

Comparative Analysis: Traditional vs. AI-Driven Incident Detection and Response Systems

Bertrand Kalisa, Landry Ishimwe Karangwa, Fred Shumbusho

Computer Science and Computer Engineering

University of Arkansas

¹Bmakalisa@uark.edu

²leishimw@uark.edu

³fshumbus@uark.edu

Abstract

As cyber threats grow in complexity and frequency, the need for timely and effective incident detection and response (IDR) systems has become more pressing than ever. This paper compares traditional rule-based detection methods with AI-driven systems, focusing on key metrics such as detection accuracy, false positive/negative rates, and operational efficiency. Through analysis of recent research and public datasets, the study finds that while traditional systems remain reliable for detecting known threats, AI-powered systems offer superior performance, especially in handling evolving and unknown threats. The paper also discusses trade-offs, limitations, and future considerations in adopting AI-based cybersecurity infrastructure.

Keywords: Intrusion Detection Systems (IDS), Incident Detection and Response (IDR), Intrusion Detection Systems (IDS), Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Security Orchestration, Automation, and Response (SOAR), False Positive Rate (FPR), False Negative Rate (FNR), Mean Time to Identify (MTTI), and Mean Time to Contain (MTTC)

I. Introduction

Incident Detection and Response (IDR) refers to the identification, containment, eradication, and recovery process in the event of a security incident such as malware infections, unauthorized access, or data breaches. As organizations depend more on digital operations, the integrity of IDR systems directly impacts both security posture and business continuity.

Traditionally, IDR has relied on predefined rule sets and human analysis to identify threats. While effective for detecting known attack vectors, this approach falters in the face of polymorphic malware, zero-day vulnerabilities, and increasingly sophisticated threat actors. The emergence of Artificial Intelligence (AI) has led to the development of more dynamic and adaptive detection systems that promise better accuracy, reduced response time, and lower operational burden.

This study aims to provide a comparative analysis between traditional and AI-driven detection systems, examining their respective methodologies, effectiveness, and real-world implications. The analysis is divided into key focus areas such as detection accuracy, response speed, cost-effectiveness, and operational limitations.

II. Background

Traditional IDR systems are largely signature-based. They work by scanning network traffic and system logs for known patterns of malicious activity. Tools like Snort and Suricata exemplify this method, offering fast and low-resource intrusion detection. However, their rigidity makes them ineffective against previously unknown threats or sophisticated obfuscation techniques.

To address these limitations, anomaly-based systems were developed. These systems model baseline behavior and raise alerts when deviations are detected. While this improves the ability to detect unknown threats, it introduces a high false positive rate, requiring more analyst time for triage.

AI-driven systems advance this idea by using machine learning (ML) and deep learning (DL) models trained on labeled data or unsupervised clustering techniques. These models can generalize from historical data and identify patterns beyond static rule sets. Despite their advantages, AI models also introduce challenges such as high computational cost, model explainability issues, and potential vulnerability to adversarial attacks.

III. Overview

This paper is organized into three core comparative analyses that each highlight a critical dimension of traditional versus AI-driven IDR systems. The first is a comparative analysis on baseline detection methods and accuracy, which evaluates how each system identifies threats and handles detection accuracy and error rates. The second explores response speed and automation efficiency, addressing how quickly and effectively each approach responds to security incidents. The final section focuses on operational costs and adoption barriers, analyzing resource usage, infrastructure expenses, and the organizational challenges involved in deploying AI-based detection frameworks.

Each section synthesizes recent research, industry findings, and experimental datasets to support a multidimensional understanding of how traditional and AI-driven methods perform in real-world security operations. Together, these perspectives provide a comprehensive look at the trade-offs of adapting one of the systems and advantages inherent to both detection paradigms.

