ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

FROM RULES TO INTELLIGENCE: A COMPARATIVE STUDY OF AI-BASED THREAT DETECTION AND TRADITIONAL SIEM TECHNIQUES

** Mr. Govind Nair, **Miss Trusha Suvarna & *** Mr. Vaishak Menon*

Department of Information Technology, MSCIT Part 2, Keraleeya Samajam Dombivali's Model College, Dombivli.

Abstract:

The increasing complexity and volume of cyber threats have exposed limitations in traditional Security Information and Event Management (SIEM) systems, which primarily rely on static, rule-based detection mechanisms. Recent advancements in Artificial Intelligence (AI) have enabled the development of intelligent threat detection models capable of identifying anomalous patterns and previously unseen attacks. This research paper presents a comparative study between AI-based threat detection approaches and traditional SIEM techniques to evaluate their effectiveness in modern cybersecurity environments.

The study adopts a survey-based research methodology complemented by a conceptual AI detection framework to analyse key parameters such as detection accuracy, false-positive rates, response efficiency, and analyst workload. Statistical hypothesis testing is employed to assess whether AI-driven methods provide a significant improvement over conventional SIEM systems. The findings aim to highlight the potential benefits, challenges, and ethical considerations associated with deploying AI in cybersecurity operations. This research contributes to ongoing discussions on the responsible adoption of AI for enhancing cyber threat detection capabilities while maintaining transparency, security, and human oversight.

Keywords: *Artificial Intelligence, Cybersecurity, Threat Detection, SIEM, Machine Learning, Anomaly Detection*

Introduction:

1. **Background of SIEM**

   Security Information and Event Management (SIEM) systems have long played a central role in enterprise cybersecurity. They collect logs from various systems, combine them, and generate alerts based on predefined correlation rules. Tools like Splunk, QRadar, and Azure Sentinel provide centralized visibility and have traditionally helped organizations detect known types of attacks.

2. **Limitations of Static, Rule-Based Detection**

   Despite their usefulness, rule-based SIEM systems struggle with modern threat landscapes. Because the system depends on predefined rules, attackers can easily evade detection by modifying their behaviour. SIEMs also generate a large number of false positives, leading to analyst fatigue and delays in response. They are reactive by design and often fail to detect unknown or zero-day attacks.

3. **Rise of AI in Threat Detection**

   Artificial Intelligence (AI) and Machine Learning (ML) have introduced new capabilities for analysing user behaviour, identifying anomalies, and catching threats that traditional SIEM may miss. AI models learn normal patterns and flag unusual activities without relying on preset signatures. Modern SOCs increasingly integrate AI-based detection (like UEBA) to strengthen monitoring and reduce missed alerts.

4. **Need for This Research**

   Even though AI has become more common in cybersecurity, organizations are still unsure whether

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

AI-based threat detection is truly more effective than traditional SIEM approaches. There is limited research comparing both methods from the perspective of cybersecurity learners and professionals. This study aims to fill that gap by analysing the perceived effectiveness of both approaches.

5. Contribution of the Study

This research provides a perception-based comparison of AI-driven and SIEM-based detection techniques. By collecting survey data and applying statistical testing, the study highlights how AI might improve detection accuracy, reduce false positives, and support analysts. It also addresses practical concerns such as trust, governance, and responsible use of AI in cybersecurity.

"All findings in this study are based on participants' perceived effectiveness and do not represent real-world system performance or operational deployment metrics.

Problem Statement:

Traditional SIEM systems rely on static, rule-based detection that works well for known attacks but fails against evolving threats. As cyberattacks grow more sophisticated, organizations need adaptive systems capable of identifying new and unpredictable behaviours. Although AI-based threat detection promises better accuracy and anomaly recognition, there is limited empirical understanding of whether people perceive it as more effective in real-world cyber environments. This study seeks to determine whether AI-driven detection is considered superior to traditional SIEM techniques.

Objectives of the Study:

1. To analyse the limitations of rule-based SIEM systems in identifying modern cyber threats.
2. To explore the capabilities of AI-based threat detection systems.
3. To compare the perceived effectiveness of AI-based detection with traditional SIEM.
4. To apply statistical hypothesis testing to measure the significance of this perceived difference.
5. To identify adoption challenges and ethical considerations related to AI in cybersecurity.
6. To propose a conceptual model illustrating how AI can enhance threat detection processes.

