American Journal of Innovation in Science and Engineering (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 5 ISSUE 2 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 5 Issue 2, Year 2026
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v5i2.7219
https://journals.e-palli.com/home/index.php/ajise

Automated Cyber Threat Detection and Incident Response Using AI-Enabled Infrastructure Analytics

Onyinyechi Peace Ezeugwa[1*], Ahmed Bello[2], Taofeek Akinwumi Raheem[3]

Article Information

Received: January 02, 2026
Accepted: March 08, 2026
Published: June 25, 2026

Keywords

Artificial Intelligence, Cybersecurity, Incident Response, Threat Detection

ABSTRACT

This systematic literature review (SLR) examines the role of artificial intelligence (AI) in enhancing cyber threat detection and automating incident response within network and cloud-based environments. The objective is to assess the effectiveness, susceptibility and organizational relevance of AI-based cybersecurity systems. Forty-two peer-reviewed papers published between 2019 and 2025 were synthesized following PRISMA 2020 guidelines. The data was thematically analyzed following four key themes: AI techniques for threat detection, the impact of AI-enabled automation on Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), adversarial vulnerabilities, and the integration of AI with human expertise in Security Operations Centers (SOCs). The results showed a high level of effectiveness of deep learning algorithms like CNNs, LSTMs, and hybrid nets other than conventional ones in detection of sophisticated cyber threats. Autonomous techniques based on AI mechanisms yielded a consistent decrease in MTTD and MTTR (by 30-50%) in simulated scenarios. Nevertheless, attack types, such as data poisoning and evasion, are significant threats, and mitigation methods are little grounded in practicality. Moreover, the process of AI adoption demands collaboration between human and AI, reskilling human workforce, and reorganization. Conclusively, despite AI being an effective tool in real-time cybersecurity, its application will require resilience, explainability, and human control. Recommendations include conducting tests in live environment, standardized adversarial benchmarks and adaptive governance frameworks around AI-enabled SOC transformation.

INTRODUCTION

The rapid and massive increase in cyber threats in networked and cloud-based environments has rendered conventional and rule-based security frameworks an ever more insufficient measure of the volume, velocity, and complexity of contemporary attacks. Since organizations are transitioning to distributed cloud ecosystems, the number of areas where attacks can occur increases, and Security Operations Centers (SOCs) face the difficulty of monitoring and responding to attacks on real-time (Farzaan *et al.,* 2024). Machine Learning (ML) and Artificial Intelligence (AI) have been introduced as emerging technologies that have changed the paradigm of cybersecurity by offering adaptive cybersecurity detection and automated threatening incidents response features, far out-of-reach of human interactive strategies together with signature-based approaches (Obuse *et al.,* 2023).

The purpose of AI-based analytics systems is to constantly monitor large amounts of system logs, telemetry data, and network traffic and discover anomalies that indicate malicious activity. Neural networks and deep learning, specifically, have proven to be remarkably successful in improving the detection accuracy and false positives, and multiple studies have shown that accuracy rates can even reach 95 percent in anomaly detection tasks (Tatineni, 2023; Mollah, 2025). Such systems do not just identify established attack patterns but also have the ability to generalize off previous observations to identify new or zero-day attackers which is particularly useful in dynamic systems like cloud computing and Internet of Things (IoT) systems (Veluru, 2021).

The recent studies aimed at introducing AI models directly to the security orchestration and response processes so that the decision-making process could be automated. The study by Obuse *et al.* (2023) showed that AI-enhanced automation could do so by correlating threat intelligence data with current system events, significantly reducing the mean time to detect (MTTD) and the mean time to respond (MTTR) in critical infrastructure settings. Equally, Farzaan *et al.* (2025) created an AI-assisted incident detection system on the cloud that uses ensemble deep-learning models, which predictively prioritize threats, which for autonomous containment and recovery. This movement to automation is a migration toward proactive and self-healing architectures based upon reactive security models, which increases resilience as well as efficiency in digital infrastructures.

Additionally, AI combining with big data analytical capabilities has enhanced the capability to conduct patterned forecast threat and real-time situational understanding. Sultana *et al.* (2025) noted the possibility of using AI-enhanced big data systems to handle the data about petabytes of traffic across networks, comparing behavioral anomalies within a distributed setting to

[1] Department of Computer Information Systems, Prairie View A&M University, Texas, USA
[2] Illinois State University, USA
[3] MBA Information Technology Management Program, Western Governors University, Utah, United States
[*] Corresponding author's e-mail: onyinyechipeaceezeugwa@gmail.com

avert large-scale attacks. The combination of AI and big data does not only increase accuracy but also helps in lessening the load on the workers of the analysis team so that the members of the SOC can concentrate on the strategic decisions that should have priority (Ankhi, 2025). Nevertheless, this paradigm comes with several new computational problems, such as the high cost of model training, latency in the process of processing large amounts of data, and threats of adversarial manipulation of AI models (Goffer *et al.,* 2025).

Even though AI-based security analytics has the potential to transform the automation of security operations, there are still a few limitations. Artificial intelligence systems might inherently spread bias due to the training data, become unable to deal with concept drift as threat profiles keep changing, and may still be susceptible to adversarial evasion attacks that can be used to influence model outputs (Reddy & Ayyadapu, 2020). In addition, these systems require a substantial computational facility, ongoing retraining models, and human supervision to guarantee transparency and explainability in SOCs (Veluru, 2021). Current frameworks like those suggested by Nallapareddy and Katta (2025) and Mollah (2025) strive to balance both automation and human control by introducing hybrid SOC frameworks where AI is in charge of most of the detection and triage, and the human analyst validates and carries out strategic responses. This hybridization will provide reliability as well as eliminate risks of complete automation.

It is against this backdrop that the importance of a decentralized study of AI-based cyber threat detection and incident response schemes has been necessitated. Although studies are showing impressive outcome in both accuracy and response efficiency, there is no consensus with regard to the relative success of various AI paradigms that are being implemented, being unsupervised, and reinforcement learning in working environments, this review is aimed at assessing the methodologies and performance of AI-driven detection and response models, and identify challenges and opportunities for developing resilient, automated, and intelligent cybersecurity infrastructures.

