

**A FRAMEWORK FOR THE ASSESSMENT AND IMPROVEMENT OF
ZERO-DAY SECURITY ATTACKS**

BY

Eman Junid Bakri

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER SCIENCE

December, 2023

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN- 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **EMAN JUNID BAKRI** under the direction of his thesis advisor and approved by his thesis committee, has been presented and accepted by the Dean of Graduate Studies in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER SCIENCE**.



Dr. MOTAZ ALFARRAJ
Department Chairman



Dr. Suliman Al-Homidan
Dean of Graduate Studies

Date: 10th December 2023



Dr. SAJJAD MAHMOOD
(Advisor)



Dr. MAHMOOD KHAN NIAZI
(Member)



Dr. MOHAMMAD RABAH
ALSHAYEB
(Member)



© Eman Junid Bakri

2023

[Dedication]

To the precious people of my life, family, and friends.

*To the experiences we shared, the road we walked through,
and all the hardships that made us stronger.*

ACKNOWLEDGMENTS

An outstanding journey has come to an end. I would like to thank Dr. Sajjad Mahmood, my supervisor, for his endless support, patience, and understanding while he was managing my thesis journey. I truly appreciate all the effort made, and it would not have been the same experience without his guidance. Many thanks to the respected defense committee, and I am grateful for their valuable feedback. Big thanks to the professors, the friends, and the classmates who were a part of my master's journey in KFUPM, you made it worthy and meaningful. I would like to acknowledge and thank all interviews, surveys, and case study participants for sharing their experiences on zero-day attacks with us.

Lastly, I'm grateful for my family, especially my parents, who always supported, encouraged, and shared happiness. Thank you for believing in me and being by my side.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	V
TABLE OF CONTENTS	VI
LIST OF TABLES	X
LIST OF FIGURES	XII
LIST OF ABBREVIATIONS	XIII
ABSTRACT	XIV
ملخص الرسالة	XVI
1 INTRODUCTION.....	1
1.1 Motivation	3
1.2 Objectives.....	4
1.3 Contributions	4
1.4 Research Methodology	5
1.5 Thesis Document Roadmap	6
2 RELATED WORK	7
2.1 Background.....	7
2.1.1 MLR	7
2.1.2 Maturity Models	8
2.1.3 Fuzzy Analytic Hierarchy Process (F-AHP)	9
2.2 Related Work.....	9
2.2.1 Zero-day Attacks.....	9
2.2.2 Maturity Models.....	12

2.3	Research Gap	15
3	INTERVIEW BASED STUDY	16
3.1	Interview-Based Study.....	17
3.1.1	Participants.....	17
3.1.2	Interview Design	19
3.2	Questionnaire Survey	20
3.2.1	Participants.....	20
3.2.2	Survey Design.....	20
3.3	Results and Analysis	24
3.3.1	Interviews Findings.....	24
3.3.2	Questionnaire Survey Findings.....	48
4	MULTIVOCAL LITERATURE REVIEW (MLR)	56
4.1	MLR Process	56
4.1.1	Goal & Research Questions	56
4.1.2	Search Query Definition.....	57
4.1.3	Source Selection	58
4.1.4	Inclusion & Exclusion Criteria	58
4.1.5	Quality Assessment Criteria	59
4.1.6	Execution of MLR Process	61
4.2	MLR Findings	63
4.2.1	Zero-day Attacks Challenges	63
4.2.2	Zero-day Attacks Solutions and Best Practices	66
5	FUZZY ANALYTIC HIERARCHY PROCESS (F-AHP)	72
5.1	Fuzzy-AHP Process.....	74
5.2	Fuzzy AHP implementation	76

5.3	Taxonomy of zero-day attacks challenges	84
6	ZERO-DAY ATTACKS MATURITY MODEL.....	86
6.1	Model Development.....	86
6.2	The Five Knowledge Areas	88
6.3	The Five Maturity Levels.....	90
6.4	The Best Practices	92
6.5	The Assessment Method	93
6.6	Final Version of Maturity Model (Main Outcome)	93
7	CASE STUDIES.....	100
7.1	Process of Case Studies	100
7.1.1	Organization ‘A’	100
7.1.2	Organization ‘B’	101
7.1.3	Feedback Criteria.....	101
7.2	Case Studies Outcomes	101
7.2.1	Maturity assessment of organization ‘A’	102
7.2.2	Maturity assessment of organization ‘B’	104
7.2.3	Feedback Summary	106
8	WEB TOOL.....	110
8.1	The Output Web Tool	110
8.1.1	Modifications of the model:	114
8.1.2	Customization of the model:.....	115
9	DISCUSSION AND CONCLUSIONS	116
9.1	Discussion and Important Remarks	116
9.2	Implications of the Study	121

9.3	Threats to Validity	122
9.4	Conclusion and Future Work	123
REFERENCES.....		125
VITAE		137
APPENDIX A: INTERVIEWS QUESTIONS		138
APPENDIX B: SURVEY QUESTIONS.....		139
APPENDIX C: MLR RESOURCES LIST DETAILS (FORMAL & GREY).....		143
APPENDIX D: MOTOROLA ASSESSMENT TOOL (ADOPTED FROM [149])		143

LIST OF TABLES

Table 1	Summary of existing literature on Maturity Models in security.....	14
Table 2	Interviews' Participants Demographics.....	17
Table 3	Survey Participants Demographics.	21
Table 4	Examples of interviews transcript classification process (challenges).	30
Table 5	Best Practices list (Interviews outcome).....	41
Table 6	Challenges Survey Results (no. of participants).	51
Table 7	Quality assessment criteria of grey literature [23].	60
Table 8	List of challenges by formal literature and their frequency (243 resources)..	69
Table 9	List of challenges by grey literature and their frequency (71 resources).....	70
Table 10	Input for fuzzy AHP (Identified challenges list and their categories).	72
Table 11	Pairwise comparison matrix of Solutions challenges category.	77
Table 12	Pairwise comparison matrix of Resources challenges category.	78
Table 13	Pairwise comparison matrix of Consequences challenges category.....	79
Table 14	Steps 3, 4 & 5 of fuzzy AHP process (anonymity).....	79
Table 15	Steps 3, 4 & 5 of the fuzzy AHP process (resources).....	80
Table 16	Steps 3, 4 & 5 of the fuzzy AHP process (solutions).	81
Table 17	Steps 3, 4 & 5 of the fuzzy AHP process (consequences).	81
Table 18	Final ranking of the identified challenges.....	83
Table 19	Examples of data classification process (Best practices).....	87
Table 20	Zero-day maturity model [Human, organizational, & regulatory aspects KA]..	94
Table 21	Zero-day attacks maturity model [Attacks & Defenses KA].....	95

Table 22	Zero-day attacks maturity model [Systems Security KA]	96
Table 23	Zero-day attacks maturity model [Software & Platform Security KA]	97
Table 24	Zero-day attacks maturity model [Infrastructure Security KA]	97
Table 25	Maturity Score of organization 'A' using the model.	102
Table 26	Maturity Score of organization 'B' using the model.	104
Table 27	Ease of use feedback results by organizations A, and B.	107
Table 28	User satisfaction feedback results by organizations A and B.	108
Table 29	Structure of the model feedback results by organizations A, and B.	109

LIST OF FIGURES

Figure 1	Overview of Research Methodology.....	6
Figure 2	Interview Based Study Details.	16
Figure 3	Survey Participants Demographics	24
Figure 4	How frequent zero-day encountered? (By interview participants).....	27
Figure 5	List of challenges organized by category.	30
Figure 6	Frequency of each challenge (By interviews participants).....	39
Figure 7	The complete MLR process.....	62
Figure 8	The proposed hierarchy structure.	77
Figure 9	Taxonomy of zero-day attacks challenges.	85
Figure 10	Maturity model main structure elements.	92
Figure 11	Zero-day maturity model web-based tool user interface	111
Figure 12	Assessment tool page, organization information interface.....	112
Figure 13	Assessment tool page, quiz screen example.....	112
Figure 14	Organization assessment results	114

LIST OF ABBREVIATIONS

MLR	:	Multivocal Literature Review
Fuzzy AHP	:	Fuzzy Analytic Hierarchy Process
CAM	:	Content Analysis Method
RASP	:	Runtime Application Self-Protection
RND	:	Research and Development
SEI	:	Software Engineering Institute
CMM	:	Capability Maturity Model
CMMI	:	Capability Maturity Model Integration
MM	:	Maturity Model

|

ABSTRACT

Full Name : Eman Junid Bakri

Thesis Title : A Framework for The Assessment and Improvement of Zero-Day Security Attacks

Major Field : Computer Science

Date of Degree : December 2023

Security is an essential attribute of quality software. Detecting and mitigating different types of attacks is a must to have high-quality software. Organizations spend large amounts of money purchasing intrusion detection systems, antivirus software, and antispyware software. However, these solutions are not enough, and organizations continue to suffer security risks due to an ever-growing list of security vulnerabilities. One such security vulnerability is a zero-day attack. A zero-day attack describes the threat of an unknown security vulnerability in software that either the application developers are unaware of or no security patch has been released. Zero-day attacks are complex to analyze due to the lack of data until such attacks are discovered. Despite the significance of zero-day attacks, little empirical research has been conducted to understand such attacks better. No model exists to assess the maturity of managing zero-day attacks in an organization. This study aims to build a zero-day attack maturity model to enable organizations to understand their current capabilities when dealing with zero-day attacks and identify areas of improvement, following the defined knowledge areas and maturity levels. A Multivocal Literature Review (MLR) approach was used to identify challenges and respective best practices to handle zero-day attacks. The zero-day attacks maturity model and web-based tool were developed. Next, case studies were conducted to validate the model. Finally, the Fuzzy Analytic Hierarchy Process (F-AHP) was used to prioritize the identified challenges. The study's findings included a prioritized list of challenges, a maturity model of zero-day attack best practices, and a web tool acting as an interactive version of the maturity model. The study outcomes will increase the awareness of such attacks and their challenges, assess organizations' level of maturity in dealing with zero-days, and be a baseline for further research in this area supporting industries and developers.

Keywords: *Software Security, zero-day attacks, maturity model, multi-criteria decision-making, fuzzy AHP, challenges, best practices.*

ملخص الرسالة

الاسم الكامل: إيمان جنيد بكري

عنوان الرسالة: إطار عمل لتقييم وتحسين هجمات اليوم صفر الأمنية.

التخصص: علوم الحاسب

تاريخ الدرجة العلمية: ديسمبر 2023

يعتبر الأمن عنصراً أساسياً لجودة البرمجيات، حيث أصبح إيجاد والتخلص من العديد من أنواع الهجمات ضرورة لتحقيق جودة عالية. تستثمر المؤسسات مبالغ مالية ضخمة لتوفير أنظمة كشف التسلل، برامج مكافحة الفيروسات، وبرامج مكافحة التجسس. هذه الحلول ليست كافية، لذلك تعاني المؤسسات من مخاطر أمنية نظراً لوجود قائمة الثغرات الأمنية اللامتناهية. واحدة من هذه الثغرات الأمنية هي الـ day-0 أو يوم الصفر (دون انتظار). هجمات يوم الصفر توضح تهديداً من ثغرة أمنية غير معروفة في البرمجيات، حيث إنه إما مبرمجي التطبيقات ليس لديهم معرفة بوجودها، أو أنه لم يصدر لها تصحيح أمني بعد. هذه الهجمات هي معقدة نتيجةً لنُدرة البيانات عنها حتى يتم اكتشافها والعثور عليها. على الرغم من مدى أهمية هجمات اليوم صفر، هناك عدد قليل من الأبحاث التطبيقية التي أجريت لفهم هذا النوع من الهجمات بشكل أفضل. حالياً لا يوجد أي نموذج لقياس وتقييم جاهزية ونضج المؤسسات للتعامل مع هجمات اليوم صفر. تهدف الدراسة إلى بناء نموذج جاهزية في التعامل مع يوم الصفر لتمكين المؤسسات من فهم إمكاناتها الحالية في التعامل مع هذه الهجمات وتحديد مناطق التحسينات. لتحقيق ذلك، تم استخدام دراسة مبنية على المقابلات، إضافة إلى مراجعة المؤلفات متعددة المصادر لاستخراج قائمة التحديات وأفضل الممارسات للتعامل مع هجمات اليوم صفر. بعد ذلك تم بناء نموذج جاهزية التعامل مع هجمات اليوم صفر مقسماً إلى مناطق معرفية، ومستويات النضج. يتبع ذلك دراسة حالة لتجربة النموذج، وأداة ويب. في النهاية، تم استخدام عملية تحليلية هرمية لتحديد أولوية التحديات وترتيبها وفقاً لذلك. مخرجات الدراسة تتضمن قائمة مرتبة حسب الأولوية للتحديات، نموذج جاهزية التعامل مع هجمات اليوم صفر باستخدام أفضل الممارسات، وأداة ويب تمثل نسخة تفاعلية من النموذج. يُتوقع لمخرجات هذه الدراسة البحثية أن ترفع مستوى المعرفة فيما يتعلق بهجمات اليوم صفر وتحدياتها، إضافة إلى تأسيس بداية لأي أبحاث مستقبلية في هذا المجال لدعم المؤسسات والمطورين.

CHAPTER 1

INTRODUCTION

Software vulnerabilities are present at every level and type of system, allowing attackers to gain unauthorized system access [1]. The software vulnerability that the vendor has not solved and has no patch yet is called a zero-day vulnerability [2]. The zero-day vulnerability is unknown to software developers before the day of the attack [3]. Therefore, such vulnerabilities have not been patched or disclosed publicly [4]. A system remains affected by a zero-day attack until the vulnerability is detected and a patch is applied [5].

The zero-day term refers to the idea that this specific vulnerability has just been discovered and that attackers can use it to exploit and attack systems [6]. The expression originated when the exploit occurs before or on the first (or ‘zeroth’) day of an expert’s awareness of the exploit [7]. Zero-day attacks are challenging to detect since they are unknown and have no signature [8]. Due to their anonymous nature, zero-day exploits are used by attackers to gain access to systems and obtain illegal benefits [9].

Zero-day attacks can be targeted or non-targeted, depending on the target actor. When attacks are targeted, they aim to affect a specific target, like governments, public institutions, or other parties holding financial or reputation power [10]. On the other hand,

when the attack affects some system or browser users, it is considered non-targeted [10]. Software, hardware, or IoTs can all be victims of the non-targeted [10].

Zero-day attacks are challenging even for large, well-established organizations [11]. For example, in 2021, Microsoft suffered when four zero-day vulnerabilities were exploited by a group of hackers called HAFNIUM, resulting in a data breach [12]. However, after being discovered, Microsoft informed and warned their users and sent multiple patches to fix the issue [12]. One famous example is the attack on Alibaba's online retail website, which remained undetected for eight months and leaked 1.1 billion customer data in 2019 [13]. Another incident would be the zero-day attack that targeted LinkedIn in 2021 and affected around 700 million users [13].

Since these vulnerabilities are new, tackling them using standard signature-based solutions is hard, as they will have new signatures not previously identified [14]. Detection and identification of zero-day in different environments is still a challenge. Many efforts have been made earlier, but the outcomes are not up to expectations, and vulnerabilities are still rising [15].

In recent years, zero-day attacks have been shining and getting attention for multiple political and financial gains [9]. The detected vulnerabilities are considered attractive targets for cybercriminals, governments, and software organizations willing to pay massive amounts of money to access such exploits [16]. Zero-day markets exist for such purposes where stakeholders trade in vulnerabilities and exploits, depending on the market being white, grey, or black [17].

The security field has frameworks serving multiple purposes across many areas and domains [18]. Security models, including cybersecurity maturity models, were developed over the years to protect cyberspace and assess organizations and experts in the field [18]. However, no maturity model focuses on zero-day vulnerabilities and the best practices suggested to manage them. Because zero-day attacks are unknown, hard to track, and go after different targets, this study focuses on creating a zero-day attacks maturity model that shows how well an organization can handle them overall and how to get better at dealing with them.

1.1 Motivation

Malware is becoming more effective in dealing with new threats rapidly (speed) with new techniques and methods [19]. Specifically, zero-day attacks are considered a serious security concern, holding the highest priority of malware detection systems (MDSs)[20]. As Alex Fagioli said, "The number of zero-days will increase from one per week in 2015 to one per day in 2021, with the application attack surface growing by 111 billion new lines of code every year" [21]. As zero-day exploits are previously undiscovered, they add an element of surprise, resulting in extreme damage financially, operationally, and in terms of reputation [21], [22]. Due to the severity of the threat and the recent surge in the number of zero days, it is critical that security professionals are cognizant of the entanglements and potential recommended best practices. This is the primary impetus for conducting this research.

1.2 Objectives

This study aims to build a zero-day attack maturity model to enable organizations to evaluate their maturity levels to handle such attacks. The developed maturity model will guide security experts in different organizations when dealing with zero-day attacks. The sub-objectives of this research are as follows:

- 1- Identify the challenges and respective best practices to deal with zero-day attacks.
- 2- Develop a taxonomy of challenges associated with handling zero-day attacks.
- 3- Build a Zero-day Attacks Maturity Model utilizing best practices.
- 4- Develop a web tool to present the zero-day attacks maturity model.
- 5- Prioritize the identified challenges using a Fuzzy AHP.

1.3 Contributions

The key contributions of this research include:

- A set of challenges and their recommended best practices for managing zero-day attacks.
- A taxonomy of challenges associated with handling zero-day attacks.
- A zero-day attacks maturity model, recommended for security practitioners' guidance and support.
- A web tool based on the maturity model for more interactive, easier access for security teams and organizations interested.
- A prioritized list of challenges using Fuzzy AHP.

1.4 Research Methodology

To achieve research objectives, a mixed-method approach, including several stages, was used. First, for data collection, an interview-based study was conducted, performing semi-structured interviews and questionnaire surveys with security experts from different levels of expertise. Then, a Multivocal Literature Review (MLR) was conducted to survey papers published in the domain (formal & grey) and identify the key factors related to challenges, best practices, or solutions that existed to deal with zero-day attacks. As a result of data collection and analysis, a list of best practices and a list of challenges will be ready. The challenges list will be the input to the fuzzy analytical hierarchy process (fuzzy AHP) for prioritization, which results in a challenges taxonomy. On the other hand, best practices will be represented as a zero-day attacks maturity model developed to help security experts and increase awareness regarding zero-day attacks. Furthermore, multiple case studies were performed, testing the proposed maturity model and receiving feedback from a real environment. Finally, a web tool of the maturity model has been developed for a more accessible, easy-to-use format. Figure 1 shows an overview of the research methodology used in the study. The details of the research methodology are discussed in the coming sections. The research questions addressed in the study are as follows:

RQ1: What challenges are encountered when dealing with zero-day attacks as identified in the literature (formal & grey) and industry?

RQ2: What are the solutions and best practices identified in the interviews and literature suggested when dealing with zero-day attacks?

RQ3: What is the final version of the zero-day maturity model developed?

RQ4: What is the output prioritization of zero-day attacks challenges resulting from the Fuzzy AHP process?

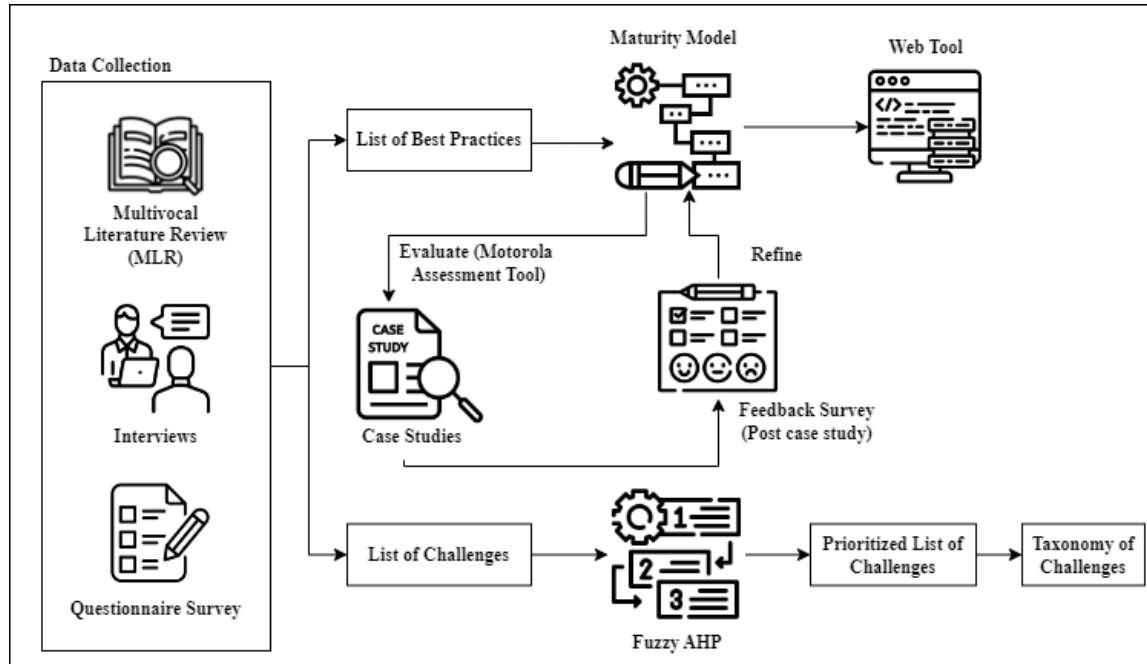


Figure 1: Overview of Research Methodology.

1.5 Thesis Document Roadmap

The remainder of this research is organized as follows: Chapter 2 describes the background and related work. Chapter 3 presents the interview-based study. Chapter 4 describes the MLR process. Chapter 5 explains the fuzzy AHP. Chapter 6 presents the maturity model. Chapter 7 clarifies the case studies, while Chapter 8 highlights the web tool. Finally, Chapter 9 provides the discussion, threats to validity, and conclusions.

CHAPTER 2

RELATED WORK

2.1 Background

Introducing the concepts of Multivocal Literature Review (MLR), the maturity models, and the fuzzy analysis hierarchy process (F-AHP).

2.1.1 MLR

The Multivocal Literature Review (MLR) is a version of a Systematic Literature Review (SLR) that combines evidence and knowledge from the peer-reviewed literature published in journal and conference papers with the grey literature represented by white articles, blog posts, videos, etc. [23] [24]. Formally published literature is normally referred to as white literature, while grey literature is the informally published one [25]. The value of MLRs is presented by providing insights into both state-of-the-art (formal) and state-of-the-practice (grey) regarding a given topic for both researchers and practitioners [24], [26]. Since SLR typically will not include the non-published grey literature produced by SE practitioners, so it is limited in some aspects [26]. Similarly, SE practitioners usually do not publish in academic sources, which limits their knowledge to be shared [26]. MLRs highlight considering multiple sources rather than entirely depending on the knowledge reported in academic settings (formal literature) [23] [25].

2.1.2 Maturity Models

Maturity Model (MM) is an organized assortment of entities that portray the attributes of an activity or a process progressing from the initial stage of development to an advanced one [27], [28]. It is meant to influence persistent improvements and effectively manage multi-component, complicated elements [29]. Started at Carnegie Mellon University when SEI (Software Engineering Institute), led by Paul et al., developed the Capability Maturity Model (CMM) [30] [31]. Capability Maturity Model (CMM) is a management model to achieve a disciplined and mature software process in organizations [32]. It essentially presents a framework to help assess project management capability and manage software development processes [33] [34]. This model works at five levels of organizational capability maturity [33]. In the beginning, CMM was applied in the software industry to specify the maturity level of a specific software [34]. Later, it was applied in other areas, such as manufacturing projects, enterprise intelligence, consultancy practice, etc. [34], [35]. Similar to other CMMs, Capability Maturity Model Integration (CMMI) models offer guidance for the development of processes [36]. CMM Integration (CMMI) organizes established approaches within a framework to assist your organization in evaluating its organizational maturity or process area capability, determining priorities for enhancement, and implementing these improvements [36]. In a business or development environment, the chosen CMMI model can act as a roadmap for enhancing organizational processes [36].

2.1.3 Fuzzy Analytic Hierarchy Process (F-AHP)

The Analytical Hierarchy Process (AHP) is a powerful, effective decision-making support method [37]. AHP is considered a successful way to decide among the complex criteria structure in different levels [38]. However, during comparison, the subjective judgments might be imprecise, for that fuzzy sets were combined with AHP [39]. Fuzzy Analytical Hierarchy Process (F-AHP) is an extension of the classical AHP that combines AHP with fuzzy set theory [38], [40]. Meaning that the decision-makers fuzziness and logical thinking are considered, and the uncertainty of human preference is modeled [38], [40], [41]. So, F-AHP can facilitate decision making set goal weight, guidelines, and alternatives, to define how consistent different criteria are [42], [43].

2.2 Related Work

This section reviews the research state in terms of zero-day attacks and maturity models.

2.2.1 Zero-day Attacks

Several studies have been conducted discussing zero-day vulnerabilities and addressing their criticality. Most of the studies were solutions forwarded, in which different methods, algorithms, systems, approaches, or frameworks were suggested for managing zero-day attacks. These solutions were used for the purpose of detection, prevention, defense, or prediction of zero-days, and would be implemented in several mediums like networks, web, cloud, virtual machines etc. Al-Rushdan et al. presented a mechanism for the detection and prevention of zero-day for the Software Networks (SDN) [44]. Their proposed design worked by isolating the infected user with zero-day, thus preventing the vulnerabilities from accessing other users [44]. Asif et al. designed an Intrusion Detection System (IDS)

that is based on honey tokens, which act as a trap for the attacker [45]. This system aims to protect infrastructure networks from different security attacks, specifically zero-day attacks [45]. Another proposed approach by Shanmugam et al. uses an anomaly detection technique to provide security for web application users [46]. This approach works by adding an extra layer of security on the top of the web application while remaining unchanged [46]. Bu et al. introduced an integration method of deep learning with phishing detection logic to detect zero-day phishing attacks [47]. They test the proposed approach over three real-life datasets, and it reflects the highest recall among the latest deep learning methods [47]. Naderi-Afooshteh and Kwon et al. presented Cubismo, an automated system that discloses malware in server-side web applications [48]. In particular, it allows the detection of previously undetectable 53 zero-day malware in the wild out of 56 [48]. Millar et al. proposed a novel deep-learning approach operating as a zero-day Android malware detector [49]. Moreover, Kumar Singh et al. defined a framework for detecting and prioritizing zero-day attacks [22]. This framework identified zero-day attacks using probabilistic approaches and then ranked the detected vulnerabilities based on severity [22]. Another study by Wang and Zhang with the aim of evaluating network robustness against zero-days using proposed network diversity modeling and metric function [50]. Moreover, Ali and Rehman et al. introduced a comprehensive review analyzing and comparing many machine learning and deep learning algorithms used recently in detecting zero-day attacks [51]. Finally, a study by Mbona et al. explained the effectiveness of semi-supervised ML approaches for zero-day network intrusion attack detection [52]. In 2020, Jeong et al. presented a hybrid approach to restrict the zero-day resulting damage using a combination of a honeypot, a queue, and a signature-based network intrusion detection

prevention system (NIDPS) [53]. In 2023, Ahmad et al. presented an SLR study reviewing all available detection methodologies and algorithms for detecting zero-day attacks, including ML and DL [54]. Murugan S et al. and Kumaar A et al. in 2024 used machine learning to offer a dependable method in detecting zero-day vulnerabilities in software systems [55]. Another research in 2024 by Jones and Omar et al., introduces the GEADD method (GPT-2 Enhanced Attack Detection and Defense) [56]. This is a novel strategy merging the GPT-2 model with metaheuristic optimization methods to improve the detection of zero-day threats [56].

From another perspective, some studies focus on risk estimation and risk assessment of zero-day attacks. Ye et al. presented a risk assessment method for zero-day vulnerabilities in internal networks [57]. This method used a proposed vulnerability discovery and graph generation algorithm in addition to four security metrics [57]. Albanese et al and Jajodia et al provided a framework for zero-day vulnerability risk evaluation [58]. The suggested framework consists of a polynomial algorithms group for efficiently estimating the k-zero-day safety of likely large networks [58]. Moreover, Chatzipoulidis et al. introduced a risk prediction methodology for information infrastructures as a proactive approach that analyzes vulnerabilities and measures the risk of zero-day [59]. A novel attack graph-based approach for predictive risk evaluation of zero-day was suggested and discussed in [60]. Another practical cyber-attack method against remote terminal unit (RTU) is proposed by Dai et al., intending to compute the possibility of exploiting a known or zero-day attack by applying a Bayesian attack graph model in an automation system [61].

