

# BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

## FACULTY OF BUSINESS AND MANAGEMENT

FAKULTA PODNIKATELSKÁ

## INSTITUTE OF INFORMATICS

ÚSTAV INFORMATIKY

# THE CASE MANAGEMENT APPROACH IN THE DESIGN OF A KNOWLEDGE MANAGEMENT SYSTEM USED BY CSIRT TEAMS

CASE MANAGEMENT JAKO PŘÍSTUP K DESIGNU KNOWLEDGE MANAGEMENT SYSTÉMŮ  
POUŽÍVANÝCH CSIRT TÝMY

## MASTER'S THESIS

DIPLOMOVÁ PRÁCE

### AUTHOR

AUTOR PRÁCE

**Bc. Dušan Tichý**

### SUPERVISOR

VEDOUCÍ PRÁCE

**Ing. Petr Sedlák**

**BRNO 2023**

# Assignment Master's Thesis

Department: Institute of Informatics  
Student: **Bc. Dušan Tichý**  
Supervisor: **Ing. Petr Sedlák**  
Academic year: 2022/23  
Study programme: Information Management

Pursuant to Act no. 111/1998 Coll. concerning universities as amended and to the BUT Study Rules, the degree programme supervisor has assigned to you a Master's Thesis entitled:

## **The Case Management Approach in the Design of a Knowledge Management System Used by CSIRT Teams**

### **Characteristics of thesis dilemmas:**

Introduction  
Aim of the Thesis  
Theoretical Background  
Problem Analysis and Current Situation  
Proposals and Contribution of Suggested Solutions  
Conclusions  
References  
Appendices

### **Objectives which should be achieve:**

The thesis aims to explain what case management is, how it can be applied to support the work of incident response knowledge workers and what kind of economic and knowledge management benefits it will bring to an organization. This proposed approach will be demonstrated in a real-life example, presenting the main processes/steps of solving a spear-phishing incident using described case management system.

### **Basic sources of information:**

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Deadline for submission Master's Thesis is given by the Schedule of the Academic year 2022/23

In Brno dated 5.2.2023

L. S.

---

doc. Ing. Miloš Koch, CSc.  
Branch supervisor

---

doc. Ing. Vojtěch Bartoš, Ph.D.  
Dean

## **Abstrakt**

Tématem této práce je využití case management přístupu při designu knowledge management systémů pro IR (skupiny reakce na incidenty) CSIRT týmů. Cílem práce je vysvětlit pojem case management, jak může být aplikován při podpoře rozhodování znalostních pracovníků skupiny reakce na incidenty a jaké benefity přináší toto použití case management přístupu organizaci z hlediska ekonomického a z hlediska znalostního kapitálu. Práce popisuje návrh informačního systému založeného na principech case managementu, návrh transformuje stávající procesy v procesy využívající knowledge management a pokročilou automatizaci. Návrh je demonstrován na prototypu, který prezentuje hlavní procesy a kroky znalostního pracovníka při řešení spear-phishing incidentu.

## **Summary**

The topic of this thesis is an application of the case management approach when designing knowledge management systems used by the Incident Response part of CSIRT teams. The thesis aims to explain what case management is, how it can be applied to support the work of incident response knowledge workers, and what kind of economic and knowledge management benefits it brings to an organization. The thesis proposes a case management-based information system design that transforms an organization's processes into ones that leverage knowledge management and automation principles to support the expert workers. The transformation is demonstrated on a real-life prototype, presenting the main processes/steps of solving a spear-phishing incident using the described case management system.

## **Klíčová slova**

CSIRT, Incident Response, Knowledge Management, Case Management, Kybernetická bezpečnost

## **Keywords**

CSIRT, Incident Response, Knowledge Management, Case Management, Cyber security

# Rozšířený abstrakt

Pokročilé bezpečnostní hrozby jsou trend, kterému organizace čelí stále častěji, protože se stávají pro útočníky stále dostupnějšími. Tento fakt organizace nutí neustále zvyšovat požadavky na svoji kybernetickou bezpečnost, a to ve formě zabezpečení infrastruktury, školení uživatelů, řízení a auditů kybernetické bezpečnosti.

Napříč všem opatřením, jednou z nejúspěšnějších i nejsnazších forem kybernetického útoku je phishing, obzvláště jeho cílená forma spear-phishing. Úspěšnost těchto útoků můžeme přisuzovat lidskému faktoru a vysoké efektivitě sociálního inženýrství. Pro úspěšný útok útočník musí pouze získat přístup k typické formě firemní komunikace, například získá vzorek oběžníku, výplatní pásky nebo jiného rutinní emailu. Vzory těchto zpráv jsou navíc často dostupné ve veřejně dostupných zdrojích, často zveřejněné přímo danou organizací. Takovému útoku s vysokou pravděpodobností neodolá ani trénovaný profesionál, protože rutinní činnosti typicky nevyžadují zvýšenou pozornost a lidé je často řeší ve volných chvílích nebo z nutnosti.

Z toho vyplývá že není ekonomicky ani prakticky možné zabezpečit organizaci takovým způsobem, který by jí zaručil absolutní ochranu před jakoukoliv formou kybernetické hrozby. Právě naopak, organizace musí být na krizový scénář připravena, protože v opačném případě jí hrozí, že dopad útoku bude její nepřipraveností ještě umocněn.

Pokud chce organizace zavést systematické řešení, které je schopné reagovat na potenciální incidenty, může sestavit firemní CSIRT tým (Computer Security Incident Response Team, doslovně “Tým pro reakci na počítačové bezpečnostní incidenty”).

Tato práce se soustředí na analýzu současného stavu procesů, nástrojů a informačních systému používaných CSIRT týmy při řešení bezpečnostních incidentů, s cílem tyto procesy modernizovat s důrazem na automatizaci a využití znalostního kapitálu. Výsledkem analýzy je identifikace nedostatků v daných oblastech, která má za následek přetížení expertních pracovníků. Toto přetížení je způsobeno z kvalitním detekčním metod a již zmíněnou zvyšující se frekvencí kybernetických útoků.

Výstupem této práce je návrh informačního systému využívající principy case managementu (řízení případů) a knowledge managementu (řízení znalostí). Tento informační systém umožňuje automatizovat zpracování příchozích hlášení o potenciálních incidentech pomocí extrakce zájmových údajů a jejich obohacení na základě informačních zdrojů třetích stran a předchozích znalostí získaných organizací.

Uložení a využití znalostního kapitálu získaného při zpracování případů je další z vlastností popisovaného informačního systému. Informační systém je schopný vyhodnotit riziko představované kontextem a významem identifikovaných zájmových údajů a je schopný sám vykonat nebo doporučit vhodnou reakci. V případech, kdy je reakce, respektive výběr správného postupu, přenechán na expertním pracovníkovi je pak systém schopný uložit jeho postup v rámci případu i v rámci jednotlivých zájmových údajů. Tímto může poskytnout rozšířený kontext expertnímu pracovníkovi při příštím setkání s daným zájmovým údajem nebo případem podobným již řešenému případu, ve kterém se některý zájmový údaj vyskytoval.

Pro praktickou demonstraci navrhovaného systému využívám prototyp vyvinutý v rámci výzkumného projektu <sup>1</sup>, kterého jsem se účastnil. Jedná se o prototyp informačního systému, který implementuje část popsaných procesů a nástrojů. Prototyp je zaměřený na scénář, ve kterém expertní pracovník skupiny reakce na incidenty řeší hrozbu typu spear-phishing.

Poslední částí praktické kapitoly je ekonomické zhodnocení, které posuzuje, zdali je popsané řešení vhodným bezpečnostním opatřením z hlediska velikosti investice. Kapitola se věnuje ceně implementace pro vybranou organizaci, jelikož náklady závisí na kybernetické vyspělosti a vybavenosti organizace a na jejích zkušenostech a schopnostech se zaváděním podobných procesů a opatření. Pro finanční hodnocení navrhovaného řešení je použita metoda návratnosti investice do bezpečnosti ROSI doporučená agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

---

<sup>1</sup>Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb (ORION) [Kód projektu VI20202022164], vedoucí projektu RNDr. Daniel Tovarňák, Ph.D. Dostupné z <https://www.ics.muni.cz/veda-a-vyzkum/resene-projekty/49407>

## **Bibliographic citation**

TICHÝ, Dušan. The Case Management Approach in the Design of a Knowledge Management System Used by CSIRT Teams [online]. Brno, 2023 [cit. 2023-05-08]. Available at: <https://www.vutbr.cz/studenti/zav-prace/detail/150888>. Master's Thesis. Brno University of Technology, Fakulta podnikatelská, Ústav informatiky. Supervisor Ing. Petr Sedlák.

## **Declaration**

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

In Brno dated 13.5.2023

.....

Bc. Dušan Tichý

## **Acknowledgements**

I would like to thank my advisor, Ing. Petr Sedlák, for inspiring my interest in the managerial and legal view of cybersecurity. Next, I would like to thank RNDr. Daniel Tovarňák, Ph.D., who led the ORION project and also to all coworkers. The project was a significant inspiration for the topic of my thesis and interest. Last but not least, I want to thank my significant other and my family for supporting me.

# Contents

<b>Introduction</b>	<b>14</b>
<b>Aim of the Thesis</b>	<b>16</b>
<b>1 Theory</b>	<b>17</b>
1.1 Information Security and Cybersecurity . . . . .	17
1.1.1 CIA Triad . . . . .	17
1.1.2 Common Understanding of Cybersecurity . . . . .	18
1.1.3 Cybersecurity Threat, Vulnerability and Risk . . . . .	18
1.1.4 Three-Component Risk Assessment . . . . .	19
1.2 Cybersecurity Incident and Incident Management . . . . .	20
1.3 Terminology CSIRT, CERT or SOC . . . . .	23
1.3.1 Computer Security Incident Response Teams . . . . .	23
1.3.2 Security Operations Centres . . . . .	25
1.3.3 The General Internet Community’s Expectations of CSIRTs (RFC 2350) . . . . .	25
1.4 Incident Handling and Response Process . . . . .	28
1.4.1 CSIRT Member Roles . . . . .	28
1.4.2 Phases of Incident Handling . . . . .	31
1.5 Ticketing Systems . . . . .	38
1.5.1 Request Tracker for Incident Response (RTIR) . . . . .	38
1.6 Case Management . . . . .	38
1.7 Observables . . . . .	39
1.8 Business Process Model and Notation (BPMN) . . . . .	40
1.8.1 Process Diagram . . . . .	41
1.8.2 Activities . . . . .	41
1.8.3 Participants . . . . .	42
1.8.4 Events . . . . .	42
1.8.5 Other Common Elements . . . . .	43
1.9 Return on Security Investment (ROSI) . . . . .	44

1.9.1	Metodology . . . . .	44
1.9.2	ROSI Calculation . . . . .	45
<b>2</b>	<b>Current State Analysis</b>	<b>46</b>
2.1	Information Systems . . . . .	48
2.1.1	RTIR . . . . .	50
2.1.2	Network Monitoring . . . . .	52
2.1.3	Logs . . . . .	53
2.1.4	Data Centre Infrastructure Management / IP Address Man- agement . . . . .	53
2.1.5	Incident Reporting Form . . . . .	53
2.2	Critique of the Current Approach . . . . .	53
2.2.1	Unstructured Data and Automation . . . . .	54
2.2.2	Knowledge Management . . . . .	55
2.3	Conclusion . . . . .	55
<b>3</b>	<b>Solution</b>	<b>57</b>
3.1	Restructurization of Support Systems . . . . .	57
3.2	Case Management . . . . .	59
3.2.1	Case Overview . . . . .	60
3.2.2	Incident Report Automated Processing . . . . .	61
3.2.3	Automated Preliminary Analysis . . . . .	62
3.2.4	Automated Resolution . . . . .	64
3.2.5	Expert Resolution . . . . .	68
3.3	Phishing Use-Case Demonstration of Case Management Assisted Incident Resolution . . . . .	70
3.3.1	Conceptual Overview . . . . .	71
3.3.2	The Phishing Incident . . . . .	83
3.4	Investment Evaluation . . . . .	91
	<b>Conclusion</b>	<b>94</b>
	<b>Bibliography</b>	<b>95</b>

List of Figures	103
List of Tables	105
Glossary	108

# Introduction

With advanced cybersecurity threats being more frequent and more accessible to malicious actors, organizations have to invest more in protection and defensive measures. However, the most successful attacks are frequently not aimed at vulnerabilities in the infrastructure or in publicly facing systems. The most successful is phishing, one of the most accessible and frequent attacks—the undeniable success of phishing points to the most significant vulnerability in the organization, the users, and their susceptibility to social engineering. Even among trained expert staff, if an adversary gathers enough information to closely mimic routine processes or events in the standard workflow of a person, the odds of a potential attack succeeding are very high. [1, 2]

That leads to the conclusion that it is not economically and practically feasible to build a security measure great enough and train staff well enough that the possibility of a successful attack that can severely impact an organization could be ignored. In fact, the organization must be ready for this scenario. Otherwise, it may suffer even greater losses because of inappropriate responses.

If an organization wants a systematic solution capable of reacting to potential incidents, one possible option is to establish a Computer Security Incident Response Team (CSIRT). It is common practice to support the work of a CSIRT team using some request tracking system, typically in the form of a ticketing system. Ticket-based systems originate in a user-centric approach, typically expecting a ticket (short message describing the problem) written by a user in a non-structured non-standardized way.

This approach is proving problematic because the CSIRT team often has to deal with an overwhelming amount of reports by either a mass of automated detections or by a large number of user reports, e.g., originating from a phishing campaign. The ticketing systems allow prioritization and categorizing of the tickets. However, the system cannot capture and utilize knowledge potentially stored in the systems through decisions made by the CSIRT team.

This presents an opportunity for a design of an information system capable of not only storing the decisions of its users but for a system that can extract knowledge from its users and be able to learn and apply it in future tasks. The knowledge can be further supported and expanded by utilizing external sources of information that can be built into the system works by design. The system could simplify the work of the CSIRT's expert workers by automating routine tasks and allowing them to focus on tasks requiring expertise, supporting the expert's work with contextual information gained from external sources.

This thesis aims to outline the benefits of such an approach in incident handling response and to design an information system that implements described principles for CSIRT teams.

# Aim of the Thesis

This thesis aims to explain the current state of incident handling and response workflows in CSIRT teams. The Current State Analysis chapter focuses on the analysis and evaluation of a particular CSIRT team that uses a ticket-based system as a central solution for its processes. The analysis uses BPMN diagrams that describe the incident handling and response processes from the perspective of an expert worker, an incident handler, as he interacts with the ticketing system.

The Solution chapter of the thesis aims to explain the case management knowledge-focused approach and how it can be leveraged when designing an information system capable of supporting experts' work in the cybersecurity domain, specifically to support the incident response process. The chapter aims to combine the case management approach with the results of the current state analysis to design a case management-based information system that can replace the current ticketing system. The goal is to design a system that can support the expert's work using automated tools to transform incoming reports into structured data that can be enriched using external threat intelligence sources. The system will also be capable of preserving and leveraging decisions made by the expert workers, as this is a knowledge capital that can be used to support the automated processes and the expert's work by presenting historical data when the system or the worker encounters a situation similar to one already experienced. The capabilities of such design will be demonstrated on a working prototype in a scenario of a spear-phishing incident.

The final part of the chapter is the economic evaluation of the investment in the context of the chosen organization using the ROSI method recommended by the ENISA.

# 1. Theory

The Theory chapter consists of two parts, the first being the theoretical background focusing on cybersecurity teams, primarily on the incident handling and response processes. Moreover, it explains the concepts of observables, ticketing systems, and case management.

The second part, methodology, describes BPMN and ROSI methods used in the Current State Analysis and Solution chapters. The BPMN is used to describe and analyze the organization's cybersecurity processes. The ROSI is used to evaluate the economic feasibility of the proposed solution.

## 1.1. Information Security and Cybersecurity

Information and data will always be critical assets for a society whose value will continue growing. Today it is already possible to rank information among the main factors that constitute the development of society. Therefore, **Information Security** (known as **InfoSec**) grows in importance to provide confidentiality, integrity, and availability of information and information systems and protect them from unauthorized access, use, disclosure, disruption, modification, or destruction [3].

### 1.1.1. CIA Triad

The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability.

- **Confidentiality** - The act of protecting data from being observed or accessed by any unauthorized entity (person). An example would be preventing passwords from being stolen.
- **Integrity** - The act of maintaining data in its full form without filtering, truncating, or their lost (complete); data are not altered or aggregated (accurate); they stay unchanged regardless of how or how often it's accessed and no matter how long it's stored (consistent) and finally, data cannot be accessed by

any unauthorized entity (person). An example is preventing, e.g., ransomware type of malware.

- **Availability** - The act of maintaining data accessible to use when needed. An example is preventing attacks that can take down the organization's network or its services.

### 1.1.2. Common Understanding of Cybersecurity

Considering Information Security, we encounter the term *cybersecurity*. In today's society, cybersecurity is often used as a synonym for Information Security. In practice, between these terms is not a big difference. Information Security refers to organizations' procedures and practices to protect their data. At the same time, cybersecurity presents a set of legal, organizational, technical, and educational means to ensure the protection of **cyberspace** (a digital environment consisting of information systems, services, and communication networks enabling the creation, processing, and exchange of information) [4].

The NIST defined cybersecurity as: "*Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*" [5, 6].

ENISA addresses the concept of cybersecurity throughout the document *Definition of cybersecurity – Gaps and overlaps in standardization* [7] where it recognizes five different domains within the term cybersecurity: Communications Security, Operations Security, Information Security, Military Security, and Physical Security. A deconstruction of these components constituting the term cybersecurity is illustrated in Figure 1.1.

### 1.1.3. Cybersecurity Threat, Vulnerability and Risk

In cybersecurity, there is a close relationship between cybersecurity threat, vulnerability, and risk.

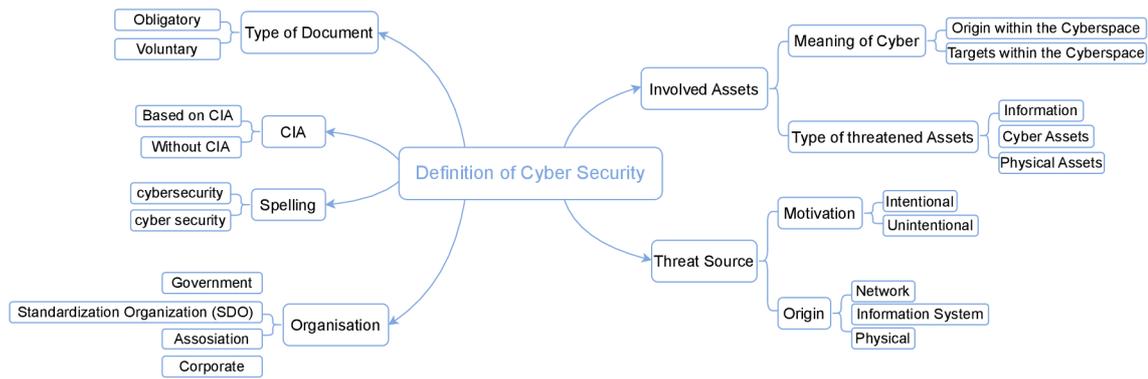


Figure 1.1: Components Constituting the Definition of Cybersecurity Defined by ENISA [7, p. 13]

**Cybersecurity threat** can be defined as any (intentional or accidental) circumstances or events with the potential to negatively impact an organization, its functionality, image or reputation, organizational assets (any data, device, or another component that needs to be protected from a company’s perspective) or individuals. **Cybersecurity vulnerability** is a weakness of an asset or a weakness of a security measure that one or more threats can exploit. **Cybersecurity risk** is the possibility that a particular threat will exploit the asset’s vulnerability and cause damage. [8, 9]

To conclude, the intersection of organizational assets, their vulnerability, and the existence of threats present a risk.

#### 1.1.4. Three-Component Risk Assessment

Risk assessment, as a part of risk management, is a process used to determine the likelihood of a risk occurring and its potential impact.

In the Czech Republic, Asset and Risk Management is one of the obligations given by Decree No. 82/2018 Coll. Without knowing what assets the organization has and what risks threaten it, most other obligations given by the law cannot be effectively fulfilled. By risk management, the organization identifies what risks threaten the organization and its assets and how the assets need to be protected, i.e., what security measures need to be put in place, and prioritizes the implementation of these security measures.

Risks are identified based on relevant *asset-vulnerability-threat* combinations. For risk assessment, a calculation using the following Formula 1.1 influenced by **three components** is used: impact, threat, and vulnerability, where *impact* means the asset value of the respective attribute (confidentiality, integrity, availability).

[10, pp. 69]

$$RISK = IMPACT \times THREAT \times VULNERABILITY \quad (1.1)$$

The risk assessment defines the following levels of risk according to the acceptability criteria. The exact values may vary depending on the regulation under which the organization falls – in the Czech Republic, this is determined by the NCISA based on Decree No 82/2018 Coll. on Security Measures [8] and the Act No 181/2014 Coll. on Cyber Security [4]:

- **Low** - The risk is considered to be acceptable.
- **Medium** - The risk can be reduced by less demanding measures or, in the case of higher, more demanding measures, the risk is acceptable.
- **High** - The risk is unacceptable in the long term, and systematic action must be initiated to eliminate it.
- **Critical** - The risk is unacceptable, and action must be taken immediately to eliminate it.

## 1.2. Cybersecurity Incident and Incident Management

Incident management is a process used by IT Operations and DevOps to respond to and address unplanned events that can affect service quality or service operations., i.e., incidents are limited to computers, network appliances, networks, and the information inside this equipment or in transit.

Incident management consists of various areas such as incident handling, vulnerability handling, announcements and alerts, and others. This thesis focuses on incident handling provided by cybersecurity teams as a service to society, of which workflow is described in more detail in Section 1.4.