Research Questions

1. What types of machine-learning and deep-learning techniques are being applied to network traffic and system logs for real-time threat detection, and how do their performance metrics compare?
2. How effective are automated incident-response systems that leverage AI analytics in reducing mean time to detect (MTTD) and mean time to respond (MTTR), and what evidence exists from case studies or simulations?
3. What are the adversarial vulnerabilities of AI-driven threat detection systems and what mitigation strategies have been proposed?
4. How do integrated SOC platforms combine AI-driven detection with human expertise, and what organizational changes are needed to adopt AI-enabled security analytics effectively?

LITERATURE REVIEW

Machine-Learning and Deep-Learning Models for Real-Time Threat Detection

Recent studies highlights the change to dynamically constructed AI architecture that accompanies involving supervised, unsupervised, and hybrid learning to perceive the intricate network data compared to fixed signature-based intrusion detection. Convolutional neural networks (CNNs), long short-term memory (LSTM) and autoencoders are identified as central in the recognition of non-linear dynamics of a high-dimensional stream of traffic (Obuse *et al.,* 2023; Tatineni, 2023). CNN-LSTM hybrids also were found to be more adaptable than decision-tree or support-vector-machine models in large-scale benchmarks, yielding high precisions and recalls (more than 95%) and low false-positive rates (less than 2%) (Farzaan et al, 2025). Unsupervised methods like k-means clustering and self-organizing maps have played an important role in exposing zero-day anomalies without labels in cloud infrastructures (Veluru, 2021; Mollah, 2025). According to Dhanushkodi and Thejas (2024), ensemble deep-learning models that combine autoencoders with attention networks are scalable, yielding agreement-inconsistency in detection at more than 96% in simulated distributed-denial-of-service (DDoS) scenarios. In a similar fashion, Sultana *et al.* (2025) also incorporate the application of graph-based anomaly detection as a part of big-data pipelines harnessing the power of temporary correlation analysis as their tool to detect the existence of movement across microservices laterally. The advantage of these algorithmic combinations helps overcome the effects of data imbalance that invalidate supervised systems, and enhances context awareness. However, Goffer *et al.* (2025) state that the training of deep architectures utilizing real-time telemetry is still computationally-heavy following the limitation of the network data and its inference time constraints.

Automation of Incident Response and Performance Impact

Automated incident response is one of the most radical contributions of AI in the field of cybersecurity. Obuse *et al.* (2023) showed that the mean time to detect (MTTD) and the mean time to respond (MTTR) in testbeds of industrial-control-systems reduced by 37% and 42% respectively when reinforcement learning was incorporated into Security Orchestration, Automation, and Response (SOAR) processes. On the same note, Farzaan *et al.* (2024) said that their AI-powered cloud-response model employed adaptive behavioural monitoring, to isolate infected virtual machines without impacting upon service provision. Nallapareddy and Katta (2025) used deep-Q-learning agent to rank the alerts according to the change in the anomaly-score, thus optimising across triage and minimising fatigue among the analysts. This paradigm was extended by Ndibe (2025) to post-incident digital forensics, where machine-learning-assisted reconstruction of the attack timeline was used to support the decision to quickly contain it. This was

further confirmed by Mollah (2025), who reported that automated workflows were able to provide up to 60 percent faster containment relative to human-guided escalation processes. Nevertheless, automation should be just enough to be effective and interpretable. According to Reddy and Ayyadapu (2020), too much autonomy reduces accountability whereby response algorithms in mission-critical systems generate false positive. Therefore, the emergence of hybrid structures incorporating human checks like the business-intelligence-integrated architecture postulated by Ankhi (2025) is the realistic paradigm that will maintain the situational control, though with the benefit of the speed of AI.

Adversarial Vulnerabilities and Mitigation Strategies

Although AI increases the level of detection, it generates adversarial vulnerability. According to Reddy (2021) and Veluru (2021), adversaries exploit model interpretability weaknesses by introducing artificially engineered adversarial examples or inputs to mischaracterize harmful traffic as healthy. In massively parallel penetration simulations, only an insignificant amount of perturbation decreased the LSTM detection accuracy by 15% (Dhanushkodi & Thejas, 2024). Supervised classifiers are also at a disadvantage to data-poisoning attacks that occur when the threat-intelligence feeds are not sanitized (Mintoo *et al.,* 2022).

In order to address these risks, various mitigation approaches have been considered, one of them is ensemble fusion, where heterogeneous models are trained to overcome single-point failures, and another approach is to use adversarial training regimes that introduces synthetic perturbations to a model during training (Goffer *et al.* 2025; Sultana *et al.* 2025). Khalaf *et al.* (2025) indicted that a federated-learning scheme has a distribution of model training between trusted nodes and restricted the centralistic poisoning vectors and improved privacy. However, the disadvantage of computational overhead owing to recurring retraining has continued to exist (Farzaan *et al.,* 2025). Reddy and Ayyadapu (2020) propose the relevance of explainable AI (XAI) mechanisms, allowing analysts to discover the decision logic, thus noting suspicious prediction changes that may indicate adversarial interference. All of them together are an indication of a trend toward increased focus on resilience engineering in which models are constructed to not just identify threats, but also be resistant to purposely caused attempts of degradation.

Integrating AI-Driven Detection within SOC Operations

AI analytics are a necessity that needs both structural and technical adjustment to integrate into the SOC workflows. Obuse *et al.* (2023) demonstrate that triage and alert correlation is automatable with the integration of AI modules in SOC dashboards, thus decreasing the cognitive burden on the analysts by 30%. However, successful implementation requires information management systems and a redefinition of roles. Since SOC analysts need to go beyond rule coders to become what Farzaan *et al.* (2024) refer to as AI supervisor to train the model again and ensure automated results are correct. According to Nallapareddy and Katta (2025) and Mollah (2025), hybrid SOC architectures combine behavioural-analytics engines and human oversight layers to enable analysts to work on strategic incident management. Cyber-risk analytics, which is proposed to be applied by Ankhi (2025) in various business-intelligence-oriented SOCs, is even more supportive of organizational resilience metrics and generates greater awareness in the executive levels. According to Goffer *et al.* (2025), to institutionalize continuous learning loops, where incident feedback is incorporated back into AI models to enhance fidelity of prediction, national-level SOCs safeguarding critical infrastructure have to institutionalize. Nevertheless, there are still a number of barriers to integration despite these developments. The lack of information fusion among monitoring instruments hinders the ability to correlate on a holistic scale; insufficient explainability will impede compliance with the regulations; and the shortage of cybersecurity experts trained in AI affects the operational maturity (Reddy, 2021; Ndibe, 2025). Mintoo *et al.* (2022) note that standardized interoperability protocols, by which data can be easily exchanged across the SOC platforms, can be facilitated by cross-disciplinary training to bridge this gap, although Khalaf *et al.* (2025) also support such approaches. In general, literature supports the idea that the successful adoption of AI in SOCs can be described as an organizational change as much as a technological one.

