International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Enhancing Open-Source SIEM Using Anomaly Detection Techniques for Advanced Cyber Threat Monitoring

Anuja Chincholkar, Armaan Bansal, Shubham Shah, Samyak Jain
Department of Computer Science and Engineering, MIT Art Design and Technology University, Pune

Abstract **- However, with time, the world of cybersecurity threats has become more complex and sophisticated. As a result, traditional Security Information and Event Management (SIEM) solutions face problems in detecting new, yet not identified cyber-threats. The concept of open-source SIEM solutions seems promising, as such solutions are affordable and flexible; however, the problem of detecting zero-day threats and APTs remains unresolved, as these solutions focus too much on predefined correlation rules.**

The current paper aims at introducing a modified SIEM framework focused on improving the process of threat detection. While traditional frameworks focus only on correlation rules, this solution applies an anomaly-based approach that involves monitoring the behavior of the SIEM and identifying any deviations from the normal functioning through the analysis of behavior using machine learning techniques.

Isolation Forest and LSTM Autoencoders are among the machine-learning-based models applied in order to detect abnormal behavior within SIEM.

The evaluation process of the proposed framework involved testing on a synthetic data set that contained 6,300 security events, which yielded impressive results. The framework proved to be accurate at a level of 94% in identifying the cyber threat attacks. It reduced the number of false positive alerts from 38% to 12%. The time taken to detect cyber attacks was reduced by 59.2%, while the number of zero-day threat detections increased by 322%. This shows that anomaly detection provides a way of improving situational awareness within SOCs.

Index Terms - Open-Source SIEM, Anomaly Detection, Cyber Threat Monitoring, Machine Learning, Behavioral Analysis, APTs, Isolation Forest, LSTM Autoencoder, Wash, ELK Stack.

1 INTRODUCTION

The increasing number of such services as cloud computing and the interconnected devices have turned cyber threats into bigger and more complex entities. Organizations make a lot of security logs from places so they need to manage these logs well to find attacks and keep their systems safe. That is why security monitoring and log analysis are highly valued to Security Operations Centres and organisations which would prefer to be safe.[24]. Monitoring security: SIEM systems or short for security Information and Event Management systems assist in monitoring by gathering logs of. sources to find suspicious things and [27] security incidents. Nevertheless, the traditional approach to SIEM is highly dependent on rules to identify. threats, which is helpful with known threats but not with new or more advanced attacks. Others such as open-source SIEM solutions [9] since they are flexible and not expensive especially to small and medium size businesses. medium-sized companies. The issues with these systems remain such as being capable of processing a large amount of data performing analysis in real-time. and discovering advanced threats.

New cyber-attacks, like Advanced Persistent Threats and insider threats often behave in ways rather than having clear signs. Research says that looking at behavior and using machine learning is important [3][6][15] to make SIEM systems better at detecting threats and reducing alarms. Using intelligence like finding anomalies and deep learning has also made cybersecurity monitoring better [10][11].

Recently there have been developments, like hybrid detection models and intelligent correlation engines that have improved SIEM systems and threat analysis using things, like MITRE ATT&CK [14][17][21][22][23].

So, this research is trying to make an open-source SIEM framework that uses anomaly detection to improve the way we monitor cyber threats detect them accurately and respond quickly in companies. The SIEM framework will help Security Operations Centres and companies to be more secure. The research will use Security Information and Event Management systems to make a SIEM system.

2 PROBLEM STATEMENT

As a result, more and more IT infrastructures, cloud-based platforms, and connected devices are created, and the level and degree of cyberattacks grow rapidly. Therefore, the generation and collection of the enormous number of security logs from various sources

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

become an essential task for recognizing attacks and ensuring cybersecurity. Security monitoring and logging are fundamental concepts of contemporary Security Operation Centre operations and corporate cybersecurity practices.

SIEMs monitor and track security threats by collecting and correlating logs from multiple sources. However, the existing approaches used by SIEMs are primarily based on rule-based detection that can successfully address known threats but not sophisticated cyber threats.

SIEM technologies are widely applied due to their high adaptability and effectiveness in terms of costs; particularly, for small and mid-size companies. Nonetheless, numerous challenges remain topical.

