

ThreatPulse: An AI-Enhanced SIEM Framework for Web Vulnerability Detection and Threat Intelligence

Parth Patil, Suyash Thanage, Ganesh Dubey, Omkar Patil, Dr.Siddharth Hariharan.

Department of Information Technology
Pillai College of Engineering
Navi Mumbai, India

Abstract—With the rapid growth of web applications, cyber assaults are becoming more and more frequent and complex at an exponential rate. Efficient Security Information and Event Management (SIEM) systems are imperative in modern cyber-security. Conventional SIEM solutions mostly rely on rule-based event correlation and signature-based detection, which limits their ability to detect advanced web attacks, zero-day threats, and new attack patterns. Recent advances in Artificial Intelligence (AI) and Machine Learning (ML) have improved threat detection by providing intelligent anomaly detection, automated analysis and improved incident response.

This survey reviews recent studies on AI-enabled lightweight SIEM systems for web application security, focusing on intelligent event correlation, machine learning-based intrusion detection, AI-aided Security Operations Centers (SOCs), and web application vulnerability detection. The report provides a comparative analysis of existing approaches to identify their strengths, limitations and research gaps. From these observations, the survey explores the ThreatPulse framework, which consists of rule-based detection, machine learning, adaptive analyst feedback, collaborative scam website notification, and a centralised blacklist repository of malicious websites. The survey discusses recent research trends and offers insights into the development of lightweight, intelligent, and collaborative SIEM systems for modern web application environments.

Index Terms—Security Information and Event Management (SIEM), Artificial Intelligence, Machine Learning, Web Application Security, Intrusion Detection, Security Operations Center, Threat Intelligence.

I. INTRODUCTION

The rapid growth of web applications, cloud computing and digital services has led to a massive increase in the cyber threat landscape. Modern web applications are handling sensitive data like financial transactions, medical records, authentication credentials and confidential business data. Therefore, cyberattacks on these applications have become more sophisticated, which necessitates security mechanisms that provide ongoing surveillance, rapid threat detection, and effective incident response [1], [2].

Security Information and Event Management (SIEM) systems are essential for modern Security Operations Centers (SOCs) by aggregating, normalising, correlating, and analysing security events produced from multiple data sources. Traditional SIEM platforms primarily depend on predefined correlation rules and signature-based detection methods to detect malicious activities. While effective against known

attacks, these techniques often fail to detect zero-day exploits, changing attack patterns, and sophisticated multi-stage cyber intrusions [3].

Recent advances in Artificial Intelligence (AI), Machine Learning (ML) and anomaly detection techniques have created new opportunities to improve SIEM capabilities. Intelligent detection models can identify abnormal behavioural patterns, reduce false positives, and improve the identification of complex cyber dangers that cannot be effectively detected with static correlation rules alone. These developments have inspired researchers to adopt AI based analytics in security monitoring frameworks to enhance decision making and automate threat detection [4], [5].

This survey provides a complete overview of the state-of-the-art AI enhanced lightweight SIEM systems for web application security. This paper provides a review of traditional SIEM architecture, machine learning based detection methods, event correlation techniques, detection of web application vulnerabilities and AI assisted security operations. Beside, the survey not only points out the existing research gaps, but also proposes an AI-enhanced lightweight SIEM framework, named ThreatPulse, integrating intelligent threat detection, collaborative scam website notification, and centralised verified malicious website repository to improve the web application security.

II. BACKGROUND

The growing complexity of online dangers has increased the need for intelligent security monitoring systems that can detect malicious activities in real time. Today, Security Operations Centers (SOCs) depend on Security Information and Event Management (SIEM) systems for centralised log management, event correlation, threat detection and incident response. This section deals with the basic principles that form the basis of AI-augmented SIEM systems and web application security.

A. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) integrates Security Information Management (SIM) and Security Event Management (SEM) into a unified platform. SIEM solutions continuously collect security logs from multiple sources including firewalls, intrusion detection systems, operating systems, web servers, authentication services, databases,

and network devices. The collected logs are normalized, correlated, and analyzed to identify suspicious activities before generating alerts for security analysts. Modern SIEM platforms also provide centralized dashboards, compliance reporting, incident investigation, and threat visualization capabilities [1], [3].

