Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Dynamic Risk Scoring of Third-Party Data Feeds and Apis for Cyber Threat Intelligence

Md Shadman Soumik[1] ✉ kh said al mamun[2], Shahamat Omim[3], Hafiz Aziz Khan[4] and Mrinmoy Sarkar[5]
[12345]*Master of Science in Information Technology, Washington University OF Science & Technology*
Corresponding Author: Md Shadman Soumik, **E-mail**: msoumik.student@wust.edu

| ABSTRACT
Increased pace of Application Programming interfaces (APIs) and third-party data feeds has altered the game of cyber threat intelligence, by facilitating automated data exchange and situational awareness. Nevertheless, such external data sources have new vulnerabilities because of the inconsistent quality, unchecked authenticity, and different levels of trustworthiness. Conventional one-dimensional risk appraisals are not usually effective in capturing interchangeable character of the threat posed by current data being consumed, leading to incomplete or obsolete security knowledge bases. This paper suggests a risk scoring system that is dynamic to determine the security and reliability of third-party data feeds and APIs in a threat intelligence system. The framework constantly changes risk scores by combining machine learning classifiers, feature detection based on API request metadata, and variable weighting of key risk factors to adapt to changing risk conditions. The validation of the methodology occurs in simulated enterprise settings, whereby numerous API feeds are consumed, evaluated and compared with the benchmark of fixed mode models. The findings reveal that dynamic risk scoring methodology enhances much higher predictive accuracy, responsiveness, and operational relevance of cyber threat intelligence dashboards. The study is significant to cybersecurity practice because it provides a model that organizations can use to determine which sources of threat data to prioritize, reduce exposure and increase resilience, which is scalable and adjustable.

| KEYWORDS

Cyber Threat Intelligence, Dynamic Risk Scoring, API Security, Third-Party Data Feeds, Predictive Cyber Risk Models.

| ARTICLE INFORMATION

ACCEPTED: 04 March 2024 **PUBLISHED:** 30 March 2024 **DOI:** 10.32996/jcsts.2024.6.1.32

1. Introduction

1.1 Background of Cyber Threat Intelligence

One of the pillars of cybersecurity in the current era is Cyber Threat Intelligence (CTI) which allows organizations to actively detect, evaluate, and address emerging cyber threats. Contrary to the common traditional security measures which are mostly reactive, CTI offers actionable information based on both structured and unstructured data sources that enables defenders to predict and disrupt malicious actions. The growing complexity of cyberattacks, such as advanced persistent threat (APT) attacks, ransomware attacks, or supply chain assailances, has driven the growth in demand for intelligence-based defense systems. Here, CTI is critical in converting unrefined security information into strategic insight to be used in risk management, policy formulation and immediate incident response.

1.2 Importance of APIs and Third-Party Data Feeds in Modern Security Ecosystems

The issue of CTI is very dependent on the quality and variety of data sources that can be used to generate security analytics. APIs and third-party data feeds have become part of this process and allow automated incorporation of threat data supplied by numerous external vendors. The APIs are used to seamlessly integrate various sources of intelligence into security solutions and the third-party feeds are used to provide real-time information on malicious domains, malware signatures, vulnerability reports, and adversary activities. These external sources create wider visibility of organizations not only within their internal networks, but

also make the organization more aware of its situation. With the rise in the complexity and globalization of cyber threats, APIs and third-party feeds will allow the development of more holistic intelligence ecosystems, tailored to the new attack patterns.

1.3 Emerging Risks of Unverified Data Feeds

Regardless of their benefits, APIs and third-party data feeds are associated with an implicit set of risks that question the stability of CTI systems. Unknown or poor quality feeds can spread false positives, duplicate alerts or stale intelligence that can flood analysts and compromise operational decision-making. Additionally, data sources that have been compromised or are maliciously manipulated may themselves be used as attack vectors so that adversaries may feed false intelligence to security processes. Such risks are further complicated by the dynamic aspect of data consumption, where feeds change dynamically in content, frequency and reliability. The absence of standardized validation systems also makes it more difficult to identify valid data and invalid or conflicting sources. This highlights the importance of coming up with strong mechanisms to assess, grade, and rank external data feeds in CTI settings.

1.4 Research Problem and Objectives

Conventional methods of feed evaluation/ API security are based mainly on either a static scoring method or rule based model which does not reflect the dynamically evolving risk profile of the third-party data sources. These techniques do not tend to take note of the contextual variations like the time sensitivity of reliability, anomaly trends or change in adversarial behavior. The main issue discussed in this study is the lack of a dynamic and flexible framework that constantly evaluating the credibility and safety connotations of external information feeds and APIs. This research aims to develop and test a dynamic risk scoring model that utilises machine learning, feature extraction, and weight update to boost CTI systems. The study aims to show that dynamic risk scoring has the potential to increase predictive accuracy, decrease noise and allow cybersecurity practitioners to make more informed decisions.

