



AI-Driven Cyber Threat Intelligence Platform for Proactive Threat Detection and Prediction

¹Sahithi Panda, ²Teki Aditya Raj, ³Sonabha Manisha, ⁴R Chaitanya Kumar

Department of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India

Abstract : In the evolving cybersecurity landscape, traditional threat intelligence platforms often rely on passive data collection from known sources, which delays the detection of emerging threats. Our AI-Powered Cyber Threat Intelligence Platform enhances existing technologies by integrating advanced machine learning models, data collection from unconventional sources, and predictive analytics. A unique feature of our approach is predictive threat analytics using time-series models such as ARIMA and LSTM which forecast potential threats based on historical attack patterns. This allows organizations to anticipate future risks, providing valuable time for mitigation strategies. The platform also implements AI-driven prioritization and risk scoring, automatically ranking threats based on their potential impact on the organization. The interactive dashboard visualizes these threats in real time, offering an intuitive representation of attack patterns and suggested mitigations. By combining AI-driven analysis, and predictive capabilities, our platform offers a proactive, scalable, and precise cybersecurity solution that surpasses traditional threat intelligence platforms.

IndexTerms - Attack Pattern Analysis, Cyber Threat Intelligence, Incident Monitoring, Real-Time Threat Visualisation, Risk Scoring, Security Operations Center(SOC), SIEM Dashboard, Time-Series Forecasting, Threat Prediction.

I. INTRODUCTION

As our reliance on the internet grows, so do cyberthreats and cybercrimes. As cyber dangers have increased, cybersecurity has changed to use cutting-edge technologies and expert-driven procedures to combat cybercrimes. Traditional detection methods are ineffective against sophisticated and zero-day attacks because cyber criminals are constantly refining their methods to circumvent security measures. Traditional security methods have limitations, including weak system configurations and unqualified users, making them less effective. The future of cybersecurity lies in automation, where AI-driven systems can adapt and learn to detect emerging and sophisticated cyberattacks [1].

The ability to predict, detect, and respond to emerging threats in real-time is critical for modern cybersecurity frameworks. Here, Artificial Intelligence (AI) has become an essential element in cyber threat intelligence by facilitating the automated identification and response to cyber threats. In Contrast to traditional approaches that depend on set rules, AI-based systems can examine large-scale data patterns, detect anomalies, and adapt to new attack strategies without the need for human assistance [2]. Integrating AI into cyber threat intelligence allows for proactive threat hunting, reducing the reliance on reactive security measures. AI-powered systems can correlate threat data across multiple sources, generate real-time alerts, and improve the efficiency of security operations centers (SOCs) [2]. As threat detection plays its role in the rapidly evolving cybersecurity landscape, traditional reactive defense mechanisms often fail to address sophisticated and emerging threats. Threat prediction is crucial as it enables organizations to anticipate cyber-attacks before they occur, shifting from a reactive to a proactive security posture. By leveraging predictive analytics, machine learning, and historical attack data, cybersecurity systems can identify vulnerabilities, forecast potential threats, and implement preventive measures. This not only reduces response time and minimizes damage but also enhances overall network resilience. Predictive threat intelligence allows security teams to allocate resources effectively, prioritize risks, and mitigate attacks before they cause significant harm, ultimately strengthening an organization's cybersecurity framework [3].

Time-series models play a crucial role in cyber threat prediction by analyzing historical attack patterns, identifying trends, and forecasting future security threats. Evolving through various methodologies, it's clear that there exist models that are exemplary for Time-Series Analysis in Machine Learning, as well as Deep Learning approaches. The proposed methodology in this project revolves around the ARIMA and LSTM models, which is highly competent for forecasting. By leveraging this model, researchers can improve accuracy and reduce uncertainties in predictive analytics [4].

