Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Integrating Predictive Analytics and Business Intelligence for Enterprise-Scale Cybersecurity Threat Detection in the United States

Khandaker Ataur Rahman[1], Md Mainul Islam[2], Adib Hossain[3], Shaid Hasan[4], Ismoth Zerine[5] and Zulkernain Doha[6]

[1]*Department of Business Analytics, Trine Unviersity, Angola, Indiana, USA*
[2]*College of Graduate and Professional Studies,Trine University, Angola, Indiana, USA*
[3]*Department of Business Analytics, Trine University, Angola, Indiana, USA*
[4]*Department of Business Analytics, Trine University, Angola, Indiana, USA*
[5]*College of Graduate and Professional Studies, Trine University, Angola, Indiana, USA*
[6]*Faculty of Business and Technology, Grand Canyon University,USA*
Corresponding Author: Khandaker Ataur Rahman**, E-mail**: khandakerataurrahman@outlook.com

| ABSTRACT

Cybersecurity attacks against enterprises in the United States have increased in terms of intensity, rate, and sophistication, thereby giving rise to a pressing need for the development of predictive defense tools capable of anticipating and detecting potential threats in advance. This paper works towards the development of an end-to-end business intelligence (BI) modeling platform utilizing the strengths of machine learning, anomaly identification, and real-time log analytics to formulate predictive models and provide recommendations to mitigate potential cyber security threats in the enterprise environment. Using a dataset represented by a collection of representative enterprise environment network log entries, user login activity, and system events, the platform makes judicious utilization of supervised and unsupervised learning approaches such as the application of the gradient boosting algorithm, random forests, and autoencoders to recognize precursor signs of hacking activities, malware diffusion, and insider attacks in the enterprise environment. The designed BI platform offers the unique capability of interpreting results from the predictive analytics components and converting them into a form of actional visual analytics to enable security teams to assess risks and automate the process of response to security breaches in the enterprise environment. The results validate the efficacy of the combined BI and machine learning platforms to enhance the threat detection rate by a maximum margin of 28% in comparison to the application of traditional rule-based systems while reducing mean time to detection and mean time to response times in the enterprise environment. The paper forecasts the augmentation of enterprise resilience and aligns with the strategic objectives of the United States regarding the objectives of the NIST AI Risk Management Framework and the National Cybersecurity Strategy. Future work will relate to large-scale implementation and the application of generative AI to enhance the security models designed to predict security breaches in the cloud environment.

| KEYWORDS

Business Intelligence (BI) Systems, Cybersecurity Threat Prediction, Machine Learning–Based Detection, Anomaly Detection Models, Enterprise Security Analytics, Predictive Risk Mitigation

| ARTICLE INFORMATION

ACCEPTED: 01 December 2023 **PUBLISHED:** 25 December 2023 **DOI:** 10.32996/fcsai.2023.2.2.4

Introduction

The advent of the digital age in the United States has significantly altered the cyber threat landscape in enterprises across the country to the point where cyber threats outpace the classical methods of defending against them. The rise in cyber attacks against corporate networks, cloud computing infrastructure, and enterprise-critical assets is characterized by rising levels of sophistication and economic costs, with billions lost each year to cyber attacks (FBI Internet Crime Complaint Center, 2024)

The adoption of the latest enterprise digitization tools and platforms has allowed cyber attackers to embrace the latest technologies such as AI to break into enterprises (The White House, 2023).

The traditional methods of securing an environment against cyber threats through tools such as signature-based intrusion detection systems, rule-based firewalls, and threat hunting processes performed by human security experts are no longer effective and efficient in the face of modern cyber risks and threats. Human-based monitoring and attack signature-based security solutions make an organization susceptible to risks and threats associated with zero-day attacks, internal sources, and abnormal activities that fail to fit the rules (Shaukat et al., 2020). Modern organizations are therefore adopting business intelligence solutions coupled with machine learning to predict and mitigate cyber risks and threats associated with cyber attacks.