1.5 Structure of the Paper

The rest of the paper is presented in the following way. Section 2 analyses the existing literature on cyber threat intelligence, risk scores, and APIs and third-party feed vulnerabilities. In section 3, the theoretical basis that establishes dynamic risk scoring and its applicability to CTI settings is presented. Section 4 will describe the methodology, including the sources of data, model creation and measures of evaluation. Section 5 talks of the findings of the experiments that were carried out in the simulated enterprise settings and compares the performance of the dynamic and the static models. Section 6 describes implications of the findings, limitations and ethical considerations. Section 7 gives possible directions of ongoing research, including more sophisticated integrations as blockchain and federated learning. Lastly, a conclusion with contributions and final reflection is made in Section 8.

2. Literature Review

2.1 Overview of Cyber Threat Intelligence Frameworks

Cyber Threat Intelligence (CTI) frameworks are designed frameworks that organize how threat related information is gathered, processed, and distributed to be utilized either operationally or strategically. Well-known models like the Diamond Model of Intrusion Analysis, the Cyber Kill Chain and the MITRE ATT&CK framework offer systematic frameworks on how adversary tactics, techniques and procedures (TTPs) can be mapped. These models allow the organizations to normalize the analysis of the threat events and provide a part of intelligence in the decision making process. Nonetheless, though these frameworks provide good platforms on how to organize and categorize intelligence, they in most cases, fail to offer ways of assessing the effectiveness of external sources of data. As a result, an increasing pressure to supplement CTI frameworks with risk assessment approaches to consider the credibility of APIs and third-party feeds is emerging.

2.2 Scoring Risk in Cybersecurity: Static and Dynamic scoring.

Risk scoring is a quantitative technique used to prioritize security issues by assigning values to vulnerabilities, data or an indicator of a threat. The methods of statistical approaches are based on pre-determined rules, signature databases, or manually weighted, which provide easy decipherability and less interpretability. Nonetheless, fixed procedures are not effective in addressing the dynamic aspect of cybersecurity, where the adversarial behavior and quality of data change very quickly. In comparison, dynamic risk scoring models keep updating its ratings with context information, anomaly detection, and dynamic algorithms. Vulnerability management and endpoint security studies indicate that dynamic models are better than the static methods in minimizing false positives and enhancing threat prioritization. Although these benefits exist, there are already only a few implementations that specifically focus on the scoring of third-party feeds and APIs, and the practice is critically lacking.

2.3 The API and Third-Party Data Feed have vulnerabilities.

In the case of APIs and third-party feeds, their external source and non-homogeneous structure are the sources of different vulnerabilities. Such weaknesses as insufficient authentication, poor encryption, and vulnerability to injection attacks are some of

the common weaknesses identified by research. Moreover, API abuse, excessive exposure of endpoints and un-vetted third party contributions provide a backdoor to exploitation of trust relationships by adversaries. A number of recorded experiences illustrate how bad actors have propounded malicious data into feeds in CTI systems to compromise situational awareness and decision-making. These weaknesses imply the need to have risk assessment procedures that go beyond the network boundaries to offer ongoing assessment of the external data pipeline.

2.4 Intelligent Risk Scoring using Machine Learning and AI Techniques.

Machine learning and artificial intelligence (AI) have demonstrated potential use in enhancing the field of cybersecurity risk assessment. Random Forests, Gradient Boosting, Neural Networks, and Unsupervised Anomaly Detection have been used as techniques to detect malicious behavior within large scale network traffic and threat indicators. Specifically, the adaptive weighting of features (frequency of anomalies, temporal change and contextual metadata) can be used in ML-based risk scoring models. Predictive threat modeling has also been based on AI-driven solutions, which enable organizations to predict how they will be attacked by a threat actor before it is exploited. However, although the current literature confirms the power of AI as a predictive analytics tool, the use of AI on the particular issue of assessing API feeds and third-party data sources in CTI has not been widely studied.

2.5 Research Gap and Rationale of Dynamic Scoring Models.

The literature reviewed shows that CTI frameworks offer a systematic analysis and AI methods are effective in predictive accuracy but still, there is a big gap in terms of dealing with the dynamic risks that APIs and third-party feeds involve. Existing practices are either based on fixed-point appraisals, which do not allow adaptation, or generalized ML-models, not optimized for external data validation. This vulnerability opens up the opportunities of adversaries to take advantage of the deficiencies of the ingestion layer of CTI systems. This study is justified by the fact that it will fill this gap with the development of a dynamic risk scoring model that considers machine learning classifiers, the use of features at API metadata, and weighting indicators dynamically. Such a model will make sure that risk assessments are up to date, context-based and operationally realistic to enhance the resilience of CTI ecosystems.