B. Web Application Security

Web applications remain a very attractive target for cyber-criminals because they typically handle sensitive user information and critical business data. The most common types of attacks are SQL injection (SQLi), cross-site scripting (XSS), session hijacking, malicious API requests, phishing attacks, and brute-force authentication attacks. Regular monitoring of network traffic, authentication events, user activities and application logs is required to detect these threats. Recent researches have shown the effectiveness of intelligent vulnerability discovery and machine learning techniques to improve the security of web applications. [6], [7].

C. Artificial Intelligence in SIEM

The use of Artificial Intelligence (AI) and Machine Learning (ML) has greatly improved the detection of threats by allowing security systems to recognize abnormal behavior instead of depending solely on predefined signatures. Complex attack patterns can be identified, detection precision improved and false positive alerts reduced using machine learning algorithms such as Random Forest, Support Vector Machine (SVM), XGBoost and deep learning models. AI-assisted monitoring also benefits security analysts by automating threat analysis and speeding incident response. [4], [5], [8].

D. Security Operations Center (SOC)

The Security Operations Center (SOC) is responsible for constant monitoring, detection, investigation and response to cybersecurity incidents. Today, SOC's are adding more AI-powered analytics, automation and smart decision support to their operations to help improve efficiency and take pressure off analysts. Recent work has discussed the growing role of Large Language Models (LLMs) and AI agents in improving SOC automation and incident response activities [9], [10].

III. RESEARCH METHODOLOGY

In this work, we perform this survey by using a systematic literature review methodology to identify, classify and analyse the recent research in the domains of AI-enhanced Security Information and Event Management (SIEM) systems, web application security, machine learning-based intrusion detection, graph-based behavioural analysis, and adaptive cybersecurity frameworks.

The selected studies were analysed based on research purpose, detection techniques, datasets, deployment environment, advantages, limitations, and research gap. The literature collected was then sorted into major research themes for systematic comparison and critical analysis.

In this section, we present a paper selection process inspired by PRISMA and research trend analysis.

IV. LITERATURE SURVEY

The recent developments in Security Information and Event Management (SIEM) systems have been orientated toward improving the threat detection using Artificial Intelligence (AI), Machine Learning (ML), intelligent event correlation, intrusion detection systems and automated incident response. Researchers have proposed different approaches to overcome the limitations of traditional rule-based SIEM platforms while improving scalability, detection accuracy and operational efficiency. In this section, we review the most relevant research work related to AI-enhanced SIEM systems, web application security, intrusion detection and intelligent cybersecurity monitoring.

A. AI-Enhanced SIEM Systems

A unified SIEM architecture consisting of Zeek IDS, Slips, and ELK Stack was proposed by Muhammad *et al.* [1] for the purpose of machine learning-based live traffic analysis. Their framework showed that open-source SIEM platforms can effectively integrate intelligent threat detection while providing for centralised log analysis. But it was evaluated on a limited attack scenario, and it required a lot of computational resources.

Sheeraz *et al.* [2] proposed an optimised correlation engine based on Intel Hyperscan for enhancing multi-layered attack detection. The proposed engine achieved significant correlation time reduction and detection performance improvement over traditional SIEM correlation mechanisms. Even with these improvements, the solution was still focused on optimising the rules and had little in the way of adaptive learning capabilities.

Manzoor *et al.* [3] analysed the trade-offs between security and performance of open-source SIEM solutions to support organisations with limited cybersecurity budgets. Their results highlighted that low-cost SIEM platforms provide monitoring functionalities at the budget level, but lack advanced AI-driven analytics and intelligent automation functionalities provided by enterprise-grade solutions.

B. Machine Learning-Based Threat Detection

Since machine learning makes it possible to detect new attack patterns, it has become a key part of state-of-the-art intrusion detection systems in recent years. Patil *et al.* [4] proposed an intelligent intrusion detection framework for improving detection accuracy using supervised learning algorithms. Similarly, Ferozuddin and Rizvi [5] introduced an AI-based anomaly detection model that can detect abnormal network behaviour and reduce false positive alarms.

Yedalla [8] showed the effectiveness of predictive threat detection by using machine learning and artificial intelligence techniques to find anomalies. Together, these studies show that machine learning can significantly improve cybersecurity monitoring, but many existing techniques require large training datasets and the models must be retrained periodically.

C. Web Application Security

Web applications are still one of the most targeted types of cyberattacks because they are exposed to the Internet and they often interact with sensitive user information. Brandi *et al.* [6] proposed an automated approach to identify input handling vulnerabilities in web applications that can be used for early detection of security weaknesses in application testing.