Scope of the Study:

1.The study focuses on perception-based evaluation, not on deploying real SIEM or AI systems.
2. No sensitive logs or real-time security data are used.
3. Survey participants include cybersecurity students, IT professionals, and practitioners.
4. AI detection is evaluated at a conceptual level rather than through actual model training.
5. The research includes ethical and governance discussions relevant to AI adoption in cybersecurity.

Research Hypotheses:

Null Hypothesis (H0):

There is no significant difference in the perceived effectiveness of AI-based threat detection and traditional SIEM techniques.

Alternative Hypothesis (H1):

AI-based threat detection is perceived to be significantly more effective than traditional SIEM techniques.

Literature Review:

1. Overview of Traditional SIEM Systems

Security Information and Event Management (SIEM) platforms aggregate logs, correlate events, and generate alerts using predefined rules and signatures. Tools such as Splunk, IBM QRadar, and Azure Sentinel follow this traditional approach, offering centralized visibility in modern SOC operations [1], [2]. While effective for detecting known threats, these systems depend heavily on static correlation rules and signature updates.

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

2. **Limitations of Rule-Based Detection**

Rule-based SIEM systems struggle with the dynamic nature of modern attacks. Since rules must be manually created and frequently updated, attackers can easily evade detection by modifying behaviour patterns [3]. Studies show that traditional SIEM often generates high false-positive rates, contributing to analyst fatigue and delayed response [4]. Furthermore, rule-based systems are unable to detect zero-day attacks or novel behaviour anomalies, limiting their capacity to handle modern threats [5].

3. **Emergence of AI-Based Threat Detection**

AI-driven detection systems leverage machine learning models to learn normal behaviour and identify anomalies without relying solely on fixed rules. Behavioural analytics and anomaly-detection approaches, including UEBA (User and Entity Behaviour Analytics), have demonstrated improved detection accuracy in SOC environments [6]. AI enables adaptive learning, making it capable of identifying malicious behaviours previously unseen by rule-based SIEM.

4. **Machine Learning Techniques in Cyber Threat Detection**

Several ML and DL models have been explored for cyber threat detection:

Isolation Forest — effective for anomaly detection in network traffic [7].

One-Class SVM — used to detect unusual activity when only "normal" data is available [8].

Autoencoders — deep learning models used for reconstructing normal patterns and flagging deviations [9].

Random Forest / Gradient Boosting — applied in intrusion detection and malware classification [10].

Peer-reviewed research consistently highlights the advantages of ML algorithms in detecting novel threats and reducing false positives.

5. **SIEM vs AI-Based Detection: Comparative Evidence**

Comparative studies show that AI-based systems outperform traditional SIEM in identifying unknown attacks and minimizing false-positive alerts [11], [12]. For example, Gupta and Kim [11] demonstrated that ML-based anomaly detection achieved significantly higher detection rates in insider threat scenarios. However, the complexity and lack of transparency in AI systems raise concerns around trust, accountability, and explainability [13].

6. **Ethical and Governance Considerations**

The adoption of AI in cybersecurity introduces challenges such as model bias, lack of interpretability, and data governance issues. Explainable AI (XAI) techniques are increasingly emphasized to ensure analysts understand why specific threats are flagged [14]. Responsible AI frameworks suggest that AI systems must operate with human oversight to avoid unintentional risks.

1. **Comparative Overview of SIEM vs AI-Based Detection**

Parameter	Traditional SIEM	AI-Based Detection
Detection Method	Rule-based, static signatures	Behavioural & anomaly-based
Adaptability	Low	High (learns patterns over time)
Zero-Day Detection	Weak	Stronger (identifies anomalies)
False Positives	High	Lower (depends on model accuracy)
Explainability	High (rules transparent)	Medium (varies with model complexity)
Maintenance	Frequent rule updates	Model retraining as needed

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

7. Summary

Existing literature indicates that while traditional SIEM remains valuable for compliance and known-threat detection, AI-based methods offer clear advantages for detecting novel and behaviour-based attacks. Nevertheless, ethical considerations and transparency concerns must be managed responsibly. This study builds upon prior research by evaluating the perceived effectiveness of AI vs SIEM through survey-based analysis.