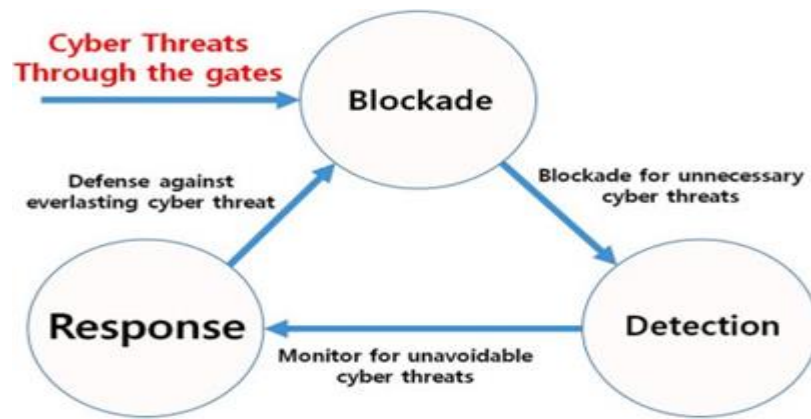


Fig. 1. The three elements of cybersecurity

The fast pace of ever-increasing cyber-attacks requires threat detection to increase at par, bringing in real-time threat intelligence and adaptive defense mechanisms that help combat such spiraling threats. Real-time threat intelligence involves continuous data collection, normalization, and analysis across various sources to rapidly identify and respond to threats. Organizations leveraging real-time threat intelligence can track new attack vectors, malware behavior, and vulnerabilities in real-time, enabling proactive defenses against emerging cyber threats.[5]. Integrating real-time threat intelligence significantly reduces the time needed to detect and respond to threats. Traditional security measures rely on static rules, causing delays in identifying emerging risks, whereas real-time intelligence enables instant detection and response. Standardization of the security operations dashboard is essential for the efficient operation of a security operations center (SOC).

It must comprehensively express the business activities of the SOC and allow security analysts to quickly identify and respond to cyber threats. An SOC dashboard should provide real-time visibility into security events, automate threat detection processes, and enhance operational efficiency by integrating data from multiple security tools such as SIEM, IDS, and IPS [6].

For effective security operations and intrusion response activities, it is necessary to detect cyberattack attempts in real time. A Security Information and Event Management (SIEM) dashboard is a critical tool for cyber threat intelligence (CTI) as it provides real-time monitoring, correlation, and analysis of security events across an organization's network. It helps cybersecurity teams detect, investigate, and respond to potential threats efficiently. The SIEM dashboard helps security teams visualize critical security alerts and prioritize response actions based on severity.

II. LITERATURE REVIEW

Artificial intelligence (AI) has become a critical tool in cyber threat detection, intelligence gathering, and predictive security measures. Sun et al. [10] highlighted the role of cyber threat intelligence (CTI) mining in proactive cybersecurity defense, emphasizing the need for advanced data mining and natural language processing (NLP) to extract actionable insights from large-scale threat intelligence sources.

Uppalapati [2] explored the integration of machine learning (ML) models for real-time cyber threat analysis, focusing on classification techniques that enable automated threat detection and response mechanisms.

Singh and Jha [11] proposed a machine learning framework leveraging Naïve Bayes and Support Vector Machines (SVM) to enhance malware detection and intrusion classification, demonstrating improved threat identification accuracy.

Lim et al. [12] extended this approach by applying deep learning architectures, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, to cyber threat anomaly detection, showcasing how these models can improve real-time security monitoring.

Furthermore, Dwivedi et al. [4] introduced a time-series forecasting approach using S-ARIMA, CNN, and LSTM, designed to predict future cyber threats, enabling organizations to implement proactive mitigation strategies. Collectively, these studies establish a foundation for AI-driven cybersecurity methodologies, underscoring the importance of integrating real-time detection with predictive analytics to strengthen cybersecurity resilience and defense strategies.

III. METHODOLOGY

3.1 Background Study

The evolution of cybersecurity threats has driven the adoption of advanced technologies, such as Artificial Intelligence (AI), to enhance threat detection and mitigation. The growing complexity of cyber-attacks, including Advanced Persistent Threats (APTs), polymorphic malware, and adversarial exploits, has highlighted the limitations of traditional security measures. For instance, Wang et al. [7] demonstrated the effectiveness of an AI-driven network threat detection system that leverages deep learning models to enhance IoT security. This approach underscores the increasing importance of AI in analyzing vast datasets and identifying potential threats in real-time.

The study "Real-Time Detection and Tracking Using Multiple AI Models and Techniques in Cybersecurity" [8] explores the integration of machine learning, deep learning, and anomaly detection algorithms to enhance cybersecurity defenses. The research demonstrates that combining multiple AI models improves the accuracy and speed of cyber threat detection, allowing for real-time tracking of malicious activities. By leveraging AI-driven threat intelligence, the system adapts dynamically to evolving attack patterns, enabling rapid mitigation of cyber threats. The findings highlight the synergies between AI models, which collectively enhance detection capabilities, reduce false positives, and strengthen cybersecurity frameworks. Additionally, the study emphasizes the importance of ethical AI implementation, ensuring transparency and fairness in automated cybersecurity decisions. The results suggest that integrating AI-based threat detection into security operations centers (SOCs) can significantly enhance real-time incident response and resilience against cyber threats.

