Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation

MEHDI AKBARI GURABI and LASSE NITZ, Fraunhofer FIT, Sankt Augustin, Germany and RWTH Aachen University, Aachen, Germany
ANDREJ BREGAR, Informatika d.o.o., Maribor, Slovenia
JAN POPANDA, Fraunhofer FIT, Sankt Augustin, Germany
CHRISTIAN SIEMERS, Airbus Protect GmbH, Munich, Germany
ROMAN MATZUTT and AVIKARSHA MANDAL, Fraunhofer FIT, Sankt Augustin, Germany

Cybersecurity playbooks assume an increasingly important role as threat-specific documents for guiding operators in the context of cyber incident response. However, these playbooks are mostly unstructured or semi-structured, which significantly limits their utility when it comes to automating response and reporting steps, complying with cybersecurity directives, or sharing best practices for incident response across organisations. We thus argue that cybersecurity playbooks must transition to interoperable and machine-readable formats from generation, via management and utilisation to cross-organisational sharing. In this work, we identify and structure key requirements based on expert interviews as a first step toward this transition. From these requirements, we derive a framework for further guidance during the transition to structured security playbooks and their utilisation in a tool-assisted fashion. We discuss the implications of our framework and lessons learned before outlining directions for future research.

CCS Concepts: • **Security and privacy** → **Security services**; • **Software and its engineering** → *Requirements analysis*;

Additional Key Words and Phrases: Cybersecurity playbooks, response and recovery, machine-readability

ACM Reference format:
Mehdi Akbari Gurabi, Lasse Nitz, Andrej Bregar, Jan Popanda, Christian Siemers, Roman Matzutt, and Avikarsha Mandal. 2024. Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation. *Digit. Threat. Res. Pract.* 5, 3, Article 34 (October 2024), 11 pages.
https://doi.org/10.1145/3688810

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101020560 (CyberSEAS).
Authors' Contact Information: Mehdi Akbari Gurabi (corresponding author), Fraunhofer FIT, Sankt Augustin, Germany and RWTH Aachen University, Aachen, Germany; e-mail: mehdi.akbari.gurabi@fit.fraunhofer.de; Lasse Nitz, Fraunhofer FIT, Sankt Augustin, Germany and RWTH Aachen University, Aachen, Germany; e-mail: lasse.nitz@fit.fraunhofer.de; Andrej Bregar, Informatika d.o.o., Maribor, Slovenia; e-mail: andrej.bregar@informatika.si; Jan Popanda, Fraunhofer FIT, Sankt Augustin, Germany; e-mail: jan.popanda@fit.fraunhofer.de; Christian Siemers, Airbus Protect GmbH, Munich, Germany; e-mail: christian.c.siemers@airbus.com; Roman Matzutt, Fraunhofer FIT, Sankt Augustin, Germany; e-mail: roman.matzutt@fit.fraunhofer.de; Avikarsha Mandal, Fraunhofer FIT, Sankt Augustin, Germany; e-mail: avikarsha.mandal@fit.fraunhofer.de.

ACM 2576-5337/2024/10-ART34
https://doi.org/10.1145/3688810

1 Introduction

The large-scale transition from physical systems and services to interconnected digital ones benefits both organisations and users by making respective functionalities more easily accessible and efficient. At the same time, adversarial actors benefit from this transition, as it allows for automated attacks targeting a wider range of potential victims. Organisations hence have to protect their systems and services against an increasing number of cyberattacks [27]. While reviewing the detected incidents is challenging due to the high number of false alarms [3], subsequent handling of detected incidents is costly and resource-intensive, which often leads to security teams being under-resourced for this task [26].

Repetitive tasks that diminish **Security Operation Center (SOC)** staff enthusiasm and concentration significantly motivate the need for security orchestration and automation in the SOC [27]. Security orchestration and automation enable analysts to address crucial issues more efficiently and with optimised response times. However, challenges such as training gaps, highlighted by Crémilleux et al. [8], emphasise the importance of capturing knowledge in playbooks to offer SOC staff vital insights. These gaps are evident when experienced security professionals may possess insufficient knowledge in specialized domains, and analysts are often limited to interpreting logs. Capturing tactical decision-making knowledge remains difficult, and the issue of retaining skilled staff also underscores this knowledge capturing requirement [22]. To tackle the aforementioned issues, SOC teams could also significantly enhance their effectiveness by collectively and collaboratively exchanging **cyber threat intelligence (CTI)** [6]. Nonetheless, a significant research gap remains to be addressed: the current state of incident response documentation lacks the requisite structure and a systematic workflow.