Bakir [Bakir2025] proposed UniEmbed, a machine learning framework that can detect SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks by using multiple feature fusion techniques. The proposed model obtained better detection accuracy, demonstrating the efficacy of AI-based methods in protecting modern web applications.

D. AI-Driven Security Operations

There are recent works that studied the adoption of Artificial Intelligence in Security Operations Centers (SOCs). Srinivas and Kirk [9] have studied the application of Large Language Models (LLMs) and intelligent agents to automate SOC operations, emphasising their ability to enhance incident investigation and analyst productivity. Ali *et al.* [10] similarly showed how AI-driven optimisation methods can enhance cybersecurity incident response, reducing investigation time and increasing operational efficiency.

E. Critical Analysis

The literature review shows that considerable progress has been made in the area of AI-enhanced cybersecurity monitoring using machine learning, intelligent event correlation, automated intrusion detection, and SOC automation. But there are still several evident limitations. Many of the existing SIEM platforms still depend heavily on predefined correlation rules, while AI-enabled approaches often require high computational resources and extensive training datasets. Furthermore, collaborative threat intelligence sharing, adaptive analyst feedback and lightweight deployment for small and medium-sized organisations have been paid little attention. The above observations motivate the development of the proposed ThreatPulse framework presented later in this survey.

V. COMPARATIVE ANALYSIS

The studies that have been reviewed have shown significant progress in improving Security Information and Event Management (SIEM) systems thru the application of Artificial Intelligence (AI), Machine Learning (ML), event correlation, intrusion detection, and automated incident response [1], [2], [4]. While each of the proposed solutions improves the effectiveness of cybersecurity monitoring, none of them fulfill the requirements of lightweight deployment, adaptive learning, collaborative threat intelligence, and web application-focused security.

Table I presents a comparison between conventional SIEM systems and the proposed ThreatPulse framework based on key functional characteristics identified throughout the literature.

As summarized in Table I, existing SIEM solutions have strong capabilities in centralized log collection, rule-based

event correlation and security monitoring. However, some studies have pointed out limitations in terms of high deployment costs, dependence on static correlation rules, computational overhead, and limited adaptability for evolving cyber dangers [2], [3].

Recent studies have shown that the combination of Artificial Intelligence and Machine Learning significantly improves the accuracy of intrusion detection and anomaly identification compared to traditional signature-based techniques. AI-based detection frameworks are able to detect complex attack patterns with the lowest false positive alerts, thus improving the cybersecurity monitoring and incident response [4], [5], [8].

Research into AI-assisted Security Operations Centers has demonstrated the growing importance of intelligent automation in threat hunting and incident response. The use of Large Language Models (LLMs) and intelligent agents can greatly enhance analyst productivity and speed up security decision-making. However, these features are mostly lacking in lightweight SIEM solutions for small and medium-sized organizations [9], [10].

As a whole, the literature work reviewed suggests that an ideal lightweight SIEM framework should combine intelligent threat detection, adaptive learning, collaborative threat intelligence, centralized monitoring, and affordability in one integrated platform. These observations directly motivate the proposed ThreatPulse framework, which we discuss in the following sections.

VI. EXISTING CHALLENGES

Tho SIEM systems have made significant advancements, a number of practical challenges continue to hinder their effectiveness in modern cybersecurity environments [2], [3].

The majority of traditional SIEM platforms depend heavily on pre-defined correlation rules and manually configured detection policies. The fast evolution of cyber dangers makes it more and more challenging to keep these rules up-to-date, often leading to late detection of emerging attack techniques and sophisticated cyber assaults. [2].

While Artificial Intelligence and Machine Learning have certainly improved threat detection capabilities, most AI solutions are computationally expensive, need high-quality labeled datasets and periodic retraining of models. These requirements limit their usage in organizations with scarce cybersecurity infrastructure and financial resources. [4], [5], [8].

Another big challenge is alert fatigue, where security analysts are overwhelmed by the volume of alerts generated by existing SIEM platforms. A high rate of false positives leads to longer investigation times and the possibility of missing real security incidents.

Current SIEM solutions also have limited visibility into web application-specific activities such as authentication events, malicious API requests, phishing websites, and application-layer attacks. Furthermore, collaborative threat intelligence sharing and centralized repositories of verified malicious websites remain largely unexplored in lightweight SIEM environments.