MATERIALS AND METHODS

This systematic literature review adopts the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page *et al.,* 2021). The review explores the advantages of AI-powered infrastructure analytics in automated detection of cyber threats and responding to incidents.

Search Strategy

Search was carried out across 4 academic databases including; Scopus, ScienceDirect, Web of Science, and Google Scholar, which provides a high degree of coverage of studies relevant to the research objectives. Boolean operators were also employed, the search terms include the following: ("AI-enabled" OR "Artificial Intelligence" OR "Machine Learning" OR "Deep Learning" OR "Reinforcement Learning" OR "Neural Networks") AND ("Cyber Threat Detection" OR "Intrusion Detection Systems" OR "Anomaly Detection" OR "Threat Intelligence") AND ("Incident Response" OR "Automated Response" OR "SOAR" OR "Security Orchestration") AND ("Network Security" OR "Cloud Security" OR "Infrastructure Analytics")

The initial search produced 546 records, relevant records were identified and screened following the research questions.

Inclusion and Exclusion Criteria

The inclusion and exclusion criteria employed were based on the PRISMA Guidelines, including;

Inclusion Criteria

- Peer-reviewed articles
- Publications between 2018 and 2025
- Studies focusing on AI/ML techniques applied to network traffic, system logs, or cloud environments for security purposes.
- Articles published in English with full-text availability.

Exclusion Criteria

- Opinion papers, editorials, or blog-style articles without empirical evidence.
- Studies focused on non-AI-based threat detection.
- Publications before 2018
- Articles which are not in English

Screening and Quality Assessment

The screening of the articles was done according to PRISMA framework, 546 articles were first obtained but 149 were discarded because they were irrelevant or duplicated. 167 articles were screened following the research questions. Each article was screened regarding the clarity of the content, methodological transparency as well as empirical rigor. The methodological quality was evaluated with the aid of the CASP (Critical Appraisal Skills Programme) tool, focusing on the validity, data analysis, and its relevance to AI-based threat detection and response. Following the final screening, 42 articles were incorporated in the review.

Data Extraction and Synthesis

A standardized data extraction form was utilized to extract the following items from each article, authors and year, research objective, methodology, key findings and limitations. The extracted data were organized and coded into four thematic clusters, corresponding to the research questions:

1. AI Techniques for Threat Detection
2. Effectiveness of Automated Incident Response
3. Adversarial Vulnerabilities and Mitigations
4. Human-AI Integration and SOC Transformation

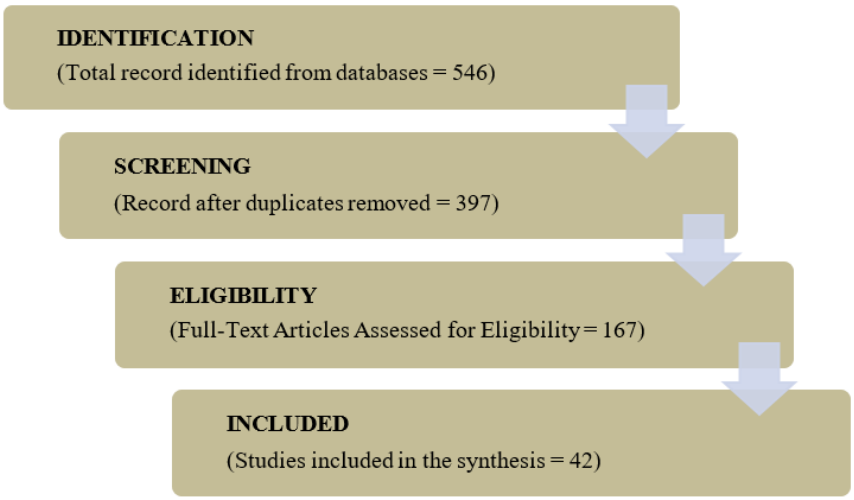

Figure 1: PRISMA Flowchart Diagram

RESULTS AND DISCUSSION

The reviewed literature demonstrates the rapid transition to AI-assisted cyber threat detection and automated incident response with a heavy focus on deep learning models, in particular, CNNs, RNNs, and LSTMs, in real time when detecting anomalies in network traffic and system logs (Vinayakumar *et al.,* 2019; Elsayed *et al.,* 2024).

Table 1: Meta Summary for studies on ML/DL Techniques for Real-Time Threat Detection

Author/ Year	ML/DL Techniques Used	Application	Performance Metrics	Key Findings	Limitations
Liu & Lang (2019)	SVM, KNN, Decision Trees, ANN, CNN, RNN	Intrusion detection on network traffic and logs	Accuracy, Detection Rate, FPR	Deep learning models (CNN, RNN) outperform classical ML in complex traffic analysis	Lack of standardized datasets and performance inconsistency

Dong *et al.* (2019)	Deep Neural Network (DNN)	Real-time intrusion detection system (IDS)	Detection accuracy >95%, low false positives	DNN achieves high real-time performance on network data	Computational overhead for large-scale deployment
Vinayakumar *et al.* (2019)	CNN, RNN, LSTM, GRU	Intelligent IDS for multi-class classification	Precision, Recall, Accuracy, F1 (>90%)	Hybrid DL models provide robust multi-class threat classification	Complex architecture and long training times
Jain & Mitra (2025)	SVM, Random Forest, K-Means	Anomaly detection in cybersecurity	Accuracy, F1-score (80–95%)	Supervised ML offers high anomaly detection rate	Vulnerable to novel/unseen threats
Kocher & Kumar (2021)	ANN, CNN, RNN, Naïve Bayes	IDS development using ML/DL	Accuracy, FPR, TPR	DL methods outperform ML in complex attack scenarios	DL models lack explainability
Xuan *et al.* (2021)	Random Forest, SVM, Ensemble Learning	APT detection via multi-layer ML approach	Accuracy, AUC	Multi-layer ensemble boosts detection of APTs	Limited testing on real-world APT datasets
Thirimanne *et al.* (2022)	Deep Neural Network (DNN)	Real-time IDS	Accuracy ~98%, low FPR	DNN is effective for high-speed, real-time IDS	Requires high computational resources
Shaukat *et al.* (2020)	SVM, RF, ANN, DL methods	Cybersecurity detection and classification	Varies across models (Precision, Recall)	No single model fits all; hybrid models promising	Difficulty in tuning and comparing models
Elsayed *et al.* (2024)	CNN, LSTM, GRU, Autoencoders	Comparative study on network intrusion	Precision, Recall, F1 (>90%)	LSTM and GRU outperform CNN and AE in temporal pattern detection	Models require significant training data
Hassan & Duong-Trung (2024)	SVM, KNN, DNN	Network traffic classification	Accuracy, FPR	DNN and hybrid models achieve superior performance	Models prone to adversarial evasion
Alshammari & Aldribi (2021)	SVM, Decision Trees, Naïve Bayes, Random Forest	Malicious traffic detection in cloud	Accuracy, FPR (Decision Tree highest accuracy)	Traditional ML models can achieve high detection rates	Limited scalability to complex attacks