Concurrently, the recent European NIS2 Directive emphasises standardised cyber incident reporting and CTI exchange among European member states [11]. To comply with such regulations, organisations must fulfil several cybersecurity requirements and follow specific incident response procedures, such as standardised reporting mechanisms to national authorities [21]. The Directive expands the scope by requiring that more entities and sectors implement cybersecurity measures. Thus, playbooks can help in structuring the documentation, sharing best practices, and where possible, automating the execution steps to enhance the scalability of the response processes. Achieving this requires the introduction of a formal machine-readable playbook format and the establishment of a multi-level process to enable analysts to unify incident response procedures using information from various sources. Adopting such machine-readable playbooks could significantly aid security operators, especially in **Computer Emergency/Incident Response Teams (CERTs/CIRTs)**. This concept should integrate different abstraction levels, utilising (un)-structured formats for knowledge and metadata capturing, graphical modelling notations, and executable forms with proper mapping schemes.

Due to the wide variety of dependencies, actors, and challenges in incident response, we identified the need for a comprehensive requirements-to-framework approach. The first step toward achieving structured formats for knowledge exchange and incident response automation is requirements engineering. This design aims to bridge communication gaps between various security actors and advanced security components to result in a holistic playbook-assisted incident handling solution and ensure feedback procedures to improve the details of existing security response documents.

Contributions: In this work, we present the requirements for playbook utilisation, playbook-assisted incident handling, reporting and automation in cybersecurity, as well as our conceptual framework for the generation and management of machine-readable playbooks. Further, we briefly introduce our developed playbook management tool as the core component for facilitating the playbook-assisted incident response and the respective connections to other components and actors of the framework within incident handling, reporting, and automation. We highlight efforts to integrate the playbook-assisted incident response approach with systems and actors commonly involved in incident response to enhance their capabilities. Additionally, we discuss the addressed requirements and our lessons learned and provide potential directions for future work.

2 Background and Related Work

In this section, we provide the necessary background and present related work. To this end, we first give an overview of the state-of-the-art incident response and automation approaches and related standardisation efforts before outlining related works focused on playbooks.

Background: The massive volume of security data presents a significant challenge due to the increased resource demand and associated costs, particularly for security teams that are often under-resourced [1]. It is necessary that these teams possess up-to-date strategies, which include the context, techniques, indicators, and actionable recommendations to proactively combat potential cyber threats [28]. An organisation's response to cyberattacks is orchestrated through well-defined policies and procedures that focus on eliminating and recovering from such incidents [10].

To facilitate the incident handling process, Threat Intelligence Platforms are employed to centralise, refine, and disseminate threat data from various sources. This not only saves analysts' time but also enhances internal and external intelligence sharing. Additionally, the adoption of **Security Orchestration, Automation, and Response (SOAR)** tools is becoming critical due to the increasing security demands. SOAR improves security operations by automating routine tasks and consolidating threat data, thereby aiding the efforts of human analysts [19]. When integrated with **Security Information and Event Management (SIEM)** systems, which focus on threat identification through data analysis, a more robust incident response strategy is formed. Despite these advancements, there is still a need for standardisation and methodological approaches in employing SIEM and SOAR systems in incident response procedures [19]. Academic research in this field is burgeoning, aiming to explore these challenges and propose novel solutions [5, 24].

Previous efforts in [15] discussed the necessity for standardised security automation, addressing challenges such as scalability and knowledge management. Additionally, [18] highlighted the critical role of stakeholder engagement and the risks of excessive automation in incident response. Other studies considered the security incident process, related standards, and decision-making in incident analysis [4, 25]. Furthermore, Karlzen et al. conducted a comprehensive review of automatic incident response solutions, categorising them using the MITRE D3FEND[1] framework and comparing academic concepts with commercial products [12].

Related Work: The authors of [23] critiqued the current state of playbook design in cybersecurity incident response, noting a lack of discipline that potentially damages its effectiveness. They suggested a formal, model-based design approach and introduced a prototype tool. Moreover, Akbari Gurabi et al. [2] developed a tool particularly aimed at capturing and sharing incident response knowledge. This tool represents a promising foundation for enhancing automation and collaboration. However, identifying strategies for its integration into existing processes and frameworks remains a crucial area for further investigation. Meanwhile, [20] delved into the ambiguities of playbook definitions and applications, highlighting that playbooks are not always interchangeable among organisations due to unique interpretations and emphasis on different aspects of incident response.

