

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Predictive Cyber Security Framework Using Machine Learning and Threat Intelligence

Shahzad Ahmad*

Department of Computer Science, Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Sub Campus Rajanpur, 32300, Punjab, Pakistan
Email: shahzadahmed42408@gmail.com

Nihal Khan*

Department of Computer Science, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: nihalkhangorchani@gmail.com

Noor Fatima*

Department of Information Technology, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: nfnoorfatima44@gmail.com

Tayyaba shakoor*

Lecturer, Department of Computer Science, KFUEIT, sub campus Rajanpur, punjab, pakistan
Email: tayyabashakoor2455@gmail.com

Muhammad Shahzad*

Department of Computer Science, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: mr.shahzad07863@gmail.com

Shehla Bibi*

Department of Computer Science, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: shehlabibi2006@gmail.com

Hasnain Nawaz*

Department of Computer Science, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: hasnainnawaz394@gmail.com

Aliza Batool*

Department of Information Technology, KFUEIT, Sub Campus Rajanpur, 33500, Punjab, Pakistan
Email: alizabatool844@gmail.com

ABSTRACT

State-of-the-art security systems are often unable to counter modern threats effectively, since many of them are still based on a signature-based approach. Therefore, they fail to detect zero-day attacks and multi-stage Advanced Persistent Threats (APTs). While individual components - log-based ML classification, NLP-driven dark-web analysis, CTI enrichment - have each been explored separately, no existing framework integrates all three within a unified, CTI-fused architecture explicitly oriented toward reducing SOC alert volume. Additionally, the paper identifies lab-to-production drift as a critical design consideration for future validation. This paper presents a concept for a five-layer-based predictive security approach that, in the early stages of a potential attack, aims to detect and prevent it by using structured and unstructured internal and external data. The core layer for the estimation of threat probabilities is a log layer, where, by means of a Random Forest algorithm, structured log data, as well as communication records, are processed in order to compute a threat probability. In addition to the log layer, there is a text layer where, using LSTM/Transformer, unstructured textual reports from the dark web and open-source intelligence (OSINT) are processed. A fusion layer combines these outputs with Cyber Threat Intelligence (CTI), linking indicators to known malware campaigns. The framework aims to improve SOC efficiency by prioritizing high-confidence, context-rich alerts over raw volume. The paper also identifies model validation and data-drift awareness as essential considerations when transferring laboratory-trained models into real systems, with concrete mitigation mechanisms proposed as future work. However, an empirical validation as well as an implementation of the presented concepts is still to be done in the future.

Key words

Conceptual Framework, Predictive Security, Machine Learning, Cyber Threat Intelligence, Design Science

1. Introduction

Moving to a purely defensive posture is not sufficient. Security has traditionally been seen as a form of incident response, stopping an attack in progress and managing the aftermath once it has occurred. Modern attackers, however, are equipped with sophisticated tools, including zero-day exploits and ransomware, that allow them to defeat traditional security measures (Sarker, 2024). Thus, the focus of much of the current cybersecurity research is on attempting to predict and prevent an attack before it occurs. This shift toward proactive cybersecurity underlies the growing research interest in predictive approaches, as it is likely to be more effective than incident response in the long run.

Incorporating Machine Learning (ML) and integrating it with Threat Intelligence significantly increases the detection capabilities of such a system. The Machine Learning component in the system aims to identify unknown patterns and indicators of

an attacker's intent and past behavior within the large amounts of telemetry data. When combined with Threat Intelligence, this system aims to detect, identify, and characterize unknown threats while providing contextual information. The main goal of this study is to design a predictive framework that aims to provide early warning of potential cyber-attacks. This framework is designed to assist security teams in determining which threats are more critical to handle and will also aid in minimizing false negatives. A system that only alerts security teams after an attack has occurred is of little value to organizations where delayed alerting and constrained decision-making time critically undermine effective response (Bella & Lee, 2025). This paper presents the conceptual design; empirical validation remains future work.

2. Literature Review

3.1 Emerging Trends in Predictive Cybersecurity

The world of cybersecurity is now entering a new era where predictive analytics and ML are becoming increasingly central. Recent research suggests that AI has evolved from a potential threat vector to a defensive tool that detects signals that indicate a threat before an attack even begins. With the help of tools such as time series analysis and anomaly detection, these systems have become highly adept at detecting upcoming attacks. A key finding of this research is that it does not merely react to anomalies but rather provides advance alerts to catch the early signals of a threat (Al Abdulwahid, 2025; JS et al., 2024).

When examining the research on predictive analytics, it is clear that machine learning and security systems have made them more effective. By modeling behavior and analyzing data on a regular basis, it is now possible to detect suspicious changes that are hidden from the general public before they occur. In fact, the trend is changing; in the future, cyber defense will not be limited to providing just alerts, but rather it will have to predict ahead of time so that the threat is eliminated before it even arises (Okpala & Chukwumanya, 2025; Nazim et al., 2025; Oye et al., 2024).