A. Comparative Analysis on Baseline Methods & Detection Accuracy

To analyze the effectiveness of traditional and AI-driven IDR systems, we reviewed findings from three recent and relevant academic sources: Reddy et al. (2024), MDPI Journal on Computing (2024) and Nature Scientific Reports (2025)

Each study evaluated the performance of various detection approaches using benchmark datasets such as CICIDS2017, UNSW-NB15, NSL-KDD, and KDD Cup 99. These datasets contain a mix of normal and malicious traffic, covering a broad spectrum of attack types including DDoS, insider threats, malware infections, and port scans.

Performance was assessed using four core metrics:

- **Detection Accuracy:** Proportion of actual threats correctly identified.
- **False Positive Rate (FPR):** Benign events mistakenly flagged as malicious.
- **False Negative Rate (FNR):** Threats that evade detection.
- **Response Time:** Time taken to detect and respond to an incident.

Traditional baseline detection methods rely on fixed signatures or predefined rules to flag threats. While effective in detecting known patterns, they often generate high volumes of false positives and fail to recognize novel or modified threats. Signature-based detection is fast and computationally inexpensive, making it suitable for environments where known threats dominate.

Anomaly-based systems, an evolution of traditional approaches, introduce behavior modeling to detect deviations. While this improves the ability to identify unknown attacks, it also increases the rate of false positives. Analysts often struggle with alert fatigue, diverting attention from real threats.

AI-driven detection methods employ supervised learning models such as support vector machines, random forests, and decision trees, which are trained on historical attack data. Deep learning models like convolutional neural networks and long short-term memory networks further enhance detection by learning complex temporal and spatial relationships in traffic data.

So, according to Reddy et al. (2024), traditional IDS systems achieve around 89% detection accuracy but suffer from high false positive rates (8–10%). In contrast, AI-powered systems reached up to 98.6% detection accuracy with a false positive rate as low as 1.9%. Deep learning models were particularly effective in recognizing complex, evolving threats such as polymorphic malware and insider attacks.

Despite the performance gains, AI systems introduce their own set of challenges. Overfitting, data privacy, and lack of interpretability remain persistent issues. Moreover, they require significant compute resources and careful tuning to avoid learning irrelevant or biased patterns.

In summary, AI-based methods significantly improve detection accuracy and reduce error rates, making them better suited for dynamic threat environments. However, due to their resource demands and complexity, a hybrid model that combines traditional speed with AI's adaptability is often the most effective solution in operational settings.

B. Comparative Performance Analysis: Speed and Efficiency

Analyzing quantitative data reveals significant differences in response speed and efficiency between traditional manual incident response and AI-driven SOAR-based approaches. While precise benchmarks are difficult due to variations in organizational maturity, incident complexity, and metric definitions , available data points and vendor reports illustrate clear trends.

Industry Data Points:

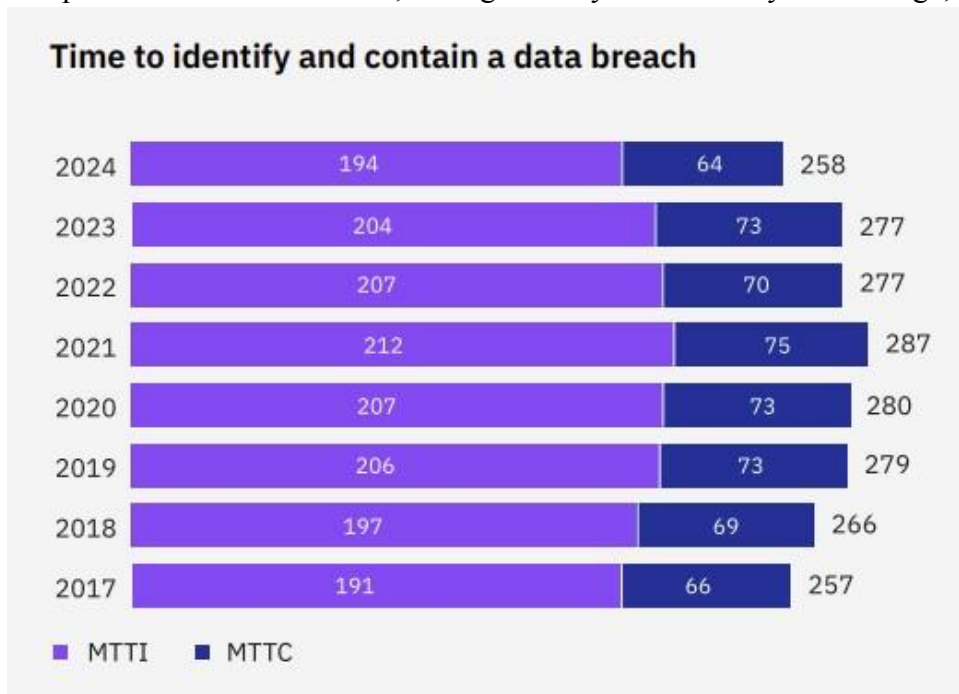
- **Mandiant Data:** Mandiant, now part of Google Cloud, is a recognized leader in dynamic cyber defense, threat intelligence, and incident response services. Its annual M-Trends report offers key insights into attacker behaviors and the effectiveness of organizational detection and response efforts. One of the core metrics reported is dwell time, the number of days an attacker remains in a compromised environment before detection. This measure is critical for understanding how long threat actors can operate undetected, with the median value representing the midpoint in a sorted data set.

