Empirical Study on Automation, AI Trust, and Framework Readiness in Cybersecurity Incident Response

Olufunsho Falowo and Bou Abdo Jacques *

Posted Date: 5 December 2025

doi: 10.20944/preprints202512.0348.v1

Keywords: incident response; artificial intelligence; automation; trust in AI; cybersecurity frameworks; SOAR; AI governance; survey study; digital ethics; framework modernization

 doi:10.20944/preprints202512.0348.v1

Article

Empirical Study on Automation, AI Trust, and Framework Readiness in Cybersecurity Incident Response

Olufunsho Falowo * and Bou Abdo Jacques *

School of Information Technology, University of Cincinnati, Ohio United States
* Correspondence: falowooi@mail.uc.edu (O.F.); bouabdjs@ucmail.uc.edu (B.J.)

Abstract

The accelerating integration of artificial intelligence (AI) into cybersecurity operations has introduced new challenges and opportunities for modernizing incident response (IR) practices. This study explores how cybersecurity practitioners perceive the adoption of intelligent automation and the readiness of legacy frameworks to address AI-driven threats. A structured, two-part quantitative survey was conducted among 194 U.S.-based professionals, capturing perceptions on operational effectiveness, trust in autonomous systems, and the adequacy of frameworks such as NIST and SANS. Using binary response formats and psychometric validation items, the study quantified views on AI's role in reducing mean time to detect and respond, willingness to delegate actions to autonomous agents, and the perceived obsolescence of static playbooks. Findings indicate broad support for the modernization of incident response frameworks to better align with emerging AI capabilities and evolving operational demands. The results reveal a clear demand for modular, adaptive frameworks that integrate AI-specific risk models and decision auditability. These insights provide empirical grounding for the design of next-generation IR models and contribute to the strategic discourse on aligning automation capabilities with ethical, scalable, and operationally effective cybersecurity response.

Keywords: incident response; artificial intelligence; automation; trust in AI; cybersecurity frameworks; SOAR; AI governance; survey study; digital ethics; framework modernization

1. Introduction

This study extends the conceptual foundation established in prior research [1–4], which collectively highlight the growing complexity and frequency of cybersecurity incidents and the corresponding need to rethink incident response (IR) strategies in an AI-driven threat landscape. Earlier work, particularly [4], examined the technical, administrative, and hybrid capabilities that shape current IR practices, revealing both strengths and significant capability gaps. Building on these insights, the present study moves beyond literature-based analysis by incorporating practitioner-informed evidence through a targeted survey that captures real-world perceptions of automation, AI trust, and the readiness of existing frameworks for modernization.

The survey instrument developed for this study was carefully constructed to explore the evolving intersection between intelligent automation and incident response. It includes items designed to evaluate whether existing tools are sufficient to address AI-driven threats, the extent to which organizations are adopting agentic AI, and the effectiveness of these tools in reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Additional questions assess levels of trust in autonomous decision-making, perceptions of AI's impact on traditional IR playbooks, and the degree to which organizations are investing in workforce retraining. The survey also explores whether current regulatory frameworks are keeping pace with the rapid advancement of AI technologies.

By translating theoretical debates into quantifiable practitioner perspectives, this study provides a data-driven lens on the current state of IR transformation. The responses collected offer empirical

 doi:10.20944/preprints202512.0348.v1

validation or challenge to assumptions raised in earlier studies [1–4], particularly regarding automation efficacy, trust thresholds, and AI integration into IR workflows. This study plays a pivotal role in connecting theory to practice. It serves as the empirical engine that powers the framework innovation will be explored in fufure works.

2. Background Literature

2.1. Efficacy of Current Automation Tools

The integration of automation into cybersecurity practices has evolved over several decades, beginning with basic rule-based intrusion detection systems and maturing into today's AI-enhanced, context-aware platforms [5,6]. Initially, automation was used primarily to reduce repetitive manual tasks, such as log analysis and alert triage. However, as cyber threats became more sophisticated and voluminous, the limitations of manual intervention became clear. This led to increased investments in automation not only as a support mechanism but also as a critical component of active defense strategies. Today, automation is expected to play a central role in detection, response, containment, and even predictive defense mechanisms.

A growing body of interdisciplinary literature now examines the efficacy of these automation tools from technical, operational, and organizational perspectives. Scholars are exploring how AI-driven automation impacts key performance metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), how it affects analyst workload and cognitive fatigue, and how organizations calibrate trust in automated decisions [7,8]. For instance, another paper echoes detection and incident orchestration as rapidly advancing areas in security automation. Other studies report that mature organizations leveraging intelligent automation have successfully reduced MTTR notably. Researchers also link optimized MTTD and MTTR with improved service availability, incident containment, and organizational resilience. Collectively, this broad scholarly interest emphasizes the importance of empirically evaluating whether cybersecurity professionals perceive current automation tools as effective, adaptable, and capable of meeting the demands of today's dynamic threat landscape.

2.2. Integration of Agentic AI in IR Workflows

The integration of agentic artificial intelligence, which refers to AI systems capable of making autonomous decisions, is beginning to reshape the structure and expectations of incident response workflows [9]. Although this remains a relatively new frontier, there is growing interest within the cybersecurity community in exploring how these systems can enhance operational agility and threat containment. As adversaries increasingly use AI to launch faster and more evasive attacks, many organizations are starting to recognize the strategic need to respond with equally advanced AI-enabled defenses.

Academic research is actively examining how agentic AI might support or automate various stages of the incident response lifecycle, including triage, containment, and escalation. New models propose leveraging large language models, context-aware threat intelligence, and collaborative frameworks that combine human expertise with machine efficiency [9–11]. While full autonomy remains a subject of careful consideration, many organizations appear open to piloting co-managed or semi-autonomous solutions that extend the capacity of security teams while preserving human oversight. This reflects a broader change in mindset, where AI is increasingly seen not only as a tool for attackers but also as a necessary asset for defenders. Understanding how organizations prepare for and implement agentic AI is critical for evaluating the future direction of intelligent incident response.

2.3. Impact of Automation on MTTD/MTTR

Research across the cybersecurity field has shown that automation can significantly improve how quickly threats are detected and resolved. Two important measures often used to evaluate this are Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) [7,8]. When parts of the response process, such as identifying threats, investigating alerts, and taking action, are automated,

 doi:10.20944/preprints202512.0348.v1

organizations can react much more quickly. This faster reaction reduces the chances that an attack will spread or cause serious damage.

Beyond just speed, quicker detection and response can also bring wider benefits. Companies that respond faster to threats tend to experience fewer disruptions, lower costs from outages, and greater trust from customers and stakeholders. These advantages make it important to examine how cybersecurity teams feel about the effectiveness of automation in their day-to-day work. Understanding their views can help clarify whether automation is delivering the real-world improvements that many experts believe it can.

2.4. Trust and Risk Perception in AI-Driven Decisions

Trust is one of the biggest challenges when it comes to using artificial intelligence (AI) in cybersecurity [12], especially in situations where quick and accurate decisions are critical. While company leaders often support the use of AI to improve speed and efficiency, many frontline cybersecurity professionals are still cautious. Some worry about letting AI make decisions without a human double-checking the outcome. Their concerns often include the risk of AI making wrong judgments, being unpredictable, or not showing clearly how it reached its conclusions [12–14].

Researchers share these concerns and have highlighted several issues that can arise when AI is used in sensitive security situations. For example, AI systems can sometimes be tricked by specially crafted data or make decisions based on patterns that humans cannot see or understand [12–14]. Because of this, experts agree that it is important to have safety checks in place. These may include rules to guide AI behavior, the ability to track how decisions are made, and keeping humans involved in the process. Understanding how much cybersecurity professionals trust AI, and what risks they see, is an important step in deciding how and when these tools should be used.

2.5. Shifts in Playbooks, Training, and Regulation

The growing use of artificial intelligence and automation in cybersecurity is leading many organizations to rethink how they respond to security incidents [15,16]. There are many evidents that indicate that traditional methods that once relied heavily on manual decision-making and fixed procedures are no longer sufficient in a landscape where cyber threats evolve quickly and AI is part of both the problem and the solution. As a result, companies are beginning to revise their playbooks, which are the step-by-step plans used during a cyberattack, to better reflect how AI tools are being used to detect and respond to threats in real time [17,18].

Alongside these changes, there is an increasing focus on training and upskilling the cybersecurity workforce [19]. Many professionals now need to learn how to work alongside AI systems, understand their outputs, and make informed decisions when AI recommends a course of action. This shift requires not only technical training but also a broader understanding of how to manage new types of risks that come with AI-driven operations [19]. As a result, organizations are investing in reskilling programs that prepare analysts and security teams for these modern and AI-enhanced environments.

At the same time, there are growing conversations about whether existing laws, regulations, and industry guidelines are keeping up with the pace of technological change [20]. As AI becomes more involved in cybersecurity, questions arise about who is responsible when something goes wrong, how decisions made by AI can be reviewed, and what safeguards are necessary to ensure ethical use. Understanding whether organizations are adapting both their internal training programs and their external compliance efforts is essential for building future strategies that are not only effective but also responsible and trustworthy in the age of intelligent automation.

2.6. Research Gap: Fragmented SOAR Integration and Underutilized Automation

Despite increased discussions in Security Orchestration, Automation, and Response (SOAR) technologies, many organizations still face considerable barriers in effectively integrating these solutions into everyday incident response workflows, to the extent of reducing the upward trending nature of security threats; this claim is echoed in the literature reviewed in prior works [1–4]. These difficulties often stem

 doi:10.20944/preprints202512.0348.v1

from fragmented tool ecosystems, non-standardized or immature playbooks, and poor interoperability across platforms. As a consequence, automation is often under-deployed in critical phases like detection, triage, and containment, diminishing its potential to reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). With reference to the these papers [1–4], this study identifies a clear research gap in understanding how industry practitioners are navigating these integration challenges, and to what extent current SOAR deployments are aligned with modern threats and AI-enhanced workflows. By empirically examining these dynamics, this study seeks to illuminate the operational realities of automation uptake and orchestration within diverse cybersecurity environments.

2.7. Research Questions

1. What are the emerging priorities and expectations of cybersecurity teams regarding automation and artificial intelligence integration in incident response practices? This question focuses on the operational dimensions, such as SOAR adoption, agentic AI use, MTTD/MTTR reduction, and trust in AI. This research question is captured by the survey questions (Table 3.2). It also attempt to addresses the above research gap (Fragmented SOAR Integration and Underutilized Automation).
2. To what extent do cybersecurity professionals perceive existing incident response frameworks as adequate for modernization in the age of AI-driven threats? This question targets framework evaluation and modernization, aligning with the set of survey questions described in the methodology section of this study. It also reflects emphasis on assessing adaptability, ethical alignment, and the scalability of frameworks like NIST and SANS.

3. Methodology

3.1. Methodology Overview

This study adopts a structured, quantitative survey [21] design to investigate two core research questions related to automation, AI trust, and the modernization readiness of existing incident response frameworks. To address the first research question, the methodology incorporates a dedicated set of ten survey items aimed at capturing practitioner perspectives on operational automation priorities. These questions focus on beliefs about the effectiveness of current automation tools, the adoption of agentic AI systems, expectations around reductions in MTTD and MTTR, trust in autonomous decision-making, and perceptions of whether AI-enabled workflows influence the relevance of traditional incident response playbooks. The exclusive use of Yes or No responses ensures clarity, reduces interpretive differences, and enables the aggregation of consistent and comparable quantitative insights.

To address the second research question, an additional set of ten survey items was developed to evaluate practitioner perceptions of existing incident response frameworks and their readiness for modernization in an AI-driven environment. These items explore attitudes toward lifecycle flexibility, governance alignment, ethical safeguards, scalability, regulatory adequacy, and the need for updated classifications of automation tools. The separation of the survey into two focused parts ensures that the methodology captures both operational realities and framework-level expectations. It also provides a structured means of linking practitioner sentiment to the broader modernization themes. Together, these two survey components offer an integrated and empirically grounded approach to understanding how AI is reshaping the landscape of incident response practices.

3.2. Sampling Strategy and Statistical Significance

To ensure generalizability of the findings, the study targets a statistically significant sample of not less than 140 cybersecurity and IT leaders. This sample size was calculated using a 95 percent confidence level, a 4.97 percent margin of error, and a 10 percent response rate from the estimated U.S. population of 613,500 Computer and Information Systems Managers [22]. The survey design complies fully with ethical research protocols and has been approved by the University of Cincinnati Institutional Review Board (IRB). All responses are fully anonymized, with no collection of IP addresses, geographic

 doi:10.20944/preprints202512.0348.v1

location, or contact details, thus ensuring the privacy and security of all participants while encouraging honest and unbiased feedback on automation readiness and industry expectations.

3.2.1. Statistical Significance & Sample Size Calculation

As briefly mentioned in prior paragraph, according to the United States Bureau of Labor Statistics [22], there were approximately 613,500 Computer and Information Systems Manager positions in 2023, with a projected job outlook growth of 17% from 2023 to 2033 (classified as much faster than average). Therefore, with reference to this study, this Bureau of Labor Statistics' figure serves as the benchmark population for identifying and surveying IT leaders in the United States for the purpose of this study. To determine a statistically significant sample size, we applied a 95% confidence level, a 4.97% margin of error, and a 10% response proportion from the general population of 613,500. Based on these parameters and standard sample size calculation for finite populations, the resulting required sample size of IT leaders to be surveyed is approximately 140. Refer to the detail calculation below.

To determine the appropriate sample size for surveying 10% of a general population of 613,500 individuals, we used the standard sample size formula for finite populations. We set a confidence level of 95% (z = 1.96), a margin of error of 4.97% (e = 0.0497), and a response proportion (p) of 0.10. The formula for calculating the sample size n is as follows:

$$n = \frac{\left(\frac{z^2 \cdot p \cdot (1-p)}{e^2}\right)}{1 + \left(\frac{z^2 \cdot p \cdot (1-p)}{e^2 \cdot N}\right)}$$

Substituting the values:

$$z = 1.96, \quad p = 0.10, \quad e = 0.0497, \quad N = 613{,}500$$

Step 1: Compute the numerator of the formula:

$$z^2 \cdot p \cdot (1-p) = 1.96^2 \cdot 0.10 \cdot (1 - 0.10) = 3.8416 \cdot 0.10 \cdot 0.90 = 0.345744$$

$$\frac{0.345744}{0.0497^2} = \frac{0.345744}{0.00247009} \approx 139.974$$

Step 2: Compute the denominator:

$$1 + \left(\frac{0.345744}{0.00247009 \cdot 613{,}500}\right) = 1 + \left(\frac{0.345744}{1515.2615}\right) \approx 1 + 0.0002281 = 1.0002281$$

Step 3: Final sample size calculation:

$$n = \frac{139.974}{1.0002281} \approx 139.942$$

Conclusion: Based on this calculation, a sample size of approximately **140 respondents** is statistically sufficient to achieve a 95% confidence level with a 4.97% margin of error when surveying a target population of 613,500, assuming a 10% response proportion.