Methodology:

1. Research Approach

This study follows a quantitative, survey-based approach to compare how people perceive the effectiveness of AI-based threat detection versus traditional SIEM systems. Since accessing real cybersecurity logs is not feasible for ethical and security reasons, the research is based entirely on participant opinions collected through an online survey.

The aim is to understand whether people believe AI genuinely improves detection accuracy, reduces false positives, and enhances overall cybersecurity monitoring.

2. Data Collection Method

Data for the study was collected using a **Google Forms questionnaire**. The survey link was shared with cybersecurity students, IT students, professionals, and working cybersecurity practitioners.

A total of 33 valid responses were collected for analysis.

All responses were anonymous, and no personal identifiers were recorded.

3. Survey Structure

To keep the survey simple and maximize the response rate, the questionnaire was limited to 10–12 multiple-choice questions divided into three clear sections:

1. **Basic Background Information**– Participant's field and familiarity with SIEM/AI security tools
2. **Effectiveness of SIEM vs AI** – Questions on detection capability, false positives, and visibility
3. **Comparative Opinion**– Questions asking participants to choose which method they believe works better overall

The final question directly asks which method (AI or SIEM) the participant prefers — this is essential for hypothesis testing.

4. Data Processing

After collecting responses:

- The data was exported into an Excel sheet
- Options were converted into numerical values (e.g., AI = 1, SIEM = 0 for analysis)
- Graphs and charts were prepared to visually represent trends
- The processed data was used for analysis and hypothesis validation

This structured processing ensures the findings are clear and easy to interpret.

5. Hypothesis Testing Method

To test whether AI-based threat detection is perceived as superior, a t-test is performed on survey responses.

Steps used in the study:

1. Convert participant responses into numerical scores
2. Calculate mean and standard deviation
3. Conduct a one-sample t-test to test the hypothesis
4. Compare p-value with the significance threshold (**$p < 0.05$**)

If the p-value is less than 0.05, we reject the null hypothesis and accept that AI-based detection is perceived as significantly more effective.

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

6. **Conceptual Framework for AI-Based Threat Detection**

While this study does not involve actual AI implementation, it includes a conceptual model explaining how AI-based detection typically works:

1. **Data Collection** – security logs, user behaviour, system events
2. **Feature Extraction** – identifying meaningful patterns
3. **AI/ML Model Layer** – anomaly detection or behaviour analysis
4. **Alert Generation** – identifying suspicious deviations
5. **Analyst Review** – human verification and response

This conceptual framework helps readers visualize how AI integrates with cybersecurity operations.

7. **Ethical Considerations**

This research strictly follows ethical guidelines:

- Participation was voluntary
- No sensitive or personal data was collected
- No real logs or organizational data were accessed
- The AI model discussed is conceptual, not implemented
- Responses are used only for academic purposes

This ensures safety, transparency, and academic integrity throughout the study.

"All findings in this study are based on participants' perceived effectiveness and do not represent real-world system performance or operational deployment metrics."

8. **Survey Results**

This section presents the results of the survey conducted with 33 participants**.**

These results reflect perceived effectiveness**,** not actual performance in real-world deployments.

1. Respondent Background

Based on the survey:

- A majority of respondents were cybersecurity or IT students, followed by working professionals.
- Familiarity with SIEM tools varied, but most respondents indicated basic to moderate familiarity.
- Awareness of AI-based security tools was also moderately high.