3.2 Pre-processing

Hernandez-Suarez et al. [8] state that acquiring real-world malware and DoS attack datasets is a challenging and time-consuming process due to privacy concerns, legal restrictions, and the high cost of maintaining controlled environments. Many publicly available datasets suffer from data imbalance, lack diversity, and may not reflect modern cyber threats. The study explains that existing malware datasets often contain outdated or misclassified samples, making them ineffective for training accurate models. The use of fake data generators in cybersecurity is essential due to the difficulty of acquiring real-time threat intelligence datasets while ensuring privacy and security compliance.

In this project, a synthetic SOC Data Generator is implemented to generate randomized security event logs, network traffic patterns, and attack simulations using the Faker library instead of relying on real-time data. This SOC Data Generator is implemented as a dedicated class within the system, enabling the controlled creation of realistic-looking threat data. The generated data includes threat types, severity levels, attack vectors, geographic coordinates, timestamps, IP addresses, confidence scores, and status information, ensuring diverse cybersecurity scenarios for analysis.

The pre-processing pipeline ensures that the synthetically generated data is properly formatted, structured, and normalized before being analyzed and visualized in the SOC Dashboard. This approach enables the demonstration of threat detection, prediction, and mitigation capabilities while eliminating dependencies on restricted real-time threat feeds, making the system adaptable for cybersecurity simulation and testing.

3.3 Experimental Framework and Setup

This experimental approach leverages a SIEM dashboard integrated with machine learning-based threat detection and prediction models to enhance real-time monitoring, anomaly detection, and predictive analytics. The SIEM dashboard serves as a centralized interface, visualizing threat intelligence, risk assessment, and system alerts while integrating synthetic data generation for model testing and improvement.

The SIEM dashboard is designed as a multi-layered, real-time threat intelligence system that integrates various data processing and machine learning components. The Frontend Layer consists of an interactive UI built with Dash/Plotly, allowing security analysts to visualize threats, generate reports, and configure system settings. The Backend Layer processes requests via a Flask API server, which handles report generation, data caching (30-sec refresh window), and WebSocket/SSE for real-time updates. The Processing Layer ensures efficient threat data transformation by integrating synthetic data generation, real-time data processing, feature extraction, and time-series forecasting (ARIMA/LSTM). This modular setup enables the seamless flow of data between system components, ensuring low latency and high accuracy in threat detection. The SIEM dashboard functions by continuously collecting, analyzing, and displaying cyber threat intelligence in real time. HTTP/WebSocket requests trigger the retrieval of historical threat data, time-series predictions, and anomaly detections from the Data Layer, which stores threat history, model weights, and system logs.

The Processing Layer extracts key features and applies time-series forecasting models like ARIMA and LSTM to predict upcoming threats. The SIEM Dashboard leverages Dash and Plotly to provide interactive visualizations of security data, enabling real-time monitoring and analysis of cybersecurity threats. By utilizing Pandas for data processing and ReportLab for report generation, the platform offers comprehensive insights and documentation for security operations. Flask serves as the backend framework, managing data flow and user interactions, while the Datetime library handles time-sensitive data, supporting the platform's real-time capabilities.

The Risk Scorer (Ensemble Model) assigns severity scores, which are fed back for model retraining to enhance detection accuracy. The processed results are stored in databases and displayed on the SIEM dashboard, providing security teams with real-time insights, alerts, and automated report generation for proactive cyber defense.