3.3. Survey Part One

Variables and Survey Questions

Binary Variables (Yes/No)

- Belief in current automation tools keeping pace with AI-driven threats
- Adoption of agentic AI systems in incident response
- Perceived reduction in MTTD/MTTR due to automation
- Trust in AI-driven decision-making without human intervention
- Support for autonomous triage and containment
- Belief that benefits of AI-driven automation outweigh the risks

 doi:10.20944/preprints202512.0348.v1

- Perception that AI workflows make traditional IR playbooks obsolete
- Evidence of retraining efforts for managing AI-powered tools
- Belief that regulatory frameworks lag behind automation trends
- Support for new classification/taxonomy of agentic AI tools

Argument for Use of Binary Variables (Yes/No)

The use of binary (Yes/No) variables [23] in this study is a deliberate methodological choice to support the empirical objectives of a broader work. This format promotes clarity, reduces interpretive variance, and enables consistent quantification of practitioner perceptions regarding automation readiness, trust in AI, and organizational alignment. By focusing on aggregate frequencies and group differences, the binary structure allows for efficient statistical analysis and comparison across respondents, surfacing notable adoption trends and trust dynamics. These variables serve as the foundation for the survey questions and provide a reliable means of translating subjective views into actionable data. Ultimately, the insights generated from this approach directly support the broader contribution of this work by identifying where existing incident response workflows may fall short and by informing the development of scalable, automation-ready frameworks.

Survey Questions

Table 1. Survey: Assessing Industry Expectations and Adoption of Automation in Incident Response.

#	Question	Reason for Inclusion
1	Do you believe current automation tools can keep pace with evolving AI-driven attack techniques?	Gauges confidence in existing automation's ability to evolve alongside AI-enabled threats.
2	Are you currently integrating agentic AI systems into your cybersecurity incident response processes?	Measures adoption of advanced AI technologies beyond basic automation.
3	Has automation significantly reduced the mean time to detect/respond (MTTD/MTTR) incidents in your org?	Evaluates perceived effectiveness and ROI of automation in practice.
4	Do you trust AI-driven decision-making without human intervention in high-stakes incident scenarios?	Assesses trust threshold for agentic AI autonomy.
5	Would you support a move toward autonomous incident triage and containment without analyst oversight?	Determines openness to full-cycle automation.
6	Do you believe the benefits of AI-driven automation outweigh the risks of false positives/negatives?	Evaluates industry risk tolerance in balancing speed vs. accuracy.
7	Are AI workflows making your current IR playbooks obsolete or less relevant?	Explores whether traditional IR documentation is misaligned with current AI capabilities.
8	Are security teams in your organization undergoing retraining to manage AI-powered automation tools?	Captures organizational investment in upskilling for AI-augmented operations.
9	Do you believe regulatory frameworks are lagging behind AI-driven cybersecurity automation trends?	Surfaces gaps between innovation and regulation/compliance.
10	Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?	Probes whether current language/frameworks are insufficient to describe new AI capabilities.

Note. These questions were designed to explore automation trends, trust in AI, organizational readiness, and framework adequacy in light of agentic AI adoption.

 doi:10.20944/preprints202512.0348.v1

The Quality of the Survey Questions

The quality of the survey questions in this study is grounded in their direct alignment with the core constructs of AI-driven automation adoption in incident response. Each of the ten binary questions was carefully designed to address a specific operational dimension, including automation readiness, trust in autonomous decision-making, MTTD/MTTR effectiveness, upskilling efforts, and regulatory adequacy. This targeted approach ensures conceptual coherence across all items and supports both descriptive and inferential analysis. Limiting the survey to ten questions reflects a strategic decision to maintain respondent engagement, minimize fatigue, and maximize data integrity. By focusing on depth rather than quantity, the survey captures high-value practitioner insights without compromising analytical rigor. The resulting data provide a reliable foundation for understanding current industry practices and informing actionable recommendations for intelligent automation in cybersecurity operations.

Psychometrics Questions to Validate Participant Responses [24,25]

To enhance the reliability and interpretive validity of the survey findings, psychometrics-based statements were included to triangulate and reinforce key constructs assessed in the questions. These items serve as internal consistency checks and are intended to validate responses. These psychometric items help confirm that participants' responses are not only consistent but also grounded in practical organizational realities, thereby strengthening the survey's construct validity.

3.4. Survey Part Two

Variables and Survey Questions

Binary Variables (Yes/No)

- Belief in NIST's adequacy for addressing AI-driven threats
- Customization or extension of traditional frameworks like NIST or SANS
- Perception that the IR lifecycle is too rigid for modern threats
- Belief that current IR frameworks are scalable for autonomous response
- Belief that current frameworks lack ethical guidance on AI decisions
- Preference for simpler, modular IR frameworks
- Perception that tabletop exercises fail to model AI-powered threats
- Difficulty mapping AI/ML indicators into current frameworks
- Existence of a separate AI threat modeling process
- Support for industry-wide revision of IR frameworks to include AI

Argument for Use of Binary Variables (Yes/No)

The use of binary (Yes/No) variables [23] in this study provides a structured and efficient way to assess practitioners' views on the readiness of existing incident response frameworks for AI-driven threats. Each variable corresponds to a specific, measurable dimension of framework evaluation, including perceptions of rigidity, scalability, ethical gaps, and the capacity to support AI and machine learning processes. This binary format reduces ambiguity, enhances response clarity, and allows for easy aggregation of data across different organizational settings. By focusing on the presence or absence of key capabilities such as ethical oversight or modularity, the binary approach supports comparative analysis and helps identify consistent patterns in practitioner sentiment. These variables form the empirical basis for evaluating the suitability of frameworks like NIST and SANS and play a critical role in guiding the development of modernization strategies proposed in this research.

The Quality of the Survey Questions

As already echoed in prior paragraphs and sections, the quality of these ten survey questions lies in their clear alignment with core dimensions necessary for evaluating the adaptability of legacy incident response frameworks in the age of AI-driven threats. Each question targets a specific operational,

 doi:10.20944/preprints202512.0348.v1

structural, or governance-related variable, including flexibility, scalability, ethical oversight, and support for AI-specific processes such as threat modeling and autonomous decision-making. The binary Yes or No format ensures simplicity and consistency in responses, which supports clear statistical interpretation and comparison across participants. The questions are theoretically grounded, practically relevant, and designed to surface meaningful practitioner insights that can guide actionable framework enhancements. Together, they provide a focused yet comprehensive diagnostic tool to assess whether frameworks like NIST and SANS are keeping pace with evolving cybersecurity demands.

Table 2. Survey: Effectiveness of Traditional IR Frameworks in the Age of AI-Driven Attacks.

#	Question	Reason for Inclusion
1	Do you think the NIST IR framework adequately addresses threats posed by AI-driven attacks?	Evaluates continued relevance of NIST against emerging threats.
2	Has your organization customized or extended traditional frameworks like SANS or NIST to accommodate AI-based threats?	Checks for deviation from or augmentation of standard models.
3	Do you find the existing IR lifecycle (Preparation → Detection → Containment → Eradication → Recovery) too rigid today?	Tests perceptions of flexibility within current frameworks.
4	Are current IR frameworks scalable enough to support autonomous or AI-assisted incident resolution at enterprise scale?	Probes scalability limitations of traditional frameworks.
5	Do you believe that current frameworks lack guidance on ethical oversight of AI-agent decisions during incidents?	Explores a normative gap in the frameworks regarding AI governance.
6	Would a simpler, modular incident response framework be more effective for AI-era threats?	Seeks appetite for a redesign focused on agility and simplicity.
7	Have traditional tabletop exercises failed to capture the complexity of AI-powered threat scenarios?	Identifies simulation limitations in capturing AI-driven dynamics.
8	Do you find it challenging to map AI or ML threat indicators (e.g., model drift) into existing framework categories?	Investigates the structural mapping difficulty of modern indicators into legacy frameworks.
9	Does your organization maintain a separate AI threat modeling process outside the standard IR framework?	Looks for emergence of parallel models to supplement perceived framework gaps.
10	Would you support industry-wide revision of existing IR frameworks to formally include AI/agentic threat dimensions?	Assesses willingness to collectively redefine standards.

This table summarizes survey items designed to assess the perceived effectiveness of traditional incident response frameworks in the context of emerging AI-driven threat dynamics.

Psychometrics Questions to Validate Participant Responses [24,25]

To enhance the reliability and interpretive validity of the survey findings, psychometrics-based statements were included to triangulate and reinforce key constructs assessed in the questions. These items serve as internal consistency checks and are intended to validate responses. These psychometric items help confirm that participants' responses are not only consistent but also grounded in practical organizational realities, thereby strengthening the survey's construct validity.

3.5. Survey Part Two

Variables and Survey Questions

Binary Variables (Yes/No)

- Belief in NIST's adequacy for addressing AI-driven threats
- Customization or extension of traditional frameworks like NIST or SANS
- Perception that the IR lifecycle is too rigid for modern threats
- Belief that current IR frameworks are scalable for autonomous response
- Belief that current frameworks lack ethical guidance on AI decisions

 doi:10.20944/preprints202512.0348.v1

- Preference for simpler, modular IR frameworks
- Perception that tabletop exercises fail to model AI-powered threats
- Difficulty mapping AI/ML indicators into current frameworks
- Existence of a separate AI threat modeling process
- Support for industry-wide revision of IR frameworks to include AI

Argument for Use of Binary Variables (Yes/No)

The use of binary (Yes/No) variables [23] in this study provides a structured and efficient way to assess practitioners' views on the readiness of existing incident response frameworks for AI-driven threats. Each variable corresponds to a specific, measurable dimension of framework evaluation, including perceptions of rigidity, scalability, ethical gaps, and the capacity to support AI and machine learning processes. This binary format reduces ambiguity, enhances response clarity, and allows for easy aggregation of data across different organizational settings. By focusing on the presence or absence of key capabilities such as ethical oversight or modularity, the binary approach supports comparative analysis and helps identify consistent patterns in practitioner sentiment. These variables form the empirical basis for evaluating the suitability of frameworks like NIST and SANS and play a critical role in guiding the development of modernization strategies proposed in this study.

Table 3. Survey Questions on Effectiveness of Traditional IR Frameworks in the Age of AI-Driven Attacks

#	Survey Question	Reason for Inclusion
1	Do you think the NIST IR framework adequately addresses threats posed by AI-driven attacks?	Evaluates continued relevance of NIST against emerging threats.
2	Has your organization customized or extended traditional frameworks like SANS or NIST to accommodate AI-based threats?	Checks for deviation from or augmentation of standard models.
3	Do you find the existing IR lifecycle (Preparation → Detection → Containment → Eradication → Recovery) too rigid today?	Tests perceptions of flexibility within current frameworks.
4	Are current IR frameworks scalable enough to support autonomous or AI-assisted incident resolution at enterprise scale?	Probes scalability limitations of traditional frameworks.
5	Do you believe that current frameworks lack guidance on ethical oversight of AI-agent decisions during incidents?	Explores a normative gap in the frameworks regarding AI governance.
6	Would a simpler, modular incident response framework be more effective for AI-era threats?	Seeks appetite for a redesign focused on agility and simplicity.
7	Have traditional tabletop exercises failed to capture the complexity of AI-powered threat scenarios?	Identifies simulation limitations in capturing AI-driven dynamics.
8	Do you find it challenging to map AI or ML threat indicators (e.g., model drift) into existing framework categories?	Investigates the structural mapping difficulty of modern indicators into legacy frameworks.
9	Does your organization maintain a separate AI threat modeling process outside the standard IR framework?	Looks for emergence of parallel models to supplement perceived framework gaps.
10	Would you support industry-wide revision of existing IR frameworks to formally include AI/agentic threat dimensions?	Assesses willingness to collectively redefine standards.

This table presents survey questions used to assess perceptions of traditional IR framework effectiveness in the context of emerging AI-driven cybersecurity challenges.

The Quality of the Survey Questions

As already echoed in prior paragraphs and sections, the quality of these ten survey questions lies in their clear alignment with core dimensions necessary for evaluating the adaptability of legacy incident response frameworks in the age of AI-driven threats. Each question targets a specific operational, structural, or governance-related variable, including flexibility, scalability, ethical oversight, and support

 doi:10.20944/preprints202512.0348.v1

for AI-specific processes such as threat modeling and autonomous decision-making. The binary Yes or No format ensures simplicity and consistency in responses, which supports clear statistical interpretation and comparison across participants. The questions are theoretically grounded, practically relevant, and designed to surface meaningful practitioner insights that can guide actionable framework enhancements. Together, they provide a focused yet comprehensive diagnostic tool to assess whether frameworks like NIST and SANS are keeping pace with evolving cybersecurity demands.

Reliability & Validity

To ensure statistical significance, generalizability, and measurement accuracy, this study incorporates psychometric validation statements alongside a core set of binary survey questions. The targeted sample size of at least 140 respondents was calculated based on a population of over 600,000 IT leaders, yielding a confidence level greater than 95 percent and a margin of error below 4.97 percent. The inclusion of validation statements helps improve the reliability of the instrument by assessing the internal consistency of responses across related constructs. These statements are designed to indirectly validate how participants interpret and respond to key binary questions, strengthening both the credibility and robustness of the findings.

Outreach Strategy for Survey Distribution

This study's outreach strategy focuses on distributing the survey to cybersecurity professionals across the United States. The goal is to reach individuals with practical, field-based experience who can offer meaningful insights into current incident response practices and automation trends. To ensure relevance and diversity, the survey was shared through targeted professional communities and platforms such as LinkedIn cybersecurity groups, ISC2 member forums, ISACA professional networks, and other reputable private practitioner communities online. The survey itself was hosted on Qualtrics, a secure and widely adopted academic survey platform[1]. This approach maximizes participation from qualified respondents and supports the collection of data that aligns closely with the study's research objectives.

4. Results

As echoed in the methodology section, this study received approval from the Institutional Review Board (IRB) of the University of Cincinnati, ensuring full compliance with ethical research standards and protocols.[2] Following approval, a structured survey instrument was designed and distributed to collect empirical data relevant to the study's objectives. The primary target audience comprised professionals in the United States who are actively engaged in cybersecurity or information security roles, ensuring that responses were grounded in real-world operational experience.

Outreach efforts focused on both local and online professional chapters, as well as broader practitioner communities, to achieve diverse and representative participation.[3] The survey remained open from the first week of September 2025 through the first week of October 2025. During this one-month window, a total of 194 valid responses were received, providing a robust dataset for subsequent analysis of trends, perceptions, and readiness levels within the cybersecurity community.

Given the dual focus of this empirical study, the results are presented in two distinct parts: Part 1 summarizes responses to the ten questions addressing Research Question 1 (focused on AI trust and automation), while Part 2 presents findings aligned with Research Question 2 (focused on framework readiness and modernization).[4] Each section provides quantitative summaries, key thematic insights,

[1] The requirements that form the foundation for these survey was approved by the University of Cincinnati Institutional Review Board (IRB) under Protocol ID: `2025-0022-UC`. All responses are anonymous and no personally identifiable information is collected.