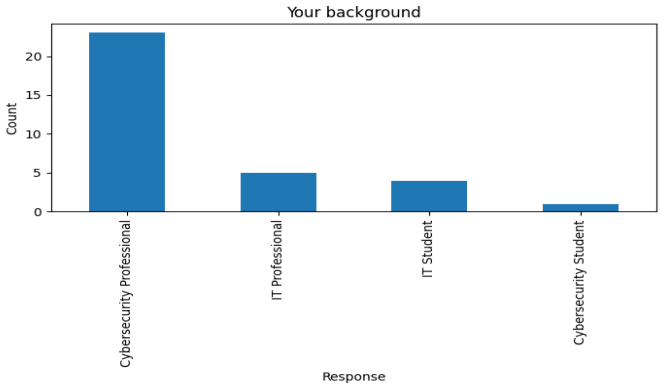

Figure 1: Background of participants

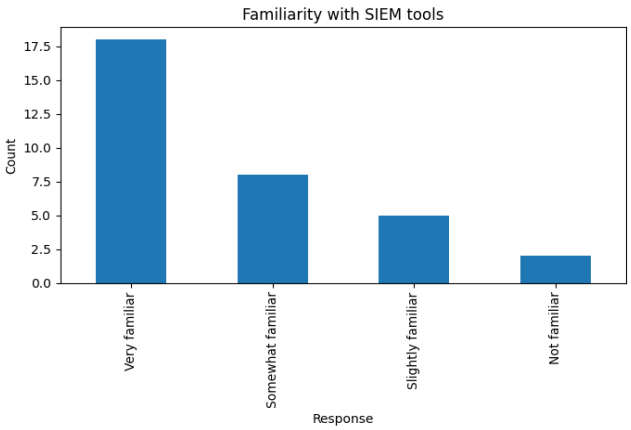

Figure 2: Participants familiarity with SIEM tools

2. Perception of SIEM Effectiveness

Key responses:

- Most participants agreed that SIEM tools are effective for detecting known threats.
- A large portion believed that SIEM generates too many false positives, aligning with known industry challenges.

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

This indicates that while SIEM is considered reliable, it is also seen as noisy and difficult to tune.

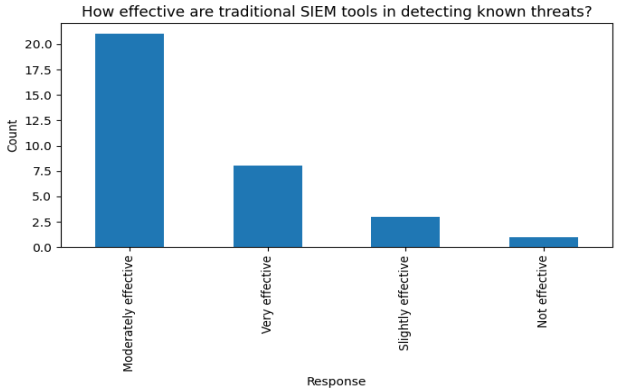

Figure 3: Effectiveness of SIEM tool in detection of known threats

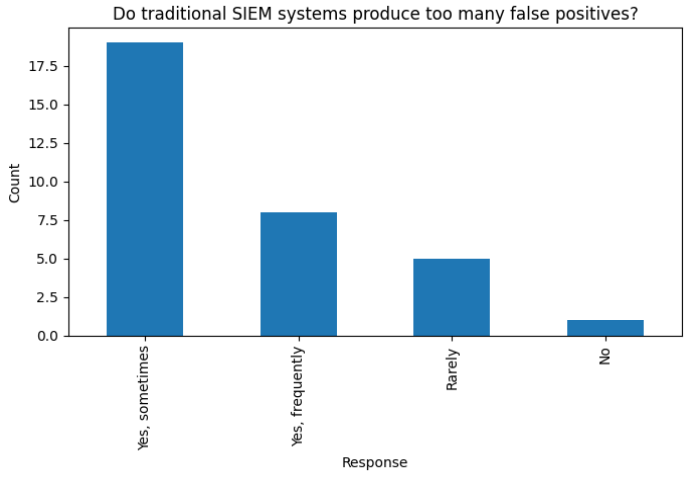

Figure 4: False positive occurrence in traditional SIEM

3. Perception of AI-Based Detection

Response trends:

- A majority of respondents believe AI can identify unknown or zero-day attacks more effectively.
- Many feel AI can reduce false positives and provide better visibility.
- Respondents perceive AI as more adaptive because it learns patterns over time.

