOC integration*. Master's thesis. Jyväskylä, Finland: JAMK University of Applied Sciences. 2020.
[29] Olga De Troyer and Erik Janssens. "A feature modeling approach for domain-specific requirement elicitation". In: *4th IEEE International Workshop on Requirements Patterns (RePa 2014)*. 2014, pp. 17–24.
[30] Don Batory. "Feature models, grammars, and propositional formulas". In: *9th International Conference on Software Product Lines (SPLC 2005)*. 2005, pp. 7–20.

[31] Julie Steinke et al. “Improving cybersecurity incident response team effectiveness using teams-based research”. In: *IEEE Security & Privacy* 13.4 (2015), pp. 20–29.

[32] Karam Ignaim, Sultan M Al Khatib, and João M. Fernandes Khalid Alkharabsheh. “Approach to attributed feature modeling for requirements elicitation in scrum agile development”. In: *Journal of Theoretical and Applied Information Technology* 101.9 (2023).

Biographies

Karam Mustafa Ignaim is assistant professor at Al Balqa Appiled University, Jordan. She received her BSc degree in Information Technology and the MSc degree in Computer Science, both from Al Balqa Applied University, and the PhD degree in Software Engineering from University of Minho, Portugal. Her research interests include software product lines, feature modelling, software reuse, cybersecurity, and software maintenance.

João M. Fernandes is full professor at Universidade do Minho, Portugal. He conducts his research activities in software engineering, with a special interest in software modelling, requirements engineering and software

business. He is the main author of the book 'Requirements in Engineering Projects', Springer in 2016. He has been involved in the organisation of various international events, including ACSD 2003, DIPES 2006, GTTSE 2009, PETRI NETS 2010, ACSD 2010, the MOMPES Workshops Series (2003–2012) and ICSOB 2015.