3.2 Machine Learning Models in Security

In the world of cybersecurity, ML algorithms are now handling every kind of difficult task. Whether it is decision trees or neural networks, they have all proven their worth in different situations. For example, when it comes to structured data or telemetry, models like Random Forest are effective. But if the data is unstructured, like text-based or semi-structured reports, then the results of SVMs and neural networks are revealing. In fact, each model has its own strengths that make it perfect for a particular task (Sundar et al., 2025; Naseer, 2023).

Recently, some research has shown that deep learning models, especially LSTM and transformer architectures, have proven to be highly effective at predicting the early signals of cyberattacks, and their real-time performance has never been better. And when compared to GBM, it becomes clear that the choice of model depends on the organization's own goals - some need to remember as much as possible, so there is an optimal balance between precision and recall. The 'one size fits all' formula never works in cybersecurity research (Al Abdulwahid, 2025; JS et al., 2024).

3.3 Threat Intelligence

A key challenge is the ‘noise’ of raw text and alerts that confuse security teams. This is where cyber threat intelligence (CTI) contextualizes ambiguous indicators. When threat intelligence is added, such as dark web mentions, exploit mentions, or malware family data, to the model, it doesn’t just pick up on signals but also starts to understand the rich ‘context’. This lets the system know which threats are truly serious, enabling more informed decisions (Dalal, 2020; Mishra et al., 2022).

Research from CTI on the dark web has shown that when it comes to semi-structured data, SVM and ANN perform well on semi-structured text, while tree-based models suit structured logs. The clear implication is that if text intelligence is harnessed properly for ML, it can be highly beneficial. However, a limitation exists; studies working on CTI also say that data preprocessing and event extraction are significant challenges. If the intelligence is not structured properly, its predictive value is lost, and all the hard work diminishes significantly (Zenebe, 2022; Ghazi et al., 2018).

3.4 Hybrid And AI-Driven Frameworks

In today’s research, the hybrid AI framework is increasingly being used due to the lack of clarity of the system’s decisions, the use of old data, and the need to test results in real time. Another study suggests that predictive analytics and machine learning will change cyber defense strategies in the future and make digital infrastructure significantly more resilient. According to a major review, deep learning has shown great performance, but some old problems still persist (Hermawan, 2025; Alazab et al., 2024).

Similarly, the research being done on AI-powered frameworks suggests that when combined with structured telemetry, unstructured text, and threat intelligence, attacks can be detected more comprehensively. It is likely that in the future, these systems will be the backbone of cybersecurity, which will be able to collect information from independent sources and analyze it.

Table 1: Comparison of Existing Predictive Security Frameworks

Study	ML Approach	CTI Integration	SOC Focus	Alert Drift Handling
Al Abdulwahid (2025).	Time series	No	No	No
JS et al. (2024).	Anomaly detection	No	No	No
Alazab et al. (2024).	Deep learning	Partial	No	No
Hermawan (2025)	Hybrid AI	Partial	No	No
Mishra et al. (2022).	ML + CTI	Yes	No	No
Proposed Framework	RF LSTM/Transformer	+ Full Fusion	Yes	Identified

Summarized in Table 1 above are the individual components of predictive security addressed in the current body of research studies. Although these frameworks facilitate the various components of predictive security using ML and hybrid approaches, none

of them have focused on security using ML-based detection for the integration of CTI while attempting to reduce the current volume of SOC alerts using predictive security. This research study attempts to bridge this identified gap in current research studies by proposing a 5-layer architecture framework for predictive security.

3. Research Gap

There is a significant research gap in the current state of Threat Intelligence (TI) and Machine Learning (ML) integration. Current approaches to cybersecurity address two separate problems: attack detection and information extraction. However, there is a substantial shortfall in the amount of work that has been undertaken to develop a unified predictive framework that integrates both of these components. Recent work by Nalluri et al. (2025) proposed a framework that undertakes ML-TI integration, but it does not seek to address the issue of reducing the volume of SOC alerts. The work presented in this paper will fulfill this gap by the introduction of a five-layered architecture.

A second major research gap within the information processing in the cybersecurity context concerns the assessment of the latency of developed models and their robustness in real-time processing. Most of the current research models and techniques are validated on benchmark datasets, and their performance is measured in terms of various evaluation metrics. However, in cybersecurity, the current attack tactics and strategies of attackers are changing very fast, and also the data used for training and testing the models are subject to drift over time. Therefore, there is a need to assess the latency of current models and their robustness in real-time processing (Ashfin, 2024; Bai & Fang, 2024). This research gap can be considered as future work of the current research study.

A third, critical gap in the state of the art and practice concerns the aspects of explainability and analyst trust. In addition to a high classification quality, alert filtering systems also need to support their users in understanding the reasons behind their decisions, in order to gain their acceptance as opposed to becoming ‘black boxes’ that are not to be trusted by analysts (Rao, 2022). This critical gap, however, is not yet addressed by the proposed architecture, but instead it is a challenge that can be addressed by additional components (SHAP, LIME, etc.) that can be integrated into the architecture as future work.