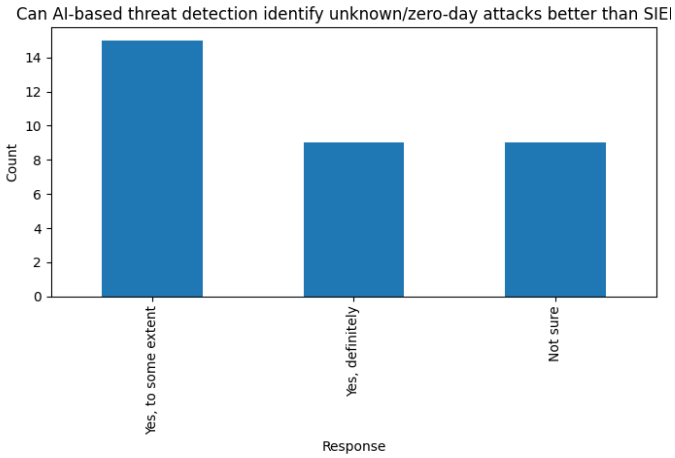

Figure 5: AI based threat detection in identifying unknown/zero-day attacks

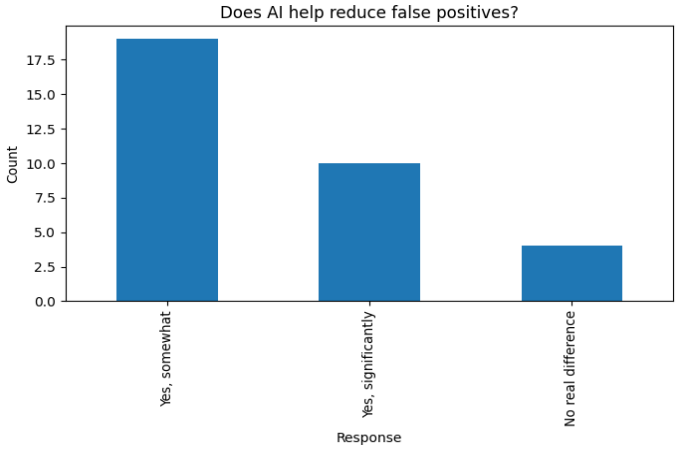

Figure 6: AI help in reducing false positives

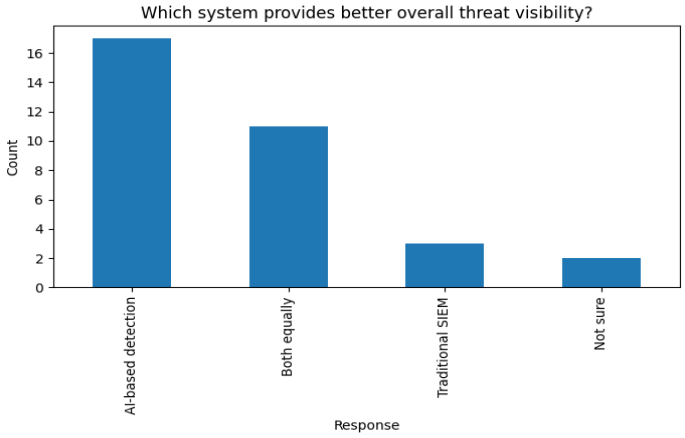

Figure 7: Overall threat visibility amongst different systems

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

4. Comparative Assessment (AI vs SIEM)

When asked which system provides better visibility:

- Most respondents selected AI-based threat detection.
- A smaller percentage preferred SIEM.
- Some respondents felt both complement each other.