[2] IRB approval confirms that participant rights, confidentiality, and informed consent procedures were reviewed and aligned with institutional and federal ethical standards.

[3] Survey invitations were disseminated through LinkedIn posts, practitioner mailing lists, and professional associations such as ISC2 and ISACA to maximize response diversity.

[4] This structure ensures clarity in analysis and helps maintain alignment between survey design and research objectives.

 doi:10.20944/preprints202512.0348.v1

and visualizations that support the interpretation of practitioner sentiment across both operational and strategic dimensions of cybersecurity incident response.

4.1. Use of Diverging Likert and Pie Charts for Visual Clarity

The visualization strategy for the survey results uses a combination of diverging Likert bar charts and pie charts to communicate binary and categorical findings in a clear and intuitive manner.[5] The diverging Likert charts highlight the directional sentiment of responses by visually separating affirmative and negative selections, allowing readers to quickly recognize polarity and degree of alignment. Complementing this, the pie charts reinforce proportionality and distribution, supporting rapid visual comparison across questions. The combined use of these two chart types enhances cognitive accessibility, increases interpretive precision, and ensures strong communicative value for the survey findings presented in this study.

4.2. Survey Result - Part One

4.3. Psychometric Analysis

From a psychometric standpoint, and with reference to Table 4, the survey demonstrates strong internal consistency and construct validity, particularly when examining related items such as "Are you currently integrating agentic AI systems into your cybersecurity incident response processes?" (84% Yes) and "Has automation significantly reduced the mean time to detect/respond (MTTD/MTTR) incidents in your organization?" (92% Yes). The high positive alignment between these items suggests convergent validity, meaning participants who report integrating AI systems also tend to perceive tangible performance gains. This implies that responses are coherent and reflect a shared underlying construct, namely AI-enabled operational efficiency. Conversely, the low trust in fully autonomous decision-making (13% Yes) correlates inversely with support for autonomous triage (37% Yes), indicating discriminant validity as respondents differentiate between efficiency benefits and risk acceptance. Together, these patterns support the reliability of the instrument in capturing nuanced practitioner attitudes toward automation maturity, trust, and governance.

Table 4. Survey Responses on AI-Driven Automation in Cybersecurity Incident Response.

No.	Survey Question	Yes (%)	No (%)
1	Do you believe current automation tools can keep pace with evolving AI-driven attack techniques?	30	70
2	Are you currently integrating agentic AI systems into your cybersecurity incident response processes?	84	16
3	Has automation significantly reduced the mean time to detect/respond (MTTD/MTTR) incidents in your organization?	92	8
4	Do you trust AI-driven decision-making without human intervention in high-stakes incident scenarios?	13	87
5	Would you support a move toward autonomous incident triage and containment without analyst oversight?	37	63
6	Do you believe the benefits of AI-driven automation outweigh the risks of false positives or negatives?	17	83
7	Are AI workflows making your current incident response (IR) playbooks obsolete or less relevant?	20	80
8	Are security teams in your organization undergoing retraining to manage AI-powered automation tools?	74	26
9	Do you believe regulatory frameworks are lagging behind AI-driven cybersecurity automation trends?	41	59
10	Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?	79	21

This table summarizes binary response patterns regarding the readiness, risk perception, and operational impact of AI-driven automation in cybersecurity incident response.

[5] This choice was guided by the need to ensure that both academic and practitioner audiences can immediately interpret trends without relying solely on numerical tables.

 doi:10.20944/preprints202512.0348.v1

This psychometric analysis, this study argues is important because psychometric evaluation in empirical studies ensures that the observed trends are not random but reflect consistent cognitive patterns among respondents. By correlating conceptually linked items, this study assess whether the survey measures distinct yet logically connected constructs, such as automation effectiveness and trust. The coherence between integration and MTTD reduction validates the tool's internal logic, while divergence between trust and autonomy attitudes confirms interpretive soundness. Thus, the survey's response structure demonstrates both reliability (stability across similar constructs) and validity.

4.4. Response to Question #1

With reference to question #1 in Table 4, the charts in Figure 1 collectively reveal that a large majority (70%) of respondents do not believe current automation tools are keeping pace with AI-driven threats, while only 30% express confidence in their adequacy. This contrast suggests that most practitioners perceive a widening capability gap between defensive automation and adversarial innovation. The visualization reinforces the notion that existing tools may require significant evolution, particularly through agentic or adaptive AI integration, to remain effective in rapidly changing threat environments.

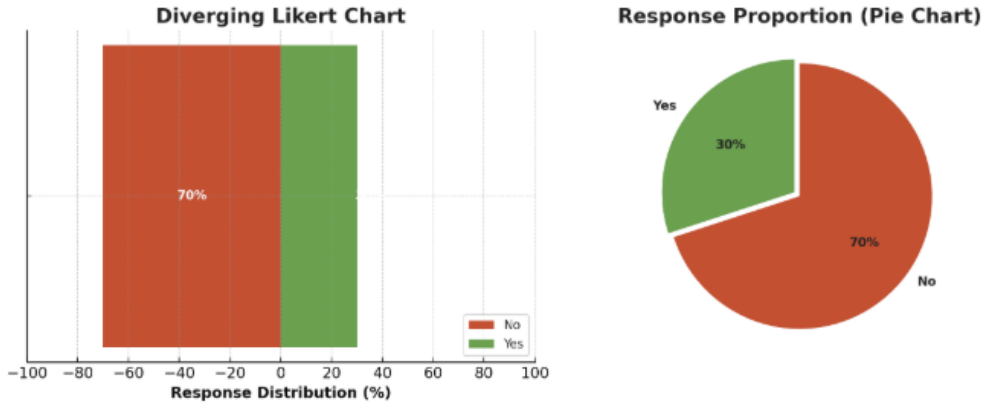

Figure 1. Response to Question #1.

Response to Question #2

With reference to question #2 in Table 4, the charts in Figure 2 show that an overwhelming majority (84%) of respondents reported that their organizations are already integrating agentic AI systems into their cybersecurity incident response processes, while only 16% indicated otherwise. This result suggests that AI integration has moved beyond the experimental phase and is becoming an operational reality for most security teams. The visualization highlights a strong trend toward automation maturity and reflects a growing recognition of AI as an enabler of faster detection, triage, and response within modern security operations.

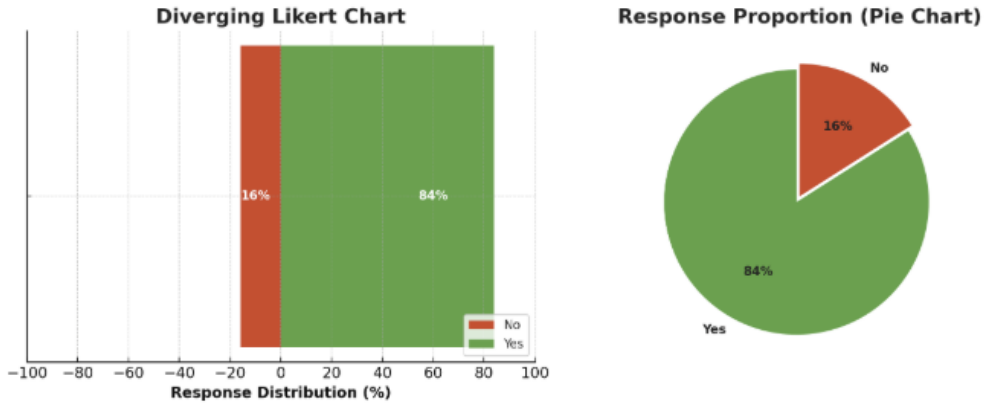

Figure 2. Response to Question #2.

 doi:10.20944/preprints202512.0348.v1

Response to Question #3

With reference to question #3 in Table 4, the charts in Figure 3 indicate that an overwhelming majority (92%) of respondents confirmed that automation has significantly reduced the mean time to detect and respond (MTTD/MTTR) to incidents in their organizations, while only 8% disagreed. This high level of agreement underscores the operational value of automation in accelerating incident response and minimizing dwell time. The visualization reinforces the perception that automation technologies, particularly when supported by AI, are yielding measurable efficiency gains in detection and containment processes within cybersecurity operations.

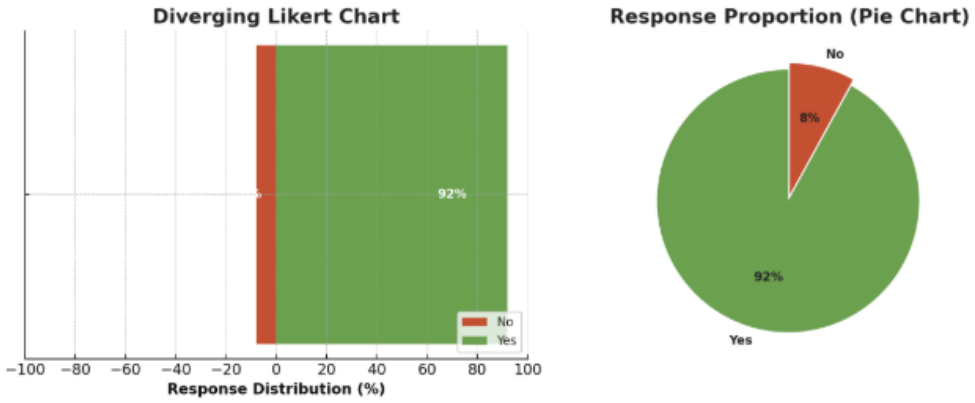

Figure 3. Response to Question #3.

Response to Question #4

With reference to question #4 in Table 4, the charts in Figure 4 reveal that only 13% of respondents expressed trust in AI-driven decision-making without human intervention, while a significant majority of 87% indicated distrust. This strong divergence highlights a persistent skepticism toward fully autonomous decision systems in high-stakes cybersecurity contexts. The visualization reflects practitioners' preference for maintaining human oversight where risk tolerance is low and accountability remains paramount, underscoring the ethical and operational barriers to complete AI autonomy in incident response.

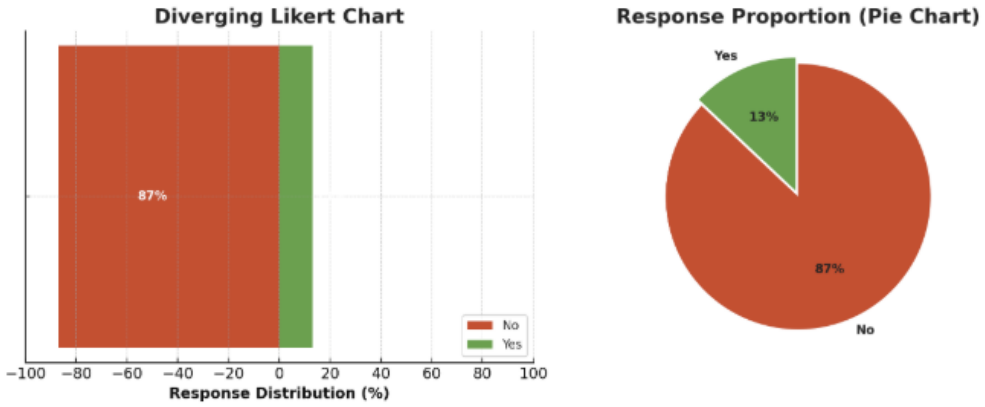

Figure 4. Response to Question #4.

Response to Question #5

With reference to question #5 in Table 4, the charts in Figure 5 show that 37% of respondents would support a move toward autonomous incident triage and containment without analyst oversight, while 63% expressed opposition. This response indicates a cautious attitude toward removing human involvement from critical decision points in cybersecurity operations. The visualization illustrates that although some practitioners acknowledge the potential efficiency of autonomy, a majority remain hesi-

 doi:10.20944/preprints202512.0348.v1

tant to relinquish human control, reflecting enduring concerns about accountability, error management, and trust in AI-driven systems.

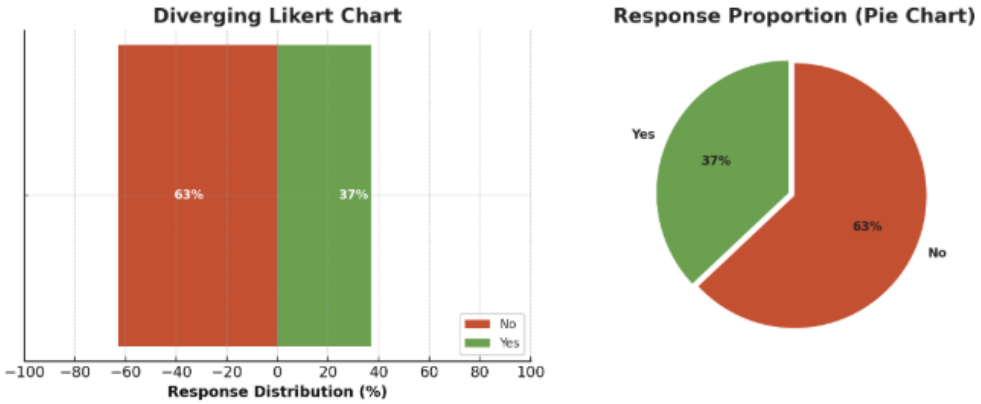

Figure 5. Response to Question #5.

Response to Question #6

With reference to question #6 in Table 4, the charts in Figure 6 show that only 17% of respondents believe the benefits of AI-driven automation outweigh the risks of false positives or negatives, while 83% disagreed. This finding highlights a pronounced level of caution among practitioners regarding the reliability of AI outputs in operational contexts. The visualization suggests that while automation is valued for efficiency, confidence in its precision and dependability remains limited, emphasizing the ongoing need for human validation and robust error-mitigation mechanisms within AI-assisted cybersecurity workflows.

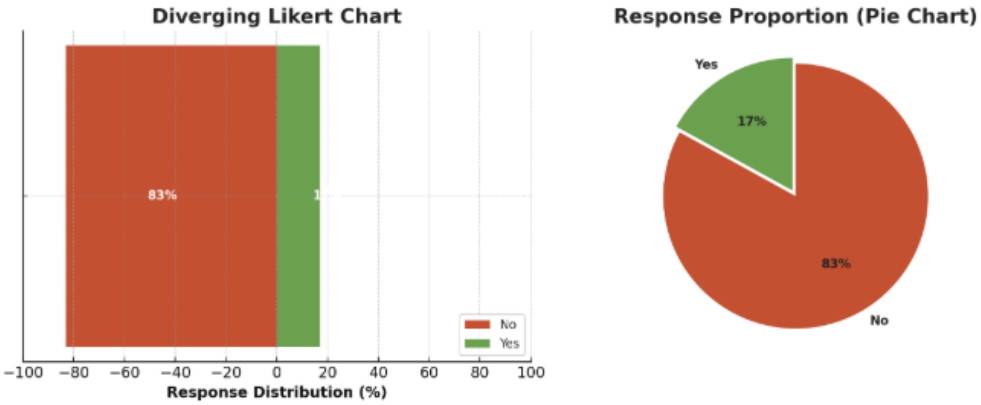

Figure 6. Response to Question #6.

