

Towards Intelligent Incident Response: A Review of Adaptive and Automated Planning and Orchestration Approaches

Abir Benhizia, Abir Laraba, Mohamed Ali Kandi, Romain Laborde
IRIT, Université de Toulouse, CNRS
Toulouse, France

Abir.Benhizia@irit.fr, Abir.Laraba@irit.fr, Mohamed-Ali.Kandi@irit.fr, Romain.Laborde@irit.fr

Abstract—The growing use of Artificial Intelligence (AI) by cyber attackers is changing the threat landscape. It enables attackers to launch adaptive and rapid attacks, which challenge traditional incident response activities. While Security Operations Centers (SOCs) increasingly leverage standardized processes, automation, and playbooks to sweeten response efficiency, investigation and containment phases continue to be the main bottleneck and the reason that drives elevated Mean Time To Respond (MTTR). This paper examines the latest studies on how to improve these activities' workload, using a global incident response playbook presented as a structured diagram of steps and decisions, based on the BPMN 2.0 standard. We discuss the effectiveness of a set of AI-assisted investigation and playbook/AI-driven containment approaches on MTTR reduction and identify limitations in real-world applicability, especially for long-term containment, and we propose our approach to address these gaps, providing a more adaptive, context-aware framework for sustained incident response.

Index Terms—Cybersecurity, Incident Response, Security Orchestration.

I. INTRODUCTION

IN 2025, Anthropic uncovered a coordinated cyberespionage campaign in which attackers leveraged artificial intelligence (AI) to automate reconnaissance, exploit development, and lateral movement [5]. This incident serves as a primary example of how AI is fundamentally reshaping the cybersecurity topography, augmenting offensive capabilities to unprecedented levels [3]. The observed changes were also highlighted in the annual threat reports from Palo Alto Networks Unit 42 [30] and Elastic Security Labs [13], which indicate that adversaries are increasingly exploiting the speed and scale of AI to conduct attacks that blend seamlessly with legitimate enterprise activity. In this global context, Europe has appeared as one of the primarily target; the 2025 CrowdStrike European Threat Landscape Report identifies the region as a focal point for eCrime, nation-state, and hacktivist actors, with France ranking fourth among the most targeted nations [12].

To counter high-velocity threats, organizations are transitioning from static defenses to structured Incident Response (IR) frameworks. These frameworks use playbooks to translate high-level security standards into threat-specific workflows, providing Security Operations Centers (SOCs) with actionable guidance for real-time detection and analysis [2]. However, the effectiveness of these frameworks is increasingly challenged

by the "AI-savviness" of modern adversaries. AI-assisted attacks enable quick adaptation and automated evasion to security controls, creating dynamic threat profiles that classic, static IR systems—which often cannot learn from past incidents—struggle to manage [4]. Thus, detection alone is no longer sufficient; response mechanisms must evolve to match the speed and adaptability of the attacks they confront.

These changes underscore the need for IR mechanisms that support both investigation and containment in a robust, adaptive manner. Short-term containment, such as isolating compromised assets, blocking suspicious IP addresses, and killing suspicious processes, is increasingly difficult to execute at the pace of AI-driven lateral movement. At the same time, long-term containment, including sustained access control, continuous monitoring, and forensic evidence preservation, remains largely underexplored, leaving organizations vulnerable to recurring threats. While detection technologies have advanced rapidly, an important Mean Time to Respond (MTTR) is still defined by the difficulty of moving from detection to incident understanding, which represents the investigation phase; then to actions to implement, which represents the containment phase. Optimizing these workflows to reduce the MTTR is therefore essential for maintaining operational resilience [21].

Objective: This position paper focuses on the Investigation and Containment phases of incident response. Using Business Process Model and Notation, version 2 (BPMN 2.0) modeled IR global playbook as a reference, we review recent research, assess its impact on MTTR, and identify gaps in workflow automation, highlighting our approach to addressing these gaps through intent-driven playbooks.

The remainder of this paper is organized as follows. Section II introduces Security Operations Centers (SOCs), incident response frameworks, incident response phases, playbooks, and BPMN 2.0 modeling. Section III reviews recent research on the investigation and containment phases, evaluates their impact on MTTR, and identifies main achievements, limitations, and gaps in automation, AI-assisted techniques, and playbook-driven SOC operations. Section IV provides a high-level overview of the adoption of intent-driven adaptive playbooks that aim to enhance long-term containment effectiveness, while highlighting potential avenues for optimization and further research.