The ethics and vulnerability market aspects of zero-day vulnerabilities are a highlighted perspective in research. Egelman et al. reflect on the ethical side, and the implications of

the zero-day markets as discussed on the New Security Paradigms Workshop panel happened in 2013. In addition, topics related to the big bounty programs and the rewarding concept for finding vulnerabilities were discussed. B. Wicker et al. highlighted the incident when the WannaCry ransomware attack in 2017 exploited a Microsoft Windows vulnerability that had been discovered previously by the U.S. National Security Agency (NSA) [62]. The ethical part mentioned is that the NSA informed Microsoft about it only after losing control of the developed assets designed initially to benefit from the vulnerability [62]. Li et al. studied and showed a vulnerability market model considering market fraud and uncertainty [63]. In addition, they illustrated a game theoretic framework representing the interactions between the vulnerability owners and customers [63].

2.2.2 Maturity Models

Several security models were developed to protect cyberspace [18]. They focus on a specific security aspect, including asset, identification, data, physical components, network, risk, and application [18]. Compared to other existing models, maturity models present a practical approach for evaluating a system or an organization [18]. In 1989, Humphrey et al. offered a capability maturity model for software quality assessment, which became the basic model adapted for cybersecurity [64]. Consequently, maturity models in recent years have been applied widely for securing significant cyberspace such as e-commerce, e-government, health, and education [65].

The Cybersecurity Capability Maturity Model (C2M2) was created in 2012 and managed by the U.S. government energy sector and the Department of Energy (DOE)[66]. The C2M2's goal is to assist organizations of all types, sizes, and sectors in evaluating and improving their cybersecurity programs and strengthening their operational resilience. An

updated C2M2 version 2.1 was released in June 2022 [66]. Moreover, Proença, D. & Borbinha et al. developed a maturity model using the established approach ISO/IEC 27001, contributing to enhancements in information security management systems [67]. This model aims to provide an assessment for organizations in order to figure out how mature their information security management systems are [67].

Al Hanaei & Rashid et al. presented a capability maturity model DF-C²M², which supports organizations evaluating the maturity of their digital forensics capabilities and identifying possible improvements according to business requirements [68]. Besides, Kassou & Kjiri et al. proposed an SOA Security Maturity Model (SOASMM) to help assess the SOA security maturity of organizations [69]. Al-Matari et al. adapted specific rules from the ISM3 model and presented a security maturity model assessing organizations' security [70]. In addition, Hamza et al. developed a secure IoT-requirement implementation maturity model (SIOT-RIMM) to assess improving requirement engineering processes in software development organizations regarding their IoT privacy and security [71].

Rojas et al. proposed a web applications security maturity model against cyber-attacks directed at the health sector [72]. This model included the main vulnerabilities mentioned by the Open Web Application Security Project for attacks that identify the weakness of the evaluated web system [72]. Researchers at Pacific Northwest National Laboratory (PNNL) developed the Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) to enable Operational Technology (OT) stakeholders, including cybersecurity in different stages of critical operational technology [73]. In addition, Von Solms et al. defined a maturity model to help African Union member states evaluate their Cyber Security status against a specific part of the convention [74].

Table 1: Summary of existing literature on Maturity Models in security

Reference	Year	Key factor
Humphrey et al. [64]	1989	The basic model adapted for cyber security.
C2M2 [66]	2012	Assist organizations in evaluating and improving their cybersecurity programs
Kassou & Kjiri et al. [69]	2012	Assessing SOA security maturity of organizations.
Al Hanaei & Rashid et al. [68]	2014	Evaluating the maturity of organizations' digital forensics capabilities.
Von Solms et al. [74]	2015	Help African Union member states evaluate their Cyber Security status against a specific part of the convention.
Proença, D. & Borbinha et al. [67]	2018	Improving Information Security Management Systems of organizations based on ISO/IEC 27001.
Gourisetti et al (PNNL) [73]	2019	Enable Operational Technology (OT) stakeholders, including cybersecurity in different stages.
Rojas et al [72]	2019	- A web applications security maturity model.

		- Included the main vulnerabilities mentioned by the Open Web Application Security Project
Hamza et al. [71]	2020	Assess improving requirement engineering processes in terms of their IoT privacy and security
Al-Matari et al. [70]	2021	Adapted specific rules from ISM3 model and presented a security maturity model

2.3 Research Gap

Several techniques and methods have been proposed in the literature to handle zero-day attacks. These methods, frameworks, and tools were discussed from network, cloud, and web application perspectives. However, no systematic empirical study has identified the challenges and best practices to handle zero-day attacks from a theory and industry perspective. Moreover, no zero-day attack maturity model has been proposed for organizations reflecting their overall capabilities and charting a path toward higher levels of maturity dealing with zero days. Hence, there is a need to develop a maturity model to assist organizations in better understanding, planning, and managing zero-day attacks.

CHAPTER 3

INTERVIEW BASED STUDY

In order to address the research questions, a mixed-method approach as suggested by [75] was used. First, a qualitative interview-based study was conducted to collect challenges faced and best practices for dealing with zero-day attacks, in addition to insights from security experts currently working in the industry. Next, a questionnaire survey was used to validate and receive feedback on the interviews' findings. Figure 2 provides a detailed overview of the interviews' study details. Both interviews and survey findings were synthesized, forming the final outcomes. The details of the interviews and survey processes will be discussed in the coming sections.

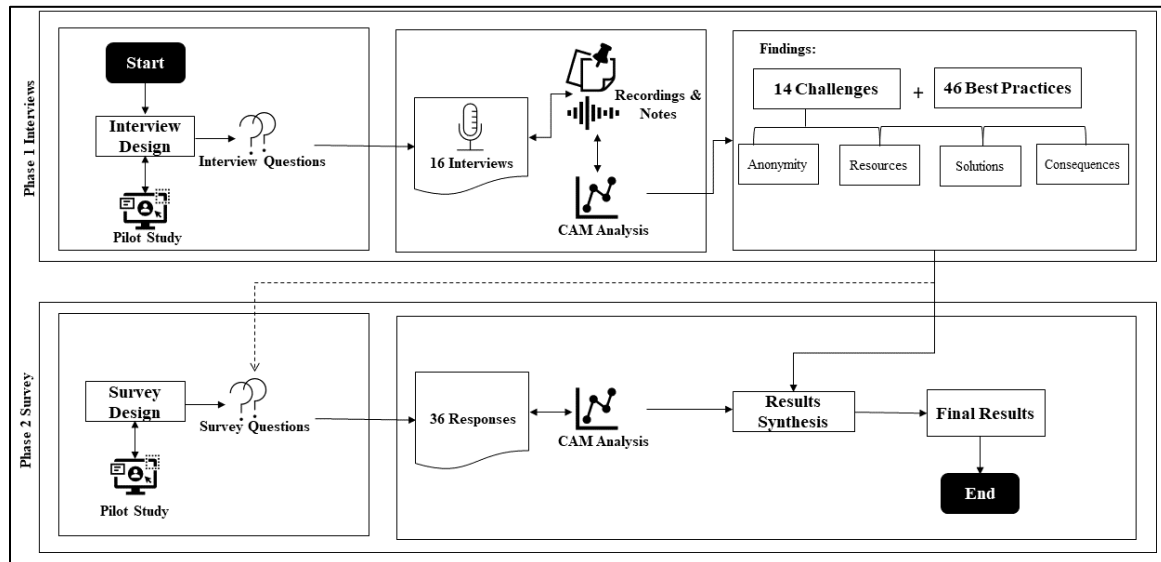


Figure 2: Interview Based Study Details.

3.1 Interview-Based Study

3.1.1 Participants

To address research questions from the industry perspective, semi-structured interviews were conducted with 16 security practitioners located mostly in Saudi Arabia (13), some in UAE (1), Egypt (1), and Kuwait (1). Our selection criteria include (1) The participant should be a security expert currently working in industry, (2) He/she should have some knowledge and practical experience in zero-day attacks. (3) He/she should have at least one year of experience or more occupying a security position. Having such a selection criterion ensures that the participants are highly qualified security experts working in the field; it also ensures the quality and the value of the data received. The participants were approached using LinkedIn social networking, and were mostly holding the title of Security Engineer, Security Analyst, Cybersecurity Consultant, Security officer, Specialist, etc. The utilized sampling technique was quota sampling, where participants are recruited based on predefined characteristics set earlier [76]The participants were all currently working in industry and had 2 – 30 years of experience in the security field. Table 2 summarizes the participants' demographic information.

Table 2: Interviews' Participants Demographics.

Participant ID	Role/Job Title	Years of experience
A	Cybersecurity Consultant	20+ years in IT field
B	Cybersecurity Analyst	4 years

C	Cybersecurity Consultant	4+ years
D	Cybersecurity Consultant, red teamer specialized	12+ years
E	Cyber security engineer, working inside the SOC center	3+ years
F	Archive Information Security Officer	+27 years in IT & Cybersecurity
G	Head of Cybersecurity	7+ years
H	Cybersecurity Consultant	7 years
I	SOC analyst	5+ years
J	Senior Regional Cybersecurity Engineer	9+ years
K	Cybersecurity Consultant, Specialist & International Trainer	12+ years
L	Chief Information Security Officer	10+ years
M	Cybersecurity Instructor & Consultant	8+ years
N	Senior Cybersecurity Consultant/ Engineer	2+ years
O	Cybersecurity Engineer	3+ years

P	Digital Forensic Incident Response (DFIR) Analyst & Consultant	5+ years
---	---	----------

3.1.2 Interview Design

The online semi-structured interviews lasted 50-90 minutes on average. The interview questions were tested first using a pilot study with a security Ph.D. student and a teaching assistant, which suggested important remarks and helped refine the interview questions. The interviews were recorded with permission and transcribed earlier to be ready for analysis and synthesis.

The interview questions (Appendix A) were designed to fill the gap and cover all aspects of the proposed research topic. A focused literature review was done, scanning multiple security research papers discussing zero-day vulnerabilities to end up with interview questions. Those questions were refined after round 1 of interviews adding several questions for round 2. The questions were divided into four main sets, each of them focusing on a different aspect related to zero-day attacks. The first set's main focus was zero-day attacks in general; questions related to the concept of zero-day itself, the frequency, and the disclosure decision were discussed. The second set was directed towards challenges faced when dealing with zero-day attacks including some missing security practices that might participate to make zero-days harder, from a security expert perspective. The third question set was solutions-directed, highlighting best practices, security controls, techniques, or some recommendations that might minimize the impact of zero-day attacks witnessed or used by the experts. The last set of questions was forwarded

to the organization maturity when dealing with zero-days and any suggestions for a new model that might help. An additional set of questions discussing the consequences of zero-days was available to ask when it is possible within the flow to make the interviews more dynamic.

3.2 Questionnaire Survey

Based on the interviews' findings, a list of challenges and recommended best practices were extracted. The questionnaire survey was designed to validate these findings and collect some insights to ensure certain factors and their importance.

3.2.1 Participants

A total of 36 security experts participated in the survey; the majority were located in Saudi Arabia (30), followed by UAE (4), then Algeria (1), and Germany (1). All participants occupy a security position at the present time, including SOC analyst, Cybersecurity Manager, Analyst, Consultant, Engineer, etc., with a range of 1 -18 years of field experience. Demographic information of the survey participants is presented in Table 3 and Figure 3, respectively. The survey participants were recruited using quota sampling with similar conditions to the interview participants mentioned earlier. The participants were contacted using their LinkedIn profiles, ensuring their authenticity, and the survey was available for around a month, from the end of March to the end of April 2023.

3.2.2 Survey Design

(Appendix B) The survey was divided into two question groups, one related to zero-day attacks' challenges and the other to best practices. The questions represented as 5-Point Likert Scale questions ranging from 'strongly agree' to 'strongly disagree,' a ranking

question for prioritization, and open-ended questions. This way, the participants were mostly asked if they would agree that this specific challenge/best practice is related to zero-day attacks. Followed by a space to add any extra challenge, best practice, or even an expert opinion related to zero-day.

Table 3: Survey Participants Demographics.

Participant ID#	Role/Job Title	Country	Years of experience
1	Cybersecurity Analyst	Algeria	1 year
2	Cybersecurity Specialist	Saudi Arabia	3 years
3	Senior Advisor Incident Response	Saudi Arabia	6 years
4	Senior Cybersecurity Analyst	Saudi Arabia	3 years
5	Penetration Tester	Saudi Arabia	1 year
6	Penetration Tester/ Vulnerability Assessment	Saudi Arabia	1 year
7	Incident Response Specialist	Saudi Arabia	5 years
8	Digital Forensic Incident Response (DFIR)	Saudi Arabia	5 years
9	Cybersecurity Advisor	Saudi Arabia	5 years
10	Penetration Tester	Germany	8 years

11	Information Security Officer	Saudi Arabia	3 years
12	Cybersecurity Specialist	Saudi Arabia	3 years
13	Penetration Tester	Saudi Arabia	4 years
14	Information Security Specialist	Saudi Arabia	2 years
15	Senior SOC Analyst	Saudi Arabia	4 years
16	Cybersecurity Analyst	Saudi Arabia	2 years
17	Digital Forensic Incident Response (DFIR) Engineer	Saudi Arabia	8 years
18	Cybersecurity Analyst	Saudi Arabia	2 years
19	SOC Analyst	Saudi Arabia	18 years
20	Security Engineer	Saudi Arabia	6 years
21	Digital Forensic Incident Response (DFIR)	Saudi Arabia	4 years
22	Cybersecurity Analyst	Saudi Arabia	1 year
23	Cybersecurity Analyst	Saudi Arabia	2 years
24	Security Analyst	Saudi Arabia	1 year

25	SOC Analyst	Saudi Arabia	2 years
26	Chief Information Security Officer	Saudi Arabia	15 years
27	Backend Developer for DFIR SaaS	Saudi Arabia	3 years
28	Senior Security Analyst	UAE	7 years
29	Cybersecurity Analyst	Saudi Arabia	2 years
30	Threat Intelligence Analyst	UAE	7 years
31	Cybersecurity Consultant	Saudi Arabia	5 years
32	SOC Engineer	UAE	3 years
33	SOC Manager & Independent Security Consultant	UAE	10 years
34	Cybersecurity Consultant	Saudi Arabia	7 years
35	Digital Forensic Incident Response (DFIR) Specialist	Saudi Arabia	3 years
36	Senior Cybersecurity Engineer	Saudi Arabia	3 years

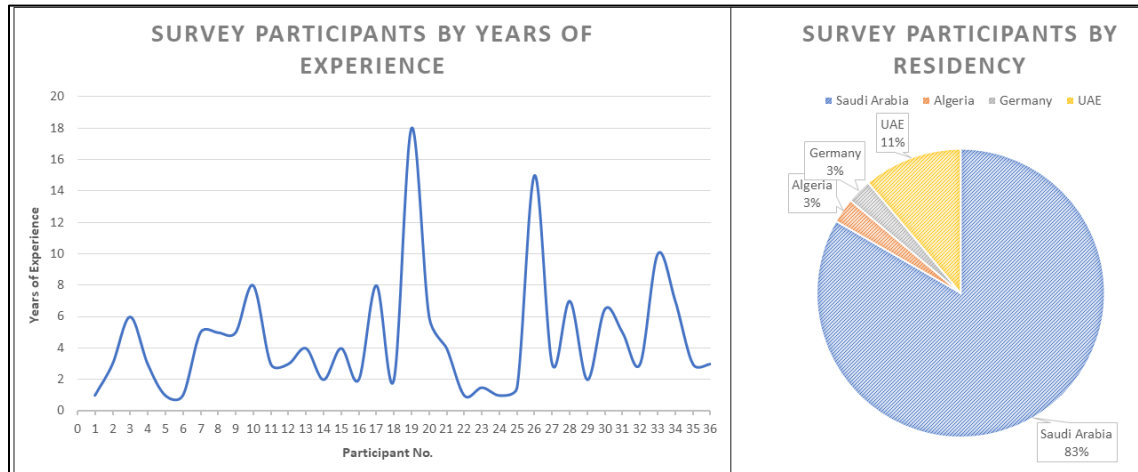


Figure 3: Survey Participants Demographics (a) by years of experience, (b) by residency place.

3.3 Results and Analysis

3.3.1 Interviews Findings

Interview responses were analyzed using the Content Analysis Method (CAM). In CAM, data is analyzed according to occurrences of keywords or following certain patterns [76]. The interview answers were reviewed and analyzed to derive meaningful outcomes. Certain keywords were highlighted, like the frequency, the disclosure, the impact, the solutions, and some real-life scenarios, etc., all related to zero-day attacks. Then, different cases belonging to each keyword were identified to explain the keyword widely. For example, for the “frequency” keyword, multiple cases would be defined as (frequent, not frequent, or it depends), and based on these cases, we can look deeper into how the experts’ opinions were reflected. Following this approach, the interview data was analyzed

according to the following categories: frequency and disclosure of zero-day attacks, zero-day attack challenges and consequences, solutions and best practices, as well as tools and maturity related to zero-day.

3.3.1.1 Frequency of Zero-day Attacks

Practitioners were asked about how frequently they encounter zero-day attacks as a part of their duties in security. Most participants indicate that zero-day attacks are encountered very frequently. Participants B, C, H, J & M stated it is an everyday situation as zero-day attacks exist everywhere and are commonly faced with almost every system somehow having a zero-day vulnerability. Participant J even stated:

“Zero-day attack happens every minute, maybe less than a minute. Basically, you're saying here, how frequently can a zero-day attack happen? It happens while we're speaking; it's just nonstop.”

Closer to that, Participant K said general zero-days happen weekly. However, participants K and M share an opinion that it happens very frequently, but not all of the zero-days encountered are severe or have considerable impact. Participant M even clarified with a common security observation stating that every year in December, the security community faces a severe dangerous zero-day. Participant P considered it has a monthly frequency, in which each month or two, we hear of a zero-day happening somewhere.

On the other hand, participants E, F, G, & I mentioned it is not a frequent event to be encountered, maybe once a year on average. Quoting participant I as follows:

“They don’t occur on a high frequency like normal attacks. However, whenever they occur, they can be the most destructive because they are undetected for a very long time.”

Other participants highlighted that frequency depends on certain company or domain factors. For example, participant A clarified that it is more common in software or systems, whereas it is a rare incident for devices or hardware. Participants L & O also said it depends on the size of the company and the number of security controls or solutions it has. Mentioning an important remark on the topic participant, O said:

“If the company initially has no process to recognize the zero-day vulnerability, So, it will not know about it, so the frequency will be zero as no one is searching for a zero-day vulnerability. in which it is a problem in itself.”

Summarizing what security experts shared was divided into three categories: very frequent, not frequent compared to others, and it depends (on company resources and security controls). Figure 4 highlights the percentage and opinions of participants in each category.

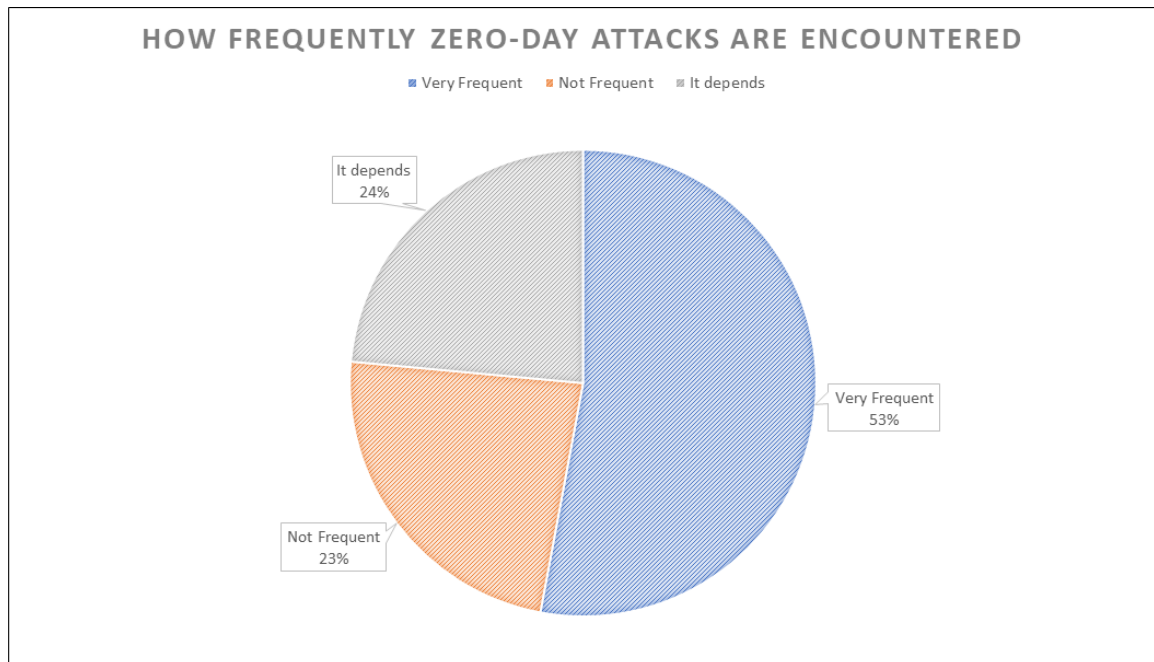


Figure 4: How frequent zero-day encountered? (By interview participants)

3.3.1.2 Public Disclosure of Zero-day Attacks

Participants were asked to balance whether companies normally disclose having a zero-day in their system within the organization or not. Disclosure means sharing with fellow organization employees, stakeholders, or even customers that we have encountered a zero-day. Sometimes, that might include announcing such important news to the public. Generally, participants almost agreed that companies usually do not disclose having a zero-day to the public. However, they report to the vendors having a zero-day attack to create a patch or to an authority depending on laws and regulations in different countries.

Participant J provides an example from Europe; in Europe, there is a General Data Protection Regulation (GDPR) authority that regulates companies hacked or attacked to

disclose the full attack scope or if any information has been leaked. Participant G mentioned that in the U.S., they have several laws and regulations for disclosure, especially what is called an Initial Public Offering (IPO). Participants B, D, E, F, and O mentioned that in Saudi Arabia, there is a National Cybersecurity Authority (NCA) to which each unauthorized access must be reported, following the data protection regulations. For financial sectors, participant L identified SAMA as they reported incidents that happened to it.

Participant F stated that the disclosure decision depends on different factors as companies have rules, and some might update their customers as required. In contrast, participant H mentioned that the decision is in the vendors' hands (for example, Microsoft), not the companies when they usually assign CV numbers for all existing vulnerabilities and announce that to their customers. Participants C & F highlighted that zero days are reported to the vendors in order to fix the issue and release a patch.

Participants I, K & M clarified that normally companies do not disclose unless they are forced by a law or regulations. To elaborate, participant M indicated the reason is related to maintaining their reputation, while Participant N guessed that disclosing might give attackers another chance to attack. However, participant K brought to light a significant remark as he said:

“Unfortunately, there is something called silent patch, for example upgrading from version 1.5 to 1.6, without telling their customers that the reason of this update release is a dangerous vulnerability. Which some users will not find a motive to update their software/system.”

From another perspective, Participant P showed that the public announcement happened after the patching, maybe considering the reasons mentioned earlier. Finally, participant O summarizes the disclosure decision in two points: an advantage (benefit) and law. Precisely, he said,

“Is it an advantage to disclose a zero-day for you or not? also, does the law force you to disclose or not?”

By advantage, would a company benefit from announcing a zero-day in the first place? It differs. For example, coming from vendors or entities selling cyber security solutions, the advantage is for sure not announcing being attacked. But it is different when it is announced by companies in the market, as “I’m the first in which patched and solved a zero-day before other vendors.” It would make a different impact.

3.3.1.3 Zero-day Attacks Challenges & Consequences

Practitioners were asked about the challenges they normally faced managing or dealing with zero-day attacks. The mentioned challenges were identified under several sections: challenges related to anonymity, challenges related to resources, challenges related to security tools, and challenges related to consequences. Figure 5 illustrates the detailed list of challenges.

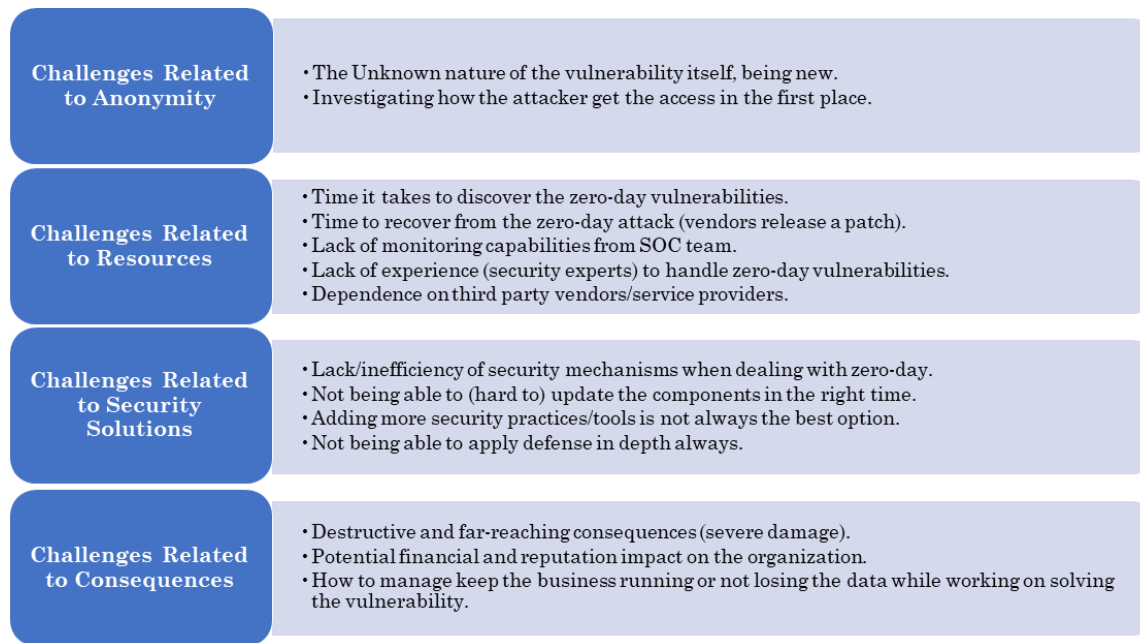


Figure 5: List of challenges organized by category.

The classification process was done through multiple steps and rounds. The first author looked into the interviews' transcript, finding keywords and connections then grouping them together based on their indications. Next, these findings were discussed with the second author refining the categories and their challenges. Finally, some samples were given to third and fourth authors of the study for a final cross validation of the process. Therefore, the final outcome of the classification process is ready and valid. Table 4 shows an example of some transcript samples being categorized.

Table 4: Examples of interviews transcript classification process (challenges).

Raw Data	Keywords	Indication	Category

“... is not knowing where this vulnerability location is (mostly as bug in code) and is there a vulnerability in this system or environment or not.” -Participant N	Not knowing where ... location is Is there a vulnerability ... or not	There is an indication of anonymous details related to zero-day attacks, in terms of, when, where, and how this attack happens.	Anonymity
“...That we do not know about the vulnerability itself, and the vulnerability is not public and not announced and nobody knows about it, so here we need to investigate and search for certain artifact that clarify there is a zero-day attack.” -Participant P	We do not know. Not public Not announced Nobody knows about	There is an indication of anonymous details related to zero-day attack, in terms of, when, where, and how this attack happens.	Anonymity
“...Because most companies implementing security solutions think they're secure. but it is the opposite as every tool can be bypassed. and second, doing it the	Every tool can be bypassed. Think they're secure	There is an indication related to the limitations' security tools might have when	Security Tools /Solutions

right way, also keep this technology audit and managed.” -Participant M		dealing with zero-days.	
--	--	-------------------------	--

3.3.1.3.1 Challenges Related to Anonymity

In terms of anonymity, the most common challenge mentioned by the interviews participants was the unknown nature of the zero-day itself being a new vulnerability. With a majority of almost 62.5% of total participants, it takes the first place among the challenges’ list. Participants A & B mentioned that since it is a new vulnerability, the company itself will not be aware of it. So, there is an unawareness of what system would be exploited, and how it is exploited. Participant C expressed this as the portion of unknown risk related to this vulnerability, while participant G expressed the same idea as the information related to this attack being rare. Participant I focused on awareness from end user perspective being the weakest part of most attacks, he said:

“...While the end user is not aware enough of such kinds of attacks, it becomes very easy for the threat actors to use the zero-day exploit against him/her and stay undetected for a long time and achieve their objectives.”

