

How Artificial Intelligence Is Transforming Cybersecurity Incident Response

Chidi Theodore Udeze¹, Oluwatosin Falebita², Semiu Temidayo Fasasi³

¹Wellsfargo Bank, 194 S wood Avenue Iselin NJ, 08830. USA

Email : ogasampikin@gmail.com

²Colorado State University, Fort Collins, CO, 80523, USA

Oluwatosinfalebita@outlook.com

³Department of Mechanical Engineering, Colorado State University, Fort Collins, CO, 80523, USA

fasasitemidayo16@gmail.com

Abstract

Artificial Intelligence (AI) is revolutionizing the field of cybersecurity incident response by empowering organizations to identify, analyze, prioritize, contain, and recover from cyber threats faster and more accurately. However, the currently used incident response strategies rely on manual investigations, pre-defined rules and human decisions, meaning they suffer from alert fatigue, delayed response and are hard to deal with complex and evolving attacks. These are where AI-powered solutions come in with machine learning, deep learning, natural language processing, predictive analytics, generative AI, and agentic AI. These technologies help with the automated detection of anomalies, behavioral analysis, correlation of threat intelligence, classification of incidents, risk scoring, and adaptive response. AI can also be used to ease repetitive analytical tasks in the SOC and to aid in rapid decisions when dealing with a complex incident. But as automation goes up, there are problems with false-positives, model drift, adversarial manipulation, data quality, explainability, privacy, and governance. This study explores the intersection of AI with the cybersecurity incident response lifecycle and assesses the impact of AI on improving cybersecurity detection effectiveness, response automation, predictive defence, and cyber resilience of organisations. It also reflects on implementation needs, human oversight, governance arrangements and new prospects for autonomous security operations. The study concludes that with proper integration of AI into existing cybersecurity processes, organizations can find faster, more adaptable, and resilient incident response capabilities.

Keywords: Artificial Intelligence, Cybersecurity, Incident Response, Machine Learning, Threat Detection, Predictive Analytics, Agentic AI, Automated Response, Cyber Resilience, Security Operations Centers.

1. Introduction

Artificial Intelligence (AI) is also transforming Cybersecurity by allowing security systems to analyze massive amounts of security data and uncover deep patterns, detect anomalies, and help provide quicker responses to new cyber threats. Security solutions that rely on rule-based detection and manual intervention are no longer effective in today's enterprise environment due to the increasing sophistication, speed, and scale of attacks. AI and Machine Learning (ML) offer advanced tools for intelligent threat detection, behavioural analysis, automated classification, and ongoing security monitoring, bolstering organisations' capacity to detect malicious activities before they can have a substantial impact (Mohamed, 2025; Manoharan & Sarker, 2023).

AI-driven transformation is well suited to cybersecurity incident response, which involves analyzing multiple alerts across a variety of formats and making decisions in seconds about investigation, containment, eradication, and recovery. AI-driven incident response systems can now correlate security events, prioritize threats based on risk, suggest response actions, and automate certain containment steps, thus minimizing reliance on human intervention and either enhancing response efficiency. AI-integrated incident response systems can now correlate security events, prioritize threats based on risk, recommend response steps, and automate some containment actions, reducing dependence on manual intervention and potentially improving the efficiency of incident response (Chirra, 2023; Maddireddy & Maddireddy, 2023). Previous uses of AI in cybersecurity have proven its worth in threat detection and response, and, more recently, in predictive and increasingly autonomous security operations (Dalal, 2018; Khan et al., 2024).

This shift continues with the advent of predictive analytics and agentic AI. Predictive AI can detect patterns linked to potential attacks and help in proactive risk management, and agentic AI can enhance the autonomy of threat detection, decision-making, and automated actions to mitigate threats (ABDULRAHMAN et al., 2025; Kshetri, 2025). Automated incident response can also help mitigate alert overloads, skill gaps in the security industry, and the growing number of security events that are faced by Security Operations Centers (SOCs) (Ismail et al.,

2023; Uzoma et al., 2023).

But AI-powered incident response comes with its own set of challenges, such as false positives, model accuracy, adversarial attacks, explainability, data quality, privacy issues, and overreliance on AI-driven decisions. Therefore, businesses need to strike the right balance between automation and human control and management. This research study thus explores the role of AI in cybersecurity incident response, especially in intelligent detection, automated investigation, predictive threat intelligence, autonomous response, operational gains, challenges of implementation and the governance needs for effective and resilient cyber defense.

II. Artificial Intelligence in Modern Cybersecurity Incident Response

Artificial Intelligence (AI) has evolved from a supplementary cybersecurity technology into an important component of modern incident response. Conventional response processes often rely on predefined rules, manual investigation, and security analysts to interpret large volumes of alerts. AI and Machine Learning (ML) improve this process by identifying complex patterns, detecting anomalies, correlating security events, and supporting faster response decisions (Mohamed, 2025; Dalal, 2018). The integration of AI into Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR), and threat-intelligence platforms enables organizations to move toward more adaptive security operations.

2.1 Evolution of Incident Response

Traditional incident response generally follows a sequential process involving detection, analysis, containment, eradication, recovery, and post-incident review. However, increasing attack volumes and sophisticated threat techniques make purely manual processes difficult to scale. AI introduces automation into these stages by continuously processing network, endpoint, application, and user activity. AI-driven systems can identify abnormal behavior and prioritize potentially severe incidents, allowing security teams to concentrate on high-risk events (Chirra, 2023; Maddireddy & Maddireddy, 2023).

2.2 Core AI Technologies

Modern cybersecurity incident response incorporates several AI techniques. Machine learning

supports classification and anomaly detection, while deep learning can identify complex patterns across large security datasets. Natural Language Processing (NLP) can extract useful information from threat reports, security alerts, and unstructured intelligence. Predictive analytics extends incident response from reactive detection toward anticipating potential attacks (Manoharan & Sarker, 2023; ABDULRAHMAN et al., 2025). More recently, agentic AI has introduced systems capable of planning actions, interacting with security tools, and executing response workflows with limited human intervention (Kshetri, 2025).