The 2025 M-Trends report, based on Mandiant Consulting investigations conducted throughout 2024, revealed a significant reduction in dwell time over the past decade. In 2014, the overall median dwell time was 205 days, whereas by 2024, it had dropped to just 11 days. Notably, dwell time for intrusions discovered internally, through security alerts or reports from personnel, remained shorter than those identified via external notifications such as from law enforcement, cybersecurity firms, industry partners, or even adversaries themselves through ransom notes. This trend underscores the growing importance and effectiveness of internal threat detection capabilities.

Median Dwell Time, 2011-2024

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11
External	—	—	—	—	320	107	186	184	141	73	28	19	13	11
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9	10

- **IBM Data:** Detecting data breaches remains a persistent challenge across all industries, regardless of the response approach. According to the IBM Cost of a Data Breach Report 2024, the global average time to identify and contain a breach was 258 days, with the average time to detect alone being 194 days, as shown in the figure below. Even in the well-regulated financial sector, the average detection time was still 168 days. Breaches involving stolen or compromised credentials were particularly difficult to uncover and mitigate, taking an average of 292 days longer than any other attack vector. Similarly, breaches exploiting employee access, such as phishing and social engineering attacks, also proved difficult to resolve, lasting 261 days and 257 days on average, respectively.



IV. Limitations of Traditional Incident Response

Traditional IR processes, often heavily reliant on manual efforts, struggle to keep pace with the current threat landscape. Key limitations include:

- **Slow Response Times:** Manual investigation, analysis, and remediation steps inherent in traditional IR lead to significant delays in detection, containment, and recovery, increasing the window of opportunity for attackers and amplifying potential damage. The average time to identify and contain a breach can extend to hundreds of days.
- **Analyst Burden and 'Toil':** Security analysts are often consumed by repetitive, low-value tasks such as manual log review, alert triage, data enrichment, and basic containment actions. This type of work, often referred to as 'toil' in Site Reliability Engineering (SRE) contexts, is manual, repetitive, automatable, tactical, offers no enduring value, and scales linearly with service growth, consuming valuable analyst time and contributing to burnout.
- **Alert Fatigue and Inconsistency:** The sheer volume of alerts generated by disparate security tools overwhelms analysts, leading to 'alert fatigue' where critical alerts may be

missed. Manual processes are also prone to inconsistency and human error, particularly under pressure.

- **Scalability Challenges:** Manual IR processes do not scale effectively with the growth of IT infrastructure, increasing attack surfaces, or rising threat volumes. Adding more analysts is often unsustainable due to cost and talent shortages.
- **High Operational Costs:** The reliance on manual labor, the inefficiencies of tool-switching, and the extended time frames associated with manual response contribute significantly to the high operational costs of traditional IR.