So, anonymity of zero-day meant as participant N refers to *“... is not knowing where this vulnerability location is (mostly as bug in code) and is there a vulnerability in this system or environment or not. (The unknown nature).”*

Another aspect of challenges related to anonymity is the investigation of how attackers gain access in the first place. Participants B, J, N, P all agreed that the need to search how attackers access the system is a challenge to clarify there exists a zero-day vulnerability. Participant P clarified the problem as:

“... our problem is not in the zero-day itself as it is in the idea "we will investigate until we reach the point where how the attacker gain access, here is the challenge. That we do not know about the vulnerability itself, and the vulnerability is not public and not announced and nobody knows about it, so here we need to investigate and search for certain artifact that clarify there is a zero-day attack.”

3.3.1.3.2 Challenges Related to Resources

Resources have a direct role in organizations’ ability to defend against any type of attacks. Hence, there is a need to shed light on challenges related to resources. Time, security teams (experienced personnel), and any third party involved (like vendors) are considered resources. Challenges related to any hardware or software solutions are discussed under the security tools section.

In terms of time, security experts define time of discovery and time of recovery as critical elements when managing zero-days. Time of discovery represents the detection time mentioned by Participant E, I, O, and where/how to start looking for vulnerabilities. Participant I explain it is a challenge as he said:

“...Most probably there will be a huge time gap between when the attack had occurred and when it was detected. Based on this gap, the risk and impact will be evaluated.”

Time of recovery represents the time needed by vendors to close the vulnerability and release a patch. It is simply the time needed to solve the issue. Participants H, I, O all agreed it is a challenge to close a vulnerability in a short time. Participant H commented on the reason it is a problem:

“...time to recovery (speed in minutes), so attackers won't have the chance (enough time) to get to the internal organization network critical assets.”

Participant O summarized time constraint as *“...vulnerabilities usually go through a long process to close it, so to close a zero-day in a very short time; a day, two, or three days is a challenge in itself.”*

In terms of security teams and personnel, participants D, I thought that sometimes the problem is related to the experience of security experts to handle zero-day attacks. Participant D said *“...It is the lack of experience (from security experts) sometimes worldwide when dealing with different scenarios.”*

Participant I addressed this as the limitations of skilled resources that can reactively and proactively act against such attacks. Clarifying that normally there is no proper incident response, threat intelligence and threat hunting programs. On the other hand, Participants A, C, I, J specified that the problem is mainly related to the monitoring capabilities of the SOC team being weak. Participant C explained the lack of such skills and their impact as follows:

“...Most organizations do not have monitoring capabilities from the security operation center, the capabilities of applying threat hunting and compromise assessments, which

leave them blind and that's what let attackers reach their objectives and exploiting such attacks.”

Participant J empathized with the SOC team although it is a challenge, it is not an easy job to do saying: *“People who live in the SOC basically have a very tough time to protect organizations from attacks, because attackers always try to find a way around the security controls that the organization have. And this is what they live on. You know they live on the challenge. They live on the excitement of breaking through security controls...”*

Final remark as a resources challenge, participants A, D considered waiting and depending on third party vendors/service providers as a main challenge. There is this scenario of uncertainty when there is no response from the vendor and there is no released patch yet. In addition, it might cause some/all services related to the components affected to be disabled waiting for the vendor’s update.

3.3.1.3.3 Challenges Related to Security Tools/Solutions

Security solutions includes any security hardware, software, mechanisms, architecture which is used in organizations by practitioners nowadays. Participant A, E, G, I, J addressed the challenge as the inefficiency or the lack of such solutions in dealing with zero-days. They said the problem especially is in solutions that rely on signatures to detect cyberattacks not on behavioral analysis. Participant J said: *“...your typical security tools will not see zero-day attacks, antivirus for example, because antivirus relies on signatures...”* Then he added:

“...The problem is how do you tune your security tools to make sure that the next stage or the next step, or the intention of that attacker does not reach its purpose.”

Participants K & M mentioned that the problem is not only in the solutions but having/adding more security practices is not always the best option. Participant K responded that:

“...adding more security means adding more code, which has the possibility to include vulnerabilities. Having vulnerabilities in security tools like antiviruses or firewalls itself means the attackers can exploit them and maybe access with higher privileges...”

Participant M added an important remark: *“...companies have security teams, budget, IDS, IPS, firewalls, technologies etc. So why, with all of these, do we still have attacks? Because there is a difference between implementing a technology and following/applying what is the most right. As 90% of leaked data is stolen from already encrypted databases. so why? People would think that implementing security controls infers that I'm totally safe...”* Then he added:

“...Because most companies implementing security solutions think they're secure. but it is the opposite as every tool can be bypassed. and second, doing it the right way, also keep this technology audited and managed.”

Finally, participant K highlighted another challenge as not being able to or it is hard to update the components at the right time. He explained in detail: *“A lot of systems are not homogeneous (one component only); no, they usually consist of multiple components. The single program or product used relies on a core developed by ten programming (software) components, each of these components has further their dependencies. So, this one product*

purchased by a company has tens of multiple components. If a vulnerability was encountered in one of the inner components or one of its dependencies, then how to deal with it? it is so complex.”

Another challenge that was specified by participant K is related to the defense in depth mechanism and how it is applied in organization. Although applying defense in depth would enhance security in organizations. However, it might increase the difficulty making it harder to use the network for normal users, which leads companies sometimes to give higher privileges to their employees. So, implementing such a mechanism is not an easy task.

3.3.1.3.4 Challenges Related to Consequences

Consequences are represented by the impact suffered by multiple parties as a result of being a zero-day attack target. This impact includes financial loss, loss of data, loss of business availability (services shutdown), reputation sabotage or even severe unrecovered damage.

According to participants A, B, E, F, G & K, it varies depending on the companies' scale, the services they provide, and their security defenses. To illustrate, usually for governmental entities and large organizations, it would be a loss of confidentiality to have unauthorized access to their data. Participants C, H, J & P said it depends on the attackers' motive or purpose. Quoting participant P:” *...The main objectives of zero-day are either gaining access or privilege escalation. What comes after that is what defines the impact that happened. Using a zero-day unknown vulnerability, using attackers' skills moving*

from end point to another depending on threat actor objective.” In addition, participant H added:

“...these APT groups have their own goals and agenda. Their motivation differs, when we know their motivation, we know what to protect. Stealing confidential data, destroying the business, getting certain information. depends on APT group motivation...”

Around 9 out of 16 participants addressed the potential financial or reputation impact on the organization. To illustrate, participant J spoke extensively on the topic:

“...A reputation I think is big for reputable companies if you think about finance sector, for example, they will lose their reputation if a cyber-attack has hit them, their reputation would be just damaged, and they will lose customers...”

Then he elaborates *“...for example hotel chains have been attacked in the past and those attacked hotel chains typically they lose their customers just because the personal data of those customers has been exposed, and people tend to avoid those hotels and they don't go back to them...”*

For the severe damage that might occur as a result of zero days, participants F, M, P, & H acknowledged these destructive consequences as a challenge. Participant M emphasized the matter, saying, *“...if attackers attack specific targets, it usually causes extreme damage depending on their goal. & zero-day market becomes big business.”*

The last challenge as consequences would be how to manage keep the business running or not losing the data while working on solving the vulnerability. Participants B, D, F, K, & M admit it is one of the challenges identified in industry.

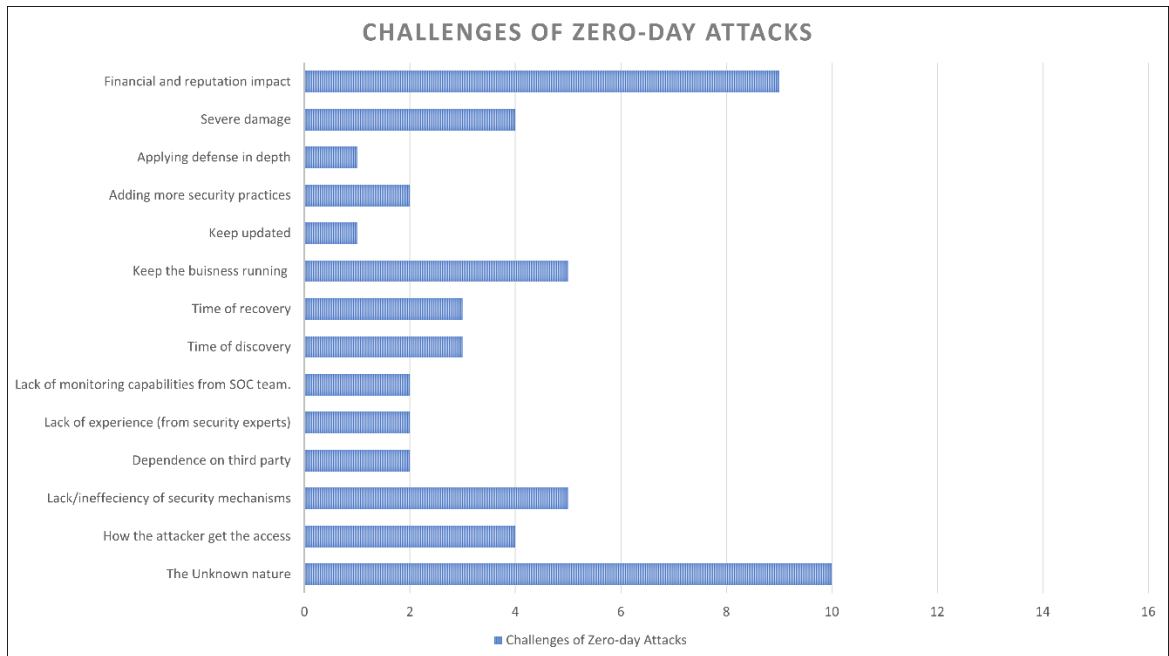


Figure 6: Frequency of each challenge (By interviews participants).

3.3.1.4 Zero-day Attacks Solutions and Best Practices

Participants were asked about solutions or best practices to handle or defend against zero-day attacks effectively. Participants all agreed that there is no such solution to prevent zero-day attacks totally, but all suggested practices are to minimize their impact or resulting damage. Participant A reflected that the solutions applied depend on the company itself and the medium, whether the web, emails, or network. In addition, participant C mentioned that solving an exploit starts with the vendors themselves who are developing the software. Participant G clarified it depends on TTPs (Tactics, Techniques, and Procedures); exploiting the vulnerability itself may be new (as a zero-day), but the techniques and tactics that are used may be common. Participant I mentioned that it should be multiple layers of

security applied to achieve better defenses *“I believe the successful defense starts with the ability of detecting the first hit. Organizations must deploy multiple layers of security that make it harder for the attackers to achieve their objectives. These layers should cover the entry points of the organization and its data...”*

Moreover, participant P stated that it is important for security teams in organizations to have a full inventory of the entire infrastructure in the organization. Having this inventory list of all products used and exist, makes you aware of what you have to be able to defend. Then, he suggested categorizing these applications on which is more critical to the business. So, you know and act better in critical situations which to solve first. Participant L suggested a strategy including three environments; development environment, test environment, and production environment when releasing a product to minimize any bugs or vulnerabilities. To highlight an important remark, participant J commented, *“...It's a strategy, more than the number of tools. if I've seen companies struggle. I've seen them with too many tools, which is very common nowadays. You might see an organization of 15 to 50 tools. 15- 50 security tools in their arsenal. The problem is not in the tools. The problem on how to operate those tools, how to integrate those tools, and this is why many organizations these days actually think of looking for consolidation trying to actually minimize the number of security tools because it becomes unbearable...”* Additional solutions suggested included patching & monitoring (from the vendor), access controls, EDR, NDR, NAC, zero-trust architecture, defense-in-depth mechanism, and having a strong SOC team.

Based on what experts introduced, it is not a matter of a specific tool or solution. It is a collection and layers of security healthy practices, which are applied in the right way, with

knowledge, and implemented on both organizational and individual levels. A total of 46 best practices were collected from interviews as suggested by the security practitioners, witnessing they were impactful based on their experience in industry. Table 5 shows the complete list of best practices collected from interviews.

Table 5: Best Practices list (Interviews outcome).

Best Practices Collected from Interviews				
All organizations should follow Cyber security Authorities regulations and recommendations.	Be prepared for future attacks because it will happen.	Monitor your system & know your assets.	You cannot prevent zero-day attacks but try your best to detect them.	Proper network segmentation & isolation.
Focus on user awareness & education.	Apply defense-in-depth strategy.	Apply the SASE architecture.	Keep all software, firewalls, and browsers updated.	Multi-layer network architecture
Train employees in threat mitigation.	Apply zero trust architecture.	Apply the least privileges principles.	Create rules inside security controls to be based on behaviors.	Use secure ports for your network.

Have a solid SOC center to detect and have 360° view of the organization work.	Invest in security control tools like DLP, sandboxing, etc.	Systems baselining and hardening (Detection).	Follow the logs and traffic on the firewalls themselves, and watch the tickets itself, using multiple different ports, different protocols.	Minimize the number of devices facing the Internet.
Apply policies and standards for ex; NCA policy, OPT standards, ISO standards etc.	Use MITRE framework	Make sure to backup, frequent backups make sure you can survive worst-case scenarios.	Zero Day Initiative (big bounty programs).	Apply EDR and NDR solutions.
PURPLE team collaboration to discover vulnerabilities before attackers do.	Cover each stage in attacks lifecycle (Cyber Kill Chain) is crucial for detection.	Care of internal systems/servers as well as external servers/systems.	Apply threat intelligence, vulnerability scanning, and patch management.	Do not focus on zero-days as the real obsession, focus more on having a secure infrastructure.

Have Research and development team (RND), to research vulnerabilities and try to fix them.	Use monitoring and deception technologies/ techniques.	Safe/secure administration of systems.	Build use cases in the SOC, to identify zero-day vulnerabilities (identify vulnerable devices).	Have an inventory list of the entire infrastructure in the organization. Then, categorize these applications on which is more critical to the business.
Apply human security hygiene concept.	Use initial or temporary solutions to limit the impact of this zero-day.	Do not share passwords and keys between systems.	Do not leave default credentials/configurations of security tools as it is. (Coming from vendor)	Monitoring for persistence techniques.

Invest in security teams.	Use encryption methods.	Apply system security hygiene concept.	Apply Quality of service (QoS) policy to distribute the requests on multiple zones.	Monitoring for suspicious communication.
---------------------------	-------------------------	--	---	--

3.3.1.5 Tools and Maturity

Participants were asked about the potential for designing a tool or a model specifically for zero-day attacks and how well it would be received and used by the industry. To initiate the topic, participants were encouraged to discuss how different or similar zero-day should be treated compared to other vulnerabilities. Participants J, K, & L, who answered that they should be treated similarly, tended to look at the technical aspects of the vulnerability and the process to solve the attack as it is all similar whether it is a known or unknown vulnerability. Participant J explained:

“I think they should be treated similarly to be honest, because if you cannot protect the organization already from the existing vulnerabilities, it means that you are not ready for a zero-day attack.”

Participant L also shared his opinion: *“...after detecting the zero-day attack, the mechanism to avoid this type of attack by patching this vulnerability, for that it is the same...”*

Interestingly, Participant K made a point saying “...similarly, other vulnerabilities should be treated similar to zero-days (not the other way around), we should always have done monitoring your assets, analyzing requests, security reviews frequently, following updates and news related to vulnerabilities...”

However, those who answered zero-day should receive a different treatment defended their opinions with strong arguments. Participant M argued that it should be treated in a special way, as zero-day normally gets prioritized to be solved first when other vulnerabilities are present. He said, “...All companies encounter different types of vulnerabilities every day. However, if the company receives a report that has a SQL injection or any type of vulnerability, the other hand, received a report having a zero-day, then, of course, zero-day would have the priority to start solving it. As the losses or the impact cannot be predicted at all. It has priority in protection and remediation as well...”

Participants N & O based their opinions on the unknown and unexpected nature of the zero-day vulnerability, so we need to deal with more care and protection. Moreover, participant O added that zero-day detection requires a high level of experience, and zero-day more likely would have a high level of severity, hence a higher priority. Participants A, E, & P stated it is different due to the way security people handle or manage the attack, it is monitored based on suspicious behavior. To clarify, participant P mentioned, “...The way security people handle it is different. In the case of known vulnerabilities, I'm only waiting for the patch, and I already have the rules ready. detection and prevention are available as rules and feed everything, so if it is known, I have rules to prevent this. However, in the case of zero-day, no one knows about it; it is different. We rely on behavior to detect the

unknown, because techniques and tactics used by attackers are different, every threat actor is different than others...

In Participant I's opinion, zero-day should be treated the same as other vulnerabilities in some areas and differently in others. He explained this by saying, "...relying on some security solutions to detect all kinds of attacks without properly creating effective rules on these solutions that cover most of the attack cycle will ultimately result in detection and eventually prevention failures. When an organization relies on a solution where its detection is mainly based on signatures of certain attacks, it will result in successful defense evasion and achieving the attackers' objectives at the end. So, it's very important to utilize the security solutions in place all together to effectively cover each and every stage in most of the attack lifecycle..."

From a different perspective, participants were asked about how helpful it would be to have a model or tool to give some feedback and recommendations on organizations' maturity dealing with zero-day. Starting with participant J, he stated that such tools are a necessity these days "... Many organizations today ask for security services in the sense of security advisory services, they ask for incident response assessment, they do penetration testing, they do gap analysis. They ask for these types of things. Why they are asking for this because they understand that they have gaps. They want to tighten their security tools. They understand that they need to do better when an incident happens..." However, he mentioned that it might not be considered by organizations highly if it's only for zero-day, although it will be helpful "... a maturity security tool that takes into consideration all the concepts that we spoke about zero-day attacks, then I think it will help organizations to be considered. If it's only Zero Day, it might not fly with many organizations..."

Participant L hesitated for a while thinking it is a technical security tool to cover detection, mechanism, procedure of zero-day, saying it is really hard for a single tool to cover all aspects of zero-day. Then, after realizing it is a criteria-based model to evaluate maturity and give feedback to organizations, he highly supported the idea, and I quote, “...*the idea is very excellent, the market needed something like that, I've never seen something similar...*” Participant K commented that it would be helpful, but the idea is in the actual implementation of the model in the real-world, not the model itself (how well it is going to be used and implemented by the industry). also, it depends on the organizations or the side to be interested or not. Other participants A, E, I, M, N, O, P all supported the idea and thought it would add value. Participant I clarified, “... I believe this will be really good for sure; some organizations perform some of this in a *manual way*. ...*So having a tool/model as you suggest will definitely be effective and will help reduce the time and effort the company spends on this part. it could be effective for both known and zero-day attacks.*”

Participant M connected the need for such a model to some famous incidents encountered in security as he said, “...After log4j zero-day become so popular and people now know how effective it can be in destroying a business or causing damage, so I guess yes organizations will be interested...”

Moreover, participant N stated that it might help increase organizations' awareness and expand their knowledge of zero-day attacks: “*It is very excellent and helpful, as many organizations do not know how prepared they are to deal with zero-day attacks. So having such a tool or a criterion specifying each level each organization belongs. It supports organizations who are not fully aware of this area...*”

Participant O responded positively as follows: “...yes, of course there will be an interest in such a topic. Vendors usually depend on the experience they collect from people, people working for them, the behavior, scenarios implemented previously, and how it performed, etc. Implementing such a tool is excellent...” he added and suggested, “...Hopefully, organizations will be so interested in such a tool, as the result of it will be excellent and helpful in sha Allah. I support having knowledge areas. As you mentioned, that is what I was thinking of as a challenge, but having a KAs will be easier and much clearer to follow. The idea is really excellent, I do not see much similar tools existed, and a lot of people depends on the features of the products themselves, they do not use certain model to measure their performance (maturity level).”

3.3.2 Questionnaire Survey Findings

3.3.2.1 Responses to Zero-day Attacks Challenges Statements

Participants were asked to participate by agreeing on and grading each challenge statement from 1 (strongly disagree) to 5 (strongly agree) based on their experience in the industry. There were 14 challenges statements in total collected and analyzed from the interviews responses. Table 6 reflects the number of participants under each option.

Ch1: The Unknown nature of the vulnerability itself, being new. The first challenge was mostly agreed on, with the highest majority of 32 participants. On the other hand, 3 participants disagreed, and one was neutral.

Ch2: Investigating how the attacker got the access in the first place. Another challenge related to anonymity was mostly agreed on by 25 participants, while 6 disagreed, and 5 were neutral about it.

Ch3: Lack/inefficiency of security mechanisms when dealing with zero-day (tool perspective/limitations of security solutions). The third challenge focused on the solutions aspect and tool perspective. Although responses were more into the agreement side by the majority of 24 participants. However, a considerable 10 participants were neutral about it, and only 2 disagreed.

Ch4: Dependence on third-party vendors/service providers. For this challenge statement, responses fluctuate, with a majority being neutral 14 participants. This was followed by 8 participants who disagreed, 7 agreed, 5 strongly agreed, and finally, 2 strongly disagreed (a total of 12 agreements and 10 disagreements).

Ch5: Lack of experience (from security experts) to handle zero-day vulnerabilities. Around 72.23% of participants agreed with this challenge statement, while 19.45% disagreed, and 8.34% were neutral.

Ch6: Lack of monitoring capabilities from the SOC team. A total of 21 participants agreed with the statement, while 9 disagreed and 6 were neutral.

Ch7: Time it takes to discover zero-day vulnerabilities. The survey participants approved it as a challenge, with a large number of 30 agreements. Compared to other choices, the results show 3 neutral and 3 disagree answers.

Ch8: Time to recover from the zero-day attack (vendors release a patch). Answers were mostly leaning to agreements by 19 participants. However, 10 answered neutrally and another 7 disagreed.

Ch9: How to manage to keep the business running or not losing the data while working on solving the vulnerability. Around 66.67% of respondents acknowledged it is a challenge, while 19.45% disagreed with the statement, and 13.89% were neutral about it.

Ch10: Not being able to (hard to) update the components at the right time. This challenge statement was approved by 22 participants, neutral to 10 participants, and disapproved by 4 of them.

Ch11: Adding more security practices/tools is not always the best option. (More tools = more code, = more vulnerabilities). A closer gap for this statement between 19 participants agreeing and 12 being neutral about it. However, only 5 participants disagreed.

Ch12: Not being able to apply defense in depth always, as sometimes if applied correctly it might become harder to use the network for normal users. For this statement, 19 participants agreed that applying defense in depth mechanism is not easy, while 9 participants disagreed and 8 were neutral about it.

Ch13: Destructive and far-reaching consequences (severe damage). A small gap was found between the responses to this statement as 17 people agreed, and 13 were neutral regarding the damage being a challenge. On the other hand, the rest of the 6 participants disagreed.

Ch14: Potential financial and reputation impact on the organization. In response to the last challenge, 61.12% of participants agreed with the statement, 9 were neutral about it, and 5 disagreed.

Table 6:Challenges Survey Results (no. of participants).

Challenge	No. of Participants (out of 36)		
	Agree	Disagree	Neutral
1: The Unknown nature of the vulnerability itself, being new.	32	3	1
2: Investigating how the attacker got the access in the first place.	25	6	5
3: Lack/inefficiency of security mechanisms when dealing with zero-day (tool /limitations of security solutions).	24	2	10
4: Dependence on third party vendors/service providers.	12	10	14
5: Lack of experience (from security experts) to handle zero-day vulnerabilities.	26	7	3

6: Lack of monitoring capabilities from SOC team.	21	9	6
7: Time it takes to discover the zero-day vulnerabilities.	30	3	3
8: Time to recover from the zero-day attack (vendors release a patch).	19	7	10
9: How to manage to keep the business running or not losing the data while working on solving the vulnerability.	24	7	5
10: Not being able to (hard to) update the components at the right time.	22	4	10
11: Adding more security practices/tools is not always the best option. (More tools = more code, = more vulnerabilities).	19	5	12
12: Not being able to apply defense in depth always, as sometimes if applied correctly it might become harder to use the network for normal users	19	9	8
13: Destructive and far-reaching consequences (severe damage).	17	6	13

14: Potential financial and reputation impact on the organization.	12	5	9
--	----	---	---

3.3.2.2 Responses to Zero-day Attacks Best Practices Statements

Participants were asked to grade each best practice statement from 1 (strongly disagree) to 5 (strongly agree) based on their experience in the industry. There were 46 best practices in total collected and analyzed from the interviews' responses.

For the best practices statements listed, responses were mostly leaning into agreements side with most statements having 20+ participants approvals. Moreover, around 11 best practices suggested gets 30+ agreements which represent the majority of participants. For example, practice number 3 stated as "Monitor your system & know your assets" got a total of 26 strongly agreements, 6 agreements, 2 neutral, and 2 disagree responses. In addition, practice number 37 stated as "Having a qualified team to solve the vulnerabilities encountered and investigate the tickets (invest in security teams)" has 21 strong agreements, 10 agreements, 4 neutral, and 1 disagreement responses. Based on the two mentioned examples among participants having 32 and 31 agreements respectively, it clearly reflects the highest majority of participants' opinions. Only 2 best practices (number 10 and number 25) received below 20 agreements, with a total of 19, and 18 agreements respectively, which is still a considerable high number.

3.3.2.3 Responses to Open Ended Questions (Additional Challenges or Best Practices)

Participants were given two open-ended questions, and asked to suggest other challenges and best practices if they have any in mind. For challenges, around 50% of participants added nothing or kept the space empty with no answer. Other participants suggested some challenges which mostly fall under the challenges mentioned as a part of the list. For example, participant no.4 write “Some of the security tools even the biggest in market they are not detecting same these behaviors, because it’s unknown and no buddy they know it, even you build a defense in depth module” which basically combines the “inefficiency of security tools” “the unknown nature” and “the inability to always apply defense in depth” which all listed previously. Participant no.28 mentioned “Catching the first steps of the attacker and knowing how he was able to get access into the network is the hardest part of investigation.” Which also comes under the challenge we have of “investigating how the attacker gets access in the first place”.

Other participants explained a bit regarding the topic, some of them mentioned the security teams and to align communication that we’re having a zero-day. Other participants highlighted the idea that the impact differs between organizations, and it depends on the type of organization whether it is IT, financial etc., as we discussed earlier in interview results.

For best practices, around 61.12% provide no answer mentioning that it has been covered already in the survey. Using sandboxes, having use cases, building a good SOC team, network segmentation, monitoring, update when available, and have a 360 view of the

activities etc. were some of the practices written by the participants, in which in a way or another match the practices collected earlier.

CHAPTER 4

MULTIVOCAL LITERATURE REVIEW (MLR)

MLR is defined as all literature that can be accessed on a specific subject, which encompasses both published (formal) literature as in journal and conference papers and grey literature as in blog posts, videos, and white papers [25] [23] [77]. In the context of this research, zero-day attack-related studies will be collected and analyzed to discover challenges and best practices. Papers from formal and grey literature will be filtered according to specific criteria to end up with the official set of resources related to the topic. The extracted challenges and best practices data will be analyzed and presented in a list representing this research topic's state-of-the-art.

4.1 MLR Process

4.1.1 Goal & Research Questions

The MLR aims to collect challenges and best practices mentioned or discussed in previous research from both published sources and online unpublished work. That's all for providing useful insights on this topic to all stakeholders interested in zero-day attack knowledge, including other researchers, security experts, and organizations. Choosing MLR over the Systematic Literature Review (SLR) provides a wider spectrum of the data we're looking for, as security practitioners mostly write grey literature. This means both academic and industry points of view are considered and analyzed.

To address the goal of the MLR study, the following research questions are discussed:

RQ1: What are the challenges encountered when dealing with zero-day attacks?

RQ2: What are the solutions and best practices suggested to deal with zero-day attacks?

4.1.2 Search Query Definition

The search query can be obtained by multiple combinations of terms extracted from the research questions and constructed using Boolean characters “OR” and “AND” [78]. The main keywords of this research would be “challenge”, “best practice,” and, “zero-day”. Multiple variations and synonyms of the keywords were included to cover all possible search varieties. For the challenge, “difficulty” and “risk” might be some synonyms. For zero-day, the words “attack,” “vulnerability,” and “threat” are all included to cover all attack lifecycles. However, after the general search, we figured out the “best practice” keyword was not included explicitly in research using this term, as no studies specifically discussed this side. Therefore, we decided to go for “detection” or “prevention” terms for better results, as most studies were solutions forwarded proposing either an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS).

Following these considerations, the search query was defined as follows.