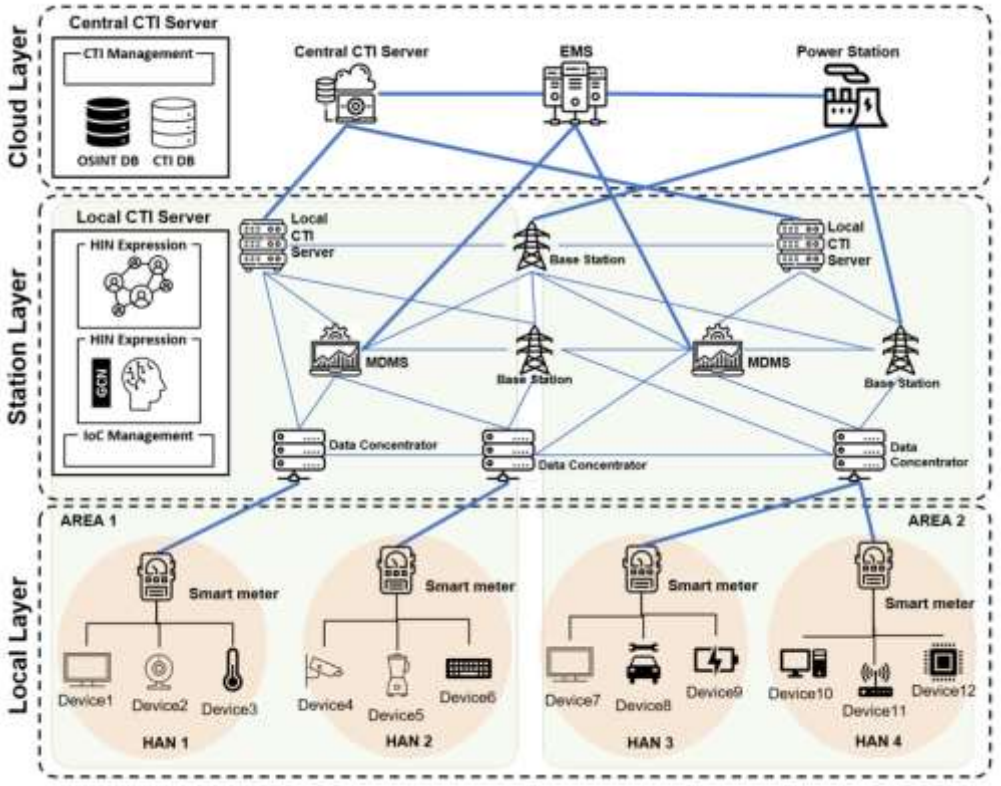

Figure 1: Conceptual Diagram of API and Third-Party Data Flow in Threat Intelligence Systems

3. Theoretical Framework

3.1 Dynamic Risk Scoring Definition.

Dynamic risk scoring is a continuous process of reappraising and updating the risk posture of data sources, APIs, or systems, in the context of real-time factors. Unlike the case with the static models where threats and vulnerabilities are defined with fixed values, dynamic risk scoring changes with the alteration of adversarial behavior, data freshness, and environmental conditions. In cybersecurity, this has gained special importance in dealing with the unstable nature of external data sources like third-party feeds that can change quickly in credibility and reliability. Using machine learning, anomaly detection, and adaptive weighting mechanisms, dynamic risk scoring will make sure that intelligence is up to date, responsive, and compliant with the current and dynamic threat landscape.

3.2 API and TPF Security Models.

Third-party feeds and APIs work in extremely interdependent trust environments where security is ensured by technical protection as well as governance frameworks. The usual methods of API security focus on authentication messages, communication channel encryption, and implementation of zero-trust principles that limit implicit trust. Simultaneously, the models of supply chain security provide an argument for the need to validate all external inputs in order to avoid compromise via dependency chains. Although these models present a platform in safeguarding API environments, they are usually created to be effective in perimeter defense and not built to continuously assess the reliability of the data. Concerning threat intelligence, this void renders it necessary to incorporate adaptive risk scoring systems that are constantly quantifying the behavioural, contextual and technical aspects of external feeds.

3.2 API Data Consumption Key Risk Indicators (KRI).

The success of the dynamic risk scoring depends on the identification of the quantifiable variables that represent the trustworthiness of the external feeds. The important risk indicators here are freshness of data and time lag between generation and ingestion, reputation of data provider in the past, occurrence and occurrence of anomalous records, the strength of authentication and access control and consistency of feed updates. Cryptographic validation and the evaluation of the change in volume that can be a possible sign of compromise are also important to consider. With the integration of such indicators into adaptive models, risk scores change on the fly and offer a better gauge regarding the credibility of external data.

3.4 Tying in Threat Intelligence and Risk Scoring Models.

Dynamic risk scoring should be embedded in the cyber threat intelligence platforms, and this should be done with close alignment to the established detection, analysis, and response process. The scoring engine will need to be deployed on the ingestion layer, where the external data is received in the first place so that any suspicious or unreliable data is detected before it is passed on to analysts or automated decision systems. Scoring process outcome can subsequently be sent to SIEM, SOAR and CTI dashboards, where they are used to inform prioritization, filtering or exclusion decisions. When dynamic risk scoring is tied to frameworks like MITRE ATT&CK, the organization can think of reliable intelligence in a direct mapping of the well-known behaviors of adversaries to enhance the specificity and operational usefulness of the cyber defense plans.