The efficiency of IR activities is generally evaluated using time-based metrics. Among these, Mean Time to Respond (MTTR) quantifies the average time needed to investigate, contain, and remediate an incident. Shorter MTTR values are associated with reduced attacker dwell time and enhanced SOC efficacy. Hence, MTTR is used as the main metric to assess improvements proposed by selected research works focusing on the Investigation and Containment phases [25][7].

Despite structured frameworks, automation, and playbooks, challenges remain in reducing response times and enhancing operational efficiency, especially during Investigation and Containment. The subsequent section reviews a set of selected research works that provide methods, tools, or playbook enhancements targeting these two phases, evaluates their impact on MTTR reduction, and identifies remaining gaps and possibilities for future improvements.

III. PROBLEM ANALYSIS AND EXISTING WORKS

A. Investigation Phase

The investigation phase focuses on identifying, analyzing, and understanding security incidents. As illustrated in Figure 1, it encompasses all steps beginning with alert comprehension, followed by contextual enrichment—such as assessing the reputation of Indicators of Compromise (IOCs) and incorporating threat intelligence, incident classification, and the precise determination of the incident type. Enhancements made at each stage directly influence the MTTR.

Historically, the incident response process was primarily manual, counting on analysts' expertise to correlate alerts, interpret and understand the context, and determine appropriate remediation actions [6]. While manual processes offered flexibility in decision-making, they increasingly became difficult to sustain as infrastructure scaled and attack frequency increased, leading to delayed detection and prolonged response times [25].

Early automation efforts focused on data collection, log aggregation, and basic alerting. However, increasingly stealthy attack techniques often rendered traditional SOCs unable to respond promptly, with MTTR extending to multiple days [20]. This led to the adoption of advanced automation tools, including SOAR platforms, Extended Detection and Response (XDR) — which integrates alerts across multiple security layers for centralized detection and response — and AI-assisted methods, which use machine learning to analyze data, detect patterns, and support or automate response actions [9].

The approaches that integrate AI and machine learning have reported measurable improvements in MTTR. For example, authors adapting generative AI and automated agent systems claimed reducing the MTTR by approximately 65% compared to legacy systems by coordinating adaptive actions across diverse data sources [27]. Likewise, AI-driven alert triage, correlation, and automated analysis have been reported to be able to reduce MTTR 22% to 61%, transforming response times from half a day to a few hours while facilitating analyst workload and reducing false positives [7] [29].

When mapped against the phases defined in the BPMN diagram, most investigation-oriented contributions enhance the

initial stages of the workflow: triage, enrichment, and incident type identification. These results, however, remain difficult to generalize; the investigation phase remains cognitively demanding and context sensitive. The reviewed studies, despite the announced improvements, reported that those improvements are primarily based on simulation environments or controlled workflows rather than heterogeneous operational SOCs. In the real world, integration challenges, data quality issues, and the complexity of today's incidents continue to cause delays and uncertainty, limiting the extent to which investigations can be fully automated.

An enhanced investigation does not automatically deliver effective containment. Once the incident type, scope, and impact are set, the response process shifts from exploratory analysis to action-oriented mitigation. This transition marks the shift from investigation to containment, where response activities evolve into more structured, deterministic, and automation-friendly.

B. Containment Phase

The containment phase is different from the investigation as it requires direct intervention in the operational landscape. Following the modeled BPMN workflow (Fig. 1), this transition occurs after incident classification and dedicated playbook selection, and focuses on executing response actions to limit damage, prevent lateral movement, and stabilize affected systems. Unlike the investigation phase, which relies on continuous interpretation and hypothesis testing, containment is defined by repeatable, well-structured mitigation steps, making it particularly suitable for playbook-driven and automated execution [10]. However, this suitability varies significantly between short-term and long-term containment activities.

The majority of incident response playbooks available and used by the industry till now are human-written, providing step-by-step guidance for analysts during containment [14]. While effective for knowledge capture and repeatability, these playbooks are not directly executable by automation platforms. Recent research has explored the LLM-assisted transformation of legacy playbooks into Collaborative Automated Course of Action Operations (CACAO) formats, allowing machine-readable execution that facilitates faster, more consistent, and partially automated response [2]. Such approaches have shown interesting improvements in SOC performance, particularly in reducing MTTR; however, existing studies are largely proof-of-concepts, and real-world validation in operational SOCs remains limited, leaving actual MTTR gains unquantified.