(‘zero-day’ **OR** ‘zero day’) **AND**

(‘attack’ **OR** ‘threat’) **AND**

(‘detection’ **OR** ‘prevention’ **OR** ‘risk’ **OR** ‘vulnerabilit*’ **OR** ‘challenge’ **OR** ‘difficult*’)

4.1.3 Source Selection

This includes specifying the databases confirmed to apply the search query and derive the output list of academic and grey sources. To locate available formal literature, five databases were considered including: (1) *IEEE Xplore*¹, (2) *Springer Link*², (3) *ACM Digital Library*³, (4) *Science Direct*⁴, and (5) *Wiley Online Library*⁵. The selection of these databases was derived from the intention of considering as many sources as possible to support the process of literature review. These search engines are highly recognized and respected in software engineering and computer science field, and have variety of resources between journals, articles, conference papers, etc. all needed to satisfy our research questions.

For the grey literature, as widely considered in other MLR studies [23] [25] *Google search*⁶ was used for finding grey resources. In addition, *Sans*⁷ and *isBuzz*⁸ websites were included in the search process as confirmed widely known sites for cybersecurity topics and articles.

4.1.4 Inclusion & Exclusion Criteria

¹ <https://ieeexplore.ieee.org/Xplore/home.jsp>

² <https://link.springer.com/>

³ <https://dl.acm.org/>

⁴ <https://www.sciencedirect.com/>

⁵ <https://onlinelibrary.wiley.com>

⁶ <https://www.google.com/>

⁷ <https://www.sans.org/emea/>

⁸ <https://informationsecuritybuzz.com/>

The inclusion and exclusion criteria procedure ensures that only studies relevant to the research topic and questions are included. To satisfy this purpose, the criteria for this research included research studies from journals and conferences presented in English. In addition, studies related to the search term and keywords were included, while duplicated publications (keep recent) and incomplete text articles and books were excluded.

The full inclusion/exclusion criteria for formal literature are as follows.

Inclusion criteria:

- Studies published in English.
- Studies discuss risks, problems or vulnerabilities related to zero-day attacks.
- Studies present solutions to deal with zero-day attacks through prediction, detection, and/or prevention.
- For duplicate publications of the same study, only the recent and most complete version will be included.

Exclusion criteria:

- Non-English publications.
- Papers that are not directly linked to the research questions.
- Books, book chapters, and non-full text articles are excluded.

4.1.5 Quality Assessment Criteria

Quality assessment criteria reflect the decision-making process of evaluating and filtering the selected studies based on their quality. This ensures that the final resources list has the

most relevant research studies. For formal literature, the quality assessment criteria include the following questions:

- Is the objective of the research clearly defined?
- Is the study methodology clearly defined?
- Is the presented approach clearly explained?
- Are the findings of the study clearly stated and supported by reporting results?
- Does the study add value to the academia or the industry community?

For the grey literature, we define one criterion as the inclusion/exclusion combined with the quality assessment adopted from the grey literature guidelines [23]. The list of grey resources was tested against the criteria given a score where each statement/question scored as (0 or 1), excluding resources below a threshold of 5. Table 7 presents all the details of the grey literature quality assessment criteria.

Table 7: Quality assessment criteria of grey literature [23].

Criteria	Questions
Authority of the producer	• Does the author have expertise in the area? (e.g., job title principal software engineer)
Methodology	• Does the source have a clearly stated aim? • Is the source supported by authoritative, contemporary references? • Does the work cover a specific question? • Does the work refer to a particular population or case?
Objectivity	• Is the statement in the sources as objective as possible? Or is the statement a subjective opinion?

	• Are the conclusions supported by the data?
Date	• Does the item have a clearly stated date?
Outlet type ⁹	• 1st tier GL (measure = 1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers • 2nd tier GL (measure = 1): Moderate outlet control/Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as Stack Overflow), Wiki articles • 3rd tier GL (measure = 0): Low outlet control/ Low credibility: Blogs, emails, tweets

4.1.6 Execution of MLR Process

To successfully execute the MLR, a generic search phase was performed in the beginning to explore the research topic and better understand the papers published in this area. This step helped me better write the research questions and decide on the keywords. Next, the research questions and keywords were confirmed after trying several variations of the search, and the search query was resolved. The formal part of the literature search started first. The inclusion/exclusion criteria were reviewed and confirmed, as well as the quality assessment criteria. After that, the search query was applied to the five academic databases mentioned earlier to get the initial set of results without any filtering. The results list gets reduced when inclusion/exclusion criteria are implemented and filtered further by the quality assessment criteria. We have the final list of formal academic papers complete and ready for data extraction and synthesis, including 243 published papers.

⁹ Media Outlet: A means of communication or publication, like a newspaper, website, or television channel through which news, information, or entertainment is broadcasted.

The grey part of the MLR process started next, defining the criteria. As stated by the guidelines paper [23], part of the MLR process started next, defining the criteria. As stated by the guidelines paper [23], the inclusion/exclusion criteria and the quality criteria are combined for the grey literature. So, the criteria get defined, reviewed, and prepared in advance. The search string was implemented in the defined sites and search engines identified, then filtered by criteria to have the final list of grey resources having 71 papers in total. The MLR process ended with 314 resources combining formal and grey literature results. Figure 7 highlights the detailed representation of the MLR process. Details of MLR's formal and grey list of resources, extracted data, frequency, etc., are in Appendix C.

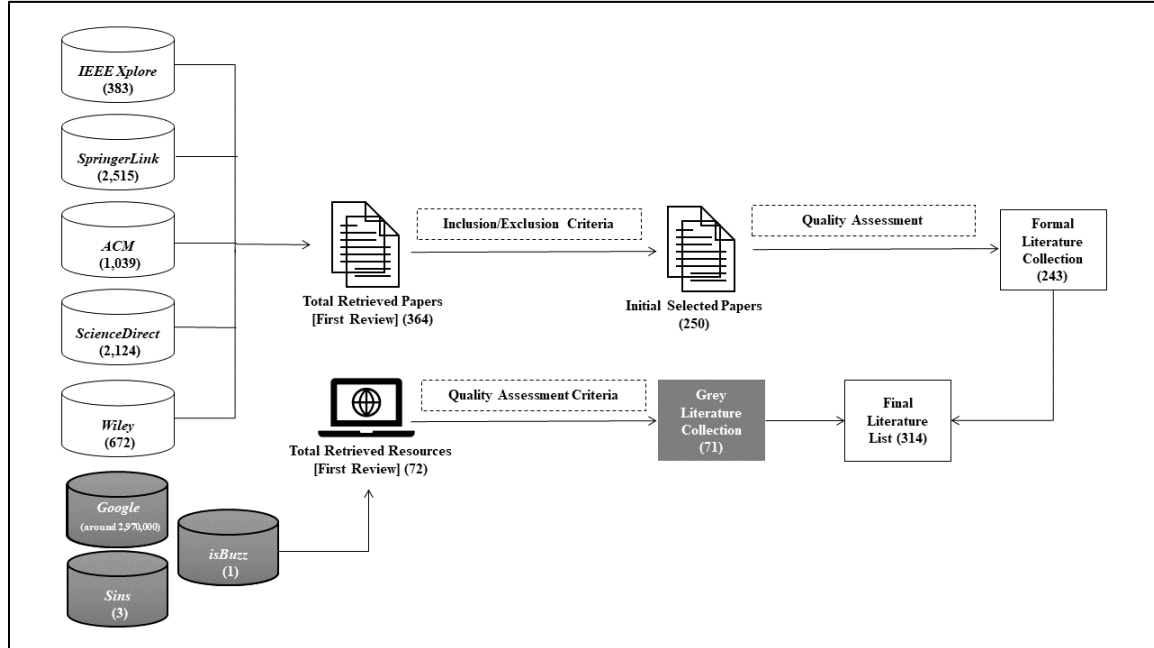


Figure 7: The complete MLR process.

4.2 MLR Findings

4.2.1 Zero-day Attacks Challenges

This section presents challenges related to the nature of zero-day attacks and limitations of various detection techniques.

4.2.1.1 The nature of zero-day attacks

The Zero-day vulnerability is classified as the most harmful threat for different organizations [79]. Although several techniques exist to tackle attacks like upgrading, antiviruses, and system patching, it is still a challenge to tackle zero-day attacks due to the lack of information related to the attacking nature [79], [80]. Zero-day attacks are difficult as there are no known signatures related to zero-day malicious attacks [81]. Timeliness of threat is an essential factor when dealing with zero-day exploits [82]. According to [82], the reason for zero-day effectiveness is that it is hard to detect such attacks for extended periods (months or even years) [82]. Even when the threat is identified, it takes days or sometimes weeks for patching to be completed [82], [83]. On average, a zero-day attack may stay continuously for 312 days [8], [84]. Besides, attackers are always ahead of defenders, not only in time but also in knowledge and skills [22], [84].

Fagioli et al. stated that zero-day risks commonly include financial harm, reputational damage, and operational chaos [21]. In terms of cost, the value of such vulnerabilities is huge to attackers since the problem is unknown to the developers of infected software and

hardware [85], [86]. A Ponemon Institute study reflects the average worldwide loss of companies due to zero-day attacks exceeded 7.7 million dollars per company, with a continuous rise of 19% yearly [87]. Due to its value, Fernandes et al. mentioned that zero-day vulnerabilities are sold in crime packs at underground markets [88]. The trade-in zero-day markets differs based on whether a market is white, grey, or black [17]. The interests of the audience of such markets are better satisfied when vulnerabilities are still unpatched, leading for no public disclosure [89]. The exploit can be reused for the damage related to zero-days, and sometimes additional exploits or new varieties of zero-day attacks keep being generated [90], [91]. To illustrate, Kaur et al. stated that if such worms are not detected and contained at the right time, they can cause severe havoc or potentially disable the Internet [92].

4.2.1.2 Techniques-based limitations

Intrusion detection is a known cyber security mechanism used in host and/or network environments to detect malicious activities [93]. For attack detection, methods are classified as Signature-based (Misuse based), Anomaly-based, and Hybrid based methods [93]. In addition to machine learning techniques, deep learning techniques, honeypots, and blacklists are all used to detect zero-day attacks, but each method has its own limitations.

Signature-based methods are usually unable to detect zero-day attacks, as they require frequent updates of the signature database [94], [95], [96]. So, as the database does not include a matching signature, any new attack needs to be extracted and stored [97]. Anomaly-based methods can detect zero-day attacks usually, but they suffer from a high false-positive rate [98], [99], [100]. This is because they may fail to differentiate between

known attacks and benign activities, leading to incorrect classification of valid software as malware [101] [102]. Therefore, the misuse and anomaly detector are considered complementary, which leads to the hybrid approach that uses both methods [103] [93].

Honeypots are systems designed to deceive the potential attacker with an emulated system to keep him away from the real system [104]. However, an attacker might figure out a honeypot based on prior knowledge of fingerprinting [104]. Innab et al. mentioned that using honeypots involves many risks, as getting attacked leads to attacking other computer systems on the network [104]. Mirza et al. considered the main limitation of a honeypot is being passive, not active [105]. Milenkoski et al. classified honeypots as low-interaction and high-interaction, discussing the pros and cons of both [93]. Low-interaction honeypots are not expensive and helpful for encountering labeled malicious activities, but they are not flexible, can be recognized easily by attackers, and cannot detect zero-day attacks [93]. High-interaction honeypots (pure) are flexible and can detect zero-day attacks, but they are expensive, and labeling recorded attacks can be time-consuming [93].

Blacklists consist of a list of phishing URLs and IP addresses detected previously, which are updated in certain intervals [106]. Since the lifetime of these websites is so short, this list will not contain all phishing websites at any specific moment [107]. The attacker will utilize the time between starting the attack and its detection to deceive many users [107]. Therefore, blacklist methods are not able to detect zero-day phishing URLs [108], [109]. These URLs will not be identified as they are not included previously in the blacklist [108]. This means, by using new IP addresses not involved before in malicious activities, attackers can easily surpass a blacklist [110].

Intrusion detection systems based on machine learning or deep learning techniques might be commonly used recently. Supervised learning techniques may be effective in detecting known attacks but cannot detect unknown or zero-day attacks as they depend on labels. For example, one-class SVM has a very low zero-day detection rate because its classification boundary of zero-day activities is poor [111]. Unsupervised learning algorithms do not rely on labels, so there is no difference between known or unknown attacks. However, they may encounter misclassification of known attacks compared to supervised. Kumar et al. stated that detecting zero-day attacks using ML or neural network techniques ignores several elements like the frequency of particular byte streams in network traffic and their correlation [112]. Especially for neural network models that require higher traffic for correct prediction [112]. Usman et al. mentioned existing systems relying on antivirus, blacklists, or ML techniques do not accurately classify zero-day attacks [113]. In addition, these systems are not updated regularly due to the high management cost [113]. Tables 8 & 9 list all challenges collected and their frequency out of all formal and grey literature resources.

4.2.2 Zero-day Attacks Solutions and Best Practices

Several methods, approaches, and frameworks have been developed based on techniques mentioned earlier for zero-day attack prediction, prevention, and detection. These mechanisms are applied in different mediums such as networks, the web, mobile devices, etc., which was mainly the focus of formal literature.

Popoola et al. presented a Federated Deep Learning (FDL) method for zero-day botnet attack detection to avoid data privacy leakage in IoT edge devices [114]. In this method, an optimal Deep Neural Network (DNN) architecture is employed for network traffic classification [114]. Besides, Barbhuiya presented DroidLight, a lightweight intrusion detection system that can detect zero-day malware. The algorithm relies on one-class classification and probability distribution analysis [115]. Moustafa et al., presented a Distributed Anomaly Detection (DAD) system to discover zero-day attacks in edge networks [116]. The proposed approach applies Gaussian Mixture-based Correntropy, a novel ensemble one-class statistical learning model developed to effectively monitor and recognize zero-day attacks in real-time from edge networks [116].

Grace et al. presented RiskRanker, a scalable proactive scheme to identify zero-day Android malware (with two-order risk analysis) [117]. A study by Millar et al. presented a novel multi-view deep-learning Android malware detector with no specialist malware domain [49]. The detector was evaluated with a zero-day attack scenario using Drebin and AMD benchmarks [49]. The weighted average detection rates were 91% and 81%, respectively, with up to 57% enhancement over the state-of-the-art and 77% reduction in false positives [49].

Nathezhtha et al. proposed a three-phase attack detection system named Web Crawler-based Phishing Attack Detector (WC-PAD) [118]. It takes the web traffic, web content, and Uniform Resource Locator (URL) as input features; based on these features, the classification of phishing and non-phishing websites is done [118]. In addition, Sejr et al. proposed an interpretable and straightforward unsupervised pipeline that can detect and explain zero-day web attacks with high precision [119]. Abdelnabi et al. build a new

similarity-based phishing detection framework named VisualPhishNet based on a triplet Convolutional Neural Network (CNN) [120]. Li et al. discussed ObjLupAnsys which explored 61 Node.js packages and detected 61 exploitable zero-day vulnerabilities [121]. Besides, Tang et al proposed ZeroWall, an unsupervised approach, which works with an existing WAF in pipeline to detect zero-day Web attacks effectively [122].

Kim et al. presented an early detection system, ZASMIN (Zero-day Attack Signature Management Infrastructure), for novel network attack protection [123]. This system provides early detection function and validation of attacks when the attacks start to spread on the network [123]. Karanth et al. showed ZDVUE, a tool for automatic prioritization of suspicious JavaScript traces, leading to early detection of potential zero-day vulnerabilities [124]. The algorithm uses a combination of correlation analysis and mixture modeling. Failed attempts may leave attack traces in the form of malicious JavaScript code samples on victim machines [124]. In this paper, they show how such traces resulting from millions of client computers worldwide can reflect valuable information about potentially dangerous zero-day vulnerabilities, allowing patching of the vulnerability before it is exploited [124]. Medeiros et al. used an approach implemented with the DEKANT tool. They evaluated practically with a set of open-source PHP applications and WordPress plugins, finding 16 zero-day vulnerabilities [125].

On the other hand, best practices were the main focus of most grey literature resources. Several suggestions were made to prevent, protect, and defend against zero-day attacks. Patch management was suggested by [126] mentioning that the sooner to apply the patch, the reduced the risk of the attack. Another source suggests having Runtime application self-protection (RASP) agents because of their ability to recognize unusual behaviors [127]

[128]. From the team perspective, multiple sources encourage the education of the employees and train them on how to act in certain incidents [129] [130]. Implementing an IDS or IPS solution, Web Application Firewall (WAF), Next-Generation Antivirus (NGAV), and having an Incident Response Plan (IRP) were some of the listed solutions [131] [132] [133]. Moreover, having a zero trust architecture [134], endpoint detection and response (EDR) solutions, and threat intelligence are some of the effective solutions recommended [135]. Finally, it is a must to mention the Zero Day Initiative, as listed by several sources, to help organizations and security teams understand the attackers and their approaches better [126] [136] [137].

Table 8: List of zero-day attacks challenges identified by formal literature and their frequency (out of 243 resources).

ID	Challenge	Frequency (243)
1	limitations of anomaly, signature-based methods, honeypots, blacklists, ML in defending zero-days	68
2	Being Unknown in nature (information is not available)	55
3	Cannot be tackled using conventional security tools/systems/methods (inefficiency/lack)	32
4	The zero-day vulnerability is a harmful threat (cause damage)	22
5	Time of detection/discovery (Attack time exceeded analysis time)	19
6	Financial value/impact	17
7	Attackers are ahead of defenders/developers (highly skilled, in time, knowledge)	13
8	Time of Recovery (time for the patch to be released)	13

11	Zero-days change their own representations or behavior (new variants) or grow in number	10
9	Early Disclosure of zero-day attacks (The amount of malicious activity after publication is much higher)	8
10	The zero-day market (included in crime packs sold at underground markets)	6
12	Political gains/impact	6
14	The value of zero-day vulnerabilities to attackers	5
13	Operational value/impact	3
15	Users are unaware of malicious incident/ not applying patches or fixes	2
16	Preserving usability/availability of the protected assets	2
17	Poor visibility into the security exposure and vulnerability to attack.	1

Table 9: List of zero-day attacks challenges identified by grey literature and their frequency (out of 71 resources).

ID	Challenge	Frequency (71)
1	Unknown nature of zero-days (Only party aware are attackers themselves)	29
2	Destructive and far-reaching consequences (severe damage)	23
3	Zero-Days give attackers the Upper Hand (ahead in term of time, knowledge, and skills)	16
4	Zero-days are valuable financially	16
5	Inefficiency of conventional security tools and signature-based detection methods	15
6	Zero-days sold at illegal markets or the dark web	13

7	Time of discovery	13
8	Time of recovery (to release a patch)	9
9	Zero-days are on a rise (increasing number)	9
10	Political Motives of governments and businesses	8
11	Users are unaware of the exploit (do not apply a patch sometimes)	5
12	Zero-day vulnerabilities can take multiple forms	3
13	Lack of visibility	1

CHAPTER 5

FUZZY ANALYTIC HIERARCHY PROCESS (F-AHP)

The analytic hierarchy process (AHP) is a powerful tool for multi-criteria decision-making in which a problem in a hierarchical approach starts from a goal, then criteria and sub-criteria, then alternatives [39]. However, the basic AHP does not consider the personal judgments vagueness therefore the fuzzy logic was embedded into AHP [138]. To deal with the uncertainties and fuzziness of complex real-world problems and guide decision-makers when multiple criteria exist, a method like fuzzy AHP is needed [139].

The challenges previously collected by MLR and interviews were combined, arranged, and categorized. Fuzzy AHP created a logical conclusion about the most important challenge and the highest-ranking category. The full list of challenges organized into categories, which are the main inputs to fuzzy AHP, is presented in Table 10.

Table 10: Input for fuzzy AHP (Identified challenges list and their categories).

Categories	Challenges per category
Anonymity and Definition	Ch1: The Unknown nature of the vulnerability itself, being new. Ch2: Investigating how the attacker gets access in the first place. Ch16: Political Motives of governments and businesses. Ch19: Zero-days are on a rise (increasing number). Ch20: Zero-day vulnerabilities can take multiple forms. Ch24: The value of zero-day vulnerabilities to attackers.

Resources	Ch4: Dependence on third party vendors/service providers. Ch5: Lack of experience (from security experts) to handle zero-day vulnerabilities. Ch6: Lack of monitoring capabilities from SOC team. Ch7: Time it takes to discover the zero-day vulnerabilities. Ch8: Time to recover from the zero-day attack (vendors release a patch). Ch15: Zero-Days give attackers the Upper Hand (ahead in terms of time, knowledge, and skills). Ch17: Users are unaware of the exploit (do not apply a patch sometimes). Ch21: Preserving usability/availability of the protected assets.
Security Solutions	Ch3: Lack/inefficiency of security mechanisms when dealing with zero-day (tool perspective/limitations of security solutions). Ch10: Not being able to (hard to) update the components at the right time. Ch11: Adding more security practices/tools is not always the best option. (More tools = more code, = more vulnerabilities. Ch12: Not being able to apply defense in depth always, as sometimes if applied correctly it might become harder to use the network for normal users. Ch22: Poor visibility into the security exposure and vulnerability to attack. Ch26: limitations of anomaly, signature-based methods, honeypots, blacklists, ML in defending zero-days.
Consequences	Ch13: Destructive and far-reaching consequences (severe damage). Ch14: Potential financial and reputation impact on the organization. Ch18: Zero-days sold at illegal markets or the dark web.

	Ch9: How to manage to keep the business running or not losing the data while working on solving the vulnerability. Ch23: Operational value/impact. Ch25: Early Disclosure of zero-day attacks (The amount of malicious activity after publication is much higher).
--	--

5.1 Fuzzy-AHP Process

To achieve the intended goal and perform fuzzy AHP, the following steps should be applied:

Step 1: Compose the hierarchical structure.

This includes defining the process's goal, criteria, and sub-criteria and creating a hierarchy process with identified levels.

Step 2: Construct the pair-wise comparison matrix using fuzzy numbers.

The elements of the pairwise comparison matrix are a triangular fuzzy number where the least value (l) is the first component, the second component (m) is the mean of numbers, and the upper value (u) represents the third component.

Step3: Calculate S_i the priority weight for each row of the pair-wise comparison matrix.

Following these equations, calculate the weight by row first, then by column, and then invert the lower and upper to find fuzzy weight.

$$S_i = \sum_{j=1}^m F_{g_i}^j \otimes [\sum_{i=1}^n \sum_{j=1}^m F_{g_i}^j]^{-1} \quad (5.1)$$

$$\sum_{j=1}^m F_{g_i}^j = (\sum_{j=1}^m l_j, \sum_{j=1}^m m_j, \sum_{j=1}^m u_j) \quad (5.2)$$

$$\sum_{i=1}^n \sum_{j=1}^m F_{g_i}^j = (\sum_{i=1}^n l_i, \sum_{i=1}^n m_i, \sum_{i=1}^n u_i) \quad (5.3)$$

$$[\sum_{i=1}^n \sum_{j=1}^m F_{g_i}^j]^{-1} = \left(\frac{1}{\sum_{i=1}^n l_i}, \frac{1}{\sum_{i=1}^n m_i}, \frac{1}{\sum_{i=1}^n u_i} \right) \quad (5.4)$$

Step 4: Compute the fuzzy weight.

$$\widetilde{A}_1 \otimes \widetilde{A}_2 = (l_1, m_1, u_1) \otimes (l_2, m_2, u_2) \quad (5.5)$$

Step 5: Calculate the final weight vector (The normalized weight).

$$W_{ij} = \left(\frac{w_{ij}}{\sum_{j=1}^n w_{ij}} \right) \quad (5.6)$$

Step 6: Identify the final ranking.

5.2 Fuzzy AHP implementation

To prioritize the challenges and corresponding categories, an online questionnaire survey was used and sent to security experts to participate. Thirty-two security practitioners with 1 -18 years of experience in the field participated in the survey. Thirty-one participants were from Saudi Arabia, and one was from UAE. They all occupied important positions in security, such as SOC analyst, DFIR consultant, security engineer, penetration tester, etc. The survey was open from mid-May to mid-October 2023. The number of participants might be considered low in general; however, several similar research studies have performed fuzzy AHP with a similar number of participants. Examples would be [140] and [141], in which all performed studies with a survey with below ten people participating. The details of implementing fuzzy AHP in this research are as follows:

Step 1: The constructed hierarchy structure of identified challenges and their categories.

A hierarchical structure was developed based on the identified challenges and their categories. Figure 8 presents the structure, with the goal of prioritizing the zero-day attack challenges.

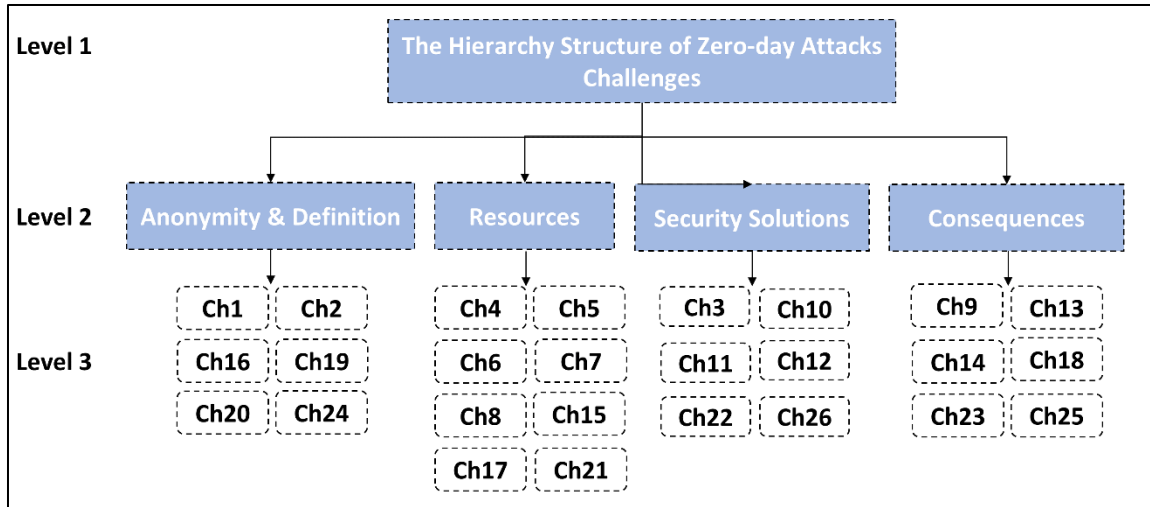


Figure 8: The proposed hierarchy structure.

Step 2: Performing the pair-wise comparison.

Tables 11, 12, 13, and 14 present the pairwise matrices for each of the challenges categories,

Table 11: Pairwise comparison matrix of Solutions challenges category.

Solutions	Ch3	Ch10	Ch11	Ch12	Ch22	Ch26
Ch3	(1,1,1)	(6,7,8)	(7,8,9)	(7,8,9)	(6,7,8)	(5,6,7)
Ch10	(1/8, 1/7, 1/6)	(1,1,1)	(6,7,8)	(6,7,8)	(5,6,7)	(6,7,8)
Ch11	(1/9, 1/8, 1/7)	(1/8, 1/7, 1/6)	(1,1,1)	(2,3,4)	(3,4,5)	(3,4,5)
Ch12	(1/9, 1/8, 1/7)	(1/8, 1/7, 1/6)	(1/4, 1/3, 1/2)	(1,1,1)	(4,5,6)	(6,7,8)
Ch22	(1/8, 1/7, 1/6)	(1/7, 1/6, 1/5)	(1/5, 1/4, 1/3)	(1/6, 1/5, 1/4)	(1,1,1)	(2,3,4)
Ch26	(1/7, 1/6, 1/5)	(1/8, 1/7, 1/6)	(1/5, 1/4, 1/3)	(1/8, 1/7, 1/6)	(1/4, 1/3, 1/2)	(1,1,1)

Table 12: Pairwise comparison matrix of Resources challenges category.

