Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Unaddressed Limitations in Security Information and Event Management (SIEM) Systems

Anousha Amir
Department of Computer Science (Cyber Security) ILMA University, Main Ibrahim Hyderi Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan
Email: aanousha783@gmail.com

Muhammad Sammak Anjum
Department of Computer Science, (Cyber Security) ILMA University, Main Ibrahim Hyderi Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan
Email: sammak946@gmail.com

Humaiz Shaikh
Department of Software Engineering, ILMA University, Main Ibrahim Hyderi Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan Email: humaiz0416@gmail.com

Faraz Ahmed Shaikh
Office of Quality Enhancement Cell, Dawood University of Engineering and Technology, Karachi, Sindh, Pakistan Email: dr.humaiz@ilmauniversity.edu.pk

ABSTRACT

Security Information and Event Management (SIEM) systems are the base for enterprise Security Operation Centers (SOCs); however, they are faced with three main overlapping weaknesses: lack of context to provide alerts about potential threats, inadequate rule-based approach to detect insider threat and alert fatigue due to too many alerts. Lots of solutions have been offered to cope with these problems; however, there is no comprehensive model that can meet all these demands. The model offered in this paper consists of four layers that improve existing SIEMs without replacing the platform. The first layer describes the components of data used by SIEMs. The second layer offers an approach to improve alerts based on the concept of kill chain. The third layer uses unsupervised machine learning methods, specifically Isolation Forest and One-Class SVM to detect insider threat. The fourth layer improves the traditional two-level alerts' model by introducing five levels of alerts. SOC improvement on the grounds of the feedback mechanism principle. The model is evaluated in light of four defined aspects and its theoretical consistency and practical feasibility are studied. The analysis proves that the multi-level structure provides a solution to all the discussed challenges in an integral and cumulative manner. Therefore, it could be considered as a novel theoretical achievement in the area of SIEM and insider threats research. The next step will consist in practical validation of the approach in real businesses

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Keywords: SIEM, Insider Threat Detection, Alert Fatigue, False Positive Management, Killchain Classification, Isolation Forest, Machine Learning, Security Operations Center, Behavioral Biometrics, Anomaly Detection.

Introduction

Background and Context

Today's world of cyber security has transformed into an unstable environment from being stable previously. All organizations across different sectors experience advanced attacks. The Security Information and Event Management (SIEM) system plays an important role in the overall protection strategy developed by the firm. It works as the key component of the Security Operation Centers (SOCs), collecting data from all network sources (including firewalls, intrusion detection systems, end-point sensors) for correlation of security events.

However, at the same time, although they are of great importance, modern SIEMs have certain weaknesses. According to Bryant & Saiedian [1], one of the main problems of traditional SIEM solutions is a huge number of alerts, which usually do not provide the necessary context and information on the connection between particular events and a certain stage of a cyber attack. This leads to alert fatigue, which means that security experts get a lot of alerts, and they can no longer understand if particular alerts indicate the presence of danger or it is just noise. Moreover, there is constant criticism of a binary nature of SOC activities, in which all the false alerts are divided into one group of “false positives,” which results in bad practice of continuous improvement and poor understanding of the situation in the organization [2].

Insider threat problem is another critical component of this matter. Since insiders are able to utilize legitimate credentials and are familiar with internal infrastructure specifics, their malicious activities such as stealing information, violating permissions, damaging IT infrastructure or robbing money are almost impossible to distinguish from regular operations when analyzing the process in terms of perimeters protection [3]. Numerous studies have been performed in order to develop the appropriate anomaly detection system, but the empirical evidence proves that most of them were created using simulated data that did not manage to capture the real complexity of processes and logging schemes as well as behavioral changes that could be observed in real world [3].

In this respect, AI and ML have opened up a possibility to address the existing challenges. In the opinion of researchers such as Komka et al. [6] and Mohamed and Arabo [7], the unsupervised learning algorithms such as Isolation Forest, as well as calibrated one-dimensional Convolutional Neural Network (1D-CNN), can be implemented into the operational SIEM systems in order to improve the anomaly detection mechanism and decrease false positive rates. However, despite the mentioned approaches have already proven themselves to be efficient, there are still some challenges to be overcome including model calibration, thresholding, alert budgeting, and human-machine collaboration.

As the recent research indicates, fighting the alert fatigue requires more than technological innovation; we need to revise the role of an analyst within a Security Operation Center (SOC). As Tariq et al. [5] point out, the three main components of a

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

modern SOC are automation, augmentation, and human-machine cooperation and, nowadays, there is no way to effectively solve the problem of analyst fatigue. Based on the information collected, we can conclude that the solution to the problem should involve a number of different strategies including ICMs and incident classification along with the human-machine cooperation development.

Problem Statement

Despite the SIEM solution becoming an integral part of the enterprise's security monitoring process, there is still a gap in how the SIEM systems operate. The challenge in updating the alert management approach in order to improve the threat detection process remains persistent.

The limitations of the existing alert management practices are evident in the following three aspects:

First, the traditional SIEM architecture relies heavily on the static nature of rule-based correlation, which does not contain sufficient data to contextualize the alerts within a particular perspective of the incident under analysis as Bryant and Saiedian [1] demonstrate.

Secondly, the detection of insider threats in SIEM tools is far from being efficient. Erola et al. [2] proved that standard SIEM tools used in a sandboxed environment are unable to identify insider threats because they generate numerous false alerts, as well as having inefficient risk scoring and poor log context. There are machine learning solutions which in theory could solve this problem; however, in practice, the efficiency of these solutions has not been tested yet in the corporate environment.