2.3 AI-Driven Incident Response Lifecycle

AI can support nearly every stage of the incident response lifecycle. During event collection and detection, algorithms analyze large volumes of telemetry and identify anomalies. During investigation, AI correlates seemingly unrelated events and assists with identifying attack patterns. During prioritization, risk-based models can rank incidents according to severity and potential organizational impact. Automated playbooks can then support containment and remediation, such as isolating affected endpoints or blocking malicious activity, subject to organizational controls and authorization (Ismail et al., 2023; Uzoma et al., 2023).

2.4 From Reactive to Predictive and Autonomous Response

The most significant transformation is the movement from reactive security operations toward predictive and increasingly autonomous defense. AI-powered threat intelligence can identify patterns associated with emerging threats and support early intervention (ABDULRAHMAN et al., 2025). Agentic AI further extends automation by enabling coordinated reasoning and action across cybersecurity tools, potentially reducing response latency and analyst workload (Kshetri, 2025). Nevertheless, human oversight remains important for high-impact decisions because inaccurate models, adversarial manipulation, false positives, and inappropriate automated actions can create additional security risks (Mohamed, 2025; Khan et al., 2024).

Table 1. Evolution from Traditional to AI-Driven Cybersecurity Incident Response

Incident Response Dimension	Traditional Approach	AI-Assisted Approach	Advanced AI/Agentic Approach
Threat Detection	Rules and signatures	ML-based anomaly detection	Adaptive behavioral and predictive detection
Alert Analysis	Manual investigation	Automated correlation	Autonomous multi-source reasoning
Incident Prioritization	Static severity levels	Dynamic risk scoring	Context-aware autonomous prioritization
Threat Intelligence	Manual collection and review	Automated intelligence extraction	Continuous intelligence analysis and action
Investigation	Analyst-driven	AI-assisted investigation	AI-driven attack-path and root-cause analysis
Containment	Manual security actions	Automated playbooks	Agentic response across security tools
Remediation	Human-directed	Automated recommendations/actions	Context-aware autonomous remediation
Learning	Periodic rule updates	Continuous model training	Adaptive and feedback-driven learning
Analyst Role	Primary decision maker	AI-assisted decision maker	Human supervisor and strategic decision maker
Response Objective	React to incidents	Detect and respond faster	Predict, prevent, and autonomously respond

Source: Synthesized from Mohamed (2025), Chirra (2023), Kshetri (2025), ABDULRAHMAN et al. (2025), Manoharan and Sarker (2023), Khan et al. (2024), Dalal (2018), Maddireddy and Maddireddy (2023), Ismail et al. (2023), and Uzoma et al. (2023).

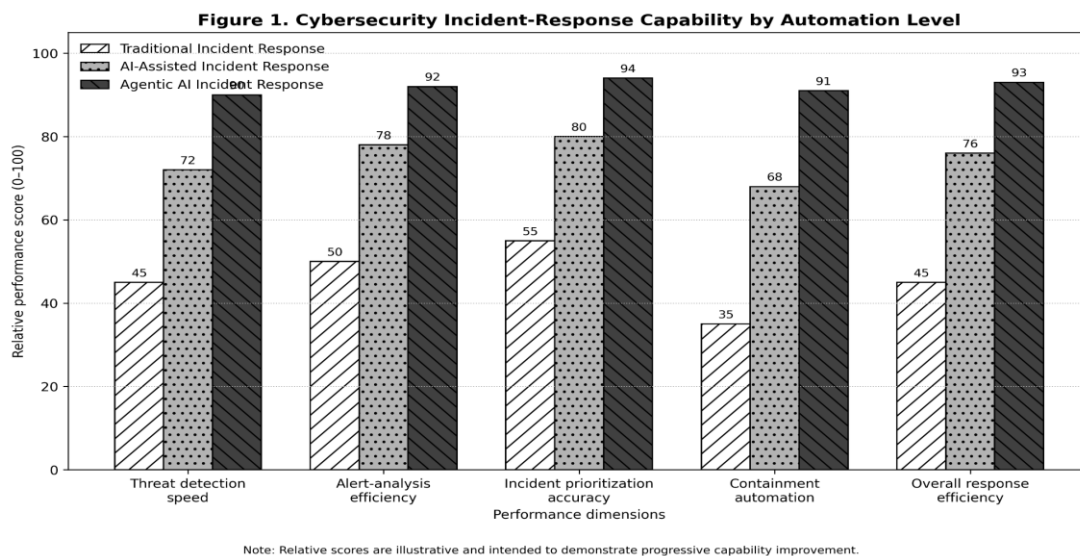


Fig 1: Scores represent illustrative relative performance levels (0–100) used to demonstrate the progressive improvement in threat detection, analysis, prioritization, containment, and overall incident-response efficiency as AI automation increases.

2.5 Implications for Modern Security Operations

The integration of AI changes the role of cybersecurity personnel from manually processing large numbers of alerts toward supervising intelligent detection and response systems. AI can improve operational efficiency, reduce repetitive tasks, accelerate incident analysis, and strengthen organizational cyber resilience (Maddireddy & Maddireddy, 2023; Uzoma et al., 2023). However, effective implementation requires reliable data, appropriately trained models, secure integration with existing infrastructure, continuous monitoring, and clearly defined human-oversight mechanisms. Thus, AI should be viewed not simply as a replacement for security professionals but as an intelligent capability that augments human expertise and enables more scalable incident response (Chirra, 2023; Ismail et al., 2023).