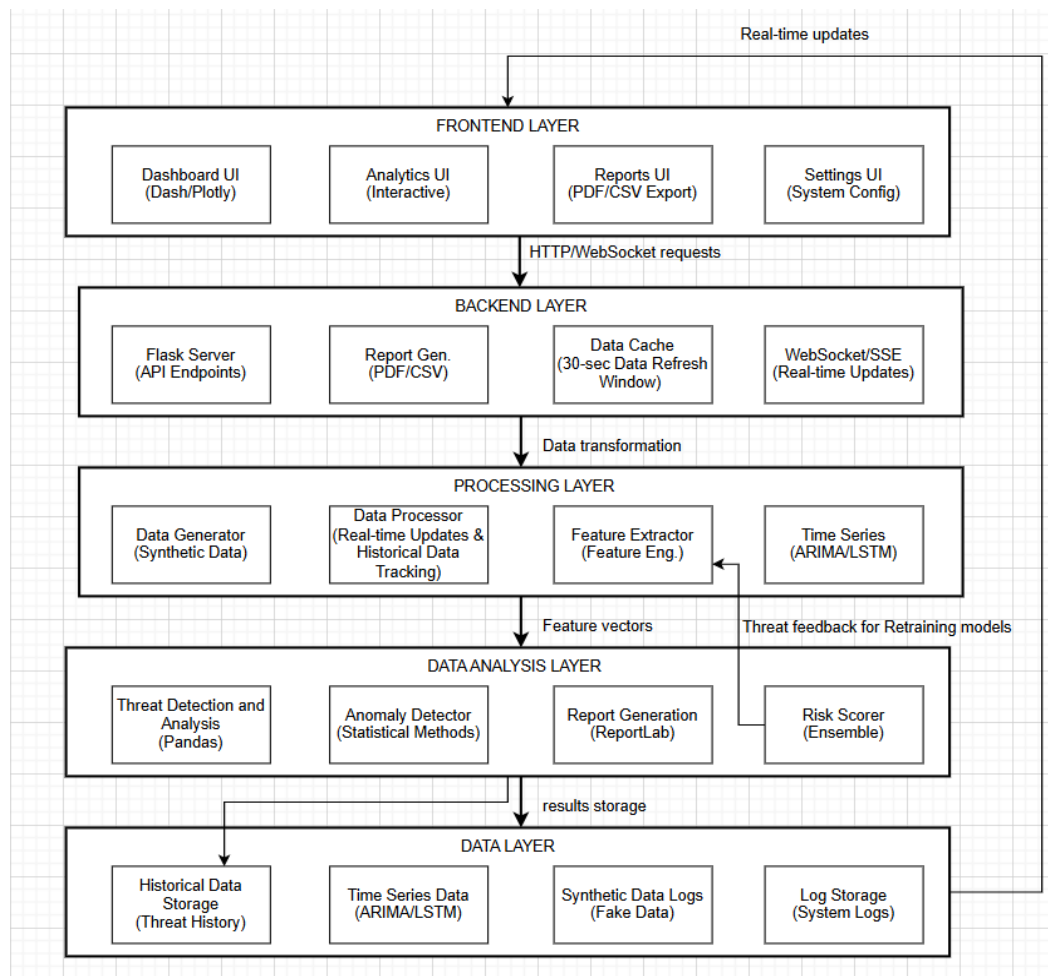


Fig. 2. SOC Dashboard Architecture

3.4 Technology Stack Implementation in SIEM Dashboard

3.4.1 Dash Framework(Interactive Dashboard)

Dash is used in the project to develop an interactive and web-based SOC dashboard that enables real-time monitoring of cybersecurity threats. It provides a frontend interface for security analysts to visualize and interact with threat intelligence data. Dash allows for seamless integration with Flask APIs to fetch real-time updates, ensuring a responsive and continuously updating dashboard. The layout management and callback functions in Dash enable dynamic updates without requiring full-page reloads, allowing users to filter threats, adjust parameters, and interact with live security data efficiently.

3.4.2 Plotly (Data Visualization & Threat Analysis)

Plotly is utilized to generate interactive visualizations that enhance the analysis of threat data. It supports a wide range of charts and graphs, including line charts for threat trends, bar charts for severity analysis, scatter plots for anomaly detection, and geographic maps for attack origin visualization. The SIEM dashboard employs real-time updates to refresh Plotly visualizations every 30 seconds, providing security analysts with up-to-date insights on cyber threats. Additionally, hover tooltips, zooming, and filtering capabilities in Plotly enable in-depth exploration of security incidents and attack patterns. This integration of Dash and Plotly ensures an engaging, interactive, and real-time monitoring system for cybersecurity threat detection and analysis.

3.4.3 Pandas (Data Analysis)

Pandas, a powerful data manipulation library, is utilized extensively in the SIEM Dashboard for data analysis and processing. The platform uses Pandas to handle synthetic threat data generated by the SOCDataGenerator class (the class which generates the random fake data using faker library), performing operations such as data cleaning, aggregation, and statistical analysis. Pandas DataFrames provide a flexible and efficient way to manage and analyze large datasets, enabling the platform to identify patterns, detect anomalies, and calculate risk scores. The use of Pandas ensures that the dashboard can efficiently process and analyze threat data, providing valuable insights to security analysts.

3.4.4 ReportLab (Report Generation)

The SIEM Dashboard employs ReportLab, a library for generating PDF documents, to create downloadable reports for SOC analysts. The platform uses ReportLab to format and export threat data, including threat types, severity levels, and mitigation recommendations, into professional-quality PDF reports. These reports are designed to be easily shared and reviewed, providing actionable insights and documentation for security operations. The integration of ReportLab into the dashboard ensures that users can generate comprehensive reports that support decision-making and incident response. These downloadable PDF reports ensure that security analysts can efficiently review, share, and archive actionable cybersecurity insights. By automating report generation, the platform enhances incident response workflows, enabling seamless integration of security findings into organizational risk management.