TABLE I: Comparison Between Conventional SIEM Systems and the Proposed ThreatPulse Framework

Feature	Conventional SIEM	ThreatPulse
Centralized Log Collection	✓	✓
Rule-Based Threat Detection	✓	✓
Machine Learning-Based Detection	Limited	✓
Behavioral Threat Analysis	Limited	✓
Real-Time Alert Generation	✓	✓
Web Application Security Monitoring	Limited	✓
Email Notification to Trusted Users	✗	✓
Collaborative Scam Website Notification	✗	✓
Centralized Blacklisted Website Dashboard	✗	✓
Verified Scam Website Repository	Limited	✓
Threat Intelligence Sharing	Limited	✓
Explainable AI Alerts	✗	✓
Analyst Feedback Integration	✗	✓
Adaptive Learning Support	Limited	✓
Deployment Complexity	High	Low
Resource Consumption	High	Low
Deployment Cost	High	Low
Lightweight Deployment	Limited	✓
Suitable for SMEs and Educational Institutions	Limited	✓
Scalability for Web Applications	Moderate	High
Dashboard Visualization	Basic	Advanced
Incident Response Support	Moderate	Enhanced

The solutions to these challenges will be the development of intelligent, adaptive and cost-effective SIEM frameworks that can support continuous learning, collaborative cybersecurity and efficient web application monitoring.

VII. RESEARCH GAP

The literature survey shows several important gaps in the research that still limit the effectiveness of current Security Information and Event Management (SIEM) systems for the security of modern web applications [1], [3].

Most conventional SIEM platforms primarily depend on predefined correlation rules and signature-based detection mechanisms. While these approaches remain effective against known attacks, they exhibit limited adaptability toward evolving cyber threats, zero-day exploits, and sophisticated attack campaigns [2].

Recent studies have been able to introduce Artificial Intelligence and Machine Learning in intrusion detection and threat analysis, however, these solutions require a lot of computing power, large labelled datasets and constant retraining. This constrains their application in lightweight environments [4], [5].

Another significant limitation of the reviewed literature is the absence of collaboration in sharing of threat intelligence. Current lightweight SIEM solutions are predominantly focused on monitoring activities within a single deployment and rarely offer dissemination of verified phishing domains or malicious websites among trusted users and organisations [9], [10].

Furthermore, the surveyed systems have limited facilities to keep a centralised repository of verified malicious websites.

Security analysts often analyse phishing domains and malicious websites during incident response, but this information is rarely retained in an easily accessible blacklist database for future use and proactive defence.

The research gaps indicate the need for an intelligent, lightweight and adaptive SIEM framework that can incorporate machine learning, analyst feedback, collaborative scam website notification and centralised blacklist management. The proposed ThreatPulse framework addresses these limitations by combining intelligent threat detection with practical security features designed for web application environments.

VIII. PROPOSED FRAMEWORK

Given the limitations found in the surveyed literature, the present paper proposes an AI-enhanced lightweight Security Information and Event Management (SIEM) framework for web application security. The presented framework seeks to integrate intelligent threat detection, adaptive learning and lightweight deployment, while being suitable for small and medium-sized organisations that cannot afford enterprise-grade SIEM platforms.

Log collection, event normalisation, hybrid threat detection, behavioural correlation, real-time alert generation, and centralised security monitoring are integrated into a unified architecture. Unlike traditional SIEM systems that largely depend on static correlation rules as their primary detection method, the proposed framework combines rule-based detection with machine learning and behavioural analysis at the session level to enhance the detection of known and emerging cyber dangers. [1], [2]

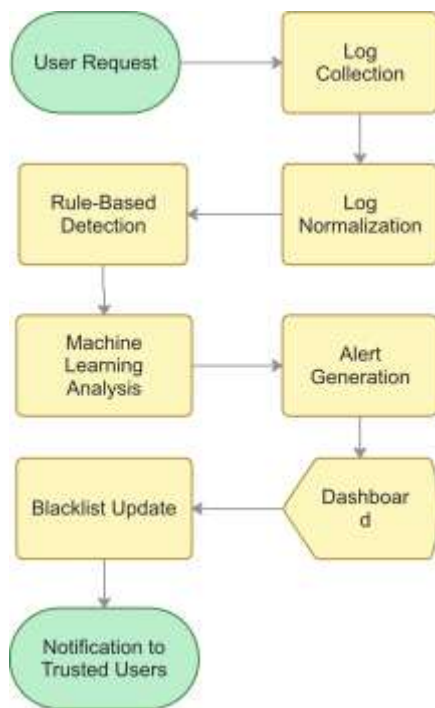


Fig. 1: Workflow of the Proposed ThreatPulse Security Monitoring Process.

