International Journal of Research and Development in Engineering Sciences
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
International Conference on Emerging Trends in Engineering, Technology and Management 2025
11-12th April 2025 , www.icetm.in , ICETM 2025 , Hybrid Mode
Viswam Engineering College (Autonomous) , Madanapalle , Andhra Pradesh , India
Conference Proceedings , https://doi.org/10.63328/IJRDES-V7C1-ICETM2025
Regular Issue, Vol. 7, ICETM 2025 , Pages: 89 – 93 , ISBN : 978-81-984440-5-9
Received: 14 January 2025 ; *Accepted:* 03 April 2025 ; *Published:* 30 June 2025
https://doi.org/10.63328/IJRDES-V7CIP14
https://www.youtube.com/watch?v=SDUbCIqzEPo
Conference Paper : Original – Applied Research – Qualitative Research Paper

Cyber Threat Intelligence Platform for Real-Time Attack Detection using SIEM

R Obulakonda Reddy [1] , K SREEJA [2] , K Venkata Lokesh[3], G Tarun [4], N Sreevani [5] , Ravindra Lal Weeraratne Koggalage [6]

[1-5] Department of Computer Science and Engineering (Cyber Security), Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
[6] Department of Computer Engineering, General Sir John Kotelawala Defence University, Rathmalana, Sri Lanka ; koggalage@kdu.ac.lk

* *Corresponding Author : R Obulakonda Reddy ; r.obulakondareddy@iare.ac.in*

Abstract: Cybersecurity threats are rising in frequency and sophistication, which calls for the enhancement of better, real-time threat detection systems. This paper introduces a cyber threat intelligence (CTI) platform that combines a deep learning-based detection model with real-time log analysis with the utilization of security information and event management (SIEM) systems. A deep neural network trained with stochastic gradient descent (SGD) is at the heart of the proposed gadget, which uses log data to detect malicious activity. Logs are collected and consumed from the Wazuh platform, permitting real-time correlation and possibility tracking. A tailored dashboard presents a friendly interface for visualizing alerts and designs. The suggested structure mixes detection precision, machine scalability, and functioning responsiveness in changing network environments. Experimental outcomes demonstrate that the model is highly accurate and responsive in determining dangers, structuring its feasibility for real-time business environments.
Keywords: Cyber Threat Intelligence, Deep Neural Network, Real-Time Detection, SIEM, Wazuh.

1. Introduction

Organizations now face a greater attack surface due to rapid advancement of cyber technology, making them susceptible to a wide variety of cyberthreats. Traditional protection solutions such as firewalls and antivirus software are not sufficient enough to strike upon and respond to cutting-edge attacks in real-time. Because of this weakness in defenses, Cyber Threat Intelligence (CTI) systems—which offer practical insights about risk actors and their tactics—have become more and more popular. CTI infrastructures augment safety operations through the assistance of permission for proactive risk detection, danger looking, and incident reaction. But most current CTI solutions either do not feature real-time capabilities or depend heavily on static rule-based exclusive engines, which are ineffective in opposition to zero-day and adaptive threats. To deal with these challenges, this research suggests a hybrid CTI model that takes advantage of device learning—particularly a deep neural network (DNN) educated with the utilization of Stochastic Gradient Descent (SGD) combined with a scalable SIEM (security information and event management) device, Wazuh, to detect danger in real-time. The device proposed can consume logs from any number of endpoints and read them in real-time to encounter anomalies that suggest malicious activity. The DNN variant employs supervised learning in order to categorize incoming log input as benign or malicious, enhancing detection accuracy while minimizing false positives. Further, the integration with Wazuh allows for centralized log administration, rule-based correlation, and warning technology. In order to make the available machine operational and efficient, an internet dashboard is

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, ICETM 2025 , https://doi.org/10.63328/IJRDES-V7CIP14

created that gives safety analysts a tangible interface to present threats, monitor log trends, and create reports. The platform is designed to ensure key threats are detected and resolved in a timely manner, reducing potential loss to the organization.

2. Related Work

Recent developments in cyber threat intelligence (CTI) have revolved around combining artificial intelligence with real-time tracking frameworks to improve risk detection precision and alleviate analyst workload. Ravikiran and Rashmi incorporated an AI-SIEM framework, which combines several deep learning knowledge models, such as CNN, FCNN, and LSTM, for effective cyberattack type, utilizing better event profiling and preprocessing techniques. Additionally, Kaleem described a comprehensive familiarization-integrated SIEM-SOAR framework that uses open-supply equipment in conjunction with Wazuh and ELK to detect and respond to threats in real time at a reasonable cost.