Response to Question #7

With reference to question #7 in Table 4, the charts in Figure 7 show that only 20% of respondents believe AI workflows are making their current incident response (IR) playbooks obsolete or less relevant, while 80% disagreed. This result indicates that despite the growing influence of AI in cybersecurity operations, traditional IR frameworks continue to hold practical relevance. The visualization suggests that practitioners still rely heavily on structured procedural guidance, even as AI-driven tools become more integrated into their workflows, reflecting a gradual rather than disruptive transition toward automation in incident response practices.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 December 2025 doi:10.20944/preprints202512.0348.v1

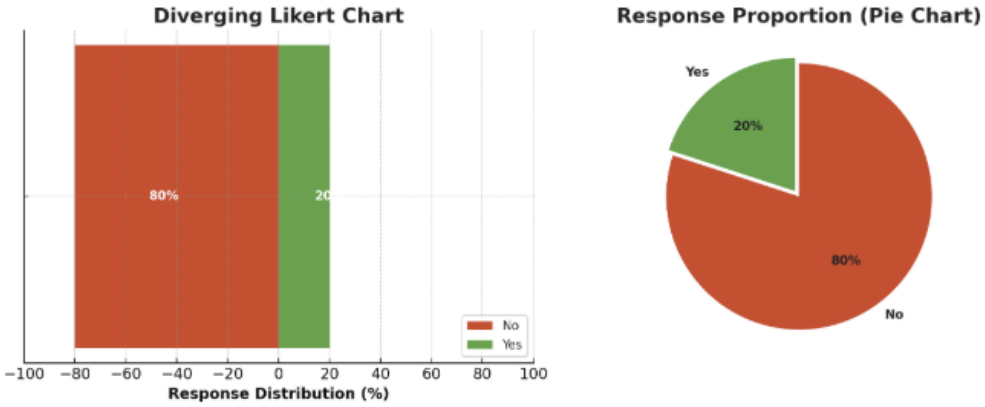

Figure 7. Response to Question #7.

Response to Question #8

With reference to question #8 in Table 4, the charts in Figure 8 show that 74% of respondents reported that their security teams are undergoing retraining to manage AI-powered automation tools, while 26% indicated otherwise. This finding reflects a proactive adaptation trend among organizations as they prepare their workforce for AI-integrated cybersecurity environments. The visualization highlights an encouraging shift toward skill modernization and capacity building, suggesting that many organizations recognize the importance of upskilling analysts to effectively leverage AI-driven automation and maintain operational readiness.

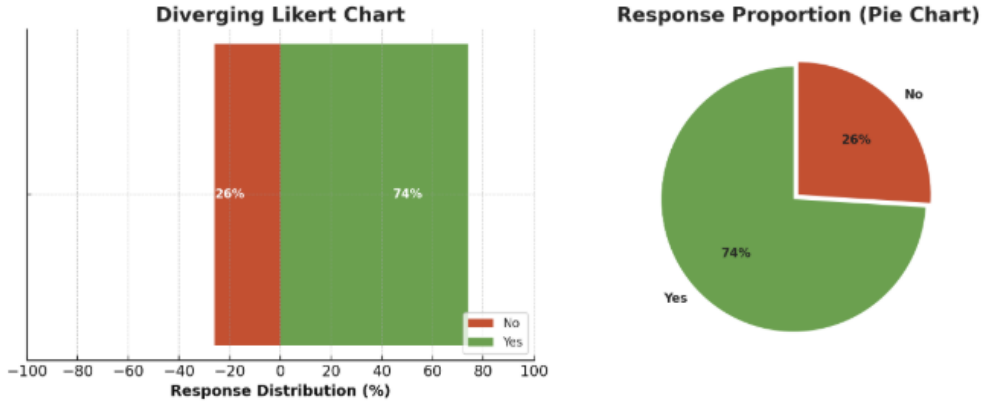

Figure 8. Response to Question #8.

Response to Question #9

With reference to question #9 in Table 4, the charts in Figure 9 indicate that 41% of respondents believe regulatory frameworks are lagging behind AI-driven cybersecurity automation trends, while 59% disagreed. This relatively balanced response suggests that while many practitioners recognize progress in policy and compliance adaptation, a significant portion still perceives a misalignment between technological innovation and regulatory evolution. The visualization emphasizes the ongoing debate regarding the adequacy of governance structures to address the pace and complexity of AI integration in cybersecurity practices.

 doi:10.20944/preprints202512.0348.v1

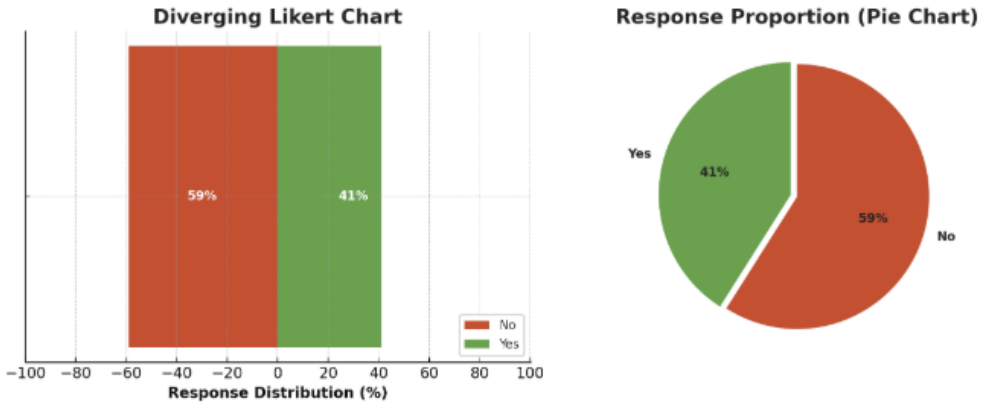

Figure 9. Response to Question #9.

Response to Question #10

With reference to question #10 in Table 4, the charts in Figure 10 show that 79% of respondents would advocate for a new classification or taxonomy of automation tools to reflect varying levels of agentic AI, while 21% opposed the idea. This strong level of support highlights a growing recognition of the need for clearer standards and definitions to distinguish between traditional automation and emerging AI-driven systems. The visualization underscores practitioners' desire for structured frameworks that can guide the governance, evaluation, and deployment of AI capabilities within cybersecurity operations.

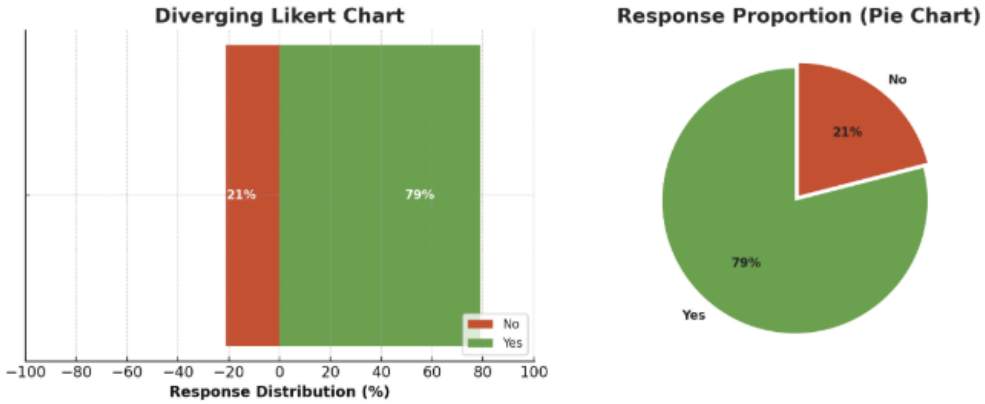

Figure 10. Response to Question #10.

Survey Result - Part Two

Psychometric Analysis

From a psychometric perspective, the survey responses in Table 5 exhibit strong internal consistency and construct validity, reflecting coherent practitioner perceptions about the readiness of existing incident response frameworks for AI-driven threats. The close alignment between questions such as the scalability of current frameworks (61% Yes), the call for modular structures (73% Yes), and the overwhelming support for industry-wide revision (96% Yes) demonstrates convergent validity, as these items collectively measure a shared construct of framework modernization. Conversely, the low affirmative responses regarding the customization of traditional frameworks (20% Yes) and the maintenance of separate AI threat modeling processes (21% Yes) reinforce discriminant validity, showing that organizations distinguish between theoretical endorsement of modernization and its actual implementation. The near balance in responses about ethical guidance (51% Yes, 49% No) further indicates healthy response variance rather than bias, suggesting that participants critically assessed each item independently. Together, these patterns affirm that the instrument reliably captures the cognitive and operational dimensions of practitioner attitudes toward the evolution and adequacy of incident response frameworks in the AI era.

 doi:10.20944/preprints202512.0348.v1

Table 5. Survey Responses on Framework Modernization and AI-Era Incident Response.

No.	Survey Question	Yes (%)	No (%)
1	Do you think the NIST IR framework adequately addresses threats posed by AI-driven attacks?	59	41
2	Has your organization customized or extended traditional frameworks like SANS or NIST to accommodate AI-based threats?	20	80
3	Do you find the existing IR lifecycle (Preparation → Detection → Containment → Eradication → Recovery) too rigid today?	40	60
4	Are current IR frameworks scalable enough to support autonomous or AI-assisted incident resolution at enterprise scale?	61	39
5	Do you believe that current frameworks lack guidance on ethical oversight of AI-agent decisions during incidents?	51	49
6	Would a simpler, modular incident response framework be more effective for AI-era threats?	73	27
7	Have traditional tabletop exercises failed to capture the complexity of AI-powered threat scenarios?	53	47
8	Do you find it challenging to map AI or ML threat indicators (e.g., model drift) into existing framework categories?	55	45
9	Does your organization maintain a separate AI threat modeling process outside the standard IR framework?	21	79
10	Would you support industry-wide revision of existing IR frameworks to formally include AI/agentic threat dimensions?	96	4

Note. This table summarizes how cybersecurity professionals assess the adequacy and adaptability of existing IR frameworks amid rising AI-based threats.

Response to Question #1

With reference to question #1 in Table 5, the charts in Figure 11 show that 59% of respondents believe the NIST Incident Response (IR) framework adequately addresses threats posed by AI-driven attacks, while 41% disagreed. This near-majority confidence suggests that although many professionals still find value in NIST's foundational structure, a substantial portion perceives limitations when confronting the complexity and adaptability of AI-enabled threats. The results indicate an emerging divergence in practitioner sentiment: some view existing frameworks as sufficiently robust with minor updates, whereas others anticipate the need for structural reform to manage autonomous and agentic threat models. The visualization highlights this nuanced balance between satisfaction with established practices and recognition of the need for modernization within AI-era incident response strategies.[6]

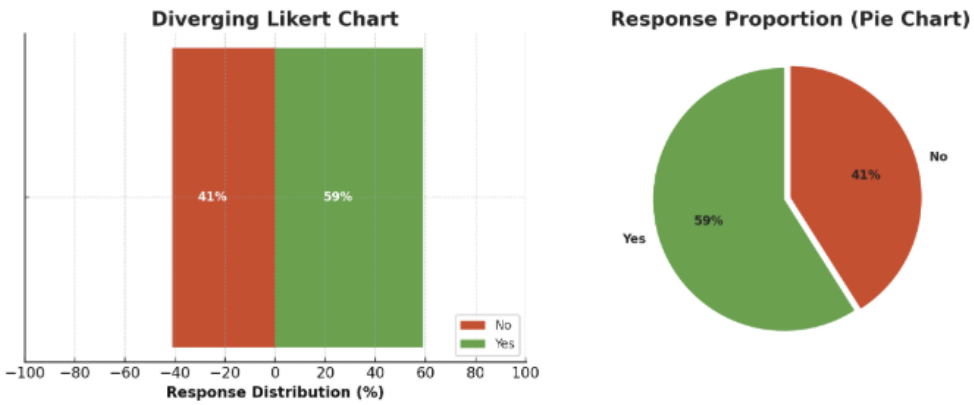

Figure 11. Response to Question #1: NIST IR Framework and AI-Driven Threats.

[6] Dashboard in Figure 11 is showing Diverging Likert and Horizontal Bar Charts illustrating responses to the question on whether the NIST IR framework adequately addresses AI-driven threats.

 doi:10.20944/preprints202512.0348.v1

Response to Question #2

With reference to question #2 in Table 5, the charts in Figure 12 show that only 20% of respondents indicated that their organizations have customized or extended traditional frameworks such as SANS or NIST to accommodate AI-based threats, while 80% reported no such adaptation. The Diverging Likert Chart and Pie Chart together demonstrate a clear implementation gap between the recognition of AI-driven risks and the actual modification of governance frameworks to address them. This finding suggests that while practitioners may acknowledge the limitations of existing structures, most organizations continue to rely on conventional frameworks without formal integration of AI considerations. The result underscores a key area for improvement, translating conceptual awareness of AI-era threats into tangible framework modernization and applied organizational practice.[7]

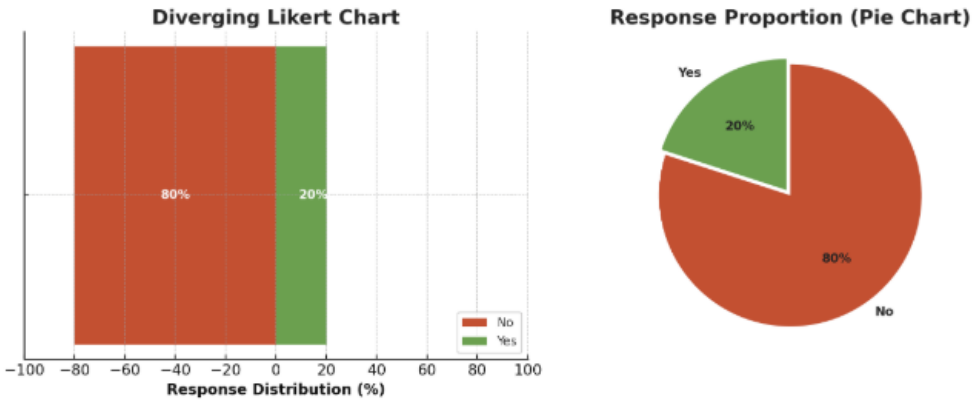

Figure 12. Response to Question #2: Customization or Extension of Traditional Frameworks for AI-Based Threats.