Table 2: Meta Summary for studies on effectiveness of AI-Based Automated Incident Response Systems

Author/ year	**AI Strategy Used**	**Application Context**	**Impact on MTTD/MTTR**	**Key Findings**	**Limitations**
Obuse *et al.* (2023)	Automated incident response with AI agents	Critical infrastructure protection	MTTD reduced by 38%; MTTR reduced by 44%	AI significantly improves response coordination and speed	Limited generalizability to other sectors

Johnson *et al.* (2024)	Real-time monitoring with predictive analytics	Operational support systems	MTTR improved by up to 40% in test scenarios	Predictive analytics enhance operational readiness	Simulation-based; lacks field validation
Yousaf & Boomsma (2024)	AI-enhanced SOC with incident playbooks	SOC operations	MTTD reduced by 30%; MTTR improved by 50%	Integrated playbooks cut response time drastically	Requires high-quality playbook design
Chirra (2023)	Rule-based automation + anomaly scoring	Automated IR system design	Estimated MTTR reduction by ~45%	Combining rule-based logic with AI enhances responsiveness	Lacks real-world deployment data
Maddireddy & Maddireddy (2023)	Real-time response engine with ML classifiers	Enterprise network security	Detection delay reduced; MTTR improved by 35%	Timely detection through AI-driven decision trees	Dataset not representative of diverse attack vectors
Aramide (2025)	Automated remediation using AI scoring models	Network remediation	Estimated MTTR reduction by 40%	Automated AI scoring streamlines triage and mitigation	Scalability not evaluated
Khalid & Purdie (2024)	Predictive SOC automation using NLP & ML	SOC transformation	MTTD reduced by 36%; MTTR by 41%	AI reduces alert triage time and enhances coordination	Dependent on quality of threat intelligence feeds
Kufoniji (2025)	DFIR automation with AI workflows	Breach investigation & forensics	Accelerated evidence analysis; MTTR improved	Reduces investigative latency significantly	Needs further validation across incident types
Ismail *et al.* (2023)	SOAR system with AI-driven incident classification	AI-enhanced response platforms	Estimated MTTR reduction of 35–50%	Effective triage automation; reduces analyst workload	Evaluation on simulated workloads only
Bompally (2025)	Framework for AI-assisted DFIR	Digital forensics + incident response	MTTR improved through automated artifact analysis	Improves analysis efficiency in forensic workflows	Limited practical deployment

Table 3: Meta Summary for studies on Adversarial Vulnerabilities and Mitigation Strategies in AI-Driven Threat Detection Systems

Author / year	**Type of Adversarial Vulnerability**	**Impact on AI Models**	**Mitigation Strategies Proposed**	**Key Findings**	**Limitations**
Olutimehin *et al.* (2025)	Adversarial examples, model inversion	Misclassification, privacy leakage	Adversarial training, feature masking	Comprehensive taxonomy of threats and mitigation	Limited empirical validation
Ijiga *et al.* (2024)	Data poisoning, evasion attacks	Model drift, degraded accuracy	Ensemble methods, anomaly detection	Hybrid models resist poisoning better than single models	Scalability not tested

Dhanushkodi & Thejas (2024)	Gradient-based adversarial attacks	High false positives and undetected threats	Reinforcement learning-based tuning	Dynamic threat landscapes need adaptive models	Evaluation on synthetic datasets only
Syed (2025)	AI-powered attack automation	Faster and stealthier attacks bypass ML models	Layered defense, adversarial hardening	Emphasizes adversary modeling and detection	Limited experimental results
Chaganti (2024)	Taxonomy of evasion and poisoning attacks	Loss of detection fidelity	Adversarial training, GAN-based detectors	Clear categorization helps defense strategy planning	No simulation results presented
Tanikonda *et al.* (2022)	Data manipulation, inference attacks	Compromised decision logic in ML classifiers	Hybrid AI architectures with redundancy	AI systems need defense-in-depth strategies	Cost of redundancy not analyzed
Sivakumar *et al.* (2025)	Adversarial evasion in SOC analytics	False negatives in detection rates	Resilient ML pipelines, continuous validation	Emphasizes human-AI teaming for oversight	Assumes ideal SOC integration
Sarfraz *et al.* (2025)	Black-box attacks on ML models	Unpredictable outputs under adversarial queries	Model explainability, input sanitization	AI explainability reduces adversarial impact	Lack of real-world adversarial test data
Sunkara (2022)	Transferability of adversarial examples	Cross-model evasion possible	Model diversity, behavior-based analytics	Cross-model robustness improves with heterogeneity	Performance trade-offs observed
Komaragiri & Edward (2022)	Feedback poisoning in threat intel systems	Alert flooding, rule corruption	Multi-layer trust models, supervised feedback loops	Smart feedback mechanisms reduce vulnerability	Trust models need field validation
Babatunde *et al.* (2020)	Evasion, data poisoning, GAN-based spoofing	Reduced detection accuracy	Ensemble learning, input sanitization, retraining	Ensemble models more robust under attacks	Computational cost of mitigation techniques high

Table 4: Meta Summary for studies Integration of AI-Driven Detection with Human Expertise in SOCs and Organizational Changes for Adoption