Marinho and Holanda used machine learning and natural language processing (NLP) in the context of open-source intelligence (OSINT) to identify new risks on social media platforms. They integrated their device with the MITRE ATT&CK framework for base profiling. By leveraging models like BERT and Long former to extract IOC from the open web using scalable microservices and cloud-native hardware, Balasubramanian and Nazari's TSTEM platform also improved real-time CTI.

Aminu and Akinsanya developed an adaptive security system integrating real-time analytics with technology such as Apache Kafka and SDN, targeted at enhancing resilience against dynamic threats through proactive hazard-sharing and situational awareness. Even as those methods flaunt strong detection capabilities and extractions of intelligence, the majority rely on sophisticated multi-version structures or external fact resources. In testing, our suggested machine prioritizes lightweight, real-time detection through the employment of a centered deep neural network with SGD, accompanied by Wazuh for efficient and scalable log-based total chance monitoring.

3. Proposed Methodology

The suggested Cyber Threat Intelligence (CTI) system is intended to facilitate real-time danger detection using a lightweight model of deep learning and a scalable SIEM solution. This methodology concentrates on three fundamental pillars: log statistics collection and preprocessing, deep neural network-based threat detection, and SIEM-driven alerting and visualization.

System Overview

The CTI platform's general layout is shown in Fig. 1. From various endpoints, logs are collected and sent to the Wazuh SIEM agent, which carries out log parsing, normalization, and simple rule-based analysis. Those logs additionally are pushed to the personal custom, gaining deep knowledge of the module for real-time classification into benign or malicious classes. Protection analysts can examine chance reviews, receive real-time alerts, and export summaries for further analysis after the labeled consequences are then combined back into the Wazuh dashboard and a specially designed web-based dashboard.

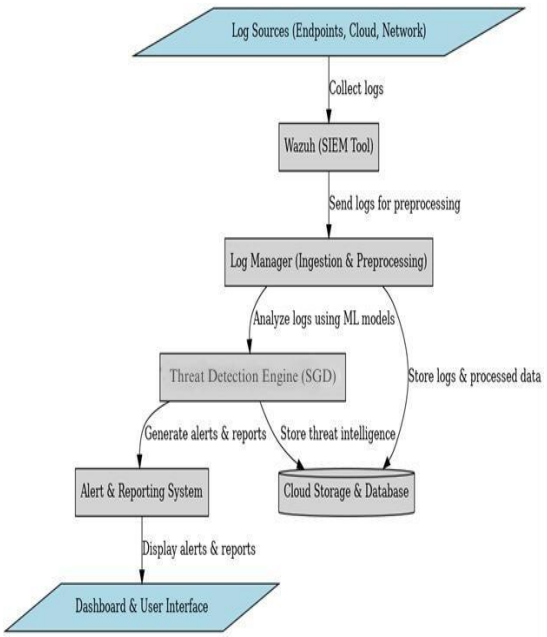

Figure. 1 System Architecture of the Proposed CTI Platform

Data Preprocessing

The raw logs from endpoints are unstructured and quite heterogeneous. Therefore, preprocessing is necessary prior to inputting them to the detection variant. The preprocessing pipeline includes

- Logs parsing to structured key-value formats
- Tokenizing log messages
- Converting text to numerical vectors with one-warm encoding or TF-IDF (depending on characteristic layout)
- Normalization of characteristic values for best-suited model overall performance

During training, every log message is categorized as either benign or malicious based only on incident summaries or known signatures.

Deep Neural Network-Based Threat Detection

A fully connected feedforward deep neural network (DNN) at the core of the detection system was trained using binary

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, ICETM 2025 , https://doi.org/10.63328/IJRDES-V7CIP14

go-entropy as the loss feature and stochastic gradient descent (SGD) as the optimizer.

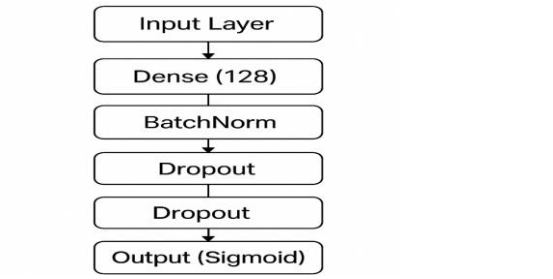

Figure. 2 System Architecture of the Proposed CTI Platform

The architecture consists of more than one dense layer of ReLU activation, batch normalization, and dropout layers for avoiding overfitting. The DNN architecture is depicted in Fig. 2.