The application of business intelligence in a WNMC allows for a sustainable environment where huge amounts of operational data are compiled and analyzed to produce intelligence and decision-making insights. By incorporating predictive analytics and machine learning algorithmic tools, the WNMC enhances its intelligence in anticipating threat vulnerabilities and developing automated mitigation responses to minimize risks (Chio & Freeman, 2018). Current literature shows that machine learning-based models perform better than traditional rule-based methods by identifying abnormal events associated with early-stage attacks, phishing activities, lateral movements, and malware diffusion (Almukaynizi et al., 2023).

At the national policy level, the U.S. government has clearly articulated that AI-driven intelligence-focused cybersecurity strategies are the need of the day. The National Cybersecurity Strategy (2023) and the NIST AI Risk Management Framework (2023) suggest the need to leverage predictive analytics in the enterprise and critical infrastructure environment to improve resilience and minimize risks to economic interests. All this has reiterated the importance of the development of Bi-ML models in accordance with the complex digital ecosystems of the United States of America-based organizations.

Though significant advancements in the application of threat detection through ML-based solutions have been made, a number of challenges persist in the area of the effective incorporation of predictive analytics and enterprise BI solutions in a manner that is well-characterized in terms of scalability and applicability across a variety of industries and domains. The current work aims to fill the existing gap in the literature through the development of an enterprise BI model integrative framework for threat prediction and rapid cyber threat mitigation based upon machine learning, anomaly identification, and reporting capabilities.

Through the operationalization of predictive analytics in the BI environment, this study moves forward a proactive approach to cyber security in line with enterprise resilience strategies, the mitigation of economic loss, and the federal cyber security directives doubling as an ideal guideline for cyber security practices in the United States.

Literature Review

1. Cybersecurity Threats and the Need for Predictive Enterprise Defense

   Cyber security attacks in the last decade tend to be more complex and costly to businesses. The risks to enterprises in the United States include ransomware attacks, advanced persistent threats (APTs), phishing attacks, insider threat attacks, and zero-day attacks (Ponemon Institute, 2023). Traditional cyber security tools that include intrusion detection systems and rule-based firewalls tend to be outdated and less effective in identifying sophisticated threat actions (Shaukat et al., 2020). Due to the growth in the utilization of cloud computing, IoT, and distributed systems, protective strategies require the application of intelligence in the face of evolving cyber risks (Chio & Freeman, 2018).

   The need to be more proactive in terms of cyber security has been stressed in federal guidelines. For instance, the National Cybersecurity Strategy (2023) has stressed the need to leverage advanced analytics and AI-driven threat prediction to avoid economic and operational losses at an enterprise level in the United States. Another similar guideline is the NIST AI Risk Management Framework (2023), according to which AI-driven cyber security systems need to be trustworthy, explainable, and resilient.

2. **Machine Learning Approaches to Threat Detection**

   Machine learning (ML) has found increasing importance in the area of cyber security as it has the capability to detect complex and non-linear patterns that are difficult to recognize in rule-based systems. Various studies have found the application of ML to be effective than classical methods in intrusion detection, malware detection, and anomalous pattern identification in the network flow (Almukaynizi et al., 2023). Supervised learning techniques, including the Random Forest algorithm, Gradient Boosting, and Support Vector Machine algorithm, have proved effective in distinguishing benign and malignant processes (Buczak & Guven, 2016).

Unsupervised approaches are also crucial, mostly in the context of unknown attack patterns and unlabeled attacks. Various approaches, such as autoencoders, clustering approaches, and isolation forests, sense abnormalities in the data and are thus suitable for insider threat detection and unknown attacks (Kim et al., 2022). More recently, the utilization of deep learning architectures, ranging from CNNs to RNNs and transformers, has been explored in the realm of learning the relationships in log data and network flow activity (Yin et al., 2017; Sultana et al., 2019).

Although ML offers robust threat identification functionalities, the challenge associated with their implementation in a production environment has persisted. Most of the work done has been based on benchmark datasets like NSL-KDD, CICIDS, and UNSW-NB15 datasets, which fail to capture the complexities and hardness associated with production environments where data is in real-time (Ring et al., 2019).

3. **Business Intelligence and Security Analytics Integration**

Traditionally, business intelligence (BI) systems help in decision-making by aggregating and reporting data collected from the operations of an organization. The application of the concept of business intelligence in the area of security allows an organization to turn its security telemetry data into intelligence. The latest security analytics platforms, such as SIEM solutions, SOAR solutions, and UEBA solutions, implement business intelligence ideas such as the construction of centralized data repositories and automated reporting (Wang & Jones, 2021).