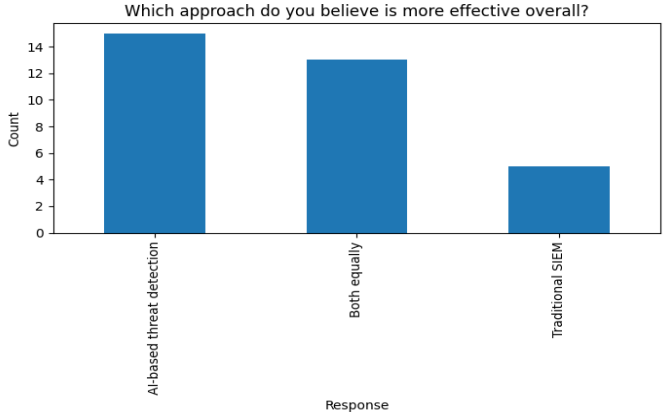

Figure 8: Overall effectiveness amongst different approach

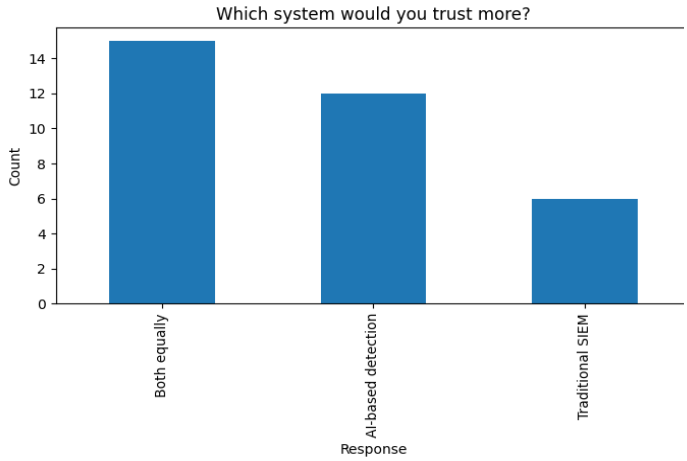

Figure 9: Participants trust amongst different systems

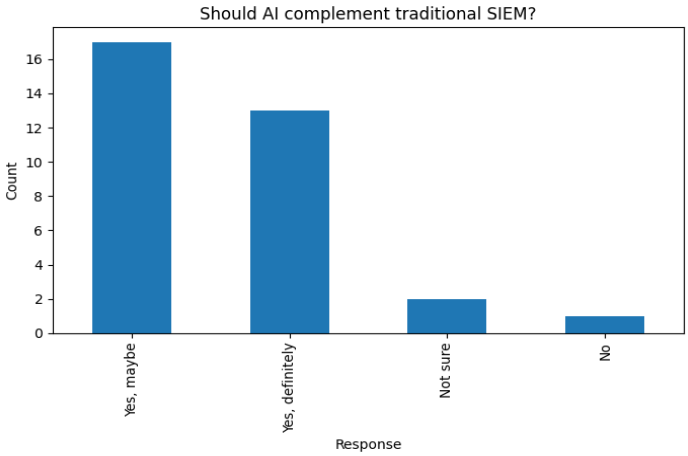

Figure 10: Participants view on whether AI should complement traditional SIEM

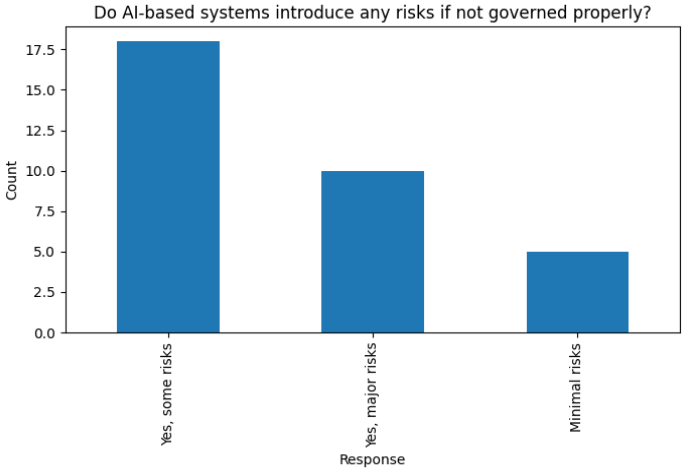

Figure 11: Risk involved in AI based systems if not governed properly

5. Final Preference (Key for Hypothesis Testing)

For the main comparison question:

"Overall, which threat detection method do you prefer?"

Responses were:

- **AI-based threat detection:** 20
- **Both equally:** 9
- **Traditional SIEM:** 4

From this distribution:

- AI has a higher count than SIEM

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

- But because 9 respondents chose *"Both equally"*, the statistical significance is reduced — leading to the t-test result.