V. AI-Driven Incident Response (SOAR) Workflow

AI-driven incident response, primarily facilitated by Security Orchestration, Automation, and Response (SOAR) platforms, represents a significant evolution from traditional manual methods. SOAR technology aims to connect disparate security tools, automate repetitive tasks, and orchestrate complex workflows to accelerate incident handling with potentially minimal human intervention. Gartner defines SOAR as technologies enabling organizations to collect security threat data and alerts, perform analysis and triage using both human and machine power, and drive standardized incident response activities through digital workflows.

The core capabilities of SOAR platforms are:

- **Security Orchestration:** This refers to the integration and coordination of various security tools and technologies (e.g., SIEM, EDR, firewalls, threat intelligence platforms, vulnerability scanners, email security gateways) from potentially different vendors. SOAR platforms use APIs, pre-built connectors, or custom integrations to allow these tools to communicate and work together seamlessly within a unified console. This eliminates the need for analysts to manually pivot between different tool interfaces, streamlining workflows. Orchestration enables the coordination of complex actions across multiple systems as defined in playbooks.
- **Security Automation:** SOAR platforms automate repetitive, time-consuming, and often low-level tasks within the incident response lifecycle. Common automated tasks include alert triage, data enrichment (e.g., automatically querying threat intelligence feeds for IP/domain reputation, gathering user context), opening/closing tickets, executing containment actions (like blocking an IP, isolating an endpoint, disabling a user account), scanning for vulnerabilities, or removing malicious files. This automation is typically driven by "playbooks" or "runbooks".
- **Response:** SOAR platforms provide a central console for managing incidents, tracking progress, documenting actions, and facilitating collaboration among security team members. They often include case management features, dashboards for visualizing metrics and operational status, and reporting capabilities. Some platforms incorporate AI and machine learning (ML) to analyze data, identify patterns, prioritize alerts more intelligently, suggest response actions, or even dynamically adapt playbooks based on evolving threats.

Typical AI/SOAR Workflow:

- **Alert Ingestion:** SOAR platforms ingest alerts from integrated security tools (SIEM, EDR, email filters, etc.).
- **Automated Triage and enrichment:** Upon receiving an alert, the SOAR platform often triggers a predefined playbook. Initial steps typically involve automated triage (classifying alert severity based on rules) and enrichment (gathering contextual information from threat intelligence feeds, asset databases, user directories, vulnerability scanners, etc.).
- **Playbook Execution:** Based on the enriched alert data and playbook logic, the SOAR platform automatically executes subsequent steps. This might involve further investigation actions (e.g., detonating a suspicious file in a sandbox), containment actions (e.g., isolating the host via EDR integration, blocking the sender's domain), or notification actions (alerting relevant personnel). These actions are orchestrated across multiple integrated tools.
- **Human Intervention Point:** Playbooks can be designed to be fully automated or include specific points requiring human review and approval before critical actions (like system shutdowns or widespread blocking) are taken. This allows for expert judgment in sensitive situations.
- **Case Management and Reporting:** All actions, findings, and data are typically logged within the SOAR platform's case management system, providing a detailed audit trail and facilitating post-incident reporting.

By automating and orchestrating these steps, SOAR platforms aim to significantly reduce the time taken for detection, validation, investigation, containment, and initial remediation, shifting the focus of human analysts towards more complex threats and strategic tasks.

VII. Automation vs. Human Intervention: A Balanced Perspective

The integration of AI and automation via SOAR platforms introduces significant efficiencies but also necessitates a careful evaluation of the balance between automated processes and human expertise in incident response.