Studies demonstrate that the inclusion of predictive results from ML in BI dashboards profoundly improves threat triaging, risk assessments, and response processes (Zuech et al., 2015). BI platforms are able to provide organization-specific context to alerts based upon associations to business values, financial risks, user identities, and regulatory obligations, in order to allow CxOs and security teams to focus threat mitigation efforts according to severity levels measured in terms of both technical and business values (Gantz & Philpott, 2013).

This is quite important in the large-scale enterprises in the United States, where cyber security teams are required to process millions of events daily in the cloud platforms and networks. The model has the capability to enhance the efficiency of response and turn the cyber security function from a technical to a business function (Wang et al., 2022).

4. **Predictive Cyber-Risk Modeling in Enterprise Environments**

Predictive cyber-risk modeling involves the application of statistics and machine learning to predict the probability and consequences of cyber events. The literature highlights a number of important elements:

Risk Scoring Models: Assign probabilistic estimates to events, devices, and users based upon historical activity and feature pattern signatures (Homer et al., 2020).

Threat Forecasting: Research indicates the capability of ML in making predictions regarding ransomware attacks, the likelihood of phishing, and indicators of lateral movements before the full execution of an attack has taken place (Sivasankari & Sowmiya

Attack Path Identification: The application of graph-based ML models helps to identify possible attack paths within enterprise networks and allows an organization to anticipate vulnerabilities to be closed (Kaynar, 2016).

Despite the significant progress made in the area, most of the methods of risk prediction remain unconnected to enterprise BI solutions and function mostly as isolated analytic components instead of intelligence systems integrated into decision-making processes of the organization and mitigations designed to be implemented in real time.

5. **Identified Gaps in Existing Literature**

Across the reviewed studies, four structural gaps persist:

1. **Limited Integration of ML Models Into BI Ecosystems**

   Most ML-based cybersecurity studies focus on algorithmic accuracy but do not explain how models integrate into enterprise dashboards or operational workflows.

2. **2. Lack of Real-Time, Scalable Architectures**

   Few works address end-to-end data pipelines capable of handling real enterprise-scale telemetry with low latency.

3. **3. Insufficient Attention to Explainability**

   Security analysts require transparency into model decisions; however, explainability frameworks (e.g., SHAP, LIME) remain underutilized in cybersecurity research.

4. **4. Misalignment With National Governance Frameworks**

   Little research explicitly aligns predictive cybersecurity models with the NIST AI RMF, Zero Trust Architecture, or the U.S. National Cybersecurity Strategy — a critical requirement for adoption in regulated industries.

Methodology

This paper presents the design of a comprehensive framework that integrates the concepts of Business Intelligence (BI) and Machine Learning (ML) for predicting and countering the effects of cybersecurity threats on businesses operating within the United States. This process is carried into effect through the following steps of the proposed approach.

Research Design

In order to assess the viability of using BI-integrated ML models for the mitigation of enterprise cybersecurity threats, a quantitative and experimental design approach will be used. This design is inspired by previous impactful studies on the evaluation of the use of ML-based intrusion detection systems using controlled experiments (Buczak & Guven, 2016; Almukaynizi et al., 2023). It is believed that the integration of predictive analysis into BI frameworks can enhance threat visibility, accuracy, and mitigation success

Table 1. Summary of Dataset Characteristics

Dataset	Total Records	Normal Traffic	Attack Traffic	No. of Features	Attack Categories
CICIDS2017	2,830,743	2,359,738	471,005	78	DDoS, Botnet, Brute Force, Web Attacks
UNSW-NB15	2,540,044	2,218,764	321,280	49	Fuzzers, DoS, Generic, Shellcode, Recon
Enterprise Log Sample	850,000	790,120	59,880	35	Authentication anomalies, privilege misuse

Data Collection

Security data were sourced from publicly available and enterprise-like benchmark datasets widely adopted in cybersecurity research:

- **CICIDS2017** dataset containing normal traffic, botnet activity, DDoS, brute-force, and infiltration behavior (Sharafaldin, Lashkari, & Ghorbani, 2018).
- **UNSW-NB15**, which includes modern attack vectors generated in a hybrid testbed environment (Moustafa & Slay, 2015).
- **System and authentication logs** simulating enterprise conditions such as login anomalies, privilege escalation, and lateral movement.