Response to Question #3

With reference to question #3 in Table 5, the charts in Figure 13 show that 40% of respondents find the existing incident response (IR) lifecycle — consisting of Preparation, Detection, Containment, Eradication, and Recovery — to be too rigid for modern operational realities, while 60% disagree. The Diverging Likert Chart and Pie Chart collectively indicate that although the traditional phased lifecycle remains widely accepted, a growing segment of professionals perceive it as inflexible when addressing AI-driven and adaptive threat environments. This emerging minority view suggests that while structured response models retain practical value, there is increasing demand for frameworks that allow iterative adaptation, faster response loops, and embedded automation intelligence to handle evolving threat dynamics more effectively.[8]

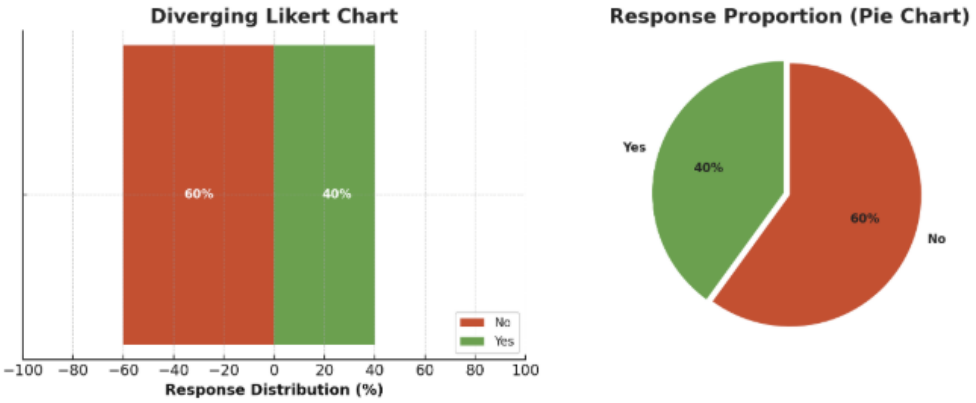

Figure 13. Response to Question #3: Perceived Rigidity of the Traditional IR Lifecycle.

[7] Dashboard in Figure 12 is showing Diverging Likert and Pie Charts illustrating responses to whether organizations have customized or extended traditional frameworks like SANS or NIST to accommodate AI-based threats.

[8] Dashboard in Figure 13 is showing Diverging Likert and Pie Charts illustrating responses to whether the existing IR lifecycle is considered too rigid for AI-era cybersecurity operations.

 doi:10.20944/preprints202512.0348.v1

Response to Question #4

With reference to question #4 in Table 5, the charts in Figure 14 indicate that 61% of respondents believe that current incident response (IR) frameworks are scalable enough to support autonomous or AI-assisted incident resolution at the enterprise level, while 39% disagree. The Diverging Likert Chart and Pie Chart illustrate a moderate level of confidence in the scalability of existing frameworks, suggesting that a majority of practitioners view them as capable of adapting to partial automation and AI integration. However, the sizeable minority expressing doubt highlights ongoing challenges in scaling traditional frameworks to meet enterprise-wide AI deployment demands. These findings suggest that while scalability is not perceived as a fundamental limitation, the successful implementation of AI-assisted response strategies may depend on refining framework flexibility and interoperability across enterprise environments.[9]

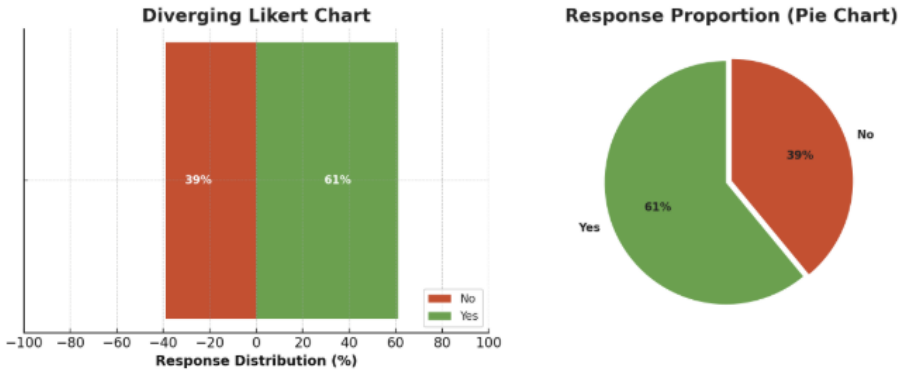

Figure 14. Response to Question #4: Scalability of Current IR Frameworks for AI-Assisted Incident Resolution.

Response to Question #5

With reference to question #5 in Table 5, the charts in Figure 15 show that 51% of respondents believe that current incident response (IR) frameworks lack sufficient guidance on the ethical oversight of AI-agent decisions during incidents, while 49% disagreed. The Diverging Likert Chart and Pie Chart together indicate a nearly even split in perceptions, highlighting a significant point of contention among cybersecurity professionals. This close division suggests that although a slight majority acknowledges ethical governance gaps in existing frameworks, many practitioners still consider current guidelines adequate when paired with human oversight. The result underscores an emerging discourse around the ethical dimensions of AI-driven automation, suggesting that as autonomy in decision-making increases, frameworks must evolve to include explicit principles for accountability, transparency, and ethical validation.[10]

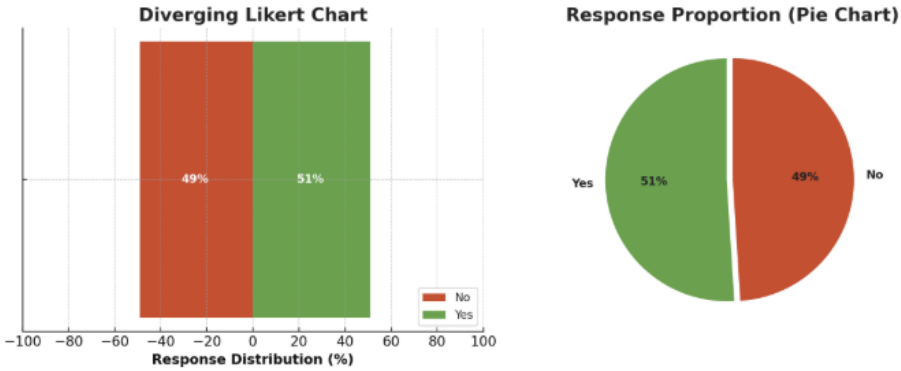

Figure 15. Response to Question #5: Ethical Oversight of AI-Agent Decisions in Current Frameworks.

[9] Dashboard in Figure 14 is showing Diverging Likert and Pie Charts illustrating responses to whether current incident response frameworks are scalable enough to support autonomous or AI-assisted resolution at enterprise scale.

[10] Dashboard in Figure 15 is showing Diverging Likert and Pie Charts illustrating responses to whether current frameworks provide adequate ethical oversight for AI-agent decisions during cybersecurity incidents.

 doi:10.20944/preprints202512.0348.v1

Response to Question #6

With reference to question #6 in Table 5, the charts in Figure 16 reveal that 73% of respondents believe a simpler and more modular incident response (IR) framework would be more effective for addressing AI-era threats, while 27% disagreed. The Diverging Likert Chart and Pie Chart collectively illustrate a strong practitioner preference for frameworks that emphasize adaptability, scalability, and simplicity. This finding suggests a growing recognition that the traditional, linear IR models may not fully support the speed and complexity of AI-enabled threat environments. The results underscore the evolving expectation that future frameworks should integrate modular structures capable of rapidly adjusting to the unpredictable dynamics of autonomous and intelligent threat landscapes.[11]

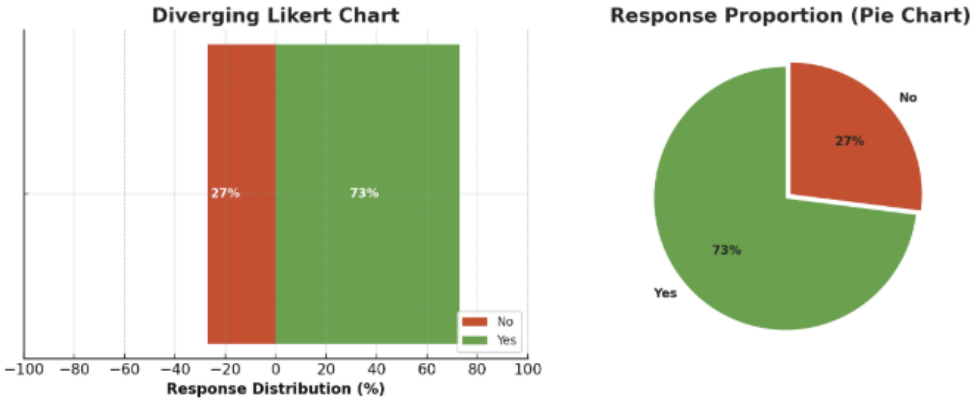

Figure 16. Response to Question #6: Preference for a Modular and Simplified Incident Response Framework.

Response to Question #7

With reference to question #7 in Table 5, the charts in Figure 17 show that 53% of respondents believe traditional tabletop exercises have failed to capture the complexity of AI-powered threat scenarios, while 47% disagreed. The Diverging Likert Chart and Pie Chart together indicate a near-even distribution of opinions, with a slight majority suggesting that existing training and simulation methods are insufficient for addressing AI-driven incidents. This result highlights a growing awareness that conventional tabletop exercises, which often rely on static and predefined scenarios, may not adequately model the unpredictability and adaptive behaviors associated with machine learning or autonomous attack patterns. The findings emphasize the need for next-generation simulation environments capable of incorporating dynamic AI-agent behaviors to better prepare cybersecurity teams for the evolving threat landscape.[12]

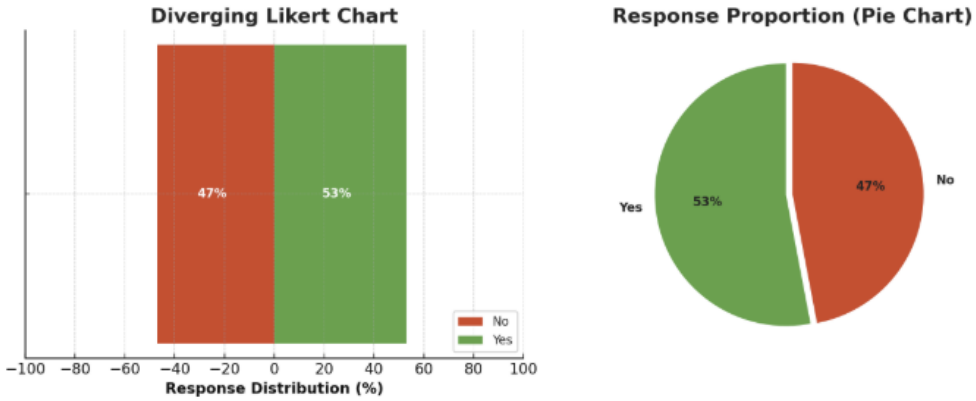

Figure 17. Response to Question #7: Adequacy of Traditional Tabletop Exercises for AI-Powered Threat Scenarios.

[11] Dashboard in Figure 16 is showing Diverging Likert and Pie Charts illustrating responses to whether a simpler, modular incident response framework would be more effective for addressing AI-era threats.

[12] Dashboard in Figure 17 is showing Diverging Likert and Pie Charts illustrating responses to whether traditional tabletop exercises have failed to capture the complexity of AI-powered threat scenarios.

 doi:10.20944/preprints202512.0348.v1

Response to Question #8

With reference to question #8 in Table 5, the charts in Figure 18 show that 55% of respondents find it challenging to map AI or machine learning (ML) threat indicators, such as model drift, into existing incident response (IR) framework categories, while 45% disagreed. The Diverging Likert Chart and Pie Chart indicate that a majority of practitioners experience difficulty integrating emerging AI-related indicators into traditional response taxonomies. This finding highlights a growing operational and conceptual gap between established framework structures and the evolving nature of AI-based threats. It suggests that as threat intelligence becomes more algorithmically complex, current frameworks may require redefinition or augmentation to accommodate new forms of telemetry, such as behavioral drift, model poisoning, and autonomous attack vectors.[13]

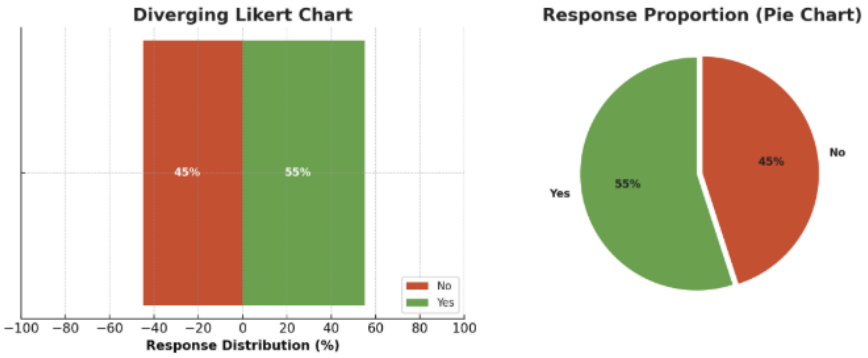

Figure 18. Response to Question #8: Challenges in Mapping AI or ML Threat Indicators into Existing Framework Categories.

Response to Question #9

With reference to question #9 in Table 5, the charts in Figure 19 show that only 21% of respondents indicated that their organizations maintain a separate AI threat modeling process outside the standard incident response (IR) framework, while 79% reported that no such process exists. The Diverging Likert Chart and Pie Chart clearly illustrate that most organizations continue to operate within conventional frameworks without isolating AI-specific threat modeling activities. This result highlights a significant gap between theoretical acknowledgment of AI-driven risks and the practical establishment of dedicated mechanisms to address them. The finding suggests that, while awareness of AI-related vulnerabilities is increasing, integration into organizational response structures remains limited, underscoring the need for more formalized and specialized AI threat modeling frameworks within enterprise cybersecurity governance.[14]

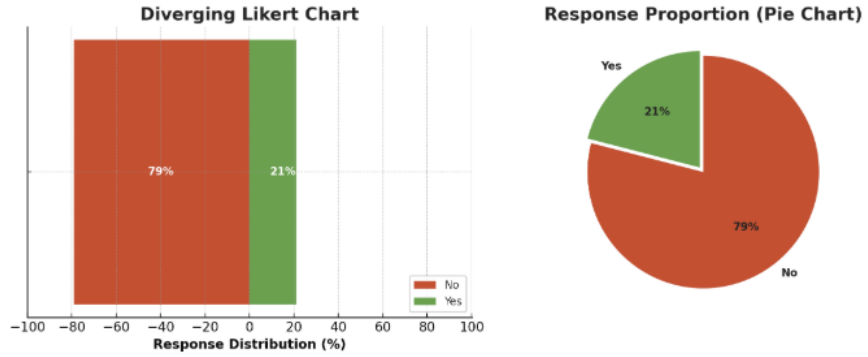

Figure 19. Response to Question #9: Existence of a Separate AI Threat Modeling Process.

[13] Dashboard in Figure 18 is showing Diverging Likert and Pie Charts illustrating responses to whether mapping AI or ML threat indicators into existing incident response framework categories presents challenges.