The study by [19] conducted a thorough analysis of various incident response formats and focused on the core concepts required for the standardisation of incident response. Moreover, [10] focused on creating playbooks specific to vulnerabilities in **industrial control systems (ICS)**. They contributed to the field by mapping out the landscape of incident response standardisation and offering a process model for mapping recommendations from security advisories to generate ICS vulnerability playbooks. This effort resulted in practical contributions, including an open-source application and various recommendations aimed at refining security advisory and playbook standards. While these efforts aim to leverage playbooks to improve cybersecurity measures and enhance incident response capabilities, our work distinctly focuses on playbook management as a key element for advancing incident response and reporting by integrating standardisation, collaboration, automation, and feedback processes.

[1] https://d3fend.mitre.org/

3 Methodology

We started by identifying the necessity of requirement analysis as the initial step toward developing and exchanging structured playbooks for automation and reporting. This preliminary phase was facilitated by a series of structured expert interviews. These interviews were designed to capture the nuanced insights needed for preparing a vocabulary and tool to augment the efficiency of knowledge capture and exchange, and to steer automation strategies.

Initially, the playbook management tool was developed as a stand-alone tool to aid human operators in the creation, management, and sharing of machine-readable cybersecurity playbooks. In five online interview sessions, we interviewed ten domain experts from two security companies, one national research and education network organisation, and two universities. Although the selection of institutions is relatively small, it captured diverse perspectives from both industry and academia, ensuring practical insights and real-world applicability of the derived knowledge. The experts' backgrounds include threat detection, incident response, security services and consultation, and data visualisation within the cybersecurity domain. We conducted another round of interview sessions during development to ensure the vocabulary and tool address the realistic needs of human operators. We gathered feedback on the implementation of our approach, vocabulary applicability, user experience, and outputs. The feedback also covered overall impressions concerning readability, semantics, interoperability, and practical application.

After this, we focused on identifying strategies for integration into existing processes and frameworks. Our goal was to ensure that the tool could be effectively leveraged across various organisational structures and incident response scenarios for documentation, automation, and reporting purposes. We aimed to increase the tool's maturity by validating its use in a critical infrastructure environment. Recognising the complexity of this effort, we proceeded with a phase of requirements engineering. We collaborated with both infrastructure and technology providers to integrate the playbook management tool with systems commonly used in incident response. Requirements for a playbook-assisted incident response toolset were derived from discussion sessions with domain experts in SOCs and CERTs, aligned with three pilots in a project on critical infrastructures. Additionally, we held detailed discussions with security experts from a major cybersecurity player in Germany, a Slovenian SOC in the energy domain, and the **Slovenian national CERT (SI-CERT)** to develop our concept and framework. To categorise and validate the requirements, we conducted semi-structured discussion sessions. These sessions helped us converge the identified requirements, analyse their relevance, and discuss validation scenarios and remaining challenges. In this work, we present a set of requirements collected during this process, along with a conceptual framework and a proof-of-concept realisation that connects relevant systems and actors. In addition to incident response, we also focused on communication activities between relevant actors, such as SOCs, CERTs/CSIRTs, and national authorities.

4 Requirements

Playbook-centered incident handling is complex and encompasses phases of decision-making, reporting, collaboration, and incident response. Particularly, the shift from unstructured or semi-structured playbooks to structured formats is essential to enhance the process. However, the transition to machine-readable playbooks from only human-readable ones presents its own set of conceptual challenges: (a) Manually creating structured machine-readable playbooks is time- and resource-intensive. (b) Synchronising high-level playbooks, such as those in **Business Process Model and Notation (BPMN)** format, with executable workflows is challenging. (c) Establishing the workflow requires precise planning and decision-making, especially when deciding which tasks should be automated rather than performed by a human.

The complexity of the concept requires a solid integration of various components, each providing specific functions necessary for successfully handling cybersecurity incidents. At first, we identified the key functionalities essential for cybersecurity response procedures:

Playbook management: this function encompasses the systematic organisation and maintenance of playbooks to ensure they remain current and accessible.
Playbook selection: this allows users to select the most fitting playbooks from a repository designed for particular types of incidents.
Playbook execution: this pertains to the practical application of playbooks, where prescribed actions are carried out to mitigate incidents.
SIEM integration and analysis: this is vital for the collation and examination of security events to shape strategies for incident response.
Sharing platform integration and CTI exchange: this function is crucial for the dissemination of CTI among various platforms, enhancing the handling of incidents via collective efforts.
Collaboration and work coordination facilities: the tool set should facilitate collaboration, coordination and synchronisation among various groups and stakeholders engaged in incident management.
Reporting facilities: this functionality enables the creation of detailed reports that document the incident, the applied response measures, and the outcomes for CERTs/CIRTs and national authorities.