The fourth gap in existing work, related to data fusion, although theoretically simple to integrate historical logs and CTI with alert streams in real time, is extremely challenging to implement and to achieve reliable operation, with considerable development effort required (Dutta & Kant, 2020; Montasari et al., 2020). In this paper, a Fusion Layer is proposed within the 5-layer architecture to integrate ML-based information with the CTI information.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

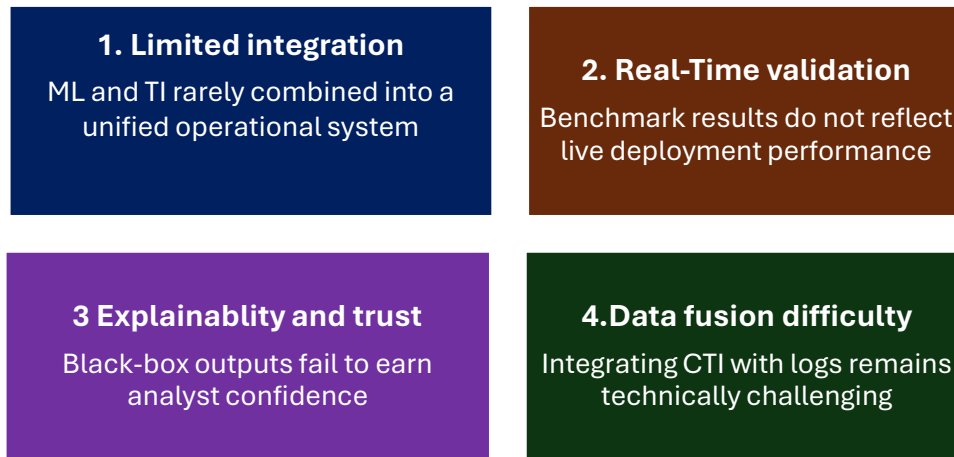
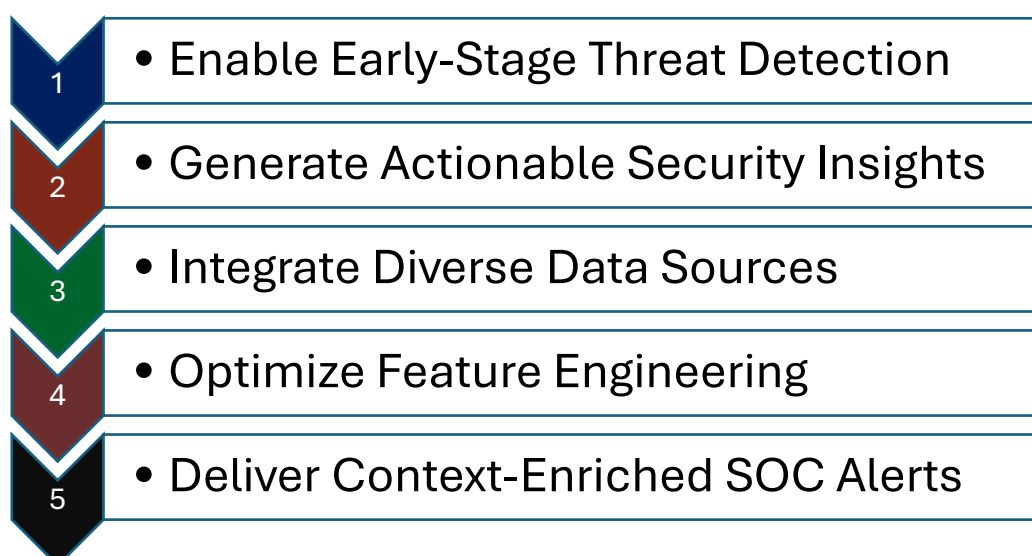


Figure 1: Identified Research Gaps in ML and Threat Intelligence

This study addresses mainly Gap 1 (ML-TI integration) and Gap 4 (data fusion) by proposing a 5-layer architecture for predictive cybersecurity. The other two gaps (Gap 2: real-time validation and Gap 3: explainability) are important for future research.

4. Research Objectives

1. Propose a predictive framework to enable early-stage threat detection.
2. Integrate ML with Threat Intelligence to generate security intelligence.
3. To enable the processing of logs (of different structures) and unstructured Threat Intelligence feeds.
4. To outline feature engineering strategies that can enhance the performance of the models.
5. To design context-enriched alert prioritization in order to enhance decision



making of security incidents by SOC analysts.

Figure 2: Research Objectives for the Proposed ML-TI Framework

5. Research Questions

1. How can machine learning and threat intelligence be integrated to enable early-stage threat detection?
2. Which data sources are most useful and efficient for threat prediction?
3. Which ML models are most suitable for processing structured and semi-structured security data?
4. Does threat intelligence fusion improve prediction quality?
5. What are the design considerations to support the implementation in a Security Operations Center (SOC) and analyze alerts in a meaningful way?

6. Methodology

This study was conducted by following the principles of Design Science Research (Hevner et al., 2004), i.e., it aims at developing a conceptual framework of predictive cybersecurity in the field of Information Systems instead of realizing an empirical study.