3.4.5 Flask (Backend Logic)

Flask, a lightweight Python web framework, serves as the backbone of the SIEM Dashboard's backend logic. The platform uses Flask to handle HTTP requests, manage data processing, and serve the Dash application. Flask's simplicity and flexibility make it an ideal choice for building scalable web applications, allowing the SIEM Dashboard to efficiently manage data flow and user interactions. The framework's integration with Dash ensures seamless communication between the frontend and backend, enabling real-time updates and data visualization.

3.4.6 Datetime Library (Time Management)

The Datetime library is used in the SIEM Dashboard to manage and manipulate time-related data. The platform utilizes Datetime to generate timestamps for synthetic threat data, calculate time intervals for data caching, and manage time-based features in visualizations and reports. The library's robust functionality allows the dashboard to accurately track and display temporal patterns in threat data, providing users with insights into the timing and frequency of cybersecurity incidents. The use of Datetime ensures that the platform can effectively handle time-sensitive data, supporting real-time monitoring and analysis. These libraries and frameworks collectively enable the SIEM Dashboard to deliver a comprehensive and interactive cybersecurity solution, providing users with the tools they need to monitor, analyze, and respond to threats effectively.

3.5 Hybrid AI Models

3.5.1 ARIMA-LSTM Hybrid Model (Threat Prediction)

The SIEM Dashboard integrates a hybrid AI model combining ARIMA (Autoregressive Integrated Moving Average) and LSTM (Long Short-Term Memory) for enhanced cyber threat prediction. This approach leverages ARIMA's strength in capturing linear trends and seasonality, while LSTM learns complex non-linear patterns and long-term dependencies in security data. By combining these two techniques, the system provides a more accurate and adaptive threat forecasting mechanism, allowing security teams to anticipate cyber threats before they materialize.

The hybrid model processes historical threat data and applies both statistical forecasting and deep learning techniques to detect patterns and anomalies. It combines the predictive outputs using a weighted ensemble method, where ARIMA contributes 60% and LSTM 40% to the final forecast. The system also integrates trend factors, seasonal adjustments, and confidence intervals to refine predictions. This predictive capability enables proactive security measures, allowing SOC analysts to prepare mitigation strategies 48 hours in advance. By capturing both linear and non-linear threat behaviors, the hybrid model enhances the overall resilience of cybersecurity operations, providing a robust and intelligent approach to threat anticipation and response.

3.5.2 Ensemble Risk Scoring

The platform implements an ensemble risk scoring system that integrates predictions from the hybrid AI model along with other machine learning models for comprehensive threat assessment. The risk scoring process combines predictions from the ARIMA-LSTM hybrid model with other model outputs using the formula $\text{Risk Score} = \sum(w_i \times s_i)$, where w_i represents the weight for model i and s_i represents the score from model i .

The system incorporates additional factors including time-based patterns and trend factors, providing a robust framework for risk assessment. This ensemble approach creates a comprehensive risk scoring system that adapts to changing threat landscapes by combining the strengths of different models and methodologies. This implementation demonstrates a sophisticated approach to threat detection and analysis, combining traditional machine learning models with advanced hybrid AI approaches. The integration of these different methodologies provides a robust framework for threat detection and prediction, with each component contributing specific strengths to the overall system.

3.6 Real-Time Threat Visualization

The SIEM dashboard provides a real-time visualization of threat detection by continuously processing synthetically generated threat data through its threat detection engine. The system operates on a 30-second refresh cycle, dynamically updating the dashboard to simulate how real-time threat detection works. With each refresh, newly generated attack patterns are introduced, allowing the dashboard to display fluctuations in threat levels, evolving attack vectors, and changing risk severity in an interactive manner.