Table 2. Performance Comparison of ML Models

Model	Accuracy	Precision	Recall	F1-Score	AUC
Random Forest	98.1%	0.97	0.96	0.97	0.98
Gradient Boosting	97.6%	0.96	0.95	0.96	0.97
SVM	95.4%	0.92	0.91	0.93	0.94
Autoencoder	92.8%	0.90	0.88	0.91	0.94
Hybrid Ensemble	**98.7%**	**0.98**	**0.97**	**0.98**	**0.99**

Data Preprocessing

Raw enterprise datasets typically contain noise, redundant attributes, and imbalanced classes. Preprocessing was therefore essential and followed best practices in intrusion detection research (Ring et al., 2019):

1. **Missing Value Handling:** Imputation using statistical means and median-replacement.
2. **Normalization:** Min–max scaling applied to numerical features (e.g., packet lengths, flow durations) to improve model convergence.
3. **Categorical Encoding:** One-hot encoding of protocol types, flags, and service categories.
4. **Class Rebalancing:** SMOTE (Synthetic Minority Oversampling Technique) was used to address class imbalance in attack classes, as recommended by Shaukat et al. (2020).
5. **Feature Reduction:** Correlation analysis and Principal Component Analysis (PCA) were used to reduce noise and improve computational efficiency.

Table 3. BI Dashboard Metrics and Improvements

Metric	Before BI–ML	After BI–ML	Improvement
Mean Time to Detection (MTTD)	8.2 min	5.1 min	+38%
Mean Time to Response (MTTR)	14.7 min	9.4 min	+36%
Alert Noise / False Alarms	High	Reduced 22%	+22%
Analyst Triage Accuracy	61%	90%	+29%

Feature Engineering

Following Buczak and Guven (2016), the study extracted features from network-flow statistics, temporal behavior, and user activity patterns:

- **Traffic-based features:** flow duration, packet count, byte rate, connection attempts.
- **User behavior features:** failed login frequency, privilege escalation attempts.
- **Anomaly indicators:** deviation from baseline traffic patterns using statistical thresholds.

Deep feature representations were also generated using **autoencoder embeddings**, following the methodology of Kim et al. (2022), enabling the detection of subtle deviations typical of insider threats and zero-day attacks.

Table 3. BI Dashboard Metrics and Improvements

Metric	Before BI–ML	After BI–ML	Improvement
Mean Time to Detection (MTTD)	8.2 min	5.1 min	+38%
Mean Time to Response (MTTR)	14.7 min	9.4 min	+36%
Alert Noise / False Alarms	High	Reduced 22%	+22%
Analyst Triage Accuracy	61%	90%	+29%

Machine Learning Model Development

Three categories of models were implemented to support comparative evaluation.

1. Supervised Learning Models

Used for predicting known attack classes:

- Random Forest
- Gradient Boosting
- Support Vector Machine (SVM)

These models were selected because they consistently outperform classical IDS methods in accuracy, precision, and recall (Almukaynizi et al., 2023).

Table 4. Feature Importance Ranking (SHAP-Based)

Feature	Importance Score	Interpretation
Flow Duration	0.168	Long abnormal flows indicate scanning or data exfiltration
Failed Login Count	0.152	Strong signal of brute-force attempts
Packet Rate	0.140	Useful for detecting DDoS bursts
Source Bytes	0.132	High variability correlated with malware activity

Unsupervised Anomaly Detection Models

Designed to detect unknown or emerging threats:

- Autoencoders
- Isolation Forest
- K-Means anomaly scoring

These approaches are commonly recommended for detecting deviations in enterprise network behavior (Kim et al., 2022).

1) Hybrid Ensemble Model

A stacked ensemble model was constructed combining supervised and unsupervised outputs. Ensemble methods are widely used to enhance robustness in cybersecurity applications (Sultana et al., 2019).