III. AI Technologies Transforming Cybersecurity Incident Response

Artificial Intelligence is reshaping cybersecurity incident response by moving security operations from predominantly rule-based and manual processes toward intelligent, automated, predictive, and adaptive defense. Machine learning and deep learning can identify anomalous patterns across large volumes of network, endpoint, and security-event data, allowing threats to be detected before conventional signatures or rules are available (Mohamed, 2025; Manoharan & Sarker, 2023). AI therefore strengthens the early stages of incident response by

improving detection accuracy, reducing alert overload, and supporting faster identification of malicious activity (Dalal, 2018; Khan et al., 2024).

3.1 Intelligent Threat Detection

AI-powered threat detection applies supervised, unsupervised, and deep learning techniques to recognize abnormal behaviors, malicious traffic, malware characteristics, suspicious user activities, and emerging attack patterns. Unlike static rule-based detection, machine learning models can learn from historical and real-time data to identify previously unknown indicators of compromise. This capability is particularly valuable in environments where attack techniques change rapidly (Mohamed, 2025; Manoharan & Sarker, 2023). AI can also correlate multiple security signals to distinguish genuine incidents from benign events, thereby improving the efficiency of security analysts (Khan et al., 2024).

3.2 Automated Incident Investigation

AI assists incident investigation by correlating logs, endpoint telemetry, network events, user behavior, and threat intelligence. Automated analytical processes can establish relationships between seemingly independent events and help identify the probable source, scope, and progression of an attack. AI-driven incident response systems can consequently reduce the amount of manual investigation required from security teams and accelerate incident triage (Chirra, 2023; Ismail et al., 2023).

3.3 Predictive Threat Intelligence

Predictive analytics extends incident response from detecting existing attacks to anticipating potential threats. AI models can analyze historical incidents, threat indicators, behavioral patterns, and environmental vulnerabilities to estimate emerging risks and support proactive defensive actions. The integration of AI-driven threat intelligence with automated response can improve cyber resilience by enabling organizations to prioritize threats according to their predicted impact and likelihood (ABDULRAHMAN et al., 2025).

3.4 Agentic AI for Autonomous Security Operations

Agentic AI represents a further development in cybersecurity automation by enabling AI systems to interpret security situations, determine appropriate actions, execute response

procedures, and adapt based on outcomes. Rather than simply recommending a response, agentic systems can potentially coordinate multiple security functions, such as investigation, containment, threat hunting, and remediation. This capability supports more autonomous security operations while creating a greater need for human oversight, authorization controls, and governance (Kshetri, 2025).

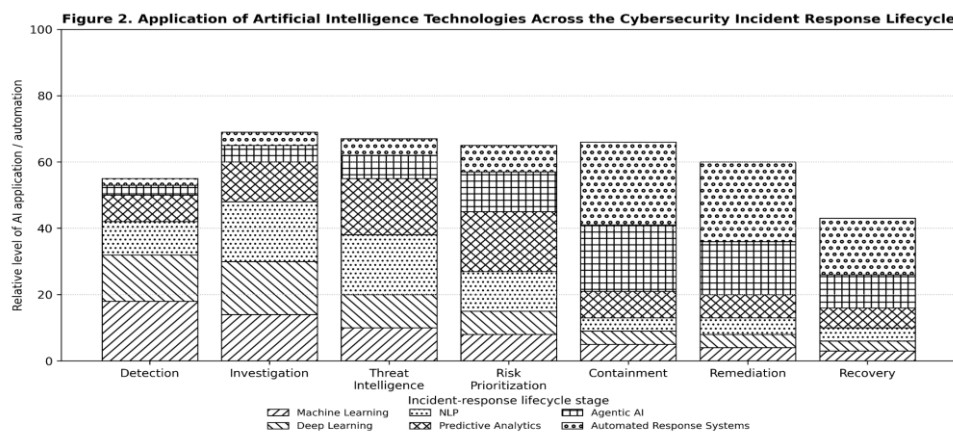
Table 2. AI Technologies and Their Applications in Cybersecurity Incident Response

AI Technology	Incident Response Application	Primary Contribution	Key References
Machine Learning	Anomaly and threat detection	Identifies abnormal and malicious patterns	Mohamed (2025); Manoharan & Sarker (2023)
Deep Learning	Malware and behavioral analysis	Detects complex attack patterns	Mohamed (2025); Khan et al. (2024)
Natural Language Processing	Threat intelligence and incident analysis	Extracts actionable information from unstructured data	Mohamed (2025)
Predictive Analytics	Threat forecasting and risk assessment	Supports proactive incident prevention	ABDULRAHMAN et al. (2025)
Agentic AI	Autonomous investigation and response	Enables adaptive decision-making and action	Kshetri (2025)
Automated Response Systems	Containment and remediation	Reduces response time and manual intervention	Chirra (2023); Maddireddy & Maddireddy (2023)
AI-Assisted Decision Support	Alert prioritization and response recommendations	Improves analyst efficiency and decision quality	Ismail et al. (2023); Uzoma et al. (2023)

3.5 AI-Assisted Decision Support and Automated Response

AI can support security analysts through dynamic risk scoring, incident prioritization, recommended response actions, and automated security playbooks. When integrated with Security Information and Event Management (SIEM), Security Orchestration, Automation and

Response (SOAR), Endpoint Detection and Response (EDR), and related technologies, AI can facilitate rapid containment actions such as isolating compromised endpoints, blocking malicious indicators, disabling suspicious accounts, and initiating recovery procedures (Maddireddy & Maddireddy, 2023; Uzoma et al., 2023). Such automation can reduce response time and improve consistency, although high-impact actions should remain subject to appropriate human and governance controls (Chirra, 2023; Ismail et al., 2023).



Note: Illustrative conceptual distribution synthesized from Mohamed (2025), Chirra (2023), Kshetri (2025), ABDULRAHMAN et al. (2025), Maddireddy and Maddireddy (2023), Ismail et al. (2023), and Uzoma et al. (2023).