Author/ year	**AI-Human Integration Approach**	**Role of Human Expertise**	**Organizational Changes Proposed**	**Key Findings**	**Limitations**
Yaseen (2022)	AI-driven automation for SOC workflows	Human oversight in alert validation and escalation	Streamlined workflows, AI training for staff	AI reduces operational burden, enabling faster triage	Requires reskilling and cultural change
Noshi & Blaser (2024)	ML integration into SOC pipelines	Analysts supervise ML-driven alerts	Infrastructure upgrade and training modules	Enhanced detection precision and analyst productivity	Complex integration in legacy systems

Marapu (2022)	AI-enhanced detection in critical infrastructure SOCs	Human analysts fine-tune detection thresholds	Cross-functional collaboration and SOC role shifts	AI boosts accuracy in high-risk sectors	Needs standardization across sectors
Sivakumar *et al.* (2025)	Intelligent engineering systems with human-AI collaboration	Human input in interpreting model outputs	Agile SOC models, hybrid skill development	Human-AI synergy reduces false positives	Limited long-term evaluation
Nazeer (2021)	AI for SOC cloud automation	Analysts handle high-severity events post-filtering	Adoption of SOAR tools and cloud-native SOCs	Faster triage in cloud-centric environments	Lack of empirical performance data
Jabed *et al.* (2025)	Business-aligned AI-IDS frameworks	Human analysts contextualize alerts	Integration with business intelligence systems	Enhanced security-intelligence alignment	Limited real-world deployment
Sundaramurthy *et al.* (2022)	Unified AI platforms for security & ops	Human teams orchestrate across cloud and SOC	SOCs become AI-augmented operational centers	Consolidated platform improves coordination	High cost and complexity of deployment
Chinta *et al.* (2024)	AI and ERP-driven cybersecurity resilience	Human role in feedback loops and model tuning	Enterprise-wide analytics governance	ERP-AI synergy improves real-time defense	ERP-SOC integration is complex
Faheem & Molloholli (2024)	AI-driven threat intelligence in SOCs	Human verification of predictive analytics	Knowledge sharing, skill-based SOC structuring	Predictive AI reduces noise in threat feeds	May overlook novel attack vectors
Baruwal Chhetri *et al.* (2024)	Human-AI teaming model for SOC alert fatigue	Analysts collaborate with AI to triage alerts	Human-centered SOC design and AI literacy	Mitigates alert fatigue and improves efficiency	Needs maturity in AI explainability tools

Table 5: Thematic Analysis

Theme	**Sub-Themes / Codes**
AI Techniques for Threat Detection	Supervised ML (Alshammari & Aldribi, 2021; Jain & Mitra, 2025; Hassan & Duong-Trung, 2024) Deep Learning Models (Vinayakumar *et al.,* 2019; Thirimanne *et al.,* 2022; Elsayed *et al.,* 2024; Liu & Lang, 2019) Hybrid and Ensemble Models (Kocher & Kumar, 2021; Xuan *et al.,* 2021; Shaukat *et al.,* 2020) Unsupervised/Anomaly Detection (Jain & Mitra, 2025; Elsayed *et al.,* 2024)
Effectiveness of Automated Incident Response	SOAR & AI-Orchestrated Responses (Yousaf & Boomsma, 2024; Ismail *et al.,* 2023; Khalid & Purdie, 2024) MTTD/MTTR Improvements (Johnson *et al.,* 2024; Aramide, 2025; Obuse *et al.,* 2023) Simulation and Proof-of-Concept Evidence (Chirra, 2023; Bompally, 2025; Maddireddy & Maddireddy, 2023) AI in DFIR (Kuforiji, 2025; Bompally, 2025)

Adversarial Vulnerabilities and Mitigations	Evasion & Data Poisoning Attacks (Olutimehin *et al.,* 2025; Babatunde *et al.,* 2020; Syed, 2025) Defense Strategies (Ijiga *et al.,* 2024; Chaganti, 2024; Komaragiri & Edward, 2022) Explainability & Monitoring (Sarfraz *et al.,* 2025; Sivakumar *et al.,* 2025; Sunkara, 2022) - Threat Taxonomies (Chaganti, 2024; Syed, 2025)
Human-AI Integration and SOC Transformation	Human-in-the-loop SOC Models (Baruwal Chhetri *et al.,* 2024; Yaseen, 2022; Noshi & Blaser, 2024) Organizational Change (Sundaramurthy *et al.,* 2022; Marapu, 2022; Chinta *et al.,* 2024) - AI-Driven Predictive SOCs (Faheem & Molloholli, 2024; Jabed *et al.,* 2025) Human-AI Teaming (Baruwal Chhetri *et al.,* 2024; Sivakumar *et al.,* 2025)

Although these models have high accuracy and reduce false-positive rates, they also have complexities in operation: training time and computational requirements (Kocher and Kumar, 2021). As far as automated incident response is concerned, a variety of studies (Yousef and Boomsma, 2024; Obuse *et al.,* 2023) show significant improvements in MTTD and MTTR, and the AI systems perform better in combating cyber incidents compared to the traditional working processes. However, these systems may not be really validated in an environment other than simulation. The integrity of detection systems is at risk due to data poisoning, evasion attacks and model inversion (Olutimehin *et al.,* 2025; Babatunde *et al.,* 2020), and mitigation is divided and under-testing. Furthermore, the implementation of AI in Security Operations Centers (SOCs) has led to the required organizational shift, encompassing the reskilling of the human workforce and shift to hybrids (Baruwal Chhetri *et al.,* 2024; Yaseen, 2022). Nonetheless, the issues of adoption continue to exist because of historical infrastructure, the lack of explainability, and the cultural reluctance towards automation.