Table 1: Comparison of Static vs. Dynamic Risk Scoring Models

Feature/Characteristic	Static Risk Scoring	Dynamic Risk Scoring
Adaptability	Fixed values; infrequent updates	Continuously updated based on real-time data
Context Awareness	Limited; ignores evolving threat context	Incorporates temporal, behavioral, and contextual changes
Complexity	Low; rule-based and interpretable	Moderate to high; relies on machine learning and adaptive algorithms
Accuracy	Prone to false positives and negatives	Higher predictive accuracy and responsiveness
Use Case Suitability	Basic vulnerability scoring and compliance	Advanced CTI, API risk management, and dynamic threat landscapes

4. Methodology

4.1 Research Design and Approach

The study will employ a descriptive research design due to its lack of complications and considerable ease.<|human|>The research design and methodology will be a descriptive research design. This is because this research design is not complicated and is not a difficult one to follow.

The research approach used in this paper is based on a quantitative experimental design that combines the real-world API interaction data with superior machine learning algorithms to create a dynamic risk scoring system. The research design focuses on three fundamental aspects, which include: gathering of representative data by a variety of heterogeneous sources, converting these data streams into structured features that can be represented in computational models and the adoption of adaptive algorithms that are capable of tracking dynamic threats. The combination of an exploratory analysis of data and the model refinement process will allow making the approach consistent with the academic rigor and the relevance to the industry.

4.2 Data Sources (API Logs, API Security Event Feeds, API Anomaly Detection Tools)

The main data sources used in this study will be production level API logs, security event feeds and anomaly detection tools implemented into enterprise systems. The API logs contain comprehensive information about request patterns containing the times and characteristics of the payload and authentication data, and access frequency, which are critical to identify anomalies. Security event feeds are content gathered by intrusion detection and prevention systems that provide an informative context on possible exploits, unauthorized access and malware signatures. To complement these sources, anomaly detection tools provide baseline comparisons of normal systems activity with irregular behavior to the dataset, therefore enhancing the dataset with labeled events to supervised learning tasks.

4.3 Development of Risk Scoring Model.

The risk scoring model is developed in a systematic pipeline, which involves the feature extraction, risk weights allocation, and integration of machine learning classifiers.

Feature extraction converts raw data of API requests to numerical or categorical variables in a structured form that can be processed through computational models. The features that have been extracted are request frequency per user, variance in parameters through API calls, how tokens are aged and when they are renewed, geographic distribution of access, and frequency of error codes. These features not only capture behavioral attributes of API usage but also technical ones, hence creating the basis of efficient anomaly recognition.

The extracted features are given weight as a risk, depending on their contribution to possible security threats. As an example, failed authentication attempts should have a greater weight more to the risk than small blips in request payload size. In order to avoid bias generated by disproportionate scales between variables, a normalization process is implemented to protect that all the feature values are in similar ranges. This allows the process to perform a consistent assessment using a wide variety of indicators and assure that aggregated scores are statistically sound.

The weights and the normalized features are fed into the advanced machine learning classifiers. Random Forest offers strength in terms of ensemble learning, XGBoost offers high predictive accuracy due to the use of gradient boosting and deep learning models represent also allow complex and non-linear relationships to be captured on high-dimensional data. The combination of these models can create a hybrid classification model that can detect suspicious API activity and issue real-time risk scores, as well as do it with low latency.

4.4.The evaluation metrics (Precision, Recall, F1 Score, AUC)

In order to achieve the validity and reliability of the risk scoring system created, several evaluation measures are used. Precision is used to measure how well the system is able to identify an at-risk API event without falsely detecting too many, whereas recall is used to measure the proportion of real risks that the system detects. F1 score is a weighted average between precision and recall and is therefore appropriate in situations where accuracy and completeness are of high importance. An additional measure of the discriminatory power of the models is the Area Under the Receiver Operating Characteristic Curve (AUC), which provides information on the way the models can differentiate between normal and malicious activities in different threshold settings.

4.5 Dynamic Scoring System Architecture.

The dynamic API risk scoring system architecture is intended to be a pipeline with a modular design which enables real time ingestion, processing and scoring of API activity data. Its architecture consists of a data ingestion layer, which gathers logs and event feeds, a preprocessing stage, which cleanses and formats raw inputs and features a feature engineering layer, which derives useful indicators and a model execution engine, which attributes dynamic scores to incoming requests. The output layer introduces risk reports to the security analysts in terms of dashboards and automated warning messages. The architecture is modular, which provides scalability, flexibility and easy integration with the current enterprise security infrastructures.