The playbook-assisted response relies on integration with external systems, such as SIEM and CTI sharing platforms. The primary actors involved in the framework are SOCs, CERTs/CIRTs, national CERTs, and other organisations that could benefit from sharing playbooks. We derived requirements for a playbook-assisted incident response tool set from the discussion sessions mentioned in Section 3. These requirements are given in Table 1.

5 Framework

Figure 1 depicts the conceptual framework consisting of the information flow and relations between the incident handling components. In the context of incident handling, a **Continuous Integration/Continuous Delivery (CI/CD)** flow begins with the log correlation of SIEM and progresses through several steps when a SOC alarm is triggered. This chain of actions starts with the incident use case, extends by the SOC analysis via investigation playbooks through a **Security Incident Response Platform (SIRP)** and ends with response actions taken by the CERT/CIRT.

It is vital for an effective SOC to ensure a broad spectrum of rules and instructions to cover a wide range of possible scenarios without increasing false alerts. The associated effort leads many companies to outsource their SOC. Direct feedback from analysts is required through CI/CD to facilitate adjustments to generic incident use cases into more refined versions. Therefore, providing them with adjustable incident response procedures (investigation playbooks) and logs of their execution allows for enhancing their feedback to security engineers to fine-tune the distinct type of incident. When a SOC alarm is validated as a security incident, processed investigation playbooks and identified Indicators of Compromise can be shared with the response team, enabling the improvement of response strategies.

Further, the preliminary phase of transition from unstructured guidelines to structured playbooks involves extracting information from existing documentation and creating the workflows by translating it into a standardised format (e.g., BPMN). After that, the created workflows should be translated and synchronised to a machine-readable standard using a playbook management tool. Afterwards, supplementary information, such as basic metadata or detailed instructions and automation capabilities, can be incorporated into the playbook. The playbooks can be operated by SOC and CERT members to detect incidents and respond accordingly with the actions on confirmed affected assets and systems. The playbooks should be continuously revised and enhanced based on the feedback from the operation. Additionally, the reports to national CERTs can be generated in an automatic and standardised way facilitating communication and receiving feedback from the authorities. Moreover, as the playbooks are organisation-specific and may include confidential and private information [16], a generalisation and sanitisation step is required before sharing them with the community. After a review process with a human in the loop to check comprehensive privacy and confidentiality issues and confirm the shareable

Table 1. Requirements for Playbook-Assisted Incident Handling, Reporting and Automation in Cybersecurity

ID	Requirement	Description
R.1	Adherence to technological standards	Ensure compatibility with standard modelling notations, execution languages, and automation formats, such as BPMN, CACAO, JSON.
R.2	Adherence to legislative frameworks	Strictly conform to legislative frameworks and requirements, for example, NIS2.
R.3	Reusability	Facilitate efficient reuse of playbook components, legislative and reporting rules, code snippets, and standard modelling constructs.
R.4	Readability	Ensure machine-readability for automation and human-readability to assist users in the process.
R.5	Coverage of multiple abstraction levels	Provide playbooks across a spectrum of abstraction levels, ranging from descriptive to technical.
R.6	Multipurpose suitability	Keep playbooks applicable for diverse purposes and staff (administrative, technical, and legal).
R.7	Adaptability/modifiability	Allow playbooks to be easily and effectively altered, customized, enhanced, and tailored by stakeholders throughout their lifecycle.
R.8	Consistency	Ensure modifications of surrounding processes maintain playbook consistency in different forms.
R.9	Design and development lifecycle	Adopt a multi-stage lifecycle for playbook development, from conception to execution, with appropriate mappings and human interaction.
R.10	Functional integrability	Develop playbooks that directly support incident response (IR) and investigation activities.
R.11	System integrability	Enable developed playbooks to connect extensively with external systems and platforms. It includes import/export functionality for external information such as recent threats or relevant tactics, techniques, and procedures.
R.12	Shareability	Allow for the sharing of playbooks, definitions, and rules within and across organisations.
R.13	Collaboration ability and empowerment	Promote collaboration both vertically and horizontally, especially between SOCs and CERTs.
R.14	Reporting ability	Standardize reporting structures to bolster CTI sharing and legal compliance.
R.15	Standardisation of playbook management	Standardise procedures for incident handling across sectors, infrastructures, SOCs, and stakeholders.
R.16	Confidentiality	Realise access control for playbooks and safeguard confidential information within them.