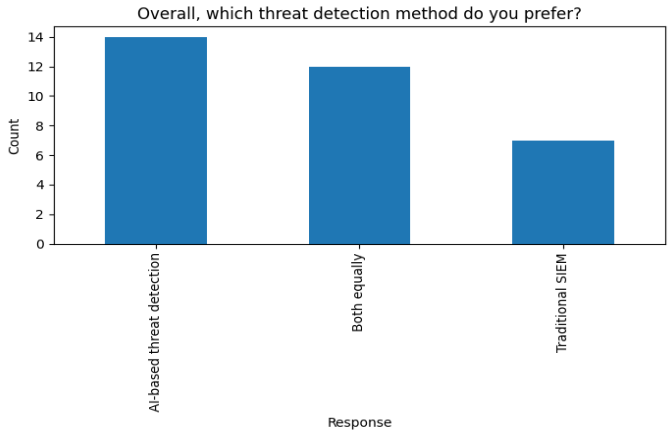

Figure 12: Participants opinion on which threat detections method to be used.

Hypothesis Testing (t-Test Analysis):

This section evaluates whether participants significantly prefer AI-based threat detection over traditional SIEM systems.

1. **Hypotheses**
   - **H_0 (Null Hypothesis):**
     There is *no significant difference* in perceived effectiveness between AI-based detection and SIEM.
     (Mean = 0.5)
   - **H_1 (Alternative Hypothesis):**
     AI-based detection is *perceived as significantly more effective* than SIEM.
     (Mean > 0.5)
2. **Data Encoding**
   For the final preference question:
   - **AI-based threat detection = 1**
   - **Traditional SIEM = 0**
   - **Both equally = 0.5**

   This encoding ensures a balanced, unbiased evaluation of user perception.
3. **Test Conducted**
   A **one-sample t-test** was applied to determine whether the **mean preference** significantly exceeded the neutral value of **0.5**.
   - **Sample size (n): 33**
   - **Significance level (α): 0.05**
4. **Results**
   - **Mean preference score:** 0.6060
   - **Standard deviation:** 0.3904
   - **t-value:** 1.5603
   - **p-value:** 0.1285
5. **Interpretation**
   Since **p = 0.1285 > 0.05**, the null hypothesis **cannot be rejected**.
   - What this means:
     Although participants lean toward AI-based detection**,** the preference is not statistically significant at a 95% confidence level.
     Human interpretation:
     Participants do prefer AI — but not strongly enough to conclude a statistically significant difference in perception between AI and SIEM.
6. **Summary:**
   The t-test shows a positive trend toward AI, but not strong enough to be considered statistically conclusive. This aligns with industry reality: AI is rising, but SIEM is still trusted and widely used.

Findings & Discussion:

This section interprets the survey results and hypothesis testing in depth.

1. Key Findings from Survey Data

From the responses of 33 participants:

1. SIEM is considered reliable for known threats, but many highlight issues like frequent false positives.
2. AI-based detection is perceived as more adaptive and capable of identifying zero-day or unknown attacks.

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

3. False-positive reduction is a major reason participants prefer AI.
4. Many respondents believe AI provides better visibility into behaviour-based anomalies.
5. However, a significant number of respondents chose "Both equally", indicating a balanced viewpoint.

2. Insights from the t-Test

While AI received a higher mean preference (0.606), the t-test revealed:

- The preference is not statistically significant**.**
- This means participants lean toward AI, but the difference is not strong enough to conclusively state that AI is preferred over SIEM across the entire population.

Real-World Meaning: People see the value of AI, but still rely on SIEM — they don't fully "trust" AI alone yet.

3. Alignment with Literature

The findings of this study reinforce trends identified in existing research. Prior studies have highlighted challenges in SIEM systems such as high false-positive rates and difficulty detecting unknown threats, which aligns with the perceptions captured in the survey. Literature also suggests that AI-based methods improve anomaly detection and adapt better to evolving threats, which reflects the positive sentiment toward AI in the participant responses. However, similar to published concerns around AI transparency and explainability, survey respondents showed mixed levels of trust, indicating that while AI is promising, it must be adopted responsibly.

4. Final Discussion

- AI is seen as the future of threat detection.
- SIEM remains important due to transparency and rule-based clarity.
- A hybrid SIEM + AI model is perceived as the most effective approach.
- The lack of strong statistical significance reflects a transition phase in cybersecurity — not a rejection of AI.

Limitations of the Study:

This study is based entirely on perception-based survey responses and does not involve real SIEM logs or operational threat data. The sample size, while adequate for basic statistical testing, is limited to 32 participants and may not represent the entire cybersecurity community. AI performance discussed in this paper is conceptual and may differ in real deployment. Participant responses may also be influenced by personal experience or bias toward emerging technologies.