[14] Dashboard in Figure 19 is showing Diverging Likert and Pie Charts illustrating responses to whether organizations maintain a separate AI threat modeling process outside the standard incident response framework.

 doi:10.20944/preprints202512.0348.v1

Response to Question #10

With reference to question #10 in Table 5, the charts in Figure 20 show that an overwhelming 96% of respondents would support an industry-wide revision of existing incident response (IR) frameworks to formally include AI and agentic threat dimensions, while only 4% expressed opposition. The Diverging Likert Chart and Pie Chart together reveal a near-unanimous consensus among cybersecurity professionals on the need to modernize current frameworks to better address the realities of AI-driven threats. This result reinforces the growing recognition that legacy models, though foundational, no longer provide sufficient guidance for managing autonomous decision-making systems, adaptive adversarial behaviors, and ethical accountability in machine-assisted incident response. The strong consensus underscores the urgency of initiating a coordinated, industry-wide effort to redefine standards, terminology, and governance principles that reflect the operational and ethical complexities of the AI era.[15]

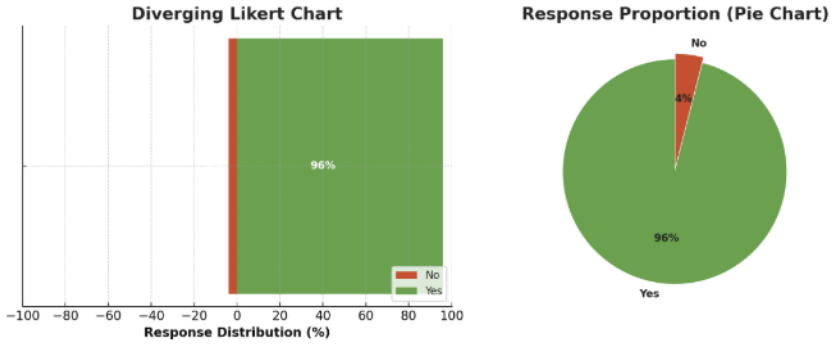

Figure 20. Response to Question #10: Support for Industry-Wide Revision of IR Frameworks to Include AI Threat Dimensions.

5. Discussion

5.1. Impact of Increased Sample Size on Margin of Error and Confidence Interval Precision

The target sample size initially calculated in Section 3.3.2.1 was approximately 140 participants. However, by the end of data collection, a total of 194 cybersecurity professionals had completed the survey. This higher-than-expected participation rate represents a positive outcome for the study, as it increases the statistical power, reduces sampling error, and enhances the precision of the estimated proportions. In general, the margin of error (MOE) decreases as the sample size increases, since sampling error is inversely proportional to the square root of the sample size $(1/\sqrt{n})$. [16]

The margin of error for a proportion is given by:

$$\text{MOE} = z_{\alpha/2}\sqrt{\frac{p(1-p)}{n}}$$

where $z_{\alpha/2}$ is the critical value of the standard normal distribution (1.96 for a 95% confidence level), p is the sample proportion, and n is the sample size. Using the most conservative estimate ($p = 0.5$) which produces the maximum possible margin of error, we have:

$$\text{MOE}_{140} = 1.96\sqrt{\frac{0.25}{140}} = 0.0828 \text{ (or } 8.28\%)$$

$$\text{MOE}_{194} = 1.96\sqrt{\frac{0.25}{194}} = 0.0704 \text{ (or } 7.04\%)$$

[15] Dashboard in Figure 20 is showing Diverging Likert and Pie Charts illustrating responses to whether respondents would support an industry-wide revision of incident response frameworks to formally include AI and agentic threat dimensions.

[16] An online sample size calculator available at https://www.calculator.net/math-calculator.html was also used to verify the accuracy of the computed sample size. This tool provided an independent validation of the statistical parameters, including confidence level and margin of error.

 doi:10.20944/preprints202512.0348.v1

This represents approximately a 15% improvement in precision:

$$\frac{8.28 - 7.04}{8.28} \times 100 \approx 15\%.$$

To illustrate this improvement, consider two key survey proportions:

- **AI Integration (84% Yes):** 95% CI for $n = 140$: [77.9%, 90.1%]; 95% CI for $n = 194$: [78.8%, 89.2%].
- **MTTD/MTTR Reduction (92% Yes):** 95% CI for $n = 140$: [87.5%, 96.5%]; 95% CI for $n = 194$: [88.2%, 95.8%].

To further highlight the importance of this increase in survey responses are items below that provide strong support for framework modernization:

- **NIST Framework Adequacy (59% Yes):** 95% CI with $n = 140$: [50.8%, 66.8%]; 95% CI with $n = 194$: [52.1%, 65.9%].
- **Support for Framework Revision (96% Yes):** 95% CI with $n = 140$: [92.5%, 99.5%]; 95% CI with $n = 194$: [93.3%, 98.7%].

These narrower confidence intervals demonstrate that collecting 194 rather than 140 responses meaningfully reduces uncertainty and increases the reliability of the findings. This enhancement improves the credibility of the results and strengthens the empirical conclusions drawn about automation adoption, efficiency improvements, and practitioner expectations in AI-driven incident response practices.

5.1.1. Selective Use of PDF and CDF Visuals for Latent Continuous Interpretation

Probability Density Functions (PDFs) and Cumulative Distribution Functions (CDFs) were used selectively in this study for survey questions that conceptually reflect transitions along an underlying continuum, such as perceived trust in AI systems or readiness for autonomous triage.[17] These visualizations help approximate how practitioner sentiment might distribute across a conceptual scale, allowing deeper insight into tendencies that are not immediately evident in raw binary charts. Since many survey questions do not map cleanly to underlying continuous constructs, PDF and CDF visuals were not applied universally, ensuring that the method remains analytically appropriate and does not impose a false sense of continuity on inherently discrete data.

5.2. Part One

Findings Related to Research Question on Emerging Priorities and Expectations

The survey results provide compelling evidence that cybersecurity teams are rapidly embracing automation and artificial intelligence (AI) integration as a central component of modern incident response practices. The strongest indicators of this operational shift are reflected in the high affirmative responses to questions related to AI adoption and measurable performance improvement. Specifically, 84% of respondents reported integrating agentic AI systems into their cybersecurity incident response workflows, while an even higher 92% confirmed that automation has significantly reduced their mean time to detect and respond (MTTD/MTTR) to incidents. These results demonstrate that AI integration is no longer theoretical but is producing tangible efficiency gains in operational environments. Moreover, the finding that 74% of organizations are retraining their teams to manage AI-powered automation tools highlights a proactive approach to capability development, signaling that AI is being institutionalized as part of the cybersecurity skillset and operational culture.

At the same time, the survey exposes practitioners' evolving expectations and concerns about the maturity and governance of automation. Although there is strong adoption, skepticism persists regarding autonomous decision-making, as shown by the low trust level (13%) and limited support (37%) for fully autonomous triage without analyst oversight. This tension suggests that while cybersecurity teams value automation's speed and precision [16,26], they also prioritize human judgment,

[17] While the survey items are binary or categorical, some reflect constructs that behave as latent continuous variables, making PDF and CDF plots suitable for illustrative purposes without misrepresenting the original data.

 doi:10.20944/preprints202512.0348.v1

oversight, and accountability in high-stakes scenarios. The overwhelming 79% support for creating a new taxonomy of automation tools to classify levels of agentic AI further illustrates the demand for structured frameworks that can guide governance, integration, and ethical deployment. Together, these findings confirm that the emerging priorities of cybersecurity teams revolve around enhancing operational efficiency through AI, strengthening human-AI collaboration, and establishing clear frameworks for trustworthy and adaptive automation, effectively addressing the research gap of fragmented SOAR integration and underutilized automation in incident response.

Probability and Cumulative Distribution [27–30] of MTTD/MTTR Improvement

Figure 21 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question [18] , "Has automation significantly reduced the mean time to detect/respond (MTTD/MTTR)?" where 92% of respondents answered in the affirmative. The PDF exhibits a sharply peaked distribution near 0.9, indicating that the majority of respondents strongly agree that automation has substantially improved detection and response efficiency, with minimal variation across participants. This concentration demonstrates a high level of consensus on the operational benefits of automation and AI integration. The corresponding CDF rises steeply in the same region, confirming that nearly all cumulative probability lies within the upper range of agreement. Collectively, these distributions provide quantitative evidence supporting the research question, suggesting that efficiency improvement through automation represents a dominant and consistent priority among cybersecurity teams in modern incident response practices.[19]

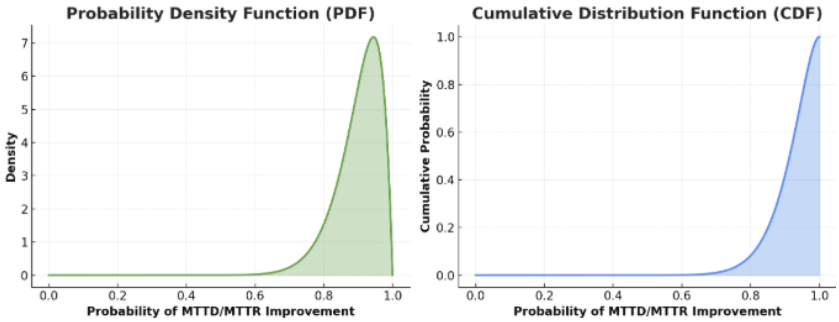

Figure 21. PDF and CDF.

Probability and Cumulative Distribution of Agentic AI Integration

Figure 22 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Are you currently integrating agentic AI systems into your cybersecurity incident response processes?" where 84% of respondents answered in the affirmative. The PDF demonstrates a strong concentration of probability near 0.8, indicating that the majority of respondents have already implemented or are actively integrating AI-driven systems within their incident response workflows. This peak suggests a high level of operational

[18] **Probability Density Function (PDF):** In the context of binary survey questions (Yes/No), a Probability Density Function (PDF) helps visualize how responses are distributed across the two options. While the term "PDF" is traditionally used for continuous variables, in binary data it effectively shows the proportion of respondents selecting "Yes" compared to "No." This type of chart is useful for clearly identifying trends in agreement or disagreement. For example, if 70 percent of participants answered "Yes" to a question about trusting AI in decision-making, a PDF-style bar graph would make this dominant preference easy to see. It offers a straightforward way to summarize how responses are spread across binary choices.
Cumulative Distribution Function (CDF): The Cumulative Distribution Function (CDF) is especially helpful when analyzing how responses accumulate across binary or grouped binary questions. Although traditionally used for continuous variables, a CDF adapted for binary survey results can show the cumulative percentage of "Yes" responses across a series of questions or categories. This is valuable for observing how support or trust in a concept, such as automation, increases across related prompts. It helps reveal patterns in how sentiments build, whether gradually or sharply, and provides a broader view of respondent attitudes that may not be evident from individual questions alone.

[19] Here's the dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Has automation significantly reduced the mean time to detect/respond (MTTD/MTTR)?" (92% Yes).

 doi:10.20944/preprints202512.0348.v1

adoption and consistency across organizations. The corresponding CDF rises sharply in the same region, showing that cumulative probabilities reach near-total agreement within a narrow interval. Together, these distributions provide quantitative validation of the research question, confirming that the integration of AI represents a core and emerging operational priority among cybersecurity teams seeking to enhance speed, precision, and adaptability in incident response practices.[20]

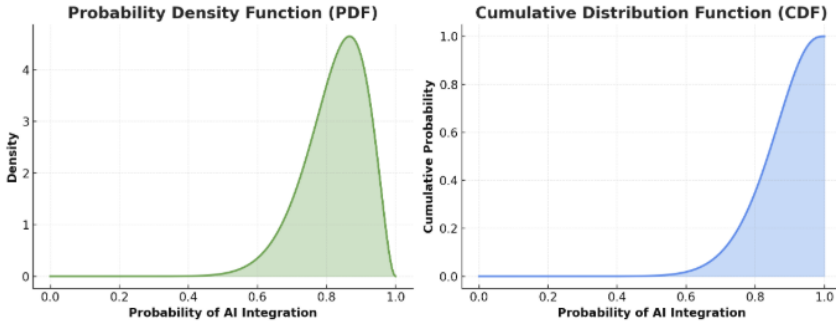

Figure 22. PDF and CDF of Agentic AI Integration.

Probability and Cumulative Distribution of Team Retraining for AI-Powered Automation

Figure 23 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Are security teams undergoing retraining to manage AI-powered automation tools?" where 74% of respondents answered in the affirmative. The PDF demonstrates a moderate concentration around 0.7, suggesting that most organizations are actively investing in workforce development to adapt to AI-driven operational environments. The shape of the distribution indicates a broad but consistent level of engagement across respondents, reflecting varied stages of training implementation. The CDF rises steadily in the same region, showing that cumulative probabilities approach near-total agreement before the 0.8 threshold. Together, these distributions quantitatively reinforce the research question by highlighting that team retraining represents a key emerging priority, underscoring how cybersecurity teams are evolving their skills and competencies to align with automation and artificial intelligence integration in incident response practices.[21]

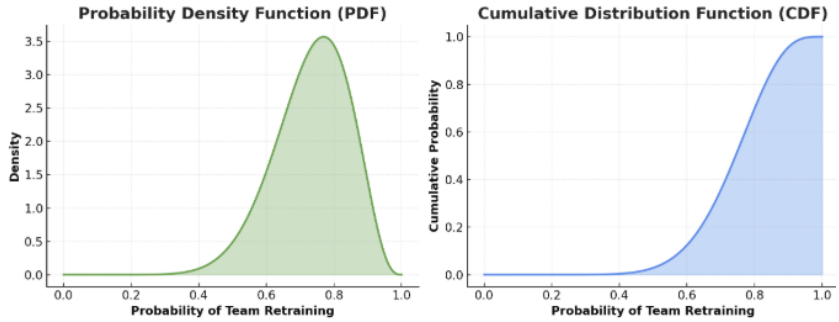

Figure 23. PDF and CDF of Team Retraining for AI-Powered Automation.

Probability and Cumulative Distribution of Support for New Classification of Automation Tools

Figure 25 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?" where 79% of respondents answered in the affirmative. The PDF shows a strong peak around 0.8, indicating that most practitioners agree on the need for clearer categorization and governance of automation tools as AI capabilities evolve.

[20] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Are you currently integrating agentic AI systems into your cybersecurity incident response processes?" (84% Yes).

[21] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Are security teams undergoing retraining to manage AI-powered automation tools?" (74% Yes).

 doi:10.20944/preprints202512.0348.v1

This concentration reflects widespread consensus among respondents, suggesting that cybersecurity professionals view structured classification as essential to managing operational complexity and ethical considerations associated with agentic AI. The CDF increases rapidly through the same range, showing that the cumulative probability reaches near-total agreement shortly after the 0.8 mark. Together, these distributions quantitatively confirm that developing a formal taxonomy of automation tools is an emerging expectation among cybersecurity teams, aligning directly with the research question's emphasis on the priorities guiding AI and automation integration in incident response.[22]

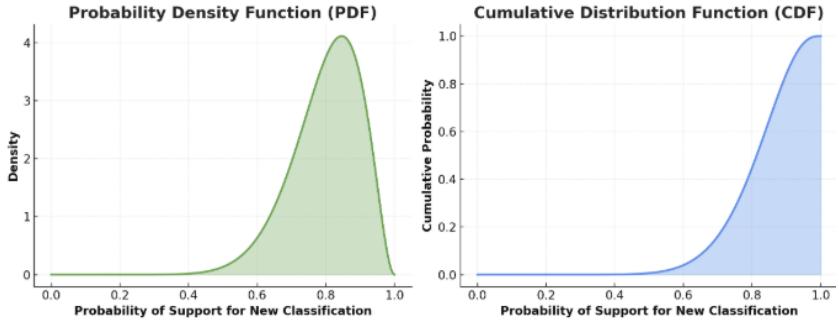

Figure 24. PDF and CDF of Support for New Classification of Automation Tools.