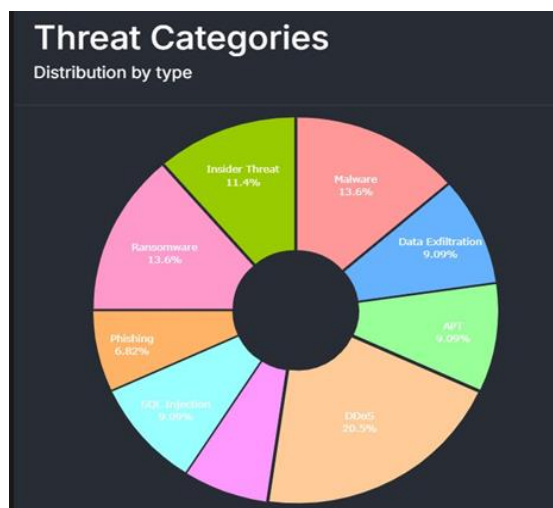


Fig. 3. Threat detection Pie Chart

Rather than detecting actual cyber threats, this project simulates the visual representation of security incidents, helping analysts understand how detection mechanisms operate in live environments. The threat analytics charts, severity distributions, and attack timelines are updated in real-time, offering insights into how security events unfold over time. By visualizing this process, the dashboard effectively demonstrates how an operational SIEM would detect and respond to threats, making it a powerful training and analysis tool for understanding cybersecurity monitoring workflows.

3.7 Threat Analytics

The SIEM dashboard provides real-time threat intelligence by visualizing threat types, severity, sources, and attack vectors. The Threat Intelligence Overview tracks attack categories like DDoS, malware, and zero-day exploits, while the Severity Distribution monitors risk levels and response statuses. The Threat Activity Timeline tracks threats over time, enabling proactive threat detection and incident response.

3.7.1 Threat Intelligence Overview

The Threat Intelligence Overview is a central feature of the SIEM Dashboard, offering a high-level summary of the current threat landscape. It categorizes threats into distinct types such as DDoS attacks, malware infections, and zero-day exploits. By tracking these categories, the dashboard provides a clear picture of the prevalent attack vectors and their potential impact on the organization. This overview helps analysts quickly identify the most pressing threats and prioritize their response efforts accordingly.



Fig. 4. Threat Intelligence Overview

3.7.2 Severity Distribution

The Severity Distribution visualization is a critical tool for assessing the risk levels associated with different threats. It categorizes threats based on their severity—ranging from low to critical—and tracks their response statuses, such as active, mitigated, or resolved. This distribution allows analysts to gauge the overall risk posture of the organization and allocate resources effectively to address high-severity threats.

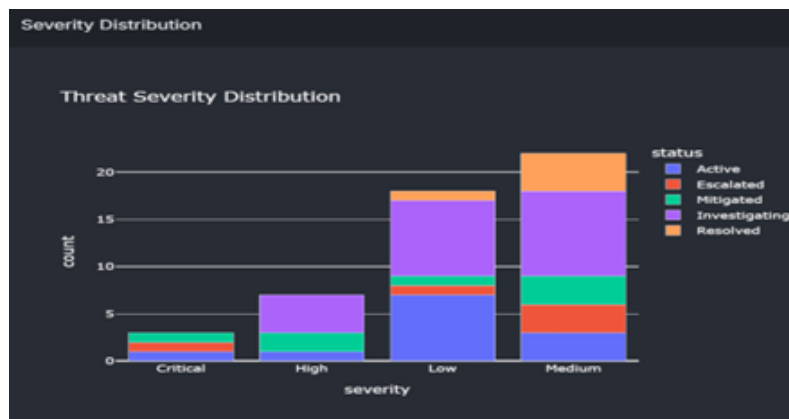


Fig. 5. Threat Severity Distribution

3.7.3 Threat Activity Timeline

The Threat Activity Timeline provides a chronological view of threat occurrences, enabling analysts to track the evolution of threats over time. This timeline highlights patterns and trends in threat activity, such as spikes in specific attack types or changes in threat sources. By visualizing these temporal patterns, the dashboard facilitates proactive threat detection and incident response. Analysts can use this information to anticipate future threats, adjust security strategies, and implement preventive measures to mitigate potential risks.



Fig. 6. Threat Trend Analysis

3.8 Threat Forecast

The Threat Forecast graph visualizes the predicted number of threats over the next 48 hours using historical threat data. The solid blue line represents past threat activity, while the dashed orange line indicates the forecasted threats generated by a time-series prediction model (ARIMA and LSTM). The shaded region around the forecast denotes the uncertainty range, providing a confidence interval for the predictions.



Fig. 7. Threat Forecast graph

By analyzing past trends in threat activity over time, the model identifies patterns and fluctuations to anticipate cyber threats for the next 48-hour period. This allows proactive security planning, enabling SOC teams to mitigate risks before they escalate. The model continuously updates based on new threat data, ensuring real-time adaptability and improved prediction accuracy to counter evolving cyber threats.

3.9 Evaluation Metrics

Aminu et al. [5] evaluate their threat detection system using performance and quality metrics to ensure accuracy and efficiency. Detection accuracy, precision, recall, and false positive/negative rates assess the system's ability to correctly classify threats, while response time measures how quickly threats are identified. Scalability ensures the system can process large security datasets without degradation. Additionally, quality metrics such as data completeness, consistency, and timeliness validate the reliability of threat intelligence. The dashboard responsiveness and alert accuracy are also measured to ensure timely and actionable security notifications.