Resources	Ch4	Ch5	Ch6	Ch7	Ch8	Ch15	Ch17	Ch21
Ch4	(1,1,1)	(2,3,4)	(2,3,4)	(1/3, 1/2, 1/1)	(2,3,4)	(2,3,4)	(3,4,5)	(3,4,5)
Ch5	(1/4, 1/3, 1/2)	(1,1,1)	(3,4,5)	(1/3, 1/2, 1/1)	(3,4,5)	(2,3,4)	(4,5,6)	(3,4,5)
Ch6	(1/4, 1/3, 1/2)	(1/5, 1/4, 1/3)	(1,1,1)	(1/4, 1/3, 1/2)	(3,4,5)	(3,4,5)	(4,5,6)	(3,4,5)
Ch7	(1,2,3)	(1,2,3)	(2,3,4)	(1,1,1)	(7,8,9)	(6,7,8)	(7,8,9)	(7,8,9)
Ch8	(1/4, 1/3, 1/2)	(1/5, 1/4, 1/3)	(1/5, 1/4, 1/3)	(1/9, 1/8, 1/7)	(1,1,1)	(3,4,5)	(5,6,7)	(6,7,8)
Ch15	(1/4, 1/3, 1/2)	(1/4, 1/3, 1/2)	(1/5, 1/4, 1/3)	(1/8, 1/7, 1/6)	(1/5, 1/4, 1/3)	(1,1,1)	(5,6,7)	(6,7,8)
Ch17	(1/5, 1/4, 1/3)	(1/6, 1/5, 1/4)	(1/6, 1/5, 1/4)	(1/9, 1/8, 1/7)	(1/7, 1/6, 1/5)	(1/7, 1/6, 1/5)	(1,1,1)	(6,7,8)
Ch21	(1/5, 1/4, 1/3)	(1/5, 1/4, 1/3)	(1/5, 1/4, 1/3)	(1/9, 1/8, 1/7)	(1/8, 1/7, 1/6)	(1/8, 1/7, 1/6)	(1/8, 1/7, 1/6)	(1,1,1)

Table 13: Pairwise comparison matrix of Consequences challenges category.

Consequences	Ch9	Ch13	Ch14	Ch18	Ch23	Ch25
Ch9	(1,1,1)	(4,5,6)	(4,5,6)	(6,7,8)	(6,7,8)	(6,7,8)
Ch13	(1/6, 1/5, 1/4)	(1,1,1)	(4,5,6)	(7,8,9)	(6,7,8)	(6,7,8)
Ch14	(1/6, 1/5, 1/4)	(1/6, 1/5, 1/4)	(1,1,1)	(6,7,8)	(5,6,7)	(5,6,7)
Ch18	(1/8, 1/7, 1/6)	(1/9, 1/8, 1/7)	(1/8, 1/7, 1/6)	(1,1,1)	(4,5,6)	(3,4,5)
Ch23	(1/8, 1/7, 1/6)	(1/8, 1/7, 1/6)	(1/7, 1/6, 1/5)	(1/6, 1/5, 1/4)	(1,1,1)	(5,6,7)
Ch25	(1/8, 1/7, 1/6)	(1/8, 1/7, 1/6)	(1/8, 1/7, 1/6)	(1/5, 1/4, 1/3)	(1/7, 1/6, 1/5)	(1,1,1)

Step 3, 4 & 5: Weights calculations

The fuzzy geometric mean value, the fuzzy weights and the normalized weights were calculated for each category challenges. Within categories, the normalized weights determine the local ranking of the challenges included.

Table 14: Steps 3, 4 & 5 of fuzzy AHP process including the fuzzification and calculating the fuzzy and normalized weights (anonymity).

Anonymity	Fuzzy Geometric mean value	Fuzzy Weights	Normalized weights	Local Rank
Ch1	(5.43, 5.72, 5.98)	(0.46, 0.52, 0.59)	0.52	1

Ch2	(2.45, 2.78, 3.12)	(0.21, 0.25, 0.31)	0.25	2
Ch16	(1.11, 1.23, 1.36)	(0.093, 0.112, 0.134)	0.11	3
Ch19	(0.61, 0.68, 0.75)	(0.051, 0.062, 0.075)	0.062	4
Ch20	(0.32, 0.37, 0.42)	(0.027, 0.034, 0.042)	0.03	5
Ch24	(0.19, 0.21, 0.23)	(0.016, 0.019, 0.023)	0.02	6

Table 15: Steps 3, 4 & 5 of the fuzzy AHP process, including the fuzzification and calculating the fuzzy and normalized weights (resources).

Resources	Fuzzy Geometric mean value	Fuzzy Weights	Normalized weights	Local Rank
Ch4	(1.622, 2.25, 2.99)	(0.112, 0.197, 0.34)	0.20	2
Ch5	(1.44, 1.89, 2.49)	(0.099, 0.17, 0.29)	0.17	3
Ch6	(1.038, 1.314, 1.68)	(0.072, 0.12, 0.19)	0.12	4
Ch7	(2.83, 3.79, 4.63)	(0.196, 0.33, 0.53)	0.33	1
Ch8	(0.75, 0.90, 1.104)	(0.052, 0.079, 0.13)	0.079	5
Ch15	(0.58, 0.67, 0.84)	(0.039, 0.059, 0.097)	0.060	6

Ch17	(0.31, 0.35, 0.42)	(0.021, 0.031, 0.048)	0.03	7
Ch21	(0.191, 0.22, 0.27)	(0.013, 0.019, 0.030)	0.019	8

Table 16: Steps 3, 4 & 5 of the fuzzy AHP process, including the fuzzification and calculating the fuzzy and normalized weights (solutions).

Solutions	Fuzzy Geometric mean value	Fuzzy Weights	Normalized weights	Local Rank
Ch3	(4.55, 5.16, 5.75)	(0.40, 0.51, 0.65)	0.51	1
Ch10	(2.26, 2.58, 2.90)	(0.20, 0.25, 0.33)	0.25	2
Ch11	(0.79, 0.97, 1.156)	(0.069, 0.096, 0.13)	0.096	3
Ch12	(0.66, 0.77, 0.91)	(0.057, 0.076, 0.103)	0.077	4
Ch22	(0.33, 0.39, 0.47)	(0.028, 0.039, 0.054)	0.039	5
Ch26	(0.22, 0.26, 0.31)	(0.019, 0.025, 0.035)	0.026	6

Table 17: Steps 3, 4 & 5 of the fuzzy AHP process, including the fuzzification and calculating the fuzzy and normalized weights (consequences).

Consequences	Fuzzy Geometric mean value	Fuzzy Weights	Normalized weights	Local Rank
Ch9	(3.89, 4.52, 5.14)	(0.34, 0.46, 0.60)	0.45	1

Ch13	(2.35, 2.70, 3.09)	(0.21, 0.27, 0.36)	0.27	2
Ch14	(1.27, 1.47, 1.70)	[0.11, 0.15, 0.20)	0.15	3
Ch18	(0.52, 0.61, 0.70)	(0.05, 0.061, 0.081)	0.061	4
Ch23	(0.35, 0.40, 0.46)	(0.031, 0.04, 0.054)	0.041	5
Ch25	(0.20, 0.23, 0.27)	(0.018, 0.023, 0.031)	0.023	6

Step6: The final Ranking of challenges.

Based on the identified results of the normalized weights, challenge #1 was ranked the highest among the identified 26 challenges, followed by challenge #7. This indicates that the unknown nature of zero-day attacks is considered the most challenging, reflecting experts' opinions. Table 19 shows the final ranking of challenges.

Locally, each category ranks out of 6 (for anonymity, solutions, and consequences) and 8 for resources. In anonymity, challenge #1 ranked first, while challenge #3 scored the highest in solutions. In resources, challenge #7 took the lead, while challenge #9 had the topmost value across consequences challenges.

Table 18: Final ranking of the identified challenges.

Challenges		Global weight	Final Rank
Ch1	The Unknown nature of the vulnerability itself, being new.	0.16	1
Ch7	Time it takes to discover the zero-day vulnerabilities.	0.104	2
Ch2	Investigating how the attacker gets access in the first place.	0.102	3
Ch3	Lack/inefficiency of security mechanisms.	0.101	4
Ch4	Dependence on third party vendors/service providers.	0.064	5
Ch5	Lack of experience (from security experts).	0.059	6
Ch8	Time to recover from the zero-day attack.	0.055	7
Ch6	Lack of monitoring capabilities from SOC team.	0.053	8
Ch9	Managing to keep the business running.	0.044	9
Ch10	Hard to update the components at the right time.	0.040	10
Ch13	Destructive consequences (severe damage).	0.027	11
Ch12	Not being able to apply defense in depth always.	0.026	12
Ch11	Adding more security practices is not always the best option.	0.025	13
Ch15	Attackers have the Upper Hand (time, knowledge, and skills).	0.024	14
Ch14	Potential financial & reputation impact on organization.	0.023	15
Ch17	Users are unaware of the exploit (do not apply a patch).	0.015	16
Ch16	Political Motives of governments and businesses.	0.014	17
Ch18	Zero-days sold at illegal markets or the dark web.	0.011	18
Ch19	Zero-days are on a rise (increasing number).	0.009	19
Ch20	Zero-day vulnerabilities can take multiple forms.	0.0085	20
Ch21	Preserving usability/availability of the protected assets.	0.0084	21
Ch22	Poor visibility into the security exposure & vulnerability	0.0072	22

Ch23	Operational value/impact.	0.0063	23
Ch26	Limitations of anomaly, signature-based methods, honeypots, blacklists, ML in defending zero-days	0.0055	24
Ch25	Early Disclosure of zero-day attacks.	0.0050	25
Ch24	The value of zero-day vulnerabilities to attackers.	0.0045	26

5.3 Taxonomy of zero-day attacks challenges

In language, taxonomy can be understood as a two-part word derived from Greek terminology as “taxis” means “division or arrangement,” and the “nomos” part refers to “law,” which can be read as a whole “laws of arrangement and division” [142]. Other definitions and explanations all refer to the same meaning as the system or science of classification [142]. The collected and analyzed insights were classified based on multiple factors. Challenges were classified based on the keywords or codes synthesized from the interviews and literature and then prioritized based on the fuzzy AHP results. Figure 9 illustrates the taxonomy of zero-day attack challenges.

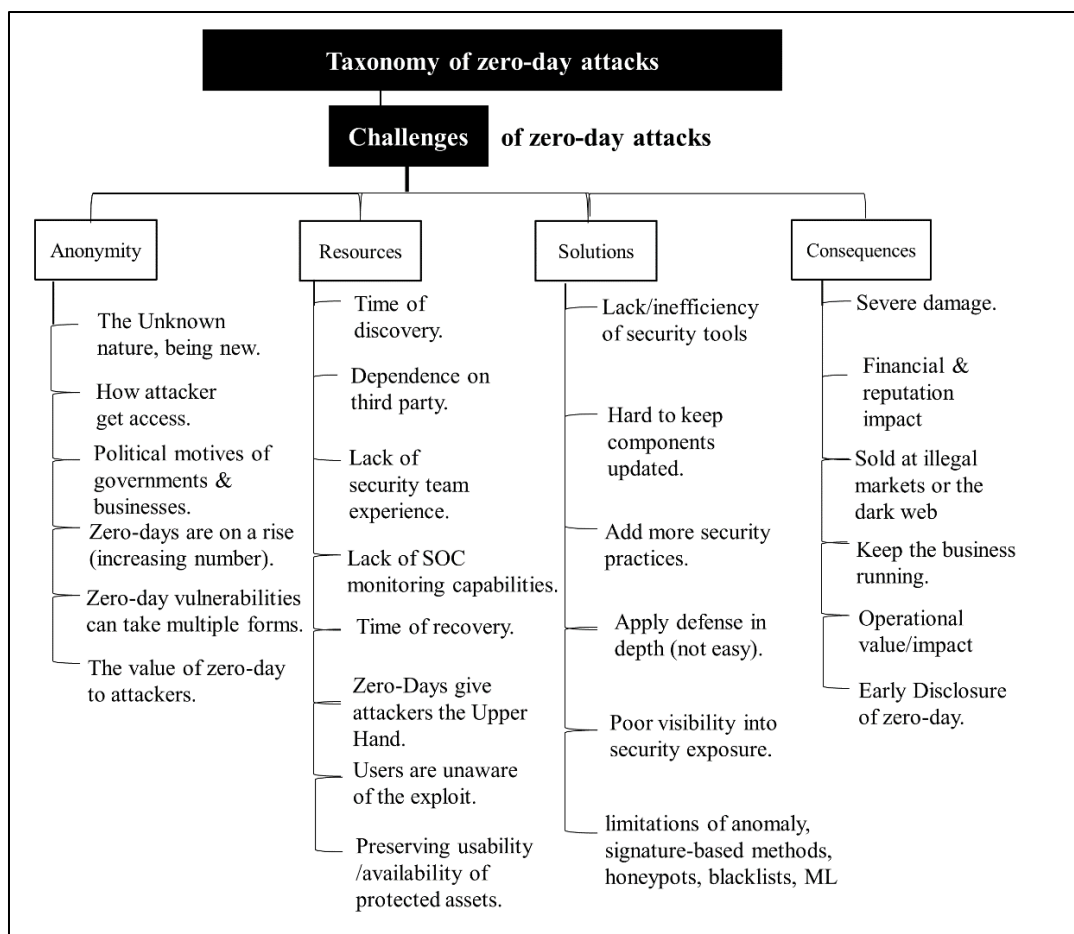


Figure 9: Taxonomy of zero-day attacks challenges.

CHAPTER 6

ZERO-DAY ATTACKS MATURITY MODEL

The maturity model is an effective tool to evaluate organizations or groups' present-day potentials and their future requirements [143]. In the context of this research, the concept of the model and the levels were adopted and inspired from [144] to develop the zero-day attacks maturity model and identify the maturity levels. The best practices to defend against zero-day attacks were distributed in terms of five knowledge areas and five maturity levels, moving from the most general to the most specific, and according to which area of cybersecurity they belong.

6.1 Model Development

After data collection, analysis, and synthesis, a list of 77 best practices was prepared and ready for use. As mentioned earlier, data were collected through multiple stages, including interviews, a questionnaire survey, and a multivocal literature review (MLR). The collected data were analyzed using the content analysis method (CAM), filtered, and paraphrased to form our best practices list. Details of the classification process are presented in Table 20. Those best practices concerning maturity levels and knowledge areas were then ordered and formed. Further explanation of the adopted knowledge areas and maturity levels can be found in upcoming subsections. The second author reviewed the developed maturity model and went through multiple iterations of improvements between the first and second

author, having numerous versions with enhanced levels of detail, to attain the ultimate version of the model presented later.

Table 19: Examples of data classification process (Best practices).

Raw Data	Data Source	Keywords	Category
“...Monitoring is very important. It is always that SOC has good skilled people to defend attacks happened. ...So, you do profiling using the logs in each application, then you start creating rules in which as mentioned previously are based on behaviors. The key pops and what happens in the security field, what new vulnerabilities, exploits exist and try to see if you have them in your organizations...”	Interviews	Monitoring creating rules ... are based on behaviors.	Software and Platform Security
“...Some organizations are ... offer financial incentives in return for new vulnerabilities. An example of a program encouraging hackers to report their bugs is the ... (ZDI), Other examples include Mozilla’s Security Bug Bounty Program, or a similar program by Google for security of its web applications...”	Formal Literature	offer financial incentives in return for new vulnerabilities. encouraging hackers to report their bugs Security Bug Bounty Program	Human, Organizational, and Regulatory Aspects
“...Instead of deploying reactive security solutions which scan, detect, and then prevent, enterprises need to adopt a zero-trust approach. Zero trust security model allows only known and approved processes to run...”	Grey Literature	enterprises need to adopt a zero-trust approach	Attacks and Defenses

6.2 The Five Knowledge Areas

According to the Cyber Security Body of Knowledge (CyBok) [145], the field of cyber security can be classified mainly into five main knowledge areas, including Human, Organizational, and Regulatory Aspects, Attacks and Defenses, Systems Security, Software and Platform Security, and Infrastructure Security, which cumulate to nineteen sub-areas.

- **Human, Organizational, and Regulatory Aspects:**

Security metrics related to (1) risk management, (2) law and regulations, (3) human factors, and (4) privacy and online rights will all be classified under this area. Risk assessment and management refers to the identification, assessment of exposure, and risk estimation with possible outcomes of any activities, then reviewing the information collected as parts of the assessments. Law and regulations cover topics like data protection, legal research and law principles, intellectual property, ethics, public international law, etc. Human factors focus more on understanding human behavior in security, the portion of human error, usable security, and user awareness and education in cybersecurity. Finally, privacy and online rights cover all aspects of privacy, such as control, confidentiality, transparency, and privacy values and technologies.

- **Attacks and Defenses:**

Security metrics discussing malware & attack technologies, adversarial behavior, security operations & incident management, and forensics were based on this area. First, malware & attack technologies study the technical details of exploits and

distributed malicious systems and their associated discovery and analysis approaches. Adversarial behavior explains the motivations, behaviors, & methods attackers use to deceive users and get access. Security operations & incident management covers the configuration, operation, and maintenance of secure systems, including the detection of and response to security incidents and collecting and using threat intelligence. Lastly, forensics represents the collection, analysis, & reporting of digital evidence supporting incidents or criminal events.

- **Systems Security:**

This area discussed security metrics like cryptography, operating systems and visualization security, distributed systems security, authentication, authorization, and accountability. It covers topics like core cryptography primitives, other protection mechanisms of operating systems, and multiple security mechanisms related to large-scale distributed systems, in addition to all the aspects of identity management and authentication technologies that provide accountability in distributed systems.

- **Software and Platform Security:**

This area presents security metrics discussing software security, web and mobile security, and a secure software lifecycle. This includes all categories of programming errors and several ways to avoid these errors and provide security. It also includes the security of web applications and the implementation of secure software practices in all stages of its development lifecycle.

- **Infrastructure Security:**

Security metrics focusing on network security, hardware security, cyber-physical systems security, physical layer, and telecommunications security are all presented in this area. Concepts related to protecting the network and telecommunications protocols in addition to the security of hardware in all stages of the design, implementation, and deployment. Moreover, this area covers topics explained as the security concerns in cyber-physical systems, for example, Internet of things (IoT) systems. Finally, issues and challenges happen in the physical layer, which belongs to the infrastructure security.

6.3 The Five Maturity Levels

The five maturity levels and their definitions were inspired by CMM model and their way of analyzing each level and what it holds [144]. These maturity levels can be explained as follows.

- **Initial:** Represents low maturity level, in which organizations have no or little practices implemented. Even when some practices exist, it is unclear why or how these practices are implemented in the organization and what the resulting impact is.
- **Managed:** Represents the minimum maturity level, where practices are implemented at the unit level. This means that units become stable, secure environments by managers implementing required practices.

- **Defined:** Represents the moderate maturity level, where practices are implemented across units, creating a framework across the organization. Meaning that organizations adapt the practices applied to their business needs.
- **Predictable:** Represents the complete maturity level, where the organization can manage their capability and performance based on applied practices and framework created.
- **Optimizing:** Represents the high maturity level, where the entire organization is focused on continuous improvements. These improvements are applied to the entities, the capability, the performance, and the practices implemented.

Figure 10 illustrates the main structure of the maturity model, including the five knowledge areas and five maturity levels.

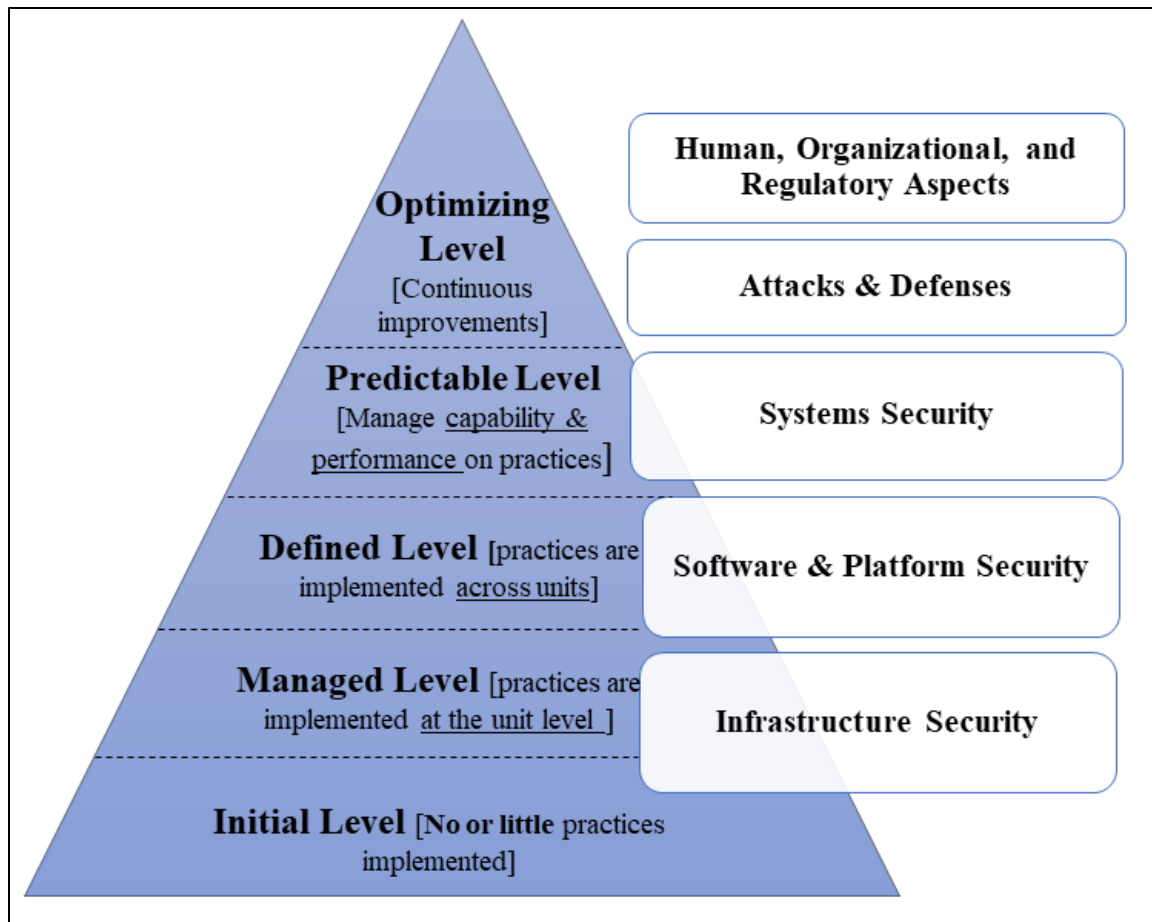


Figure 10: Maturity model main structure elements.

6.4 The Best Practices

A total of 77 best practices related to zero-day were collected, analyzed, and synthesized based on the MLR review study and the interview-based study done earlier. Results from both studies (interviews, grey and formal literature) were combined, eliminating the redundant, and then organized into the model structure.

6.5 The Assessment Method

The assessment of each best practice included in the model was done using the Motorola assessment method. This method was adopted by many models in the field of software engineering and management previously, including CMMI [146] and others [147]. The assessment works based on three aspects in terms of approach, deployment, and results. A value ranging from poor to outstanding will be selected for each aspect. So, each best practice gets a score ranging from 0 to 10 on each of these aspects.

Approach means how committed the organization and its management are to considering the practice. In addition, deployment concerns how well and consistently this practice is deployed. In the end, the results aspect refers to the impact resulting from applying this practice. The Motorola assessment tool is summarized in Appendix D.

6.6 Final Version of Maturity Model (Main Outcome)

A maturity model was developed based on findings from both the MLR study and the interview-based study performed earlier. The list included 77 best practices, representing suggested practices from literature and industry. The resulting maturity model has five

knowledge areas, each with five maturity levels, reflecting and assessing an organization's maturity when managing zero-days.

The full final version of the model is presented in Tables 21, 22, 23, 24, and 25.

Table 20: Zero-day attacks maturity model [Human, organizational, & regulatory aspects KA]

	1 Initial	2 Managed	3 Defined	4 Predictable	5 Optimizing
Human, Organizational, and Regulatory Aspects		All organizations should follow Cyber security Authorities regulations and recommendations (or vendors) in term of cyber security.	Have a qualified team to solve the vulnerabilities encountered and investigate the tickets. (Invest in security teams)	Build use cases/scenarios in the SOC, to identify zero-day vulnerability	Having an adequate Cybersecurity detection, mitigation, prevention, and recovery strategy for every business
		Apply policies and standards for ex; NCA policy, OPT standards, ISO standards etc.	Train employees/decision makers on healthy cyber practices	PURPLE team (red & blue) collaboration to discover vulnerabilities before attackers do.	Having Research and development team (RND) to research vulnerabilities, find zero-days, and try to fix them.
		- Enforce software/Internet use policies.	Have a solid SOC center to detect and have 360° view of	Increase awareness/educate users	Zero Day Initiative

		- Applying human security hygiene concept.	the organization work.		(bounty programs)
		Understand and adhere to any applicable data privacy and compliance regulations (GDPR, PCI DSS, HIPAA, etc.)			Stay informed. ---- Organizations should use threat sharing resources and vulnerability disclosures.

Table 21: Zero-day attacks maturity model [Attacks & Defenses KA]

Attacks and Defenses		Monitoring applications/Solution	Detect zero-day attacks by looking for suspicious behavior	Have an Incident Response Plan Ready	Practice/apply defense in depth.
		Input Validation	Vulnerability Scanning	Patch Management	Zero trust security model.
		Use encryption methods	Covering each stage in attacks lifecycle (Cyber Kill Chain) Use/have initial solutions, or	Invest in security control tools like DLP, Sandboxing Solutions, SPF, DMARC, DKIM, SIEM	use MITRE framework

			temporary solutions to limit the impact of a zero-day.	technologies etc.	
			Do not leave default credentials/ configurations of security tools as it is.	Work out an emergency response solution.	Apply Threat intelligence

Table 22: Zero-day attacks maturity model [Systems Security KA]

Systems Security		Remaining in control of your data	Enforce a least privilege model.	Resources available to an organization have a direct role in its ability to defend against zero-day exploits.	Apply an objective, passive and proactive approach and keep away from subjective, predictive and reactive approaches.
		Applying system security hygiene concept.	Be sure to back up: Backups for the data itself and for the datacenter.	Care of internal systems/servers and its updates as well as external servers/systems facing the Internet.	Applying the SASE architecture.
		Do not share passwords and keys between systems.	Systems baselining and hardening (Detection).		

Table 23: Zero-day attacks maturity model [Software & Platform Security KA]

Software and Platform Security		Use only essential applications.	Use a firewall/Web Application Firewall (WAF) ---- Deploy an IDS or IPS (on software level).	Use a comprehensive/Next Generation antivirus solution. ---- Safe/secure administration of systems.	Application Whitelisting
		Keep all software, web browsers, operating system Up to date. (Keep updated)	Use runtime application self-protection (RASP) agents sits inside applications' runtime	Follow the logs and traffic on the firewalls itself, and watch the tickets itself, using different ports, different protocols.	Deploy AI-based threat detection tools is the best defense against zero-day attacks.
		Assume you are compromised, and that you will get compromised again. ---- Secure code.	Browser isolation ---- Monitoring applications being created automatically	use "heuristics-based" antivirus detection software	Better Patches Could Reduce the Number of Zero-days.

Table 24: Zero-day attacks maturity model [Infrastructure Security KA]

Infrastructure Security		Minimize the number of devices	Deploy an IDS or IPS (On network level).	Adopt a multi-layered approach as	Adopt Endpoint Detection and Response (EDR) solutions
-------------------------	--	--------------------------------	--	-----------------------------------	---

	facing the Internet.		your security posture.	
	Use virtual local area networks (Virtual LAN)	Implement Network Access Control	Reduce your Attack Surface	Single packet authorization can help in providing effective protection in a network with fewer users against zero-day attacks.
	Use secure ports for your network [Secure all gateways (servers, networks, email, etc.)]	Implement IPsec, the IP security protocol.	Perform network scanning continuously through penetration testing and vulnerability findings. (Generate reports)	Monitoring for persistence techniques such as auto start extensible points, run and run once registry keys, services registration, scheduled tasks, DLL hijacking. (Detection)
	Check for unknown connection to the foreign network	Encryption of network traffic, especially the payload, to protect the integrity and confidentiality of the data traversing the network.	Network segmentation, separating the network in form of VLANs. (Prevention)	Monitoring for suspicious communication that alert for data exfiltration is very important. It's the last goal that the attacker would like to achieve is to retrieve the data outside the organization.
	Comprehensive real-time Network Analysis and	QoS, Distribute the requests on multiple zones etc.	Having an inventory list of the entire infrastructure in the organization,	

		Visibility (NAV)		then categorize applications based on criticality to business.	
--	--	---------------------	--	---	--

CHAPTER 7

CASE STUDIES

7.1 Process of Case Studies

Yin et al. introduced the concept of case study as the empirical method used to test a phenomenon within its real-life environment [148]. Case studies provide a deep understanding of how and why certain things happen in that environment. In the context of this research, two case studies were performed to test the zero-day maturity in the real environment used by its intended users. Case studies will provide insights into how helpful this model is for security experts and what sides would require improvements. Moreover, it will give assessment and feedback on field-related security practices and their implementation. The case study was performed by contacting a security team representative of each organization and requesting them to participate in our study, assuring the confidentiality of their data and identity.