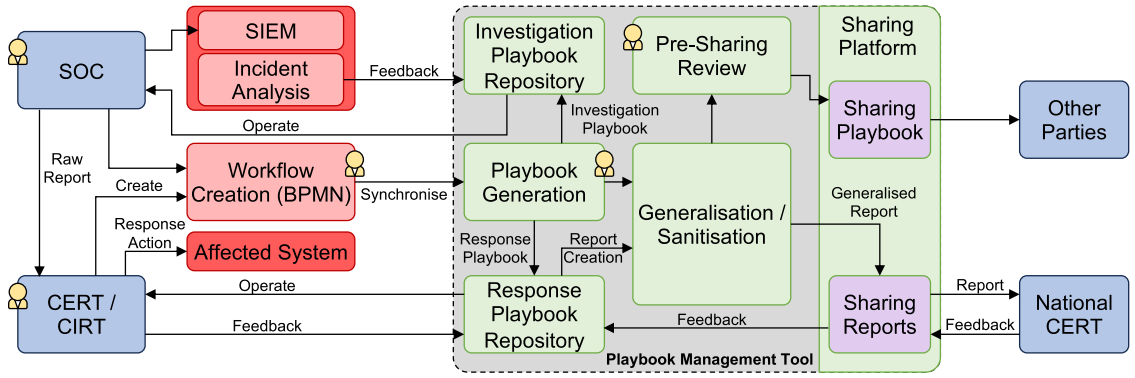
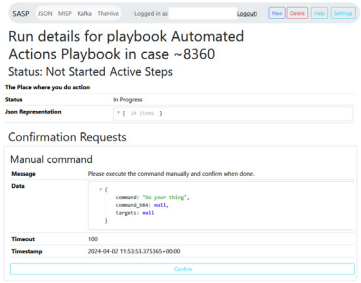
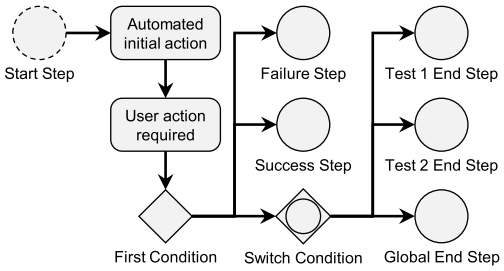


Fig. 1. Conceptual framework representing the incident handling flow. It illustrates the journey from log correlation in SIEM through various playbook-assisted steps in the SOC, in combination with response actions by the CERT/CIRT, incident reporting to national CERTs and sharing knowledge with other organisations.



(a) Tool overview page



(b) Example BPMN output

Fig. 2. Exemplary tool features, including (a) execution overview with command prompt and (b) visual representation in BPMN.

version, playbooks can be shared with other organisations to learn from best practices, enhance their response or open the window for collaborative incident response and automation [17]. The figure emphasises the importance of feedback loops, synchronisation of high-level workflows and detailed playbooks, and the role of playbooks in refining response mechanisms.

6 Realisation

For the realisation of the approach, the playbook management tool has been developed to generate and manage machine-readable playbooks through a user-friendly interface, initially adopting the in-house semantic web-based format and subsequently the OASIS consortium's **Collaborative Automated Course of Action Operations (CACAO)** standard. The CACAO specification [9] facilitates automation by providing a structured playbook that includes machine-readable instructions, for example, commands in the OpenC2[2] format, and targets, such as IP addresses to be attached to response action steps.

The tool supports importing and exporting playbooks, and integration with the MISP[3] CTI sharing platform [13] to facilitate sharing of the playbooks and reports between different teams and also with other organisations. The tool also provides the ability to export playbooks as JSON and publish them in a connected Kafka instance while providing the ability to search Kafka for already published playbooks to import. The tool has also been developed with a focus on user-centric features such as a versioning system for gradual improvements of the playbooks and automated BPMN graph generation for visual representation and synchronisation purposes.

The aim of the development is not only to facilitate the management of playbooks but also to automate their execution, saving operators' time by performing routine analysis tasks. Given the extensive range of potential responses to an incident, we have integrated the playbook management with TheHive and Cortex as an existing SIRP. Once the playbook management tool is connected to an operational TheHive instance, users are presented with an overview of open *cases* on TheHive, and they have the capability to execute a playbook on such a *case*. Commands within a playbook may be manual, interrupting the workflow to prompt the user for confirmation of command execution, or they may utilise a command for invoking Cortex *Analyzers* and *Responders*. Playbooks incorporate variables that grant access not only to the fields and artefacts of the *active case* but also to the results from previously executed *Analysers* and *Responders*. The use of conditional and loop steps enables the creation of complex playbooks that can dynamically adapt to varying scenarios. At each stage of execution, an overview page displays a JSON-formatted report detailing the current state, active steps, and any steps that necessitate attention or confirmation. Figure 2 exemplifies the tool functionality by showing the current state of playbook execution (Figure 2(a)) and the playbook's visual representation with automated monitoring actions (Figure 2(b)).