The Efficiency Gains of Automation (via SOAR):

- **Speed:** Automation dramatically accelerates response actions, reducing timelines from hours or days to minutes or even seconds for specific tasks like enrichment, initial containment, and notification.
- **Scale:** Automated systems can handle a vastly larger volume of alerts and incidents concurrently than human teams, overcoming limitations imposed by staffing levels and preventing analysts from being overwhelmed.
- **Consistency:** Playbooks ensure that responses are executed in a standardized, repeatable manner every time, reducing variability based on individual analyst experience or workload and aiding compliance efforts.
- **Resource Optimization:** By automating routine, low-level tasks (e.g., alert triage, IOC lookups, basic containment), SOAR frees up highly skilled security analysts to focus on more complex investigations, threat hunting, strategic analysis, and proactive security measures. This can also improve job satisfaction and retention by reducing tedious work.

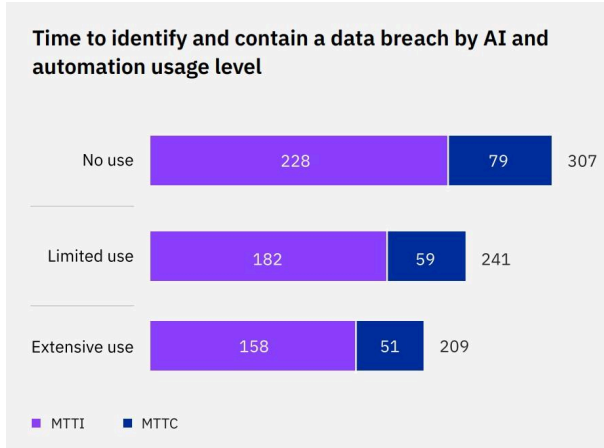
- **Cost Reduction:** Faster detection, response, and particularly containment (lower MTTC) directly translate to reduced costs associated with data breaches, system downtime, and recovery efforts. Automation can lower overall operational costs over time.
- **Accuracy:** For well-defined, repetitive procedures, automation minimizes the risk of human error inherent in manual data entry, command execution, or checklist following.

The Irreplaceable Value of Human Expertise:

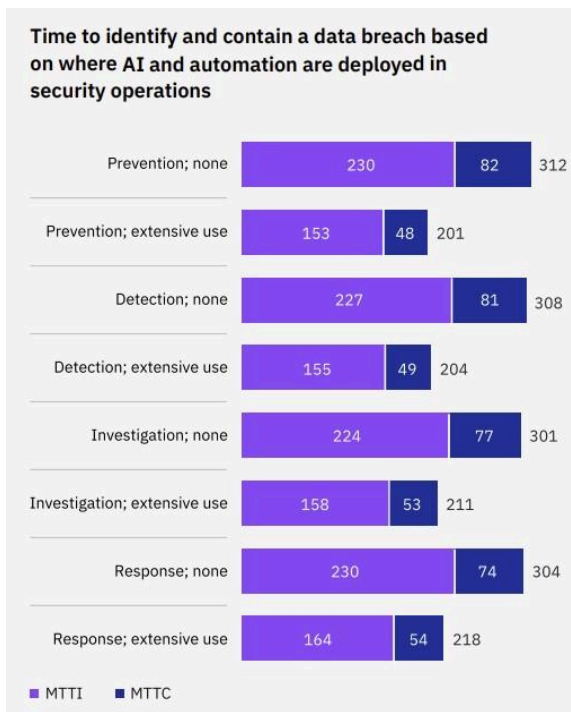
- **Contextual Understanding and Nuance:** Human analysts possess the ability to understand the broader business context, assess potential operational impacts of response actions, interpret ambiguous data, and recognize subtle patterns that purely algorithmic approaches might miss.
- **Novelty and Adaptability:** Responding effectively to zero-day exploits, sophisticated Advanced Persistent Threats (APTs), or entirely new attack vectors often requires human creativity, intuition, and adaptive problem-solving capabilities that go beyond the logic encoded in predefined playbooks. Humans can improvise when faced with unforeseen circumstances.
- **Complex Investigations and Root Cause Analysis:** Deep forensic investigations, unraveling complex attack chains, and determining the true root cause of sophisticated breaches often demand the critical thinking and analytical skills of experienced human investigators.
- **Strategic Decision Making:** Critical decisions during a major incident such as determining the appropriate level of containment versus operational impact, managing legal and regulatory obligations, coordinating public relations, or deciding on eradication strategies with long-term implications require human judgment and strategic oversight.
- **Automation Oversight and Refinement:** Humans are essential for designing, building, testing, and maintaining the automation itself (playbooks, integrations). They must also validate the outputs of automated systems, interpret AI-driven recommendations, handle exceptions where automation fails, and continuously improve playbooks based on lessons learned from real incidents.