Formal workflow modeling approaches, including Business Process Model and Notation (BPMN), have also been proposed for CACAO playbooks to enhance clarity, consistency, and re-usability [32]. The use of BPMN is very helpful for representing and formalizing workflows graphically and was adopted in our current paper. BPMN supports both short-term mitigation steps and longer-term containment strategies, providing a structured framework for automation. But mapping BPMN to CACAO is not straightforward; similar to CACAO transformations, the evaluation of BPMN-modeled playbooks has been mainly theoretical, with empirical proof in live SOC

environments still scarce. As a result, while these approaches offer powerful conceptual bases for improving automation and MTTR, their practical efficacy in operational settings remains to be fully demonstrated.

The short-term containment represents the first line of defense during an incident. It concentrates on quick and, most of the time, localized, reversible actions such as isolating compromised assets, blocking malicious accounts, and enforcing temporary network controls to control damage and prevent lateral movement. even if containment actions should be mapped to defensive countermeasure knowledge, such as MITRE D3FEND [23]. These actions usually have a limited impact on core business processes, making them well-suited for automation. Consequently, short-term containment measures are well-studied, often benefit from playbook-driven automation, and provide measurable reductions in MTTR [15][17].

The long-term containment, in contrast, represents a set of actions to sustain operational resilience and prevent threat resurgence, ensuring system stabilization and business continuity over extended incident lifecycles [21]. This phase involves implementing durable controls such as network segmentation, access policy restructuring, system hardening, access policy restructuring, system hardening, continuous monitoring, and forensic evidence preservation [26]. These measures, contrary to short-term containment actions, can directly affect service availability, user productivity, and critical business workflows, requiring careful coordination across the enterprise. As a result, long-term containment is significantly more difficult to automate: any automated actions must consider not only security effectiveness but also operational risk, making fully automated execution challenging. Effective implementation also depends on accurate threat scoping and high-quality telemetry; however, approximately 77% of organizations struggle with formal response plan execution due to limited telemetry budgets and resource constraints [1] [19].

While automation holds promise, AI-assisted containment mechanisms still require rigorous human validation to manage the growing complexity of cyber threats and reduce high false-positive rates, which can lead to severe operational disruptions [24]. Moreover, existing process models often fail against adaptive adversaries, leaving residual trust relationships exposed [19].

Overall, while efforts to improve short-term containment enhance immediate mitigation, long-term containment remains underexplored and is often limited by static playbooks. This highlights the need for dynamic, context-aware mechanisms that can evolve alongside sophisticated, multi-stage adversaries and prioritize risks based on real-time environmental context [19] [22].

C. BPMN-Based Mapping of Existing Works

Table I summarizes and maps the overall review of existing works to each sub-phase of the investigation and containment phases.

TABLE I: BPMN-based-Graph gap analysis of existing incident response research

BPMN Element	Existing Coverage	Limitations
Triage	Strong AI/SOAR support	False-positive alerts control
Enrichment	Moderate support	Business-context integration
Incident classification	Moderate AI support	Hallucination and uncertainty handling
Dedicated playbook	CACAO/BPMN support	Static and predefined playbook selection
Short-term containment	Strong automation support	Operational disruption risk
Long-term containment	Weak support	Adaptive sustained containment
Manual intervention	Common in practice	Structured human-in-the-loop support

IV. CONCLUSION AND FUTURE WORKS

AI-driven threats challenge traditional incident response, as investigation and containment contribute to high MTTR. Existing research has shown that automation, artificial intelligence, and structured playbooks can enhance SOC operations and reduce MTTR. Yet, as highlighted in the previous section, the mentioned studies relies on limited or homogeneous datasets and assumes seamless integration within early-adopter SOC environments. Playbook standardization and lifecycle management still need manual intervention, limiting the full potential of automation. As a consequence, the reported MTTR reductions (often between 30–70%) may not generalize across diverse operational contexts.

