International Journal of Informatics and Data Science Research
ISSN 2997-3961 (Online)
Vol. 2, No. 11, Nov 2025,
Available online at: https://scientificbulletin.com/index.php/IJIDSR

Adaptive AI-Driven Threat Intelligence System for Real-Time Detection of Zero-Day Cyber Attacks

Mamarizayev Mashrabjon Askar Ugli
Master of Science in Information Technology (MSc IT), Sambhram University
mashrabmamarizayev@gmail.com

Article information:
Manuscript received: 4 Sep 2025; **Accepted:** 10 Oct 2025; **Published:** 28 Nov 2025

Abstract: Zero-day cyber attacks remain one of the most damaging and difficult threats to detect due to the lack of prior knowledge and response signatures. Traditional intrusion detection systems (IDS) and signature-based security mechanisms frequently fail when confronting rapidly evolving attack vectors that exploit unknown vulnerabilities. To address this gap, this study proposes an adaptive AI-driven threat intelligence framework capable of real-time learning from dynamic threat environments. The proposed conceptual model integrates machine learning, anomaly detection, and automated threat intelligence feeds within a continuous feedback loop. In contrast to static models, the system evolves autonomously by updating detection parameters based on new behavioral patterns and contextual information. The results of this theoretical investigation highlight the potential for improved early detection capability, reduced false-positive rates, and accelerated response agility against zero-day attacks. This research contributes to the field by presenting a scalable and resilient architecture that advances proactive cybersecurity defense strategies.

Keywords: Zero-day attacks, Adaptive AI, Threat intelligence, Real-time detection, Cybersecurity.

Introduction

Cybersecurity systems are continuously confronted by increasingly sophisticated attacks that exploit undiscovered software vulnerabilities before security teams can identify and remediate them. These zero-day attacks successfully bypass conventional security controls because no prior indicators of compromise (IOCs), known signatures, or defensive methodologies exist at the moment of initial exploitation. A single zero-day incident can compromise highly confidential data, disrupt business operations, and potentially escalate into large-scale cyber espionage or destructive attacks. Furthermore, the rapid growth of cloud infrastructure, Internet of Things (IoT) ecosystems, and remote operational technologies has significantly expanded the global attack surface, enabling adversaries to discover and exploit weaknesses faster than defenders can detect or respond.

Recent advancements in automated exploit generation, malware obfuscation, and cybercrime-as-a-service markets have further amplified the volume and complexity of zero-day intrusions. Modern attackers leverage polymorphic and metamorphic malware that can continuously modify its properties during execution, rendering signature-based intrusion

detection and static analysis techniques largely ineffective. Zero-day exploits have also become profitable commodities in underground marketplaces, making them easily accessible to malicious actors with minimal technical expertise—ultimately intensifying the overall threat landscape.[1]

Traditional defense mechanisms depend on predefined rules, static blacklists, and periodically updated signature databases. These solutions inherently provide reactive protection and only become effective once an attack has already been observed and documented. As a result, detection delays are inevitable and often lead to severe operational and financial damage. Security Operation Centers (SOCs) struggle to scale manual analysis capabilities against persistent automated attack campaigns, resulting in alert fatigue, resource shortages, and reduced situational awareness. Consequently, attackers frequently maintain prolonged undetected presence within compromised environments.

In response to these challenges, artificial intelligence (AI)—particularly machine learning (ML) and deep learning (DL)—has emerged as a promising solution for proactive cybersecurity defense. AI techniques enable the identification of irregular behaviors without requiring prior knowledge of threat signatures. However, most current ML-based systems rely on static or offline training models that lack adaptive learning capabilities. These models typically require extensive labeled datasets, undergo periodic retraining, and perform inconsistently in real-world environments where data streams are highly dynamic and continuously evolving.[2]

Compounding the issue, adversaries actively develop adversarial AI strategies to poison datasets and manipulate learning mechanisms in order to evade classification. Therefore, despite AI-driven improvements in anomaly detection, adaptability, robustness, and real-time autonomous response remain insufficient in existing security solutions.

To enhance contextual understanding, many organizations have adopted Threat Intelligence Platforms (TIPs) designed to aggregate and correlate global indicators of malicious activity. Although these platforms improve awareness of previously observed attacks, they predominantly support reactive intelligence and contribute limited value when confronting entirely new or unknown exploit techniques.

Thus, adaptive AI-driven threat intelligence has become a strategic requirement for modern cybersecurity resilience. Systems equipped with continuous learning capabilities can autonomously refine analytical logic, correlate anomalies with external intelligence sources, and predict malicious intent before concrete attacks materialize. This transformation from reactive defense to proactive prevention significantly reduces detection latency while minimizing potential impact.

Motivated by these challenges, this research aims to establish a cybersecurity framework capable of delivering sustained protection in environments characterized by uncertainty, rapidly evolving threats, and minimal human intervention. The proposed conceptual model integrates adaptive machine learning, autonomous intelligence enrichment, and real-time decision-making within a closed-loop architecture.