AI's Impact on Breach Containment Speed:

- As illustrated in the figure below, organizations that made extensive use of security AI and automation identified and contained data breaches nearly 100 days faster on average compared to those that did not use these technologies at all. This dramatic improvement in speed underscores the value of AI-driven tools in accelerating breach detection and response, ultimately reducing the impact and cost of cyber incidents.

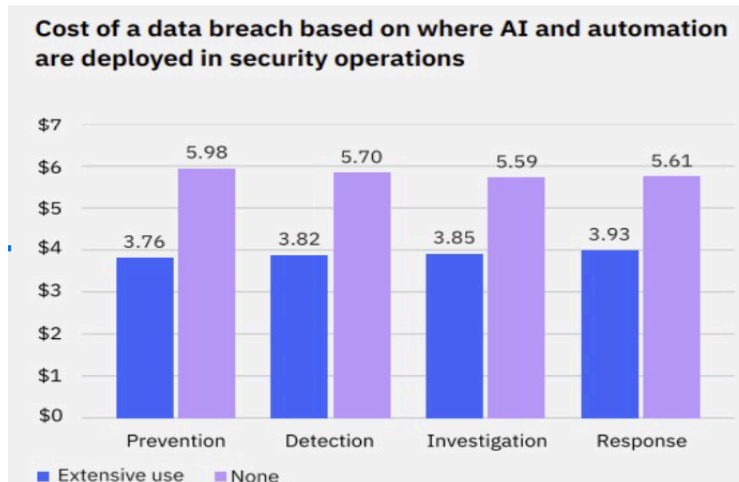


- The image below shows the application of AI and automation across security functions significantly accelerated the ability to identify and contain data breaches. Whether used in prevention, detection, investigation, or response, extensive implementation of these technologies consistently improved incident handling times. Specifically, organizations that used AI and automation extensively saw an average 33% reduction in mean time to identify (MTTI) and a 43% reduction in mean time to contain (MTTC) breaches in prevention-related scenarios, highlighting the critical role these tools play in speeding up cybersecurity operations.



VII. Cost Reductions from AI Adoption

The IBM Cost of Data Breach Report goes into detail of multiple advantages of adopting AI. The research conducted by them shows that the use of AI cut breach costs by 45.6% from USD 5.98 million to 3.67 million. It also lowered breach costs by up to a third when you compare it to traditional methods. It also reduced investigation costs by over 30 percent. When you combine these savings (prevention, detection, investigation and response as seen in the diagram below), it can save a company up to 5 million in annual cost avoidance.



- **Scalability & Resource Utilization**

When you consider the traditional SOC's, when there is an increase of alerts, let's say like ten-fold, that means hiring ten times more analysts and also that would mean buying ten times the hardware needed by those analysts. compared to AI platforms, when there is an increase of alert volume you may need to just scale up the compute and when there is calm you just scale down and don't pay for the idle servers. and also handling 100,000 more alerts would need a small cloud compute fee instead of hiring a new analyst and assigning them a new salary and a desk. when you use AI it also frees up almost four-fifths of SOC juniors according to Deloitte. when you adopt AI there is a shift from capital purchases to operational expenses which can improve financial predictions and can also lower the upfront cost hurdles.