The current proposed approaches primarily focus on investigation and short-term containment, while long-term strategies, such as sustained access control, continuous monitoring, and forensic evidence preservation, remain underexplored. Existing incident response playbooks are largely procedure-centric and static [28], and network micro-segmentation mechanisms are typically predefined and network-centric, with no unified framework to translate incident intent into adaptive, long-term containment actions [8]. This disconnect limits SOC's ability to enforce security policies dynamically and sustain protection beyond the immediate incident, highlighting a critical gap in extending automation and AI-driven mechanisms to support end-to-end, context-aware incident response.

The core goal of this PhD research is to design intent-driven security playbooks capable of dynamically generating and adapting micro-segmentation policies that support both short-term mitigation and long-term containment. An incident response intent is defined as a high-level security objective that describes the desired containment outcome [11]. It specifies what must be achieved instead of how each technical control should be configured. This approach aims to bridge the gap between playbook-level decision-making and network-level enforcement. Instead of executing only static response steps, the system interprets the incident context and

generates containment policies that can adapt as new evidence is collected [16]. This not only accelerates investigation but also maintains resilience and prevents threat resurgence over extended incident life-cycles.

Other directions can also be pursued in future work, including security and business continuity to allow for response actions to be performed automatically and reduce threats without interfering with business continuity; decision-making under uncertainty to allow the system to reason about noisy and incomplete data and determine allowable levels of risk; risk-aware automation to improve SOAR solutions and incorporate risk measures to determine dynamic actions according to enterprise risk tolerance; and lifecycle-aware incident response solutions with human-in-the-loop capabilities to ensure forensic integrity and allow SOC analysts to direct actions when necessary.

ACKNOWLEDGMENT

This work has been partially supported by the French National Research Agency under the France 2030 label (ANR-22-PECY-0001 and ANR-22-PECY-0008).

REFERENCES

- [1] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville. How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, Aug. 2020. doi: 10.1002/asi.24311.
- [2] M. Akbari Gurabi, L. Nitz, A. Bregar, J. Popanda, C. Siemers, R. Matzutt, and A. Mandal. Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation. *Digital Threats: Research and Practice*, Sept. 2024. doi: 10.1145/3688810.
- [3] Z. O. Akinpelu. Artificial Intelligence in Offensive and Defensive Cybersecurity: Opportunities, Risks, and Ethical Boundaries. *Iconic Research and Engineering Journals*, Aug. 2025. issn: 2456-8880.
- [4] M. Al-Azzawi, D. Doan, T. Sipola, J. Hautamäki, and T. Kokkonen. Red Teaming with Artificial Intelligence-Driven Cyberattacks: A Scoping Review, Mar. 2025. doi: 10.48550/arXiv.2503.19626.
- [5] Anthropic Threat Intelligence. Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign. <https://www.anthropic.com/news/disrupting-AI-espionage>, Nov. 2025. Threat intelligence report.
- [6] K. G. Boamah, A. Asante, A. Timean, and K. F. Okai. Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity. *International Journal of Science and Research Archive*, Oct. 2025. doi: 10.30574/ijrsra.2025.17.1.2933.
- [7] R. A. Bridges, A. E. Rice, S. Oesch, J. A. Nichols, C. Watson, K. Spakes, S. Norem, M. Huettel, B. Jewell, B. Weber, C. Gannon, O. Bizovi, S. C. Hollifield, and S. Erwin. Testing SOAR Tools in Use. *Computers & Security*, June 2023. doi: 10.1016/j.cose.2023.103201.
- [8] D. Canavese, R. Laborde, A. Laraba, A. Ferreira, and A. Benzekri. Game of Zones: An Automated Intent-Based Network Micro-segmentation Methodology. *IEEE Symposium on Network Operations and Management*, May 2025. doi: 10.1109/NOMS57970.2025.11073630.
- [9] S. A. Chamkar, Y. Maleh, and N. Gherabi. SOC Analyst Performance Metrics: Towards an optimal performance model. *EDPACS*, Sept. 2023. doi: 10.1080/07366981.2023.2259046.
- [10] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. Computer Security Incident Handling Guide. Nist special publication, National Institute of Standards and Technology, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.
- [11] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura. Intent-Based Networking - Concepts and Definitions. Technical report, RFC Editor, Oct. 2022. doi: 10.17487/RFC9315.
- [12] CrowdStrike Reserach Team. CrowdStrike 2025 European Threat Landscape Report. <https://www.crowdstrike.com/explore/crowdstrike-content/crowdstrike-2025-european-threat-landscape-report/>, 2025.
- [13] Elastic security Labs. Elastic-global-threat-report-2025. <https://www.elastic.co/resources/security/report/global-threat-report>, 2025.
- [14] P. Empl, D. Schlette, L. Stöger, et al. Generating ICS vulnerability playbooks with open standards. *International Journal of Information Security*, Dec. 2023. doi: 10.1007/s10207-023-00760-5.
- [15] Ismail, R. Kurnia, Z. A. Brata, G. A. Nelistiani, S. Heo, H. Kim, and H. Kim. Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence. *Information*, Apr. 2025. doi: 10.3390/info16050365.
- [16] B. Kabbani, R. Laborde, F. Barrere, and A. Benzekri. Specification and Enforcement of Dynamic Authorization Policies Oriented by Situations. In *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, May 2014. doi: 10.1109/NTMS.2014.6814050.
- [17] J. Kinyua and L. Awuah. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*, Jan. 2021. doi: 10.32604/iasc.2021.016240.
- [18] P. Kral. The Incident Handler's Handbook: GIAC (GCIH) Gold Certification. <https://sansorg.egnyte.com/dl/SzUc95nE0x>, Dec. 2011.
- [19] C. Luo, J. Goncalves, E. Velloso, and V. Kostakos. A Survey of Context Simulation for Testing Mobile Context-Aware Applications. *ACM Comput. Surv.*, Feb. 2020. doi: 10.1145/3372788.
- [20] S. Mahajan, M. Khurana, and V. V. Estrela. Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection. In *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*,