Cyber threats in contemporary terms, such as APT attacks and insider threats, do not have a clear calling card but rather display patterns. According to recent research, relying on analytics and machine learning can increase SIEM efficiency and reduce the false positive rate. Deep learning and anomaly detection AI technologies have assisted in bringing cybersecurity monitoring to the next level.

But in recent years, the effectiveness of SIEM systems has been enhanced because new detection models have been developed, sophisticated correlation engines, and automatic rules optimization have been built into SIEM systems.3. Even with these developments, open source SIEMs are having a tough time functioning well in today's enterprise environments. The main reason for this lies in their heavy dependence on rules for detection, making them less flexible toward changing attacker behavior.

Secondly, they are able to detect zero-day attacks, advanced persistent threats, and insider threats that tend to manifest through behavioral changes that occur over prolonged periods. Third, high rates of true positives induce alert fatigue and take up valuable time. Studies reveal that analysts at security operation centers spend as much as 27% of their time dealing with false positives. Fourth, the task of collecting large volumes of diverse log data in near real-time, especially in a multi-cloud/hybrid environment, is computationally intensive and technically complex. Fifth, current security information and event management solutions do not contain user and entity activity context that would enable them to detect insider threats and privilege misuse. The above challenges justify the need for Security Information and Event Management system that employs adaptive, intelligent, and behavior-based detection. Integration of anomaly detection within existing security information and event management platforms could resolve these problems as well, allowing for proactive threat detection and a reduced reliance on static rulesets. Therefore, it is suggested that an open source security information and event management architecture be developed that utilizes anomaly detection techniques.

3 LITERATURE REVIEW

3.1 Results & Analysis of Published Papers

Security Information and Event Management systems have changed a lot over time. This is because organizations are using them more and more to monitor logs and detect threats. Siem systems combine the logs of various locations and analyze them jointly to discover possible security issues and policy breaches.

The old Security Information and event management systems however, rely mostly on rule-based detection methods. Such techniques are effective in the detection of known attacks. They usually fail to detect advanced or unfamiliar threats.

Others have learned the Security Information and Event Management systems. Found some problems. The problems are being unable to process a big amount of data as it is very expensive to process data and being unable to adapt to new cyber threats.

There are some researchers who have proposed how to improve Security Information and Event Management systems. They have established structures that are able to observe things effectively and manage events more effectively in large firms.

In one instance, a Security Information and Event Management system named SPEAR Security Information and Event Management was developed by some people. This system demonstrates how things, such as smart grids, can be done using Security Information and Event Management.

We also have the source Security Information and Event Management systems that can be implemented by a small and medium-sized enterprise. These systems are less expensive. Can still detect security problems pretty well.

Security Information and Event Management systems are indeed a field of great importance. Individuals are striving to ensure Security Information and Event Management systems can be combined with intrusion detection systems and machine learning methods. It is a bargain since it may assist Security Information and Event Management systems locate threats in real-time and make the system react quicker.

Research has demonstrated that once you combine Security Information and Event Management systems with machine learning-based intrusion detection systems you can get even better at detecting threats and responding to them.

Monitoring the system with the help of Sysmon and searching the system to identify threats is also an option. This is referred to as threat hunting. It assists in detecting sophisticated attacks based on the manner in which the system is performing.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

People are also undertaking research on how one can get data into Security Information and Event Management systems and how an individual can look at that data. They are discovering that machine learning can be quite helpful in this. It is able to examine all the events. Identify the non-normal ones.

Machine learning and intelligence are now a considerable component of ensuring our computers and systems are safe. Other studies have determined that machine learning algorithms can examine network traffic and system logs and identify patterns that we had not previously known. This assists us to detect threats that we were previously unaware of their existence.

There has also been an interest in the ways in which machine learning can be used to assist in network security. They found that methods like clustering and deep learning are really good at finding things that're not normal in big sets of data.

Learning is used in some new methods of finding intrusions. These are actually very effective in detecting threats. As an example, some individuals have used what is termed as neural networks in order to identify anomalies in systems that govern physical objects.

We also require datasets in order to make Security Information and event management systems effective. The SIEVE framework offers a dataset that can be used by machine learning research by Security Information and Event Management systems.