- **Infrastructure & Compute Costs**

There is also a trade off when you compare the infrastructure cost of AI driven incident response and traditional IDS. With traditional, appliances that are on-premise will require maintenance and support, and they will also require depreciation costs each year whether you use those machines or not. With AI-driven, since they require powerful machines that usually use GPUs, this will need to be outsourced and the maintenance is usually done by other companies, so access to these high performing cloud instances will be billed per inference, and these fees just grow with usage. The cost that is saved by adapting AI services from companies like IBM is large, since this cost includes the power and cooling system cost that would have been used in the data centres. It also means IT teams spend less time on hardware upkeep, which saves the labour costs and the support overhead.

- **Always-On Monitoring & Overtime Savings**

When you adapt AI for detection, you will also save on the on-call shifts that would normally be used. This is because AI runs all day and, when you use it, you can even avoid paying up to 2× the wages that would normally be paid to off-hour shifts. These fewer night shifts mean that workers will be happier and will result in reduced hiring and training that would have come as a result of employees leaving. Some companies require “always-on monitoring,” and the adoption of AI will meet these service-level agreements, hence avoiding penalty fees for missed detection windows. Overall, there is a staffing budget reduction and reduced scheduling complexity that would have been caused by a 24×7 human roster when you adapt AI.

VIII. Adoption Limitations & Fears

Even though AI has a lot of advantages including a lot of savings that may come from adapting it, some companies have some hesitation when it comes to adapting it in their organisations. This is due to some risks and sometimes hidden costs that may come with AI. We will look at some of those fears which include adversarial Data poisoning, compliance gaps and 'black-box' systems that can require explainability tools. Deloitte research has found that attackers can sometimes feed bad data to AI models which can make them learn wrong patterns and also there is a need for real user logs to train AI which can expose personal data. All this will be looked at and more as we see barriers that may delay the adoption of AI into some companies.

- **Adversarial AI & Data Poisoning**

Since AI learns from data, Attackers can change malware enough to go past AI learnt patterns. Tiny changes like file headers can fool machine learning models and think malware is safe. the attackers can also hide some backdoor triggers while training. the model may appear normal until attackers send that hidden trigger then it misclassifies the attack. when public threat feeds have been poisoned, this can be bad for multiple organisations that may be using this shared data sources. a poisoned update can spread misclassification across very many users. there is also a fear that security teams may not be able to make the models hard enough against poisoning hence some organisations have a hesitation to adapt AI until they have a strong anti-poisoning safeguard. the lack of data-science skills needed by the former traditional analysis may delay the adoption of this AI tools.

- **Privacy Risks & Model Bias**

When Training AI on real logs, this can expose personal information like userIDs and IP addresses. if this information is not removed they might be seen by attackers hence organisations have to invest in log-scrubbings tools that can be used to remove this sensitive informations before they are used in AI pipelines. this process of Anonymizing data, which for a large organisation is usually a lot of data, takes time and computing resources and yet without this, organisations risk accidental data leaks when building or retraining AI models. There is also a risk of bias that may arise from training data that may have more examples from one user group. the AI will learn to favor that group's behavior and can cause false alarms for the underrepresented users. To prevent this, teams

must audit the datasets and then also collect balanced samples which comes with a cost of planning and labor time.

- **Governance, Compliance & Accountability**

The best AI adoption requires that you make policies, controls, and audit trails to meet the regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) . compared to static signature rules, AI models can change behavior over time, so organizations must log every model update and decision. That means having a record of all the datasets overtime, tracking model training parameters, and getting reports to show changes over time. Failing to provide transparent audit records can lead to the mistrust of shareholders which may have been caused by the fines that can be put to you. Building these governance layers requires deep communication between security and legal teams.may companies think that Ai will just plug in to the existing security systems yet it takes coding and alot of testing. companies need to plan for governance costs, dashboard creation and any other hidden costs that can come up.

- **Explainability & Integration Costs**

Ai models work like 'black boxes' where it gives you an output but it's hard to explain how it was generated. Hence you need tools like SHAP or LIME to help show why an alert was fired. they translate model decisions to clear, human-readable reasons.you will therefore need APIs to feed Ai decision into your incident response platforms.this will also require hiring developers to add explanations into your workflow.Security analysts need to be trained on how to interpret the AI generated explanations and this helps build the trust that is needed for the AI-driven alerts.