Incident management within a company's IT operations often refers to ITIL incident management [11]. The lifecycle of the incident can go through several phases. The ITIL (IT Infrastructure Library) [12, 13], a library of best practices for managing IT services and improving IT support, defines the following phases of the incident lifecycle, which can be mapped to the cybersecurity incident as well:

- **Occurrence** - an incident is an unplanned disruption to an agreed service;
- **Detection** - incident resolution starts when a user or an automated system detects an error – the goal is to shorten the time between Occurrence and Detection;
- **Diagnostics** - identification of the characteristics of the incident, match it to previous incidents, problems, and known errors;
- **Repair** - a repair to the user and recovery is still needed;
- **Recovery** - a process of restoring the failed items to their last recoverable state, required testing, final adjustment, or configuration;
- **Restoration** - a process of providing an expected service back to a user;
- **Closure** - the final step, a user and an incident handler check that a service is fully available.

Knowing the lifecycle phases can be beneficial during the incident handling process. Another purpose of observing the incident lifecycle is to improve the incident handling process itself. The long last phases can be shortened if they are found to be unjustifiably long. Decreasing the time of particular phases should not be an aim in itself. The ITIL [14, 12] also defines several measurements presenting the average elapsed time between some of the incident lifecycle phases:

- **MTTR (Mean Time to Repair)** - the average time between detecting an incident and repairing the failed component, e.g., diagnosing and replacing a failed disk. Essentially this measures the technical response to diagnose and repair the failed component. The shorter this time, the better because shortened times mean less downtime for the user. The goal is to shorten the time.
- **MTRS (Mean Time to Restore Service)** - the average time between detecting an incident and fully restoring the service to the user. This is a measure of the quality of your operational processes and system design to facilitate recovery after a failure. The goal is to shorten the time.
- **MTBF (Mean Time Between Failures)** - the average time between the restoration of service following an incident and the detection of the next incident. In this case, a long time between failures indicates a reliable service.
- **MTBSI (Mean Time Between System Incidents)** - the average time between incidents (including the MTTR and MTRS). Understanding the proportion of repair and restoration time versus failure-free time for a particular service enables prioritization of service and system improvements. For example, commit resources to improve a critical business service that experiences few but lengthy failures and give a lower priority to repairing a less business-critical service with frequent failures, which requires few resources and time to restore.

The whole lifecycle is illustrated with individual measurements in Figure 1.2.

*Cybersecurity incident* presents an event determined to have a (possible) impact on the organization by violating its security policies and prompting the need for response and recovery [15]. A well-known example of a widespread cybersecurity incident is phishing, emails that attempt to trick individuals into giving away sensitive information or login credentials [16, 17].

The well-known fact is that cybersecurity threats are increasing and becoming more complex. One of the most effective ways to counter these threats is by creating

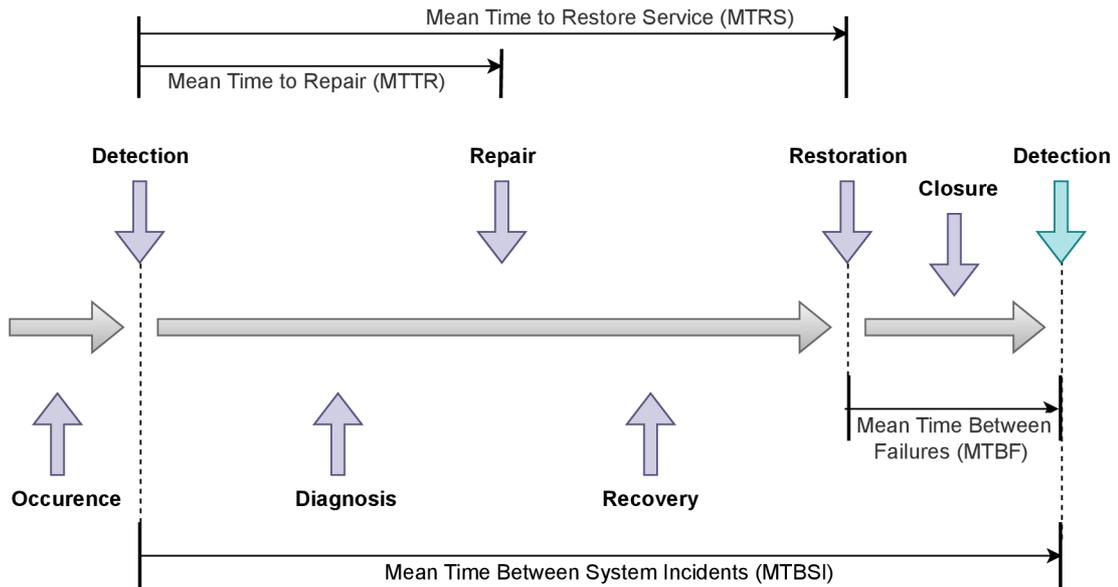


Figure 1.2: The Phases of the Incident Lifecycle [14]

a global ecosystem of cybersecurity teams, security incident response teams, and security operation centers that can communicate, share information, and respond to resulting cybersecurity incidents.

### 1.3. Terminology CSIRT, CERT or SOC

The most common terms used to describe teams related to the incident response handling process are CSIRT, CERT, and SOC. This section describes the differences among them and the services hidden behind them, also illustrated in Figure 1.3.

#### 1.3.1. Computer Security Incident Response Teams

The term **CSIRT**, or **Computer Security Incident Response Team**, was established in the 1990s, and it stands for a team of experts implementing activities supporting cybersecurity in information technology. One of the core documents issued by ENISA on forming cybersecurity teams defines a CSIRT as “a team of IT security experts who mainly respond to computer security incidents, provide the necessary services to deal with, and support its constituents to recover from a failure” [19]. The CSIRT’s main objectives are responding to security incidents in their

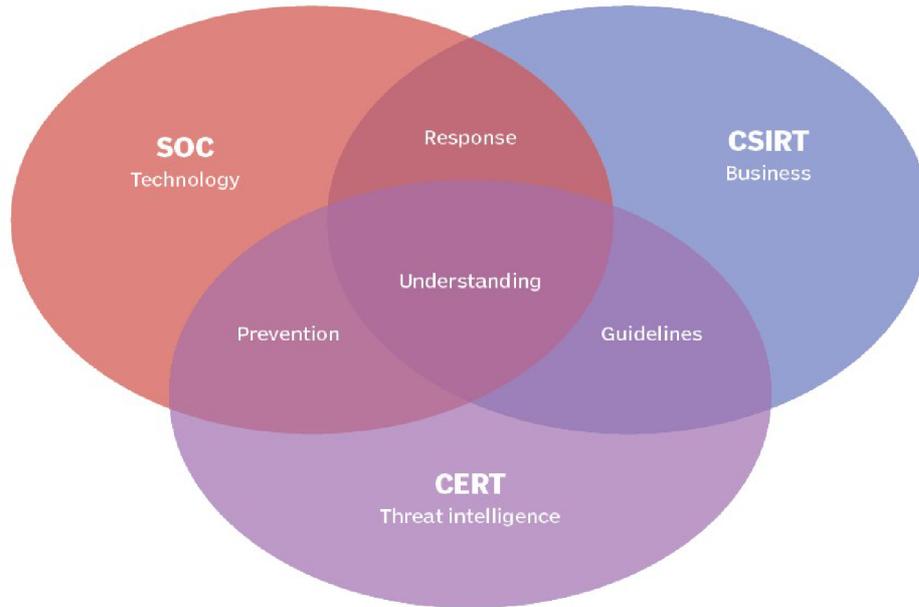


Figure 1.3: Comparison of CSIRT, CERT, and SOC Centers of Attention [18]

defined constituency (area of their responsibility) and related incident investigations in case of a possible user attack.

Nowadays, we can encounter various analogies of naming CSIRT teams. They are also known as CIRTs (Computer Incident Response Teams) or SIRTs (Security Incident Response Teams). In Europe, CSIRT is mainly used parallel to the **CERT** teams – **Computer Emergency Response Teams**.

The difference between CSIRT and CERT highly depends on the context and can be confusing. As the term, the CERT has been a registered trademark of Carnegie Mellon University since 1997. Therefore, an organization using CERT as part of a response team name must apply for authorization to use the CERT mark. Otherwise, they should not have it in use for a consulting service name or managed security service provider.

In comparison to the use of the CERT as a synonym for CSIRT team providing primarily incident handling and response, Carnegie Mellon’s CERT designation has a particular focus on operations with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks. Furthermore, a CERT should research problems with widespread cybersecurity im-

plications and develop advanced methods and tools [20]. Some organizations use CERT to reflect that their internal team's focus is subtly different from that of a typical CSIRT.

In general, CERT and CSIRT (CIRT, SIRT) can exist as permanent groups or be pulled together ad hoc in response to an event. Either way, their focus is on phases of incident handling (response), e.g., following the NIST [21] or ENISA [22] while not specified in other ways.

### 1.3.2. Security Operations Centres

While CSIRTs or CERTs focus specifically on incident response, **Security Operation Center (SOC)** [19] generally encompasses multiple aspects of security operations.

The responsibilities of SOC can vary based on the size of the organization in which it operates. In smaller organizations, CSIRTs and SOCs are often considered to be synonymous. In large enterprises, SOC mainly focuses on monitoring and detection services, and incident handling is handed over to a separate CSIRT.

For most of today's organizations, SOC represents the first line of their security. It is an in-house or outsourced team of IT security experts that monitors an organization's entire IT infrastructure 24 hours a day, seven days a week, to detect cybersecurity events in real-time.

A security operations center improves an organization's threat detection, monitoring operations and controls (intrusion detection/prevention systems, security information event management/security information management), identity management and authorization, firewall and filtering ruleset maintenance, forensics, and investigation support, or any other aspect of operational security.

### 1.3.3. The General Internet Community's Expectations of CSIRTs (RFC 2350)

The request for comment document of the number 2350 (RFC 2350) [23] represents a public document that describes the community's expectations of computer

security incident response teams (CSIRTs). Individual teams will always differ in the set of services provided, and it caused misunderstandings regarding what to expect from CSIRTs among communities in the past. As it is impossible to define a set of requirements that would be appropriate for all of them, the RFC 2350 should serve as a framework for presenting the important subjects related to the incident response that is of concern to the community. In other words, the RFC 2350 is a public document providing a general template with a list of topics, issues of concern, and interest to constituent communities to help CSIRTs complete and publish their own RFC 2350 document.

The RFC 2350 template defines several types of information that can/should be provided by the specific CSIRT team. For example, as details about CSIRT can change over time, the CSIRT should always publish in their RFC 2350 the date of its last update. Then, the CSIRT is required to guarantee to publish the location of the current version of the document, for example, on its official website page. It can also provide a mailing list for users to obtain updates through it on time.

Further, full details of how to contact the CSIRT should be listed in RFC 2350: the name of the CSIRT, mailing address, time zone (useful when coordinating incident cross time zones), telephone number or other telecommunications, public keys and encryption, operating hours and team members (at least highest management). Moreover, every CSIRT must specify what it is to and the authority under which it will do it. Following are items that at least CSIRT must include [23]:

### **Mission Statement**

The mission statement should clearly and unambiguously define the team's core activities, goals, and purposes, which are already stated in the definition of a CSIRT. In order to be considered a Computer Security Incident Response Team, the team must support the reporting of incidents and support its constituency by dealing with incidents.

## **Constituency**

A CSIRT's constituency can be determined in several ways. The definition of the constituency should create a perimeter around the group to whom the team will provide service. It could be a company's employees or its paid subscribers. It can be defined as a technological focus, e.g., users of a particular operating system or by network domain or IP address range.

## **Sponsorship/Affiliation**

The sponsoring organization, which authorizes the actions of the CSIRT, should be as this helps the users understand the background and set-up of the CSIRT.

## **Authority**

A CSIRT may or may not have the authority to intervene in operating all of the systems within its perimeter. While an organizational CSIRT will be given its authority by the organization's management, a community CSIRT will be supported and chosen by the community, usually in an advisory role. If other CSIRTs operate hierarchically within its perimeter, this should be mentioned here, and the related CSIRTs identified. This section usually varies greatly among teams.

## **Policies and Services**

The rest of the RFC 2350 should present the CSIRT's policies - types of incidents capable of solving and level of support provided, requirements on communication and authentication, and specification of the incident reporting forms, which CSIRT prepared for its users to use.

The rest of the document can (does not have to) be used for more detailed information about how the incident handling phases, such as triage or collaboration within teams, are performed.

## 1.4. Incident Handling and Response Process

Incident management, handling, and response are the fundamental activities provided by cybersecurity teams (CSIRT/CERT) [23]. The section presents the roles of the cyber security teams, primarily those responsible for the incident handling process and the phases of this process as given in the standardized documents of NIST and ENISA.

### 1.4.1. CSIRT Member Roles

Cyber security teams may consist of various members representing one or more roles with a scope of responsibilities defined, i.e., a role may be assigned to a single person or a group of people [24]. Even though various standards, regulations, or best practices appoint these roles, there is no standard set of roles, leaving this decision to each computer security incident response team [25, 26]. This section describes differences and identifies the crucial roles, mainly for the incident handling process.

With regard to the information security management system, Act No 181/2014 Coll. on Cyber Security [4] defines as obliged entities within the information security management system four main roles:

- **Cybersecurity Manager** is a security role responsible for the information security management system. It can be a person trained for this activity and demonstrating professional competence in cybersecurity management or information security management for at least three years or one year when graduating from university.
- **Cybersecurity Architect** is a security role responsible for drafting the implementation of security measures to ensure a secure architecture of the information and communication system with demonstrated professional competence by training for this position for the same period as cybersecurity manager.
- **Asset Guarantor** is a security role responsible for ensuring the development, use, and security of the asset.

- **Cybersecurity Auditor** is a security role responsible for conducting cybersecurity audits, again trained for this activity and demonstrating professional competence in conducting cybersecurity audits or audits of information security management systems for a period of at least three years or at least one year when graduated from university.

In general, there are two more related roles to define: **CISO (Chief Information Security Officer)** and **CSO (Chief Security Officer)**. CISO is a role primarily focused on securing an organization's information systems and data. In contrast, the CSO's role encompasses all aspects of security, including physical and information security, as well as human safety [27, 28]. In this context, the CISO corresponds to the cybersecurity manager role required by Act No 181/2014 Coll. on Cyber Security.

### **Incident Handling Roles**

As this thesis aims at the incident handling process, in the rest of this section, we mainly focus on the roles important for the incident handling process, especially the *incident handler*.

ENISA [22, pp. 28] identifies several essential roles for CSIRT teams providing incident handling as a service to occupy the following positions, namely *Incident Manager*, *Incident Handler*, *Duty Officer*, and *Triage Officer*.

- **Incident Manager** is responsible for coordinating all incident handling activities, i.e., the incident manager is not included in handling himself daily until more critical and complex ones occur [29]. Then, he/she is the main decision-making body and represents the incident handling team outside the team. A dedicated person without incident handling obligations can fulfill this role or one of the more senior incident handlers.
- **Incident Handler** plays a crucial role in the incident handling team. Handlers deal with the incidents – analyzing data, creating workarounds, resolving the incident, and communicating clearly about the progress to the incident manager and with the appropriate constituent(s). Moreover, they propose

improvements in the incident handling process. The role of the incident handler requires much more advanced IT security technical knowledge and strong communication and analytical skills with stress resistance.

- **Duty Officer** handles all incoming requests and carries out periodic or ad hoc activities for this role. In many organizations, the duty officer is one of the incident handlers responsible for the duty based on the predefined timetable.
- **Triage Officer** is the person responsible for the Triage phase of incident handling (see Section 1.4.2). He/she has to deal with reported incidents, decide whether it is an incident within the team's constituency, when to handle it, and who will be the incident handler. The triage officer also discusses new incidents and trends with team members to be ready for further action.

Best practices provided by FIRST, the global Forum of Incident Response and Security Teams [30], define a slightly different specification of responsible for information security incident management.

Besides the Incident Triage Coordinator (the equivalent of an ENISA Triage officer), they include forensic analysts and IT administrators. These roles are not always directly part of the incident handling and response group but are team members cooperating with incident handlers. In the case of the forensic analyst, this is debatable and depends case-by-case. However, IT administrators are often part of IT operations or separated IT departments.

The FIRST also uses for incident handlers two separate terms [31, pp. 22]: *Incident Analyst* and *Incident Responder*. Together, they correspond to the Incident Handler defined by ENISA.

1. **Incident Analyst** analyzes information security events and confirms information security incidents by assessing their potential impacts and damages. They are responsible for establishing relations and dependencies among all events and incidents or correlating new events or incidents to each other once they are identified. They are possibly performing research for new patterns describing new attacks.

2. **Incident Responder** analyzes and has to gain an understanding of a confirmed information security incident. Their responsibility is to intake, catalog, store, and track information related to the incident. They focus on reducing the loss and recovering damage by specifying countermeasures and mitigations to avoid further attacks and losses by, e.g., removing exploited vulnerabilities or weaknesses and improving overall cyber security.

In practice, more important than having separately specified people performing each role mentioned above and related tasks is to cover the services provided by these roles among the team as reasonably fulfilling the CSIRT mission.

### 1.4.2. Phases of Incident Handling

The incident handling process has many phases. It describes the sequence of steps that begin when an incident reaches the cybersecurity team. It could follow a very simple or very sophisticated model [32, 33].

There are several documents formalizing this process. The most fundamental workflow of incident handling was provided by CERT/CC [34], which consists of four phases: detection, triage, analysis, and incident response. In this section, we describe the most used ones – NIST [35] and ENISA [22], which extend CERT/CC. It is worth noting that these documents are often mutually inspired, which makes them, in some context, similar and interchangeable [36].

In addition, it is necessary to point out that in practice, the real process of each team can change as their activity is significantly influenced by human and financial resources or available technologies.

#### NIST Incident Handling Lifecycle

NIST divides incident handling and response into four main phases, illustrated in Figure 1.4.

**Preparation** phase is by NIST divided into two reactive and proactive components – *preparation* and *prevention*. The main goal is to prepare the incident response team for incident resolution by acquiring the necessary tools and resources.

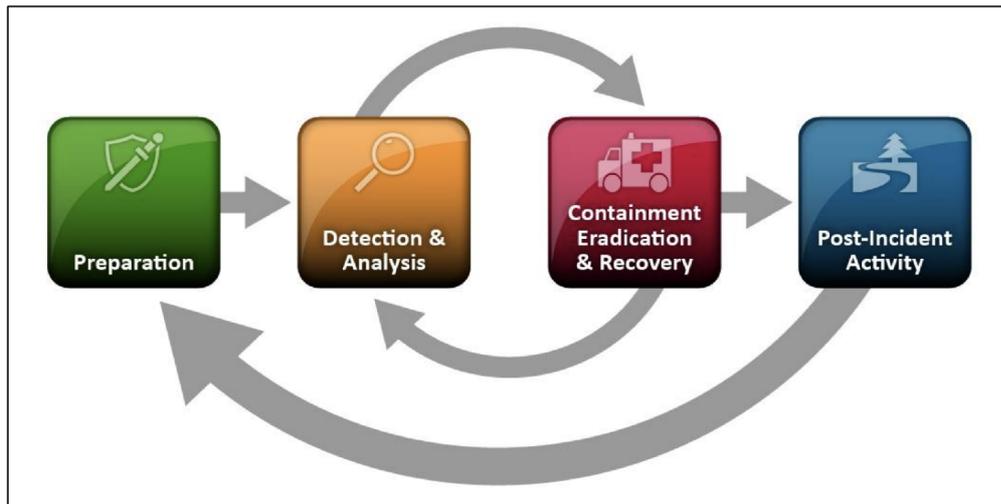


Figure 1.4: By NIST Defined Phases of Incident Response Lifecycle [35, pp. 21]

NIST lists various Incident Handler communications and facilities needed for this phase, such as contact information, issue tracking system, or so-called War room for central communication and coordination. In addition, there is a need for various protocol analyzers, packet sniffers, digital forensic software, network diagrams, port lists, and documentation of relevant software or hardware. However, the preparation phase also includes preventing incidents by ensuring that systems, networks, and applications are sufficiently secure and by implementing a set of controls based on the results of risk assessments. Prevention includes risk assessments, network security and hardening, malware prevention, and user awareness and training.

**Detection and Analysis:** First, the incidents must be detected and categorized. For many organizations, this is the most challenging part—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion detection or prevention systems, antivirus software, and log analyzers [37]. Incidents may also be detected manually, such as problems reported by users.

Organizations should be prepared to handle different incidents with different response strategies. NIST listed several common attack vectors, which can be used as a basis for defining more specific handling procedures: attacks executed from

external/removable media, web attacks, email attacks (phishing), attacks that employ brute force methods to compromise, degrade, or destroy systems, networks, or services (DDoS), impersonations (man-in-the-middle, spoofing), loss or theft of equipment, an incident resulting from a violation of an organization's acceptable usage policies and others [35, pp. 25].

The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and a deeper analysis of the effects of the incident. The incident response team should work quickly to analyze and validate each incident, following a predefined process and documenting each step taken. Every action from the incident's detection to its final resolution should be recorded and timestamped. Every document regarding the incident should be dated and signed by the incident handler. However, the incident analysis covers much more activities than just the analysis itself. Incident handlers should permanently expand their knowledge to recognize normal behavior and differentiate from others quickly. [35]

According to NIST, incident detection, categorization, initial analysis, and prioritization should take place approximately in this order. Still, because they are pretty interdependent, they often overlap. As Figure 1.4 shows, the detection and analysis phase can be repeated with more information obtained.

**Containment, Eradication, and Recovery** phase highly depend on the type of incident. The containment part is critical for many incidents, e.g., spreading ransomware among an organization's computers, quickly identifying the affected segments, and cutting them off from the world. Furthermore, containment provides time for developing a tailored remediation strategy.

After that, evidence gathering and handling of the incident starts, including forensic analysis. Although the primary reason for gathering evidence during an incident is to resolve it, it may also be needed for legal proceedings. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies [38].

Handling requires identifying the attacking hosts if it's possible. The final step is eradication and recovery. In recovery, administrators restore systems to regular operation. It may involve repairing systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets and boundary router access control lists).