The predominant type of intrusion detection systems (IDS) in the modern context is machine learning (ML) and deep learning (DL), which are substantiated in 11 out of the 11 reviewed papers. The Support Vector Machines (SVM), Decision Trees, and Random Forests are examples of supervised learning models that remain popular because of their ease of implementation and explainability (Alshammari and Aldribi, 2021; Hassan and Duong-Trung, 2024). Nevertheless, they cannot respond well to previously unknown or polymorphic threats (Shaukat *et al.,* 2020). Deep learning models, such as CNNs, RNNs, and LSTMs, provide better generalization and detection, in turn, especially when they are trained on large datasets, e.g., NSL-KDD, CICIDS2017, and custom logs (Vinayakumar *et al.,* 2019; Dong *et al.,* 2019; Elsayed *et al.,* 2024). Such models turned out to be precise and recall their results over 90 percent, and the rates of false-positive were minimized (Thirimanne *et al.,* 2022). Still, their use in real-time applications is usually restricted by the computational needs and training rigor (Kocher and Kumar, 2021; Liu and Lang, 2019). Research has proposed a set of hybrid paradigms that hybridize between traditional ML and deep learning to address the shortcomings of either paradigm. Kumar and Garg (2012) established that the use of clustering along with classification algorithms enhanced the detection rate of anomalies in enterprise networks. Xuan *et al.* (2021) have documented the improved accuracy of APT detection with the help of ensemble learning methods with the focus on model diversity as one of the essential defense mechanisms. Nonetheless, the methods that are unsupervised and semi-supervised, including autoencoders, clustering-based anomaly detection, and K-means, have not been explored in full in spite of their promise to identify zero-day threats. This is remarkable because they are relevant in the context of environments where there is a shortage of labeled data (Elsayed *et al.,* 2024; Jain and Mitra, 2025). Graph-based deep learning in detecting lateral movement in clouds had also been postulated in studies such as Farzaan *et al.* (2025), but this is still an emerging technology. With improvement, there are still constraints. There are numerous research works that are not reproducible because each has own datasets, and performance metrics are not consistent. When reporting accuracy is common, key operational factors like time-to-detect and resource consumption aspect are not mentioned (Dhanushkodi and Thejas, 2024). Not only that, but extremely limited models take into consideration adversarial threats (Olutimehin *et al.,* 2025), despite the obvious vulnerability of ML models working on evasion conditions. Explainability is also not given much attention and this complicates their implementation in operational SOC environments where the trust of analysts is vital (Sarfraz *et al.,* 2025).

The efficiency of the AI-based incident response is determined mainly by the MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond) shapes. In 10 of the reviwed studies, AI-enabled platforms showed a quantifiable positive effect in both, frequently shortening response time by a factor of 30-50 compared to traditional, manual processes of SOC (Obuse *et al.,* 2023; Yousaf and Boomsma, 2024; Aramide, 2025). The techniques used in AI are behavioral profiling, threat scoring, and SOAR (Security Orchestration, Automation, and Response). These methods automatize repetitive

procedures, enable dynamism in the implementation of playbooks, and provide speed in the triage (Ismail *et al.,* 2023; Khalid and Purdie, 2024). In the same vein, Chirra (2023) and Maddireddy and Maddireddy (2023) created prototypes that showed tremendous reduction in the latency of detection and effectiveness of response when utilizing automated workflows based on the ML classifiers and mechanisms of anomaly scoring. Johnson *et al.* (2024) showed a 40 percent increase in MTTR with predictive analytics in an enterprise, whereas Kuforiji (2025) used AI to automate the process of conducting investigations, speeding up investigations. However, the on-the-surface use of simulated environments is a serious flaw. Few studies like Obuse *et al.,* (2023 and Khalaf *et al.,* (2025) have been able to measure live SOC settings, which restricts the extrapolability of the statements. Notably, AI systems have a range of contextual awareness. Narrowly trained systems are not able to respond to dynamic threats. This issue is especially acute in cloud-based systems, where microservice and API traffic brings noise to the system and where decisions must be made based on the context. This has been emphasized in the study by Tatineni (2023) and Farzaan *et al.* (2024) and suggested that contextual reinforcement learning is more adaptable. False positives in automated response systems are another un-discussed issue that could be triggered by alerts fatigue. Detection accuracy has increased whereas the repercussions of incorrect automated responses (e.g. stopping legitimate operations) are rarely measured. According to Goffer *et al.* (2025) and Ndibe (2025), it is necessary to add human control to verify high-severity alerts to verify automated reactions.

AML presents AI-based cybersecurity systems with serious challenges. According to the literature, data poisoning, evasion attacks, model inversion are all typical menaces with the potential of increasing the detection results significantly (Olutimehin *et al.,* 2025; Babatunde *et al.,* 2020; Syed, 2025). Overall, 11 studies directly investigated AML in different degrees of depth and rigor in their approach. Adversarial evasion attacks decoad the input data so that they can get issued with a false positive by classifiers that perceive normal behavior as evil. Such attacks are especially harmful to black-box deep learning models (Sunkara, 2022). Equally, data poisoning, in which the training data is modified to worsen the performance of the models, was also shown to hurt the long-term performance (Ijiga *et al.,* 2024; Komaragiri and Edward, 2022). At least these are critical weaknesses within continuous learning systems like the online threat intelligence systems. Ensemble learning, input sanitization and adversarial training are suggestions of defensive measures. The category of ensemble techniques was also mentioned to be useful in enhancing resilience to single-point failures (Babatunde *et al.,* 2020). Nevertheless, they are associated with a greater computational cost and complexity of training (Chaganti, 2024). Adversarial training has seen little empirical testing at scale and is showing encouraging theoretical results, but could cause overfitting (or worse generalization) in a non-adversarial application. New methods involve simulating adversaries using the Generative Adversarial Networks (GANs) (Chaganti, 2024) and integrating model explainability instruments to identify the abnormal operation of the model prior to breaking down (Sarfraz *et al.,* 2025). Nevertheless, not many systems implement such defenses in a real time and not many of them have empirical measurements of adversarial resistance. One of the identified weaknesses is that standardized adversarial threat models are not available. Numerous studies are dedicated to a single type of attacks without examining more diverse attack vectors like model extraction, inference attacks or adaptive adversaries. Consequently, some of the suggested defenses might not be generalizable to multi-modal attack surfaces (Syed, 2025; Tanikonda *et al.,* 2022). Nevertheless, not much is given to cost-benefit analysis, whereas advanced defense mechanisms enhance resilience, which raises the complexity of the system, which can directly work against real-time requirements of the cybersecurity operation.