A. Proposed System Architecture

The architecture of the proposed ThreatPulse framework is illustrated in the following figure. It is designed as a lightweight AI-enhanced Security Information and Event Management (SIEM) framework, which continuously monitors the web application activities, detects malicious behaviour and helps the security analysts to respond to the cyber risks. ThreatPulse incorporates rule-based detection with machine learning techniques to enhance the detection of known and emerging attacks, unlike traditional SIEMs that heavily rely on static correlation rules.

The framework comprises a set of interconnected modules that work together to achieve log collection, event normalisation, threat detection, alert generation, centralised monitoring, and adaptive learning. The log collection module gathers security logs from authentication services, web servers, application logs, databases, firewalls, intrusion detection systems, and user activities continuously. These heterogeneous logs are normalised to a common format so as to achieve uniformity before sending them to the threat detection engine for analysis. The hybrid detection engine is the core of the framework. It analyses incoming events and detects suspicious behaviour by combining predefined security rules and machine learning algorithms. Rule-based detection allows for quick detection of known attacks such as brute-force login attempts, SQL Injection (SQLi), Cross-Site Scripting (XSS), and strange authentication activities. Machine learning algorithms analyse behavioural patterns to detect anomalies that may indicate the

presence of novel or emerging cyber dangers. [4], [5]

The alert management module receives security events that have been detected with the correct severity level assigned. The security alerts are then presented thru a centralised Security Operations Center (SOC) dashboard that allows administrators to see ongoing attacks, investigate suspicious activities, analyse historical incidents and evaluate the overall security posture of the monitored web application. The dashboard also includes statistical summaries and visualisation of detected events to facilitate faster decision-making during incident response.

ThreatPulse also includes an adaptive learning mechanism where analyst feedback can be used to improve future detection performance, thus increasing the practical usefulness of the framework. Detection models can be tuned with alerts that are flagged as false positives or real attacks, thus reducing false positives and improving system accuracy over time.

The proposed framework also extends the traditional SIEM functionality with collaborative scam website notification and centralised blacklist repository. When the system verifies a phishing or scam website, or when it is confirmed by a security analyst, the malicious domain is automatically added to the blacklist database, and can be displayed thru the dashboard. In addition, trusted users who have registered on the platform can be notified about newly discovered malicious websites, which helps to proactively raise awareness and prevent other users from visiting fraudulent domains.

To summarise, the proposed ThreatPulse architecture unites centralised monitoring, intelligent threat detection, adaptive learning, collaborative threat intelligence, and lightweight deployment into a cohesive security framework. Such capabilities enable the proposed system to be more applicable to web application security and overcome some limitations found in existing SIEM solutions.

B. Existing System Architecture

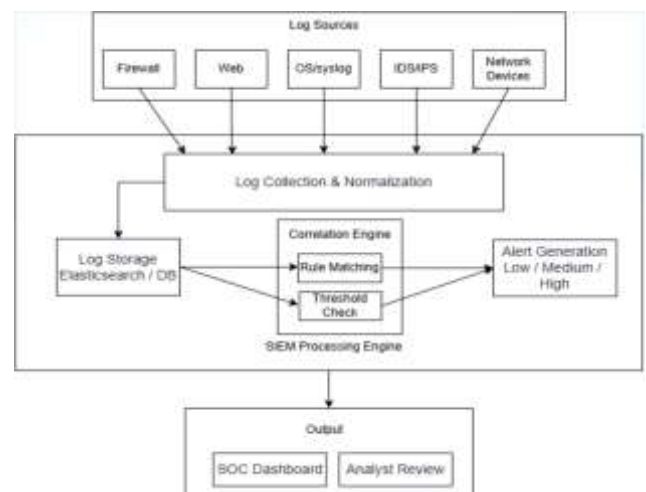


Fig. 2: Existing System Architecture of a Conventional SIEM.