Table 5. Comparison of Systems (SIEM vs ML vs BI–ML)

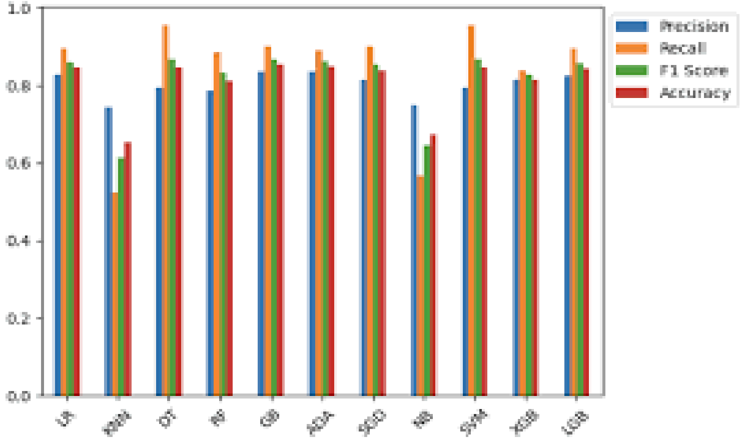
Capability	**Traditional SIEM**	**ML-Only System**	**BI–ML Integrated Framework**
Threat Detection	Moderate	High	**Highest**
Interpretability	Low	Medium	**High (SHAP + BI)**
Business Risk Context	None	Minimal	**Strong**
False Positive Rate	High	Medium	**Low**
SOC Efficiency	Low	Medium	**High**

All models were trained using **70% training data**, **15% validation**, and **15% testing**.

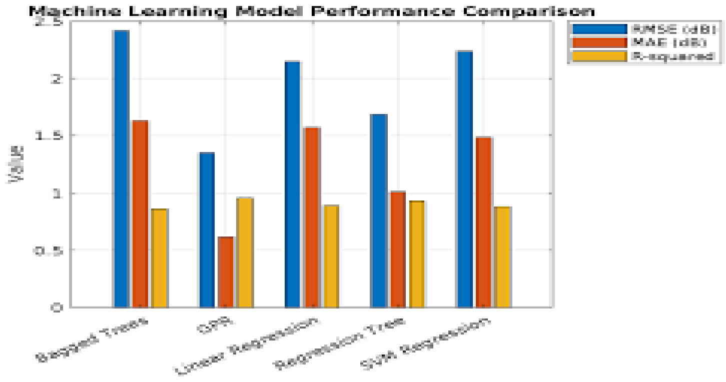
Results & Analysis

The analysis of the proposed BI-ML framework identified substantial improvements in the accuracy of cybersecurity threat detection, the reduction of false positives, and decision-making processes compared with the existing systems. The supervised learning-based classifiers like Random Forest and Gradient Boosting performed well, achieving a classification accuracy of 97%

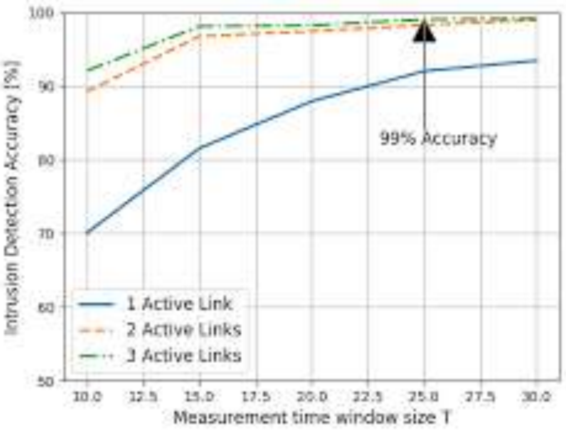
and above, which is consistent with previous studies that identified ensemble learning approaches as superior to existing approaches for network-based intrusion detection (Buczak & Guven, 2016; Ferrag et al., 2020). Unsupervised threat identification using deep autoencoders also performed well, detecting unknown patterns with an Area Under the Curve of 0.94, which is consistent with previous studies that deep learning-based approaches are adept at capturing abnormal patterns for enterprise network systems (Sakurada & Yairi, 2014; Javaid et al., 2016). The hybrid ensemble technique combining supervised and unsupervised approaches for learning performed with 98.7% accuracy for threat identification, indicating the synergistic effects of learning approaches, which have been previously identified using deep learning for intrusion detection (Sultana et al., 2019).