**Post-Incident Activity** is the last and not least important part of incident handling, including a "lessons learned" meeting with all involved parties. They can be extremely helpful in improving security measures and the incident handling process itself. Small incidents require only post-incident analysis, except for incidents performed through new attack methods of widespread concern and interest. After serious attacks, holding post-mortem meetings across the whole team is usually worthwhile. Another important post-incident activity is creating a follow-up report for each incident, which can be valuable for future use. [35]

## **ENISA Incident Handling Workflow**

ENISA expands CERT/CC incident handling workflow to nine phases with various sub-steps, illustrated in Figure 1.5.

In the initial phase, the incident is detected, reported, and registered – ENISA does not include incident detection within incident handling.

The whole process starts when the team receives the **Incident Report**. It can be done automatically by intrusion or anomaly detection system or via a third party – another cybersecurity team, IT administrators, or ordinary users.

**Registration** represents the step of the ticket registration into the incident handling system, e.g., the ticketing system. ENISA recommends using some alphanumeric references so they can be easily managed in the future. An incident report should also be linked or combined with other related already-registered incident(s).

**Triage** in ENISA guidelines refers to a French medical term that describes a situation in which we have limited resources and must decide on the priorities of actions based on the severity of particular cases.

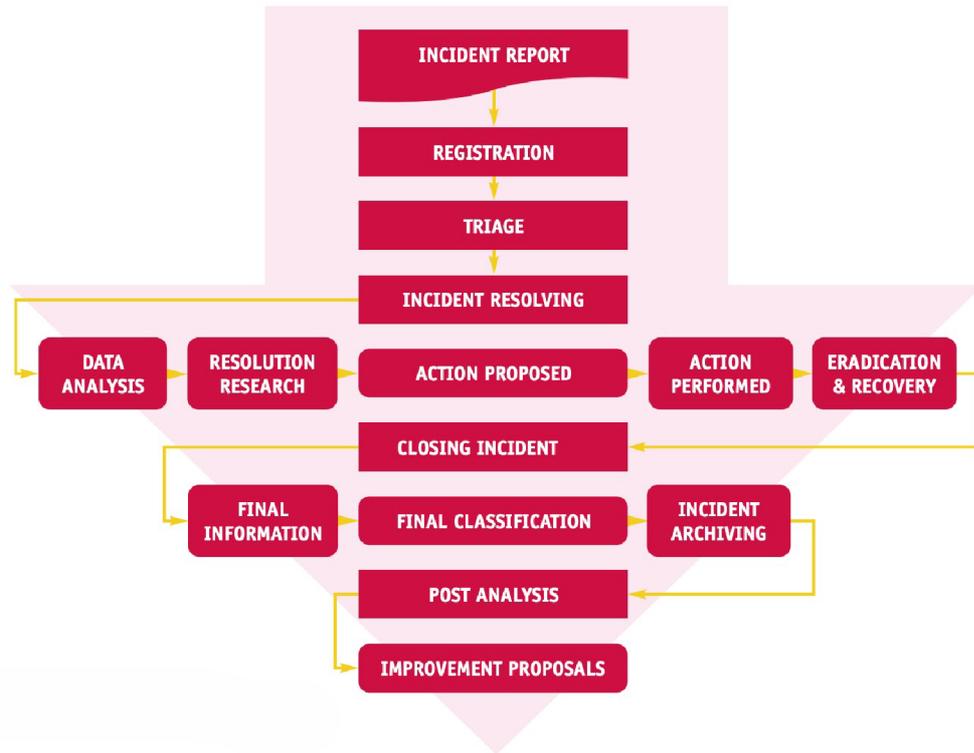


Figure 1.5: ENISA Workflow of Incident Handling - Source: ENISA Incident Management Guide [22, pp. 37]

The triage should be performed in the same way as the doctor proceeds with patients. Therefore, triage should determine the significance of the constituency, the incident reporter’s experience, the incident’s severity, and time constraints. Examples of the triage process and questions the incident handler should ask are visualized in the presented diagram (Figure 1.6).

ENISA divides the triage into three sub-phases:

- *Incident Verification* should verify whether the reported incident is an incident, e.g., automatic communication of server, email replays about undelivered email or whether the incident is from the team’s constituency.
- *Initial Classification* of the incident according to the team’s internal classification schema. Prioritization is part of the process.
- *Incident Assignment* – the incident is assigned to the incident handler.

After the initial triage process, the **Incident Resolution** phase starts. This is the longest phase that should lead to the incident solution. ENISA divides incident

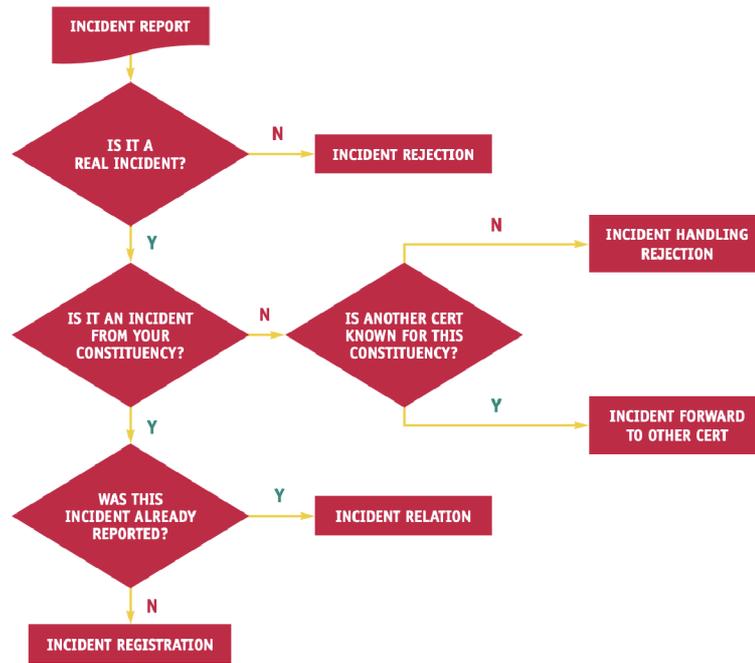


Figure 1.6: The Example of Incident Handling Triage - Source: ENISA Incident Management Guide [22, pp. 38]

resolution into five subphases (Figure 1.5), which usually repeat in a cycle several times: *Data Analysis*, *Resolution Research*, *Action Proposed*, *Action Performed*, and *Eradication and Recovery*.

**Data Analysis** is the first step, starting with notifying and collecting data from the parties involved. There are several primary sources of such data: incident reporters, monitoring systems, referring databases, and other sources – relevant log files from routers, firewalls, web applications, mail servers, DHCP servers, or authentication servers. The other parties that can help collect the necessary information are the attack targets (should be informed whenever it is identified), internet service providers (ISPs) involved, including on both attacking and attack target sides, or internet content provider and law enforcement agencies (LEA). To complete the notification and data collection tasks, the data analysis starts.

**Resolution Research** brings up observations about the incidents and draws conclusions. Subsequently, in the **Actions Proposed** phase, the team should prepare a set of concrete and practical tasks for each party involved.

In the **Action Performed** phase, the handler’s responsibility should be to check the proposed actions have been completed. However, handlers have only limited

power to force all parties to do that. The only exception is where the cybersecurity team is also in the role of, e.g., the internet service provider's CERT, and the user rules for customers state that if they do not act appropriately on proposals, it is allowed to limit their internet access. Finally, all proposed actions have one main goal – **Eradication and Recovery** of the involved systems.

When the incident resolution cycle is finished, the handlers can start with the **Incident Closure**. This phase is again by ENISA divided into more separate steps [22]. **Final Information** covers informing each party of the incident. These are mainly a source of the incident (i.e., attacker), attack targets, and/or a report of the incident (can be the same person), followed by the most important parties involved in resolving the incident – ISPs, other CERTs, and LEAs.

**Final Classification** - there are at least three points during the incident handling process when incidents can be classified, and classification can be changed. The first is at the start when you receive a report. The next point is during the resolution period and, finally, at the end of the incident handling process. Lastly, the **Archiving** of the incident data is required for a legal period. After that, the team must destroy the data.

**Post-analysis**, as the word suggests, occurs after the incident's conclusion. ENISA recommends as a good practice to wait with this phase for some time after an incident, as there is a natural resistance of incident handlers to perform the post-analysis, i.e., the resolution is made, handlers do not need to do more work as it has already been done. However, when organized periodically and systematically, post-analysis meetings can be an important and valuable part of your teams' professional life.

The result of post-analysis, or incident handling in general, should be **Proposals for Improvement** in the future. Examples of such improvements can be to teach the users, i.e., attack targets (constituency), how to describe an incident better or avoid similar incidents in the future. The CSIRT teams can advise and explain to the ISP the mechanisms of the most critical incidents and how to handle them systematically. Also, they can support or propose legal actions to related legislation parties.

## 1.5. Ticketing Systems

A ticketing system is an information system that allows users to place their requests in the form of tickets. The ticket is a record representing a user request, report, or incident. The user may be a member of an organization, business partner, customer, or automated system. [39]

The ticketing system offers multiple advantages for the company. It presents a unified place where users can place a request. It allows them to prioritize and categorize the requests, seamlessly dividing the work between multiple teams or divisions. The ticketing system's other typical benefits are statistical data and reports. In some cases, the systems also provide knowledgebase-like systems to support users' self-service. [39, 40]

### 1.5.1. Request Tracker for Incident Response (RTIR)

The Request Tracker for Incident Response (RTIR) is a particular type of ticketing system. RTIR is an extension of the popular open-source ticketing system Request Tracker (RT) [40], providing additional functionality and features designed explicitly for incident response and security teams, such as pre-configured queues or workflows. It allows incident responders (incident handlers) to create, assign, prioritize, and manage incidents in a structured manner. It also supports integrating different communication channels like email, phone, and messaging, enabling real-time collaboration between incident responders. RTIR is then designed to correlate critical data from the incident reports, which can be from both people and automated tools, and to link incident reports with a common root cause incident. [41]

## 1.6. Case Management

Case management is a term used to describe a process adopted in many fields of work, each having its definition and usage adapted to their specific needs and more or less differing from each other.

The point of case management is to provide a collaborative medium that can concentrate all information regarding a so-called *case*. The case concept is inspired by areas such as social services, medicine, or law, where a case exists to represent a specific client, treatment, or lawsuit and contains all information available to the case. [42]

In the context of the cybersecurity solution, case management represents an information system capable of concentrating all information concerning a case, e.g., cybersecurity incident. The point of the centralized solution is to provide a platform where information from multiple sources can be collected and presented to a user. It allows the preservation of decisions concerning the case, whether automated or done by users. That enables storing knowledge capital in the solution, allowing the users and automated systems to leverage historical procedures and decisions to support users' decision-making in similar cases. The concept of case management for cybersecurity, primarily incident handling and response processes, is discussed in more detail in the Solution chapter of this thesis.

## 1.7. Observables

The observable represents an event (benign or malicious) on a network or system that can be captured/observed at a particular time, characterized, and analyzed.

In cybersecurity, the concept of *Cyber-observable Objects (SCOs)* is mostly characterized by host-based and network-based information, e.g., information about an existing file, a process observed running, or network traffic occurring between two IPs. The observables, however, identify only what happened on a network or host and do not capture the who, when, or why [43].

In the operational cyber realm, observable is a central underlying element of many of the different activities involved in cyber security. Unfortunately, there are no uniform standard mechanisms for specifying, capturing, characterizing, or communicating cyber observables today. Each activity area, each use case, and often each supporting tool vendor uses its own unique approach that inhibits consistency, efficiency, interoperability, and overall situational awareness. [44]

## 1.8. Business Process Model and Notation (BPMN)

Business Process Modeling and Notation (BPMN) [45, 46], developed by the Object Management Group (OMG), is a process diagramming language designed to specify a complete business process in a standardized way.

BPMN is an open standard notation system that intends to standardize a business process model and notation in the face of many different modeling notations and viewpoints. It provides a notation readily understandable by all business users and business analysts creating the initial draft of processes to technical developers and programmers implementing the technology that will perform those processes and also to the business people who will manage and monitor those processes. Therefore, the standard is widely used in business process management [42, pp. 156].

BPMN has many rules on how things can be connected and what is valid or not valid. For this thesis, we use the latest BPMN version 2.0., a notation necessary for preparing diagrams for this thesis within the section of Current State Analysis and the proposed system in Solution to model the incident handling process and its parts.

We point out that added extensions to BPMN version 2.0 to support BPEL language (XML-based process specification language for the technical specification) [47] to be compatible with the functionality of previous BPMN version make the language less accessible to business users than professional programmers [42, pp. 156]. In the following sections, we provide only the necessary overview of diagrams and the elements that are used within the thesis. BPMN version 2.0 supports following types of diagrams:

- **BPMN core** elements to define Infrastructure, Foundation, Common, and Service packages;
- **Process diagrams**, which include the elements defined in the Process, Activities, Data, and Human Interaction packages;
- The diagrams defining how individual process interact with each other, namely **Collaboration diagrams**, **Conversation diagrams** and **Choreography diagrams**.

### 1.8.1. Process Diagram

A Process describes a sequence or flow of Activities in an organization to carry out the work. The Process is a graph of so-called Flow Elements, which can be a set of Activities, Events, Gateways, and Sequence Flows.

BPMN uses the term Process specifically to mean a set of flow elements. It uses the terms Collaboration and Choreography when modeling the interaction between Processes.

### 1.8.2. Activities

An Activity is a work (Task) performed within a Process. An Activity can be atomic or non-atomic (compound). The types of Activities as a part of a Process are Task, Sub-Process, and Call Activity, which allows the inclusion of reusable Tasks and Processes in the diagram.

A **Task** is an atomic Activity within a Process flow. A Task is used when the work in the Process cannot be broken down to a finer level of detail. Generally, an end-user and/or applications are used to perform the Task when it is executed.

Task and Sub-Process are represented by the same shape – a rectangle that has rounded corners. In Process, there can be various Tasks differentiated by markers – symbols within the rectangle. The variants of Tasks are visualized in Figure 1.7.



Figure 1.7: BPMN Tasks Overview - source: BPMN Specification [45, pp. 156–165]

A Service Task is a Task that uses some service, which could be a Web service or an automated application. A Send/Receive Task is for sending/receiving a Message. Once the Message has been sent/received, the Task is completed.

A User Task is a typical “workflow” Task where a human performer performs the Task with the assistance of a software application and is scheduled through a

task list manager. The User Task can be implemented using different technologies specified by the implementation attribute. Besides the Web service technology, any technology can be used.

### 1.8.3. Participants

Participants represent companies, departments, or roles involved in a collaboration. Participants are represented as swimlanes (pools) in collaboration, process diagrams, and square nodes in conversation diagrams (Section 1.8.5).

### 1.8.4. Events

An Event is something that happens during the course of a Process. Events affect the flow of the Process, usually have some cause or impact, and may require or allow for a reaction. The term *event* is general enough to cover many things in a Process: the start of an Activity, the end of an Activity, the change of state of a document, and a Message that arrives. These all could be considered Events. There are three main types of Events:

- *Start Events*, which indicate where a Process will start. Thus, it will not have any incoming Sequence Flows—no Sequence Flow can connect to a Start Event (Figure 1.8).
- *End Events*, which indicate where a path of a Process will end. In terms of Sequence Flows, the End Event ends the flow of the Process and, thus, will not have any outgoing Sequence Flows—no Sequence Flow can connect from an End Event (Figure 1.8).
- *Intermediate Events* indicate where something happens somewhere between the start and the end of a Process.

Both Start and End events have defined marks representing more specified events, e.g., a Message arrives from a Participant and triggers the start/end of the Process. The last mark in Figure 1.8 means multiple triggers are required before the Process can be instantiated – multiple Events.



Figure 1.8: BPMN Events Overview - source: BPMN Specification [45, pp. 83]

### 1.8.5. Other Common Elements

#### Message Flow

An **Association** is used to associate information with Flow Objects. Further, **Sequence Flow** shows the order of Flow Elements in a Process or a Choreography. Sequence Flow has only one source and only one target. The source and target must be from the set of the following Flow Elements: Events (Start, Intermediate, and End) and Activities (Task and Sub-Process; for Processes).

#### Pool

A Pool is an element of the Collaboration and Conversation diagrams. It represents participation in a Collaboration. A Pool may or may not reference a Process. A Pool is the container for the Sequence Flows between Activities (of a contained Process). The interaction between Pools is shown through Message Flows.

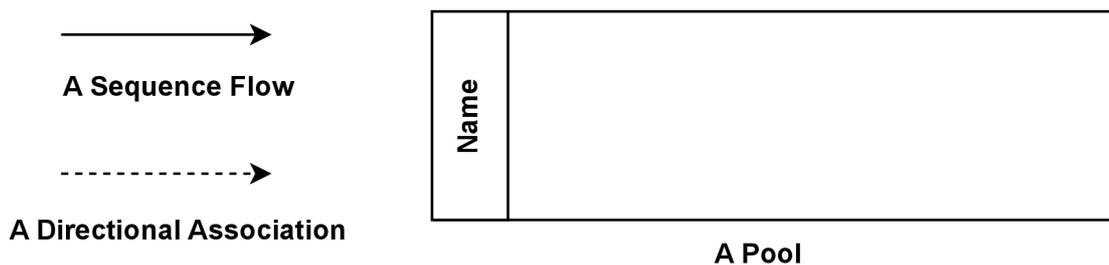


Figure 1.9: BPMN Common Elements Overview - source: BPMN Specification [45]

## 1.9. Return on Security Investment (ROSI)

The Return on Security Investment (ROSI) method is a form of security investment evaluation based on the ROI (Return on Investment) method, one of the most popular forms of investment evaluation in finance. However, the investments in security are not-for-profit. They are supposed to mitigate one or more security risks, which means they are done to prevent losses arising from said risk. The ROSI method aims to do precisely that, compare the potential investment into security against a potential monetary loss from a risk's impact.

### 1.9.1. Methodology

The ROSI method begins with a quantitative risk assessment method focused on the monetary part of the risk. The risk followed by this method is usually more generalized, e.g., loss of productivity or breach of contract.

The quantitative assessment starts by calculating the **Single Loss Expectancy (SLE)**. The Single Loss Expectancy is the expected amount of money lost from a single occurrence of the risk. The ENISA emphasizes the need to account for all affected assets and to include not only direct losses but also think about indirect losses.

It is also crucial to calculate the SLE the same way for all risks because consistency in methodology makes the results of multiple calculations comparable. Otherwise, the SLE could not be used to compare different investments.

The next step after calculating the SLE is estimating the **Annual Rate of Occurrence (ARO)**. The ARO is the probability of the risk happening in a year. The ARO can be inferred from previous experience, rely on an expert's opinion, or be calculated by a statistical method. The organization should always use the most precise method or combine multiple estimates.

The final step of the risk assessment is to calculate the **Annual Loss Expectancy (ALE)**. The ALE is calculated by multiplying the ARO by the SLE. After the risk assessment, the ALE is used in the ROSI calculation. [48, pp. 4]

### 1.9.2. ROSI Calculation

“The ROSI calculation combines the quantitative risk assessment and the cost of implementing security counter measures for this risk.” [48, pp. 5] The general definition based on the ROI would be as follows:

$$ROSI = \frac{\text{Monetary loss reduction} - \text{Cost of the solution}}{\text{Cost of the solution}} \quad (1.2)$$

However, the goal is to take the risk assessment into account. That is achieved by estimating how implementing the countermeasure will lower the ALE, resulting in a percentage called the mitigation ratio. The ROSI would be calculated as follows:

$$ROSI = \frac{ALE * \text{mitigation ratio} - \text{Cost of the solution}}{\text{Cost of the solution}} \quad (1.3)$$

## 2. Current State Analysis

The focus of my thesis is the implementation of case management principles as a means of preserving knowledge capital and allowing more automation in organization processes. The use case I have chosen is CSIRT Teams, mainly the Incident Handling process.

For this thesis, I have chosen a large organization with around 40 000 members. The organization has its own CSIRT team composed of 10 employees, one being the team leader responsible for the team's operation and reporting to the CISO. The rest of the members are specialized workers responsible for incident handling, forensic analysis, and data analysis, with different levels of seniority in each task per person. The organization considers all these workers to be incident handlers. The team always has one worker on incident handling duty for the day. From the ENISA perspective, the worker on duty is assigned the roles of the Duty Officer and the Triage Officer (Section 1.4.1).

In order to further explore the topic of my thesis, it is crucial to understand the current state of the organization in question, its processes, and its information systems. The following diagram (Figure 2.1) marks the beginning of the Current State Analysis chapter and explains the incident resolution process.

The process starts with a ticket arriving at the designated ticket queue, which will be picked up and processed by a worker (handler) of the Incident Handling team. When a new ticket arrives, it is picked up by the worker of the Incident Handling team. The worker first evaluates the constituency, which means the handler decides if the ticket is in the scope of the responsibilities of the CSIRT team. If the ticket is out of scope, the handler will try to forward it to the division responsible for such tickets, and the process ends. Otherwise, the process continues to the triage phase.