In this study, a literature study was conducted to develop a solid basis of current predictive cybersecurity and CTI-related work. Subsequently, a conceptual design for a data pipeline was developed that includes all steps from data ingestion until the generation of alerts based on generated predictions.

The proposed approach is based on two main pillars: first, on structured data in the form of logs and traffic metadata of any kind, and second, on semi-structured data, i.e. threat reports, dark web posts, etc., of a more complex and nuanced nature. Each of the two types of data requires its own kind of processing, and by combining the two streams of information, a more complete threat assessment can be created.

The current work outlines the conceptual design of the predictive framework and its theoretical foundation. Future work, however, is to be dedicated to the empirical validation of the approach.

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

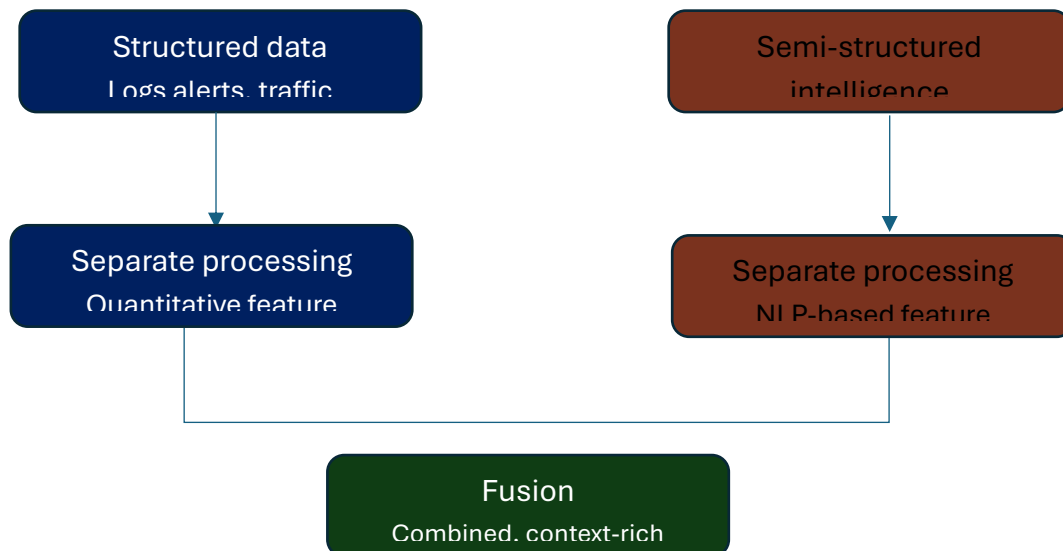


Figure 3: Proposed Methodology for Structured, Semi-Structured, and Fusion

6.1 Data Collection

The proposed system utilizes two pillars of data collection. First, the system uses structured telemetry data such as security logs, endpoint telemetry and firewall logs within the network. Secondly, it uses semi-structured threat intelligence gathered from open sources and dark web (Dalal, 2020; Ofili et al., 2024). The structured data and the semi-structured threat intelligence go through different processing in the system, and their fusion helps in creating a complete threat prediction framework (Zenebe, 2022). Using external sources for data collection early detects emerging exploits and campaigns. Accurately labeling the data collected is critical, as extracting features from raw text data is challenging. The data at the time of collection is categorized as benign, suspicious or malicious (Hermawan, 2025). These ground-truth labels can then be used for supervised learning to differentiate between normal activity and a threat. After that, the structured and semi-structured data go through different processes. These two kinds of data are integrated later to form a complete prediction framework (Zenebe, 2022). After going through the processes, each text data is assigned with some tags like malware family, threat actor, etc. Those tags are very important to model to know about the threat (Hermawan, 2025; Nagamalla & Sanapala, 2023). Thus, the internal data as well as external data are used to form a model to detect threats as early as possible (Dalal, 2020).