Fig 2: Values represent illustrative relative levels of AI application across the incident-response lifecycle. The distribution conceptually reflects the roles of Machine Learning, Deep Learning, NLP, Predictive Analytics, Agentic AI, and Automated Response Systems as discussed by Mohamed (2025), Chirra (2023), Kshetri (2025), ABDULRAHMAN et al. (2025), Maddireddy and Maddireddy (2023), Ismail et al. (2023), and Uzoma et al. (2023).

IV. Implementation, Challenges, and Enterprise Governance

4.1 Enterprise AI Incident Response Architecture

Implementing AI in cybersecurity incident response requires an integrated architecture that connects security telemetry, threat intelligence, AI analytics, and automated response capabilities. Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Orchestration, Automation and Response (SOAR) platforms can provide the operational data required by AI models. These systems enable the collection and correlation of network, endpoint, identity, application, and cloud-security events before AI models classify anomalies and prioritize

incidents (Mohamed, 2025; Manoharan & Sarker, 2023).

An effective architecture should incorporate an AI decision layer capable of behavioral analysis, anomaly detection, threat classification, risk scoring, and response recommendation. The response layer can subsequently execute predefined playbooks for actions such as isolating compromised endpoints, blocking malicious indicators, disabling suspicious accounts, or escalating high-risk incidents to human analysts. AI-enabled automation therefore extends conventional incident response by connecting detection directly to coordinated containment and remediation (Chirra, 2023; Maddireddy & Maddireddy, 2023).

4.2 Automated Incident Response Workflow

AI can automate significant portions of the incident response lifecycle. Following alert ingestion, machine learning models can correlate security events and distinguish potentially malicious activity from normal behavior. Predictive analytics can then estimate the probability and potential impact of an incident, allowing security teams to prioritize the most consequential threats (ABDULRAHMAN et al., 2025).

The workflow can progress from detection → classification → investigation → risk assessment → containment → remediation → recovery → continuous learning. Automated playbooks can execute low-risk responses rapidly, while complex or high-impact decisions can be escalated to human analysts. This human-in-the-loop approach is important because complete automation can introduce operational risks when AI models produce inaccurate classifications or encounter previously unseen attack patterns (Ismail et al., 2023; Uzoma et al., 2023).

4.3 Agentic AI and Autonomous Response

Agentic AI represents an emerging development in cybersecurity because AI agents can perceive security events, reason about possible attack scenarios, select appropriate actions, and coordinate multiple defensive tasks. Rather than merely recommending a response, agentic systems can potentially execute multi-step investigations and adaptive containment activities with limited human intervention (Kshetri, 2025).

However, autonomy should be proportional to risk. Organizations can establish graduated response levels in which routine, low-risk actions are fully automated, while actions capable of disrupting critical business services require explicit human authorization. This approach combines the speed of autonomous AI with organizational accountability and operational

control.

4.4 Enterprise Governance and Human Oversight

Enterprise governance is necessary to ensure that AI-driven incident response remains secure, explainable, accountable, and aligned with organizational policies. Governance mechanisms should define who can approve automated actions, which systems may be modified automatically, how AI decisions are logged, and when incidents must be escalated to security personnel.

Organizations should also continuously monitor model performance, false-positive rates, detection accuracy, data quality, and model drift. AI systems require regular validation because changes in network architecture, user behavior, attack techniques, and threat landscapes can reduce model effectiveness over time (Mohamed, 2025; Khan et al., 2024).

4.5 Implementation Challenges

Despite its benefits, AI-driven incident response introduces several technical and organizational challenges. Poor-quality or incomplete security data can produce unreliable predictions, while excessive false positives may increase rather than reduce analyst workload. Adversaries may also exploit weaknesses in AI models through adversarial manipulation, data poisoning, or techniques designed to evade behavioral detection (Dalal, 2018; Mohamed, 2025).

Additional challenges include integration with legacy infrastructure, cybersecurity skills shortages, computational costs, privacy concerns, explainability requirements, and organizational resistance to autonomous decision-making. Consequently, AI should complement rather than completely replace experienced cybersecurity professionals (Chirra, 2023; Ismail et al., 2023).

4.6 Evaluation of AI-Driven Incident Response

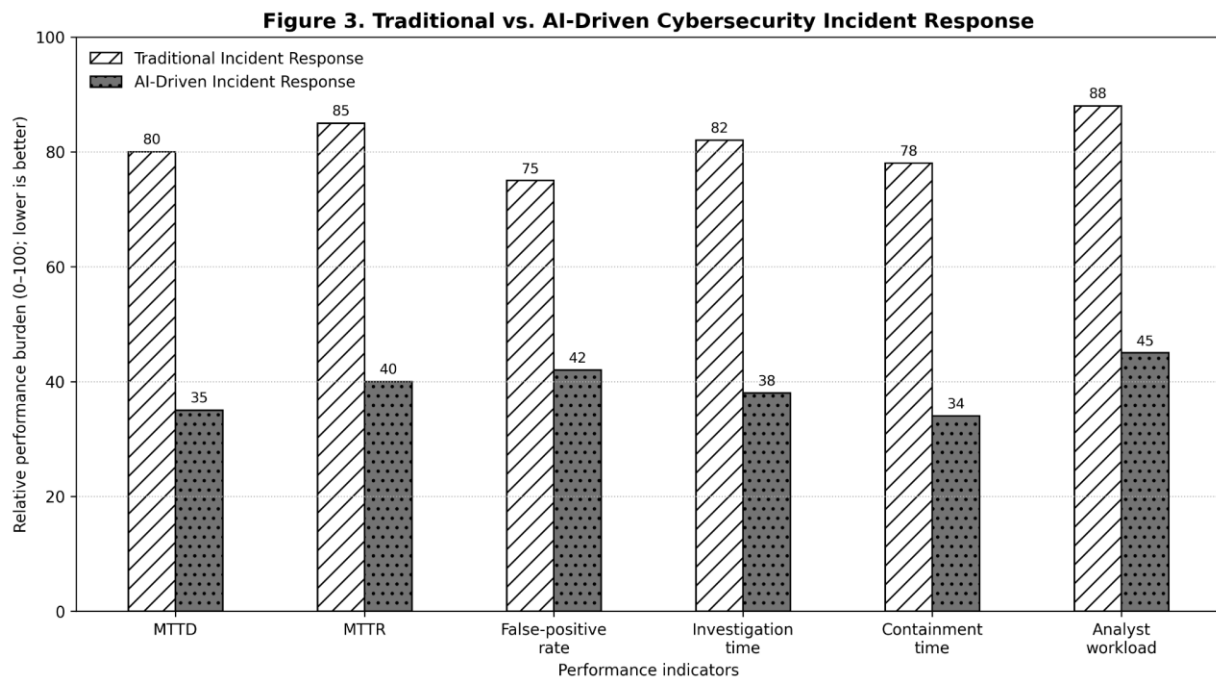
Evaluation should extend beyond detection accuracy to include operational measures such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), false-positive rate, containment success rate, analyst workload, automation coverage, and recovery time. These metrics allow organizations to determine whether AI produces measurable improvements in incident response rather than simply increasing technological complexity.