**Triage:** The triage phase is focused on the categorization and prioritization of the ticket. Categorizing aims to analyze the incident and determine the attacker's intentions. Based on that, the handler should be able to categorize the incident into one of the predefined categories, which may be based on systems such as the MITRE ATT&CK Matrix. The result of the categorization may be, for example, spear

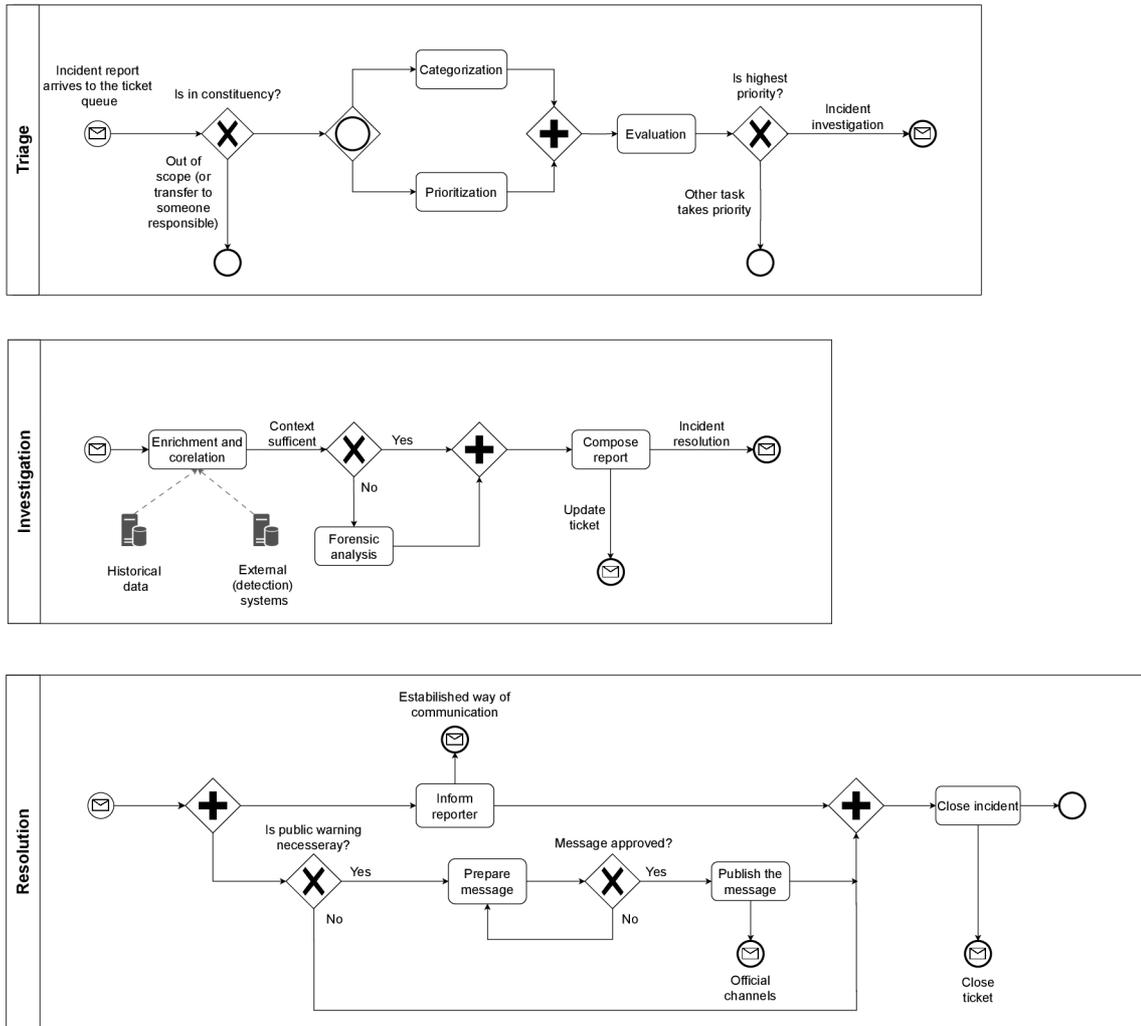


Figure 2.1: Incident Handling process

phishing, email with malware, horizontal/vertical network scan, DDoS attempt, vulnerable device, and more. Parallel to the categorization is prioritization. The point of this step is to approximately analyze the incident’s impact, such as the number of affected users, their standing in the organization, affected assets, and their importance for the organization. When the handler completes these steps, he evaluates the incident and decides if it should be handled immediately or if there is anything else that takes priority.

**Investigation:** If the incident is the highest priority, the process advances to the next step, the Investigation. In this phase, the handler looks for historical data related to the current incident, e.g., detected IP addresses already found in other incidents or phishing emails with similar payloads compared to those currently being

processed. Besides historical data, the handler uses online sources, such as OSINT platforms (platforms for sharing open-source intelligence) and VirusTotal [49], and local sources, such as flow data search, tools to identify users and other internal tools. If the analysis shows a clear picture of the situation with all impacted entities identified, the handler will compose a report, update the ticket, and move to the next phase. In rare cases, the analysis won't be able to conclude the Investigation. The handler will have to escalate the process to forensic analysis. In some cases, this may also be performed by the handler. However, in many cases, such as reverse engineering of malware, specialized workers will complete the forensic analysis. When completed, the results will be passed to the handler, who will compose the report and update the ticket, as mentioned above.

**Resolution:** The last step is called resolution and conforms mainly of informing related parties with details of the Investigation and suggesting possible resolutions. Suppose the incident is identified or expected to be widespread. In that case, the handler prepares a warning message and, when approved by its supervisor, publishes it using a well-known channel to the organization. When all related parties are informed of the results and suggested resolutions, the handler closes the ticket, marking the incident as resolved.

**This process model will serve as a base for a transition from a ticket-based approach to case management.** The goal is to model the case management system and automated processes to fit the regular workflow of an incident handler in the organization. However, this model serves purely as a conceptual overview, and further specified models focusing on certain parts of the process/system will be required.

## 2.1. Information Systems

In Figure 2.2, we can see an overview of information systems that contribute information to incident resolution. Generally, the incident is represented by a ticket in the central information system – Request Tracker for Incident Response (RTIR), a ticketing system developed specifically for the incident handling use case. This

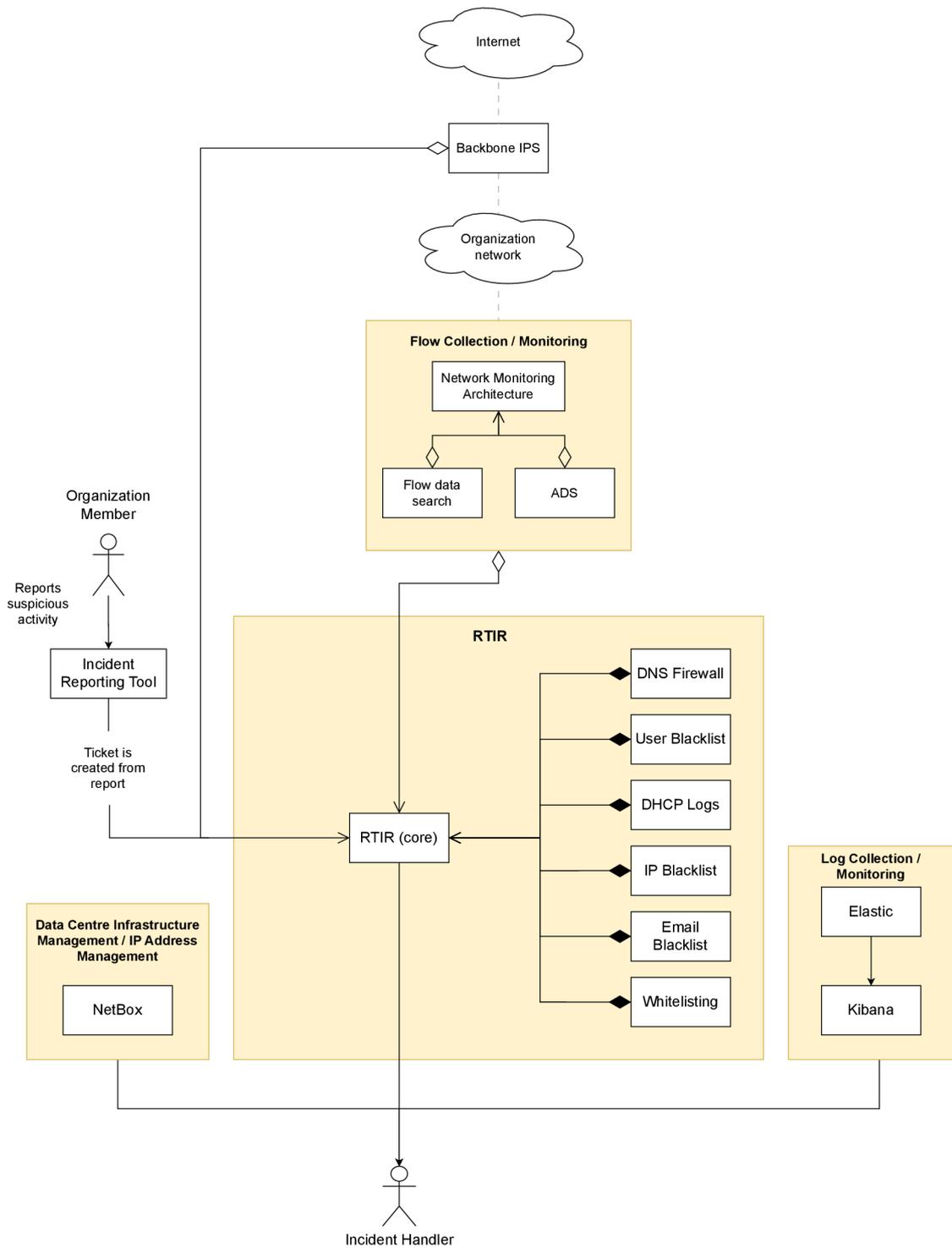


Figure 2.2: Organization’s Information Systems and Tools Related to the RTIR

section will focus on explaining the workings of RTIR, its extensions, information systems interfacing with the RTIR, and others used in the incident resolution process.

### **2.1.1. RTIR**

The first system to be discussed is the mentioned core of the process, the RTIR. In essence, the purpose of the RTIR is to track the incidents (in the form of tickets) and provide a platform where related information can be collected and stored. The tickets are divided into multiple queues, which organize tickets by category and time received. The categories are logical containers for tickets of similar nature, such as automated reports provided by Anomaly Detection Systems (ADS) or Intrusion Prevention Systems (IPS) and user reports.

#### **Tickets**

The tickets are represented as a post with chronological comments (as in forums) with controls to manipulate tickets' lifecycle. The current workflow differentiates three types of comments.

The first represents email communication between the handler and the reporter. The RTIR interface effectively transforms email communication into a forum thread to keep communication about one specific incident in one place.

The second type is a private comment, which represents a way of internal communication specific to an incident. Private comments are used predominantly to add notes to an incident or share information about the incident between multiple handlers who may work on the said incident.

The last type of comment is an activity log; this is a special type of comment as it is auto-generated by the RIRT to keep a log of changes done by handlers, such as "email was sent by handler" or "handler changed the category."

#### **Ticket Lifecycle**

RTIR supports multiple lifecycles, which can be defined at will using visual Lifecycle Workflow Builder [40]. An example of a simple lifecycle can be "created," "assigned," "in progress," "review," and "done," as seen in the following picture.

Lifecycles can be extended by simple automations, such as closing or elevating stale tickets, generating notifications on state changes, and more.



Figure 2.3: Ticket State Lifecycle

## Advanced Automation

The automation capabilities of RTIR can be further extended via extensions, which are plugins that users can develop and add to the RTIR. The extensions are Ruby scripts loaded to the RTIR, giving them access to the RTIR API and installed Ruby libraries. In our case, these scripts allow RTIR to connect to other organizations' systems, allowing the handler to look up information about organization members, query DHCP logs, and whitelist/blacklist IP addresses, emails, and domains.

## Information Systems Connected to the RTIR

As mentioned, the extensions allow the RTIR to be integrated with other information systems the organization may use in the incident handling process. In our case, these integrations are used for incident creation. In the organization, new incidents can be created in two ways: invoked by detection systems or reported by users.

The first happens when an automated tool detects or blocks abnormal behavior on the organization's network or in an information system. That may be IPS blocking DDoS or SSH attack, ADS detecting port scanning, or suspicious email detection. Based on the detection source, a record of the event is created in the corresponding (automatic) queue in the RTIR.

User reports are a manual analogy of the detections. Members of the organization can use a web-based form to submit a report of a suspected incident. This report is then submitted to the designated (general) RTIR queue.

### 2.1.2. Network Monitoring

This section will be focused on information systems related to network security, monitoring, blocking, and reporting.

Many systems in this section (and the following sections) were mentioned before, as there is no clear way to categorize them without introducing arbitrary rules. Instead, the sections will focus on the systems from different perspectives based on their responsibility in relation to the chapter's topic. For example, the ADS's responsibility in relation to the RTIR may be reporting anomalies to the incident handling team in the form of tickets. However, in relation to network security, the ADS may focus more on the anomaly detection process, not just the reporting.

#### **Flowmon**

The organization uses various Flowmon products/systems to monitor its network. The core is network flow monitoring via a combination of so-called exporters and collectors.

The *exporter*, also called a probe, is a tool used to collect and export flow data, such as NetFlow or IPFIX. Exporter allows visibility to the L2-L4 network traffic, with extensions up to L7. That means records of network communication composed of IP addresses, protocols, statistics about network quality, traffic decapsulation, in some cases, even URLs, hostnames, and other information specific to the protocol [50].

The *collector* is a standalone solution for the collection and long-term storage of flow data. It allows measuring multiple metrics, custom dashboards, and analytics, including drill-down to/querying individual flows. These advanced analysis capabilities make the collector one of the frequently used tools in network forensic analysis [51].

#### **CESNET**

The organization is part of the CESNET (Czech Education and Scientific Network) association. Membership in the association offers the organization many ben-

efits, including cybersecurity services. The CESNET offers IPS protection against DDoS and other widespread network attacks.

These services, offered to the organization by an As-A-Service model, are mostly out of the organization's control and mainly report their actions to the RTIR.

### **2.1.3. Logs**

The organization supports the ELK Stack (Elastic, Logstash, Kibana) [52] to store and query logs collected from the most important services used within the organization, such as the primary information system used by members of the organization, monitoring infrastructure, email server logs, and to some extent Windows station logs.

### **2.1.4. Data Centre Infrastructure Management / IP Address Management**

The organization uses NetBox, a tool for DCIM (Data Centre Infrastructure Management) and IP Address management. NetBox allows handlers to gather more details about IP addresses from the organization's network. The information may be device-specific or subnet-specific, such as name, location, and designation. If the IP address is assigned to the end user, it can be used for personal identification.

### **2.1.5. Incident Reporting Form**

The incident reporting tool is a simple solution that reports user-suspected malicious activity to the RTIR. It is realized by a web form on the company website where users can describe the problem and add attachments. The form is then submitted to the RTIR as an email, resulting in ticket creation.

## **2.2. Critique of the Current Approach**

The strengths of the current approach are significant. It allows the organization to have one central point where all information related to a case can be gathered

and stored. It allows for prioritizing and categorizing incoming requests (tickets) with its queue approach. It is also, to some extent, able to serve as a communication channel with the reporter. However, all information is stored plainly as static text with no context or meaning to the system itself. That means there is limited or no ability to extract knowledge from previous incidents and identify users across multiple incidents. The problems will be described more thoroughly in the following sections.

### **2.2.1. Unstructured Data and Automation**

The tickets/incidents are composed of comments that are blocks of text without any structure or relationships between them, except time of creation. That means there is no direct way to distinguish what tickets were created by autonomous systems or what caused the reaction from the autonomous system. This lack of structure makes the tickets (and comments) more challenging to comprehend for handlers. From their perspective, it is a long textual conversation between them, automated systems, and the RIRT. This is presented without structure, and the autonomous flow is not under the handlers' control.

The problem that arises from this situation is amplified even more by the fact that multiple automated systems are reacting to the handler's and each other's actions. The result is a log of messages, multiple pages long, virtually incomprehensible on the first read or for new workers who are not well experienced with the system.

Similar issues emerge on the technical side, precisely with automation and integration of other systems. Since there is no way to distinguish the purpose or source of the comments except for embedding some identifier directly into the text, the automation part is severely limited. It results in unnecessary logic in the components and the build of a considerable amount of technical debt.

Even with identifiers for the automated systems and visual clues for the users built-in, the ticket lacks structure which could emphasize dependency, decision-making, and logical sequences of actions. That sort of visualization or visual sepa-

ration is not feasible to implement with a system whose interface is based on plain text sequences.

The last significant downside of this solution is the complex, almost unrealistic correlation analysis with previous incidents. That sort of analysis would require the data to be structured in some standardized format and stored in a database in a way that would make them indexable and queryable.

A side effect is also the lack of documentation/knowledge preservation. The process is documented mainly by the handlers and, to some extent, automated tools in the central information system, the RTIR. However, the documentation is highly dependent on the wilfulness of the worker. That results in a chronic lack of concise information or complex context, which may be seen as a worker's fault. However, it is only a symptom of a sub-par information system and a lack of knowledge management orientation.

### **2.2.2. Knowledge Management**

As hinted in the previous chapter, the lack of concise information/documentation of the handler's steps when solving the incident shows a systematic lack of focus on knowledge management. This makes it hard for another handler to pick up a ticket after another worker or quickly find a related already solved ticket so that the handler can apply a solution from the previous ticket. The lack of a knowledge management-oriented approach is inherently tied to the problems in automation and correlation analysis because knowledge management promotes structured data that can translate logical decisions and thinking processes from one worker to another [53].

## **2.3. Conclusion**

The analyzed organization is well equipped with complex tools and methods to automate regular tasks in the incident handling process. However, the ticketing information system its using is not suited for the task at this scale. The system has aged to the point that replacing it with a modern one focused on knowledge

management and automation would bring the organization significant benefits in reduced workload, automation of frequent routine tasks, ability to correlate new information with historical data, and exchange gained knowledge using standardized structured formats.

## 3. Solution

The proposed solution to the described problems in the current state analysis is to replace the ticketing information system with a system more focused on preserving knowledge and using said knowledge by supporting the work of incident handlers and allowing advanced automation. That will be realized by using case management principles when designing the replacement information system. This chapter will discuss how the identified processes/workflows can be translated into a case-management-oriented information system.

The goal of the solution I am presenting is to empower incident handlers' work using tailored user interfaces, leveraging the potential to automate repetitive steps in the workflows, recognize and extract information from initially available data and enrich the information using well-known sources.

### 3.1. Restructurization of Support Systems

Several categories of information systems/services will be interfacing with the proposed case management system. The following sections will use these categories in BPMN diagrams as a cogwheel symbol, with a number specifying the group. This section will serve as an overview of the grouped systems.

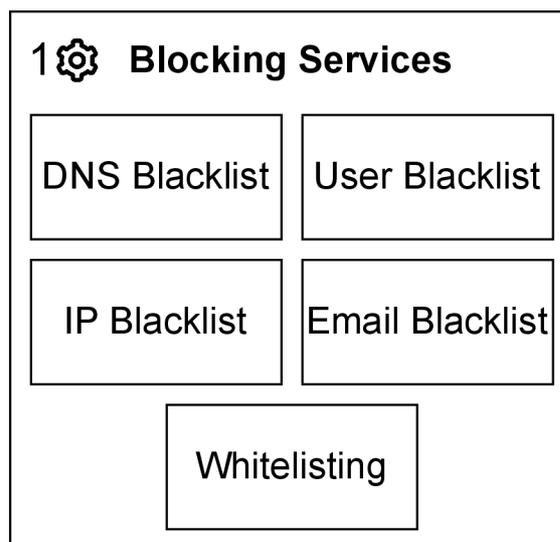


Figure 3.1: Blocking Services

The first group the case management system will interface with is *Blocking Services* (Figure 3.1). Its purpose is to block, unblock or whitelist IP addresses, DNS records, email addresses, and user accounts. Restrictions can be made on the organization's perimeter for external threats. In the case of internal origin, more aggressive restrictions can be made to isolate potentially compromised server/application from the organization's network. Whitelists are used to protect a bannable entity, such as an IP address, against blacklisting.

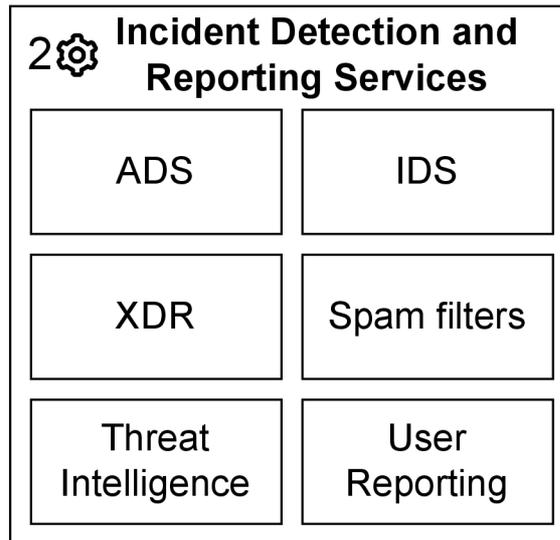


Figure 3.2: Incident Detection and Reporting Services

The second group is called *Incident Detection and Reporting Services* (Figure 3.2), which contains mainly services already described in the Current State Analysis section, with an extension of XDR, an endpoint detection system the organization will implement to increase the fidelity of malware/phishing recognition and protection.

The third group is called *Observable Detection and Correlation*. It comprises three new services used primarily by the case management system as a storage and search/correlation platform for the observables (Figure 3.3).

The fourth and last group is called *Enrichment and Incident Resolution Tools* (Figure 3.4). It consists of internal tools that allow automated forensic analysis (historical data and logs) and user recognition (identity management). Two types of third-party tools, the first for observable enrichment, mainly composed of threat

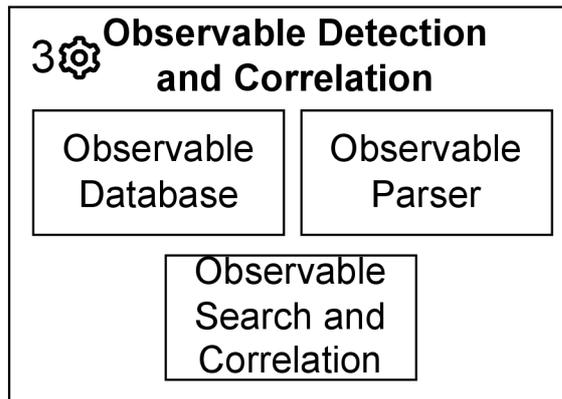


Figure 3.3: Observable Detection and Correlation Services

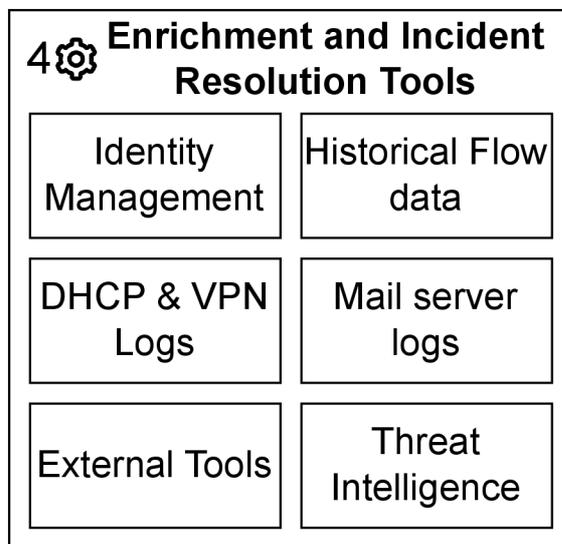


Figure 3.4: Enrichment and Incident Resolution Tools

sharing and threat intelligence platforms, and the second for risk assessment of observables such as VirusTotal [49] and Google Safe Browsing [54].