[2] https://openc2.org/
[3] https://misp-project.org/

```
{
  “action”: “start”,
  “target”: {“uri”: “NOKI_Reporter_1_0”},
  “args”: {
    “data”: {
      “noki_report”: {...},
      “report-compromised-service-description”:
        “hive-case-field:customFields.serviceName”,
      “report-initiated-countermeasures”:
        “Automated Actions Playbook”,
    },
    “datatype”: “Playbook Data”
}
```

```
“noki_report”: {
    “incident-start-timestamp”: “1713969957.229522”,
    “report-voluntary”: “Voluntary Incident Notification”,
    “reporter-e-mail”: [“john.doe@soc.org”],
    “reporter-name”: [“John Doe”],
    “reporter-organization”: “Security Ltd.”,
    “reporter-phone-number”: “+1 (212) 555-1337”
},
```

Listing 1: A Command That Invokes the NOKI Cortex Responder in the Playbook Management Tool

The analysis of requirements revealed a significant advantage in associating playbooks with incident events. This ensures that when an event is shared with authorities, the corresponding playbook is also disseminated. We developed a Cortex *Responder* that can automatically generate a report for cyber security incidents named **Nacionalni Načrt Odzivanja Na Kibernetske Incidente (NOKI)**,[4] as introduced by the Slovenian government. This effort aligns the reporting process with specifications by SI-CERT. The report forms can be filled either directly from a TheHive *Case* or through the playbook management tool as part of an automated playbook. The automated step allows for filing a report on the actions taken and attaching information about the used playbook. Once the report is created and confirmed, it is published via MISP. Listing 1 shows a command in the playbook management tool that invokes the NOKI Cortex Responder.

7 Discussion

In this section, we discuss the verification of the presented framework based on the identified requirements and validation of the tool in critical infrastructures. Further, we briefly present a lesson learned and future research directions identified.

Verification and validation of the framework: The identified requirements are met by a variety of framework components and processes. *R.1: Adherence to technological standards*, *R.3: Reusability*, and *R.4: Readability* are satisfied by the playbook management tool, which supports standard modelling notation and playbook formats, the ability to reuse existing playbooks as templates or invoke other playbooks as part of the workflow, and offering machine-readable (e.g., CACAO) and human-readable representation of playbooks. *R.16: Confidentiality* is fulfilled by utilising the Traffic Light Protocol and generalisation/sanitisation processes before sharing. Moreover, *R.7: Adaptability/modifiability* is supported by the playbook management tool's features for easy modification and versioning, as well as *R.9: Design and development lifecycle* which is upheld with version control and feedback processes. *R.2: Adherence to legislative frameworks* and *R.14: Reporting ability* are addressed by the report creation flow in the framework, report creation functionalities of the developed playbook management tool and sharing procedures with National CERT. *R.5: Coverage of multiple abstraction levels* is covered by workflow and playbook creation components, which allow for variable levels of detail from high-level BPMN to executable tasks. *R.6: Multipurpose suitability* is ensured by the framework flows, playbook management tool, and different playbook repositories from investigation to response. *R.8: Consistency* is maintained by the synchronisation of playbook generation processes. *R.10: Functional integrability*, is supported by automation related efforts and integration with SOC and CERT/CIRT operations, as well as SIEM connections, and *R.11:System integrability* with sharing platforms. *R.12: Shareability* and *R.13: Collaboration ability and empowerment* are promoted through sharing platforms and relevant conceptual components and feedback loops that encourage cooperation between SOCs and CERTs. Lastly, *R.15: Standardisation of playbook management* is satisfied by standard processes and widely used tools utilised with the help of the entire framework.

[4] https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf

In the validation scenario, we performed incident response practices for the IT/OT infrastructure of a Slovenian **Distribution System Operator (DSO)**, and demonstrated the coordination between the SOC and SI-CERT. A proof-of-concept setup of infrastructures for SI-CERT and a DSO SOC was demonstrated. The setup includes the DSO SOC's firewall, DSO IT and OT assets (e.g., workstations, servers, and systems) targeted or involved in attack scenarios, the playbook management tool, and MISP. CTI exchange, reporting, and incident response coordination for malware, phishing, and command-and-control attack scenarios were validated to test the effectiveness of the framework components. The DSO SOC and SI-CERT collaborated to sanitise, edit, and share playbooks via MISP. Integration with the MISP NOKI object enables automated sharing of incident indicators, regulatory NOKI information, and playbook data for proper incident response.