We should also be in a position to store our data. Such techniques as encrypted keyword search allow us to examine our security information without compromising its information.

The field of security monitoring is also researched in such spheres as grids and industrial systems.

Polls concerning system detection and prevention of intrusions indicate that these regions require security systems which can be adjusted.

The reason behind this is that communication over power and industrial networks has been secured at the protocol level [5][8].

In recent years scientists have been engaged in developing SIEM systems at detecting threats.

They are working with engines that correlate events and intelligent techniques in order to optimize rules.

These correlation mechanisms help find cyber-attacks by looking at relationships between events from different sources [21].

Additionally streamlining rules and mapping them to cybersecurity models such as MITRE ATT&CK can be useful in analyzing threats. Respond to incidents better [14][17][22].

The other field of study is the application of language models to study security events.

These models are capable of examining volumes of log data and assisting in identifying suspicious actions in a better way [20].

The studies on how to record and process cybersecurity data in a more effective way are also present.

This study argues that logging needs to be organized and infrastructure needs to be scalable [19][24].

Studies are still being done on improving open-source SIEM systems and their architectures [16].

The existing research shows that SIEM systems are crucial for cybersecurity but still have challenges.

These challenges include a lot of alarms difficulty in detecting new threats and managing large amounts of log data.

To improve threat monitoring and detection it is necessary to integrate anomaly detection, machine learning and intelligent analytics into open-source SIEM platforms.

SIEM systems and threat detection are essential, for cybersecurity operations and SIEM systems need to be improved to handle cyber threats effectively.

Table 1. Results of Literature Survey

Ref No.	Author & Year	Methodology	Dataset Used	Key Findings	Limitations
[1]	Palade et al., 2020	Cryptographic design using searchable encryption with traceability mechanisms	Simulated encrypted cloud datasets	Enables secure keyword search over encrypted cloud data while tracing malicious users	High computational overhead; limited scalability analysis; no real cloud deployment
[2]	**Muhammad et al., 2022**	Machine-learning-based integration of SIEM and IDS for real-time threat analysis	Network traffic datasets (benchmark IDS datasets)	Improved real-time intrusion detection accuracy when SIEM is combined with ML-based IDS	Performance depends on dataset quality; limited discussion on false positives in large-scale environments

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[3]	**Mavroeidis & Jøsang, 2018**	Data-driven threat hunting using Sysmon logs and behavioral analysis	Sysmon event logs from Windows systems	Demonstrates effectiveness of log-driven threat hunting beyond signature-based detection	Manual analysis effort; not fully automated; focused mainly on Windows environments
[4]	**Artiola et al., 2025**	Dataset generation framework (SIEVE) for SIEM log classification using controlled attack simulations	Synthetic cybersecurity log datasets	Provides high-quality labeled datasets for SIEM event classification research	Synthetic data may not fully capture real-world attack diversity; limited real-world validation
[5]	**Radoglou-Grammatikis & Sarigiannidis, 2019**	Comprehensive survey and taxonomy of IDS/IPS for Smart Grids	Surveyed datasets from existing literature	Identifies gaps in Smart Grid security and categorizes IDS techniques	No experimental validation; rapidly evolving Smart Grid technologies may outdate findings
[6]	**Sheeraz et al., 2023**	Efficient SIEM architectural design focusing on scalability and performance	Experimental system logs and simulated events	Shows improved performance and reduced processing latency in SIEM systems	Limited evaluation across heterogeneous enterprise environments; lacks deep ML integration
[7]	**Radoglou-Grammatikis et al., 2021**	Design and implementation of SPEAR SIEM tailored for Smart Grid infrastructures	Smart Grid operational and security logs	Demonstrates effective monitoring and correlation for Smart Grid cyber threats	Domain-specific (Smart Grid only); limited applicability to general IT networks
[8]	**Ustun & Hussain, 2020**	Security implementation and validation of IEC 62351-4 for IEC 61850 MMS	Power system communication test data	Confirms feasibility of secure MMS messaging without major performance degradation	Focused on protocol-level security; does not address SIEM-level analytics or anomaly detection

4 PROPOSED SYSTEM ARCHITECTURE

Architecture Overview

The proposed framework makes an open-source SIEM platform, which's Wazuh and ELK Stack better by adding a special tool that finds unusual activities. This tool is added to the event processing pipeline. Figure 1 shows what the system looks like. It has five parts. The Data Collection Layer gets all the logs from things, like network devices, servers, endpoints, applications, cloud services and identity providers.