## 3.2. Case Management

In this section, we will propose a design for the case management system. The design will focus on generic incident cases with an emphasis on extensibility and customizability. Moreover, a demonstration of a spearphishing prototype will follow in Section 3.3.

The following diagrams show how the previously described ticket-based incident handling process can be transformed into modernized case-management-centered processes focusing on automatization and knowledge preservation.

### 3.2.1. Case Overview

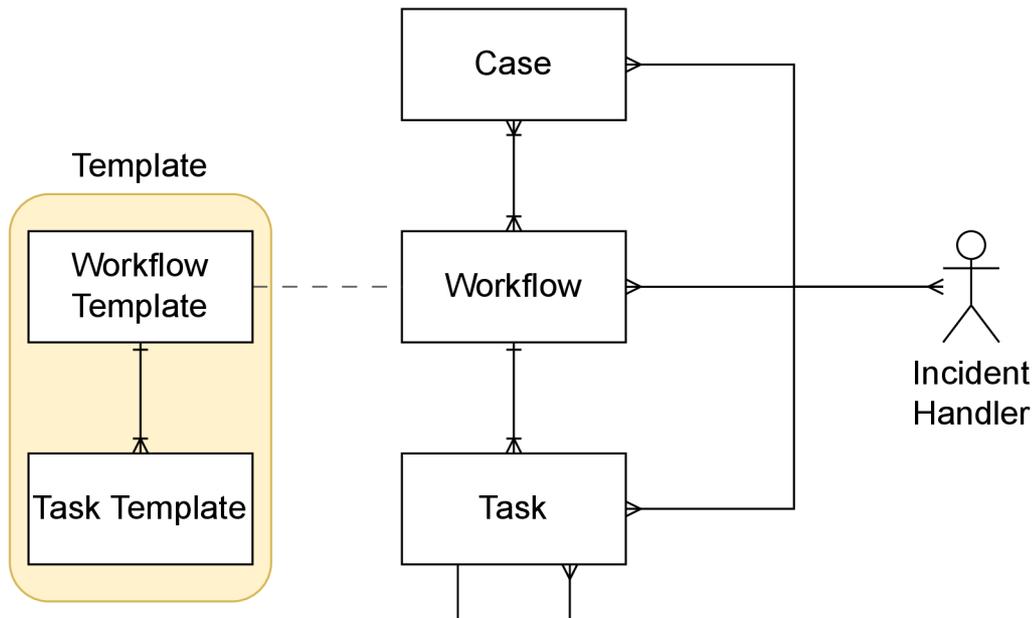


Figure 3.5: Case Overview

The implementation of the case management system in our solution is based on general principles of the case management approach described in Section 1.6. In this implementation, the *case* comprises a name, description, and one or multiple workflows. The *workflow* represents a logical container. Its attributes are a name, a template the workflow is based upon, and a group of tasks with the same primary focus or motivation.

*Tasks* are the smallest organizational units, representing individual decisions or automated steps in the process. A task comprises a name, description, and data payload, for example, a list of suspicious domains. A task may also optionally contain a decision, data input operation, or data modification operation, e.g., select suspicious domains. The final pair of attributes the tasks have are a reference to

the workflow they are part of, their position in the task hierarchy in the form of a parent and children, and user comments.

A unique type of component is the already mentioned *workflow template*. It represents a prepared set of tasks (actions, decisions, data manipulation). These can be used in combination with automated categorization methods to pre-prepare expected case structure, further lowering the amount of non-routine work required by the human expert.

### 3.2.2. Incident Report Automated Processing

The arrival of an incident report to a report queue marks the beginning of the incident handling process. The incident report contains some structured data describing an event that could be considered an incident. The content of the report is as crucial for this step as its structure because if the report contains enough information that can be processed by automated tools using a well-known structure, a large portion of the triage can be automated, as seen in the following diagram.

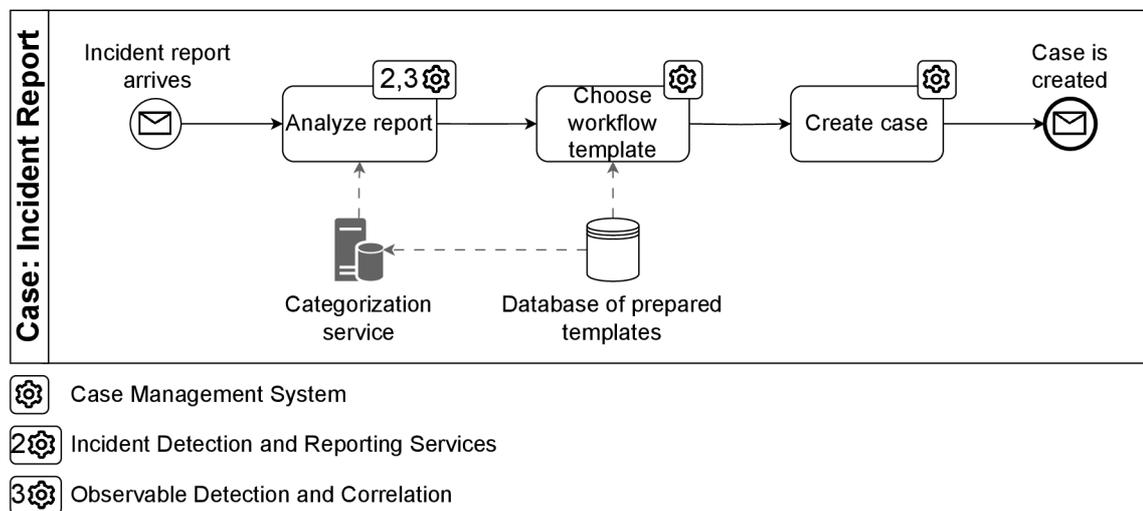


Figure 3.6: Incident Report Processing

In Figure 3.6, we can see the processing of new incoming incident reports, as discussed above. The first part of report processing is focused on categorization, which means selecting one of the prepared case workflow templates, such as automated detection, suspected phishing by mail server filter, user-reported phishing,

and user-reported event. The templates are created by the organization and can be extended or modified, or new templates can be created based on typical use cases. Templates are selected based on a set of rules implemented by the organization via a categorization service; when the template is selected, the case can be created using the template and filled with information from the report. The creation of the case marks the beginning of the *Automated Preliminary Analysis* described in the next step.

### **Disclaimer**

In theory, incident reports can arrive in different forms or/and by multiple channels. However, it would be preferred to unify the channel and the form to keep the automated components simple and sustainable. This issue should ideally be solved before the solution processes the incident report. Because of that, we will assume all reports to follow the same structure and means of delivery.

### **3.2.3. Automated Preliminary Analysis**

This process is responsible for extracting information from the incident report and finding correlated information to the case. This is possible by leveraging the concept of observables for information storage and processing. The following diagram (Figure 3.7 ) explains the preliminary analysis process and how the observables are used to store and process the information.

The first step in the process is to identify all observables in the report data payload. That could be a phishing email in which our focus is primarily on identifying email addresses, URLs, and attached files. Other frequent use cases may include IP address recognition in case of automated attack detection or malware hashing in case of an XDR report of suspected software. The result of this step is a bulk of observables with relationship data describing the context in which they were found.

The next step, enrichment, focuses on using the *Enrichment and Incident Resolution* toolset to find related information from external and internal sources to collect more information about IP addresses, domains, emails, files, and other previously recognized observables. That may result in new observables being created

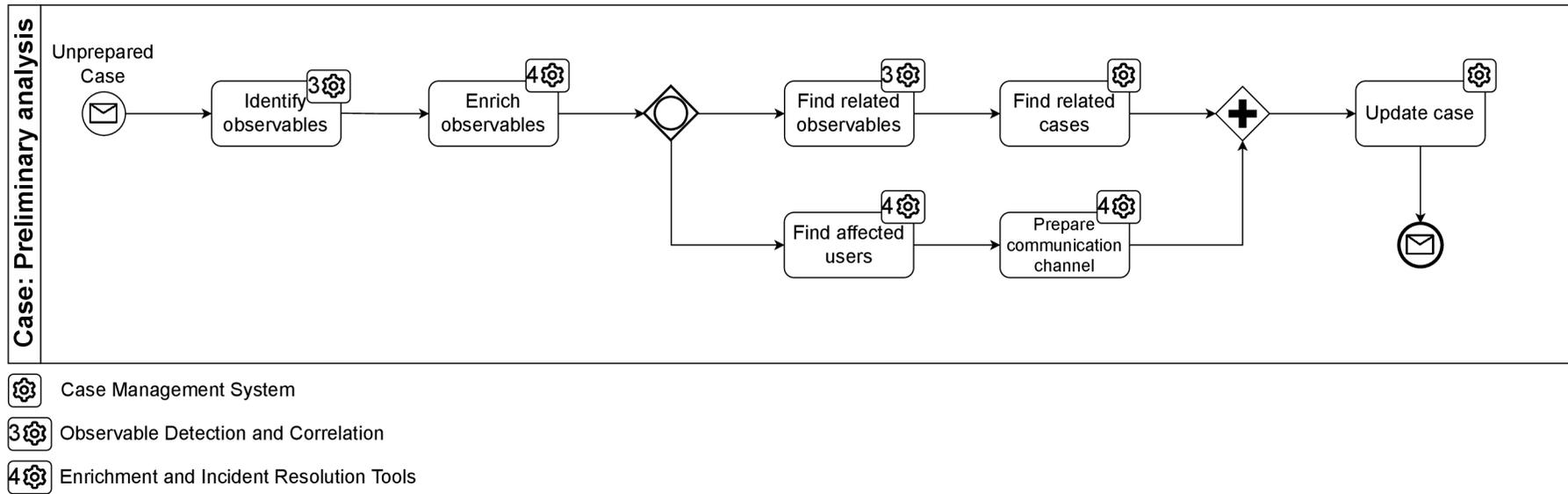


Figure 3.7: Automated Preliminary Analysis Process

or new relationships between existing observables being recognized, such as domain translating to IP address or leading to file download.

The enriched observables are then passed to the next part of the process. This part is composed of two parallel sub-processes.

The first subprocess is devoted to finding related observables and, via them, identifying related cases, which can support the handler's decisions by presenting already resolved similar cases.

The other parallel part of the process is searching for affected users; this is also achieved by using the collected observables, e.g., the user can be identified by their email address, the IP address that it had assigned at the time, or by their VPN connection. When an affected user is identified, a communication channel is prepared.

When both parallel lines of the process are completed, it moves to the final step of this process. In this last step, the case is updated with all the information in the enriched observable bundle detailing relations and means used to enrich said observables. After all available information has been collected and added to the case, the following process focused on automated resolutions can begin.

### **3.2.4. Automated Resolution**

This process uses information collected in the previous process to assess risk and, in combination with previous decisions, static rules, and thresholds, decides if an automated decision, even if just preliminary, is necessary. Figure 3.8 illustrates the process in detail.

The Automated Resolution process starts with a risk assessment of identified observables. The risk assessment is done by combining multiple information sources that may include: previous cases and decisions, reputation databases, malware analyzers and databases.

- **Previous cases and decisions.** For example, if an incident handler marked a domain at a particular time as malicious. This is the most valuable source

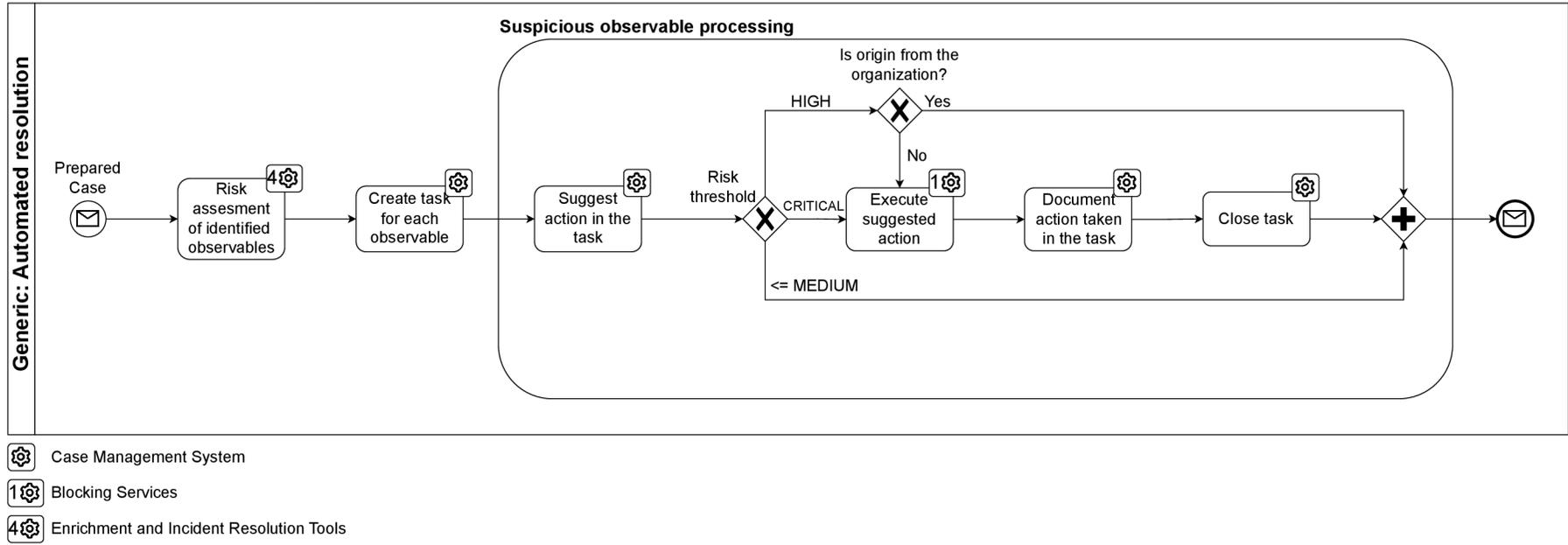


Figure 3.8: Automated Resolution Process

of information because externally acquired information may not be up-to-date and may contain (or miss) specific bias for the information publisher.

- **Reputation databases.** The organization has access to third-party curated reputation databases, which can provide a risk score about IP addresses, domains, and emails. This is a reliable source of information. However, it may not always be up to date and is not always effective against more targeted threats, such as attacks that target only the organization, e.g., a targeted spear-phishing campaign.
- **Malware analyzers and databases.** Services such as VirusTotal [49] allow clients to upload suspected malware samples and receive calculated risk scores and user scores. This is a unique information source because, unlike reputation databases, it does not rely mainly on reports from other users/organizations. The benefit of malware analysis is the availability of anti-virus/anti-malware software, which VirusTotal uses to assess the risk.

In the end, the gathered information is evaluated, and all observables are assigned a risk level.

### **Suspicious Observable Processing**

The following series of steps in the process is called *Suspicious Observable Processing*. The point of this section is to evaluate whether automated action is necessary, e.g., the risk is greater than the impact of false positive detection/blocking. The automated risk assessment process used resembles risk assessment methods used in the risk management as described Section 1.1.4.

The process begins by updating the observable record in the case and creating a task for the observable resolution with an assessed level of potential risk. The record-keeping is essential for post-analysis by the incident handler and for later automated analysis if the case is linked to another one as a related-resolved case.

The next step is to evaluate the assigned risk level and whether it is over a certain threshold. In this case, the organization uses a five-level system, using

the keywords: "CRITICAL," "HIGH," "MEDIUM," "LOW," and "NONE." The generalized meaning of the levels is:

- CRITICAL - The action is highly suggested and automatically executed, even if the identified subject/source is within the organization.
- HIGH - The action is suggested and automatically executed if the origin is outside the organization; otherwise, blocking is suggested as a recommended action to the incident handler.
- MEDIUM - The automated action is not desirable because either the automated detection was not able to achieve a high level of confidence or the risk score acquired from external services was not high enough or conflicted between multiple sources. No matter the origin, blocking and further investigation is suggested to the incident handler.
- LOW - This level suggests a high chance of false positives. Not executing blocking action is recommended, and further investigation is suggested to the incident handler.
- NONE - There is no indication of malice, no automated action is taken, and not recommended. A manual investigation may be needed, but the decision is left to the incident handler.

If an automated action is taken, it is documented in the task, and the task is closed. Automatically resolved tasks are assigned a special flag for the incident handler or reviewer to know what tasks were solved with and without human interaction. Tasks that were left for the handler to decide are left in the open state and will be resolved in the following process.

To conclude, the task has three possible ending states: a solution is suggested and automatically applied, a solution is suggested but requires the handler's confirmation, or a solution is not suggested due to a lack of information.

### 3.2.5. Expert Resolution

The last process in the chain of incident resolution processes is focused on the application of expert skills and knowledge by a specialized worker, the incident handler (Figure 3.9).

The process starts when all automated jobs are finished, potential victims are identified, and the only non-resolved tasks are those waiting for human intervention. **In contrast to the ticketing approach, most task decisions are either executed or have suggested courses of action based on the analysis done in previous steps.**

The incident handler begins working on the case when it is assigned to them by the supervisor or is self-assigned. The handler first needs to review the case and assess the completeness of the identified observables, evaluate the detections, and confirm that all potential victims were identified. To support the review and validation, the handler references other cases that include similar/the same observables or have other shared links.

After the handler reviews all the available information to the case, he/she can decide whether a more manual investigation is needed. If that is the case, he/she may obtain more information by other means and correct or extend the information available, either by editing the current information saved in the case or by using the comment section of tasks to provide more context. When the handler obtains the necessary information, the process can continue by reviewing the automated decisions and suggestions. At this point, the handler can override any automated decision and document its action in the case.

When the handler finishes the review process, he/she can move to the next step, the tasks that require human interaction. Generally, the handler will encounter two types of tasks needing input. The first are tasks with a risk assessment below a threshold that would justify automated action. These require the handler to assess the situation using external sources or expert knowledge to decide whether the action suggested in the task should be executed. The handler can decide on its action and optionally explain his/her decisions in the task's comment section. The other group of tasks consists of tasks identifying potential victims. The handler can use

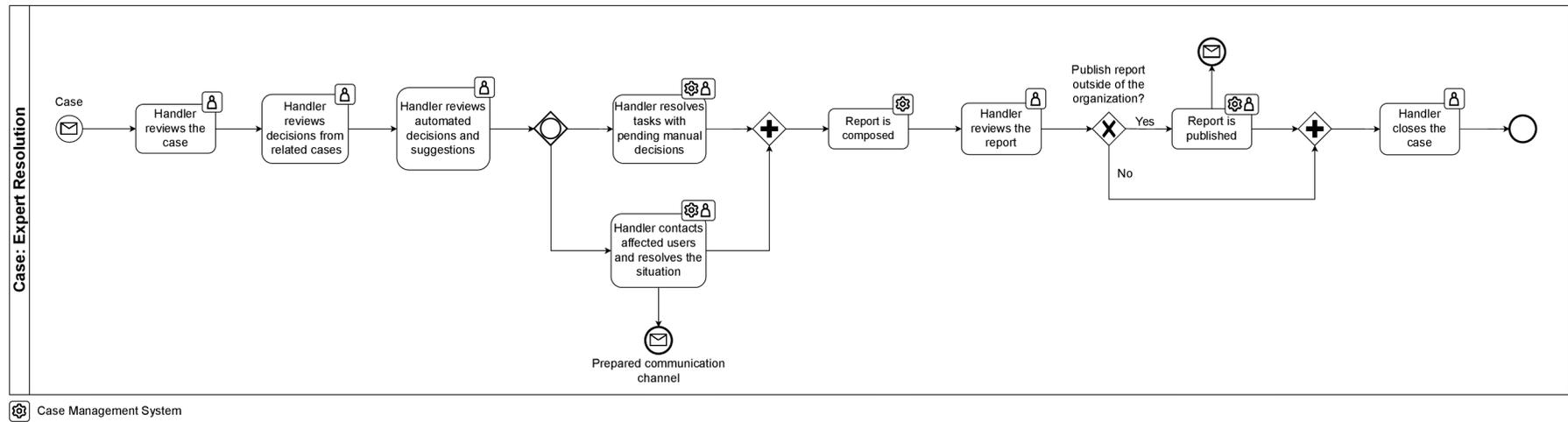


Figure 3.9: Expert Resolution Process

prepared communication channels to contact the victim with suggested resolution, ask questions or recommend further actions. Their conversation is linked to the task and archived.

When all tasks are resolved, the case moves to the last part of the process, reporting and lessons learned. The report is automatically composed of the identified information and includes all actions taken by the automated systems and the incident handler. The report can be modified before publishing. For example, to hide sensitive information or include information not included in the case decision-making process. When the handler validates and adjusts the report, it is saved to the organization database and may be published to external sources.

With all tasks finished, the handler closes the case. All information stored in the case, especially the decisions made by the handler, is essential for future cases as the system can learn from the handler's actions when it encounters similar or the same observable. The learning also happens more indirectly because handlers can review the steps of other team members who worked on similar cases in the past. The team uses this fact in two ways. The first is to share new or unique types of cases between the team members so that everyone is always up to date with new incoming threats and methods attackers use. The second use case is to support and assist the handler's decision when encountering a similar case to one already solved. This option is useful when the team integrates new members or trains juniors.

### **3.3. Phishing Use-Case Demonstration of Case Management Assisted Incident Resolution**

This section presents a high-level overview of a case-management-based incident-handling system prototype. The system focuses highly on automation and streamlining processes in the incident-handling process.