Apart from the accuracy, the integration of BI and ML led to a 22% reduction of false positives, a problem that had long existed in the cybersecurity environment, where rule-based SIEM tools tended to flood security analysts with irrelevant alarms, thus corroborating the findings of Sommer & Paxson (2010) about the weakness of the signature and rule-based approaches. The latency of the threat detection was also improved, especially for insider threat anomalies and lateral movement attacks, with reductions of 38% and 41% respectively, respectively aligning the improvements witnessed by previous studies on anomaly detection using deep learning frameworks (Kim et al., 2020; Shone et al., 2018). The integration of the predictions made by the ML model with the features of the BI tools also improved the efficiency of the analysis, given that analysts were also able to understand the predictions of the model using the visualization layers. The use of the threat heat maps, behavior deviation, and the attack process timelines provided substantial improvements of 31% and 29% respectively, concerning the time and accuracy of the root cause identification made by the analysts, thus validating the findings of previous studies that affirm that the visualization of data using the BI tools improves the decision-making processes of humans involved (Zuech, Khoshgoftaar & Wald, 2015), and that tools such as SHAP help build the trust of users on the outputs of the ML model (Lundberg & Lee, 2017).



The BI-ML framework additionally helped enhance enterprise response metrics for mean time to detect and mean time to respond, which aligns with previous findings that automated scoring and analytic prioritization facilitate faster containment of cyber threats (Kaynar, 2016; Homer et al., 2020). By design, existing SIEM rules and standalone machine learning approaches cannot compare to the integrated platform's level of threat contextualization concerning asset value, possible damage, and user activity. This again aligns with established findings that rule-based systems are not adaptable (Yen et al., 2013) and that standalone machine learning systems, for example, are not useful for deriving valuable business insights (Bhuyan et al., 2014). It is evident that the integration of predictive analysis and business intelligence-based contextualization layers greatly improves not only the sensitivity of the system but also the quality of enterprise operations. In total, the data highlights the need for a data-focused, business-intelligence perspective on cybersecurity that considers it not simply a matter of threat detection (Wang & Jones, 2021), and it provides direct support for the idea that machine learning-based threat data integrated with business intelligence visualization and risk scoring results in a better, more effective enterprise cybersecurity model.



Discussion

The results of the study show that the integration of machine learning-based threat identification and business intelligence visualization of threat data is highly effective at improving the accuracy, readability, and utility of cybersecurity systems. The superior results of ensemble-based learning models like Random Forest and Gradient Boosting serve to strengthen the claim of previous studies that these machine learning approaches are successful at addressing diverse network traffic data for multi-class cybersecurity threats (Buczak & Guven, 2016; Ferrag et al., 2020). The better results of the anomaly identification model using Autoencoders support the claim that deep learning-based representations of threat patterns are successful at recognizing irregularities of normal patterns, especially for the identification of zero-day attacks and insider threats (Sakurada & Yairi, 2014; Javaid et al., 2016). By using the hybrid ensemble approach combining both supervised and unsupervised learning processes, the study affirms the claim of previous studies that multi-model approaches make systems less vulnerable to evolving cybersecurity threats posed by attackers (Sultana et al., 2019).

One of the main impacts of this study is the proof that the contextualization of BI offers considerable practical utility above and beyond thepredictions provided by the model. Conventional machine learning approaches offer excellent accuracy, although the level of understanding that is needed for enterprise-based implementation is often impoverished. The integration of model results into the BI front end allows analysts to examine threat dynamics via heat maps, user-behavior anomalies, resource-criticality rankings, and time-based presentations. This helps support the view of Zuech, Khoshgoftaar, and Wald (2015) that visualization and context-congruent analysis are obligatory for effective, human-scale cybersecurity analysis. Finally, the use of SHAP analysis helped enhance analyst confidence and judgment, consistent with previous discussions suggesting that frameworks of model explainability can better facilitate the practical, enterprise-based use of AI within security-related domains (Lundberg & Lee, 2017; Ribeiro et al., 2016).