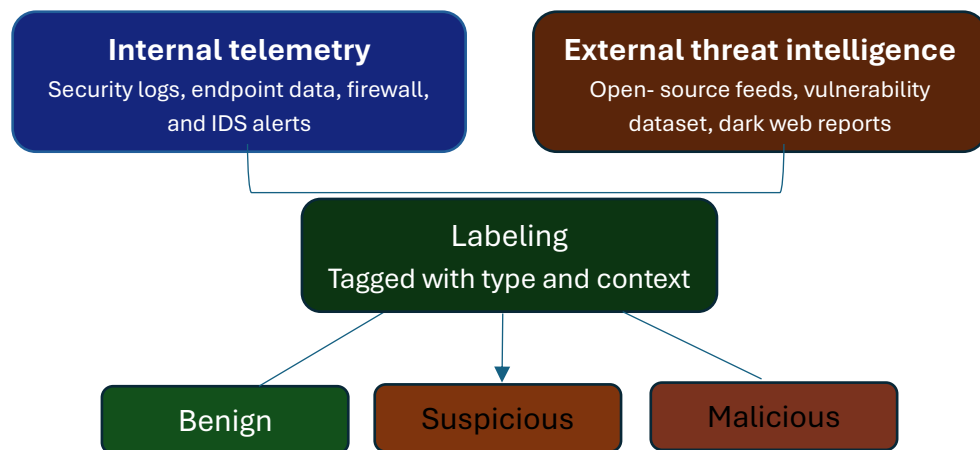


Figure 4: Internal and External Data Sources with Labeling Process

Table 2: Summary of Data Categories, Source, and Purpose

Data Category	Type	Sources	Purpose
Structured Telemetry	Internal	Security logs, endpoint telemetry, firewall events	Reveals internal, real-time network activity
Semi-Structured Intelligence	External	Open -source threats feeds, dark web posts	Provides early indicators of new exploits and campaigns
Ground-Truth Labels	Classification	Benign, suspicious, malicious category	Supervises the model to distinguish normal from threat activity
Contextual Tags	Enrichment	Malware family, threat actor name	Helps the model interpret threat characteristics

6.2 Data Analysis

The analysis cycle begins by transforming the raw collected data into a human-understandable format, starting with the raw telemetry data as well as the gathered threat intelligence. Firstly, the raw data is pre-processed to remove any superfluous data, for example, the same entry that has been logged multiple times. This step is critical to removing noise from the data model. The remaining data is then normalized

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

for the timestamp field, and the text portion of the data is tokenized. This phase includes the process of extracting quantitative patterns and features from structured information in order to analyze traffic activity. At the same time, feature signals are also extracted from the semi-structured information in the form of contextual data, including, for example, the name of malware and even information regarding known vulnerabilities in the form of their respective CVE IDs. These two sets of features then provide a comprehensive framework for analyzing network traffic to facilitate early detection of potential threats. The subsequent step is the correlation of the extracted features with the Indicators of Compromise (IOCs) to identify potential threats. In this respect, the proposed framework goes beyond simple anomaly detection (Koloveas et al., 2021). Finally, both accuracy and recall are prioritized, as missing a single security risk is unacceptable (Kumar, 2023).

7. Proposed Framework

The entire framework revolves around five different layers that work in a seamless flow. The first is data ingestion, where logs and feeds are collected, and then there is the pre-processing stage, where the scattered data is cleaned according to criteria so that the model can get the right input. The next step is machine learning inference, where the model derives the risk probability of each activity, which is immediately followed by threat intelligence fusion to make the predictions more robust and 'contextual' with the context of the real world (Shimu, 2025). The alert prioritization layer generates the final output of alerts, which are prioritized for SOC analysts to deal with most urgent threats and reduce huge amounts of low priority alerts for human analysis. The framework produces more than simple anomalies and provides full contextual information for every alert generated. The framework analyzes suspicious activity of IP address that has been previously unknown. It also receives historical information of campaigns from CTI feeds and increases confidence when previously unknown IP address is related to an old campaign (Umar & Abbas, 2022; Lima et al., 2025).