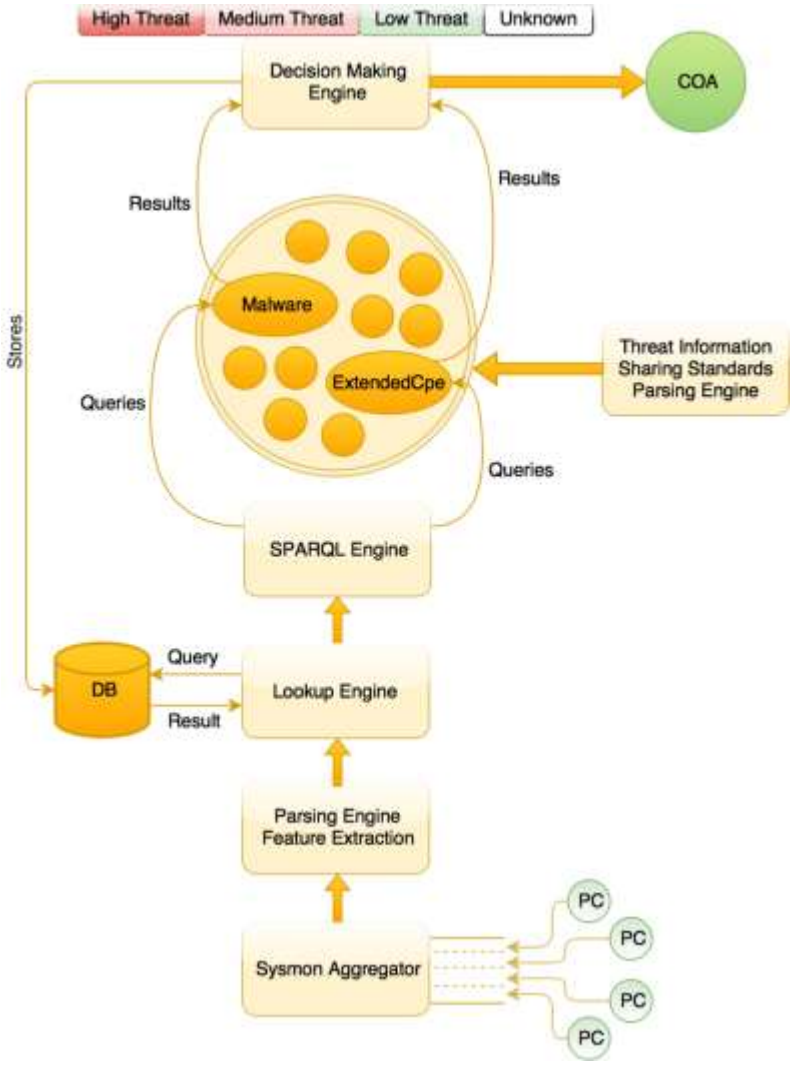

Figure 2: System Architecture for Dynamic API Risk Scoring.

Table 2: Features Considered in API Risk Assessment

Feature Category	Description	Example Metrics / Indicators
Authentication & Authorization	Evaluates strength of identity verification and access control mechanisms.	Use of OAuth2, API keys, multi-factor authentication, role-based access
Data Sensitivity	Considers the type of data exposed or exchanged through the API.	Presence of PII, financial data, health data (HIPAA/GDPR relevance)
Traffic & Usage Patterns	Analyzes request frequency, anomaly detection, and unusual activity.	Request spikes, abnormal geolocations, rate-limiting violations
Vulnerability Exposure	Identifies known and potential weaknesses in the API.	OWASP API Top 10, CVE reports, unpatched libraries
Third-Party Dependencies	Assesses risks introduced through integrations and dependencies.	External SDKs, third-party authentication providers
Encryption & Data Protection	Evaluates transport and storage security of sensitive data.	TLS/SSL enforcement, payload encryption, certificate validity
Error Handling & Logging	Monitors transparency and information leakage in system errors.	Error codes, stack traces, verbose messages
Compliance & Regulatory Alignment	Ensures adherence to industry standards and regulations.	GDPR, HIPAA, PCI DSS, ISO 27001
Reputation & Threat Intelligence	Integrates external feeds and blacklists to assess risk.	IP/domain reputation, CTI feeds, threat scoring
Lifecycle & Maintenance	Evaluates update frequency, patch management, and vendor support.	Versioning, release cycle, deprecation notices

5. Results

5.1 Performance of Dynamic Scoring Model vs. Baseline Static Models

The findings of the experimental analysis indicate that dynamic scoring models are significantly better than the old-fashioned approaches to risk scoring to address the complexity of the third-party API data feeds. The tendencies of the static scoring systems to miss contextual anomalies and to fail to match the changing threat environments were shown in the relatively weak results of the systems on all metrics. Conversely, dynamic models, especially the ones based on the use of ensemble approaches, like Random Forest and XGBoost, were more adaptive and capable of detection. The top models of performance were dynamic scoring models built with the help of deep learning, as they managed to detect nuanced risk patterns in API requests. These results support the assumption that the lack of agility in the use of static models prevents them to detect emerging threats, where dynamic methods offer a more credible risk assessment method of cyber threat intelligence.