7.1.1 Organization ‘A’

Organization A is a large-scale organization located in Saudi Arabia that is concerned with developing safe digital solutions. It has developed or partnered on many platforms, including some logistics and financial solutions.

7.1.2 Organization ‘B’

Organization B is a large-scale semi-governmental organization that provides customer services in the defense, electronics, information technology, telecommunications, energy, and security sectors.

7.1.3 Feedback Criteria

After performing the case studies with the two organizations, the teams’ representatives were asked to participate in a post-case study questionnaire survey to provide feedback on the model and evaluate their experience. The evaluation was performed based on three criteria elements:

- **Ease of use:** This assesses the usability of the model and how clear and easy it is to be used by the users without extra training or knowledge.
- **User Satisfaction:** This assesses how satisfied the user is after using the model and if it satisfies the purpose for which it was developed. Moreover, it can evaluate whether it is applicable to be used and adapted in organizations later or not.
- **The structure of the model:** This assesses the model structure, the arrangement of areas, elements, and practices and whether it requires any adjustments.

7.2 Case Studies Outcomes

The outcomes of each organization assessment are presented in Table 26 and Table 27, respectively. The results of each organization assessment include the score at each maturity level, the overall maturity score of the organization, and the level of maturity the organization is currently at when completing the assessment. Notice that a maturity score of 7 or above reflects a mature organization.

7.2.1 Maturity assessment of organization ‘A’

The overall maturity score of the organization equals 7.065, and since it is slightly above 7 so, following the Motorola assessment tool, it is a mature organization. However, the score is higher than but still close to approximately 7, which reflects the need to improve the security to increase maturity. Since it got a low score at the optimizing level, then maybe implementing the security practices at that level is a good starting point.

Table 25: Maturity Score of organization ‘A’ using the model.

Maturity level	Number of security practices	Maturity Score per level	Status
Initial	0	-	-
Managed	20	7.25	Qualified
Defined	21	7.37	Qualified
Predictable	18	7.09	Qualified
Optimizing	18	6.76	Not Qualified
	Overall Score	7.065	Mature at Predictable level

7.2.1.1 Managed Level

At the managed level, best practices were mostly approached, deployed, and received impact with an outstanding and qualified manner from the organization ‘A.’ However, practice no.33, ‘to remain in control of your data’, which belongs to the systems security area, was in the fair range in terms of deployment and results. In addition, practice no.59 and 63, which are located in the infrastructure security area, all received fairly level. This

includes minimizing the number of devices facing the internet and applying the Comprehensive real-time Network Analysis and Visibility (NAV) solution. One security practice deployed and impacted weakly on organization 'A' is whether the organization keeps all software, web browsers, and operating systems up to date or not.

7.2.1.2 Defined Level

Best practices were mostly evaluated at the defined level as partially qualified, qualified, and outstanding. However, the evaluation fluctuated regarding certain practices. For example, practice no.36, which infers to apply the least privilege model, was assessed as qualified in terms of approach and deployment, but the impact on the organization was weak. Moreover, security practice no.48, referring to 'deploying an IDS or IPS at the software level,' received a weak assessment in terms of deployment and results.

7.2.1.3 Predictable Level

Best practices at this level were assessed differently as more fluctuations appeared within the evaluation. Security practices no. 28, 40, 69, and 70 were all evaluated fair in terms of deployment and results. This included having an emergency response solution, caring about internal systems/servers as well as external servers/systems, adopting a multi-layer approach, and reducing the attacks surface. Network segmentation representing practice no.72 was deployed fairly but had weak results. Finally, belonging to the human and organizational aspects area, practice no.10 was poorly deployed and had poor effects. Practice no.10 refers to having a purple team to discover vulnerabilities as a collaboration between red and blue teams.

7.2.1.4 Optimizing Level

A variety of evaluation responses were received at this level. Although there are still a good number of qualified and outstanding responses, there are also many fair implementations of practices. Security practices no.30, 41, and 75 are all fairly assessed in all aspects, and no.32 had fair deployment and results. This refers to applying a zero-trust security model, an objective, passive, and proactive approach, implementing single packet authorization. and respectively threat intelligence. On the other hand, security practices no.42 and 58 were weakly implemented. This includes applying the SASE architecture and applying patches correctly. In the end, one poor assessment was for the application of practice no.13 by having a Research and Development team (RND) search for vulnerabilities in organization 'A.'

7.2.2 Maturity assessment of organization 'B'

The overall maturity score of the organization is 8.42, and since it is above 7, it reflects a mature organization. Organization B is currently at the optimizing level, which shows a great level of security is implemented in the organization. Moreover, this probably highlights the great efforts of the security team and management as well.

Table 26: Maturity Score of organization 'B' using the model.

Maturity level	Number of security practices	Maturity Score per level	Status
Initial	0	-	-
Managed	20	8.59	Qualified
Defined	21	8.38	Qualified

Predictable	18	8.74	Qualified
Optimizing	18	8.44	Qualified
	Overall Score	8.42	Mature at Optimizing level

7.2.2.1 Managed Level

The high maturity score of this level for organization B would expectedly be assessed with qualified and outstanding practices implementations. A deviation from that would be practice no.17, which was assessed as fair in deployment and results, and no.45, which was marginally qualified in all aspects. Security practice no.17 introduces the use of monitoring applications, while no.45 stating to assume you are compromised and that you will get compromised again.

7.2.2.2 Defined Level

At the defined level, organization B continued the secure behavior, successfully implementing most of the practices at this level. However, detecting zero-day attacks by analyzing suspicious behavior was deployed, resulting weakly in the organization. Moreover, whether the organization has initial or temporary solutions to limit the impact of a zero-day practice was approached and deployed fairly according to the assessment but had a weak impact. The organization was marginally qualified regarding training employees or decision makers on healthy cyber practices specifically in deployment and results.

7.2.2.3 Predictable Level

With the highest maturity score of 8.74, this level has security practices applied in organization B, mostly at the outstanding level. The only exception is practice No. 9, being qualified in terms of approach and marginally qualified in deployment and results. Security practice no.9 follows the “human, organizational aspects” knowledge area, assessing whether the organization builds use cases/scenarios in the SOC to identify vulnerabilities or not.

7.2.2.4 Optimizing Level

Practices at the optimizing level in organization B are considered mature enough to be at this level. Practice no.13 was fairly approached and achieved results, defined as having a Research and Development team (RND) to research vulnerabilities. Finally, practice no.74 to adopt Endpoint Detection and Response (EDR) solutions had a fair approach and deployment within the organization, but the impact was poor.

7.2.3 Feedback Summary

The representatives of both organizations completed the feedback forms, covering the three aspects of ease of use, user satisfaction, and the structure of the model evaluation. The representative of organization A mostly agreed with the feedback statements, except for some neutral statements. One of them is related to the knowledge of zero-day and its practices if it is required to use the model. The answer neutral can reflect that it depends on several factors to judge such a statement. Organization B representative perceived all three aspects positively, with the answers fluctuating between agreement and strongly agreement. However, for the “ease of use” section, they were neutral regarding the model representations being easy to use and the need for some training. Both representatives

complemented the model, mentioning it was comprehensive and useful. However, the only negative feedback was related to the model being long for the audience. Tables 28, 29, and 30, present the feedback results in terms of ease of use, user satisfaction, and structure of the model respectively.

Table 27: Ease of use feedback results by organizations A, and B.

No.	Ease of use	Organizations' viewpoint (n = 2)							
		Agreement			Disagreement			Neutral	
		Strongly Agree	Agree	SA/A %	Strongly Disagree	Disagree	SD/D %	Neutral	Neutral %
1	The model representation is easy to learn	1	0	50%	0	0	0	1	50%
2	No inconsistencies are noticed while using the model	1	1	0	0	0	0	0	0
3	A little knowledge of Zero-days and security practices is required to learn how to use the model.	1	0	50%	0	0	0	1	50%
4	It is necessary to learn the practices arranged for each Knowledge area.	1	1	100 %	0	0	0	0	0
5	Security experts of all levels are able to use and understand the model easily.	1	1	100 %	0	0	0	0	0
6	It is necessary to utilize the model to measure organizations maturity when dealing with zero-days.	1	1	100 %	0	0	0	0	0
7	It is necessary to distribute knowledge areas among various maturity levels like managed, defined etc.	2	0	100 %	0	0	0	0	0

8	Using the model is effortless, it can be used with minimal instructions.	2	0	100 %	0	0	0	0	0
9	Some training should be provided to assist the utilization of the model.	0	1	50%	0	0	0	1	50%

Table 28: User satisfaction feedback results by organizations A and B.

No	User Satisfaction	Organizations' perception (n = 2)							
		Agreement			Disagreement			Neutral	
		Strongly Agree	Agree	SA/A %	Strongly Disagree	Disagree	SD/D %	Neutral	Neutral %
1	The model can be executed in most organizations.	0	1	50 %	0	0	0	1	50 %
2	Every practice is easy to learn and clear.	0	1	50 %	0	0	0	1	50 %
3	The model is able to identify the strong and weak areas in organizations corresponding to security practices.	1	1	100 %	0	0	0	0	0
4	Using the model will improve our security maturity (especially for managing zero-day attacks).	1	1	100 %	0	0	0	0	0
5	If the model was accessible in my occupation, I anticipate I would utilize it.	1	1	100 %	0	0	0	0	0
6	I agreed with security issues identified by the model.	1	1	100 %	0	0	0	0	0
7	It is critical to present the model as an actual automated software tool measuring organizations security maturity.	2	0	100 %	0	0	0	0	0

Table 29: Structure of the model feedback results by organizations A, and B.

No .	Structure of the model	Organizations' perception (n = 2)							
		Strongly agree and agree			Strongly disagree and disagree			Neutral	
		Strongly Agree	Agree	SA/A %	Strongly Disagree	Disagree	SD/D %	Neutral	Neutral %
1	Every component of the model is self-explanatory and requires no further clarification to be utilized adequately.	0	2	100 %	0	0	0	0	0
2	Every component of the model is feasible and is suited to the organization's security.	1	0	50 %	0	0	0	1	50 %
3	The model can be used effectively to identify security maturity issues with the goal of increasing an organization's maturity when dealing with zero-days.	1	1	100 %	0	0	0	0	0
4	The distribution of security practices among various knowledge areas is valuable.	1	1	100 %	0	0	0	0	0
5	The five maturity levels of the model are valuable.	1	1	100 %	0	0	0	0	0

Based on the results, it clearly reflects that the feedback is mostly leaning to agreements, with several neutral responses. This indicates a good structure of the model, how easy and simple it is for use, and that it mostly satisfies the user.

CHAPTER 8

WEB TOOL

A web tool was developed to transfer the knowledge and findings of this study (Maturity model) into an easy-to-access, simple form for security experts to use. The online model version and assessment tool will increase the availability of the materials and will expand the usefulness for security practitioners and researchers ¹⁰.

8.1 The Output Web Tool

The output version of the web tool includes an introduction and simple explanation of the model highlighting the areas and levels concept, a pdf version of the model ready to be downloaded, an assessment tool, and a glossary (terminologies) section to clarify security-related terms mentioned in the model. The assessment tool helps reflect the organization's capabilities and maturity level and provides feedback with suggestions for improvements supported with visual elements and diagrams. Figure 11 shows screenshots of the web tool and its interface.

¹⁰ <https://zerodaymm.com/>

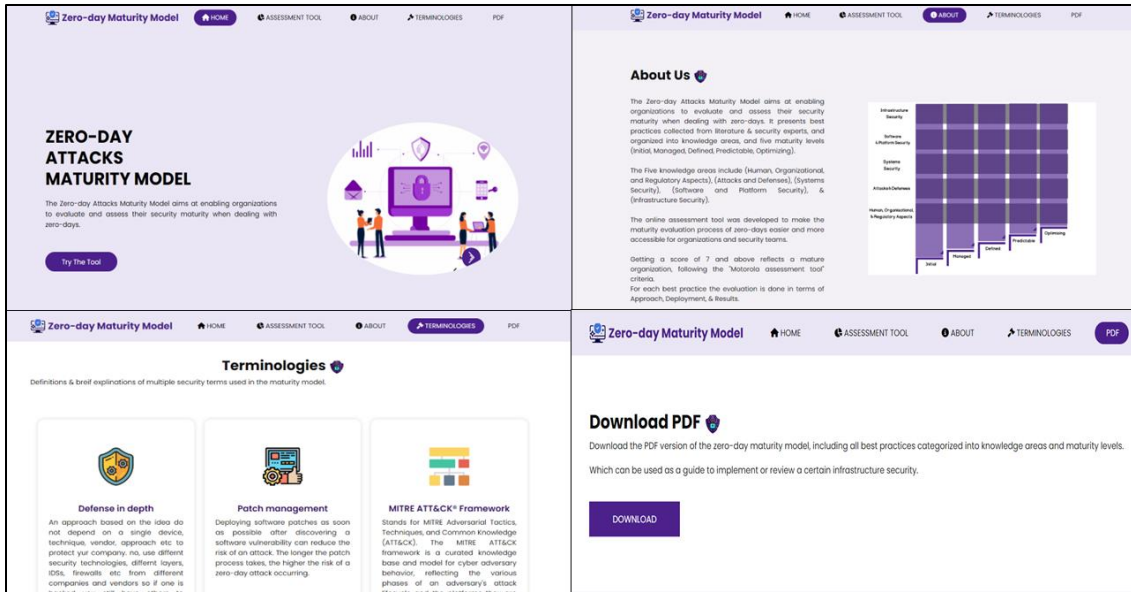


Figure 11: Zero-day maturity model web-based tool user interface. (a) Home page, (b) About us page, (c) Terminologies, and (d) Download PDF.

The details of the web pages are as follows.

Home page: Acts as an entry point and a front page for the tool.

About us: Provides a basic introduction to the zero-day maturity model, the knowledge areas, and maturity levels.

Terminologies: Provides definitions and explanations of several security terms used in the model in case any is unfamiliar.

PDF: Provides an option to download the pdf version of the model, with all best practices listed within their areas and levels in a tabular format.

Assessment tool: Here is the main page where the actual tool is located. The user started by entering organization details to proceed with the assessment. Figure 12 shows the assessment tool page, starting with the organization information interface.

The screenshot shows the 'Organization Information' page of the Zero-day Maturity Model Assessment Tool. The page has a purple header with navigation links: HOME, ASSESSMENT TOOL (active), ABOUT, TERMINOLOGIES, and PDF. The main content area is white and contains four input fields: 'Organization Name' (filled with 'NoZero Co.'), 'Email Address' (filled with 'nozero_co@gmail.com'), 'Scope for this self-evaluation' (filled with 'Identify How mature the organization security structure in dealing with zero-day attacks.'), and 'Additional notes' (filled with 'None.'). A purple 'Continue to Assessment' button is at the bottom center.

Figure 12: Assessment tool page, organization information interface.

The screenshot shows the 'Systems Security' quiz screen. On the left is a sidebar with a list of categories: Human, Organizational, and Regulatory Aspects; Attacks and Defenses; Systems Security (highlighted in purple); Managed Defined; Predictable (highlighted in purple); Optimizing; Software and Platform Security; and Infrastructure Security. The main area is titled 'Systems Security' and shows a 'Predictable Level' badge. Below this is a question: '(8)The organization cares about internal systems/servers and its updates as well as external servers/systems facing t'. The question is followed by three sections: 'Approach', 'Deployment', and 'Results'. Each section has five dropdown menus with options: Poor, Weak, Fair, Marginally qualified, and Qualified. The 'Results' section also has an 'Outstanding' option. A purple bar at the bottom of the main area displays 'Your total score is: 269.33'. At the very bottom, it says '40 of 77' and has 'Previous' and 'Next' buttons. On the right side, there is a text box with a description of the 'Predictable' level: 'General and stable deployed in all parts of the organization OR Suitable use over time across all parts of the organization OR All parts of the organization monitored and verified.'

Figure 13: Assessment tool page, quiz screen example.

When the user clicks 'Continue to Assessment,' a quiz screen appears. Figure 13 reflects an example of what a quiz screen looks like. On the left of the screen, a sidebar includes the knowledge areas and maturity levels as subsections are shown reflecting where the user is by a bold purple. On the top of the screen in the right center, the user can clearly see the

knowledge area and the maturity level, followed by the best practices they are currently examining at the moment. Below the titles, you can find all the details of the best practices page, in addition to the next and previous buttons to move between pages. The best practices are measured in terms of approach, deployment, and results with a scale from (Poor 0 - outstanding 10). Notice that an arrow is attached to the side of each option to explain what each indicates specifically in terms of approach, deployment, and results.

When the user ends up filling out the assessment, the 'next' button will turn to the 'Show the result' option. The result screen shows the organization details and the actual answer to whether the organization under test is a mature organization or not. In addition, the total score would be printed with the option to save the result as a report. Following that, a detailed form of the result would be presented with numbers in a tabular format and in a pie chart format. Figure 14 illustrates how the result per organization will appear. Notice that individual charts per each knowledge area are available as well.

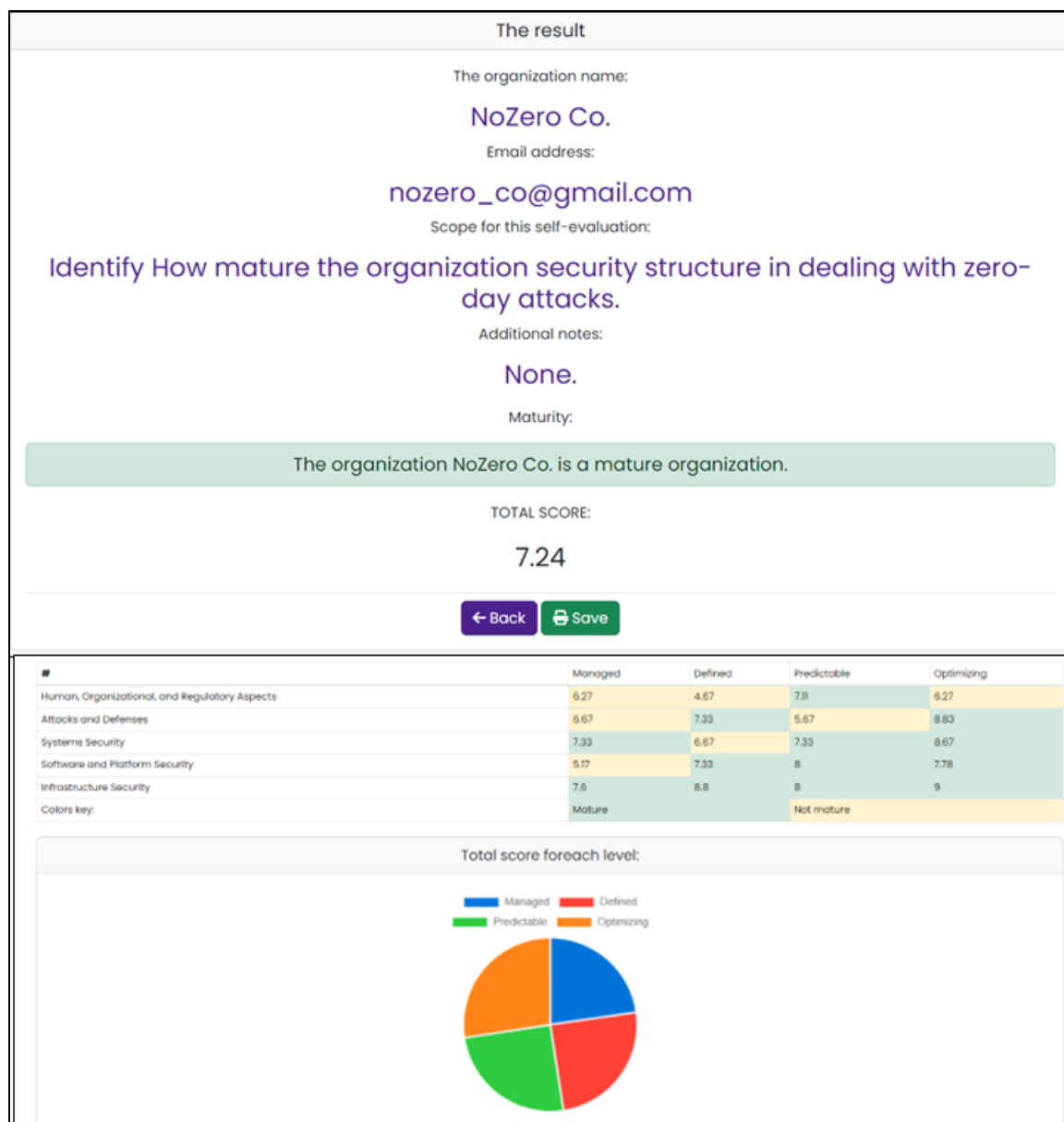


Figure 14: Organization assessment results, (a) Overall results, (b) detailed scores of individual areas and levels.

8.1.1 Modifications of the model:

Based on the feedback from the case study, some enhancements were made to provide a better-quality assessment tool. Most downside comments were concerned with how long the model was. The interactive tool provided for the case study was designed as pages for

each best practice to evaluate in terms of approach, deployment, and results. So, the participants would have 77 pages of best practices to go through. It is understandable that it would be an overwhelming experience; it will make the evaluation process seem harder and more challenging. Therefore, we tried to overcome such a problem in the web tool by providing a more appealing, easier-to-use interface. Therefore, the best practices are categorized visually by areas on the side of the screen, then by levels subsections. Overall, the challenging part was related to the usability of the tool interface, and we believe the web tool helps overcome this obstacle.

8.1.2 Customization of the model:

Extending and customization of the model is flexible and can be done in multiple ways. For example, research is not off, and there will always be new challenges occurring or new practices evolving dealing with zero-day attacks. Hence, the model can always be extended with new data in parallel with future security encounters. On the other hand, data representation and interpretation can be different. Other researchers might use the model data, with the knowledge areas and maturity levels, and interpret it differently as a web extension, a desktop app, or even combined with a certain security tool to achieve extreme real-life protection.

CHAPTER 9

DISCUSSION AND CONCLUSIONS

9.1 Discussion and Important Remarks

Some of the key observations made during the study are as follows:

Remark #1: The unknown nature outbalances the inefficiency of security tools as the lead zero-day challenge:

This is probably the main characteristic of zero-day, but it is also the main challenge. One of the root reasons is that you might have the best security tools but still encounter a zero-day. These tools should be tuned the right way, monitored by experienced practitioners, and kept up to date. In addition, this ambiguous aspect of zero-day, not knowing what to expect, where to search for, and what it looks like, is what raises the difficulty part. Also, this nature is what differentiates zero-day from other vulnerabilities, as most technologies nowadays can deal with the known ones; there is a defined clear method to detect them, unlike zero-day.

On the other hand, we can clearly say that other challenges somehow originate from the “unknown nature”. For example, the “time of detection” & “time of recovery” come as challenges because of the fact that we do not know any information about the attack or where it is located. That’s lead to security experts having a problem trying to detect, then

recover as soon as possible to minimize the attack effects. In addition to time, the consequences of the zero-days have a bigger impact because of their unknown nature as well. When attacking using a zero-day, the attacker is usually one step ahead of the defender since he/she knows more information. That's what makes zero-day more impactful and sometimes destructive. When attackers gain access, if not identified, they have the freedom to move and choose their target. So, according to their motives, whether it is destructive, financial, data leaking, reputation impact, etc., zero-day can give them the power to reach their goal. All of that leads to other challenges that originate and branch out from the main challenge, which is being a new vulnerability in itself.

Remark #2: Zero-day vulnerability is similar to yet different from other vulnerabilities (special & powerful):

This was such an important remark when discussed widely. Technically, zero-day is similar to known vulnerabilities, and it results of multiple weaknesses/flaws or vulnerabilities within the system. However, they are dangerous for a reason. As we mentioned earlier, the unknown nature, the main challenge, also made zero-days special. Normally known vulnerabilities can be detected using signature-based tools; each vulnerability that enters the system gets compared to a list of defined signatures and gets detected automatically by firewalls or antiviruses. However, zero-day vulnerabilities cannot be identified by the regular signature-based tools. That is what makes the detection process challenging and time-consuming. In addition, that initiates having a qualified security team is a must, a team that has analysts, red teamers, and blue teamers searching for any suspicious activity and creating scenarios and use cases to discover vulnerabilities before attackers do. This leads to the idea that zero-day is detected using suspicious behavior, and rules in security

controls should be based on behaviors as well. Moreover, never forget the far-reaching consequences that zero-days have over organizations. That's why they're being requested highly by attackers and sold in the black market. Adding to that, the zero-day initiative and the bug bounty programs proves the power it has. Zero-day vulnerabilities are different than known vulnerabilities, but if searching for similarity, other vulnerabilities should be treated similarly to zero-day. Imagine the level of protection and security organizations would have if all vulnerabilities were treated similarly to zero-day. Organizations need to be prepared and fully secured, taking every threat seriously and managing vulnerabilities actively. This all means that when following zero-days best security practices, from the most general to the most specific practices, you protect entities from zero-day and other less risky vulnerabilities, not the other way around.

Remark #3: Time of discovery vs. Time of recovery:

Time to discover and detect that an organization has a zero-day vulnerability and the time to recover from the attack, create a patch, and update the system were both challenges mentioned when dealing with zero-day attacks. However, discussing which is more critical and challenging can be a dilemma. Going back to “the unknown nature”, since it is ambiguous, then the time to detect and discover that we have a vulnerability or know about it in the first place might be logically longer. Considering that it might stay for weeks in a system with no one knowing or sometimes if no one is looking (searching) for a zero-day regularly it might stay undetected longer. On the other hand, when discussing “time of recovery”, at least the concerned party has some knowledge regarding the vulnerability and it's now depending on the vendor side to release a patch or the security team skills to solve the issue. Based on what is mentioned, “time of discovery” seems more ambiguous and

uncertain, while “time of recovery” seems more controllable under certain circumstances. Referring to the survey results “time of discovery” was highly agreed on as a challenge by 30 participants. However, “time of recovery” participants fluctuates in their choices having 19 agreements and 10 being neutral. Results can be close sometimes as both of them have high approval, but it showed that participants were a little more certain about “time of discovery” for the reasons discussed earlier.

Remark #4: Formal vs. grey literature point of view on challenges:

After conducting a multivocal literature review and passing through hundreds of resources formal and grey, a major question might be about the remarkable differences between the two. An important remark would be the differences of priorities from each side’s point of view. For example, looking at the frequency table stated above, the challenges with the highest frequencies are different between the two sets of data. From the industry perspective, it is focused more on anonymity and consequences. The unknown nature of zero-day, followed by the destructive damage, was the most frequent among grey industry sources. That’s probably due to the practical nature of their daily duty activities; this ambiguity of not knowing when or where the attacks might happen and then the impact it might leave is a concern for practitioners inspired by their work environment. On the other hand, formal literature resources were highly concerned with the limitations of the security methods (like signature-based and honeypots etc.) coming the highest in frequency. That’s probably due to the nature of their work as academic researchers. In academia, people work to develop new methods, systems, or tools to solve a phenomenon and test the impact of such methods on the field of study. So, from an academic perspective this is what concerns them the most, noticing many developed tools and techniques are still limited or have

shortcomings dealing with zero-day attacks. However, based on formal literature frequency, the unknown nature still comes second in terms of challenges. This challenge acts like a baseline for all other challenges and it is agreed on by both academia and industry. In the end, we can clarify from the challenges point of view, academia is more solutions concerned while industry is more consequences concerned.

Remark #5: Fuzzy AHP vs. Frequency prioritization point of view on challenges:

Fuzzy AHP was used to rank challenges found based on their priority. However, based on the data collected, how effective in this case would "the frequency" factor be across multiple resources in prioritizing challenges? In addition, how close or different would the results coming from fuzzy AHP, and frequency be in such a situation?

First of all, the frequency factor in this case is inconsistent. There are three different frequency tables depending on the data source category. The total number of sources in each category is different as well, with 243 formal literature, 71 grey literature, and 16 interview records. Hence, the most frequent in formal literature has 68 out of 243 compared to the most frequent in grey literature appearing in 29 out of 71 sources, highlighting it is not the same challenge topping the list in both scenarios. Fuzzy AHP creates a middle ground where the entire list is being tested as a whole for prioritization, which solves the inconsistency issue.

Second, the frequency perspective is still insufficient to judge for prioritization. Being mentioned in too many sources does not indicate a prioritized factor in common sense. Having only 16 interview participants compared to 243 literature sources might push certain challenges to be mentioned a lot in research, but it is not an indication of how often

it should be prioritized in real-life situations. Considering the fuzzy survey was conducted with 36 experts, it feels more in line with the prioritization concept in actual scenarios.