- June 2024. doi: 10.1002/9781394196470.fmatter.
- [21] G. Malik. Business Continuity & Incident Response. *Journal of Information Systems Engineering and Management*, Apr. 2025. doi: 10.52783/jisem.v10i45s.8891.
 - [22] P. Maynard, Y. Cherdantseva, A. Shaked, P. Burnap, and A. Mehmood. Consistent and Compatible Modelling of Cyber Intrusions and Incident Response Demonstrated in the Context of Malware Attacks on Critical Infrastructure. *Journal of Cybersecurity and Privacy*, June 2026. doi: <https://www.mdpi.com/2624-800X/6/4/109>.
 - [23] MITRE. MITRE D3FEND: A Knowledge Graph of Cybersecurity Countermeasures. <https://d3fend.mitre.org/>. Accessed 2026-06-28.
 - [24] N. Mohamed. Cutting-edge advances in AI and ML for cybersecurity: a comprehensive review of emerging trends and future directions. *Cogent Business & Management*, Dec. 2025. doi: 10.1080/23311975.2025.2518496.
 - [25] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone. Incident response recommendations and considerations for cybersecurity risk management: A csf 2.0 community profile. NIST Special Publication 800-61 Rev. 3, National Institute of Standards and Technology, Apr. 2025. doi: 10.6028/NIST.SP.800-61r3.
 - [26] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero Trust Architecture. Technical report, National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
 - [27] S. Roy. AgenticCyber: A GenAI-Powered Multi-Agent System for Multimodal Threat Detection and Adaptive Response in Cybersecurity, Dec. 2025. doi: 10.48550/arXiv.2512.06396.
 - [28] D. Schlette, P. Empl, M. Caselli, T. Schreck, and G. Pernul. Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors. In *2024 IEEE Symposium on Security and Privacy (SP)*, May 2024. doi: 10.1109/SP54263.2024.00060.
 - [29] M. Turcotte, F. Labrèche, and S.-O. Paquette. Automated Alert Classification and Triage (AACT): An Intelligent System for the Prioritisation of Cybersecurity Alerts, 2025. doi: 10.48550/arXiv.2505.09843.
 - [30] Unit 42. 2025 Unit 42 Global Incident Response Report. <https://www.paloaltonetworks.com/engage/unit42-2025-global-incident-response-report>, 2025.
 - [31] M. Vielberth. Security Operations Center (SOC). In S. Jajodia, P. Samarati, and M. Yung, editors, *Encyclopedia of Cryptography, Security and Privacy*. Springer Berlin Heidelberg, Feb. 2021. doi: 10.1007/978-3-642-27739-9_1680-1.
 - [32] M. Zych, V. Mavroeidis, K. Fysarakis, and M. Athanatos. Reviewing BPMN as a Modeling Notation for CACAO Security Playbooks. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, July 2023. doi: 10.1109/CSR57506.2023.10224922.