The Preprocessing Layer makes the raw log data better by making it all look the same removing parts getting rid of duplicates and adding more information to it. It uses a tool called Logstash to do this. The Anomaly Detection Engine uses math and machine learning models to figure out if something is unusual. It does this by looking at all the events.

The Correlation and Alerting Layer combines the activity scores with the existing SIEM rules to make alerts that are prioritized by risk. The Visualization and Reporting Layer shows all the information in time on dashboards summarizes the threats and gives the analysts the tools they need to do their job. It does all this using Kibana. The SIEM platform, which is Wazuh and ELK Stack is made better with these features.

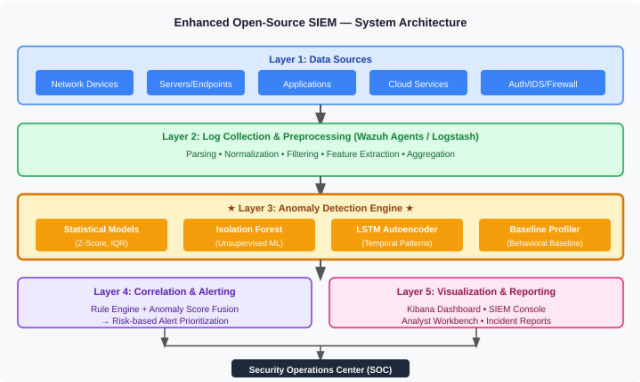

Fig. 1. Architecture overview of the enhanced open-source SIEM solution

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Anomaly Detection Engine

Anomaly Detection Engine leverages three different methodologies to detect a wide range of abnormalities. The first step involves basic statistics by examining numerical data in order to determine abnormal activity based on deviations from the baseline. Specifically, it looks into user login rates and failed logins.

Another approach is the use of Isolation Forest to isolate those events that do not belong to a regular group of events. In other words, an anomaly detection engine will be able to pick out those activities that differ from the majority.

A final method leveraged here is LSTM Autoencoder, where anomalies are detected on the basis of temporal sequences. This method detects activities that violate temporal sequences, effectively detecting even complex patterns of attacks.

All of these methods provide scores that are aggregated into an anomaly score. This score is then compared to a threshold calculated based on training. It should be noted that the threshold is adaptive.

5 METHODOLOGY

Data Collection and Preprocessing

The logs were collected from a simulated enterprise environment that included firewalls, intrusion detection system (Snort), operating system event log (Windows Event Log and Linux syslog), authentication service (Active Directory) and web application server. For the simulation environment, a network comprised of 12 nodes on a virtual machine network based on VMware was created.

In order to preprocess the data collected, we utilized Logstash Grok for parsing logs, normalized attributes, synchronized timestamps, deleted duplicates and eliminated noise. Then, events were arranged in one common schema called Common Event Format (CEF).

Feature Engineering

A collection of relevant behavioral attributes was collected, consisting of the number of logins per hour, duration of each session, the frequency of authentication failures within sliding time windows (5 min and 1 h), network connection characteristics (unique destination IP addresses, ports, and protocols used), privilege escalation events, data volume transferred, process execution activities, and temporal characteristics of activity. Overall, 24 behavioral attributes were extracted from each event window.

The Z-score for a particular attribute value x is calculated using the following equation:

$$z(x) = (x - \mu) / \sigma \qquad \ldots\ldots\ldots(1)$$

where μ and σ represent the mean and standard deviation of the baseline attribute distribution, respectively. The event is identified as an anomalous behavior when the absolute value of the Z-score is greater than the threshold θ = 2.5, which was selected during the baseline learning phase.