The SIEM dashboard focuses on threat detection and prediction using synthetic data generation rather than real-time threat feeds. Since Fake Data Generator is used, the system does not implement traditional accuracy metrics like detection accuracy or anomaly detection efficiency. Instead, the performance evaluation is based on epoch vs. loss values, ensuring the model optimizes over continuous training cycles. The prediction models (ARIMA, LSTM) assess forecasting performance, determining trends in cyber threats. Synthetic data generation enhances data completeness, ensuring the system remains adaptable. This dashboard emphasizes real-time monitoring and predictive analytics, enabling a proactive cybersecurity approach despite the absence of real-world attack data.

IV. RESULTS AND DISCUSSION

The research paper by Singhal evaluates the effectiveness of integrating multiple AI models for real-time cyber threat detection and tracking. The study demonstrates that machine learning, deep learning, and anomaly detection techniques significantly enhance threat identification accuracy. The results indicate that the AI-driven system consistently achieved high precision, recall, and F1-scores, ensuring efficient threat classification. The system's dynamic tracking capabilities allowed for the real-time monitoring of evolving cyber threats, improving adaptive defense mechanisms. The integration of multiple AI models reduced false positives and negatives, enhancing overall cybersecurity resilience [10].

Building upon the AI-driven cybersecurity framework presented by Singhal [10], this project integrates real-time detection, predictive analytics, and visualization tools to simulate how a cyber threat monitoring system operates. Instead of detecting real-time attacks, this system provides a visual representation of threat detection and forecasting using synthetic threat data. The SIEM Dashboard, built with Dash and Plotly, dynamically updates every 30 seconds, visually demonstrating how threat levels fluctuate, attack patterns evolve, and risk severity changes over time.

The project leverages Pandas for data processing, enabling real-time analysis of generated security logs and trends. Threat visualization is achieved through interactive graphs, heatmaps, and trend analysis plots, showcasing how cyber threats might be detected in a real-world SOC environment. This simulation effectively replicates how a functional SIEM system would analyze, classify, and predict cyber threats, offering security analysts an intuitive and interactive platform for understanding cybersecurity monitoring workflows.

In this project, epoch vs. loss tracking is used to evaluate model performance instead of traditional accuracy-based metrics, as the system relies on synthetic threat data rather than real-time security feeds. During training, the LSTM model learns from historical threat data generated by the SOC Data Generator to predict cyber threats 48 hours in advance. Each epoch represents a full pass of the training data through the model, with the loss function (e.g., Mean Squared Error - MSE) measuring the difference between predicted and actual threat levels.

Initially, the loss is high, indicating inaccurate predictions, but as the model iterates through multiple epochs, it refines its parameters, gradually reducing the loss value. For example, after the first epoch, the loss may be 1.5, but by the tenth epoch, it could decrease to 0.4, signifying improved forecasting accuracy. If the loss stabilizes at a low value, the model is considered well-trained, whereas an increasing loss after multiple epochs indicates overfitting, requiring adjustments like regularization. This iterative learning process ensures the model effectively recognizes threat patterns, making it capable of proactive cybersecurity threat forecasting despite the absence of real-world attack data.

The threat mitigation process in this project follows a structured approach integrating real-time detection, predictive analytics, and automated response mechanisms. Once a threat is detected and classified based on its severity, mitigation actions are triggered accordingly. High and critical threats prompt immediate alerts and automated responses, such as firewall rule updates, IP blocking, or access restrictions, minimizing potential risks. For medium and low-severity threats, analysts review security events through the SOC Dashboard, allowing for manual intervention and further investigation. The system continuously refreshes every 30 seconds, ensuring real-time updates on newly detected threats and their mitigation status. Additionally, the platform generates security reports in PDF, CSV, and Excel formats, providing insights into past incidents, response times, and mitigation effectiveness. By integrating real-time monitoring with predictive threat intelligence, the system ensures an adaptive and proactive cybersecurity defense strategy.

V. CONCLUSION AND FUTURE WORK

This project successfully integrates a simulation platform for threat detection, prediction, and mitigation using an SOC Data Generator, providing a visual representation of cybersecurity monitoring rather than real-time threat detection. The system utilizes Pandas, Plotly, and Dash to simulate threat detection visualization, demonstrating how an operational SIEM would analyze security events. Additionally, ARIMA/LSTM models are used to simulate cyber threat forecasting for the next 48 hours, showcasing predictive analytics in cybersecurity. The SIEM dashboard refreshes every 30 seconds, updating synthetic threat data to illustrate how real-time detection and risk assessment work in practice. While this system does not process real-world threats, it offers an

interactive and educational simulation of how detection, analysis, and reporting mechanisms function in an operational security environment.