Probability and Cumulative Distribution of Support for New Classification of Automation Tools

Figure 25 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?" where 79% of respondents answered in the affirmative. The PDF shows a strong peak around 0.8, indicating that most practitioners agree on the need for clearer categorization and governance of automation tools as AI capabilities evolve. This concentration reflects widespread consensus among respondents, suggesting that cybersecurity professionals view structured classification as essential to managing operational complexity and ethical considerations associated with agentic AI. The CDF increases rapidly through the same range, showing that the cumulative probability reaches near-total agreement shortly after the 0.8 mark. Together, these distributions quantitatively confirm that developing a formal taxonomy of automation tools is an emerging expectation among cybersecurity teams, aligning directly with the research question's emphasis on the priorities guiding AI and automation integration in incident response.[23]

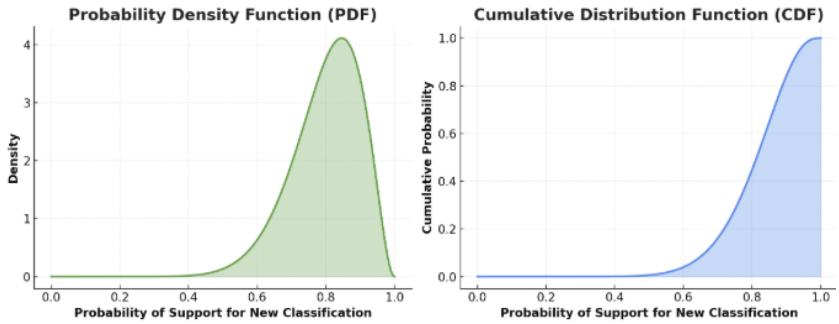

Figure 25. PDF and CDF of Support for New Classification of Automation Tools.

Probability and Cumulative Distribution of Perceived Adequacy of Current Automation Tools

Figure 27 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Do you believe current automation tools

[22] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?" (79% Yes).

[23] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI?" (79% Yes).

 doi:10.20944/preprints202512.0348.v1

can keep pace with evolving AI-driven attack techniques?" where only 30% of respondents answered "Yes" and 70% responded "No." The PDF displays a peak around 0.3, indicating that most participants have limited confidence in the capability of current automation tools to match the sophistication of AI-enabled threats. The distribution's skew toward lower probabilities reflects widespread skepticism about tool adaptability and resilience. The CDF rises gradually, reinforcing that cumulative agreement remains low until higher probability thresholds, suggesting strong consensus that automation lags behind adversarial innovation. Together, these distributions quantitatively support the research question by illustrating a critical expectation gap, emphasizing that advancing automation intelligence remains a pressing operational and strategic priority for cybersecurity teams.[24]

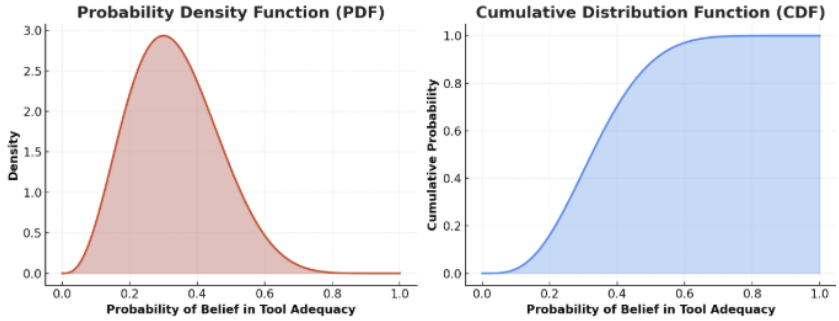

Figure 26. PDF and CDF of Perceived Adequacy of Current Automation Tools.

Probability and Cumulative Distribution of Perceived Adequacy of Current Automation Tools

Figure 27 presents both the Probability Density Function (PDF) and the Cumulative Distribution Function (CDF) for the survey response to the question, "Do you believe current automation tools can keep pace with evolving AI-driven attack techniques?" where only 30% of respondents answered "Yes" and 70% responded "No." The PDF displays a peak around 0.3, indicating that most participants have limited confidence in the capability of current automation tools to match the sophistication of AI-enabled threats. The distribution's skew toward lower probabilities reflects widespread skepticism about tool adaptability and resilience. The CDF rises gradually, reinforcing that cumulative agreement remains low until higher probability thresholds, suggesting strong consensus that automation lags behind adversarial innovation. Together, these distributions quantitatively support the research question by illustrating a critical expectation gap, emphasizing that advancing automation intelligence remains a pressing operational and strategic priority for cybersecurity teams.[25]

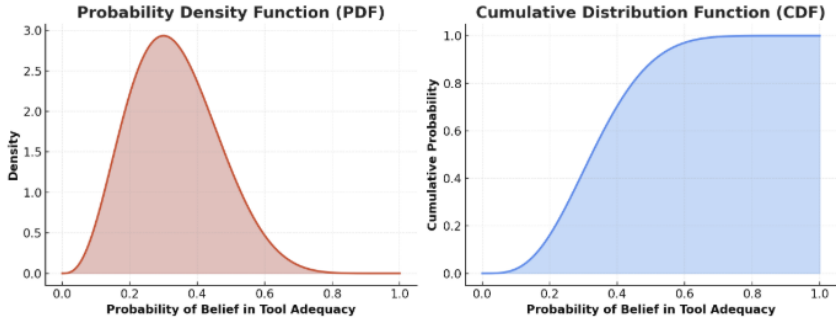

Figure 27. PDF and CDF of Perceived Adequacy of Current Automation Tools

[24] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Do you believe current automation tools can keep pace with evolving AI-driven attack techniques?" (30% Yes, 70% No).

[25] Dashboard illustrating the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) for the survey response "Do you believe current automation tools can keep pace with evolving AI-driven attack techniques?" (30% Yes, 70% No).

 doi:10.20944/preprints202512.0348.v1

5.3. Empirical Reassessment of Automation Relevance

Based on the evidence presented in Table 2.4 of prior study by Falowo et al - 2023 [4]), only 38.89% of the reviewed literature acknowledged automation as a relevant factor in cybersecurity incident handling. This relatively low recognition provides an empirical counterpoint to the findings from the current survey presented in Table 4, where more than 90% of practitioners affirmed that automation has significantly reduced detection and response times. Rather than discrediting the earlier systematic literature review, this new evidence extends its interpretation by showing that while earlier scholarly work underrepresented the importance of automation, real-world practice has advanced considerably. The survey results therefore provide an empirical rejection of the earlier limited perception of automation's relevance, illustrating that modern cybersecurity teams now view intelligent automation and AI integration as central to efficiency, adaptability, and resilience in incident response operations.

Part Two

Findings Related to Research Question on Framework Modernization and Adequacy

The survey findings provide compelling evidence that cybersecurity professionals recognize both the enduring value and the growing limitations of traditional incident response (IR) frameworks in the context of AI-driven threats. Among the top responses, 96% of participants expressed strong support for an industry-wide revision of existing IR frameworks to formally include AI and agentic threat dimensions, representing near-unanimous consensus on the need for modernization. Similarly, 73% of respondents favored a simpler, modular framework design, signaling a preference for greater flexibility and adaptability over rigid, linear models such as the conventional Preparation–Detection–Containment–Eradication–Recovery cycle. These results reveal that practitioners overwhelmingly view modernization as essential for ensuring responsiveness to autonomous and adaptive threats, emphasizing the importance of scalability, interoperability, and practical usability. The high level of agreement across these items demonstrates that professionals are not rejecting established standards like NIST and SANS, but rather calling for their evolution to align with emerging operational realities.

At the same time, the survey reveals nuanced challenges that reinforce why modernization is both necessary and complex. While 59% of respondents still believe the NIST IR framework adequately addresses AI-driven threats, 41% disagree, reflecting a moderate confidence gap in its current applicability. Furthermore, 55% reported difficulty mapping AI or machine learning (ML) threat indicators, such as model drift or data poisoning, into existing framework categories, highlighting conceptual gaps between static frameworks and dynamic AI behaviors. A similar division emerged around ethical governance, where 51% agreed that current frameworks lack adequate guidance on AI-agent decision oversight. Together, these findings underscore a growing practitioner awareness that while existing frameworks remain foundational, they must be expanded to include adaptive logic, ethical accountability, and AI-specific threat modeling. Collectively, the data confirm that modernization is not merely a theoretical aspiration but an operational imperative for sustaining effectiveness in AI-era cybersecurity.

6. Conclusion

The empirical results of this study confirmed that many cybersecurity professionals perceive gaps in current incident response practices, especially in the context of AI-enabled threats. A majority of respondents expressed limited confidence in legacy frameworks' ability to scale, integrate autonomous decision-making, or sustain ethical oversight at operational speed. These findings align with broader trends in the literature. Studies have shown that automated incident response mechanisms can significantly reduce downtime and improve service reliability [31], while others note that the success of such systems depends on model robustness, data quality, and alignment between machine decision-making and human oversight [32,33]. Together, these patterns underscore the tension between aspirations

 doi:10.20944/preprints202512.0348.v1

for intelligent automation and the operational risks that practitioners must navigate, as echoed in the survey responses captured in this study.

However, the design and analytic approach of this paper include inherent limitations that must be acknowledged. First, the binary response format, while promoting clarity and simplifying statistical aggregation, may have reduced complex practitioner perspectives into oversimplified dichotomies. As a result, certain contextual nuances or middle-ground opinions could have been lost in translation from real-world complexity to yes-or-no responses. Second, there is a possibility of sampling bias in which respondents who are more actively engaged with automation and AI practices were more inclined to participate in the study. This may underrepresent the viewpoints of practitioners from under-resourced or less AI-prepared organizations. These limitations highlight the importance of cautious interpretation when generalizing the findings.

Looking ahead, the empirical insights from this study serve as a critical foundation rather than a conclusive assessment for the introduction of the idea of framework modernization. The patterns, however observed (from the responses) in practitioner sentiment justify exploring a modular framework and AI-oriented approach, but the proposal of such framework must remain grounded in the evidence collected. For this reason, future work will introduce a validation roadmap that includes external discussions, pilot studies, and iterative adjustments. These mechanisms will help ensure that the any proposed framework evolves not solely from the authors' design vision but also from authentic engagement with the operational realities and feedback of cybersecurity professionals.

6.1. Clarifying Findings on Tabletop Exercises and AI-Powered Threat Scenarios

Based on the data analyzed in study, there is no evidence indicating that traditional tabletop exercises have categorically failed to capture the complexity of AI-powered threat scenarios.[26] Rather, the findings suggest that while tabletop exercises remain valuable, they may not fully address the dynamic characteristics of AI-driven threats such as model drift, adversarial behavior, and autonomous decision cycles. The survey indicates a perceived gap between existing exercise formats and the demands of AI-era threat simulation, highlighting an opportunity for enhancement rather than a failure of current practices. These insights encourage further refinement of tabletop exercises to better reflect the evolving threat landscape shaped by intelligent and adaptive adversarial technologies.

6.2. Methodological Bias Reflections

This study, which presents the empirical foundation for a broader effort, may reflect certain methodological limitations stemming from construct validity bias [34,35]. This type of bias occurs when the operationalization of survey questions does not fully or accurately capture the underlying constructs they are intended to measure. While the binary survey structure enhanced clarity and consistency in data collection, it may have oversimplified complex practitioner attitudes regarding automation, AI integration, and incident response workflows. The questions may not have adequately distinguished between different levels of automation maturity or contextual factors influencing tool adoption. As a result, some of the findings could reflect generalized sentiment rather than nuanced operational realities, potentially narrowing the interpretive scope of the thematic synthesis that followed.

A second potential limitation involves framing effects [36,37], where the phrasing and sequencing of survey items may have influenced respondents to emphasize gaps or deficiencies in existing frameworks. Given the authors' longstanding experience in large-scale enterprise environments, the wording and structure of the instrument may have inadvertently signaled a preference for modernization or AI-readiness as baseline expectations. This framing could lead to responses that are more critical of traditional frameworks such as NIST or SANS than might otherwise emerge in a neutral or exploratory setting. While the study employed robust design principles and sought a diverse respondent pool, recognizing

[26] Survey responses demonstrate practitioner uncertainty and mixed confidence levels, which should not be misinterpreted as definitive conclusions about the inadequacy of tabletop methodologies.

 doi:10.20944/preprints202512.0348.v1

the potential influence of framing effects is important to ensure transparency, support future replication, and encourage ongoing empirical scrutiny of both survey design and interpretive conclusions.

6.3. Limitations and Future Work

Although the survey methodology in this study was designed to ensure statistical rigor, psychometric reliability, and empirical relevance, certain limitations must be acknowledged. First, while the target sample size of 140 cybersecurity professionals was exceeded with 194 valid responses, the sampling was restricted to practitioners based primarily in the United States. This geographic concentration may limit the generalizability of findings to global cybersecurity practices, where variations in regulatory environments, maturity levels, and AI/automation adoption rates could yield different perspectives. Second, the reliance on self-reported data introduces the potential for response bias, as participants may have overestimated or underestimated their organization's level of AI integration, automation maturity, or framework alignment. Although psychometric checks such as internal consistency and construct validity were applied to mitigate this risk, subjective interpretation remains an inherent limitation of perception-based surveys. Third, while the survey's binary and Likert-style questions were effective for quantitative analysis, they do not fully capture the qualitative depth of practitioner reasoning or contextual nuances behind certain responses. Future work should therefore complement these findings with semi-structured interviews, case studies, or longitudinal field research to deepen understanding of how automation and AI are reshaping incident response practices in real-world environments. Finally, it is important to note that this empirical study does not attempt to prescribe an immediate replacement for existing frameworks but rather seeks to identify evidence-based gaps and practitioner expectations that logically inform the modernization efforts elaborated in subsequent or future study.

6.4. Transition to Framework Modernization Study

The analyses presented in this study collectively reveal that automation and artificial intelligence have become embedded, operational priorities across the cybersecurity domain. The empirical evidence from practitioners demonstrates widespread integration of agentic AI systems, measurable reductions in mean time to detect and respond (MTTD/MTTR), and significant retraining of cybersecurity teams to manage AI-powered automation tools. These results highlight that, although adoption is growing, trust in full AI autonomy remains low, suggesting that human oversight continues to play a crucial role in ensuring ethical and adaptive response decisions. Thus, the findings confirm that automation's relevance has shifted from a theoretical discussion in literature to a concrete, measurable transformation in practice, providing a strong empirical foundation for the next phase of inquiry.