The primary objectives of this study are to:

- ✓ Enable real-time anomaly detection and autonomous model evolution
- ✓ Minimize dependency on labeled datasets and manual interventions
- ✓ Enhance the prediction of unknown exploit behavior
- ✓ Improve operational scalability for next-generation digital ecosystems

By introducing an intelligent and adaptive threat detection paradigm, this research strives to

overcome the critical limitations of traditional defense techniques and advance zero-day cybersecurity protection strategies.

Literature Review

Zero-day attack detection has remained a critical research problem for cybersecurity due to the lack of pre-existing threat signatures and behavioral indicators. Earlier detection systems have largely depended on signature-based approaches, such as traditional IDS technologies, which fail to identify novel exploits that do not match known malicious patterns . This limitation has shifted the focus of recent research toward behavioral-based and anomaly detection methods that attempt to classify suspicious activities by learning normal system behavior.

Machine learning (ML) models have been increasingly utilized to detect anomalies in network traffic and system logs. However, a major challenge in ML-driven security is the dependency on large-scale, labeled datasets for effective training . Labeled datasets for zero-day behaviors are either scarce or non-existent, creating performance degradation in real-world systems. Researchers have attempted to introduce unsupervised and semi-supervised learning to reduce reliance on labeled data , yet these models often generate high false-positive alerts, making them difficult to deploy at scale.[3]

To refine anomaly detection, recent studies incorporate deep learning (DL) architectures such as LSTM, autoencoders, and graph neural networks . These models show promise in identifying unknown patterns, but their training requirements are computationally expensive and slow to adapt in real-time threat scenarios. Moreover, adversaries increasingly develop adversarial AI techniques that manipulate deep learning detectors by introducing subtle perturbations into features to evade classification . This emerging threat highlights a need for models with stronger robustness and adaptability.

Alongside ML advancements, Threat Intelligence Platforms (TIPs) have evolved to enable coordinated intelligence sharing among organizations. TIPs enhance detection by integrating indicators of compromise (IOCs), attack signatures, malware samples, and vulnerability feeds from multiple trusted sources . However, current TIP systems primarily operate on reactive intelligence, where only previously observed threats are shared. Consequently, their utility declines when facing brand-new exploits without historical fingerprint data.[4]

Recent research increasingly investigates hybrid threat detection models, where AI-driven anomaly detection is combined with context-aware threat intelligence correlation . These models reduce false alarms and improve detection relevance by evaluating the maliciousness of events within a broader situational context. Despite these advancements, most hybrid frameworks still rely on static model updates, meaning the underlying detection algorithms require periodic retraining. This approach becomes inefficient in rapidly shifting cyber environments where attacks continuously evolve.

A new direction in the literature focuses on developing adaptive and online learning systems that dynamically update analytics based on new data without full retraining [5]. Studies of reinforcement learning and streaming analytics technologies show strong potential for enabling autonomous defense evolution, but existing implementations remain mostly experimental and fragmented across specific domains.

In summary, the literature reveals three persistent challenges in zero-day detection research:

Challenge	Description	Remaining Limitation
Signature dependency	Traditional IDS and TIP rely on known threats	Zero-day evasion

Static AI models	ML/DL unable to adapt continuously	Requires frequent retraining
High false positives	Noise from anomaly detection	Analyst overload

Therefore, despite considerable progress, a unified and scalable solution capable of real-time autonomous adaptation has not yet been fully realized. This research aims to address these gaps by proposing a self-learning adaptive AI-driven threat intelligence system capable of evolving in sync with the threat landscape, thereby improving detection rates and reducing operational fatigue in cybersecurity environments.[6]

Methodology

This research employed methods of cyber-threat data observation, expert analysis, comparative study, and simulation-based theoretical examination. Reliable data were collected from real-time network monitoring systems, publicly available cyber-attack datasets, threat intelligence feeds, and professional security incident reports. Interviews and expert insights from cybersecurity specialists were analyzed to ensure scientific credibility.

Observational methods were used to track anomalies in network traffic and identify unusual behavioral patterns that may indicate zero-day exploit attempts. Comparative analysis helped evaluate how adaptive artificial intelligence improves detection when compared to static signature-based intrusion detection systems. Through theoretical simulation, the ability of machine learning models to react to newly emerging threats without prior knowledge was assessed.

Advanced global cybersecurity practices and current national cyber defense policies were studied. Based on this analysis, key conditions necessary for the effective deployment of adaptive AI-driven threat intelligence were identified, including continuous model updating, automated threat correlation, and rapid decision-making capability.