Furthermore, if we end up comparing both methods and the top challenge recorded, it will be as follows. Taking the majority as formal literature with 243 sources, the most frequent challenge is related to the limitations security methods have in defending against zero-day. While the fuzzy AHP prioritizes the unknown nature of zero-day as the most challenging list item, keeping the security methods limitations as number 24. The two lists have many differences in the order of elements especially at higher ranks, which shows that experts opinions might reflect different qualities than the frequency factor. Although frequency could be a great factor in showing which side of zero-day is under the light in the research field, it is covered and discussed widely in published and grey resources. It is not sufficient to determine the priority of certain challenges over others in the list, as the fuzzy AHP did.

9.2 Implications of the Study

The implications of this study can be divided into practical and theoretical implications. In terms of theoretical implications, an organized list and a taxonomy of challenges related to zero-day vulnerabilities were defined. In addition, a zero-day maturity model encapsulating 77 best practices to manage zero-day vulnerabilities arranged into meaningful areas and levels was introduced. All of that enriches the literature published in the field of security, especially research covering zero-day vulnerabilities. Taking into consideration, the MLR

process makes the outcomes of many multiple sources gathered in one place which acts as a milestone or bookmark to come back to when reading about zero-days.

However, the zero-day maturity model web tool summarizes this study's practical implications. The tool represents an accessible version of the model in which organizations, individuals, and communities may check the maturity levels of their security structures in relation to zero-day attacks.

9.3 Threats to Validity

Several potential threats to the validity of this study were presented. First, this study applied a combined interview-based and survey research approach. An internal threat might be related to interviews and survey participants. The recruited interview and survey samples were mostly, with a high rate from Saudi Arabia. Therefore, the sample might be biased, as recruiting a more diverse sample might reflect more interesting remarks in the results.

A possible external threat to the study is ensuring the credibility of the survey participants. The survey was done online to reach experts willing to volunteer to participate. However, the credibility of the participants is an essential factor in receiving correct information for the study's success. Therefore, participants were sampled through their LinkedIn profiles, ensuring the authenticity of their positions. In addition, all participants were guaranteed to be currently occupying their positions working in the field.

An external validity of the model would be that the list of best practices is long. Having 76 best practices is a plus, but sometimes users might get lost where to start or overwhelmed

by the number of list practices. There were trials to enhance the experience in the web tool, which had different sections and subsections.

Moreover, the way case studies were conducted might raise construct validity. In an ideal scenario, the researcher normally relocates to the real-life environment for the case study to observe how the developed method, tool, or framework behaves in its world. However, since our model assesses organizations' security and reflects a score of their capabilities of dealing with zero-day, it was almost impossible to be exposed to organizations' security systems. Due to the situation's sensitivity (security schemes), a representative of the organizations to which a case study was applied was authorized to perform the case studies and test the model in its real environment.

Finally, the ranking of the challenge could have a potential conclusion validity. As the ranking was concluded by challenge #1, holding the highest importance, this conclusion might be due to other factors. One is the placement of certain challenges in the survey delivered to experts. There is a potential that challenges presented earlier in the beginning of the study will hold higher ratings in the final rank. That doesn't decrease the importance of the rank and the process of prioritization performed, but it could infer that the ranking might be influenced even minorly by other factors.

9.4 Conclusion and Future Work

This research conducted a mixed-methods approach to understand zero-day attacks from literature and industry perspectives and identify the challenges and best practices related to such attacks. This approach included interviewing 16 security experts from different

sectors in the industry and getting feedback from 36 other security experts online, in addition to conducting an MLR study. Identifying challenges and recommended best practices will help security practitioners better understand, plan, and defend against zero-day attacks.

The outcomes of this study are represented by the identified list of challenges and best practices, a taxonomy of zero-day challenges, a zero-day attacks maturity model, and a web assessment tool of zero-day based on the maturity model. Hopefully, Following the suggested practices will guide security experts and increase awareness related to zero days.

For future work, we plan to conduct more empirical studies to better understand zero-day attacks from theory and industry perspectives. We sense the need to investigate these types of attacks more in research and maybe present findings in a more accessible form to security experts working in the industry by adding more features to the web tool after a while of use.

For future research directions, zero-day is an interesting and wide area of research. Even away from challenges and best practices, other areas of zero-days might be potential research directions like disclosure, frequency, factors affecting its rise, etc. Moreover, the security tools in the market that deal with zero days might be an attractive research topic. Studies can dive deep into all these tools, compare them, highlight their strengths and weaknesses, etc. In addition, from a technical point of view, there is always a chance to build a specialized security solution or enhance a certain method/framework.

References

- [1] W. Zheng, P. Deng, K. Gui, and X. Wu, “An Abstract Syntax Tree based static fuzzing mutation for vulnerability evolution analysis,” *Inf. Softw. Technol.*, vol. 158, p. 107194, Jun. 2023, doi: 10.1016/j.infsof.2023.107194.
- [2] Md. Asaduzzaman and Md. M. Rahman, “An Adversarial Approach for Intrusion Detection Using Hybrid Deep Learning Model,” in *2022 International Conference on Information Technology Research and Innovation (ICITRI)*, Jakarta, Indonesia: IEEE, Nov. 2022, pp. 18–23. doi: 10.1109/ICITRI56423.2022.9970221.
- [3] N. Evans and X. Yuan, “Observation of recent Microsoft Zero-Day vulnerabilities,” in *Proceedings of the 49th Annual Southeast Regional Conference on - ACM-SE '11*, Kennesaw, Georgia: ACM Press, 2011, p. 328. doi: 10.1145/2016039.2016131.
- [4] V. T. Do, P. Engelstad, B. Feng, and T. van Do, “Strengthening Mobile Network Security Using Machine Learning,” in *Mobile Web and Intelligent Information Systems*, vol. 9847, M. Younas, I. Awan, N. Kryvinska, C. Strauss, and D. van Thanh, Eds., in *Lecture Notes in Computer Science*, vol. 9847, Cham: Springer International Publishing, 2016, pp. 173–183. doi: 10.1007/978-3-319-44215-0_14.
- [5] S. Shah and B. M. Mehtre, “An overview of vulnerability assessment and penetration testing techniques,” *J. Comput. Virol. Hacking Tech.*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.
- [6] S. Regi, G. Arora, R. Gangadharan, R. Bathla, and N. Pandey, “Case Study on Detection and Prevention Methods in Zero Day Attacks,” in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India: IEEE, Oct. 2022, pp. 1–4. doi: 10.1109/ICRITO56286.2022.9964873.
- [7] S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, “A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions,” *J. Supercomput.*, vol. 75, no. 8, pp. 4543–4574, Aug. 2019, doi: 10.1007/s11227-016-1850-4.
- [8] R. Kaur and M. Singh, “Automatic Evaluation and Signature Generation Technique for Thwarting Zero-Day Attacks,” in *Recent Trends in Computer Networks and Distributed Systems Security*, vol. 420, G. Martínez Pérez, S. M. Thampi, R. Ko, and L. Shu, Eds., in *Communications in Computer and Information Science*, vol. 420, Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 298–309. doi: 10.1007/978-3-642-54525-2_27.
- [9] R. Kaur and M. Singh, “Two-Level Automated Approach for Defending Against Obfuscated Zero-Day Attacks,” in *Risks and Security of Internet and Systems*, vol. 8924, J. Lopez, I. Ray, and B. Crispo, Eds., in *Lecture Notes in Computer Science*, vol. 8924, Cham: Springer International Publishing, 2015, pp. 164–179. doi: 10.1007/978-3-319-17127-2_11.
- [10] C. A. Teodorescu, “Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks,” *Inform. Econ.*, vol. 26, no. 2/2022, pp. 46–56, Jun. 2022, doi: 10.24818/issn14531305/26.2.2022.05.

- [11] Y. Sun, L. Yin, Y. Guo, F. Li, and B. Fang, "Optimally Selecting the Timing of Zero-Day Attack via Spatial Evolutionary Game," in *Algorithms and Architectures for Parallel Processing*, vol. 10393, S. Ibrahim, K.-K. R. Choo, Z. Yan, and W. Pedrycz, Eds., in Lecture Notes in Computer Science, vol. 10393, Cham: Springer International Publishing, 2017, pp. 313–327. doi: 10.1007/978-3-319-65482-9_21.
- [12] A. M. Pitney, S. Penrod, M. Foraker, and S. Bhunia, "A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities," in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, Split / Bol, Croatia: IEEE, Jul. 2022, pp. 1–6. doi: 10.23919/SpliTech55088.2022.9854268.
- [13] C. Wiens, "The Top 5 Zero-Day Attacks of the 21st Century," *MixMode*. Jul. 29, 2021. [Online]. Available: <https://mixmode.ai/blog/the-top-5-zero-day-attacks-of-the-21st-century/#:~:text=The%20Top%205%20Zero-Day%20Attacks%20of%20the%2021st,2019%29%20...%205%20Marriott%20International%20%28September%202018%29%20>
- [14] Y. S. AlMahmeed and A. Y. Al-Omay, "Zero-day Attack Solutions Using Threat Hunting Intelligence: Extensive Survey," in *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, Sakhir, Bahrain: IEEE, Oct. 2022, pp. 309–314. doi: 10.1109/ICDABI56818.2022.10041568.
- [15] M. Anwer, G. Ahmed, A. Akhunzada, S. Hussain, and M. Khan, "Comparative analysis of soft computing approaches of zero-day-attack detection," in *2022 International Conference on Emerging Trends in Smart Technologies (ICETST)*, Karachi, Pakistan: IEEE, Sep. 2022, pp. 1–5. doi: 10.1109/ICETST55735.2022.9922937.
- [16] P. Kumar and R. K. Sheth, "A Review on 0-day Vulnerability Testing in Web Application," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*, Udaipur, India: ACM Press, 2016, pp. 1–4. doi: 10.1145/2905055.2905357.
- [17] T. Stevens, "Cyberweapons: power and the governance of the invisible," *Int. Polit.*, vol. 55, no. 3–4, pp. 482–502, May 2018, doi: 10.1057/s41311-017-0088-y.
- [18] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, Las Vegas, NV, USA: IEEE, Dec. 2016, pp. 1–7. doi: 10.1109/PCCC.2016.7820663.
- [19] A. Dhammi and M. Singh, "Behavior analysis of malware using machine learning," in *2015 Eighth International Conference on Contemporary Computing (IC3)*, Noida, India: IEEE, Aug. 2015, pp. 481–486. doi: 10.1109/IC3.2015.7346730.
- [20] J.-Y. Kim, S.-J. Bu, and S.-B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders," *Inf. Sci.*, vol. 460–461, pp. 83–102, Sep. 2018, doi: 10.1016/j.ins.2018.04.092.
- [21] A. Fagioli, "Zero-day recovery: the key to mitigating the ransomware threat," *Comput. Fraud Secur.*, vol. 2019, no. 1, pp. 6–9, Jan. 2019, doi: 10.1016/S1361-3723(19)30006-5.
- [22] U. K. Singh, C. Joshi, and D. Kanellopoulos, "A framework for zero-day vulnerabilities detection and prioritization," *J. Inf. Secur. Appl.*, vol. 46, pp. 164–172, Jun. 2019, doi: 10.1016/j.jisa.2019.03.011.

- [23] V. Garousi, M. Felderer, and M. V. Mäntylä, “Guidelines for including grey literature and conducting multivocal literature reviews in software engineering,” *Inf. Softw. Technol.*, vol. 106, pp. 101–121, Feb. 2019, doi: 10.1016/j.infsof.2018.09.006.
- [24] V. Garousi, A. Rainer, M. Felderer, and M. V. Mäntylä, “Introduction to the Special Issue on: Grey Literature and Multivocal Literature Reviews (MLRs) in software engineering,” *Inf. Softw. Technol.*, vol. 141, p. 106697, Jan. 2022, doi: 10.1016/j.infsof.2021.106697.
- [25] B. Kitchenham, L. Madeyski, and D. Budgen, “How Should Software Engineering Secondary Studies Include Grey Material?,” *IEEE Trans. Softw. Eng.*, vol. 49, no. 2, pp. 872–882, Feb. 2023, doi: 10.1109/TSE.2022.3165938.
- [26] V. Garousi, M. Felderer, and M. V. Mäntylä, “The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature,” in *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering*, Limerick Ireland: ACM, Jun. 2016, pp. 1–6. doi: 10.1145/2915970.2916008.
- [27] R. Wendler, “The maturity of maturity model research: A systematic mapping study,” *Inf. Softw. Technol.*, vol. 54, no. 12, pp. 1317–1339, Dec. 2012, doi: 10.1016/j.infsof.2012.07.007.
- [28] M. Ormazabal, J. M. Sarriegi, and E. Viles, “Environmental management maturity model for industrial companies,” *Manag. Environ. Qual. Int. J.*, vol. 28, no. 5, pp. 632–650, Aug. 2017, doi: 10.1108/MEQ-01-2016-0004.
- [29] J. Gomes and M. Romão, “Maturity Models in Healthcare IS/IT Investments: Challenges and Trends,” in *Advances in Logistics, Operations, and Management Science*, M. Khosrow-Pour D.B.A., Ed., IGI Global, 2021, pp. 1997–2013. doi: 10.4018/978-1-7998-3473-1.ch137.
- [30] I. Hausladen and M. Schosser, “Towards a maturity model for big data analytics in airline network planning,” *J. Air Transp. Manag.*, vol. 82, p. 101721, Jan. 2020, doi: 10.1016/j.jairtraman.2019.101721.
- [31] S. Nugawela and D. Sedera, “Capability Maturity Model for Agricultural Supply Chain Management Software:,” in *Advances in E-Business Research*, S. Lokuge and D. Sedera, Eds., IGI Global, 2021, pp. 196–216. doi: 10.4018/978-1-7998-4942-1.ch011.
- [32] H. Saiedian and N. Carr, “Characterizing a software process maturity model for small organizations,” *ACM SIGICE Bull.*, vol. 23, no. 1, pp. 2–11, Jul. 1997, doi: 10.1145/1031167.1031168.
- [33] K. Crowston and J. Qin, “A capability maturity model for scientific data management: A Capability Maturity Model for Scientific Data Management,” *Proc. Am. Soc. Inf. Sci. Technol.*, vol. 47, no. 1, pp. 1–2, Nov. 2010, doi: 10.1002/meet.14504701359.
- [34] L. Shen, X. Du, G. Cheng, and X. Wei, “Capability Maturity Model (CMM) method for assessing the performance of low-carbon city practice,” *Environ. Impact Assess. Rev.*, vol. 87, p. 106549, Mar. 2021, doi: 10.1016/j.eiar.2020.106549.
- [35] G. P. Shukla and G. K. Adil, “A four-stage maturity model of green manufacturing orientation with an illustrative case study,” *Sustain. Prod. Consum.*, vol. 26, pp. 971–987, Apr. 2021, doi: 10.1016/j.spc.2021.01.009.

- [36] CMMI Product Team, “CMMI for Software Engineering, Version 1.1, Continuous Representation (CMMI-SW, V1.1, Continuous),” p. 2315414 Bytes, Aug. 2002, doi: 10.1184/R1/6572396.V1.
- [37] T. Demirel, N. Ç. Demirel, and C. Kahraman, “Fuzzy Analytic Hierarchy Process and its Application,” in *Fuzzy Multi-Criteria Decision Making*, vol. 16, C. Kahraman, Ed., in Springer Optimization and Its Applications, vol. 16. , Boston, MA: Springer US, 2008, pp. 53–83. doi: 10.1007/978-0-387-76813-7_3.
- [38] G. Kabir, “COMPARATIVE ANALYSIS OF AHP AND FUZZY AHP MODELS FOR MULTICRITERIA INVENTORY CLASSIFICATION,” *Int. J. Fuzzy Log. Syst.*, p. 17, 2011.
- [39] Y. Liu, C. M. Eckert, and C. Earl, “A review of fuzzy AHP methods for decision-making with subjective judgements,” *Expert Syst. Appl.*, vol. 161, p. 113738, Dec. 2020, doi: 10.1016/j.eswa.2020.113738.
- [40] M. S. Dwi Putra, S. Andryana, Fauziah, and A. Gunaryati, “Fuzzy Analytical Hierarchy Process Method to Determine the Quality of Gemstones,” *Adv. Fuzzy Syst.*, vol. 2018, pp. 1–6, Oct. 2018, doi: 10.1155/2018/9094380.
- [41] C.-N. Lin, “A Fuzzy Analytic Hierarchy Process-Based Analysis of the Dynamic Sustainable Management Index in Leisure Agriculture,” *Sustainability*, vol. 12, no. 13, p. 5395, Jul. 2020, doi: 10.3390/su12135395.
- [42] I. Mahdavi, H. Fazlollaht, A. Heidarzade, N. Mahdavi-Am, and Y. I. Rooshan, “A Heuristic Methodology for Multi-Criteria Evaluation of Web-Based E-Learning Systems Based on User Satisfaction,” *J. Appl. Sci.*, vol. 8, no. 24, pp. 4603–4609, Dec. 2008, doi: 10.3923/jas.2008.4603.4609.
- [43] S.-L. Lin, C.-S. Wang, and H.-L. Yang, “Applying Fuzzy AHP to Understand the Factors of Cloud Storage Adoption,” in *Intelligent Information and Database Systems*, vol. 8398, N. T. Nguyen, B. Attachoo, B. Trawiński, and K. Somboonviwat, Eds., in Lecture Notes in Computer Science, vol. 8398. , Cham: Springer International Publishing, 2014, pp. 282–291. doi: 10.1007/978-3-319-05458-2_30.
- [44] H. Al-Rushdan, M. Shurman, S. H. Alnabelsi, and Q. Althebyan, “Zero-Day Attack Detection and Prevention in Software-Defined Networks,” in *2019 International Arab Conference on Information Technology (ACIT)*, Al Ain, United Arab Emirates: IEEE, Dec. 2019, pp. 278–282. doi: 10.1109/ACIT47987.2019.8991124.
- [45] M. K. Asif and Y. S. Al-Harthi, “Intrusion detection system using Honey Token based Encrypted Pointers to mitigate cyber threats for critical infrastructure networks,” in *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, San Diego, CA, USA: IEEE, Oct. 2014, pp. 1266–1270. doi: 10.1109/SMC.2014.6974088.
- [46] J. Shanmugam and M. Ponnaivaikko, “Behavior-Based Anomaly Detection on the Server Side to Reduce the Effectiveness of Cross Site Scripting Vulnerabilities,” in *Third International Conference on Semantics, Knowledge and Grid (SKG 2007)*, Xi’an, Shan Xi, China: IEEE, Oct. 2007, pp. 350–353. doi: 10.1109/SKG.2007.63.
- [47] S.-J. Bu and S.-B. Cho, “Integrating Deep Learning with First-Order Logic Programmed Constraints for Zero-Day Phishing Attack Detection,” in *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Toronto, ON, Canada: IEEE, Jun. 2021, pp. 2685–2689. doi: 10.1109/ICASSP39728.2021.9414850.

- [48] A. Naderi-Afooshteh, Y. Kwon, A. Nguyen-Tuong, M. Bagheri-Marzijarani, and J. W. Davidson, "Cubismo: decloaking server-side malware via cubist program analysis," in *Proceedings of the 35th Annual Computer Security Applications Conference*, San Juan Puerto Rico USA: ACM, Dec. 2019, pp. 430–443. doi: 10.1145/3359789.3359821.
- [49] S. Millar, N. McLaughlin, J. Martinez del Rincon, and P. Miller, "Multi-view deep learning for zero-day Android malware detection," *J. Inf. Secur. Appl.*, vol. 58, p. 102718, May 2021, doi: 10.1016/j.jisa.2020.102718.
- [50] L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, "Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks," in *Computer Security - ESORICS 2014*, vol. 8713, M. Kutyłowski and J. Vaidya, Eds., in *Lecture Notes in Computer Science*, vol. 8713. , Cham: Springer International Publishing, 2014, pp. 494–511. doi: 10.1007/978-3-319-11212-1_28.
- [51] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, "Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection," *Electronics*, vol. 11, no. 23, p. 3934, Nov. 2022, doi: 10.3390/electronics11233934.
- [52] I. Mbona and J. H. P. Eloff, "Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches," *IEEE Access*, vol. 10, pp. 69822–69838, 2022, doi: 10.1109/ACCESS.2022.3187116.
- [53] J. H. Jeong and S. G. Choi, "Hybrid System to Minimize Damage by Zero-Day Attack based on NIDPS and HoneyPot," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South): IEEE, Oct. 2020, pp. 1650–1652. doi: 10.1109/ICTC49870.2020.9289589.
- [54] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artif. Intell. Rev.*, Feb. 2023, doi: 10.1007/s10462-023-10437-z.
- [55] S. S, S. K. A, V. Vignesh, and S. P, "Assessment of Zero-Day Vulnerability using Machine Learning Approach," *EAI Endorsed Trans. Internet Things*, vol. 10, Jan. 2024, doi: 10.4108/eetiot.4978.
- [56] Rebet Jones and Marwan Omar, "Revolutionizing Cybersecurity: The GPT-2 Enhanced Attack Detection and Defense (GEADD) Method for Zero-Day Threats," *Int. J. Inform. Inf. Syst. Comput. Eng. INJIISCOM*, vol. 5, no. 2, Apr. 2024, Accessed: May 13, 2024. [Online]. Available: <https://ojs.unikom.ac.id/index.php/injiiscom/article/view/12741>
- [57] Z. Ye, Y. Guo, and A. Ju, "Zero-Day Vulnerability Risk Assessment and Attack Path Analysis Using Security Metric," in *Artificial Intelligence and Security*, vol. 11635, X. Sun, Z. Pan, and E. Bertino, Eds., in *Lecture Notes in Computer Science*, vol. 11635. , Cham: Springer International Publishing, 2019, pp. 266–278. doi: 10.1007/978-3-030-24268-8_25.
- [58] M. S. Obaidat and J. Filipe, Eds., *E-Business and Telecommunications: International Joint Conference, ICETE 2013, Reykjavik, Iceland, July 29-31, 2013, Revised Selected Papers*, vol. 456. in *Communications in Computer and Information Science*, vol. 456. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. doi: 10.1007/978-3-662-44788-8.

- [59] A. Chatzipoulidis, D. Michalopoulos, and I. Mavridis, "Information infrastructure risk prediction through platform vulnerability analysis," *J. Syst. Softw.*, vol. 106, pp. 28–41, Aug. 2015, doi: 10.1016/j.jss.2015.04.062.
- [60] M. Keramati, "An attack graph based procedure for risk estimation of zero-day attacks," in *2016 8th International Symposium on Telecommunications (IST)*, Tehran, Iran: IEEE, Sep. 2016, pp. 723–728. doi: 10.1109/ISTEL.2016.7881918.
- [61] Q. Dai, L. Shi, and Y. Ni, "Risk Assessment for Cyber Attacks in Feeder Automation System," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, Portland, OR: IEEE, Aug. 2018, pp. 1–5. doi: 10.1109/PESGM.2018.8586312.
- [62] S. B. Wicker, "The ethics of zero-day exploits---: the NSA meets the trolley car," *Commun. ACM*, vol. 64, no. 1, pp. 97–103, Jan. 2021, doi: 10.1145/3393670.
- [63] Z. Li and Q. Liao, "Harnessing Uncertainty in Vulnerability Market," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou: IEEE, Jul. 2018, pp. 1–9. doi: 10.1109/ICCCN.2018.8487368.
- [64] W. S. Humphrey, *Managing the software process*. in The SEI series in software engineering. Reading, Mass: Addison-Wesley, 1989.
- [65] P. D. Curtis and N. Mehravari, "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA: IEEE, Apr. 2015, pp. 1–6. doi: 10.1109/THS.2015.7225323.
- [66] "Cybersecurity Capability Maturity Model (C2M2)," Energy.gov. Accessed: Nov. 24, 2021. [Online]. Available: <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>
- [67] D. Proença and J. Borbinha, "Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001," in *Business Information Systems*, vol. 320, W. Abramowicz and A. Paschke, Eds., in Lecture Notes in Business Information Processing, vol. 320. , Cham: Springer International Publishing, 2018, pp. 102–114. doi: 10.1007/978-3-319-93931-5_8.
- [68] E. H. Al Hanaei and A. Rashid, "DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations," in *2014 IEEE Security and Privacy Workshops*, San Jose, CA: IEEE, May 2014, pp. 57–60. doi: 10.1109/SPW.2014.17.
- [69] M. Kassou and L. Kjjiri, "SOASMM: A novel service oriented architecture Security Maturity Model," in *2012 International Conference on Multimedia Computing and Systems*, Tangiers, Morocco: IEEE, May 2012, pp. 912–918. doi: 10.1109/ICMCS.2012.6320279.
- [70] O. M. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, "Adopting security maturity model to the organizations' capability model," *Egypt. Inform. J.*, vol. 22, no. 2, pp. 193–199, Jul. 2021, doi: 10.1016/j.eij.2020.08.001.
- [71] M. Hamza, H. Hu, M. A. Akbar, F. Mehmood, Y. Hussain, and A. M. Baddour, "SIOT-RIMM: Towards Secure IOT-Requirement Implementation Maturity Model," in *Proceedings of the Evaluation and Assessment in Software Engineering*, Trondheim Norway: ACM, Apr. 2020, pp. 463–468. doi: 10.1145/3383219.3383286.
- [72] R. Rojas, A. Muedas, and D. Mauricio, "Security maturity model of web applications for cyber attacks," in *Proceedings of the 3rd International Conference on*

- Cryptography, Security and Privacy - ICCSP '19*, Kuala Lumpur, Malaysia: ACM Press, 2019, pp. 130–137. doi: 10.1145/3309074.3309096.
- [73] S. N. G. Gourisetti, S. Mix, M. Mylrea, C. Bonebrake, and M. Touhiduzzaman, “Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2): Next-Generation Cyber Resilience by Design,” in *Proceedings of the Northwest Cybersecurity Symposium*, Richland WA USA: ACM, Apr. 2019, pp. 1–9. doi: 10.1145/3332448.3332461.
 - [74] S. H. B. von Solms, “A maturity model for part of the African Union Convention on Cyber Security,” in *2015 Science and Information Conference (SAI)*, London, United Kingdom: IEEE, Jul. 2015, pp. 1316–1320. doi: 10.1109/SAI.2015.7237313.
 - [75] L. Bratthall and M. Jørgensen, “Can you Trust a Single Data Source Exploratory Software Engineering Case Study?,” *Empir. Softw. Eng.*, vol. 7, no. 1, pp. 9–26, 2002, doi: 10.1023/A:1014866909191.
 - [76] F. Shull, J. Singer, and D. I. K. Sjøberg, Eds., *Guide to advanced empirical software engineering*. London: Springer, 2008.
 - [77] H. Myrbakken and R. Colomo-Palacios, “DevSecOps: A Multivocal Literature Review,” in *Software Process Improvement and Capability Determination*, vol. 770, A. Mas, A. Mesquida, R. V. O’Connor, T. Rout, and A. Dorling, Eds., in *Communications in Computer and Information Science*, vol. 770. , Cham: Springer International Publishing, 2017, pp. 17–29. doi: 10.1007/978-3-319-67383-7_2.
 - [78] B. Kitchenham, “Procedures for Performing Systematic Reviews”.
 - [79] H. Al-Rushdan, M. Shurman, S. H. Alnabelsi, and Q. Althebyan, “Zero-Day Attack Detection and Prevention in Software-Defined Networks,” in *2019 International Arab Conference on Information Technology (ACIT)*, Al Ain, United Arab Emirates: IEEE, Dec. 2019, pp. 278–282. doi: 10.1109/ACIT47987.2019.8991124.
 - [80] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, “Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 1071–1086, May 2016, doi: 10.1109/TIFS.2016.2516916.
 - [81] Z. He, T. Miari, H. M. Makrani, M. Aliasgari, H. Homayoun, and H. Sayadi, “When Machine Learning Meets Hardware Cybersecurity: Delving into Accurate Zero-Day Malware Detection,” in *2021 22nd International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, CA, USA: IEEE, Apr. 2021, pp. 85–90. doi: 10.1109/ISQED51717.2021.9424330.
 - [82] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018, doi: 10.1016/j.cose.2017.09.001.
 - [83] D. Kergl, R. Roedler, and G. D. Rodosek, “Detection of Zero Day Exploits Using Real-Time Social Media Streams,” in *Advances in Nature and Biologically Inspired Computing*, vol. 419, N. Pillay, A. P. Engelbrecht, A. Abraham, M. C. du Plessis, V. Snášel, and A. K. Muda, Eds., in *Advances in Intelligent Systems and Computing*, vol. 419. , Cham: Springer International Publishing, 2016, pp. 405–416. doi: 10.1007/978-3-319-27400-3_36.
 - [84] M. Inzimam, C. Yongle, and Z. Zhang, “An Efficient Approach towards Assessment of Zero-day Attacks,” *Int. J. Comput. Appl.*, vol. 177, no. 26, pp. 34–39, Dec. 2019, doi: 10.5120/ijca2019919742.