The prototype is limited in terms of general-purpose capabilities because this project was developed as a solution capable of phishing analysis and Common Platform Enumeration (CPE) matching. That results in minor differences between the proposed generalized solution tailored to handle any incident described in previous

sections. However, the working principles and concepts are closely similar to the proposed solution. The minor differences only show the importance of the organization's input when transforming processes based on older solutions to heavily automated solutions such as this prototype. Nevertheless, the infrastructure in which the prototype is deployed closely resembles the organization's infrastructure, and the tools integrated into the prototype are the same or have a very similar interface to the organization's production toolset.

The prototype is the result of the research project lead by RNDr. Daniel To-vařňák, Ph.D. and realized by Masaryk's University Institute of Computer Science Cybersecurity and Data Management Division. I was involved in designing and developing the solution's architecture, data processing, application interfaces, automation logic, integration logic, automated scenarios (such as the demonstrated phishing scenario), and pilot testing of the solution [55, 56].

The research was supported by the Security Research Programme of the Czech Republic 2015-2022 (BV III/1 – VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20202022164 – Advanced Security Orchestration and Intelligent Threat Management (ORION).

This section's primary focus is to provide a managerial overview of a functional prototype and demonstrate this approach's advantages. The demonstration focuses on the user interface and is divided into two parts. First is an overview of the case-management system to explain common concepts and workings of the system. The second part is a use-case description. The example will follow a user story of an incident handling a phishing case from the perspective of an incident handler.

### **3.3.1. Conceptual Overview**

This section will explain the most common application components, views, and operations or actions the user will encounter.

#### **General Overview**

The first view the user will encounter is the Dashboard view (Figure 3.10). It consists of three main components. The first component contains statistical data

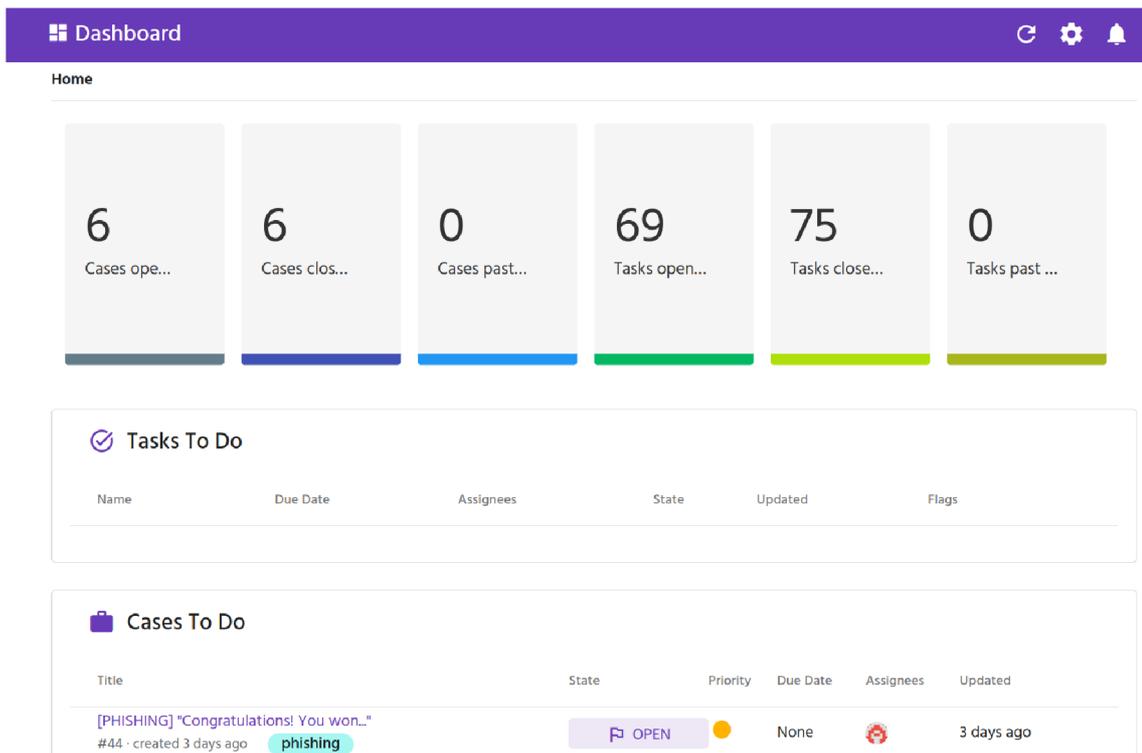


Figure 3.10: Dashboard View

about this week’s workload in the form of incidents and tasks. It gives the user an estimate of work that must be done and which was done this week. The second and third components are similar in function, containing tasks/cases ”To Do,” which in this context means tasks and cases assigned to the user. The user may interact with any items on the ”To Do” list, bringing him directly to the case/task in question.

## Case

The main view for a case is the case overview, which consists of a description, linked cases, workflows, files, and assigned tasks (Figure 3.11). Other views are represented as a tab navigation bar below the name of the case and will be explained in separate sections.

The overview section begins with the description, which contains all information extracted from the report sample by preliminary analysis, such as threat type, time of the sighting, time of analysis, results of different analytic methods, preliminary estimate, and raw threat indicator.



The preliminary analysis is executed before case creation, and while its results are presented as human-readable data, they are stored in a specialized format called *threat indicator*. This format is used as a unified input for most of the automated components the system interacts with and for unified data storage/exchange. The goal is to present the information in the threat indicator to the user in an approachable form (the case management user interface) while keeping all the information as a bundle of structured data, which makes them easy to use by automated tools.

Apart from the description, the preliminary analysis also identifies cases potentially related to the current case, presented in the "Linked Cases" component. The last element using data from the preliminary analysis is the "Files" component, which contains any files found in the report sample, such as email attachments.

The last two components in this view are "Your tasks" and the comment section. The "Your task" component is the same as seen in the "Dashboard" view. The comment section presents means of adding information to the case by the incident handler and means of sharing information between the handler or other involved parties with access to the system.

Username	Name	Email
<a href="#">pořiz</a>	Pořiz Osolsobě	p.osolsobe.13@organization.org
<a href="#">předbor</a>	Předbor Ontovéděl	p.ontovedel.52@organization.org
<a href="#">břetislav</a>	Břetislav Prokop	b.prokop.47@organization.org
<a href="#">alfons</a>	Alfons Drahoukoupil	a.drahoukoupil.4@organization.org

Figure 3.12: Case: Users Tab

## Users

This tab of the case view contains a list of related users (Figure 3.12). These users were identified in a preliminary analysis based on the IP address found in the report sample. The user sees their identifier (username in the organization), real name, and contact information. Users can be further inspected. The system can show flows, cases, and tasks the users appeared in, as seen in Figure 3.13.

Username	Framed Address	NameEmailFrom	To	Data
▼ Pořiz	10.14.43	19 Mar 2019 11:00	19 Mar 2019 18:00	id: 9 userId: fa4d789e-afde-4687-be6b-b6d580749474 acctstoptimemilliseconds: 1553014800000
▼ Pořiz	10.14.43	20 Mar 2019 08:00	20 Mar 2019 15:30	id: 10 userId: fa4d789e-afde-4687-be6b-b6d580749474 acctstoptimemilliseconds: 1553092200000

Figure 3.13: User Accounting View

## Observables

This tab of the case view contains a list of observables that appeared in the case (Figure 3.14). Similarly to the "Users" tab, the user can inspect the observables, which gives them a brief description of the observable, CTIs (references to threat intelligence), related cases, and tasks.

The screenshot shows the 'Case Detail' view for Case #44, titled '[PHISHING] "Congratulations! You won..."'. The 'Observables' tab is selected, displaying a table of related observables. The table has two columns: 'Observable' and 'Type'. The observables listed are:

Observable	Type
✉ Congratulations! You won a lot of money! Email Message #73	Email Message
📄 podvodna priloha.pdf File Reference #7	File Reference
🌐 http://amazon.com Url #4	Url
🌐 amazon.com Domain Name #1	Domain Name
🌐 https://birdsarentreal.com/ Url #6	Url
🌐 birdsarentreal.com Domain Name #3	Domain Name
📧 sender@seznam.cz Email Address #49	Email Address

Figure 3.14: Case: Observables Tab

## Assets

This tab of the case view contains a list of assets in the case (Figure 3.15). In the case of this demonstration, the only assets available are IP addresses.

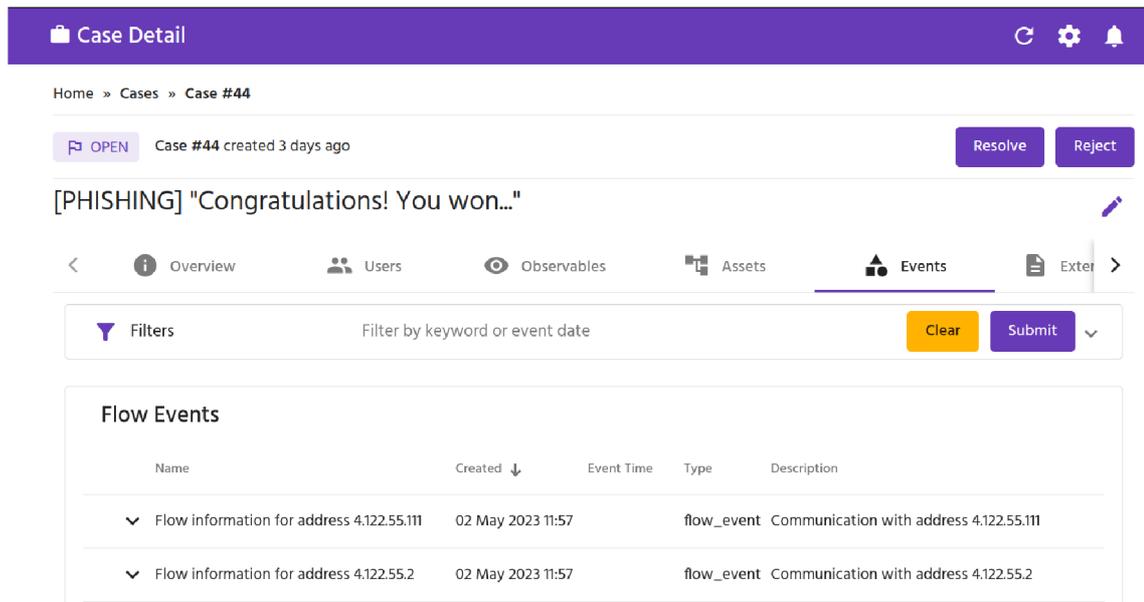
The screenshot shows the 'Case Detail' view for Case #44, titled '[PHISHING] "Congratulations! You won..."'. The 'Assets' tab is selected, displaying a table of impacted assets. Above the table is a filter section with a dropdown menu set to 'Filters', a 'Filter by type' input, and 'Clear' and 'Submit' buttons. The table has three columns: 'Asset', 'Updated', and 'Type'. The assets listed are:

Asset	Updated	Type
🌐 10.1.33/32 Ip Address #68 · created 2 months ago	2 months ago	Ip Address
🌐 10.1.42/32 Ip Address #70 · created 2 months ago	2 months ago	Ip Address
🌐 10.1.43/32 Ip Address #71 · created 2 months ago	2 months ago	Ip Address

Figure 3.15: Case: Assets Tab

## Events

This tab contains a list of detected events related to the case (Figure 3.16). Currently, the only type of events are flow events, such as communication with an IP address.



The screenshot shows the 'Case Detail' page for 'Case #44'. The breadcrumb trail is 'Home » Cases » Case #44'. The case status is 'OPEN' and it was created 3 days ago. There are 'Resolve' and 'Reject' buttons. The case title is '[PHISHING] "Congratulations! You won..."'. The navigation menu includes 'Overview', 'Users', 'Observables', 'Assets', 'Events' (selected), and 'External'. A filter bar is present with a 'Filters' dropdown, a search input 'Filter by keyword or event date', and 'Clear' and 'Submit' buttons. The 'Flow Events' table is displayed below.

Name	Created ↓	Event Time	Type	Description
✓ Flow information for address 4.122.55.111	02 May 2023 11:57		flow_event	Communication with address 4.122.55.111
✓ Flow information for address 4.122.55.2	02 May 2023 11:57		flow_event	Communication with address 4.122.55.2

Figure 3.16: Case: Events Tab

## External References

This tab contains a list of references to external systems, such as the external communication channel (Figure 3.17).

## TTPs

This tab contains a list of identified TTPs in the incident (Figure 3.18). TTP stands for Tactics, Techniques, and Procedures. It describes the behavior of an actor in a hierarchical structure. The tactic is the highest level behavior, such as phishing. The techniques give more detail about the tactic, such as Phishing for Information, Spearphishing Link, or Spearphishing Attachments. The procedures are the lowest level, most detailed descriptions in the context of a technique [57, 58].

Case Detail

Home » Cases » Case #44

OPEN Case #44 created 3 days ago Resolve Reject

[PHISHING] "Congratulations! You won..."

Users Observables Assets Events External References

Filters Filter by url, date or category Clear Submit

**External References**

Reference	Category	Platform	Created ↓
<a href="https://orion-mattermost.svc.csirt.muni.cz/CS...">https://orion-mattermost.svc.csirt.muni.cz/CS...</a> #84 · created 3 days ago	Conversation	Mattermost	May 2, 2023

Items per page: 10 Total: 1

Figure 3.17: Case: External References Tab

Case Detail

Home » Cases » Case #44

OPEN Case #44 created 3 days ago Resolve Reject

[PHISHING] "Congratulations! You won..."

Observables Assets Events External References TTPs

Filters Filter by type Clear Submit

**TTPs**

Name	Type
<a href="#">Phishing for Information: Spearphishing Link</a> Technique #5719 · created 2 months ago	Technique
<a href="#">Phishing for Information: Spearphishing Attac...</a> Technique #5718 · created 2 months ago	Technique
<a href="#">Phishing: Spearphishing Link</a> Technique #5575 · created 2 months ago	Technique
<a href="#">Phishing: Spearphishing Attachment</a> Technique #5574 · created 2 months ago	Technique
<a href="#">Phishing</a> Technique #162 · created 2 months ago	Technique

Figure 3.18: Case: TTPs Tab

## Workflow

Workflows are organization units intended to contain a whole job/work unit, for example, a phishing incident resolution (Figure 3.19). The workflow can contain multiple stages, which are composed of tasks.

**Workflow Detail** Refresh Settings Notifications

Home » Cases » Case #44 » Workflow #44

IN PROGRESS Workflow #44 created 3 days ago Reject Export To Template

### General phishing workflow

Overview Users Observables Assets Events External

**Description**

**Stages** 3 0% done Add

Name	Due Date	Assignees	State	Updated
Analysis Phase #130 · created 3 days ago	None	None	<span>IN PROGRESS</span>	3 days ago
Mitigation Phase #131 · created 3 days ago	None	None	<span>IN PROGRESS</span>	3 days ago
Revision Phase #132 · created 3 days ago	None	None	<span>PENDING</span>	3 days ago

Figure 3.19: Workflow View

## Stage

**Stage Detail** Refresh Settings Notifications

IN PROGRESS Stage #127 created 3 days ago Reject

### Analysis Phase

Overview Users Observables Assets Events External

**Description**

Analyse machine confirmed phishing

**Tasks of this stage** 8 13% done Add

Name	Due Date	Assignees	State	Updated	Flags
Confirm phishing #506 · created 3 days ago	None	None	<span>OPEN</span>	3 days ago	<span>DECISION</span>
Aggregate malicious domains #507 · created 3 days ago	None	None	<span>PENDING</span>	3 days ago	<span>AGGREGATOR</span>
Persist confirmed phishing #513 · created 3 days ago	None	None	<span>PENDING</span>	3 days ago	<span>AUTOMATED</span> <span>AUTOTRIGGER</span>

Figure 3.20: Stage View

Stages are organization units dividing workflows into smaller sub-parts, usually called *phases*. They are composed of tasks and intended to simplify/visually separate tasks or groups of tasks that depend on each other (Figure 3.20).

Stages are presented to the user in a pre-defined order, but they do not enforce the order themselves. That means a stage can begin before its parent stage or end after its child stage. That is because the stages are intended purely as a visual aid to the user. The rules that define *which* task can begin *when* are defined by the hierarchy of the tasks themselves.

## Task

A task is the smallest unit of work in the solution (Figure 3.21). The general purpose of the task is to input a value, transform input into output, trigger an external task, or make a decision. The solution distinguishes between the following types:

- Base - This task serves as a base for other types of tasks, meaning all tasks have these essential properties:
  - Name - It is the name of the task.
  - Description - The description of the task in the Markdown format.
  - Blocked By - The list of tasks that must be completed before this task.
  - Blocking - The list of tasks that require this task to be completed.
  - Predecessors - The list of tasks directly preceding this task in a logical hierarchy.
  - Successors - The list of tasks that have this task as a direct predecessor.
  - References - The list of tasks that are in some form related to this task.
  - Task Input and Task Output - The task can have an input or/and output representing the user or system input and/or output of some user or system action. The supported values are None, Boolean, Date, Datetime, Domain, Email Address, Email Message, File, File Ref, Hash, Ip, Json, Other, String, and URL.

Figure 3.21: Task View

- Automated - The task is executed by an automated system. It can be either triggered by user interaction or automatically.
- Autotrigger - The task is automatically executed when no task is blocking it. It can only be used in combination with the automated type.
- Decision - The task has a boolean value True/False is added as another task output.

- **Aggregator** - The purpose of this task is to merge output values from child tasks. It can simply merge the values in some format or use more complicated logic to merge, such as to merge only the output of tasks with True logic value.

## Workflow Templates

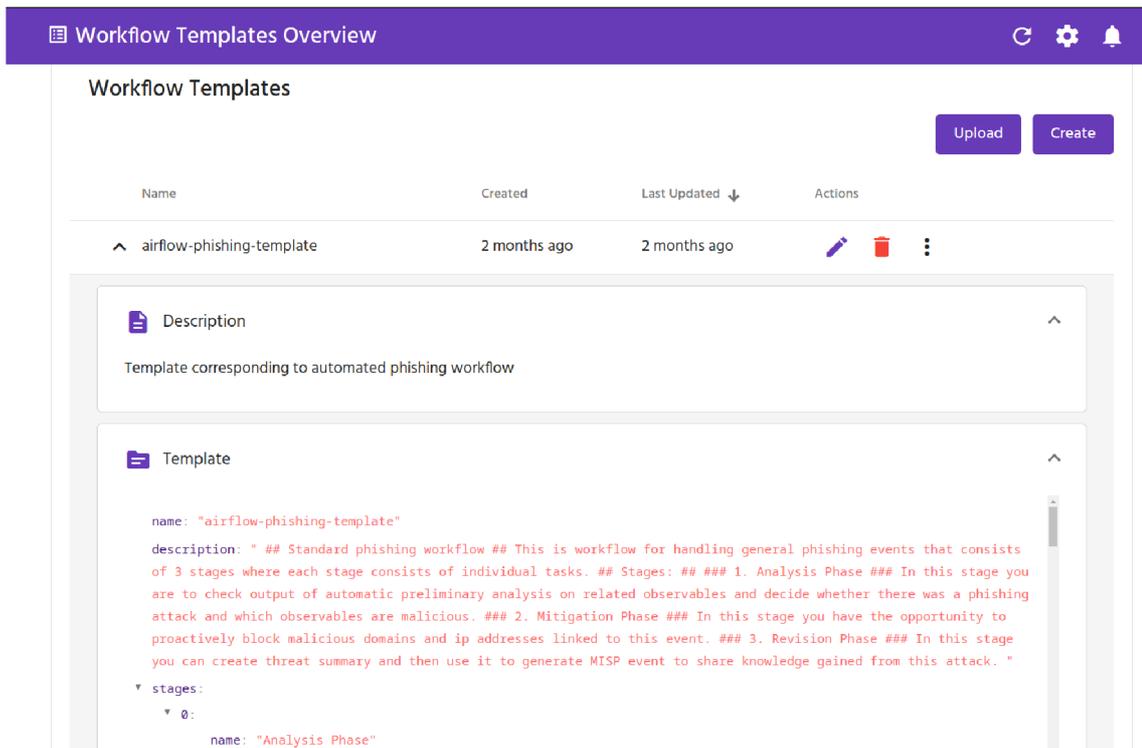
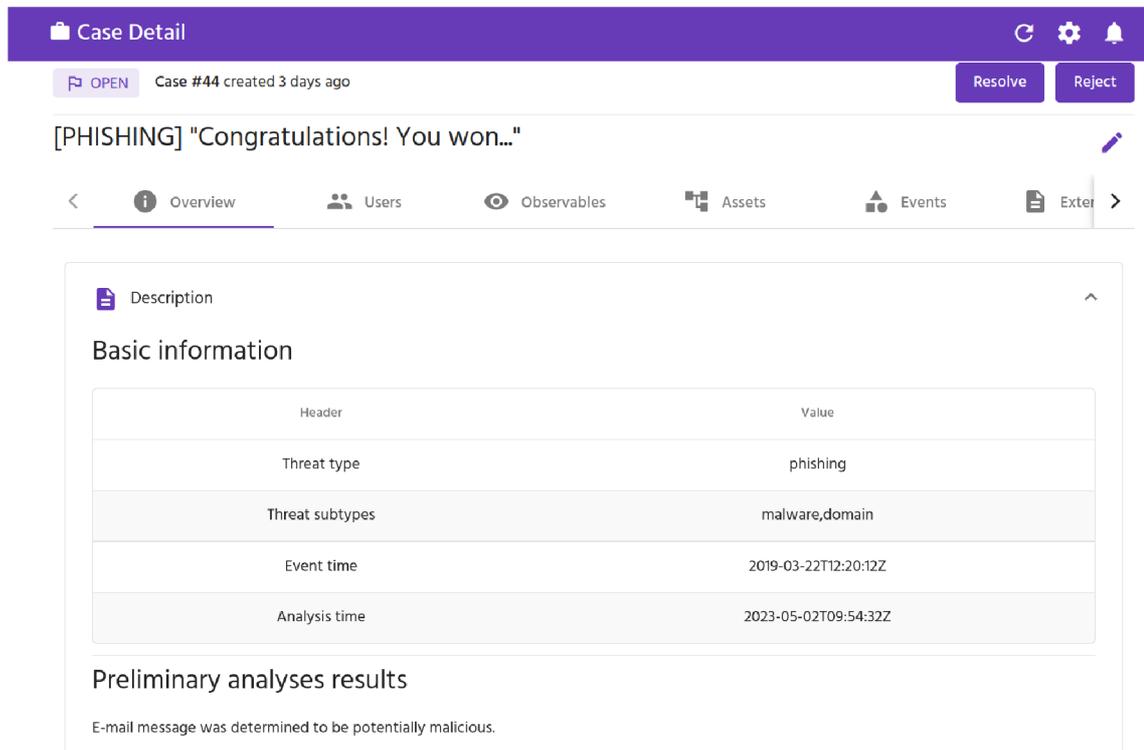


Figure 3.22: Workflow Templates View

Workflow templates are templates describing workflow concerning a specific type of incident. They describe the stages and tasks in a hierarchy. They do not and cannot include tasks, observables, or processed entities created or assigned to the case dynamically in its lifecycle. However, they include all relationships between the "static" tasks, such as the aggregator tasks in the phishing template *Analysis Phase*. The templates can be created manually using the solution's custom format or exported from the existing case (Figure 3.22).