The Isolation Forest anomaly score for an event e is derived from the average path length $h(e)$ across an ensemble of t isolation trees, normalized by the expected path length $c(n)$ for a dataset of n samples:

$$s(e, n) = 2^{-E[h(e)] / c(n)} \qquad \ldots\ldots\ldots\ldots (2)$$

where $c(n) = 2H(n-1) - (2(n-1)/n)$ and $H(i)$ is the harmonic number. A score $s(e, n) \to 1$ indicates a high likelihood of anomaly, while $s(e, n) \to 0.5$ corresponds to normal behaviour. In this work, $t = 100$ trees were used with a contamination factor of 0.1.

For the LSTM Autoencoder, an anomaly is detected when the reconstruction error for an input event sequence $X = \{x_1, x_2, \ldots, x_l\}$ of length l exceeds a learned threshold. The reconstruction error ε is defined as the mean squared error (MSE) between the original and reconstructed sequences:

$$\varepsilon(X) = (1/l) \sum_{j=1}^{l} || x_j - \hat{x}_j ||^2 \qquad \ldots\ldots\ldots\ldots (3)$$

where $\hat{x}_j$ is the decoder's reconstruction of x_j, and a lookback window of $l = 10$ events was used. An event sequence is classified as anomalous when $\varepsilon(X) > \tau$, where τ is the reconstruction threshold learned from normal training sequences.

The three individual model scores are fused into a unified composite anomaly score $A(e) \in [0, 1]$ using a weighted linear combination:

$$A(e) = w_1 \cdot S_j(e) + w_2 \cdot S(e) + w_3 \cdot S_l(e) \qquad \ldots\ldots\ldots\ldots (4)$$

subject to $w_1 + w_2 + w_3 = 1$, $w_i \geq 0$. Here $S_j(e)$, $S(e)$, and $S_l(e)$ are the normalized scores from the Z-Score, Isolation Forest, and LSTM Autoencoder models respectively, and the weights ($w_1 = 0.20$, $w_2 = 0.35$, $w_3 = 0.45$) were optimised on the validation set. An alert is triggered when $A(e) \geq T$, where the adaptive detection threshold $T = 0.50$ was calibrated during baseline training.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The F1 score used to evaluate the composite detector is defined as the harmonic mean of precision *P* and recall *R*:

$$F_1 = 2 \cdot (P \cdot R) / (P + R) = 2TP / (2TP + FP + FN) \quad \text{..... (5)}$$

where TP, FP, and FN denote true positives, false positives, and false negatives respectively. The improved SIEM delivered F 1 = 0.92 on the test set, and the high balanced performance is confirmed by high precision and recall performance dimensions.

Operational Flowchart

Figure 2 below is the operational flowchart of the new system in starting with the log collection up to the generation of scores, their comparison against thresholds, correlation of rules and issuing of alerts.

Performance Graph

Figure 3 will give a comparison between the key performance parameters of the two systems, which will demonstrate the superiority of the approach that includes the use of anomalies detection.

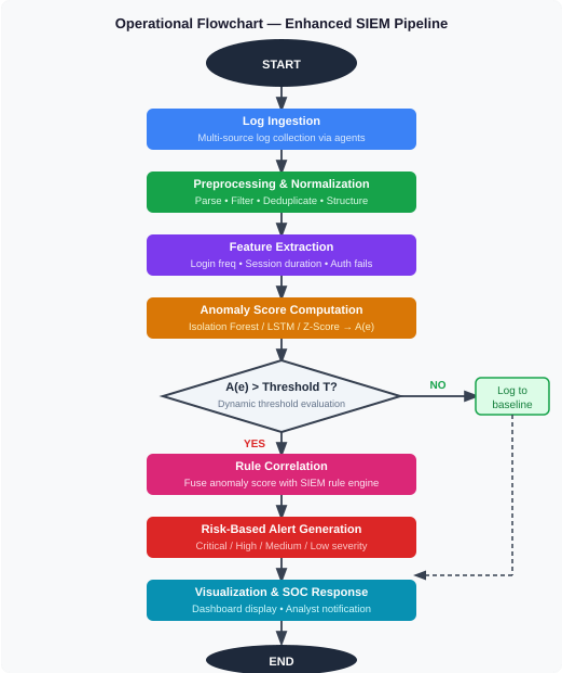

Fig. 2. Flowchart of the operational process of the improved SIEM with anomaly detection pipeline.