Over time, the alteration of Security Operations Centers (SOCs) has turned into a technical and organizational problem due to the increased integration of AI systems into operations within the cybersecurity industry. The fundamental concept is the combination of AI-based detection and human judgment, which was the focus of 10 of the studies reviewed. The AI adds to the SOC efficiency through machine triage, alert prioritization, and prediction of attack vectors (Noshi and Blaser, 2024; Faheem & Molloholli, 2024). Nonetheless, analysts continue to be instrumental in putting ambiguous alerts into perspective, making the judgment in grey areas, and authenticating high-risk automated choices (Baruwal Chhetri *et al.,* 2024). This is particularly significant in conflict situations where model decisions can be bent to suit. Research highlights the importance of role redesign of AI-enhanced SOCs. According to Yaseen (2022) and Marapu (2022), it is suggested to reshape SOC, turning them into strategic investigators who perceive AI insights as alert handlers. Such a transition involves reskilling or training, a higher level of AI literacy, and alteration of organizational culture, none of which is insignificant or applied in a single way. Another important factor is AI explainability, aspiring to mitigate the lack of interpretable models, human analysts cannot meaningfully authenticate AI-driven alerts, which decrease the trust and raise risks in the operations (Sivakumar *et al.,* 2025; Sarfraz *et al.,* 2025). Although other frameworks combine XAI tools, the majority of the frameworks use black-box DL models, and this has resulted in a tension between accuracy and transparency. A number of studies emphasize infrastructure and governance issues, Sundaramurthy *et al.* (2022) explain how legacy SOCs can hardly adjust to integrated AI platforms because of the lack of unified tools and fragmented information flow. Equally, Chinta *et al.* (2024) established that both ERP and AI threat-detection integration necessitated intricate

policy and data postulates. Such organizational obstacles retard adoption even when it is technologically ready. It is also diverse in terms of organizational readiness. Large businesses are also recording improvements in the implementation of predictive SOCs (Jabed *et al.,* 2025), but the SMEs do not have the resources to implement them extensively. Furthermore, such a psychological pressure on analysts changing to AI-driven processes is minimized in most studies, where the alert fatigue is superseded by automation bias, the excessive dependence on AI-generated results and the lack of critical analysis (Baruwal Chhetri *et al.,* 2024).

Recommendation

Following the results of this review, the following recommendations are suggested to promote the development, deployment, and governance of AI-enabled cybersecurity systems. First, future studies should focus on hybrid designs, combining accuracy of deep learning with the explainability of conventional machine learning. They should also aim at standardization of evaluation measures with the help of benchmark data such as CICIDS2017 but with the help of real-life data that would provide extended generalization. Explainable AI (XAI) tools have to be integrated into the detection systems and enhance human trust and more transparency in the relationship. In addition, organizations that wish to optimize automated incident response need to go beyond simulation where live test cultures should be considered to prove a decrease in MTTD and MTR in real-threat environments. The response platforms need to have contextual decision-making and escalation policies that strike the balance between the speed and the accuracy. Moreover, the evaluation of automated response solutions must be based on impact-centric metrics but not only response time.

In addition, in order to counter the adversarial weak point, a multi-layered counter irrational approach is necessary. The combination of adversarial training, ensemble learning and input validation in AI pipelines should be encouraged in organizations. The studies also need to shift to common adversarial testing systems to quantify the robustness of models. The cost-benefit analysis should be done to determine the overhead of running these defenses. Lastly, organizations need to implement a humanistic approach to integrating AI in order to transform SOC. These involve coordinated reskilling measures, training in AI ethics, and the introduction of human control in the robotic decision making. AI systems are not meant to substitute human knowledge.

CONCLUSIONS

The systematic literature review indicates that AI-based threat detection and, in particular, deep learning models, including CNNs and LSTMs, have a strong positive effect on detection accuracy and decreased false positives in the context of network traffic and system logs. There are, however, trade-offs between all these and computation complexity and lack of interpretability which limit their use in practice in real-time systems. Likewise, automated incident response systems based on AI analytics have proven significant improvements in MTTD and MTTR, especially by behavioral model and SOAR integrations. However, most of such systems are only tested in simulated conditions, which is a major concern when it comes to scaling of operations and levels of reliability. The critical weakness of adversarial vulnerabilities was identified. The integrity of the AI systems is still jeopardized by evasion attacks, data poisoning, and model manipulation. Although other mitigation measures like the adversarial training and the ensemble learning techniques have potential, its applicability in the real world situation has not been proven yet. Moreover, the necessity of the strong evaluation systems is critical, as the sophistication levels of the adversaries are developing.

The AI-human interaction at SOCs is becoming drastically changed. The use of AI systems is automating the detection and triage processes more than ever, and analysts are required to have new roles as strategic decision-makers. Nonetheless, organizational change, such as training, culture change, and governance follows technological change, especially in the small and medium business ventures.

REFERENCES

Alshammari, A., & Aldribi, A. (2021). Apply machine learning techniques to detect malicious network traffic in cloud computing. *Journal of Big Data, 8*(1), 90.

Ankhi, R. B. (2025). Leveraging Business Intelligence and AI-Driven Analytics to Strengthen US Cybersecurity Infrastructure. *International Journal of Engineering & Extended Technologies Research (IJEETR), 7*(2), 9637-9652.

Aramide, O. O. (2025). AI-Driven Automated Incident Response and Remediation in Networks. *International Journal of Technology, Management and Humanities, 11*(02), 1-9.

Babatunde, L. A., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2020). Adversarial machine learning in cybersecurity: Vulnerabilities and defense strategies. *Journal of Frontiers in Multidisciplinary Research, 1*(2), 31-45.

Baruwal Chhetri, M., Tariq, S., Singh, R., Jalalvand, F., Paris, C., & Nepal, S. (2024). Towards human-ai teaming to mitigate alert fatigue in security operations centres. *ACM Transactions on Internet Technology, 24*(3), 1-22.

Bompally, S. D. (2025). AI-Driven Incident Response for Digital Forensics and Incident Response: A Comprehensive Framework. *Journal of Computer Science and Technology Studies, 7*(2), 467-472.

Chaganti, K. (2024). Adversarial Attacks on AI-driven Cybersecurity Systems: A Taxonomy and Defense Strategies. Authorea Preprints.

Chinta, P. C. R., Jha, K. M., Velaga, V., Moore, C., Routhu, K., & SADARAM, G. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. Available at SSRN 5151788.

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.

Dhanushkodi, K., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE access, 12,* 173127-173136.

Dong, Y., Wang, R., & He, J. (2019). Real-time network intrusion detection system based on deep learning. In *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)* (pp. 1-4). IEEE.

Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A comparative study of using deep learning algorithms in network intrusion detection. *IEEE Access, 12*, 58851-58870.

Faheem, H., & Molloholli, M. (2024). Enhancing SOC Operations with AI-Driven Predictive Analytics and Threat Intelligence.

Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments. *arXiv preprint* arXiv:2404.05602.