Data Preprocessing

The raw logs from endpoints are unstructured and quite heterogeneous. Therefore, preprocessing is necessary prior to inputting them to the detection variant. The preprocessing pipeline includes

- Logs parsing to structured key-value formats
- Tokenizing log messages
- Converting text to numerical vectors with one-warm encoding or TF-IDF (depending on characteristic layout)
- Normalization of characteristic values for best-suited model overall performance

During training, every log message is categorized as either benign or malicious based only on incident summaries or known signatures.

Deep Neural Network-Based Threat Detection

A fully connected feedforward deep neural network (DNN) at the core of the detection system was trained using binary go-entropy as the loss feature and stochastic gradient descent (SGD) as the optimizer. The architecture consists of more than one dense layer of ReLU activation, batch normalization, and dropout layers for avoiding overfitting. The DNN architecture is depicted in Fig. 2.

4. Implementation

The intended Cyber Threat Intelligence (CTI) platform executed the employment of a modular design that combines a deep neural network (DNN) with a security information and event management (SIEM) device. The gadget combat tactics logs from endpoint devices in real-time, categorizes them based on the expert DNN model, and correlates the outcomes through the Wazuh platform.

Model Architecture and Training

The DNN model consists of two hidden layers with ReLU activation, batch normalization, and dropout to prevent you from overfitting. For binary classification, the output layer makes use of a sigmoid activation feature. The model was trained using binary move and stochastic gradient descent (SGD) on a classified data set. An early preventing mechanism was utilized to prevent overfitting. The implementation details of the DNN model are illustrated in Fig. 3, which presents the Keras-generated model summary corresponding to the architecture described in Fig. 2.

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(?)	–
dense (Dense)	(?,128)	256
batch_normalization (BatchNormalization)	(?,128)	512
dropout (Dropout)	(?,128)	0
dense_1 (Dense)	(?,64)	8,256
dropout_1 (Dropout)	(?,64)	0
output (Dense)	(?,1)	65
Total params: 9,089 Trainable params: 8,961 Non-trainable params: 128		

Figure. 3 Keras Model Summary of the Implemented DNN Architecture

Log Ingestion and Preprocessing

Endpoint logs are gathered using the usage of Wazuh retailers and transferred to a centralized log assessment device. Prior to class, the logs are preprocessed and parsed in order to pull in relevant capabilities. This entails tokenization, one-hot encoding, or TF-IDF transformation, as well as normalization. The preprocessed data is passed to the DNN classifier in real-time.

SIEM Integration

Wazuh acts as the SIEM layer, dealing with agent communication, rule-based complete detection, and alert management. The DNN version is included in this pipeline to complement conventional rule-based good judgment with adaptive device studying. When a log is marked by the version as malicious, the effect is shaped and sent back to Wazuh, where it is logged and exhibited together with other alerts. A high-level perspective of such integration is already depicted inside the typical gadget framework (Fig.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, ICETM 2025 , https://doi.org/10.63328/IJRDES-V7CIP14

1).

5. Results

The device proposed can consume logs from any number of endpoints and read them in real-time to encounter anomalies that suggest malicious activity. The DNN variant employs supervised learning in order to categorize incoming log input as benign or malicious, enhancing detection accuracy while minimizing false positives. Further, the integration with Wazuh allows for centralized log administration, rule-based correlation, and warning technology.

Classification Performance

The DNN versions were trained with historical log data and tested on an independent validation set. Four key performance indicators—precision, accuracy, recall, and F1-score—were used to evaluate the performance. These metrics provide insight into the ability of the model to become alert to malicious behaviors while avoiding spurious positives. The confusion matrix, verified in Fig. 4, shows the class outcomes, demonstrating a good balance between true positives and actual negatives with the least misclassifications.

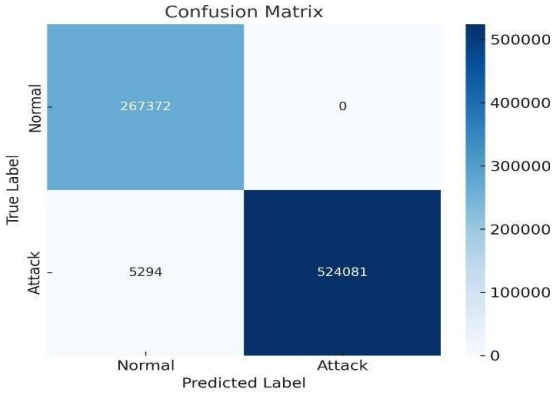

Figure.4 Confusion Matrix for DNN-Based Threat Classification

Table. 1 Displays the comprehensive performance metrics

Metric	Value
Accuracy	99.24%
Precision (Weighted Avg)	99.00%
Recall (Weighted Avg)	99.00%
F1 Score (Weighted Avg)	99.00%

These outcomes show the reliability of the version in identifying anomalies in log streams while maintaining a low false alarm cost—a desirable feature for the prudent deployment in security operations centers (SOCs).