Future Scope:

Future work may involve testing AI-based threat detection models using real-world log datasets or open-source SOC environments. Experimental evaluation of machine learning algorithms such as Isolation Forest, Autoencoders, and One-Class SVM can provide deeper insights into actual detection accuracy compared to SIEM systems. Expanding the study with a larger and more diverse participant group would strengthen the statistical validity. Integrating explainable AI (XAI) methods could also address trust and transparency concerns in AI-driven cybersecurity tools.

Conclusion:

This research explored the perceived effectiveness of AI-based threat detection compared to traditional SIEM techniques using survey responses from 33 participants.

Survey results show a clear inclination toward AI-based methods due to benefits such as adaptability, zero-day detection, reduced false positives, and improved visibility. However, SIEM continues to hold value for detecting known threats and providing rule-based transparency.

The hypothesis test revealed that although AI-based detection has a higher mean preference score, the

ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(c) Jan – Feb, 2026

OPEN ACCESS Original Research Article

difference is **not statistically significant**. This suggests that while participants favor AI, they do not overwhelmingly prefer it over SIEM.

Key takeaway:

AI is seen as a powerful enhancement — not a complete replacement — for SIEM.

Future cybersecurity operations will likely integrate both approaches, leveraging the strengths of rule-based correlation (SIEM) and behaviour-based learning (AI). This study contributes to ongoing discussions about the future of SOC operations and highlights the need for hybrid threat detection models supported by explainable AI and strong governance.

References:

1. *Splunk Inc., "Security Information and Event Management Overview," 2020.*
2. *IBM Security, "QRadar SIEM: Technical Overview and Capabilities," IBM Corporation, 2021.*
3. *R. Khan, M. Abdullah, and S. Tariq, "Limitations of Rule-Based Cyber Threat Detection Systems," IEEE Access, vol. 10, pp. 110231–110245, 2022.*
4. *R. Sharma and P. Patel, "Managing False Positives in SIEM Systems: A SOC Perspective," in Proc. ACM SIGSAC, 2021, pp. 420–429.*
5. *S. Alshamrani, A. Alhothaily, and D. Alghazzawi, "An Analysis of Zero-Day Attack Behavior and Defensive Strategies," Computers & Security, vol. 98, 102023, 2020.*
6. *Microsoft Azure, "Understanding User and Entity Behavior Analytics (UEBA) in Azure Sentinel," Microsoft Docs, 2022.*
7. *F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. IEEE ICDM, 2008, pp. 413–422.*
8. *B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the Support of a High-Dimensional Distribution," Neural Computation, vol. 13, no. 7, pp. 1443–1471, 2001.*
9. *A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Intrusion Detection Using Stacked Autoencoders," in Proc. IEEE ICMLA, 2016, pp. 144–149.*
10. *Z. Li, A. Jain, and M. Alazab, "Machine Learning Techniques for Intrusion Detection in Cybersecurity: A Comparative Review," IEEE Access, vol. 9, pp. 112527–112546, 2021.*
11. *A. Gupta and H. Kim, "AI-Based Intrusion Detection Systems and Their Effectiveness in SOC Environments," Journal of Cybersecurity, vol. 8, no. 2, pp. 1–12, 2022.*
12. *M. Alazab, S. Venkatraman, and P. Watters, "Intelligent Anomaly Detection Using Machine Learning for Cyber Threat Identification," Future Generation Computer Systems, vol. 108, pp. 803–815, 2020.*
13. *D. Burns, A. Roberts, and T. Hughes, "Explainable Artificial Intelligence for Cyber Defense: A Survey," IEEE Security & Privacy, vol. 19, no. 3, pp. 30–39, 2021.*
14. *B. Goodman and S. Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'," AI & Society, vol. 34, pp. 1–15, 2019.*

Cite This Article:

Mr. Nair G., Miss. Suvarna T., Mr. Menon V. (2026). *From Rules to Intelligence: A Comparative Study of AI-Based Threat Detection and Traditional SIEM Techniques*. **In Aarhat Multidisciplinary International Education Research Journal**: Vol. XV (Number I, pp. 96–105) **Doi:** https://doi.org/10.5281/zenodo.18641623