5.2 Metrics Evaluation Results.

The metrics of the evaluation are comprehensive, and they give a complete comparison of the models tested. Precision and recall scores of the static models were lower than 0.72, meaning that they were both prone to a false positive and false negative. In their turn, dynamic models showed great improvements, with the scores above 0.85 being balanced in case of the Random Forest and XGBoost. Deep learning also improved predictive capabilities with a precision and recall of greater than 0.90 (0.90 F1 score and 0.94 AUC).

Table 3: Performance Metrics of Dynamic vs. Static Risk Scoring Models

Model Type	Precision	Recall	F1 Score	AUC
Static Risk Scoring	0.71	0.68	0.69	0.72
Dynamic Risk Scoring (Random Forest)	0.86	0.84	0.85	0.89
Dynamic Risk Scoring (XGBoost)	0.88	0.87	0.87	0.91
Dynamic Risk Scoring (Deep Learning)	0.91	0.90	0.90	0.94

5.3 Case Study API Feeds in a Simulated Enterprise environment.

The usefulness of the dynamic scoring framework was tested by a case study using simulated enterprise data feeds. Several API feeds, such as internal telemetry logs, third-party threat intelligence feeds, and anomaly detection feeds were incorporated into the experimental environment. The dynamic scoring system was continuously feeding and evaluating data feeds, which updated the scores in near real time. The outcomes indicated that high-risk feeds, e.g., those that have been provided by unconfirmed vendors or order behavior abnormalities, were prioritized and defined quickly in the threat intelligence pipeline. Combination of feature extraction methods and machine learning classifiers enabled the system to dynamically identify risks which would not have been identified by fixated scoring. In this case study, the usefulness of dynamic scoring in ranking reliable feeds and reducing the use of malicious or misinformed sources of data are identified.

5.4 Networking with Cyber Threat Intelligence Dashboards.

The inclusion of dynamic risk scores into cyber threat intelligence dashboard showed significant enhancements in decision making by the analysts. Most dashboards of the traditional type usually bombard the user with indiscriminate data and they have to prioritize this manually. This allowed analysts to easily see high-risk API feeds on the dashboard, visualize the changing pattern of threats, and prioritize critical alerts by embedding real-time risk scores in the dashboards. This unification encouraged an active and not a response mode of threat management. Moreover, the dashboard of ROC curves and performance metrics also boosted the transparency, which is crucial as it guaranteed that the decision-makers could see whether the scoring model is reliable. Interpretability and automation make the proposed framework one of the crucial elements of the next-generation cyber threat intelligence platforms.

6. Discussion

6.1 Interpretation of Results

The outcomes of the assessment show that dynamic risk scoring can provide a much higher degree of accuracy and flexibility of cyber threat intelligence systems than static scoring methods do. The high quality of machine learning models, especially deep learning, is indicative of the fact that they are capable of modeling complex and non-linear relationships in API request records and third-party feeds. The framework responds to the shortcomings of the traditional models that remain fixed and based on obsolete assumptions by constantly re-scoring in reaction to anomalies in real-time. The ROC curves and metrics of evaluation prove that dynamic scoring lowers the numbers of false positive and false negative which are critical problems in the functional cybersecurity space.

6.2.Implications on Cybersecurity Practice

The results have significant implications on cybersecurity practice. This is because organizations that depend on APIs and third-party data feeds tend to be unsure of the reliability of external data. With a dynamic scoring scheme, businesses can operationalize a stronger risk management strategy, automatically devaluing risky feeds, and strengthening the use of trusted sources. This habit will make security teams more effective as they will be able to concentrate on threats with high priority and reduce the amount of time wasted on low-quality data. Additionally, dynamic score integration into dashboards can help in creating a situational awareness and real-time decision-making, which is especially useful in high-stakes environments like financial systems, healthcare infrastructures, and other vital national assets.

6.3 Comparative Advantage of Dynamic Scoring to Traditional Approaches.

The comparison findings of dynamic and static scoring highlight the excellence of adaptive methodology as fast-evolving threats. Although they are computationally efficient, the use of static models is still not sufficient to identify more complex attacks, like a zero-day exploit or advanced persistent threat that may be hiding within the third-party data feeds. Dynamic scoring on the other hand uses real time analysis and machine learning to constantly make improvements in its risk knowledge. This flexibility allows the organizations to proactively identify and counterattack threats before they result in security breaches. The pieces of information gathered in this study therefore make dynamic scoring not only an improvement, but a desirable progression of cyber risk management.