Table 3. Enterprise Challenges and Governance Strategies for AI-Driven Incident Response

Challenge	Potential Impact	Recommended Governance/Implementation Strategy
False positives	Alert fatigue and unnecessary response actions	Continuous model validation, threshold optimization, and human review
False negatives	Undetected or delayed attacks	Ensemble detection, threat-intelligence correlation, and continuous monitoring
Model drift	Declining detection performance	Periodic retraining, performance monitoring, and drift detection
Adversarial attacks	Manipulation or evasion of AI models	Adversarial testing, secure model development, and defensive monitoring
Poor-quality security data	Inaccurate classification and predictions	Data validation, normalization, and centralized telemetry management
Excessive automation	Unintended operational disruption	Risk-based automation and human-in-the-loop approval
Legacy integration	Implementation complexity	API-based integration with SIEM, SOAR, EDR, and XDR platforms
Lack of explainability	Reduced trust in AI decisions	Explainable AI, decision logging, and analyst-facing explanations
Privacy concerns	Unauthorized exposure of sensitive information	Data minimization, access controls, encryption, and privacy governance
Skills shortage	Difficulty operating and governing AI systems	AI-security training and multidisciplinary SOC teams
Agentic AI autonomy	Uncontrolled or inappropriate actions	Permission boundaries, action policies, audit trails, and escalation controls
Compliance requirements	Legal and organizational risk	Documented governance policies, monitoring, auditing, and accountability

Source: Synthesized from Mohamed (2025), Chirra (2023), Kshetri (2025), ABDULRAHMAN et al. (2025), Manoharan and Sarker (2023), Khan et al. (2024), Maddireddy and Maddireddy (2023), Ismail et al. (2023), and Uzoma et al. (2023).

AI-driven incident response can therefore be implemented effectively when automation, predictive intelligence, agentic capabilities, and human oversight operate within a clearly defined enterprise governance structure. Such an approach supports faster detection and response while limiting the risks associated with uncontrolled automation (ABDULRAHMAN et al., 2025; Kshetri, 2025).



Note: Lower scores indicate less time, fewer false positives, or lower analyst workload; values are illustrative for comparative visualization.

Fig 3: Values are illustrative relative performance-burden scores. Lower values indicate better outcomes, reflecting reduced detection and response times, fewer false positives, shorter investigation and containment periods, and lower analyst workload under AI-driven incident response.

V. Discussion

The integration of Artificial Intelligence (AI) into cybersecurity incident response represents a shift from predominantly reactive security operations toward intelligent, automated, and increasingly predictive defense. AI and Machine Learning (ML) can process large volumes of security events, identify abnormal patterns, correlate seemingly unrelated indicators, and support faster threat detection than conventional rule-based approaches. These capabilities are

particularly important as organizations face increasingly complex and rapidly changing cyber threats (Mohamed, 2025; Manoharan & Sarker, 2023).

5.1 AI-Enabled Detection and Investigation

AI strengthens incident response by improving anomaly detection, behavioral analysis, malware identification, and threat classification. Instead of treating every security alert independently, AI can correlate events across networks, endpoints, applications, and user activities to identify potentially coordinated attacks. This can reduce alert fatigue and allow security analysts to concentrate on high-priority incidents (Khan et al., 2024; Dalal, 2018). AI-driven investigation can also accelerate the identification of attack patterns and potential causes, supporting more informed response decisions (Chirra, 2023).

5.2 Automation and Response Efficiency

A major transformation occurs when AI is integrated with automated response mechanisms. AI-enabled systems can evaluate incidents, assign risk levels, recommend appropriate actions, and initiate predefined containment or remediation procedures. Such capabilities can reduce Mean Time to Respond (MTTR) and limit the potential impact of successful attacks (Maddireddy & Maddireddy, 2023; Ismail et al., 2023). Automated incident response is particularly valuable in environments where the volume and speed of security events exceed the capacity of human analysts (Uzoma et al., 2023).

5.3 Predictive Analytics and Cyber Resilience

AI extends incident response beyond identifying ongoing attacks by supporting predictive cybersecurity. By analyzing historical incidents, behavioral patterns, threat intelligence, and network activity, predictive models can identify indicators associated with emerging threats and provide early warnings. This strengthens organizational cyber resilience by enabling security teams to prepare defensive measures before incidents escalate (ABDULRAHMAN et al., 2025). Consequently, AI changes incident response from a purely reactive function into a more proactive risk-management capability.