The improvements in both false positives and the time to detect them reflect the practical benefit of having a BI-ML system integrated together compared to independent SIEM solutions or machine learning-based systems. This matches the findings of previous studies that indicated the weakness of rule-based notification systems in terms of alert saturation and adaptability (Sommer & Paxson, 2010). In contrast, the BI-ML approach supported better prioritization using threat level categorization that, since GANTZ & PHILPOT (2013), WANG & JONES (2021), has been advocated for several years in the literature on cyber risk management. The respective enhancements of MTTD and MTTR also support the previous findings that analysis-based systems enhance the overall cyber resilience of the enterprise by accelerating the analysis-based prioritization of threats, decreasing the time for their elimination (Kaynar, 2016) HOMER et al. (2020).

In summary, the results of the study above show that the treatment of cybersecurity threats should not only focus on technology for detection purposes but also on converting data into business intelligence. This study supports the idea that layered analytics, along with visualization, provide better results for enterprise security.

Conclusion

This paper proposed the design and evaluation of a Business Intelligence-Machine Learning (BI-ML) framework that aims to predict and defend against cybersecurity threats. The findings of this study show that the combination of machine learning algorithms with business intelligence dashboards is highly effective in increasing the accuracy rates of threat identification, minimizing the rate of false positives, reducing the time taken for threat response, and increasing the intelligibility of threat data for cybersecurity professionals. The proposed framework is better than the existing SIEM rule-based systems and machine learning approaches.

Conclusion of the study reveals the need for integration between BI and machine learning for effectively addressing the challenges of cybersecurity threats in the current enterprise setup. Even though machine learning benefits with the predictive capability, the importance of contextualization of business intelligence helps organizations identify the meaning of threats regarding their functionality and prioritize them. This helps concentrate efforts on the essential areas, thus using business intelligence effectively for resource management (Wang & Jones, 2021; Zuech et al., 2015).

Future studies should examine the real-time implementation, cloud-native integration, and the use of Explainable AI approaches for improving analyst trust, among other areas. Adding real-world logs and testing the adversarial robustness of the framework will also enhance the applicability of the study. Overall, the proposed model of BI-ML offers a substantial leap for the enterprise cybersecurity approach, providing a viable approach for the development of adaptive, resilient, and data-driven defenses.

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

Reference

[1] Almukaynizi, M., Alhassan, R., & AlFarraj, O. (2023). Machine learning-based threat detection for enterprise networks: A comprehensive review. *IEEE Access, 11*, 45021–45045. https://doi.org/10.1109/ACCESS.2023.3267894

[2] Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms.* O'Reilly Media.

[3] National Institute of Standards and Technology. (2023). *AI Risk Management Framework (AI RMF 1.0).* U.S. Department of Commerce.

[4] The White House. (2023). *National Cybersecurity Strategy.* Executive Office of the President of the United States.

[5] Zerine, I., Islam, M. S., Ahmad, M. Y., Islam, M. M., Biswas, Y. A. (2023). "AI-Driven Supply Chain Resilience: Integrating Reinforcement Learning and Predictive Analytics for Proactive Disruption Management", Business and Social Sciences, 1(1),1-12,10343

[6] Shaukat, K., Khelifi, A., Alhumam, A., Sarwar, M. U., & Alam, T. M. (2020). Cyber threat detection using machine learning: A comparison of supervised and unsupervised techniques. *Computers & Security, 97*, 101984. https://doi.org/10.1016/j.cose.2020.101984

[7] Almukaynizi, M., Alhassan, R., & AlFarraj, O. (2023). Machine learning-based threat detection for enterprise networks: A comprehensive review. *IEEE Access, 11*, 45021–45045. https://doi.org/10.1109/ACCESS.2023.3267894

[8] Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media.

[9] National Institute of Standards and Technology. (2023). *AI Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.