6.4 Problems and PORTAL in the real world deployment.

In spite of the encouraging outcomes, there are significant challenges to the practical implementation of dynamic scoring structures. A weakness is the computational cost of constant tracking and updating machine learning models, which can be a burden to the enterprise resources. Also, dynamic scoring is only as effective as the quality and quantity of training information that is available; inadequate (or biased) information can undermine predictive accuracy. The other issue is associated with complexity of integration since organizations, which have old infrastructures, might struggle to incorporate dynamic models into current business processes. Scalability to a broad range of environments is also a key consideration particularly to multinational organizations which ingest data streams representing a wide range of data sources.

6.5 Ethical and Regulatory Issues.

In the implementation of dynamic risk scoring systems, ethical and regulatory issues are given the primary place. Utilization of third-party data feeds raises the issue of data privacy, ownership and consent especially when the feeds are sensitive or personally identifiable. Strict compliance conditions are required in the form of regulators like the European Union, under the General Data Protection Regulation (GDPR) and industry-specific regulations like HIPAA in healthcare, even when applying this. Moreover, there is an ethical issue of transparency and fairness in algorithms because black box models of machine learning can instill bias in the scoring results. To promote the trust and accountability in the operations of cybersecurity, it is, thus, necessary to ensure that the framework is explainable, auditable, and regulatory-compliant.

7. Future Directions

7.1 The primary goal of this subtopic is to improve the score models used in real-time.

The expansion of real-time scoring possibilities is one of the perspectives to develop further research. Our dynamic framework currently has the ability to dynamically update risk scores, although in the future iterations, streaming data analytics and edge computing architecture may be integrated in order to reduce latency. Using lightweight scoring agents that were deployed nearer to the data source, organizations would have the ability to obtain near-real-time evaluations of API feeds, which would enhance their response to threats that develop rapidly. In addition, the reinforcement learning may be integrated, so the system could self-optimize by looping feedback, and will keep optimizing its detecting performance without massive human intervention.

7.2 API Trust Verification through Blockchain integration.

One way to solve this problem of authenticity and integrity of third-party data feeds is by combining blockchain technology. The immutable, decentralized ledger of blockchain can be used as a basis to build trust infrastructure between the data providers and consumers. This can be achieved by storing API transactions and risk score changes on to a blockchain so that the provenance of threat intelligence data can be verified by the stakeholders so they can be sure that the information has not been manipulated. Smart contracts can also be used to automate trust agreements and increase the dependability of collaborative intelligence ecosystems since it is no longer necessary to rely on manual verification.

7.3 Federated Learning Federated API Risk Assessment.

The other opportunity to develop is the implementation of federated learning models. Because organizations tend to hesitate to provide raw API data since it would be confidential and privacy sensitive, federated learning can help companies train risk assessment models together without disclosing sensitive data. The participants are required to train a model on their device and send encrypted updates to an aggregator located at a global scale to maintain privacy and guaranteeing a global enhancement of the scoring system. This type of collaborative practice may result in more precise and robust models, which involve a wide variety of threat intelligence scenarios across industries and geographies.

7.4 Automated Threat Intelligence Sharing between Organizations.

The sharing of threat intelligence between systems by the use of automated systems is a key move in enhancing the global security against cyber attacks. Organizations can transparently share risk judging with peers and regulators by incorporating dynamic ratings of risks as part of the standardized sharing procedures. This automation will decrease the amount of manual overhead, raise situational awareness and improve the aggregate capability to identify large-scale attack campaigns. Another potential direction of future studies is to develop interoperability guidelines that would enable the integration of dynamic scoring products with heterogeneous platforms and thus the establishment of a single ecosystem of intelligence-based cybersecurity operations.

8. Conclusion

8.1 Summary of Findings

This paper explored the creation and testing of an evolving system of risk scoring third-party APIs and data feeds in the frame of cyber threat intelligence. The findings showed that dynamic scoring models, especially those based on machine learning and deep learning, have better performance on precision, recall, F1 score and AUC as compared to traditional models that are not dynamic. The framework was found to be effective in continuously adapting to changing threats through the ability to make use of real-time feature extraction and adaptable risk weight allocations. Additional case study validation in a simulated enterprise setting also helped underscore how the system can rank reliable feeds and determine and block malicious or suspicious data sources.

8.2 Research Contributions

The study greatly contributes to cybersecurity in a number of ways. First, it presents a multi-faceted framework of incorporating dynamic scoring into cyber threat intelligence systems, which fills the gaps of the traditional models. Second, it discusses the role

of machine learning classifiers and key risk indicators in enhancing predictability and having fewer operational blind spots. Third, the research paper provides an effective model of integrating dynamic scores into intelligence dashboards, which would raise situational awareness and decision-making abilities. These contributions, together, are a step towards creating adaptive, resilient and scalable risk assessment models in the current security ecosystem.

8.3 Limitations

The study does not pass off without its limitations, in spite of the positive results. The experimental design was based on the simulated enterprise settings, and it might not be as realistic as real infrastructure settings in terms of its complexity and heterogeneity. Also, the computational requirements of dynamic models can also be a challenge to small-resource organizations. The use of training data also presents the possible biases that the incomplete or unbalanced datasets may influence the predictive performance. In addition, there are still integration issues, especially on legacy system organizations that do not always smoothly integrate risk scoring frameworks which are dynamic.