5.4 Agentic AI and Autonomous Response

The emergence of agentic AI introduces a further development in cybersecurity operations.

Agentic systems can potentially interpret security events, determine appropriate actions, execute response workflows, and continuously adapt based on environmental feedback. This creates opportunities for more autonomous Security Operations Centers (SOCs), particularly for repetitive and time-sensitive incidents. However, greater autonomy also increases the importance of access controls, explainability, human oversight, and clearly defined operational boundaries (Kshetri, 2025).

5.5 Challenges and Human Oversight

Despite its benefits, AI should not be regarded as a complete replacement for cybersecurity professionals. False positives, inaccurate classifications, model drift, adversarial manipulation, poor-quality training data, and insufficient explainability can undermine automated decisions (Mohamed, 2025; Khan et al., 2024). AI-driven response systems therefore require continuous monitoring, validation, and governance. Human analysts remain particularly important when incidents involve significant business, legal, financial, or operational consequences. Effective implementation should consequently emphasize human-AI collaboration, where AI handles high-volume analytical and routine response tasks while security professionals retain authority over complex and high-risk decisions (Chirra, 2023; Ismail et al., 2023).

5.6 Overall Implication

Overall, AI is transforming cybersecurity incident response by integrating intelligent detection, automated investigation, predictive threat analysis, and adaptive response into a more coordinated security lifecycle. The combined contributions of AI/ML, predictive analytics, and agentic technologies suggest that future incident response will increasingly emphasize speed, contextual awareness, automation, and continuous adaptation. Nevertheless, sustainable adoption depends on balancing automation with governance, transparency, security controls, and human judgment (Dalal, 2018; Maddireddy & Maddireddy, 2023; Kshetri, 2025).

VI. Conclusion

AI is transforming the nature of cybersecurity incident response, helping organisations transition from being mostly reactive and manual, to being more intelligent, predictive, and more automated in their defense. By leveraging AI and machine learning, organizations can enhance their capacity to detect anomalies, correlate security events, identify advanced attack

patterns, and prioritize incidents based on their potential impact, thereby fortifying the effectiveness of their security operations (Mohamed, 2025; Manoharan & Sarker, 2023; Khan et al., 2024). AI-powered incident response systems can also streamline the investigation, containment, and remediation process, mitigating response delays and alleviating the workload of cybersecurity analysts (Chirra, 2023; Maddireddy & Maddireddy, 2023; Ismail et al., 2023). Predictive analytics can further support this shift by enabling organizations to predict potential attacks and implement pro-active cyber-resilience measures (ABDULRAHMAN et al., 2025). Simultaneously, agentic AI fosters greater autonomy by allowing security systems to evaluate threats, make contextually appropriate decisions, and take action to respond to those threats with minimal human involvement (Kshetri, 2025). But careful consideration must be given to false positives, model reliability, adversarial manipulation, explainability, data quality, and human oversight to ensure that the model has a positive impact in adoption. AI should therefore be used in tandem with human cybersecurity experts, especially in cases of making critical organizational decisions during cybersecurity incidents (Dalal, 2018; Uzoma et al., 2023). In conclusion, the integration of AI into SIEM, SOAR, threat intelligence, endpoint security, and traditional incident response systems can help organizations leverage AI to enhance their cybersecurity capabilities in these ways. So the future of incident response is intelligent automation, human expertise, continuous learning, robust governance and suitable security controls.

References

1. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67(8), 6969-7055.
2. Chirra, D. R. (2023). Towards an AI-Driven Automated Cybersecurity Incident Response System. *International Journal of Advanced Engineering Technologies and Innovations*, 1(01), 429-451.
3. Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy*, 49(6), 102976.
4. ABDULRAHMAN, I. A., OGOR, U. C., AYODELE, G. T., ANADOZIE, C., & ALEBIOSU, J. (2025). AI-Driven Threat Intelligence and Automated Incident Response: Enhancing Cyber Resilience through Predictive Analytics. *Research Journal in Civil*,

Industrial and Mechanical Engineering, 2(1), 16-32.

5. Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: <https://www.doi.org/10.56726/IRJMETS32644>, 1.
6. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The most recent advances and uses of AI in cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3(4), 566-578.
7. Dalal, A. (2018). Cybersecurity and artificial intelligence: How ai is being used in cybersecurity to improve detection and response to cyber threats. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 9(3), 10-61841.
8. Aremu, A., & Anifowose, K. (2026). Global Marketing Strategies for Biotech-Based Consumer Products: Opportunities and Challenges. Well Testing Journal, 35(3), 163-178.
9. Gamba, K., & Ogar, A. (2026). Mental Health Awareness and Comprehension of Substance Use Consequences: An Analysis of students in the Department of Medicine & Surgery at University of Abuja, Nigeria. Journal of Medical and Health Studies, 7(4), 15-35.
10. Moetiara, E. (2025). Enhancing Contractor Health Risk Governance in High-Hazard Industries: A Risk-Based Prequalification and Monitoring Model from the Oil and Gas Sector. Journal of Science Technology and Social Transformation, 1(02), 17-25.
11. Anifowose, K. (2025). Development and Validation of AI-Assisted Analytical Methods for Biochemical Compound Detection in Pharmaceutical Chemistry. Journal of Applied Pharmaceutical Sciences and Research, 8(4), 41-52.
12. Gamba, K., Chase, S., Guidinger, K., & Saine, C. (2025). Empowered Healing: Unpacking Trauma from Within. International Journal of Research and Innovation in Social Science.
13. Ojuri, M. A. (2021). Measuring Software Resilience: A QA Approach to Cybersecurity Incident Response Readiness. Multidisciplinary Innovations & Research Analysis, 2(4), 1-24.
14. Awodire, M. (2022). Trend Analysis in Recurring IT Security Findings: What Repeated Vulnerabilities Reveal About Systemic Control Weaknesses. International Journal of Technology, Management and Humanities, 8(04), 119-145.
15. Taiwo, S. O. (2022). PFAI™: A predictive financial planning and analysis intelligence framework for transforming enterprise decision-making. International Journal of