Analysis and Results

The analysis of the collected cybersecurity data reveals that traditional intrusion detection systems fail to identify zero-day attacks due to their dependency on predefined signatures. During observations of network traffic, numerous anomalies were detected that did not match any known malicious patterns, confirming that conventional approaches cannot provide timely protection against newly emerging threats. The study also demonstrated that static machine learning models have limited capacity to adjust to rapid changes in cyberattack behavior, resulting in decreased accuracy and increased false alarm rates when exposed to unknown exploit vectors.[7]

In contrast, the theoretical simulation of the adaptive AI-driven model showed significant improvements in recognizing early indicators of zero-day attacks. Such improvement is explained by the model's ability to continuously learn from live threat environments and modify its decision boundaries based on real-time behavioral changes. As a result, the detection of previously unseen threats became more reliable. Furthermore, the system's integration with automated threat intelligence considerably minimized noisy alerts by validating suspicious activities with contextual information collected from global cyber incident feeds.[8]

The adaptive model not only enhanced detection performance but also accelerated response actions. In many analyzed scenarios, the system rapidly generated alerts without waiting for human intervention, which is considered crucial in preventing destructive outcomes such as data exfiltration or operational shutdowns. The persistent learning workflow also ensured that once an attack pattern was recognized, the model retained the acquired knowledge and applied it to future similar attacks, thereby reducing vulnerability exposure time.[9]

The overall results of this analysis suggest that adaptive AI-based threat intelligence frameworks outperform static systems in resilience, predictive capability, and operational agility. By maintaining continuous learning and automated intelligence enrichment, the model strengthens cybersecurity posture and helps organizations defend themselves in an environment where attackers constantly evolve. These findings support the conclusion that adaptive learning technologies are a vital pathway for advancing zero-day cyber defense strategies, enabling proactive protection rather than reactive recovery.[10]

Conclusion and recommendation

This research confirms that the evolving nature of cyber threats, particularly zero-day attacks, demands a paradigm shift from traditional reactive cybersecurity mechanisms to proactive and adaptive defense models. Systems that depend solely on signature databases or static machine learning algorithms cannot respond effectively to emerging exploits that have not yet been examined or documented by the security community. The analysis conducted throughout this study highlighted significant weaknesses in existing architectures that fail to evolve at the same pace as adversarial innovations.

By proposing an adaptive AI-driven threat intelligence system, this research offers a novel direction for enhancing early threat detection capacities in modern digital infrastructures. The combination of real-time anomaly analytics and automated intelligence enrichment forms a dynamic defense layer that continuously adapts to behavioral changes in network environments. This continuous learning ability enables faster response times, improves the accuracy of predicting malicious intent, and reduces operational fatigue caused by false positives. Moreover, the system's proactive nature minimizes attack dwell time and limits destructive impact before a zero-day vulnerability becomes publicly exploited.

Ultimately, the findings emphasize that adaptive artificial intelligence is not merely an optional enhancement but a necessary evolution for sustainable cybersecurity resilience. The proposed framework establishes a strong foundational strategy for future research and development of intelligent cybersecurity ecosystems that can autonomously understand, detect, and respond to novel cyber threats. It positions organizations to maintain trust, operational continuity, and defensive superiority in a rapidly advancing technological era.

Based on the analytical outcomes of this research, it is recommended that cybersecurity organizations and technology developers increase their focus on adaptive learning approaches when designing new defense systems. Security Operation Centers (SOCs) should actively integrate automated threat intelligence feeds to minimize human workload and accelerate decision-making. Additionally, investment in machine learning platforms capable of continuous updating is essential to ensure that detection models remain effective against rapidly changing attacker behaviors.

Further research should examine practical implementation scenarios, evaluate scalability in large-scale environments, and incorporate adversarial robustness measures to prevent manipulation of learning algorithms. Collaboration between institutions to share anonymized threat intelligence is also strongly encouraged, as collective knowledge contributes to faster global recognition of zero-day attacks. Policymakers and industry leaders should prioritize the adoption of adaptive cybersecurity technologies to secure critical infrastructures and maintain digital trust in the future.

List of used literature

1. Y. Zhang, X. Chen, and H. Li, "Zero-day attack detection based on anomaly analysis in network systems," *IEEE Access*, vol. 9, pp. 13420–13433, 2021.
2. M. Ahmed and A. Mahmood, "Machine learning for zero-day malware detection,"

Computers & Security, vol. 113, p. 102561, 2022.

3. J. Romero and P. Garcia, "Adaptive intrusion detection using online learning," *Journal of Information Security and Applications*, vol. 64, p. 103067, 2022.
4. B. Wang and K. Ren, "Threat intelligence sharing for proactive cybersecurity," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1550–1573, 2023.
5. A. Alazab et al., "Deep learning-driven cyber threat analytics: State of the art," *Future Generation Computer Systems*, vol. 142, pp. 315–329, 2023.
6. S. Park and J. Kim, "Malware behavior analysis using graph neural networks," in *Proc. IEEE ICC*, 2024, pp. 1–6.
7. C. Li, H. Zhou, and Q. Wu, "Reducing false positives in IDS using threat intelligence correlation," *Applied Intelligence*, vol. 53, pp. 4527–4542, 2023.
8. A. Javaid et al., "Reinforcement learning for zero-day exploit prevention," *Knowledge-Based Systems*, vol. 258, p. 110004, 2023.
9. S. Farooq and D. Z. Khan, "Polymorphic malware detection using AI techniques," *Expert Systems with Applications*, vol. 219, p. 119644, 2023.
10. L. Sun et al., "Adversarial robustness for cybersecurity deep learning models," *IEEE Trans. Dependable & Secure Computing*, vol. 21, no. 2, pp. 94–106, 2024.