### 3.3.2. The Phishing Incident

This section will follow a spear-phishing incident resolution process from the perspective of an incident handler. The process begins when a new case is created in the system or when a case is assigned to the handler.



The screenshot shows a web interface for a security case. At the top, a purple header bar contains the text "Case Detail" and icons for refresh, settings, and notifications. Below the header, a status bar indicates "Case #44 created 3 days ago" with "OPEN" and "Resolve" buttons, and a "Reject" button. The main content area has a title "[PHISHING] 'Congratulations! You won...'" and a navigation menu with tabs for Overview, Users, Observables, Assets, Events, and External. The "Description" tab is active, showing a "Basic information" table and "Preliminary analyses results".

Header	Value
Threat type	phishing
Threat subtypes	malware,domain
Event time	2019-03-22T12:20:12Z
Analysis time	2023-05-02T09:54:32Z

**Preliminary analyses results**  
E-mail message was determined to be potentially malicious.

Figure 3.23: Phishing Case Overview

The first thing the handler does when working on a new case is review the case description (Figure 3.23). It contains a quick overview of information recognized in the preliminary automated analysis that happened when the incident was reported and before the case was created.

In this incident, the first thing the handler sees is information about the preliminary analysis results. That begins with a table containing information about the suspected threat type, subtype(s), time of detection/event happening, and time of analysis. The analysis result follows the table, telling the handler that the email is suspected to be malicious. The result tells the handler to focus on the domain-s/URLs and attachments found in the email.

Moreover, the results are followed by detailed information about recognized similar emails, observables, and their analysis. The file observable is separated into special section because of its increased significance. The last thing in the case description is the threat indicator.

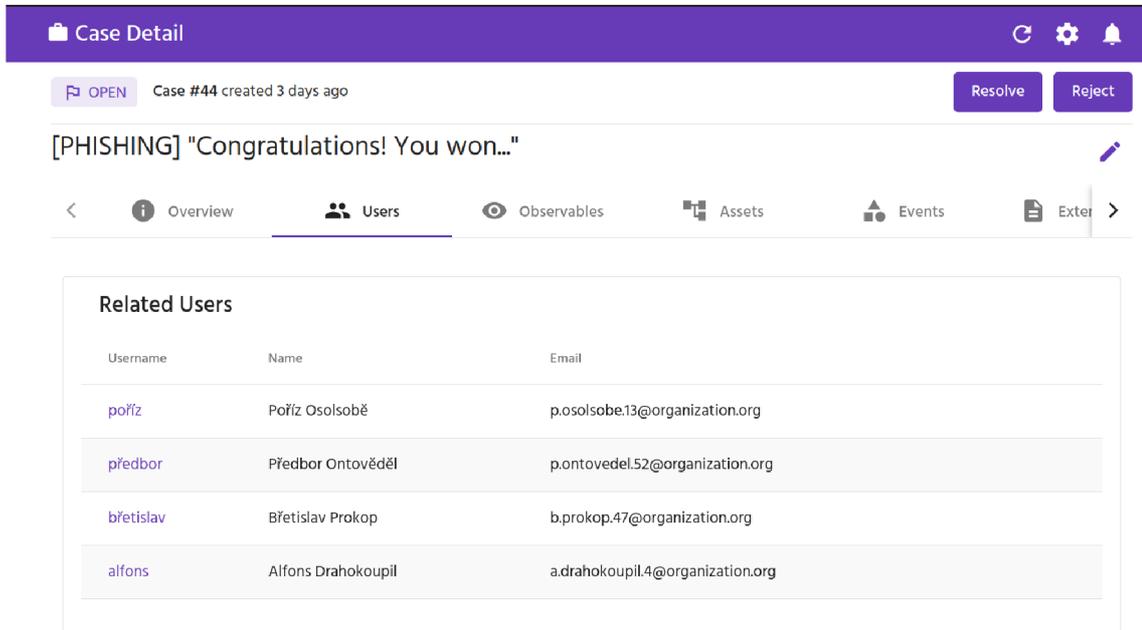


Figure 3.24: Phishing Workflow

Before investigating the workflow, the handler inspects other cards of the case. One of the most important cards is the "Users" card, which contains a list of identified affected users. The fact that the email is targeting only four users in the organization suggests that the handler is most likely dealing with spear-phishing, the targeted variant of phishing (Figure 3.24).

The description is followed by a list of linked cases, workflows, files, assigned tasks, and a comment section. This demonstration will focus on the "General phishing workflow" (Figure 3.25).

The workflow flow begins with an overview screen, similar to the case overview. It contains a general description of the selected workflow template, in this case, the phishing workflow. The picture shows that the workflow is divided into three logical units, stages, that group similar tasks. In this case, the stages represent phases of the incident resolution process, the first being the Analysis Phase.

**Workflow Detail** Refresh Settings Notifications

Home » Cases » Case #44 » Workflow #44

IN PROGRESS Workflow #44 created 3 days ago Reject Export To Template

### General phishing workflow

Overview Users Observables Assets Events External

**Description**

**Stages 3** 0% done Add

Name	Due Date	Assignees	State	Updated
<a href="#">Analysis Phase</a> #130 · created 3 days ago	None	None	<span>IN PROGRESS</span>	3 days ago
<a href="#">Mitigation Phase</a> #131 · created 3 days ago	None	None	<span>IN PROGRESS</span>	3 days ago
<a href="#">Revision Phase</a> #132 · created 3 days ago	None	None	<span>PENDING</span>	3 days ago

Figure 3.25: Phishing Workflow

**Stage Detail** Refresh Settings Notifications

### Analysis Phase

Overview Users Observables Assets Events External

**Description**

**Tasks of this stage 19** 5% done Add

Name	Due Date	Assignees	State	Updated	Flags
<a href="#">Confirm phishing</a> #519 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	<span>DECISION</span>
<a href="#">Aggregate malicious domains</a> #520 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	<span>AGGREGATOR</span>
<a href="#">Aggregate malicious IP addresses</a> #527 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	<span>AGGREGATOR</span>
<a href="#">Aggregate malicious email addresses</a> #528 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	
<a href="#">Aggregate malicious files</a> #529 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	<span>AGGREGATOR</span>
<a href="#">Analyse attachment "podvodna priloha.pdf"</a> #530 · created 5 days ago	None	None	<span>OPEN</span>	2 days ago	<span>DECISION</span>

Figure 3.26: Phishing Workflow: Analysis Phase

The Analysis Phase contains a brief description and a list of tasks the handler must complete. The first task in the phishing flow is the "Confirm Phishing" decision

task (Figure 3.26). This task allows the incident handler to confirm or override the automated preliminary decision. If the handler confirms the email as phishing, he can move to the rest of the tasks in the Analysis Phase.

The rest of the tasks in the Analysis Phase is mainly composed of decision tasks and their aggregators; for example, there is a number of tasks evaluating each flow from/to a malicious IP address with one aggregator combining the results of all decision tasks. The same flow also exists for domains and files. The first exception is task aggregating malicious email addresses because it also contains the decision form. The email address aggregator can be simplified because, at the time, there are no email address evaluation methods in use; the resolution is purely the handler's decision. The second exception is the automatic "Persist confirmed phishing task," which automatically saves the email message sample for similarity analysis when the handler confirms the email is phishing. As described, the handler needs to evaluate and aggregate multiple groups of decisions. In this example, we will focus on the malicious domains example because it is not cluttered with information but allows us to demonstrate the complete flow (Figure 3.27).

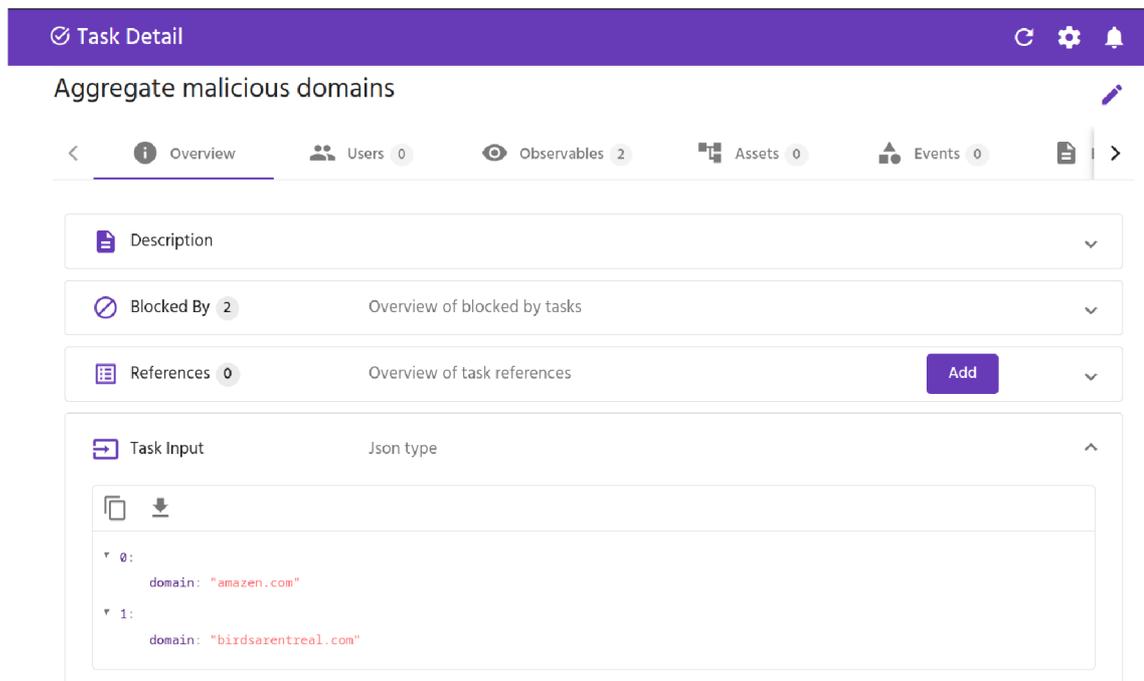


Figure 3.27: Task: Aggregate Malicious Domains

The best way to start the aggregated group of tasks is to open the aggregator task and see which tasks are blocking his completion (data aggregation). In the case of our "Aggregate malicious domains" task, we can see two "Analyse domain abc.xz" decision tasks (Figure 3.28). These tasks represent domains found in the phishing email. The handler can click on the name of any of these tasks to switch to said task.

The screenshot shows a web interface for a task titled "Analyse domain 'birdsarentreal.com'". The interface has a purple header with "Task Detail" and navigation icons. Below the header, there are status indicators: "RESOLVED" (green), "DECISION" (blue), and "Task #533 created 3 days ago". A red button on the right says "DECISION SET TO FALSE". The main content area is titled "Analyse domain 'birdsarentreal.com'" and includes a "Description" section with the following text:

**Confirm/refute result of analysis of domain birdsarentreal.com**

This task will aggregate information about domain birdsarentreal.com to help an analyst to decide whether the domain is malicious or not.

**Automated analyses result**

Observable was marked as **MALICIOUS**.

No automated analyses were done.

**Related URLs**

URL: <https://birdsarentreal.com/>

**Redirect information**

0. <https://birdsarentreal.com/>

**Screenshot**

The screenshot shows the homepage of birdsarentreal.com. The page features a navigation menu with "Home", "Truther Gear", "About Us", and "Contact Us". The main banner image shows a white van with "A MOVEMENT" and "ACTIVISM GEAR" text. Below the banner, there is a section titled "FEATURED ACTIVISM APPAREL" displaying three items: a black hoodie with a white graphic, a black t-shirt with the text "It Flies It Spies", and another black t-shirt with a graphic.

Figure 3.28: Task: Analyse Domain

The first task is evaluating the domain "birdsarentreal.com." From the handler's standpoint, the content of this domain, although suspicious, does not seem malicious. The handler will use the "Resolve To False" button to mark the domain as non-malicious and the task as finished. The handler can use the "Blocking" list of tasks to return to the original aggregator task and proceed to the following domain decision task. The following domain is "amazen.com." The handler evaluates it as malicious because of its content and obvious name similarity to Amazon. Back in the aggregator task, the handler can now use the "Join Outputs and Resolve" button to collect decisions from the decisions task and create an output containing all malicious domains. In our case, this can be seen in the Task Input and Task Output sections (Figure 3.29), wherein the input, we have both the malicious and non-malicious domain, and in the output is only the malicious domain "amazen.com."

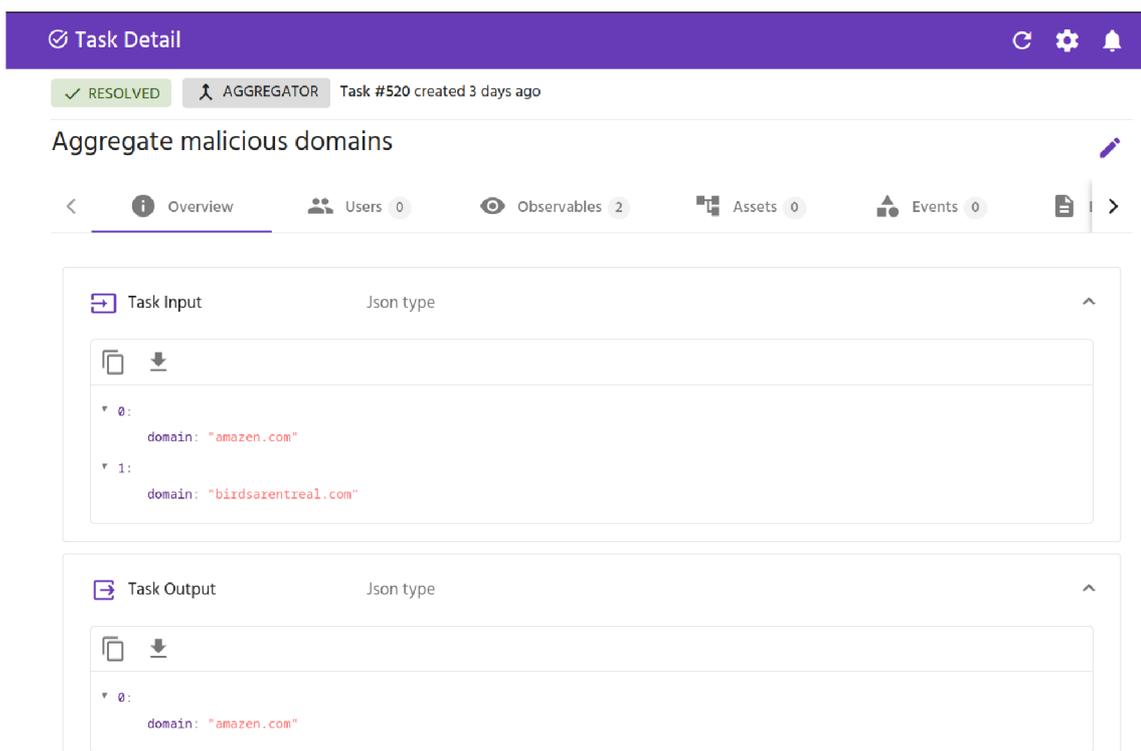


Figure 3.29: Resolved Task: Aggregate Malicious Domains

The completion of one of the aggregator branches in the Analysis Phase resulted in an automated response being triggered. That moves us to the next phase, the Mitigation Phase. In the case of our demonstration, the selected malicious domains

are automatically blacklisted, which is done by the automatic "Blacklist malicious domains" task. In Figure 3.30, the task is marked as Resolved when it receives a successful response from the service doing the blacklisting.

The screenshot shows the 'Stage Detail' interface for 'Mitigation Phase'. At the top, there's a purple header with 'Stage Detail' and navigation icons. Below it, a breadcrumb trail reads 'Home » Cases » Case #44 » Workflow #44 » Stage #131'. A status bar indicates 'IN PROGRESS' and 'Stage #131 created 3 days ago', with a 'Reject' button. The main section is titled 'Mitigation Phase' and includes a navigation menu with 'Overview' (selected), 'Users', 'Observables', 'Assets', 'Events', and 'External'. A 'Description' dropdown is visible. The 'Tasks of this stage' section shows a progress bar at 33% done and an 'Add' button. Below is a table of tasks:

Name	Due Date	Assignees	State	Updated	Flags
Blacklist malicious IP addresses #524 - created 3 days ago	None	None	PENDING	3 days ago	AUTOMATED, AUTOTRIGGER
Blacklist malicious email addresses #525 - created 3 days ago	None	None	PENDING	3 days ago	AUTOMATED, AUTOTRIGGER
Blacklist malicious domains #521 - created 3 days ago	None	None	RESOLVED	20 hours ago	AUTOMATED, AUTOTRIGGER

Figure 3.30: Phishing Workflow: Mitigation Phase

The mitigation phase is automated, and the handler only needs to wait for the automated tasks to finish. When all automated tasks are finished, the workflow moves to the last phase, the Revision Phase.

The point of the Revision Phase is to compose a report of the incident and to share the report if appropriate (Figure 3.31). This phase comprises two tasks. The first is the "Prepare case summary" task, which presents a report about the incident, automated and manual actions in the JSON format. The handler can edit the JSON data using the "Task Output" section/editor. The last task is the "Create MISP event" task. MISP is a threat intel sharing platform that allows multiple organizations/sources to exchange threat intelligence data. The JSON report can be transformed into MISP Event and published if approved.

Stage Detail

Home » Cases » Case #44 » Workflow #44 » Stage #132

PENDING Stage #132 created 3 days ago Reject

### Revision Phase

Overview Users Observables Assets Events External

Description

Tasks of this stage 2 0% done Add

Name	Due Date	Assignees	State	Updated	Flags
Prepare case summary #522 · created 3 days ago	None	None	PENDING	3 days ago	AUTOMATED AUTOTRIGGER
Create MISP event #523 · created 3 days ago	None	None	PENDING	3 days ago	AUTOMATED

Figure 3.31: Phishing Workflow: Revision Phase

With all tasks finished, the handler can return to the case using the right sidebar and use the "Resolve" button to resolve the case, which means closing the case with a successful resolution.

[PHISHING] "Congratulations! You won..."

#38 · created 1 week ago phishing RESOLVED

Figure 3.32: Case: Resolved

### 3.4. Investment Evaluation

The proposed investment presents a considerable technological challenge and monetary cost. This section uses the ROSI method to calculate if the investment is cost-effective. That means if the cost of implementing the solution is smaller than the potential impact of a risk, this solution aims to mitigate. This risk in question is an overloaded incident response team, which in turn means delayed response to incident reports.

We will use the ROSI method to calculate if the investment can efficiently mitigate the risk. The ROSI method begins by estimating the monetary value of the risk using quantitative risk assessment.

The first thing that needs to be calculated is the Single Loss Expectancy. To do that, we first need to estimate the potential impact. For an organization of this scale, the most dangerous result of a cybersecurity attack/incident is the impact on productivity. The organization already has reasonable countermeasures to mitigate the most common incidents. Assuming these countermeasures will be effective, at least to the point of the reduced attack surface, we estimate the potential loss of productivity to be around 10%. The source of the loss can be one targeted attack or multiple less impactful incidents that are not handled in time. Since we are considering a severe impact on the organization's standard procedure, we must consider recovery time. It is safe to expect the complete resolution of the incident to take multiple days and require the cooperation of multiple divisions, not only the CSIRT team. For this calculation, we will estimate an expected recovery time to be one week. That means the productivity will be restored in a week. The investigation is likely to continue afterward. Considering our estimated values, we can calculate the SLE as a 10% productivity loss for one week, which means about 800 impacted employees with an average monthly gross salary in the Czech Republic of around 43 000 CZK. The cost of the lost productivity is about  $43\,000 \text{ (monthly salary)} / 4 \text{ (one week of salary)} * 800 \text{ (the number of employees)} = 8\,600\,000 \text{ CZK}$  [59].

The second step of the quantitative risk assessment is to estimate the Annual Rate of Occurrence. The ARO measures the probability of the risk occurring in a year.

Based on previous experience and the increasing number of incidents, we estimate the ARO to be 3 - 4 times a year. Considering the cybersecurity situation will likely worsen, expecting four significant incidents in a year caused by the risk is the more realistic expectation.

The final step of the risk assessment is to calculate the Annual Loss Expectancy (ALE). That is the monetary loss the organization can expect without implementing the proposed solution. The ALE is calculated as follows:  $ALE = 8\,600\,000 * 4 = 34\,400\,000$  CZK.

Before we can calculate the ROSI, we must estimate the mitigation ratio. The mitigation ratio is a percentage estimation of how the countermeasure will effectively address the risk. In this case, we estimate that implementing the solution will lower the chance of the CSIRT team being overwhelmed by 80%.

With all estimates, we can move to the ROSI method and evaluate the investment. The ROSI method comprises three components, the ALE, mitigation ratio, and solution cost.

To estimate the cost of the solution, we will use lessons learned from developing the prototype. There are two ways to estimate the project cost. The organization can outsource the system that will serve as a base for the case management system or develop it in-house. The company decided to use the in-house option because it already has a team of competent developers who develop the tools that must be integrated into the solution. The fact that many internal systems will be integrated into the new solution and that the organization's internal development team is experienced and confident with this type of development makes in-house development more suitable. Table 3.1 describes the estimated cost of an in-house solution.