Real-Time System Integration and Output

The CTI platform was converted into a real-time simulation environment that was equally tested. Log data was consumed through Wazuh agents, processed, and tagged by way of the trained DNN model with an ordinary inference latency of significantly lower than 100 milliseconds, consistent with log entry. This low processing overhead confirms the suitability of the model for real-time applications. Classified alerts were sent to the Wazuh SIEM interface and presented in its alert dashboard, as shown in Fig. 5.

Figure.5 Wazuh Dashboard Displaying Alerts Generated by the DNN classifier

Additionally, the custom web-based CTI dashboard provided analysts with real-time prediction summaries and exportable incident reports. The output example is displayed in Fig. 6.

Figure. 6 Generated Threat Report with Classification Results and Metadata

6. Conclusion and Future Work

This paper introduced an in-reality Cyber Threat Intelligence (CTI) platform coupling a deep neural network (DNN) and a lightweight security information and event management (SIEM) structure to support accurate and scalable risk identification. Modern log preprocessing, device learning-based classification, and SIEM correlation are used in the developed system to identify threats with minimal latency and high reliability. The DNN model performed excellently on all the metrics of evaluation, including high precision and recall, which could be important in reducing false positives and overlooked detections. The integration of the device with Wazuh allows end-to-end automation from log gathering and classification to alert technology and visualization to enable timely and informed incident response. The real-time simulation confirmed that the device is ready for operational use in situations where timely risk detection and analyst support are crucial. The bespoke dashboard also improves usability by providing a centralized interface for monitoring, report creation, and risk assessment.

In subsequent versions, the platform

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, ICETM 2025 , https://doi.org/10.63328/IJRDES-V7CIP14

could be better in a number of instructions to enhance its ability to learn, accuracy, and scalability. One area of focus is integrating ongoing learning mechanisms to enable the DNN model to dynamically adjust to changing risk styles without needing to be fully retrained. Scaling the state-of-the-art binary type technique to a multiclass structure would allow the machine to differentiate between particular classes of assault, in addition to malware, reconnaissance, or brute-force attacks.

Also, incorporating explainability techniques—in addition to SHAP or LIME—could help improve transparency and analyst concurrence by providing insight into the model's decision-making process. Integration with real-time chance intelligence feeds and conformity with models such as MITRE ATT&CK could further increase detections' contextual pertinence. Finally, containerizing the platform using Docker and running it using Kubernetes may help scalable deployment to cloud-based or enterprise-grade environments.

References

[1]. J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," IEEE, 2019.

[2]. K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," IEEE, 2020.

[3]. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: A comprehensive review of AI-driven detection techniques," Journal of Big Data, vol. 11, art. no. 105, 2024.

[4]. R. Marinho and R. Holanda, "Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing," IEEE, 2023.

[5]. N. Katiyar, S. Tripathi, P. Kumar, and S. Verma, "AI and Cyber-Security: Enhancing Threat Detection and Response with Machine Learning," *Educational Administration Theory and Practice Journal*, vol. 30, no. 4, Apr. 2024.

[6]. S. Garg, R. Singh, and A. Gupta, "Machine Learning for Cyber Threat Intelligence: A Survey of Techniques and Applications," ACM Transactions on Cybersecurity, vol. 15, no. 3, 2023.

[7]. H. Kwon, M. Lee, and J. Choi, "Deep Learning-Based Intrusion Detection Systems: A Comparative Study," IEEE Security & Privacy, vol. 20, no. 5, 2024.

[8]. Y. Zhang, T. Zhang, and L. Wang, "Real-Time Network Traffic Anomaly Detection Using Hybrid AI Models," Journal of Network Security, vol. 32, no. 1, 2023.

[9]. P. Bose, R. Das, and N. Mukherjee, "AI-Powered SIEM Systems: Enhancing Automated Threat Detection and Response," Elsevier Cybersecurity Review, 2024.

[10]. J. Patel and S. Verma, "Adaptive Cybersecurity Frameworks: Integrating AI with Traditional Security Measures," IEEE Transactions on Cybersecurity, vol. 18, no. 4, 2023.