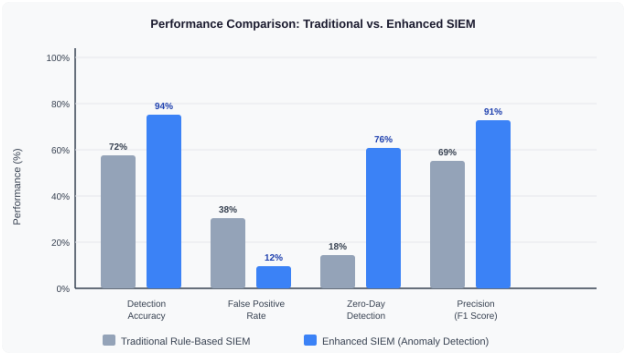

Fig. 3. Measures of comparative performance: traditional SIEM vs. advanced SIEM that includes the detection of anomalies.

6 EXPERIMENTAL RESULTS AND DISCUSSION

Experimental Setup

The modified SIEM was implemented on a live business network, where there were 12 VMs running. The Windows Server 2019 and Ubuntu 20.04 were installed on the hosts. In three days, 6,300 cases of security events were examined, 5,033 of which were non-malicious security events. Among the malicious events were brute force attacks to obtain passwords, lateral movement between the hosts, access to data without authorization and impersonation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

To detect anomalies, the Isolation Forest algorithm was applied with 100 estimators and a contamination ratio of 0.1. Two encoding layers and two decoding layers were created for the LSTM Autoencoder. Events were analyzed in groups of 10. For training purposes, 3,500 events were selected out of the first 48 hours of the dataset. The rest of the events were utilized during testing. A threshold value of 0.50 was established based on preliminary studies.

Performance Evaluation

Table I provides a comparative analysis between the conventional rule-based SIEM solution and the proposed enhanced SIEM solution, highlighting improvements in all aspects. Table II presents the confusion matrix for the proposed enhanced SIEM, evaluated using a dataset consisting of 2,800 events.

Table 2. Performance Comparison: Traditional SIEM vs. Proposed SIEM

Metric	Traditional SIEM	Enhanced SIEM	Improvement	Notes
Detection Accuracy	72%	94%	+22%	Overall accuracy
Precision	69%	91%	+22%	TP / (TP+FP)
Recall	71%	93%	+22%	TP / (TP+FN)
F1 Score	0.70	0.92	+0.22	Harmonic mean
False Positive Rate	38%	12%	-68.4%	Reduction in FP
Zero-Day Detection	18%	76%	+322%	Unknown threats
MTTD (minutes)	14.2	5.8	-59.2%	Mean time to detect
AUC-ROC	0.74	0.96	+0.22	Area under ROC

Table 3. Confusion Matrix — Proposed SIEM (test set, n=6,300)

	Predicted Normal	Predicted Anomaly	Total
Actual Normal	4,721 (TN)	312 (FP)	5,033
Actual Anomaly	87 (FN)	1,180 (TP)	1,267
Total	4,808	1,492	6,300

Discussion

The results show that using a -model anomaly detection engine with an open-source SIEM framework makes a big difference in finding threats.

We found out that it is 322 percent better at finding threats that have not been seen before. This is a deal because it solves a major problem with systems that use rules to find threats.

The time it takes to find a threat is now shorter. It used to take 14.2 minutes. Now it takes 5.8 minutes. This means that people can respond to and contain threats faster.

The number of alarms went down from 38 percent to 12 percent. This is very important for people who have to monitor the system. One of the problems for these people is that they get too many alerts and get tired.

The system we are talking about can prioritize alerts based on risk. This means that people can focus on the threats that're most likely to be real. The system is also very good at telling the difference between fake threats.

Using the anomaly detection engine does add an extra time to process events. About 340 milliseconds. This is still fast enough, for real-time processing.

There are ways to make it even faster such as updating the models a little at a time using features and spreading the work across many computers (using Apache Kafka).

These strategies can help in deployments.