<b>Name</b>	<b>Unit cost</b>	<b>Unit</b>	<b>Quantity</b>	<b>Total cost</b>
Hardware	850 000 CZK	Piece	1	850 000 CZK
Team Lead	6 000 CZK	MD	1 worker * 5 days * 20 weeks	600 000 CZK
Developer	4000 CZK	MD	6 workers * 5 days * 20 weeks	2 400 000 CZK
Tester	2 800 CZK	MD	2 workers * 5 days * 20 weeks	560 000 CZK
<b>Total Cost</b>	-	-	-	<b>4 410 000 CZK</b>

Table 3.1: The Estimated Cost Breakdown of the Solution

With the cost of the solution calculated, we can finally calculate the return on security investment (Equation 1.9.2):  $ROSI = (34\,400\,000 * 0,8 - 4\,410\,000) / 4\,410\,000 = 5.240$ . The result would be in terms of ROI interpreted as an expected return of 524%. Regarding ROSI, the proposed solution is very cost-effective.

# Conclusion

In this thesis, we analyzed the current state of processes of a CSIRT team in order to optimize and modernize them and enable the team to focus more on applying their expert knowledge and be less burdened by mundane, frequently repeating work. The optimization was achieved by transforming their processes and the information system the team was using into a solution capable of supporting the integration of automated tools. These tools support and reduce the work of the team by leveraging modern techniques such as automated data analysis using state-of-the-art tools while learning from previous decisions of the team to adapt further and improve its capabilities.

The presented solution and prototype example are non-trivial systems composed of numerous individual components, many of which were part of the organization's infrastructure even before the implementation of the case management system.

The components in question became needed primarily because of the increasing complexity of the organization structure and information systems, resulting in frequent complex forensic analysis utilizing multiple information sources. This need was promoted by increasing bureaucratic overhead, which further restricted access to some information sources. The described effects eventually led to the creation of several data retrieval tools. Each tool was developed separately and gave the CSIRT team access to a specific information system or a part of an information system.

However, the addition of automated data retrieval tools only promoted the, at the time, less prominent but more impactful issue of an exponentially increasing number of incidents. The issue has two primary causes, a rising number of attacks and improvements in detection methods.

The first cause generally results in a flood of labor-intensive tasks, which are frequently very similar and usually require only a low level of expertise. The existence of such tasks implies a need for separation into a multi-level structure which would allow deferring more mundane tasks to less knowledgeable workers. This separation is typical for IT support and other user-facing teams. In our case, the CSIRT team can defer some tasks to the IT helpdesk team, effectively creating L1 support that

can solve most of the routine tasks and escalate the rest to the L2, the CSIRT team. Paradoxically, this solution addresses the second cause better because it allows the CSIRT team to focus mainly on complicated incidents, which are more frequent with improved detection methods. The first cause was only diverted to another team, which consists of a more affordable workforce. However, the less skilled workforce is slower, and the number of incidents increases so rapidly that the cost of employing enough workers would quickly rise to financially unbearable levels. This fact made the organization recognize a need for a solution to solve these low-skill tasks with a high degree of automation or at least make the process more streamlined, requiring less input from human workers.

The case management-based solution allows the organization to address the need for automation by providing a platform designed around the necessary principle of presenting automated tasks results to experts in the form of tasks/decisions while also allowing the automated systems to learn from the handler's overrides of incorrect/imperfect automated or manual decisions of previously undecidable problems.

The Investment Evaluation section further supports the feasibility of the solution. The investment was evaluated using the Return on Security Investment method (ROSI), which The European Union Agency for Cybersecurity (ENISA) recommends. The calculation heavily depends on the organization's maturity regarding current cybersecurity equipment and processes. In the case of our chosen organization, which is well-equipped with many supporting systems, the main goal of the solution is to leverage the options the systems present and use them to their full potential. Because of this, and the organization's capabilities in terms of software development, the proposed solution proved to be more than feasible by the ROSI method.

# Bibliography

1. CRANE, Casey. *42 Cyber Attack Statistics by Year: A Look at the Last Decade* [online]. [visited on 2023-05-08]. Available from: <https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/>.
2. OLTSIK, Jon. *Cybersecurity spending and economic headwinds in 2023* [online]. [visited on 2023-05-08]. Available from: <https://www.csoonline.com/article/3685049/cybersecurity-spending-and-economic-headwinds-in-2023.html>.
3. *Minimum Security Requirements for Federal Information and Information Systems: FIPS Publication 200*. National Institute of Standards and Technology (NIST), 2006. Available also from: <https://csrc.nist.gov/publications/detail/fips/200/final>.
4. *The Act No 181/2014 Coll. on Cyber Security and Change of Related Acts (The Act on Cyber Security)*. The National Cyber and Information Security Agency, Czech Republic, 2014. English translation.
5. PAULSEN, Celia; TOTH, Patricia. *Small Business Information Security: The Fundamentals: NISTIR 7621 Revision 1* [online]. 2016. [visited on 2023-02-18]. Available from: <https://doi.org/10.6028/NIST.IR.7621r1>.
6. ORMROD, David; TURNBULL, Benjamin. Developing a Military Cyber Maturity Model for Multi-Domain Battle Mission Resilience and Success. *International Journal of Cyber Warfare and Terrorism*. 2017, vol. 7, pp. 1–13. Available from DOI: 10.4018/IJJWT.2017100101.
7. BROOKSON, Charles; CADZOW, Scott; ECKMAIER, Ralph; ESCHWEILER, Jörg; GERBER, Berthold; GUARINO, Alessandro; RANNENBERG, Kai; SHAMAH, Jon; GÓRNIAK, Sławomir. *Definition of Cybersecurity: Gaps and overlaps in standardisation* [online]. European Union Agency for Network and Information Security (ENISA), 2015 [visited on 2023-02-02]. ISBN 978-92-9204-155-7. Available from DOI: 10.2824/4069.

8. *The Decree No 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree)*. The National Cyber and Information Security Agency, Czech Republic, 2018. English translation.
9. *Security and Privacy Controls for Information Systems and Organizations: SP 800-53 Revision 5* [online]. 2020. [visited on 2023-04-02]. Available from: <https://doi.org/10.6028/NIST.SP.800-53r5>.
10. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti: Řízení rizik v oblasti kybernetické bezpečnosti* [online]. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), [n.d.] [visited on 2023-03-08]. Available from: <https://www.nukib.cz/cs/infoservis/aktuality/1868-nukib-zverejnil-pruvodce-rozenim-aktiv-a-rizik-dle-vyhlasiky-o-kyberneticke-bezpecnosti/>.
11. TØNDEL, Inger Anne; LINE, Maria B.; JAATUN, Martin Gilje. Information security incident management: Current practice as reported in the literature. *Computers & Security*. 2014, vol. 45, pp. 42–57. ISSN 0167-4048. Available from DOI: <https://doi.org/10.1016/j.cose.2014.05.003>.
12. DABADE, Tanaji D. Information technology infrastructure library (ITIL). In: *Proceedings of the 4th National Conference*. 2012, pp. 25–26.
13. GÈRVALLA, Muhamet; PRENIQI, Naim; KOPACEK, Peter. IT Infrastructure Library (ITIL) framework approach to IT Governance. *IFAC-PapersOnLine*. 2018, vol. 51, no. 30, pp. 181–185. ISSN 2405-8963. Available from DOI: <https://doi.org/10.1016/j.ifacol.2018.11.283>. 18th IFAC Conference on Technology, Culture and International Stability TECIS 2018.
14. KUHN, Janet. *Expanding the Expanded Incident Lifecycle* [online]. [visited on 2023-04-29]. Available from: <http://www.itsmsolutions.com/newsletters/DITYvol5iss7.htm>.
15. BARRETT, Matthew P. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework)* [online]. 2018. [vis-

- ited on 2023-04-29]. Available from: <https://doi.org/10.6028/NIST.CSWP.04162018>.
16. LAIN, Daniele; KOSTIAINEN, Kari; ČAPKUN, Srdjan. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In: *2022 IEEE Symposium on Security and Privacy (SP)*. 2022, pp. 842–859. Available from DOI: 10.1109/SP46214.2022.9833766.
  17. ABDILLAH, Rahmad; SHUKUR, Zarina; MOHD, Masnizah; MURAH, Ts. Mohd Zamri. Phishing Classification Techniques: A Systematic Literature Review. *IEEE Access*. 2022, vol. 10, pp. 41574–41591. Available from DOI: 10.1109/ACCESS.2022.3166474.
  18. MOYLE, Ed. *CERT vs. CSIRT vs. SOC: What's the difference?* [online]. [visited on 2023-03-12]. Available from: <https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference>.
  19. TAURINS, Edgars. *How to set up CSIRT and SOC: GOOD PRACTICE GUIDE* [online]. European Union Agency for Cybersecurity (ENISA), 2020 [visited on 2023-03-12]. ISBN 978-92-9204-410-7. Available from: <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>.
  20. *The CERT Division* [online]. [visited on 2023-03-17]. Available from: <https://www.sei.cmu.edu/about/divisions/cert/>.
  21. CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. *Computer Security Incident Handling Guide: NIST Special Publication 800-61 Revision 2* [online]. [N.d.]. [visited on 2023-02-22]. Available from: <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
  22. MAJ, Miroslaw; REIJERS, Roeland; STIKVOORT, Don. *Good Practice Guide for Incident Management* [online]. European Network and Information Security Agency (ENISA), 2010 [visited on 2023-03-12]. Available from: <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>.

23. BROWNLEE, Nevil; GUTTMAN, E. *RFC2350: Expectations for computer security incident response*. RFC Editor, 1998.
24. COOKE, Nancy J; CHAMPION, Michael; RAJIVAN, Prashanth; JARIWALA, Shree. Cyber situation awareness and teamwork. *EAI Endorsed Transactions on Security and Safety*. 2013, vol. 1, no. 2.
25. KILLCRECE, Georgia; KOSSAKOWSKI, Klaus-Peter; RUEFLE, Robin; ZAJICEK, Mark. *State of the practice of computer security incident response teams (CSIRTs)*. 2003. Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
26. RAJIVAN, Prashanth; COOKE, Nancy. Impact of team collaboration on cybersecurity situational awareness. *Theory and Models for Cyber Situation Awareness*. 2017, pp. 203–226.
27. TARALLO, Mark. *Modern Management and Leadership: Best Practice Essentials with CISO/CSO Applications*. CRC Press, 2021.
28. KARANJA, Erastus. The role of the chief information security officer in the management of IT security. *Information & Computer Security*. 2017, vol. 25, no. 3, pp. 300–329.
29. VAN DER KLEIJ, Rick; SCHRAAGEN, Jan Maarten; CADET, Beatrice; YOUNG, Heather. Developing decision support for cybersecurity threat and incident managers. *Computers & Security*. 2022, vol. 113, p. 102535. ISSN 0167-4048. Available from DOI: <https://doi.org/10.1016/j.cose.2021.102535>.
30. *Forum of Incident Response and Security Teams, Inc. (FIRST)* [online]. [visited on 2023-03-03]. Available from: <https://www.first.org/>.
31. *CSIRT Services Roles and Competencies* [online]. Version 0.9.0. 2022. [visited on 2023-03-03]. Available from: [https://www.first.org/standards/frameworks/csirts/FIRST\\_CSIRT\\_Services\\_Roles\\_and\\_Competencies\\_v\\_0.9.0.pdf](https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf).

32. MITROPOULOS, Sarandis; PATSOS, Dimitrios; DOULIGERIS, Christos. On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*. 2006, vol. 25, no. 5, pp. 351–370. ISSN 0167-4048. Available from DOI: <https://doi.org/10.1016/j.cose.2005.09.006>.
33. ROLLASON-REESE, Richard L. Incident Handling: An Orderly Response to Unexpected Events. In: San Antonio, TX, USA: Association for Computing Machinery, 2003, pp. 97–102. SIGUCCS '03. ISBN 158113665X. Available from DOI: 10.1145/947469.947496.
34. ALBERTS, Chris; DOROFEE, Audrey; KILLCRECE, Georgia; RUEFLE, Robin; ZAJICEK, Mark. *Defining incident management processes for CSIRTs: A work in progress*. 2004. Tech. rep. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.
35. CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen, et al. *SP 800-61 Revision 2: Computer Security Incident Handling Guide*. National Institute of Standards & Technology, 2012.
36. HUSÁK, Martin; ČERMÁK, Milan. SoK: Applications and Challenges of Using Recommender Systems in Cybersecurity Incident Handling and Response. In: *Proceedings of the 17th International Conference on Availability, Reliability and Security*. Vienna, Austria: Association for Computing Machinery, 2022. ARES '22. ISBN 9781450396707. Available from DOI: 10.1145/3538969.3538981.
37. SCARFONE, K; MELL, P. *NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards & Technology, 2007.
38. KENT, Karen; CHEVALIER, Suzanne; GRANCE, Timothy; DANG, Hung. *SP 800-86: Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards & Technology, 2006.
39. *What is an IT ticketing system?* [online]. [visited on 2023-05-07]. Available from: <https://www.servicenow.com/products/itsm/what-is-it-ticketing-system.html>.

40. *Request Tracker* [online]. [visited on 2023-05-06]. Available from: <https://bestpractical.com/request-tracker>.
41. *Request Tracker for Incident Response (RTIR): Incident Management Workflow* [online]. [visited on 2023-05-07]. Available from: <https://bestpractical.com/rtir>.
42. SWENSON, K.D. *Mastering the Unpredictable: How Adaptive Case Management Will Revolutionize the Way that Knowledge Workers Get Things Done*. Meghan-Kiffer Press, 2010. Landmark books. ISBN 9780929652122. Available also from: <https://books.google.cz/books?id=VqCaSQAACAAJ>.
43. *STIX Version 2.1 OASIS Standard: Part 3: Cyber Observable Core Concepts*. [online]. 2019. [visited on 2023-05-07]. Available from: <https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html>.
44. *About CybOX* [online]. The MITRE Corporation, 2012 - 2015 [visited on 2023-05-07]. Available from: <https://cybox.mitre.org/about/>.
45. *Business Process Model and Notation (BPMN) Version 2.0* [online]. Object Management Group, Inc. (OMG), [n.d.] [visited on 2023-04-16]. Available from: <http://www.omg.org/spec/BPMN/2.0>.
46. ROSING, Mark von; WHITE, Stephen; CUMMINS, Fred; MAN, Henk de. *Business Process Model and Notation-BPMN*. 2015.
47. LEYMANN, Frank. BPEL vs. BPMN 2.0: Should You Care? In: MENDLING, Jan; WEIDLICH, Matthias; WESKE, Mathias (eds.). *Business Process Modeling Notation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 8–13. ISBN 978-3-642-16298-5.
48. *Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security [Deliverable – December 2012]* [online]. 2012th ed. European Network and Information Security Agency (ENISA), [n.d.] [visited on 2023-04-10]. Available from: <https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment>.

49. *VirusTotal* [online]. [visited on 2023-03-06]. Available from: <https://www.virustotal.com/>.
50. *NetFlow and IPFIX Exporter: Flowmon Flowmon Probe*. 2023. Available also from: <https://www.flowmon.com/en/products/appliances/probe>.
51. *NetFlow and IPFIX collector with advanced reporting: Flowmon Collector* [online]. 2023. [visited on 2023-03-17]. Available from: <https://www.flowmon.com/en/products/appliances/netflow-collector>.
52. *Elastic Stack: What is the ELK Stack?* [online]. 2023. [visited on 2023-03-17]. Available from: <https://www.elastic.co/what-is/elk-stack>.
53. GAFNI, Ruti; PAVEL, Tal. The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*. 2019, vol. 7, no. 1, pp. 14–26.
54. *Google Safe Browsing* [online]. [visited on 2023-03-06]. Available from: <https://safebrowsing.google.com/>.
55. TOVARŇÁK, Daniel; ČECH, Michal; TICHÝ, Dušan; DOHNAL, Vojtěch. ObservableDB: An Inverted Index for Graph-Based Traversal of Cyber Threat Intelligence. In: *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. 2022, pp. 1–4. Available from DOI: 10.1109/NOMS54207.2022.9789882.
56. TOVARŇÁK, Daniel; DOHNAL, Vojtěch; TICHÝ, Dušan; KRÁL, Benjamin. *Software for security orchestration support and threat life-cycle management*. 2010. Available also from: <https://www.ics.muni.cz/en/research/publications/2249657>.
57. JOHNSON, Chris; BADGER, Lee; WALTERMIRE, David; SNYDER, Julie; SKORUPKA, Clem. *Guide to Cyber Threat Information Sharing: NIST Special Publication 800-150* [online]. [N.d.]. [visited on 2023-04-22]. Available from: <http://dx.doi.org/10.6028/NIST.SP.800-150>.

58. ROSS, Ron; PILLITTERI, Victoria; DEMPSEY, Kelley; RIDDLE, Mark; GUISSANIE, Gary. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: NIST Special Publication 800-171 Revision 2* [online]. [N.d.]. [visited on 2023-04-22]. Available from: <https://doi.org/10.6028/NIST.SP.800-171r2>.
59. *Průměrné mzdy - 4. čtvrtletí 2022* [online]. [visited on 2023-05-06]. Available from: <https://www.czso.cz/csu/czso/cri/prumerne-mzdy-4-ctvrtleti-2022>.

# List of Figures

1.1	Components Constituting the Definition of Cybersecurity Defined by ENISA [7, p. 13] . . . . .	19
1.2	The Phases of the Incident Lifecycle [14] . . . . .	23
1.3	Comparison of CSIRT, CERT, and SOC Centers of Attention [18] . .	24
1.4	By NIST Defined Phases of Incident Response Lifecycle [35, 21] . . .	32
1.5	ENISA Workflow of Incident Handling - Source: ENISA Incident Management Guide [22, 37] . . . . .	35
1.6	The Example of Incident Handling Triage - Source: ENISA Incident Management Guide [22, 38] . . . . .	36
1.7	BPMN Tasks Overview - source: BPMN Specification [45, 156-165] .	41
1.8	BPMN Events Overview - source: BPMN Specification [45, 83] . . .	43
1.9	BPMN Common Elements Overview - source: BPMN Specification [45] . . . . .	43
2.1	Incident Handling process . . . . .	47
2.2	Organization's Information Systems and Tools Related to the RTIR .	49
2.3	Ticket State Lifecycle . . . . .	51
3.1	Blocking Services . . . . .	57
3.2	Incident Detection and Reporting Services . . . . .	58
3.3	Observable Detection and Correlation Services . . . . .	59
3.4	Enrichment and Incident Resolution Tools . . . . .	59
3.5	Case Overview . . . . .	60
3.6	Incident Report Processing . . . . .	61
3.7	Automated Preliminary Analysis Process . . . . .	63
3.8	Automated Resolution Process . . . . .	65
3.9	Expert Resolution Process . . . . .	69
3.10	Dashboard View . . . . .	72
3.11	Full Case View . . . . .	73
3.12	Case: Users Tab . . . . .	74
3.13	User Accounting View . . . . .	75

3.14 Case: Observables Tab . . . . .	76
3.15 Case: Assets Tab . . . . .	76
3.16 Case: Events Tab . . . . .	77
3.17 Case: External References Tab . . . . .	78
3.18 Case: TTPs Tab . . . . .	78
3.19 Workflow View . . . . .	79
3.20 Stage View . . . . .	79
3.21 Task View . . . . .	81
3.22 Workflow Templates View . . . . .	82
3.23 Phishing Case Overview . . . . .	83
3.24 Phishing Workflow . . . . .	84
3.25 Phishing Workflow . . . . .	85
3.26 Phishing Workflow: Analysis Phase . . . . .	85
3.27 Task: Aggregate Malicious Domains . . . . .	86
3.28 Task: Analyse Domain . . . . .	87
3.29 Resolved Task: Aggregate Malicious Domains . . . . .	88
3.30 Phishing Workflow: Mitigation Phase . . . . .	89
3.31 Phishing Workflow: Revision Phase . . . . .	90
3.32 Case: Resolved . . . . .	90

# List of Tables

3.1	The Estimated Cost Breakdown of the Solution . . . . .	92
-----	--	----

# Glossary

**Act No 181/2014 Coll.** Act No 181/2014 Coll. on Cyber Security and Change of Related Acts (The Act on Cyber Security)

**BPMN** Business Process Model and Notation, a graphical representation for specifying business processes in a business process model

**CERT** Computer Emergency Response Team

**CERT/CC** The CERT Coordination Center, the part of Carnegie Mellon University's Software Engineering Institute

**CESNET** An association of universities of the Czech Republic and the Czech Academy of Sciences operating and developing the national e-infrastructure for science, research, and education

**CISO** Chief Information Security Officer

**CSIRT** Computer Security Incident Response Team

**CSO** Chief Security Officer

**CTI** Cyber Threat Intelligence

**Decree No 82/2018 Coll.** Decree No 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree)

**ENISA** The European Union Agency for Cybersecurity

**FIRST** Forum for Incident Response and Security Teams

**IPFIX** Internet Protocol Flow Information Export (IPFIX) is the protocol developed by the IETF working group (not CISCO) as a common, universal standard of export for Internet Protocol flow information. Cisco NetFlow v9 was the basis for IPFIX. Therefore, IPFIX is also referred to as NetFlow v10.

**MITRE ATT&CK Matrix** MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective

**NCISA** National Cyber and Information Security Agency of the Czech republic, the central body of state administration for cyber security

**NetFlow** a network protocol developed by Cisco for collecting IP traffic information and monitoring network flow

**NIST** National Institute of Standards and Technology

**OSINT** Open Source Intelligence, a framework focused on gathering information from free tools or resources

**RTIR** Request Tracker for Incident Response, the request tracker (RT) for incident response teams

**SOC** Security Operations Center

**VPN** Virtual Private Network

**XDR** Extended Detection and Response (XDR) is an extended version of Endpoint Detection and Response (EDR), a cybersecurity technology that continually monitors an "endpoint" (e.g. laptop) to mitigate malicious cyber threats