Lesson learned: The step-wise approach allows to comprehensively capture incident response measures and aligns the playbook execution with specific requirements and steps of the NIST incident response process [7]. It also properly incorporates different organisational levels and roles taking part in incident response and considers the requirements of national CERTs regarding incident reporting and CTI exchange. It resembles the **Business Process Management (BPM)** life cycle, which consists of design, modelling, execution, monitoring, and optimisation steps [14]. This work emphasise a need for development of a holistic playbook management life cycle, considering the conversion of descriptive BPMN incident response models into machine-readable playbooks (e.g., CACAO).

Future works: As a playbook is executed, the security engineer may identify additional needed activities not yet covered by the playbook. This poses a challenge because the BPMN and CACAO models must be updated consistently and coherently. Due to limited resources and time, only the executable model may be enhanced, resulting in inconsistency between the two models. Since this problem is known in Business Process Management [29], investigating reverse engineering and synchronisation of BPMN and CACAO playbooks is in the scope of follow-up work. Additionally, increasing automation for transforming un- and semi-structured playbooks into a standardised machine-readable format is an important step for transitioning to machine-readable playbooks. Further, tools assisting human operators in generalising or sanitising playbooks to remove sensitive information will be required to reduce the manual overhead currently associated with sharing playbooks. Another direction of interest is further investigating scenarios to include automated processes based on machine-readable playbooks.

8 Conclusion

As the cybersecurity landscape evolves, introducing standardised machine-readable playbooks will be important for strengthening an organisation's defence against cyber threats. This shift to machine-readable playbooks is a key advancement in cybersecurity incident response for providing a foundation for complex automation and standardised reporting, aligning with EU directives like NIS2. To take the first steps towards automation, we identified that a requirement analysis is necessary to offer a holistic conceptual framework and proof-of-concept realisation. It provides a solution for playbook-assisted incident handling and reporting, and it facilitates integration with platforms like TheHive and Cortex. The playbook management tool supports the CACAO standard format in addition to a flexible in-house vocabulary based on semantic technology, and provides functionalities like enhanced searchability, efficient version control, and CI/CD integration. As part of the playbook management life cycle, a systematic BPM approach is important for capturing comprehensive incident response information and synchronising the documentation steps.

Acknowledgements

We thank Fernando Guerrero and Mina Todorova from Airbus Protect, and Matej Breznik from Slovenian National CERT for their support and insightful feedback.

References

[1] Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin, and Robiah Yusof. 2018. Cyber threat intelligence – issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science* 10, 1 (2018), 371–379.

[2] Mehdi Akbari Gurabi, Avikarsha Mandal, Jan Popanda, Robert Rapp, and Stefan Decker. 2022. SASP: A semantic web-based approach for management of sharable cybersecurity playbooks. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–8.

[3] Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic. 2022. 99% False positives: A qualitative study of SOC analysts' perspectives on security alarms. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association, 2783–2800.

[4] Roberto Andrade, Jenny Torres, and Susana Cadena. 2019. Cognitive security for incident management process. In *Proceedings of the International Conference on Information Technology and Systems (*ICITS '19). Springer, 612–621.

[5] Tao Ban, Takeshi Takahashi, Samuel Ndichu, and Daisuke Inoue. 2023. Breaking alert fatigue: AI-assisted SIEM framework for effective incident response. *Applied Sciences* 13, 11 (2023), 6610.

[6] Xander Bouwman, Victor Le Pochat, Pawel Foremski, Tom Van Goethem, Carlos H. Ganan, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Wouter Joosen, and Michel van Eeten. 2022. Helping hands: Measuring the impact of a large threat intelligence sharing community. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association, 1149–1165.

[7] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. 2012. Computer security incident handling guide. *NIST Special Publication* 800, 61 (2012), 1–147.

[8] Damien Crémilleux, Christophe Bidan, Frédéic Majorczyk, and Nicolas Prigent. 2019. Enhancing collaboration between security analysts in security operations centers. In *Proceedings of the 13th International Conference on Risks and Security of Internet and Systems (CRiSIS '18)*. Springer, 136–142.