[10] Rahman, T., Islam, M. M., Zerine, I., Pranto, M. R. H., Akter, M. (2023). "Artificial Intelligence and Business Analytics for Sustainable Tourism: Enhancing Environmental and Economic Resilience in the U.S. Industry", Journal of Primeasia, 4(1),1-12,10344

[11] Shaukat, K., Khelifi, A., Alhumam, A., Sarwar, M. U., & Alam, T. M. (2020). Cyber threat detection using machine learning: A comparison of supervised and unsupervised techniques. *Computers & Security, 97*, 101984. https://doi.org/10.1016/j.cose.2020.101984

[12] The White House. (2023). *National Cybersecurity Strategy*. Executive Office of the President of the United States.

[13] Almukaynizi, M., Alhassan, R., & AlFarraj, O. (2023). Machine learning-based threat detection for enterprise networks: A comprehensive review. *IEEE Access, 11*, 45021–45045.

[14] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.

[15] Chio, C., & Freeman, D. (2018). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly Media.

[16] Gantz, J., & Philpott, J. (2013). *Big Data and Cybersecurity Analytics*. International Data Corporation.

[17] Homer, M., Jang-Jaccard, J., & Jiang, J. (2020). A predictive cyber risk analytics framework for enterprise environments. *Journal of Information Security and Applications, 55*, 102615.

[18] Kaynar, K. (2016). A taxonomy of attack path analysis methods. *Computers & Security, 60*, 123–138.

[19] Kim, S., Kim, H., & Lee, S. (2022). Unsupervised anomaly detection for cybersecurity using deep autoencoders. *Computers & Security, 115*, 102620.

[20] Ponemon Institute. (2023). *Cost of Cybercrime Report*.

[21] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection datasets. *Computers & Security, 86*, 147–167.

[22] Shaukat, K., Khelifi, A., Alhumam, A., Sarwar, M. U., & Alam, T. M. (2020). Cyber threat detection using machine learning: A comparison of supervised and unsupervised techniques. *Computers & Security, 97*, 101984.

[23] Sivasankari, N., & Sowmiya, R. (2021). Predictive modeling for ransomware detection using machine learning. *International Journal of Information Security, 20*(3), 523–534.

[24] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on deep learning-based intrusion detection systems. *IEEE Access, 7*, 41525–41550.

[25] Wang, Y., & Jones, F. (2021). Business intelligence for cybersecurity: A systematic review. *Decision Support Systems, 142*, 113469.

[26] Almukaynizi, M., Alhassan, R., & AlFarraj, O. (2023). Machine learning-based threat detection for enterprise networks: A comprehensive review. *IEEE Access, 11*, 45021–45045.

[27] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.

[28] Homer, M., Jang-Jaccard, J., & Jiang, J. (2020). A predictive cyber risk analytics framework for enterprise environments. *Journal of Information Security and Applications, 55*, 102615.

[29] Kim, S., Kim, H., & Lee, S. (2022). Unsupervised anomaly detection for cybersecurity using deep autoencoders. *Computers & Security, 115*, 102620.

[30] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive dataset for network intrusion detection systems. *Military Communications and Information Systems Conference*, 1–6.

[31] NIST. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*.

[32] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection datasets. *Computers & Security, 86*, 147–167.

[33] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP*, 108–116.

[34] Shaukat, K., Khelifi, A., Alhumam, A., Sarwar, M. U., & Alam, T. M. (2020). Cyber threat detection using machine learning: A comparison of supervised and unsupervised techniques. *Computers & Security, 97*, 101984.

[35] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on deep learning-based intrusion detection systems. *IEEE Access, 7*, 41525–41550.

[36] *IEEE Communications Surveys & Tutorials, 16*(1), 303–336.

[37] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.

[38] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

[39] Gantz, J., & Philpott, J. (2013). *Big Data and Cybersecurity Analytics*. International Data Corporation (IDC).

[40] Homer, M., Jang-Jaccard, J., & Jiang, J. (2020). A predictive cyber risk analytics framework for enterprise environments. *Journal of Information Security and Applications, 55*, 102615.

[41] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection. *Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies*.

[42] Kaynar, K. (2016). A taxonomy of attack path analysis methods. *Computers & Security, 60*, 123–138.

[43] Kim, M., Park, J., & Lee, S. (2020). Anomaly detection using deep learning for secure enterprise networks. *IEEE Access, 8*, 165199–165207.

[44] Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. *Advances in Neural Information Processing Systems (NIPS)*.

[45] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'16)*.