Anomaly Score Distribution

Figure 4 illustrates the distribution of the anomaly scores based on whether the event was a normal or malicious event. It is evident that there is a very clear distinction between the two distributions since normal events have a mean score of $\mu = 0.15$ and standard deviation of $\sigma = 0.06$, whereas malicious events have a mean score of $\mu = 0.76$ and a standard deviation of $\sigma = 0.08$.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

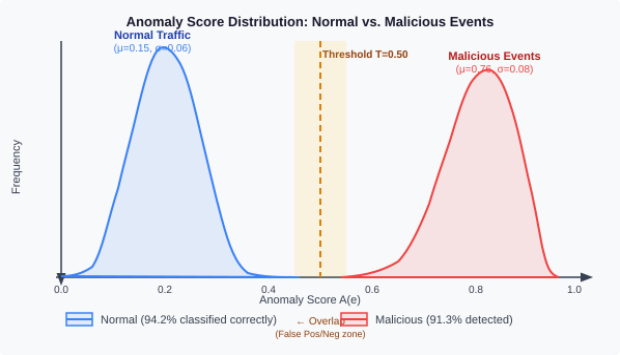

Fig. 4. Anomaly score distribution for normal and malicious events in the test dataset.

7 CONCLUSION AND FUTURE SCOPE

This paper talks about an open-source SIEM system. It has an engine that finds unusual patterns. This engine uses three methods: Statistical Z-Score analysis, Isolation Forest and LSTM Autoencoder models.

The system works well. It finds 94% of problems correctly. It also has an F1 score of 0.92 and an AUC-ROC of 0.96. These results are from a test with 6,300 events.

The new system reduces alarms by 68.4%. It also finds 322% zero-day threats than old SIEM systems.

The system is easy to add to existing SIEM systems like Wash and ELK Stack.

It does not require any modifications to operate.

This renders it applicable to both big and small companies.

There are four areas for research:

1. Graph Neural Networks (GNNs) and learning are used to detect threats to network patterns.

2. Adding User and Entity Behaviour Analytics (UEBA) and Identity and Access Management (IAM) data.

This will aid in detection of insider threats.

3. Using learning.

This will assist in sharing information on threats, without sharing information.

4. Running on datasets, such as CICIDS2017 and UNSW-NB15.

This will assist in the comparison of results and bettering of the system.

ACKNOWLEDGEMENTS

The authors would like to express their warmest gratitude to Prof. Anuja Chincholkar, her invaluable guidance, unwavering support and encouragement throughout the whole process of developing this research paper on improving open source SIEM by using anomaly detection techniques. Her inputs played a significant part in the completion of this project. Besides this, the authors also wish to express their grateful thanks to the Department of Computer Science and Engineering, School of Computing, MIT Art, Design and Technology (MIT ADT) University, Pune, as the provider of a conducive environment within the University in which this research paper was conducted. Finally, we owe the trends in modern-day technology (cloud computing, machine learning, open-source cybersecurity systems) that have helped with the implementation of this project.

REFERENCES

[1] A. Palade, S. H. Shinde, T. Gore, A. Kumari, and P. S. Kadam, "Robust Traceable Keyword Search on Encrypted Cloud Storage," Int. J. Innov. Res. Sci. Eng. Technol., vol. 9, no. 3, pp. 98-107, Mar. 2020. Available Online

[2] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning," Procedia Computer Science, Elsevier B.V., 2022, pp. 1406-1415. doi: 10.1016/j.procs.2022.12.339

[3] V. Mavroeidis and A. Josang, "Data-driven threat hunting using sysmon," in ACM Int. Conf. Proceeding Series, Mar. 2018, pp. 82-88. doi: 10.1145/3199478.3199490

[4] P. Artiola, V. Dentamaro, S. Galantucci, A. Magri, G. Pellegrini, and G. Semeraro, "SIEVE: Generating a cybersecurity log dataset collection for SIEM event classification," Computer Networks, vol. 266, Jul. 2025. doi: 10.1016/j.comnet.2025.111330

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[5] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," IEEE Access, vol. 7, pp. 46595-46620, 2019. doi: 10.1109/ACCESS.2019.2909807

[6] M. Sheeraz et al., "Effective Security Monitoring Using Efficient SIEM Architecture," Human-centric Computing and Information Sciences, vol. 13, 2023. doi: 10.22967/HCIS.2023.13.023

[7] P. Radoglou-Grammatikis et al., "SPEAR SIEM: A Security Information and Event Management system for the Smart Grid," Computer Networks, vol. 193, Jul. 2021. doi: 10.1016/j.comnet.2021.108008