[9] Bret Ed. by Jordan and Allan Thomson. 2023. CACAO Security Playbooks Version 2.0. OASIS Committee Specification Draft 05. Retrieved from https://docs.oasisopen.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html

[10] Philip Empl, Daniel Schlette, Lukas Stöger, and Günther Pernul. 2023. Generating ICS vulnerability playbooks with open standards. *International Journal of Information Security* 23 (2023), 1–16.

[11] NIS 2 Directive EU. 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555

[12] Henrik Karlzen and Teodor Sommestad. 2023. Automatic incident response solutions: A review of proposed solutions' input and output. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23)*. ACM, New York, NY, Article 37, 9 pages. DOI: https://doi.org/10.1145/3600160.3605066

[13] Vasileios Mavroeidis, Pavel Eis, Martin Zadnik, Marco Caselli, and Bret Jordan. 2021. On the integration of course of action playbooks into shareable cyber threat intelligence. In *Proceedings of the IEEE International Conference On Big Data (Big Data)*. IEEE, 2104–2108.

[14] Sanjay Mohapatra and Sanjay Mohapatra. 2013. Business process management (process life cycle, process maturity). *Business Process Reengineering: Automation Decision Points in Process Reengineering* (2013), 69–94.

[15] Pantaleone Nespoli, Dimitrios Papamartzivanos, Félix Gómez Mármol, and Georgios Kambourakis. 2017. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *IEEE Communications Surveys & Tutorials* 20, 2 (2017), 1361–1396.

[16] Lasse Nitz, Mehdi Akbari Gurabi, Avikarsha Mandal, and Benjamin Heitmann. 2021. Towards privacy-preserving sharing of cyber threat intelligence for effective response and recovery. *ERCIM News* 126 (2021), 33.

[17] Lasse Nitz, Martin Zadnik, Mehdi Akbari Gurabi, Mischa Obrecht, and Avikarsha Mandal. 2022. From collaboration to automation: A proof of concept for improved incident response. *ERCIM News* 129 (2022), 31.

[18] Megan Nyre-Yu, Kelly A. Sprehn, and Barrett S. Caldwell. 2019. Informing hybrid system design in cyber security incident response. In *Proceedings of the 1st International Conference on HCI for Cybersecurity, Privacy and Trust* (HCI-CPT '19). Springer, 325–338.

[19] D. Schlette, M. Caselli, and G. Pernul. 2021. A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2525–2556. DOI: https://doi.org/10.1109/COMST.2021.3117338

[20] Daniel Schlette, Philip Empl, Marco Caselli, Thomas Schreck, and Günther Pernul. 2023. Do you play it by the books? A study on incident response playbooks and influencing factors. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 60–60.

[21] Sandra Schmitz-Berndt. 2023. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity* 9, 1 (2023), tyad009. DOI: https://doi.org/10.1093/cybsec/tyad009

[22] Ankit Shah, Rajesh Ganesan, Sushil Jajodia, and Hasan Cam. 2018. Optimal assignment of sensors to analysts in a cybersecurity operations center. *IEEE Systems Journal* 13, 1 (2018), 1060–1071.

[23] Avi Shaked, Yulia Cherdantseva, and Pete Burnap. 2022. Model-based incident response playbooks. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–7.

[24] Muhammad Sheeraz, Muhammad Arsalan Paracha, Mansoor Ul Haque, Muhammad Hanif Durad, Syed Muhammad Mohsin, Shahab S. Band, and Amir Mosavi. 2023. Effective security monitoring using efficient SIEM architecture. *Human-centric Computing and Information Sciences* 13 (2023), 1–18.
[25] Jonathan M. Spring and Phyllis Illari. 2021. Review of human decision-making during computer security incident analysis. *Digital Threats: Research and Practice* 2, 2 (2021), 1–47.
[26] Tines. 2022. *Voice of the SOC Analyst*. Retrieved March 22, 2024 from https://www.tines.com/reports/voice-of-the-soc-analyst
[27] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. 2020. Security operations center: A systematic study and open challenges. *IEEE Access* 8 (2020), 227756–227779.
[28] Thomas D Wagner, Khaled Mahbub, Esther Palomar, and Ali E Abdallah. 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security* 87 (2019), 101589.
[29] Matthias Weidlich, Gero Decker, Alexander Großkopf, and Mathias Weske. 2008. BPEL to BPMN: The myth of a straight-forward mapping. In *Proceedings of the International Concerence on the Move to Meaningful Internet Systems (OTM '08)*. Springer, 265–282.

Received 5 May 2024; revised 31 July 2024; accepted 5 August 2024