- Scientific Research in Science Engineering and Technology, 10.
16. Ojuri, M. A. (2022). The Role of QA in Strengthening Cybersecurity for Nigeria's Digital Banking Transformation. *Well Testing Journal*, 31(1), 214-223.
 17. Ezeagwuna, D. (2022). Measuring Return on Investment (ROI) in Enterprise Service Management: The Role of Service Now in Enhancing Organizational Efficiency and Cost Reduction. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, 12(02), 59-71.
 18. Ojuri, M. A. (2022). Cybersecurity Maturity Models as a QA Tool for African Telecommunication Networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, 14(04), 155-161.
 19. Begum, S. (2022). Optimizing capital deployment in post-pandemic America: AI-powered predictive analytics for startup resilience and growth. *International Journal of Computer Applications Technology and Research*, 11(12), 700-710.
 20. Ojuri, M. A. (2021). Evaluating Cybersecurity Patch Management through QA Performance Indicators. *International Journal of Technology, Management and Humanities*, 7(04), 30-40.
 21. Ojuri, M. A. (2023). Risk-Driven QA Frameworks for Cybersecurity in IoT-Enabled Smart Cities. *Journal of Computer Science and Technology Studies*, 5(1), 90-100.
 22. Taiwo, S. O., Aramide, O. O., & Tiamiyu, O. R. (2023). Blockchain and federated analytics for ethical and secure CPG supply chains. *Journal of Computational Analysis and Applications*, 31(3), 732-749.
 23. Areghan, E. (2023). From Data Breaches to Deepfakes: A Comprehensive Review of Evolving Cyber Threats and Online Risk Management. *Communication in Physical Sciences*, 9(4), 538-553.
 24. Awodire, M. (2023). Cost optimization strategies (tagging, rightsizing, capacity planning) in enterprise cloud operations. *International Journal of Technology, Management and Humanities*, 9(04), 307-317.
 25. Ezeagwuna, D. (2023). The Impact of Low-Code/No-Code Platforms on Business Innovation: A Study of Service Now's Contribution to Enterprise Agility and Digital Growth. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, 13(02), 90-99.
 26. Taiwo, S. O., Tiamiyu, O. R., & Ayodele, O. M. (2023). Unified predictive analytics architecture for supply chain accountability and financial decision optimization in CPG

- and manufacturing networks. *Journal of Information Systems Engineering and Management*, 8(4).
27. Ojuri, M. A. (2023). AI-Driven Quality Assurance for Secure Software Development Lifecycles. *International Journal of Technology, Management and Humanities*, 9(01), 25-35.
 28. Ezeagwuna, D. (2026). AI-Driven Intrusion Detection Systems for Cybersecurity. *Journal of Science Technology and Social Transformation*, 2(02), 37-51.
 29. Mukherjee, C. (2026). AI-Based Detection of Deepfakes and Misinformation on Social Media. *Euro Vantage journals of Artificial intelligence*, 3(2), 9-30.
 30. Mehta, S. (2026). Architecting AI Governance & 'Agent-ready' data layer: Semantic Governance for Autonomous AI workflows. *Journal of Science Technology and Social Transformation*, 2(02), 29-36.
 31. Awodire, M. (2026). Researching Business Processes and Enterprise Architecture in Public Transit Dispatch Operations. *Journal of Integrated Science, Technology and Management*, 2(03), 1-13.
 32. Ezeagwuna, D. (2026). Digital Transformation and Business Resilience: How Service Now-Powered Automation Improves Organizational Performance, Risk Management, and Customer Satisfaction. *Journal of Data Analysis and Critical Management*, 2(01), 48-62.
 33. Oloruntoba, O., Odum, P., Audu, K., Adepoju, S., Ugboko, R., & Tihamiyu, O. R. (2026). Resilient geospatial data management: a comparative analysis of cloud-native and distributed ledger technology synchronization models for multi-cloud environments. *Journal of Cloud Computing*, 15(1), 87.
 34. Mehta, S. (2026). From Reactive cleanup to Real-time observability: Modernizing Enterprise Data Quality for RAG pipelines. *Journal of Science Technology and Social Transformation*, 2(01), 35-44.
 35. Oloruntoba, O., Odum, P., Audu, K., Adepoju, S., Ugboko, R., & Tihamiyu, O. R. (2026). Resilient geospatial data management: a comparative analysis of cloud-native and distributed ledger technology synchronization models for multi-cloud environments. *Journal of Cloud Computing*, 15(1), 87.
 36. Jobiullah, M. I., Begum, S., Ali, M. M., Rahman, M. M., Emon, M. S. A., & Fatima, K. (2026, April). A Machine Learning-based National Startup Capital Readiness Scoring