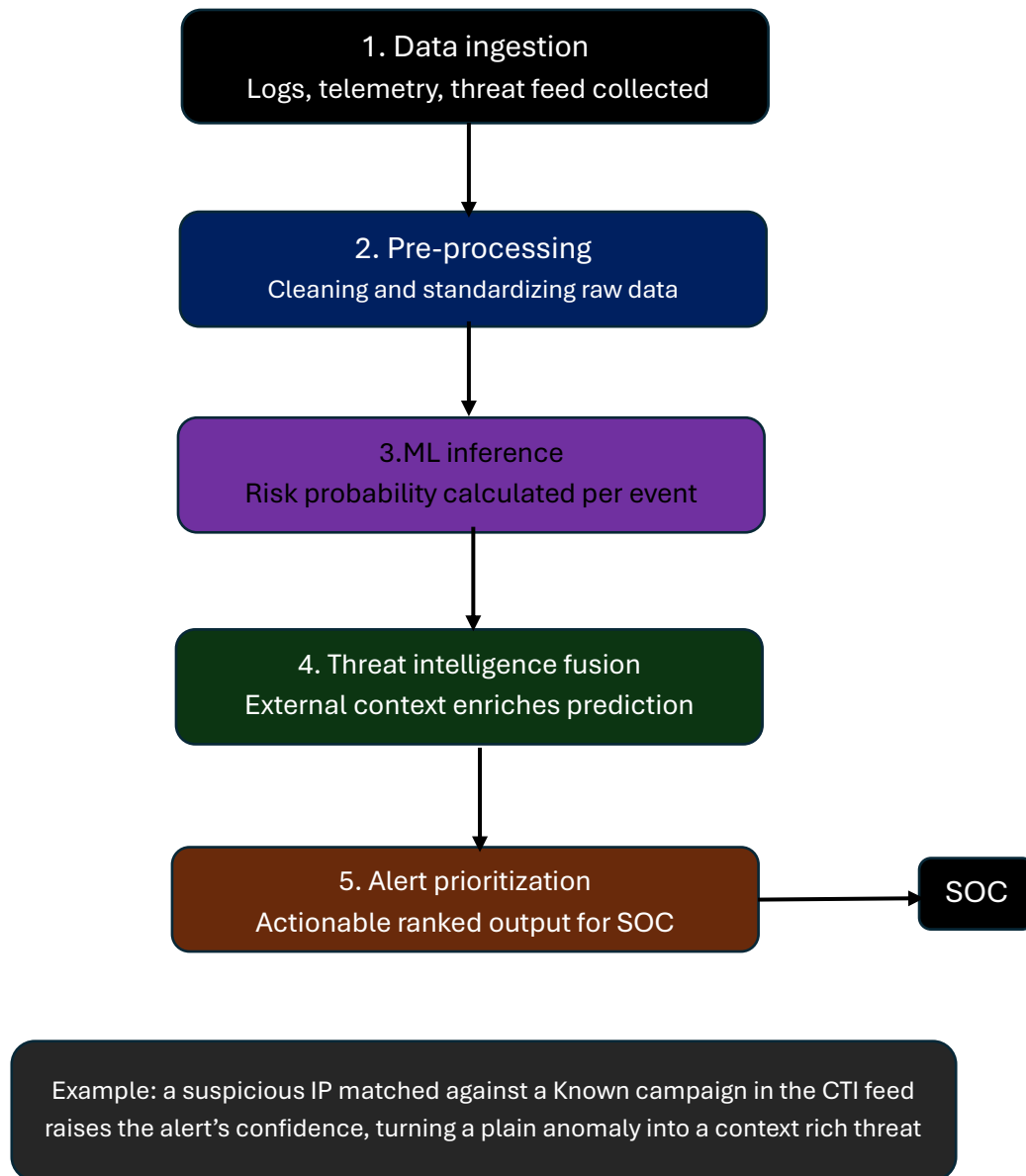


Figure 5: Proposed ML and Threat Intelligence Fusion Framework

8. Expected Outcomes

The results presented in this section are based on the expected outcomes of the proposed framework, derived from the patterns observed across existing literature on machine learning-based threat detection and intelligence-driven cybersecurity, since the framework has not yet been implemented or tested on a live dataset.

Based on the reviewed literature, hybrid systems that combine machine learning with threat intelligence are expected to outperform single-source detection systems (Pradhan et al., 2026). Deep learning models are expected to perform well on complex threats, while SVM and ANN suit semi-structured text such as dark web content.

A second expected outcome is that fusing threat intelligence with machine learning predictions improves early-warning capability. Rather than simply classifying an event as suspicious or benign, the framework is expected to assign it a priority level based on how strongly it correlates with known threat indicators, which should reduce SOC analyst workload and improve response time (Yeboah-Ofori et al., 2021; Ekundayo et al., 2024).

Third, analysts' confidence in system predictions will increase if intelligence-derived features are presented with transparent confidence scores. The fear of using a 'black-box' system is well established in security domains, and significantly worse in high-impact domains where the consequences of error are severe (Vengathattil & Shaffi, 2025).

A fourth expected outcome is a reduction in false positive rates, since anomalies that lack corroborating evidence from threat intelligence sources would automatically receive lower priority scores, allowing analysts to focus their attention on higher-confidence alerts (Yeboah-Ofori et al., 2021b).

Table 3: Summary of the Proposed Framework's Five Layers

Layer	Function	Input	Output
1. Data Ingestion	Collects raw data from internal and external sources	Security logs, endpoint telemetry, threat feeds	Raw structured + semi-structured data
2. Pre-processing	Cleans and standardizes collected data	Raw logs, raw intelligence text	Normalized, deduplicated, tokenized data
3. Machine Learning Inference	Calculates risk probability for each event	Preprocessed structured features	Threat probability score
4. Threat Intelligence Fusion	Adds external context to ML predictions	<i>ML output + CTI indicators (IOCs)</i>	Context-enriched, correlated threat score
5. Alert Prioritization	Ranks alerts by severity and confidence	Fused threat scores	Actionable, prioritized SOC alerts

9. Discussion

The world of cybersecurity is changing rapidly. The truth is that reactive alerting is insufficient. Detection is fine, but the real challenge is now prediction. Traditional

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

reactive tools have become inadequate, along with new zero-day attacks. This motivates the proposed framework because it combines network logs and threat intelligence. The goal is to anticipate threats rather than merely respond to incidents. This represents a complex undertaking, but the current literature supports such a hybrid approach. When combining raw telemetry with human-written reports, the model achieves enhanced detection capability. This enables analysis of attacker behavior and new trends at the same time (Nalluri et al., 2025; Meyer, 2025). But the reality is that threat feeds often contain noise and low-value information. Without proper filtering, the analyst's workload increases significantly. There's also the issue of 'black box' decisions. Prior incidents in critical infrastructure security have shown that when systems are not trusted, analysts disengage from them (Rao, 2022). Until analysts understand why the machine didn't make the prediction, analyst trust is not established. The framework is not without limitations. It still needs to be tested in a real-world SOC environment to validate its effectiveness.

10. Conclusion

Traditional signature-based systems are no longer sufficient. Zero-day exploits and advanced threats change so rapidly that signature-based protections cannot adequately address them, so the combination of ML and threat intelligence is a promising approach. The literature demonstrates that context-aware models turn 'reactive' defenses into 'proactive' ones, and why hybrid systems consistently outperform single-source approaches, according to the literature.