IX. Recommendations

We recommend a hybrid approach where there is a combination of both the traditional rule-based methods with AI-driven analysis to be able to get the most balance of speed and accuracy. In this approach, the AI handles the most repetitive tasks like looking through a lot of logs and flagging potential threats, since the AI can even learn from historical incidents and adapt to modified attack techniques over time. When the AI has finished processing the data, the human analyst can review its findings to verify the true positives and then eliminate the false positives. This double-checking step will help to build the trust needed for the AI-generated alerts. When you assign routine tasks to AI and then the higher-level judgments to humans, this will reduce alert fatigue since you will be leveraging the speed of AI alongside the understanding of experienced analysts.

X. Conclusion

In this paper we compared the traditional rule-based incident detention methods to the Ai-driven systems. We looked at multiple dimensions that include detection accuracy,response speed and also operational costs. We saw that traditional systems rely on fixed signatures which help them detect known threats fast with low resources used. compared to Ai systems that learn from data

recognise the threats quickly. The comparative analysis showed that AI-driven approach can reach a detection accuracy way above 90% while keeping the false positives under 2%. Traditional methods still excel in places where threats are well understood and where minimum compute resources are needed.

The study also examined response speed, cost efficiency, and scalability. AI-driven SOAR platforms can accelerate detection and containment, cutting attacker dwell time from months to days and substantially reducing breach costs. However, AI systems require careful governance, ongoing model training, and significant compute power. Traditional systems demand maintenance of rule sets and manual triage, which can slow response and lead to analyst burnout. These findings underscore the importance of policies, privacy controls, and explainability tools in any deployment. By combining automated AI workflows with human oversight, organizations can enjoy faster, more accurate incident response while managing risks and maintaining accountability. Future research should focus on field trials of hybrid systems under diverse threat scenarios to validate performance and guide best practices.

References

1. IBM Security, *Cost of a Data Breach Report 2023* (PDF) – <https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023>
2. M-Trends 2025." Google Cloud, cloud.google.com/blog/topics/threat-intelligence/m-trends-2025.
3. IBM Cost of a Data Breach Report: AI Security Cost Reduction." Veza, veza.com/blog/ibm-cost-of-a-data-breach-report-ai-security-cost-reduction-veza/.
4. Blistein, Jared. "IBM Cost of a Data Breach Report: AI Security Cost Reduction." Veza, 28 Aug. 2024, <https://veza.com/blog/ibm-cost-of-a-data-breach-report-ai-security-cost-reduction-veza/>
5. SOAR Playbooks to Optimize Incident Response." Lumifi Cyber, 2024, <https://www.lumificyber.com/fundamentals/soar-playbooks-to-optimize-incident-response/>.
6. "SOAR Security: How It Works, Use Cases, and Key Features." BlueVoyant, 2024, <https://www.bluevoyant.com/knowledge-center/soar-security-how-it-works-use-cases-and-key-features>.
7. Kaur, M., & Singh, G. (2024). *Overview on Intrusion Detection Systems for Networking Security*. Computers, 14(3), 87. <https://www.mdpi.com/2073-431X/14/3/87>
8. Reddy, A. K., Bojja, S. G. R., Saini, V., & Bonam, V. S. M. (2024). *AI Vs. Traditional IDS: Comparative Analysis of Real-World Detection Capabilities*. International Journal on Recent and Innovation Trends in Computing and Communication, 12(2), 1120–1127. <https://ijritcc.org/index.php/ijritcc/article/view/11463>
9. Yadav, R., & Thomas, D. (2025). *Signature-Based Intrusion Detection using ML/DL Empowered with Fuzzy Clustering*. Scientific Reports, 15(1). <https://www.nature.com/articles/s41598-025-85866-7>
10. Deloitte. (2023). *Enhancing Security Operations Center Efficiency through Artificial Intelligence*. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-laao-whitepaper-final.pdf>