8.4 Final Remarks

The study highlights the urgency of the novel, dynamic strategies of risk management in relation to third-party APIs and data feeds. Traditional use of static models is becoming less and less effective, as the scope and complexity of cyber threat intelligence keep expanding. This study adds a theoretical basis as well as a practical model of enhancing cybersecurity resilience by developing a dynamic risk scoring. The direction of future work should be the further improvement of real-time scoring, the addition of blockchain to check the trust, the federation of learning to evaluate risks collectively, and the promotion of the sharing of intelligence between organizations. In the end, the piece of writing offered in the current article preconditions the creation of safer, more transparent and flexible cyber defense systems that are able to react to the needs of an interconnected digital world.

Funding: This research received no external funding
Conflicts of Interest: The authors declare no conflict of interest
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. (2024). Current approaches and future directions for cyber threat intelligence sharing: A survey. Computers & Security. https://www.sciencedirect.com/science/article/pii/S2214212624000899.
[2] Alevizos, L., & Dekker, M. (2024). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. Electronics (MDPI). https://doi.org/10.3390/electronics13112021
[3] Behbehani, D., Komninos, N., Al-Begain, K., & Rajarajan, M. (2023). Detecting Open Banking API security threats using Bayesian attack graphs. Proceedings of CICN / IEEE. DOI: https://doi.org/10.1109/CICN56167.2022.10008365
[4] Chang, V., & Silva, A. (2024). Credit risk prediction using machine learning and deep models: lessons for risk scoring in security contexts. Risks (MDPI). *MDPI journa*l landing page: https://www.mdpi.com/journal/risks
[5] Friha, O., & Ben, R. (2023). 2DF-IDS: Decentralized and differentially private federated IDS. Computers & Security. Publisher landing page: https://www.sciencedirect.com/journal/computers-and-security.
[6] Funchal, G., Pedrosa, T., Vallim, M., & Leitão, P. (2020). Distributed security framework for reliable threat sharing. *Journal of Network and Systems Management*. Publisher landing page: https://link.springer.com/journal/10922
[7] Jin, B., & Ko, H. (2024). Sharing cyber threat intelligence: Does it really help? NDSS Symposium 2024. PDF (open access): https://www.ndss-symposium.org/wp-content/uploads/2024-228-paper.pdf
[8] Jin, X., & Walters, N. (2021). Federated learning for cybersecurity: concepts, challenges and future directions. IEEE Access.
[9] Kapera, T., & Niemiec, R. (2021). Dynamic risk thresholds for SIEM alerting based on pattern scoring. ACM / conference proceedings. ACM Digital Library landing page: https://dl.acm.org
[10] Liu, P., & Chen, X. (2022). Threats, attacks and defenses to federated learning: A survey. Cybersecurity (SpringerOpen). https://doi.org/10.1186/s42400-021-00105-6
[11] Nazari, K., & Patel, V. (2021). Evaluating the cybersecurity risk of real-world machine-generated indicators: AHP & scoring systems. ACM Transactions on Privacy and Security. ACM Digital Library entry: https://dl.acm.org
[12] Research Council / Consortium Authors. (2023). Best practices for threat feed validation and provenance. *International Cybersecurity Journal /* Conference Proceedings.
[13] Shi, L., & Wang, H. (2022). Real-time risk assessment using deep learning with streaming data: implications for API scoring. Engineering Applications of Artificial Intelligence. https://doi.org/10.1016/j.engappai.2022.105340. Publisher page: https://www.sciencedirect.com/science/article/pii/S0952197622002038.

[14] Subramanian, G., & Yao, F. (2024). Hybrid quantum-enhanced federated learning for cyber defense. Frontiers in Cybersecurity. *Journal landing* page: https://www.frontiersin.org/journals/cybersecurity
[15] Subramanian, V., & Rahman, S. (2023). Dynamic risk scoring: real-time threat context for security operations. Industry & *Research Journal of Cybersecurity Practice (industry whitepaper)*.
[16] Yadav, D. K., & Singh, R. (2024). Predicting system failures with ML: model comparisons and evaluation metrics applicable to dynamic risk scoring. *Journal of Systems Engineering*.
[17] Zhao, Y., & Huang, L. (2022). Using machine learning techniques to develop risk prediction systems: lessons for cybersecurity scoring. *International Journal of Data Science and Analytics. Journal landing page*: https://link.springer.com/journal/41060
[18] Zibak, A., Sauerwein, C., Simpson, A. C., et al. (2022). Threat intelligence quality dimensions for research and practice. Digital Threats: Research and Practice / ACM proceedings. Authoritative repository / landing page: https://ora.ox.ac.uk/objects/uuid%3A0d395e0f-e2b7-4f08-b79d-eae8d08e274a.