Obtaining real-time threat intelligence data is a complex and challenging task due to several technical, legal, and operational constraints. Cybersecurity incidents occur across multiple networks, organizations, and industries, making it difficult to access live attack data due to privacy regulations, data sensitivity, and confidentiality agreements. Many organizations restrict sharing threat intelligence to avoid exposing vulnerabilities that could be exploited by attackers. Additionally, cybersecurity datasets require continuous monitoring, validation, and enrichment, as raw data often contains false positives, duplicate entries, and irrelevant security logs, making real-time processing highly resource-intensive.

Future enhancements to this system will focus on implementing a real-time Security Operations Center (SOC) dashboard; several critical components must be integrated to ensure efficient threat detection, analysis, and mitigation. Real-time threat intelligence feeds from trusted cybersecurity sources such as MITRE ATT&CK, VirusTotal, and Open Threat Exchange are essential for pulling live threat indicators and continuously updating security insights. SIEM (Security Information and Event Management) integration is necessary to collect and analyze security logs from endpoints, firewalls, and network traffic, providing a centralized threat monitoring system.

Additionally, streaming data processing technologies like Apache Kafka, Spark Streaming, or the ELK Stack are required to handle large volumes of security data in real time, ensuring timely incident response. To enhance automation, AI-based threat classification and mitigation models must dynamically categorize threats and trigger automated defense mechanisms, such as blocking malicious IPs or isolating infected devices.

Furthermore, user management and role-based access control (RBAC) should be incorporated to establish secure access levels for security analysts, incident responders, and administrators, ensuring structured threat management and response coordination. Lastly, a scalable infrastructure, whether cloud-based or on-premises, must support high-speed data ingestion, storage, and real-time analytics to efficiently process security events. This will enhance SOC operations by streamlining response workflows, improving accountability, and ensuring secure access management. With these advancements, the SOC dashboard will evolve into a fully operational AI-powered cybersecurity platform, capable of handling both real-world threat intelligence and dynamic user interaction for comprehensive threat detection, prediction, and mitigation.

VI. REFERENCES

- [1] Shaukat, K., Luo, S., Chen, S. and Liu, D. 2020. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. IEEE Conference Proceedings.
- [2] Uppalapati, D. V. 2022. Cyber Threat Intelligence and Machine Learning. Fourth International Conference on Transdisciplinary AI (TransAI), 156-159.
- [3] Ogundairo, O. and Broklyn, P. 2024. Predictive Analytics for Cyber Threat Intelligence. Journal of Cyber Security, August, 1-18.
- [4] Dwivedi, S. A., Attry, A., Parekh, D. and Singla, K. 2021. Analysis and forecasting of Time-Series data using S-ARIMA, CNN and LSTM. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 131-136.
- [5] Aminu, M., Akinsanya, A., Dako, D. A. and Oyedokun, O. 2024. Enhancing Cyber Threat Detection through Real-time Threat Intelligence and Adaptive Defense Mechanisms. International Journal of Computer Applications Technology and Research, 13(8): 11-27.
- [6] Han, C.-H. 2021. Security Operation Dashboard Design by Blockade-Detection-Response. Journal of Information and Security, 21(3): 39-52.
- [7] Wang, B.-X., Chen, J.-L. and Yu, C.-L. 2022. An AI-powered network threat detection system. IEEE Access, 10: 54029-54037.
- [8] Singhal, S. 2024. Real-Time Detection and Tracking Using Multiple AI Models and Techniques in Cybersecurity. International Journal of Cybersecurity Studies, 16(16): 1-18.
- [9] Hernandez-Suarez, A. et al. 2023. ReinforSec: An Automatic Generator of Synthetic Malware Samples and Denial-of-Service Attacks through Reinforcement Learning. Sensors, 23(1231): 1-28.
- [10] Sun, N. et al. 2023. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials, 25(3): 1748-1773.
- [11] Singh, A. and Jha, R. 2023. Cyber Threat Analysis and Prediction Using Machine Learning. International Journal of Cybersecurity and Digital Forensics, 12(4): 341-356.
- [12] Lim, H., Park, J. and Kim, Y. 2023. Cyber Threat Detection Using Machine Learning. Proceedings of International Conference on Artificial Intelligence in Cybersecurity, 112-125.