- Platform: Design, Implementation, and Comparative Evaluation. In 2026 9th International Conference on Inventive Computation Technologies (ICICT) (pp. 1893-1899). IEEE.
37. Ezeagwuna, D. (2026). Enhancing Organizational Cyber Resilience Through the NIST Cybersecurity Framework. *International Journal of Technology, Management and Humanities*, 12(01), 124-140.
 38. Kola, J. N. (2026, June). Secure Financial Analytics Platforms for Regulatory Compliance and Risk Management. In 2026 IEEE 18th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 794-801). IEEE.
 39. Awodire, M. (2026). Demystifying important issues concerning management of global IT resources in the Public Transit Sector in the US. *Journal of Science Technology and Social Transformation*, 2(03), 1-15.
 40. Kola, J. N. (2026). Enterprise Business Intelligence and Financial Analytics with a focus on Enterprise Data Architecture and Predictive Risk Integration. *Adhyayan: A Journal of Management Sciences*, 16(01), 20-28.
 41. Begum, S., Akbar, Z., Islam, M. S., Rahman, M. A., Rahman, M. M., Hossen, B., ... & Raj, M. W. Z. (2026, February). IHPO-XGBoost for ESG Performance Prediction: A High-Accuracy Machine Learning Framework. In 2026 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL) (pp. 1558-1564). IEEE.
 42. Awodire, M. (2026). Responsible AI governance frameworks: bias mitigation, fairness, and compliance in production AI deployments. *Journal of Science Technology and Social Transformation*, 2(03), 26-35.
 43. Ravikumar, V. (2025). Therapeutic Bot: Ethical Concerns in AI therapy for Neurodivergence. *J Int Scient Re Rep*.
 44. Areghan, E. (2025). Cyber Resilience in Digital Twin and Smart Manufacturing Environments: Challenges, Strategies, and Future Direction. *Journal of Computational Analysis and Applications*, 34(8), 573-593.
 45. Awodire, M. (2025). Data governance and privacy-by-design frameworks (GDPR/HIPAA) in multi-cloud data pipelines. *Journal of Data Analysis and Critical Management*, 1(02), 116-126.
 46. Mehta, S. (2025). Enhancing Enterprise Data Governance Maturity Through Cloud Based Data Integration Frameworks in Modern Organizations. *International Journal of*

Technology, Management and Humanities, 11(01), 59-67.

47. Jimoh, M., & Khadijah, A. (2025). Hydroinformatics and GIS Integration for Intelligent Water Resource Management. *International Journal of Scientific Research in Science and Technology*, 12(3), 1470-1489.
48. Begum, S., Hassaan, A., Hussain, M. A., Mudaber, M., Jamshaid, Z. A., Niaz, S., & Jobiullah, M. I. (2025). AI-driven fraud detection in real-time financial transactions: A deep learning approach. *Well Testing Journal*, 34, 727-748.
49. Areghan, E. (2025). Emerging Frontiers in Cybersecurity: Navigating AI-Powered Threats, Quantum Risks, and the Rise of Zero-Trust Architectures. *International Journal of Advanced Trends in Computer Science and Engineering* 14 (3). 120, 136.
50. Ojuri, M. A. (2025). Ethical AI and QA-Driven Cybersecurity Risk Mitigation for Critical Infrastructure. *Euro Vantage journals of Artificial intelligence*, 2(1), 60-75.
51. Omolayo, O., Oloruntoba, O., Adepoju, S., & Audu, K. (2025). Comparative Analysis of Graph Partitioning Strategies for Enhancing Scalability and Performance in Distributed Graph Databases.
52. Nwaneto, C., Nwaneto, C. P., & Fasasi, S. T. (2024). The Hidden Cost of Scope Ambiguity: Why OFCI vs. CFCI Delineation Breaks Data Center Budgets. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, 16(04), 214-222.
53. Rehan, H., Janjua, J. I., Ali, R. A., & Khan, T. A. (2025, December). AI-Driven DNA Insights and Public Health Data Integration for Enhancing Personal Healthcare in Critical Disease Prevention. In *2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU)* (pp. 1-6). IEEE.
54. Awodire, M. (2025). Master Data Management (MDM) integration strategies in hybrid cloud environments. *Journal of Data Analysis and Critical Management*, 1(04), 41-50.
55. Ezeagwuna, D. (2025). Artificial Intelligence for IT Service Management: Developing a Framework for ROI Optimization Using Service Now and Machine Learning Technologies. *Well Testing Journal*, 34(S4), 394-419.
56. Chukwu, M., Huang, X., Audu, K., Wang, H., & Subasish, D. (2025). Unequal paths to nature: Mobile-phone insights into park visits in nine major cities in the United States. *Urban Forestry & Urban Greening*, 129196.
57. Nwaneto, C., Fasasi, S. T., & Jimoh, A. (2025). Advanced Building Information

- Modeling and Construction Management Integration for Project Cost Control and Schedule Optimization. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 17(01), 36-45.
58. Mehta, S. (2025). Role of Metadata Management and Data Governance in Achieving Regulatory Compliance in Enterprise Data Ecosystems. International Journal of Technology, Management and Humanities, 11(02), 144-152.
 59. Naidu, K. J. (2013). Performance Optimization Of ETL Pipelines In Distributed Data Warehouse Environments: A Network-Aware Scheduling Approach. International Journal of Advance Industrial Engineering, 1(03), 63-67.
 60. Ojuri, M. A. (2025). Quality Metrics for Cybersecurity Testing: Defining Benchmarks for Secure Code. Well Testing Journal, 34(S3), 786-801.
 61. Begum, S. (2025). Artificial intelligence and economic resilience: A review of predictive financial modelling for post-pandemic recovery in the United States SME sector. International Journal of Innovative Science and Research Technology, 10(7), 3620-3627.
 62. Nwaneto, C., Jimoh, A., & Nwaneto, C. P. (2024). Energy Audit Comparison between Residential and Commercial Buildings in Denver and Other Climate Zones. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 16(04), 223-235.
 63. Maddireddy, B. R., & Maddireddy, B. R. (2023). Enhancing network security through AI-powered automated incident response systems. International Journal of Advanced Engineering Technologies and Innovations, 1(02), 282-304.
 64. Ismail, B. I., Abdul, S., Khan, S. M., Sattar, S. A., & Muhammad, S. (2023). AI for cyber security: Automated incident response systems. Available at SSRN 5477114.
 65. Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., & Obunadike, E. (2023). Using artificial intelligence for automated incidence response in cybersecurity. International Journal of Information Technology (IJIT), 1(4), 1-32.