Despite these advances, the findings also reveal a persistent gap between automation capability and the frameworks guiding its deployment. While cybersecurity teams demonstrate readiness for AI-driven response, existing frameworks such as NIST and SANS appear static, designed for pre-AI environments that lack adaptive feedback, ethical calibration, and real-time intelligence integration. The tension between technological evolution and framework rigidity underscores a critical misalignment between operational realities and governance mechanisms. This emerging gap raises essential questions about whether legacy frameworks can evolve to accommodate AI's dynamic nature or whether entirely new structures must be developed to govern decision autonomy, accountability, and resilience in machine-led security environments.

Future work will build directly on the empirical momentum of this study by shifting focus from operational adoption to structural adequacy and will seek to evaluate whether the frameworks that currently underpin organizational cybersecurity strategies possess the flexibility, scalability, and ethical grounding required for intelligent and sustainable incident response. In doing so, this work transitions the research from validating practitioner behavior to critically assessing the governance models that must evolve to sustain trust, adaptability, and resilience in the era of AI-augmented incident response.

 doi:10.20944/preprints202512.0348.v1

6.5. Interpretation of Survey Findings and Implications for Framework Modernization

The responses outlined in Table 6 reflect a strong practitioner-driven mandate for rethinking current incident response paradigms. A significant portion of cybersecurity professionals surveyed do not believe that existing automation tools are sufficient to keep pace with AI-enabled threats, nor do they trust unregulated autonomy without safeguards. These sentiments illustrate a pressing need for evolving traditional frameworks to include components that better handle uncertainty, accountability, and modular integration. Furthermore, the expressed concerns around false positives, regulatory gaps, and decision authority highlight the inadequacy of static models when applied to dynamic and high-stakes AI scenarios.

Table 6. Survey Responses Supporting the Need for Framework Modernization.

Q#	Survey Question	How Response Supports Framework Modernization
1	Do you believe current automation tools can keep pace with evolving AI-driven attack techniques? (70% No)	Indicates a capability gap and the need for more adaptable, future-facing frameworks.
5	Would you support a move toward autonomous incident triage and containment without analyst oversight? (63% No)	Shows hesitance towards full autonomy, calling for structured human-in-the-loop mechanisms.
6	Do you believe the benefits of AI-driven automation outweigh the risks of false positives or negatives? (83% No)	Emphasizes need for safeguards, oversight, and adaptive risk thresholds in framework design.
7	Are AI workflows making your current incident response (IR) playbooks obsolete or less relevant? (80% No)	Suggests that frameworks should evolve alongside existing processes, not fully replace them.
9	Do you believe regulatory frameworks are lagging behind AI-driven cybersecurity automation trends? (41% Yes)	Points to the absence of regulatory integration and the need for ethical governance layers.
10	Would you advocate for a new classification or taxonomy of automation tools to reflect levels of agentic AI? (79% Yes)	Validates demand for structured tiering and nuanced capabilities in emerging frameworks.

Note. Responses indicate multiple signals favoring the modernization of existing frameworks.

Equally important is the insight that most respondents do not view current incident response playbooks as obsolete but instead seek a more nuanced, complementary architecture. This supports the idea that modernization should not be about discarding what works, but about augmenting existing frameworks with more intelligent, scalable, and ethically aware capabilities. The high level of agreement on the need for new classifications or taxonomies of automation tools underscores the urgency of creating more refined structures that reflect the layered nature of AI involvement in cybersecurity.[27] These empirical findings create a logical foundation for exploring new directions in framework design, as will be presented in future work.[28]

Author Contributions: Conceptualization, O.I.F. and J.B.A.; methodology, O.I.F.; software, O.I.F.; validation, O.I.F. and J.B.A.; formal analysis, O.I.F.; investigation, O.I.F.; resources, O.I.F. and J.B.A.; data curation, O.I.F.; writing original draft preparation, O.I.F.; writing review and editing, O.I.F. and J.B.A.; visualization, O.I.F.; supervision, J.B.A.; project administration, O.I.F. and J.B.A.; funding acquisition, not applicable. All authors have read and agreed to the published version of the manuscript.

[27] This selection of survey items in Table 6 represents practitioner sentiment regarding automation, trust, oversight, and evolving incident response needs. The responses serve as empirical justification for further exploration of modernized frameworks that reflect emerging AI-driven realities.

[28] This discussion draws upon the aggregate practitioner responses presented in Table 6, highlighting how survey-derived evidence informs the rationale for evolving incident response frameworks to align with AI-driven operational realities.

 doi:10.20944/preprints202512.0348.v1

Funding: This research received no external funding

Institutional Review Board Statement: This study was conducted in accordance with the Declaration of Helsinki and was approved by the Institutional Review Board of the University of Cincinnati (protocol code 2025-0022, approval date 18 June 2025). The IRB determined that the study is exempt under 45 CFR 46.104, category 2(i), which covers research involving tests, surveys, interviews, or observations of public behavior when the information obtained is non-identifiable. The IRB also waived the requirement to obtain documentation of informed consent for all adult participants. This determination applies only to the activities described in the approved protocol.

Informed Consent Statement: Written informed consent was waived by the Institutional Review Board of the University of Cincinnati because the study met the criteria for exemption under 45 CFR 46.104, category 2(i). Participation was voluntary, and respondents were informed of the study purpose and their right to discontinue at any time prior to completing the survey.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request. Survey responses were collected anonymously and do not include any information that could identify participants.

Acknowledgments: The author expresses sincere appreciation to Dr. Bou Abdo Jacques for his supervision, guidance, and constructive feedback throughout the development of this study. The author also acknowledges the support of Dr. Mustafa Yakubu, Dr. Jacob Koch, and Lily Edinam Botsyoe, who assisted in the early stage of the study by reviewing the survey questions and testing the survey distribution link to ensure proper functionality. The author further extends gratitude to the cybersecurity professionals who participated in the survey and contributed valuable insights that made this research possible.

Conflicts of Interest: The author declares no conflict of interest. The Institutional Review Board of the University of Cincinnati reviewed the study independently and had no role in the design, analysis, interpretation, or reporting of the research.

References

1. Falowo, O.I.; Popoola, S.; Riep, J.; Adewopo, V.A.; Koch, J. Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access* **2022**, *10*, 134038–134051.
2. Falowo, O.I.; Ozer, M.; Li, C.; Abdo, J.B. Evolving Malware & DDoS Attacks: Decadal Longitudinal Study. *IEEE Access* **2024**.
3. Falowo, O.I.; Abdo, J.B. 2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques. *IEEE Access* **2024**, *12*, 26759–26772.
4. Falowo, O.I.; Koshoedo, K.; Ozer, M. An Assessment of Capabilities Required for Effective Cybersecurity Incident Management-A Systematic Literature Review. In Proceedings of the 2023 International Conference on Data Security and Privacy Protection (DSPP). IEEE, 2023, pp. 1–11.
5. GICSP, E.H.; Assante, M.; Conway, T. An abbreviated history of automation & industrial controls systems and cybersecurity. *SANS Institute, Tech. Rep.* **2014**.
6. Manikanta, S.; Time, R. AI and Automation in Cybersecurity: Future Skilling for Efficient Defense. *ISACA Journal* **2024**.
7. Żurawski, S.; Chrząszcz, A.; Ciekanowski, Z.; Pauliuchuk, Y.; Pietrzyk, S.; Wyrzykowska, B. Effectiveness of information security incident management systems: identifying practices, challenges and development perspectives **2025**.
8. Gangapatnam, K. Proactive Security with AI: Revolutionizing Cloud Infrastructure Protection. *Journal of Computer Science and Technology Studies* **2025**, *7*, 277–284.
9. Kshetri, N. Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy* **2025**, p. 102976.
10. Katnapally, N.; Murthy, L.; Sakuru, M. Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques. *J. Electrical Systems* **2021**, *17*, 138–148.
11. Nadeem, F.; Adrian, G. Next-Level SOC Automation: Detecting Financial Crimes and Social Engineering with Agentic AI **2025**.
12. Taddeo, M.; McCutcheon, T.; Floridi, L. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence* **2019**, *1*, 557–560.

 doi:10.20944/preprints202512.0348.v1

13. Omrani, N.; Rivieccio, G.; Fiore, U.; Schiavone, F.; Agreda, S.G. To trust or not to trust? An assessment of trust in AI-based systems: Concerns, ethics and contexts. *Technological Forecasting and Social Change* **2022**, *181*, 121763.
14. Afroogh, S.; Akbari, A.; Malone, E.; Kargar, M.; Alambeigi, H. Trust in AI: progress, challenges, and future directions. *Humanities and Social Sciences Communications* **2024**, *11*, 1–30.
15. Lysenko, S.; Bobrovnikova, K.; Shchuka, R.; Savenko, O. A cyberattacks detection technique based on evolutionary algorithms. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2020, pp. 127–132.
16. Sarker, I.H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science* **2023**, *10*, 1473–1498.
17. De Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics* **2023**, *12*, 1920.
18. Das, R.; Sandhane, R. Artificial intelligence in cyber security. In Proceedings of the Journal of Physics: Conference Series. IOP Publishing, 2021, Vol. 1964, p. 042072.
19. Çela, E.; Vedishchev, A.; Vajjhala, N.R. Upskilling the educational workforce for AI-enhanced cybersecurity: A thematic and trend analysis. In *AI-Enabled Threat Intelligence and Cyber Risk Assessment*; CRC Press, 2024; pp. 57–75.
20. Mueck, M.D.; On, A.E.B.; Du Boispean, S. Upcoming European regulations on artificial intelligence and cybersecurity. *IEEE Communications Magazine* **2023**, *61*, 98–102.
21. Gürbüz, S. Survey as a quantitative research method. *Research methods and techniques in public relations and advertising* **2017**, *2017*, 141–62.
22. U.S. Bureau of Labor Statistics. Computer and Information Systems Managers. https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm, 2024. Accessed: 2025-06-16.
23. Nathanson, B.H.; Higgins, T.L. An introduction to statistical methods used in binary outcome modeling. In Proceedings of the Seminars in cardiothoracic and vascular anesthesia. SAGE Publications Sage CA: Los Angeles, CA, 2008, Vol. 12, pp. 153–166.
24. Arafat, S.; Chowdhury, H.R.; Qusar, M.; Hafez, M. Cross cultural adaptation and psychometric validation of research instruments: a methodological review. *Journal of Behavioral Health* **2016**, *5*, 129–136.
25. Squires, J.E.; Hayduk, L.; Hutchinson, A.M.; Cranley, L.A.; Gierl, M.; Cummings, G.G.; Norton, P.G.; Estabrooks, C.A. A protocol for advanced psychometric assessment of surveys. *Nursing research and practice* **2013**, *2013*, 156782.
26. Lysenko, S.; Bobro, N.; Korsunova, K.; Vasylchyshyn, O.; Tatarchenko, Y. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs* **2024**, *69*, 43–51.
27. Krylov, V.A.; Moser, G.; Serpico, S.B.; Zerubia, J. On the method of logarithmic cumulants for parametric probability density function estimation. *IEEE Transactions on Image Processing* **2013**, *22*, 3791–3806.
28. Delaigle, A.; Hall, P. Defining probability density for a distribution of random functions. *The Annals of Statistics* **2010**, pp. 1171–1193.
29. Potter, K.; Kirby, R.M.; Xiu, D.; Johnson, C.R. Interactive visualization of probability and cumulative density functions. *International journal for uncertainty quantification* **2012**, *2*.
30. Blanco, Y.; Zazo, S.; Principe, J. Alternative statistical Gaussianity measure using the cumulative density function. In Proceedings of the Proceedings of the Second International Workshop on Independent Component Analysis and Blind Signal Separation, 2000, pp. 537–542.
31. Yang, Y. Analyzing the Effectiveness of Automated Incident Response Mechanisms in Reducing Downtime and Improving Service Reliability in Large-Scale Distributed Systems. *International Journal of Site Reliability Engineering (IJOSRE)* **2025**, *6*, 1–10. Compares automated vs manual IR in large systems.
32. Tocchetti, A.; Corti, L.; Balayn, A.; Yurrita, M.; Lippmann, P.; Brambilla, M.; Yang, J. AI robustness: a human-centered perspective on technological challenges and opportunities. *ACM Computing Surveys* **2025**, *57*, 1–38.
33. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion* **2023**, *97*, 101804.
34. Messick, S. Validity of psychological assessment: Validation of inferences from persons' responses and performances as scientific inquiry into score meaning. *American psychologist* **1995**, *50*, 741.
35. Cronbach, L.J.; Meehl, P.E. Construct validity in psychological tests. *Psychological bulletin* **1955**, *52*, 281.
36. Tversky, A.; Kahneman, D. The framing of decisions and the psychology of choice. *science* **1981**, *211*, 453–458.
37. Tourangeau, R.; Rips, L.J.; Rasinski, K. The psychology of survey response **2000**.

 doi:10.20944/preprints202512.0348.v1

Biography of Authors

Olufunsho I. Falowo received the B.A. degree in Philosophy from the University of Lagos, Nigeria, in 2004, and the M.B.A. degree from the Isenberg School of Management, University of Massachusetts, in 2021. He is a Ph.D. candidate in Information Technology at the School of Information Technology, University of Cincinnati, Ohio. He has completed ten graduate-level courses toward the Master of Liberal Arts in Cybersecurity at Harvard University and is currently enrolled in the eleventh course (pre-capstone), with the capstone project remaining to complete the program. He has been a Certified Information Systems Security Professional since 2017, a Certified Information Security Manager since 2020, a Certified Computer Hacking Forensic Investigator since 2011, a Certified Security Analyst since 2010, and a certified ISO/IEC 27001:2005 Lead Implementer. His research interests include cloud security, security information and event management, security incident detection and response, ethical hacking, and digital forensic investigation. He has also completed executive education programs in Design Thinking at the Kellogg School of Management at Northwestern University, Cybersecurity Risk Management at Harvard University, Behavioral Economics at the University of Chicago Booth School of Business, Negotiation Strategies at the Yale School of Management, and Building Resilience and Agility at the London Business School. ORCID: 0000-0002-4460-0986

Jacques Bou Abdo is an interdisciplinary researcher with expertise in complex systems, cybersecurity, cyber warfare, computational economics, and network economics. His work focuses on understanding the universality of laws governing networks and systems, with applications in cyber and strategic deterrence, information and disinformation flows in irregular warfare, cyberattack propagation and network resiliency, infectious disease transmission, and supply chain resilience. Dr. Bou Abdo is an assistant professor in the School of Information Technology at the University of Cincinnati. He holds a Ph.D. in Management Sciences from Paris-Saclay University (2021), a Ph.D. in Computer Science from Sorbonne University (2014), an M.E. in Telecommunication Networks from Saint Joseph University (2011), a B.B.A. in Management from the Lebanese University (2010), and a Diplôme d'Ingénieur in Electrical and Electronics Engineering from the Lebanese University (2009). ORCID: 0000-0002-3482-9154.