The proposed framework comprises five layers. From ingestion to prioritization, this framework is a practical path for SOC teams; however, challenges, including data fusion and explainability, require further development. Analysts need to be confident. Establishing trust requires transparency in model decision-making, so future empirical validation on real-world datasets will be essential. Implementation constitutes the next phase of this research.

11. Recommendations

First, what is opening up for research is that researchers often rely on benchmark datasets. Real cyber threats are found in live environments, and this study identifies that a significant gap exists in real-time validation. Testing on live traffic is essential for meaningful progress in the future (Bai & Fang, 2024).

The second point is about clarity. Explainability should not be an afterthought. Tools like SHAP and LIME need to be built into the basic design of the model (Rao, 2022). This enables analysts to understand the logic of the machine. Trust must be integrated from the initial design phase.

Adopting these standards is no longer optional, but a requirement. This means that to effectively share and use threat intelligence, adherence is necessary.

SOC analysts should not serve merely as observers; their assessment must be active. Usability and reliability assessments will make the framework practical.

Finally, the system must have a feature of continuous monitoring and automatic retraining to keep up with the pace of attackers. Data drift gradually degrades model

accuracy. It is not enough to deploy the system without ongoing maintenance; the system must adapt to evolving attack patterns over time (Ashfin, 2024).

12. Future Implementation

Currently, this framework remains conceptual. Validation will occur when it is run on live traffic. The first step is to begin data ingestion in a university network or a small lab environment. Datasets like CICIDS2017 are suitable for initial training of ML models, but these are only the prerequisites. The system will then need to be connected to feeds like AlienVault through STIX/TAXII to get real-time alerts (Ofili et al., 2024). Critically, SOC analyst feedback is essential: if analysts cannot interpret alert rationale, the framework fails to meet its objectives. Such failure undermines the entire implementation. Analyst feedback serves as the primary validation mechanism for whether the framework actually works (Hasan et al., 2025).

Table 4: Proposed Future Implementation Roadmap for the Framework

No.	Step	Description
1	Lab Environment Testing	Begin data ingestion in a small lab environment and run on live traffic
2	Model Training	Use a dataset like CICIDS2017 for training ML Models as prerequisites.
3	Real-Time Threat Feed Connection	Connect the system to feeds like AlienVault through STIX/TAXII to get real-time alerts.
4	SOC Analyst Validation	Obtain feedback from SOC analysts, as their understanding of why an alert was raised validates framework effectiveness.

References

- Al Abdulwahid, A. (2025). Ai-driven identification of attack precursors: A machine learning approach to predictive cybersecurity. *Computers, Materials & Continua*, 85(1), 1751-1777.
- Okpala, C. C., & Chukwumuanya, E. O. (2025). The Future of Cybersecurity: Predictive Analytics and Machine Learning Applications. *Journal of Engineering Research and Applied Science*, 14(2), 190-201.
- Sundar, K., Reddy, P., Chaudhary, K. C., & Khan, S. (2025). A Systematic Literature Review on Cyber Threat Detection Using Machine Learning Techniques: Cyber Threat, Algorithms, and Regional Perspectives.
- Dalal, A. (2020). Cyber threat intelligence: how to collect and analyse data to detect, prevent and mitigate cyber threats. *International Journal on Recent and Innovation Trends in Computing and Communication*.

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Zenebe, A. (2022). Cyber threat intelligence discovery using machine learning from the dark web. *Communications of the IIMA*, 20(2).
- Hermawan, M. D. A. (2025). The Use of Artificial Intelligence for Cyber Threat Detection: A Systematic Literature Review of Research Methods, Accuracy, and Gaps. *Journal of Computing and Smart Ecosystems*, 1(2).
- Sahoo, P., & Das, A. INTEGRATED AI FRAMEWORKS FOR ADVANCED CYBERSECURITY AND THREAT INTELLIGENCE.
- Ofil, B. T., Obasuyi, O. T., & Osaruwenese, E. (2024). Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. *Int J Eng Technol Res Manag*, 8(11), 631.
- Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive analytics for cyber threat intelligence in fintech using big data and machine learning. *Int J Res Publ Rev*, 5(11), 1-15.
- Hasan, K., Hossain, F., Amin, A., Sutradhar, Y., Jeny, I. J., & Mahmud, S. (2025). Enhancing proactive cyber defense: A theoretical framework for AI-driven predictive cyber threat intelligence. *Journal of Technologies Information and Communication*, 5(1), 33122.
- Alazab, M., Khurma, R. A., García-Arenas, M., Jatana, V., Baydoun, A., & Damaševičius, R. (2024). Enhanced threat intelligence framework for advanced cybersecurity resilience. *Egyptian Informatics Journal*, 27, 100521.
- Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *Ieee access*, 9, 94318-94337.
- Bai, M., & Fang, X. (2024). Machine learning-based threat intelligence for proactive network security. *Integrated Journal of Science and Technology*, 1(2).
- Nagamalla, V., & Sanapala, R. K. (2023). Integrating Predictive Big Data Analytics with Behavioral Machine Learning Models for Proactive Threat Intelligence in Industrial IoT Cybersecurity. *International Journal of Wireless & Ad Hoc Communication*, 7(2).
- Nalluri, S., Malyala, M. M., Kandagiri, H., & Kandagiri, K. K. (2025, June). Nscti: A hybrid neuro-symbolic framework for ai-driven predictive cyber threat intelligence. In *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)* (pp. 14-21). IEEE.
- Ashfin, U. (2024). Machine Learning Applications in Predictive Cyber Threat Management. *Bulletin of Engineering Science and Technology*, 1(03), 01-19.
- Vengathattil, S., & Shaffi, S. M. (2025). Advanced Network Security Through Predictive Intelligence: Machine Learning Approaches for Proactive Threat Detection—An Experimental Study. *Methodology*, 2(3).
- Shimu, F. (2025). Intelligent Cybersecurity Framework Machine Learning-Driven Data Protection and Threat Intelligence Integration for Modern Digital Communications. *International Journal of Applied Mathematics*, 38(8s), 620-632.
- Umar, H., & Abbas, A. (2022). AI-Powered Threat Intelligence: Enhancing Cybersecurity with Predictive Analytics and Machine Learning.