To understand the architecture of conventional Security Information and Event Management (SIEM) systems, before

presenting the proposed framework. As shown in Fig. 2, traditional SIEM solutions collect security logs from multiple sources such as firewalls, web servers, operating systems, intrusion detection systems and network devices. The logs are normalised and then processed by a rule-based correlation engine for detecting predefined attack patterns. The generated alerts are sent to a central Security Operations Center (SOC) dashboard that is monitored and used for incident analysis.

However, it provides centralised log management and event monitoring. But the current architecture is heavily dependent on static correlation rules and predefined attack signatures. This makes it still challenging to detect sophisticated or unseen online dangers which shows the need of more intelligent and adaptive security monitoring approaches.

C. Detection Engine

The detection engine represents the core component of the proposed framework. The detection engine is the main part of the proposed framework. The combination of the different detection strategies, instead of just relying on the predefined signatures, improves the overall security monitoring.

Rule based correlation detects common attacks such as brute-force login attempts, SQL injection patterns, excessive API requests and suspicious authentication behaviour within milliseconds. The extracted log features are analysed by machine learning algorithms to detect anomalies that cannot be identified by static rules alone.

Beside intelligent threat detection, the framework includes also a collaborative threat intelligence module. In case of rule-based detection, machine learning analysis or analyst verification of a malicious website, the domain is automatically registered in a centralised blacklist repository. Authorised users can then be notified of new malicious websites that have been discovered, allowing them to take action to proactively address phishing campaigns and fraudulent domains. This joint method boosts organisational awareness and allows for quick sharing of verified threat intelligence.

D. Alert Generation and Dashboard

When malicious activity is identified, the framework generates security alerts with severity levels and descriptive information to aid analysts during incident investigations. An easy-to-use monitoring interface provides a centralised dashboard with detected attacks, security trends, recent incidents and system activity.

In addition, the dashboard allows analysts to review detected events and monitor the overall system state, which improves situational awareness and reduces the response time in security incidents. [10].

E. Adaptive Learning

One of the main objectives of the proposed framework is to enable continuous improvement of the performance of threat detection. The feedback from analysts gathered during security investigations can be used to tune the future detection models. This reduces false positives and improves detection accuracy over time.

This adaptive learning capability addresses one of the key limitations found in the surveyed literature, where most of the existing standard models for machine learning are static after deployment. Srinivas, et al., 2025

F. Framework Advantages

The proposed framework has many advantages over many existing lightweight SIEM solutions such as intelligent threat detection, better monitoring of web application activities, lesser dependence on manually defined rules, better behavioural analysis and better suitability for deployment in resource constrained environments. These features are promising a future research direction for lightweight AI-enhanced security monitoring systems.

G. Collaborative Scam Website Notification

The proposed framework enhances the conventional SIEM functionality with collaborative threat intelligence sharing. When the malicious website is detected, the system automatically sends notifications to trusted users, such as team members, colleagues or friends that are registered on the platform. The alerts contain the malicious domain, threat category, time of detection, and recommended steps to prevent it.

H. Blacklisted Website Repository

The framework also provides a centralised repository of verified malicious websites which can be accessed from SIEM dashboard. For each blacklisted domain, information about the threat category, detection timestamp, risk level, verification status, and reporting history is retained. Security administrators can review previously discovered domains, track threat tendencies and perform quick queries before permitting access to unknown websites. The repository also supports organization threat intelligence with a continuously updated database of verified malicious web resources.

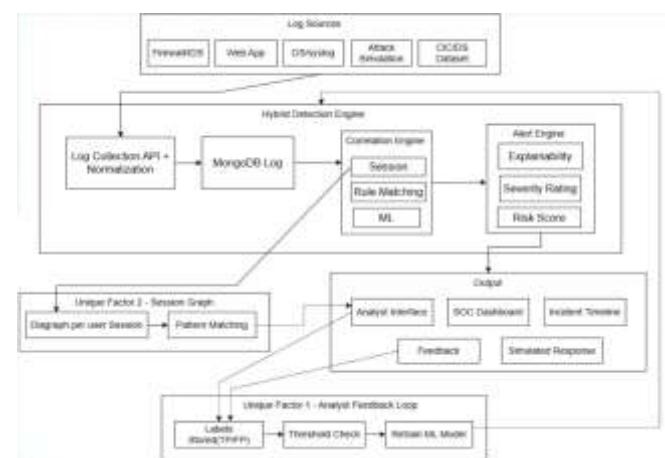


Fig. 3: Proposed ThreatPulse System Architecture

IX. FUTURE RESEARCH DIRECTIONS

Future work may include the incorporation of external threat intelligence feeds, continuous analyst feedback to improve machine learning algorithms, and lightweight SIEM deployment across cloud native environments. Further work could look at protection mechanisms in browsers, mobile alerts and automated response strategies for emerging online dangers.