Farzaan, M. A., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2025). AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments. *IEEE Transactions on Machine Learning in Communications and Networking*.

Goffer, M. A., Uddin, M. S., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., ... & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. *Journal of Posthumanism, 5*(3), 1667-1689.

Hassan, S. E. H., & Duong-Trung, N. (2024). Machine learning in cybersecurity: Advanced detection and classification techniques for network traffic environments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 11*(3).

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol, 11,* 001-024.

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.

Jabed, M. M. I., Ferdous, S., Ankhi, R. B., Gupta, A. B., & Hossain, M. S. (2025). AI-Driven Intrusion Detection Systems: A Business Analyst's Framework for Enhancing Enterprise Security and Intelligence. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8*(5), 12708-12719.

Jain, V., & Mitra, A. (2025). Real-time threat detection in cybersecurity: leveraging machine learning algorithms for enhanced anomaly detection. In *Machine Intelligence Applications in Cyber-Risk Management* (pp. 315-344). IGI Global Scientific Publishing.

Johnson, O. B., Olamijuwon, J., Cadet, E., Osundare, O. S., & Weldegeorgise, Y. W. (2024). Developing real-time monitoring models to enhance operational support and improve incident response times. *Int J Eng Res Dev, 20*(11), 1296-1304.

Khalaf, N. Z., Al Barazanchi, I. I., Radhi, A. D., Parihar, S., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of CyberSecurity, 5*(2), 501-513.

Khalid, I., & Purdie, M. S. (2024). AI-Powered SOC Operations: Revolutionizing Cyber Security Incident Response and Management.

Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing, 25*(15), 9731-9763.

Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. *International Journal of Scientific Research and Management (IJSRM), 10*(10), 981-998.

Kuforiji, J. (2025). Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. *Journal of Data Analysis and Critical Management, 1*(04), 1-19.

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences, 9*(20), 4396.

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.

Marapu, N. R. (2022). Harnessing AI for Advanced Threat Detection: Enhancing SOC Operations Across US Critical Industries. *International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3*(1), 49-62.

Mintoo, A. A., Saimon, A. S. M., Bakhsh, M. M., & Akter, M. (2022). National Resilience Through Ai-Driven Data Analytics And Cybersecurity For Real-Time Crisis Response And Infrastructure Protection. *American Journal of Scholarly Research and Innovation, 1*(01), 137-169.

Mollah, M. H. O. R. (2025). AI-Driven Threat Detection And Response Framework For Cloud Infrastructure Security. *American Journal of Scholarly Research and Innovation, 4*(01), 494-535.

Nallapareddy, V. S. S. R., & Katta, S. K. R. (2025, February). AI-Enhanced Cyber Security Proactive Threat Detection and Response Systems. In *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 1510-1514). IEEE.

Nazeer, O. A. (2021). AI-Powered Security Operations Centers (SOC) in the Cloud: Automating Threat

Detection and Response. *International Journal of Emerging Trends in Computer Science and Information Technology, 2*(2), 8-16.

Ndibe, O. S. (2025). Ai-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. *International Journal of Research Publication and Reviews, 6*(5), 389-411.

Noshi, A., & Blaser, F. (2024). Integrating artificial intelligence and machine learning for advanced cyber security in soc operations.

Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-powered incident response automation in critical infrastructure protection. *International Journal of Advanced Multidisciplinary Research Studies, 3*(1), 1156-1171.

Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-powered incident response automation in critical infrastructure protection. *International Journal of Advanced Multidisciplinary Research Studies, 3*(1), 1156-1171.

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial threats to AI-driven systems: Exploring the attack surface of machine learning models and countermeasures. Available at SSRN 5137026.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, 372.

Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology, 19*(12), 764-773.

Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating incident response: AI-driven approaches to cloud security incident management. *Chelonian Research Foundation, 15*(2), 1-10.

Sarfraz, M., Sumra, I. A., Khalid, B., & Fatima, E. (2025). AI-driven predictive threat detection and cyber risk mitigation: a survey. *Journal of Computing & Biomedical Informatics, 8*(02).

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies, 13*(10), 2509.

Sivakumar, J., Salman, N. R., Salman, F. R., Salimova, H. R., & Ghimire, E. (2025). AI-driven cyber threat detection: enhancing security through intelligent engineering systems. *Journal of Information Systems Engineering and Management, 10*(19), 790-798.

Sivakumar, J., Salman, N. R., Salman, F. R., Salimova, H. R., & Ghimire, E. (2025). AI-driven cyber threat detection: enhancing security through intelligent engineering systems. *Journal of Information Systems Engineering and Management, 10*(19), 790-798.

Sultana, S., Uddin, M., Chy, M. A. R., Hasan, S. N., Hossain, E., Kaur, H., & Kaur, J. (2025). AI-augmented big data analytics for real-time cyber attack detection and proactive threat mitigation. *International Journal of Computational and Experimental Science and Engineering, 11*(3), 5639-5647.

Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). The future of enterprise automation: Integrating AI in cybersecurity, cloud operations, and workforce analytics. *Artificial Intelligence and Machine Learning Review, 3*(2), 1-15.

Sunkara, G. (2022). AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks. *Well Testing Journal, 31*(1), 185-198.

Syed, S. A. (2025). Adversarial AI and cybersecurity: defending against AI-powered cyber threats. *Iconic Research And Engineering Journals, 8*(9), 1030-1041.

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. *Journal of Science & Technology, 3*(1).

Tatineni, S. (2023). AI-infused threat detection and incident response in cloud security. *International Journal of Science and Research (IJSR), 12*(11), 998-1004.

Thirimanne, S. P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., & Hewage, C. (2022). Deep neural network based real-time intrusion detection system. *SN Computer Science, 3*(2), 145.

Veluru, S. P. (2021). Leveraging AI and ML for Automated Incident Resolution in Cloud Infrastructure. *International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2*(2), 51-61.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE access, 7*, 41525-41550.

Xuan, C. D., Duong, D., & Dau, H. X. (2021). A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. *Journal of Intelligent & Fuzzy Systems, 40*(6), 11311-11329.

Yaseen, A. (2022). Accelerating the SOC: Achieve greater efficiency with AI-driven automation. *International Journal of Responsible Artificial Intelligence, 12*(1), 1-19.

Yousaf, Z., & Boomsma, D. (2024). AI-Driven SOC Operations: Improving Incident Response Time and Threat Analysis.