- Oye, E., Peace, P., & Owen, J. (2024, December). Predictive Analytics for Cyber Threat Intelligence.
- Rao, S. (2022). The Role of Artificial Intelligence in Predicting Cybersecurity Threats: Integrating Machine Learning with Traditional Security Frameworks. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 3(4), 11-18.
- Mishra, S., Albarakati, A., & Sharma, S. K. (2022). Cyber threat intelligence for IoT using machine learning. *Processes*, 10(12), 2673.
- Ghazi, Y., Anwar, Z., Mumtaz, R., Saleem, S., & Tahir, A. (2018, December). A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. In *2018 International Conference on Frontiers of Information Technology (FIT)* (pp. 129-134). IEEE.
- Nazim, F., Aslam, M. F., Aslam, N., Yasin, A., & Fuzail, M. (2025). Machine Learning Approaches for Predictive Cyber Threat Intelligence and Risk Management. *Kashf Journal of Multidisciplinary Research*, 2(04), 95-115.
- Naseer, I. (2023). Machine learning applications in cyber threat intelligence: a comprehensive review. *The Asian Bulletin of Big Data Management*, 3(2), 190-200.
- Meyer, J. L. (2025). Integrative and Predictive Cyber Threat Intelligence: Leveraging Machine Learning, Standardized Frameworks, and Collaborative Defense Mechanisms. *European Index Library of European International Journal of Multidisciplinary Research and Management Studies*, 5(10), 84-89.
- Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, 10(7), 818.
- Kumar, B. (2023). Cyber threat intelligence using AI and machine learning approaches. *Int. J. Bus. Manag. Visuals*, 6(1), 43-49.
- Lima, M., Viana, C., Santos, W. R., Neves, F., Campos, J. R., & Aires, F. (2025). Toward using cyber threat intelligence with machine and deep learning for IoT security: a comprehensive study: M. Lima et al. *The Journal of Supercomputing*, 81(15), 1404.
- Yeboah-Ofori, A., Mouratidis, H., Ismai, U., Islam, S., & Papastergiou, S. (2021, June). Cyber supply chain threat analysis and prediction using machine learning and ontology. In *IFIP International Conference on Artificial Intelligence Applications and Innovations* (pp. 518-530). Cham: Springer International Publishing.
- Bella, L., & Lee, A. (2025). AI-Driven Threat Intelligence and Predictive Cybersecurity: Using Machine Learning to Forecast and Prevent Cyberattacks Before They Occur.
- JS, S. M., Thirunavukkarasu, M., Kumaran, N., & Thamaraiselvi, D. (2024). Deep learning with blockchain-based cybersecurity threat intelligence and a situational awareness system for intrusion alert prediction. *Sustainable Computing: Informatics and Systems*, 42, 100955.

Online ISSN

Print ISSN

3007-3197

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A., & Daneshkhah, A. (2020). Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. In Digital forensic investigation of internet of things (IoT) devices (pp. 47-64). Cham: Springer International Publishing.
- Sarker, I. H. (2024). Introduction to AI-driven cybersecurity and threat intelligence. In AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability (pp. 3-19). Cham: Springer Nature Switzerland.
- Dutta, A., & Kant, S. (2020, December). An overview of the cyber threat intelligence platform and the role of artificial intelligence and machine learning. In International Conference on Information Systems Security (pp. 81-86). Cham: Springer International Publishing.
- Pradhan, R., Satyanarayana, B., Prashanthi, T., Rajesh, M. V., Kulkarni, S., & Singh, T. (2026). Cyber-Physical System Security Using AI-Based Intrusion Detection and Predictive Threat Intelligence Models. *International Journal of Artificial Intelligence and Machine Learning*, 6(3s), 225-236.