Future work may include the integration of cloud native monitoring capabilities to support applications deployed in hybrid and multi-cloud environments. This combination would provide a centralized view of distributed web applications while maintaining the light-weight deployment characteristics. The proposed framework can be improved by using advanced Artificial Intelligence techniques such as Deep Learning, Federated Learning, and Explainable Artificial Intelligence (XAI). These methods can improve threat detection accuracy, but they can also increase analyst confidence in automated security decisions.

A further promising direction is to integrate external threat intelligence feeds that provide an up-to-date view of malicious IP addresses, phishing domains and attack indicators. The combination of externally derived intelligence and locally generated security events can enhance proactive threat detection and incident response.

The collaborative scam website notification mechanism proposed in this framework could be further extended to a community-driven threat intelligence network in which verified malicious websites are securely shared between trusted organisations. This type of cooperation can help to reduce the number of phishing attacks by sharing the newly discovered malicious domains quickly.

By keeping the proposed architecture lightweight, future versions of the framework could also support mobile notifications, automated browser protection and integration with enterprise security tools to create a more comprehensive cybersecurity ecosystem.

X. CONCLUSION

The survey provides an extensive overview of recent trends in Artificial Intelligence augmented Security Information and Event Management (SIEM) systems for web application security. Current research demonstrates that combining machine learning, intelligent event correlation and automated security monitoring significantly enhances the detection of online dangers over traditional rule-based methods.

The literature survey also highlighted various limitations of existing SIEM solutions including reliance on static correlation rules, high deployment costs, limited application layer monitoring, lack of adequate adaptive learning capabilities, and lack of collaborative threat intelligence mechanisms.

Based on these observations, this paper proposed a lightweight artificial intelligence enhanced SIEM framework specifically for web application environments. The proposed framework combines rule-based detection, machine learning, adaptive analyst feedback, collaborative scam website notification and a centralized blacklist repository to enhance security

monitoring while still being applicable for small and medium-sized organizations.

The proposed ThreatPulse framework enhances traditional SIEM capabilities by combining rule-based detection, machine learning, adaptive analyst feedback, collaborative scam website notification, and a centralized blacklist repository. These enhancements provide a pragmatic direction to design intelligent and lightweight security monitoring solutions for web application environments and small-medium sized organizations.

REFERENCES

- [1] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated siem with ids for live analysis based on machine learning," *Procedia Computer Science*, 2023.
- [2] M. Sheeraz, M. H. Durad, M. A. Paracha, S. M. Mohsin, S. N. Kazmi, and C. Maple, "Revolutionizing siem security: An innovative correlation engine design for multi-layered attack detection," *Sensors*, 2024.
- [3] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance trade-offs in open-source siem solutions," *PLoS ONE*, 2024.
- [4] R. M. Patil, R. V. Patil, U. Pagare, R. Navandar, R. Mapari, M. Bhowmik, and S. Deore, "An intelligent machine learning framework for intrusion detection," *International Journal of Intelligent Systems and Applications in Engineering*, 2024.
- [5] S. Ferozuddin and S. W. A. Rizvi, "Ai-driven anomaly detection model for intrusion detection systems (ids)," *International Journal of Computer Applications*, 2025.
- [6] C. Brandi, G. Perrone, and S. P. Romano, "Sniping at web applications to discover input-handling vulnerabilities," *Journal of Computer Virology and Hacking Techniques*, 2024.
- [7] R. Bakir, "Uniembed: A novel approach to detect xss and sql injection attacks leveraging multiple feature fusion with machine learning techniques," *Arabian Journal for Science and Engineering*, 2025.
- [8] J. Yedalla, "Leveraging ai and machine learning tools for predictive threat detection and anomaly identification," *International Journal of Scientific and Research Publications*, 2025.
- [9] S. Srinivas, B. Kirk *et al.*, "Ai-augmented soc: A survey of llms and agents for security automation," *Journal of Cybersecurity and Privacy*, 2025.
- [10] G. Ali, S. Shah, and M. ElAffendi, "Enhancing cybersecurity incident response: Ai-driven optimization for streamlined operations," *Results in Engineering*, 2025.