- [85] W. Wang, L. Chen, L. Han, Z. Zhou, Z. Xia, and X. Chen, "Vulnerability Assessment for ICS system Based on Zero-day Attack Graph," in *2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS)*, Chongqing, China: IEEE, Dec. 2020, pp. 1–5. doi: 10.1109/ICICAS51530.2020.00009.
- [86] M. Li, W. Huang, Y. Wang, W. Fan, and J. Li, "The study of APT attack stage model," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, Okayama, Japan: IEEE, Jun. 2016, pp. 1–5. doi: 10.1109/ICIS.2016.7550947.
- [87] F. Azzedin, H. Suwad, and Z. Alyafeai, "Countermeasureing Zero Day Attacks: Asset-Based Approach," in *2017 International Conference on High Performance Computing & Simulation (HPCS)*, Genoa, Italy: IEEE, Jul. 2017, pp. 854–857. doi: 10.1109/HPCS.2017.129.
- [88] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, Apr. 2014, doi: 10.1007/s10207-013-0208-7.
- [89] S. Egelman, C. Herley, and P. C. van Oorschot, "Markets for zero-day exploits: ethics and implications," in *Proceedings of the 2013 workshop on New security paradigms workshop - NSPW '13*, Banff, Alberta, Canada: ACM Press, 2013, pp. 41–46. doi: 10.1145/2535813.2535818.
- [90] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, Raleigh, North Carolina, USA: ACM Press, 2012, p. 833. doi: 10.1145/2382196.2382284.
- [91] M. Liu, Z. Xue, X. Xu, C. Zhong, and J. Chen, "Host-Based Intrusion Detection System with System Calls: Review and Future Trends," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–36, Jan. 2019, doi: 10.1145/3214304.
- [92] R. Kaur and M. Singh, "Efficient hybrid technique for detecting zero-day polymorphic worms," in *2014 IEEE International Advance Computing Conference (IACC)*, Gurgaon, India: IEEE, Feb. 2014, pp. 95–100. doi: 10.1109/IAAdCC.2014.6779301.
- [93] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–41, Sep. 2015, doi: 10.1145/2808691.
- [94] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, "Attention based multi-agent intrusion detection systems using reinforcement learning," *J. Inf. Secur. Appl.*, vol. 61, p. 102923, Sep. 2021, doi: 10.1016/j.jisa.2021.102923.
- [95] A. Blaise, M. Bouet, V. Conan, and S. Secci, "Detection of zero-day attacks: An unsupervised port-based approach," *Comput. Netw.*, vol. 180, p. 107391, Oct. 2020, doi: 10.1016/j.comnet.2020.107391.
- [96] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artif. Intell. Rev.*, Jul. 2021, doi: 10.1007/s10462-021-10037-9.
- [97] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public

- datasets and challenges,” *Cybersecurity*, vol. 4, no. 1, p. 18, Dec. 2021, doi: 10.1186/s42400-021-00077-7.
- [98] X. Wang, Y. Yang, and Y. Zeng, “Accurate mobile malware detection and classification in the cloud,” *SpringerPlus*, vol. 4, no. 1, p. 583, Dec. 2015, doi: 10.1186/s40064-015-1356-1.
- [99] A. AlEroud and G. Karabatis, “A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks,” in *2012 International Conference on Cyber Security*, Alexandria, VA, USA: IEEE, Dec. 2012, pp. 40–45. doi: 10.1109/CyberSecurity.2012.12.
- [100] H. Hindy *et al.*, “A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems,” *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.
- [101] A. Aleroud and G. Karabatis, “Detecting Zero-Day Attacks Using Contextual Relations,” in *Knowledge Management in Organizations*, vol. 185, L. Uden, D. Fuenzaliza Oshee, I.-H. Ting, and D. Liberona, Eds., in *Lecture Notes in Business Information Processing*, vol. 185, Cham: Springer International Publishing, 2014, pp. 373–385. doi: 10.1007/978-3-319-08618-7_36.
- [102] A. Alazab, M. Hobbs, J. Abawajy, and A. Khraisat, “Developing an Intelligent Intrusion Detection and Prevention System against Web Application Malware,” in *Advances in Security of Information and Communication Networks*, vol. 381, A. I. Awad, A. E. Hassanien, and K. Baba, Eds., in *Communications in Computer and Information Science*, vol. 381, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 177–184. doi: 10.1007/978-3-642-40597-6_15.
- [103] X. Wang, Y. Yang, Y. Zeng, and C. Tang, “A Novel Hybrid Mobile Malware Detection System Integrating Anomaly Detection With Misuse Detection,” p. 8.
- [104] N. Innab, E. Alomairy, and L. Alsheddi, “Hybrid System Between Anomaly Based Detection System and Honeypot to Detect Zero Day Attack,” in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh: IEEE, Apr. 2018, pp. 1–5. doi: 10.1109/NCG.2018.8593030.
- [105] N. A. S. Mirza, H. Abbas, F. A. Khan, and J. Al Muhtadi, “Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms,” in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, Kuala Lumpur, Malaysia: IEEE, Aug. 2014, pp. 129–132. doi: 10.1109/ISBAST.2014.7013108.
- [106] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, “Defending against phishing attacks: taxonomy of methods, current issues and future directions,” *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2018, doi: 10.1007/s11235-017-0334-z.
- [107] S. Smadi, N. Aslam, and L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,” *Decis. Support Syst.*, vol. 107, pp. 88–102, Mar. 2018, doi: 10.1016/j.dss.2018.01.001.
- [108] A. Gupta and S. Kumar, “Hybrid Anti-phishing Approach for Detecting Phishing Webpage Hosted on Hijacked Server and Zero-Day Phishing Webpage,” in *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences*, M. Dave, R. Garg, M. Dua, and J. Hussien, Eds., in *Algorithms for Intelligent Systems*, Singapore: Springer Singapore, 2021, pp. 389–401. doi: 10.1007/978-981-15-7533-4_30.

- [109] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017, doi: 10.1007/s00521-016-2275-y.
- [110] A. Niakanlahiji, M. M. Pritom, B.-T. Chu, and E. Al-Shaer, "Predicting Zero-day Malicious IP Addresses," in *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense*, Dallas Texas USA: ACM, Nov. 2017, pp. 1–6. doi: 10.1145/3140368.3140369.
- [111] J. Zhang, X. Chen, Y. Xiang, W. Zhou, and J. Wu, "Robust Network Traffic Classification," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1257–1270, Aug. 2015, doi: 10.1109/TNET.2014.2320577.
- [112] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," *Complex Intell. Syst.*, May 2021, doi: 10.1007/s40747-021-00396-9.
- [113] N. Usman *et al.*, "Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics," *Future Gener. Comput. Syst.*, vol. 118, pp. 124–141, May 2021, doi: 10.1016/j.future.2021.01.004.
- [114] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices," *IEEE Internet Things J.*, pp. 1–1, 2021, doi: 10.1109/JIOT.2021.3100755.
- [115] S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "DroidLight: Lightweight Anomaly-based Intrusion Detection System for Smartphone Devices," in *Proceedings of the 21st International Conference on Distributed Computing and Networking*, Kolkata India: ACM, Jan. 2020, pp. 1–10. doi: 10.1145/3369740.3369796.
- [116] N. Moustafa, M. Keshk, K.-K. R. Choo, T. Lynar, S. Camtepe, and M. Whitty, "DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks," *Future Gener. Comput. Syst.*, vol. 118, pp. 240–251, May 2021, doi: 10.1016/j.future.2021.01.011.
- [117] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "RiskRanker: scalable and accurate zero-day android malware detection," in *Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys '12*, Low Wood Bay, Lake District, UK: ACM Press, 2012, p. 281. doi: 10.1145/2307636.2307663.
- [118] T. Nathezhtha, D. Sangeetha, and V. Vaidehi, "WC-PAD: Web Crawling based Phishing Attack Detection," in *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India: IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/CCST.2019.8888416.
- [119] J. H. Sejr, A. Zimek, and P. Schneider-Kamp, "Explainable Detection of Zero Day Web Attacks," in *2020 3rd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA: IEEE, Jun. 2020, pp. 71–78. doi: 10.1109/ICDIS50059.2020.00016.
- [120] S. Abdelnabi, K. Krombholz, and M. Fritz, "VisualPhishNet: Zero-Day Phishing Website Detection by Visual Similarity," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event USA: ACM, Oct. 2020, pp. 1681–1698. doi: 10.1145/3372297.3417233.
- [121] S. Li, M. Kang, J. Hou, and Y. Cao, "Detecting Node.js prototype pollution vulnerabilities via object lookup analysis," in *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the*

- Foundations of Software Engineering*, Athens Greece: ACM, Aug. 2021, pp. 268–279. doi: 10.1145/3468264.3468542.
- [122] R. Tang *et al.*, “ZeroWall: Detecting Zero-Day Web Attacks through Encoder-Decoder Recurrent Neural Networks,” in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, Toronto, ON, Canada: IEEE, Jul. 2020, pp. 2479–2488. doi: 10.1109/INFOCOM41043.2020.9155278.
 - [123] I. Kim *et al.*, “A case study of unknown attack detection against Zero-day worm in the honeynet environment,” p. 6, 2009.
 - [124] S. Karanth, S. Laxman, P. Naldurg, R. Venkatesan, J. Lambert, and J. Shin, “ZDVUE: prioritization of javascript attacks to discover new vulnerabilities,” in *Proceedings of the 4th ACM workshop on Security and artificial intelligence - AISec '11*, Chicago, Illinois, USA: ACM Press, 2011, p. 31. doi: 10.1145/2046684.2046690.
 - [125] I. Medeiros, N. Neves, and M. Correia, “DEKANT: a static analysis tool that learns to detect web application vulnerabilities,” in *Proceedings of the 25th International Symposium on Software Testing and Analysis*, Saarbrücken Germany: ACM, Jul. 2016, pp. 1–11. doi: 10.1145/2931037.2931041.
 - [126] “What Is a Zero Day Attack?,” *Fortinet*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/zero-day-attack>
 - [127] HHS Cybersecurity Program, “Zero-Day Attacks,” Nov. 18, 2021. [Online]. Available: <https://www.hhs.gov/sites/default/files/zero-day-attacks-tlpwhite.pdf>
 - [128] J. McKeon, “Zero-Day Attacks Threaten Healthcare Cybersecurity,” *healthit security*, Nov. 22, 2021. [Online]. Available: <https://healthitsecurity.com/news/zero-day-attacks-threaten-healthcare-cybersecurity>
 - [129] Y. Guanghui, “What Is a Zero-Day Attack?” Sep. 30, 2021. [Online]. Available: <https://info.support.huawei.com/info-finder/encyclopedia/en/Zero-Day+Attack.html>
 - [130] “What is a zero-day attack?,” *malwarebytes*. [Online]. Available: <https://www.malwarebytes.com/zero-day>
 - [131] R. Bisht, “How To Prevent Zero-Day Attacks?,” *InfosecTrain*. [Online]. Available: <https://www.infosectrain.com/blog/how-to-prevent-zero-day-attacks/>
 - [132] “ZERO-DAY ATTACK PREVENTION STEPS YOU CAN TAKE TODAY,” *HelixStorm*. [Online]. Available: <https://www.helixstorm.com/blog/how-to-prevent-zero-day-attacks/>
 - [133] J. Truong, “What is a Zero Day Attack and How Can You Protect Against It,” *hackernoon*, Jul. 18, 2021. [Online]. Available: <https://hackernoon.com/what-is-a-zero-day-attack-and-how-can-you-protect-against-it-sr1h37vq>
 - [134] S. Nayak, “Zero-Day Attacks: Understanding and Preventing Exploits,” *ColorTokens*. [Online]. Available: <https://colortokens.com/blog/zero-day-attack-enterprise-security/>
 - [135] “WHAT IS A ZERO-DAY ATTACK, VULNERABILITY AND EXPLOIT?,” *crowdstrike*, Mar. 18, 2021. [Online]. Available: <https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/>
 - [136] “Zero-day (0day) exploit,” *Imperva*. [Online]. Available: <https://www.imperva.com/learn/application-security/zero-day-exploit/>
 - [137] “Zero-day Vulnerabilities and Zero-day Exploits,” *itperfection*. [Online]. Available: <https://www.itperfection.com/network-security/zero-day-vulnerability-and-zero-day-exploits-cyber-crime-network-security-firewall-web-cybersecurity/>

- [138] M. B. Ayhan, "A Fuzzy Ahp Approach For Supplier Selection Problem: A Case Study In A Gearmotor Company," *Int. J. Manag. Value Supply Chains*, vol. 4, no. 3, pp. 11–23, Sep. 2013, doi: 10.5121/ijmvsc.2013.4302.
- [139] A. N. Patil, "FUZZY AHP METHODOLOGY AND ITS SOLE APPLICATIONS," 2018.
- [140] E. W. L. Cheng and H. Li, "Construction Partnering Process and Associated Critical Success Factors: Quantitative Investigation," *J. Manag. Eng.*, vol. 18, no. 4, pp. 194–202, Oct. 2002, doi: 10.1061/(ASCE)0742-597X(2002)18:4(194).
- [141] K. Lam and X. Zhao, "An application of quality function deployment to improve the quality of teaching," *Int. J. Qual. Reliab. Manag.*, vol. 15, no. 4, pp. 389–413, Jun. 1998, doi: 10.1108/02656719810196351.
- [142] H. Enghoff, "What is taxonomy? – An overview with myriapodological examples," *Soil Org.*, vol. 81, pp. 441–451, 2009.
- [143] A. Tiwari and D. P. Madalli, "Maturity models in LIS study and practice," *Libr. Inf. Sci. Res.*, vol. 43, no. 1, p. 101069, Jan. 2021, doi: 10.1016/j.lisr.2020.101069.
- [144] W. Curtis, W. A. Hefley, and S. A. Miller, "People Capability Maturity Model (P-CMM) Version 2.0," p. 5476938 Bytes, 2001, doi: 10.1184/R1/6581879.V1.
- [145] A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, "The Cyber Security Body of Knowledge".
- [146] S. Ali and S. U. Khan, "Software outsourcing partnership model: An evaluation framework for vendor organizations," *J. Syst. Softw.*, vol. 117, pp. 402–425, Jul. 2016, doi: 10.1016/j.jss.2016.03.069.
- [147] S. U. Khan, M. Niazi, and R. Ahmad, "Critical Success Factors for Offshore Software Development Outsourcing Vendors: A Systematic Literature Review," in *2009 Fourth IEEE International Conference on Global Software Engineering*, Limerick, Ireland: IEEE, Jul. 2009, pp. 207–216. doi: 10.1109/ICGSE.2009.28.
- [148] R. K. Yin, *Case study research: design and methods*, 3rd ed. in Applied social research methods series, no. v. 5. Thousand Oaks, Calif: Sage Publications, 2003.
- [149] Y. Mufti, M. Niazi, M. Alshayeb, and S. Mahmood, "A Readiness Model for Security Requirements Engineering," *IEEE Access*, vol. 6, pp. 28611–28631, 2018, doi: 10.1109/ACCESS.2018.2840322.

Vitae

Name	: Eman Junid Bakri
Nationality	: Syrian
Date of Birth	: 1/30/1996
Email	: eman.bakri.ejb@gmail.com
Address	: Building no. 6932, Al Salmaniyah 2nd Dist. Hofuf, Saudi Arabia. P.O Box 36421.
Academic Background	: • Master's degree, Computer science, King Fahd University of Petroleum and Minerals (KFUPM) - 2024. • Bachelor's degree, Computer science, King Faisal University (KFU) – 2018.
Work Experience	: • IT Coop Training, Saudi National Guard Hospital, 2017. • Several Projects, in mobile app development, virtual reality, and research has been done.
Publications	: • The Impact of Feature Selection on Different Machine Learning Models for Breast Cancer Classification, 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA). • A Taxonomy of Zero-day Attacks Challenges: A Fuzzy AHP Study, Empirical Software Engineering Journals, 2024 (submitted). • A Maturity Model for Managing Zero-day Attacks: Best Practices, Software: Practice and Experience Journals, 2024 (submitted).

Appendix A: Interviews Questions

Zero-day attacks

1. Have you experienced/aware of zero-day attacks while working in security? Kindly share your experience
2. How frequent zero-day attacks are encountered? and how do different stakeholders handle them usually (the process)?
3. Do companies usually disclose having a zero-day in an organization or not? What are the criteria for disclosing or not?

Zero-day attacks Challenges

1. Would you share with us the challenges security experts may face while dealing with/ managing Zero-day attacks?
2. What are the existing security practices/missing security controls that open the door for zero-days (were not effective enough that cause zero-day to occur)?
3. Are zero-day attacks challenging because of [the lack/inefficiency of security mechanisms in the company] or [the unknown nature of the attack itself (being new)]?

Zero-day attacks Solutions

1. Are there security processes/strategies that would make handling zero-days easier and more effective? What?
2. What are the best solutions/ best practices for successfully defending against zero-day attacks?
3. What technologies are these solutions used/based on (ML techniques, honey pots etc.), and for which purpose (detection, prevention, prediction etc.)?
4. What factors play a role in the decision of selecting techniques to implement based upon your experience?
5. Any additional recommendations to better manage zero-day attacks based upon your experience?

Tools & Maturity

1. Do you think zero-day vulnerabilities should be treated similarly or differently to other vulnerabilities in terms of detection/protection? Why?
2. Do you think having a tool/ criterion to evaluate how mature organizations' security practices when specifically dealing with zero-day attacks, will be helpful?

If yes, what aspects do you think should be covered/taken into consideration?

Additional Questions

1. What consequences has your company encountered when affected by a zero-day attack in the past? (Financial loss, loss of data, system shutdown etc.)

General Questions

1. Any questions or comments?

Appendix B: Survey Questions

Zero-day attacks: Challenges & Best Practices [Survey]

Section 1: Challenges

Focusing on challenges and consequences of zero-day attacks.

.....

- 1- Do you agree " The Unknown nature of the vulnerability itself, being new." is one of the challenges related to zero-day attacks?
- 2- Do you agree " Investigating how the attacker get the access in the first place." is one of the challenges related to zero-day attacks?
- 3- Do you agree "Lack/inefficiency of security mechanisms when dealing with zero-day (tool perspective/limitations of security solutions)." is one of the challenges related to zero-day attacks?
- 4- Do you agree " Dependence on third party vendors/service providers." is one of the challenges related to zero-day attacks?
- 5- Do you agree "Lack of experience (from security experts) to handle zero-day vulnerabilities." is one of the challenges related to zero-day attacks?
- 6- Do you agree "Lack of monitoring capabilities from SOC team." is one of the challenges related to zero-day attacks?
- 7- Do you agree "Time it takes to discover the zero-day vulnerabilities (Time of discovery)." is one of the challenges related to zero-day attacks?
- 8- Do you agree "Time to recover from the zero-day attack (vendors release a patch)." is one of the challenges related to zero-day attacks?
- 9- Do you agree "How to manage keeping the business running or not losing the data while working on solving the vulnerability." is one of the challenges related to zero-day attacks?
- 10- Do you agree "Not being able to (it is hard to) update the components in the right time." is one of the challenges related to zero-day attacks?
- 11- Do you agree that "Adding more security practices/tools is not always the best option. (More tools = more code, = more vulnerabilities)." is one of the challenges related to zero-day attacks?
- 12- Do you agree that "Not being able to apply defense in depth always, as sometimes if applied correctly it might become harder for normal users to use the network." is one of the challenges related to zero-day attacks?
- 13- Do you agree that "Destructive and far-reaching consequences of the attack (severe damage)." is one of the challenges related to zero-day attacks?
- 14- Do you agree that "Potential financial and reputation impact of the attack on the organization." is one of the challenges related to zero-day attacks?

Section 2: Best Practices

Focusing on solutions and best practices to deal with zero-day attacks.

.....

1- Do you agree that "All organizations should follow Cyber security Authorities regulations and recommendations (or vendors) in term of cyber security." is one of the best practices to deal with zero-day attacks?

2- Do you agree that "You cannot prevent zero-day attacks but try your best to detect them." is one of the best practices to deal with zero-day attacks?

3- Do you agree that "Monitor your system & know your assets." is one of the best practices to deal with zero-day attacks?

4- Do you agree that "Be prepared for future attacks because it will happen." is one of the best practices to deal with zero-day attacks?

5- Do you agree that "Make sure to back up, frequent backups make sure that you can survive/resist worst-case scenarios quickly (For the data itself and for the datacenter)." is one of the best practices to deal with zero-day attacks?

6- Do you agree that "Applying secure-in-depth strategy, it will maximize time for attacker before reaching data center" is one of the best practices to deal with zero-day attacks?

7- Do you agree that "Applying Zero trust architecture, to minimize the effect of zero-days and narrows its range in a smaller zone" is one of the best practices to deal with zero-day attacks?

8- Do you agree that "Proper network segmentation and isolation." is one of the best practices to deal with zero-day attacks?

9- Do you agree that "multi-layer network architecture design" is one of the best practices to deal with zero-day attacks?

10- Do you agree that "Focusing on user awareness (educate your users)" is one of the best practices to deal with zero-day attacks?

11- Do you agree that "Training employees in threat mitigation (increase awareness)." is one of the best practices to deal with zero-day attacks?

12- Do you agree that "Investing in security control tools like DLP, sandboxing etc." is one of the best practices to deal with zero-day attacks?

13- Do you agree that "Using encryption methods." is one of the best practices to deal with zero-day attacks?

14- Do you agree that "Using secure ports for your network " is one of the best practices to deal with zero-day attacks?

15- Do you agree that "Minimizing the number of devices facing the Internet " is one of the best practices to deal with zero-day attacks?

- 16- Do you agree that "Having a solid SOC center to detect and have 360° view of the organization work." is one of the best practices to deal with zero-day attacks?
- 17- Do you agree that "Applying policies and standards for ex; NCA policy, OPT standards, ISO standards etc." is one of the best practices to deal with zero-day attacks?
- 18- Do you agree that "Applying EDR and NDR solutions" is one of the best practices to deal with zero-day attacks?
- 19- Do you agree that "having a PURPLE team collaboration to discover vulnerabilities before attackers do (red and blue team exercising together)" is one of the best practices to deal with zero-day attacks?
- 20 - Do you agree that "Having a Research and development team (RND) to research vulnerabilities, find zero-days, and try to fix them" is one of the best practices to deal with zero-day attacks?
- 21 - Do you agree that "Applying the least privileges principles (restricted privileges)." is one of the best practices to deal with zero-day attacks?
- 22 - Do you agree that "using MITRE framework to have a robust countermeasures coverage for APT groups." is one of the best practices to deal with zero-day attacks?
- 23 - Do you agree that "Systems baselining and hardening (Detection)." is one of the best practices to deal with zero-day attacks?
- 24 - Do you agree that "Covering each stage in attacks lifecycle (Cyber Kill Chain) is crucial in detection of zero-day attacks." is one of the best practices to deal with zero-day attacks?
- 25 - Do you agree that "Applying the sassy architecture." is one of the best practices to deal with zero-day attacks?
- 26 - Do you agree that " Applying security hygiene concept." is one of the best practices to deal with zero-day attacks?
- 27 - Do you agree that " Using monitoring and deception technologies/techniques." is one of the best practices to deal with zero-day attacks?
- 28 - Do you agree that " Safe/secure administration of systems." is one of the best practices to deal with zero-day attacks?
- 29 - Do you agree that " Keep updated (apply updates)." is one of the best practices to deal with zero-day attacks?
- 30 - Do you agree that " Care of internal systems/servers and its updates as well as external servers/systems facing the Internet because the attack can happen through email etc." is one of the best practices to deal with zero-day attacks?
- 31 - Do you agree that " Do not focus on zero-days as the real obsession, focus more on having a secure infrastructure." is one of the best practices to deal with zero-day attacks?
- 32 - Do you agree that " Do not share passwords and keys between systems." is one of the best practices to deal with zero-day attacks?

33 - Do you agree that " Do not leave default credentials/ configurations of security tools as it is (default coming from vendor) instead follow the right way of deployment changing the default credentials / configurations." is one of the best practices to deal with zero-day attacks?

34 - Do you agree that " Applying Threat intelligence" is one of the best practices to deal with zero-day attacks?

35 - Do you agree that " Performing network scanning continuously through penetration testing and vulnerability findings (generate reports)." is one of the best practices to deal with zero-day attacks?

36 - Do you agree that " Use Patch management (how to fix issues in these reports)." is one of the best practices to deal with zero-day attacks?

37 - Do you agree that " Having a qualified team (as much as possible) to solve the vulnerabilities encountered and investigate the tickets (invest in security teams)." is one of the best practices to deal with zero-day attacks?

38 - Do you agree that " Building use cases in the SOC, to identify zero-day vulnerability (to identify impacted devices or identify vulnerable devices)." is one of the best practices to deal with zero-day attacks?

39 - Do you agree that " Following the logs and traffic on the firewalls itself, and watch the tickets itself, using multiple different ports, different protocols." is one of the best practices to deal with zero-day attacks?

40 - Do you agree that " Using/having initial solutions, or temporary solutions to limit the impact of zero-day (based on previous experiences or people analysis on zero-day or NCA/vendors recommendations)." is one of the best practices to deal with zero-day attacks?

41 - Do you agree that " Having an inventory list of the entire infrastructure in the organization, Then, categorize these applications on which is more critical to the business." is one of the best practices to deal with zero-day attacks?

42 - Do you agree that " Creating rules inside security controls based on behaviors, to detect zero-days (Detect zero-day attacks by looking for suspicious behavior)." is one of the best practices to deal with zero-day attacks?

43 - Do you agree that " Having Zero Day Initiative (bounty programs)." is one of the best practices to deal with zero-day attacks?

44 - Do you agree that " Monitoring for persistence techniques such as auto start extensible points, run and run once registry keys, services registration, scheduled tasks, DLL hijacking which is very important for detection." is one of the best practices to deal with zero-day attacks?

45 - Do you agree that " Monitoring for suspicious communication that alert for data exfiltration." is one of the best practices to deal with zero-day attacks?

46 - Do you agree that "Quality of service (QoS) policy, to distribute the requests on multiple zones etc." is one of the best practices to deal with zero-day attacks?

Appendix C: MLR Resources List Details (Formal & grey)

All details of MLR Resources, collected data, frequency can be found in the following link:

https://docs.google.com/spreadsheets/d/1iOZ3_RCZ2QyrnddHtL7UKYn1izKRJOFmTYoeuFrbmTQ/edit?usp=sharing

<https://shorturl.at/gtY26>

Appendix D: Motorola Assessment Tool (Adopted from [149])

Score	Approach (A)	Deployment (D)	Results (R)
Poor (0)	- Management does not discover any need (OR) - Ability of organization is zero (OR) - Commitment of organizational is zero	- Practices are not utilized in the organization (OR) - Organization interest is zero	Ineffective
Weak (2)	- The need is discovered by management (OR) - Support for practices starts (OR) - A few parts of the organization have the ability to undertake the practices	- Usage is fragmented (OR) - Usage is not appropriate (OR) - Implemented in several parts of the organization (OR) - Restricted to monitoring/verification of use	- Unstable result (OR) - Inappropriate result (OR) - Several parts of the organization gain a number of effectiveness outcomes.
Fair (4)	- Wide but not full commitment by management (OR) - Planning for practice establishment described (OR) - A number of supporting items for the practice exists	- Usage is fragmented (OR) - Some consistency in the usage (OR) - Implemented in a number of major parts of the organization (OR) - Usage in some parts of the organization is monitored/verified.	- Reliable and positive outcomes for a number of parts of the organization (OR) - Inappropriate outcomes for a number of parts of the organization
Marginally qualified (6)	- Some commitment from management is evident (OR) - Some of the management group becomes proactive (OR) - Practice deployment well underway across parts of the organization (OR) - Supporting items exist (OR)	- Some parts of the organization implement it (OR) - Suitable use across many parts of the organization (OR) - The usage of many parts of the organization is monitored or verified (OR)	- Positive measurable outcomes in many parts of the organization (OR) - Suitable positive results over time