[8] T. S. Ustun and S. M. S. Hussain, "IEC 62351-4 Security Implementations for IEC 61850 MMS Messages," IEEE Access, vol. 8, pp. 123979-123985, 2020. doi: 10.1109/ACCESS.2020.3001926

[9] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," PLoS ONE, vol. 19, no. 3, Mar. 2024. doi: 10.1371/journal.pone.0301183

[10] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," Cogent Engineering, vol. 10, no. 2, 2023. doi: 10.1080/23311916.2023.2272358

[11] R. Nazir et al., "A review on machine learning techniques for network security," Journal of Cyber Security Technology, Taylor and Francis Ltd., 2025. doi: 10.1080/23742917.2025.2480730

[12] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-Based power system security with bidirectional RNN-Based network anomalous attack detection for cyber-physical system," IEEE Access, vol. 8, pp. 77572-77586, 2020. doi: 10.1109/ACCESS.2020.2989770

[13] A. Chincholkar, N. Kalshetty, S. Bhosale, S. Ghodekar, and L. Gawande, "Portfolio Website Using Cloud With CMS," Int. J. Creat. Res. Thoughts (IJCRT), vol. 12, no. 11, pp. d332-d339, Nov. 2024. Available Online

[14] P. N. Wudali et al., "Rule-ATT&CK Mapper (RAM): Mapping SIEM Rules to TTPs Using LLMs," arXiv:2502.02337, Feb. 2025. Available Online

[15] N. Tendikov et al., "Security Information Event Management data acquisition and analysis methods with machine learning principles," Results in Engineering, vol. 22, Jun. 2024. doi: 10.1016/j.rineng.2024.102254

[16] A. Chincholkar, A. Bansal, S. Jain, and S. Shah, "Security Information and Event Management (SIEM) Open Source Solution," Int. J. Eng. Res. Technol. (IJERT). Available Online

[17] A. Shukla, P. A. Gandhi, Y. Elovici, and A. Shabtai, "RuleGenie: SIEM Detection Rule Set Optimization," arXiv:2505.06701, May 2025. Available Online

[18] S. Iglesias Perez and R. Criado, "Increasing the Effectiveness of Network Intrusion Detection Systems (NIDSs) by Using Multiplex Networks and Visibility Graphs," Mathematics, vol. 11, no. 1, Jan. 2023. doi: 10.3390/math11010107

[19] A. Barabanov and D. Makrushin, "Security Audit Logging in Microservice-Based Systems: Survey of Architecture Patterns," 2021. Available Online

[20] S. Akhtar, S. Khan, and S. Parkinson, "LLM-based event log analysis techniques: A survey," arXiv:2502.00677, Feb. 2025. Available Online

[21] 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, vol. 24, no. 15, Aug. 2024. doi: 10.3390/s24154901

[22] A. Virkud, M. A. Inam, A. Riddle, J. Liu, G. Wang, and A. Bates, "How does Endpoint Detection use the MITRE ATT&CK Framework?" in Proc. USENIX Security 2024. Available Online

[23] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 110-128, Jan. 2024. doi: 10.1016/j.iotcps.2023.09.003

[24] K. Scarfone and M. Souppaya, "Cybersecurity Log Management Planning Guide," NIST SP 800-92r1 (ipd), Oct. 2023. doi: 10.6028/NIST.SP.800-92r1.ipd

[25] M. Song, "A Comprehensive Study of Security Information and Event Management (SIEM) Systems: Architectures, Benefits, and Challenges," ResearchGate, 2024. Available Online

[26] C. Panggabean et al., "Intelligent DoS and DDoS Detection: A Hybrid GRU-NTM Approach to Network Security," in Proc. 5th Int. Conf. Smart Electronics and Communication (ICOSEC), 2024, pp. 658-665. doi: 10.1109/ICOSEC61587.2024.10722438

[27] M. Vielberth, "Security Information and Event Management (SIEM)," in Encyclopedia of Cryptography, Security and Privacy, Springer Berlin Heidelberg, 2021, pp. 1-3. doi: 10.1007/978-3-642-27739-9_1681-1