Thirdly, the problem of alarm fatigue is now widespread in the field of security operations, affecting employees' performance negatively. Inadequate use of detection tools, inability to categorize incidents, and lack of integration between AI and people contribute to this problem creating an enormous cognitive load on people [2], [5]. Literature review reveals the gap in the current state of affairs as the literature lacks the solution of this problem**.**

Research Objective

The objective of this research is to establish a comprehensive SIEM based framework with the implementation of machine learning techniques in order to enhance the precision rate of detecting insider threat cases, and at the same time reduce the number of false positives and alert fatigue of the analysts in Security Operations Centers.

Research Contributions

The contributions that are made in the field of enterprise information security and threat detection using SIEMs by this article are the following. **Conceptual contributions could involve such things as:**

The author provides the framework that is composed of four layers including events occurring during the process of kill-chain and incorporated in alerts generated by SIEMs. Therefore, such approach provides an opportunity to consider the situation in its comprehensive context.

The research findings demonstrate a comparative overview of two different

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

unsupervised machine learning techniques for detecting insider threats within SIEMs: Isolation Forest and One-Class SVM. It should be noted that better results were provided by Isolation Forest having the highest F1-score and control of false positives.

The author presents a more sophisticated classification of alerts including five categories of alerts' effect in contrast to the traditional classification of alerts by their true or false positiveness which helps perform root cause analysis of the wrong alerts in the future.

The author presents the principles of analyst-oriented design of SIEM dashboards including behavioral biometrics and enterprise log analysis providing non-specialists with the required information without the deep study of technology.

Significance of the Study:

The current research is relevant and makes a substantial contribution to the academic field and practice. First of all, the research incorporates the current knowledge on the threat detection using SIEM and creates the integrated model that allows overcoming the problem of the gap between offline machine learning research and the realities of SOC work, which was highlighted as one of the most urgent problems [3], [7]. On the other hand, the findings of the current research can be used by security engineers, SOC managers, and CISOs in order to use the knowledge gained from it in designing new intelligent SIEM systems that will contribute to the protection of cognitive health of security professionals.

LITERATURE REVIEW

Introduction to the Literature Review

Taking into account that nowadays there has been a rise in the number of cyber-attacks on the business infrastructure, the issue of security monitoring can also be considered an enterprise and technical one. It is essential to point out that the relevance of the necessity to implement SIEM cannot be overlooked, since they have been improving for the last twenty years, yet there are some drawbacks in the work of these tools. Nevertheless, the answer to the following four interconnected questions will help to clarify the matter. The first one concerns the features and shortcomings of SIEM, the second one deals with the notions of alarm fatigue and false positives, the third one – with insider threats, and the fourth one – with machine learning.

This review draws on seven peer-reviewed and empirically grounded studies to map the current state of knowledge, identify where consensus exists, and pinpoint the gaps that this research directly responds to. The reviewed studies are summarized in

TABLE I
Table 1: SUMMARY OF REVIEWED LITERATURE

Ref	Authors	Year	Focus Area	Key Finding	Relevance to Study
[1]	Bryant & Saiedian	2020	SIEM alert classification	Kill-chain mapping improves alert context and prioritization	Informs Layer 2 of proposed framework

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

[2]	Sacher	2020	False positive management	Binary classification suppresses continuous improvement	Informs Layer 4 categorization scheme
[3]	Erola et al.	2022	Insider threat detection	Real-world data exhibits higher variance than synthetic datasets	Highlights ML validation gap
[4]	González-	2021	Transformation Of	In order for SIEM to	Limitation of SIEM
	Granadillo et al.		SIEM	remain efficient, it has to work with AI and SOAR	
[5]	Tariq et al.	2025	Alert fatigue at SOC	Automation and collaboration between human intelligence and AI are very important	Guide to analystoriented method
[6]	Komka et al.	2025	Insiders' threats identification by machine learning	Isolation Forest algorithm performs better than OneClass SVM in terms of F1score	Guide to third-layer modeling
[7]	Mohamed & Arabo	2025	Prototype of machine learning SIEM	Thresholded 1D-CNN models do not generate false positives	Guide to third- and fourth-layer designs

SIEM Systems: Role, Limitations and Evolution

Security Information and Event Management (SIEM) solutions have been serving as the backbone of threat detection at enterprises for several years now, providing access to the data from logs and security incidents across an entire company within one pane of glass. However, there is no doubt about the disadvantages of traditional SIEM solutions. González-Granadillo et al. claim that traditional SIEM solutions lack capabilities such as incomplete visibility of the data, simple correlation techniques based on boolean logic, and human interaction, which leads to a slower reaction to incidents, potential miss of threats, and more false alarms. What is more, the authors state that unless advanced analytic capabilities and automation are implemented in SIEM systems, they will not be able to solve the problem of prevention but will serve to react to threats.

The criticism of Bryant and Saiedian touches upon the fact that traditional SIEM solutions lack contextual analysis of the alerts. Their research shows that linking the alert to its location in the attack life cycle makes it possible to see how an attack develops, and it is impossible with the help of traditional SIEM solutions

Alert Fatigue and False Positive Management

Nowadays, the task of handling the constantly growing number of alarms generated by SIEM systems is among the most complicated ones for modern security operations centers. As Tariq et al. state [5], this is a problem of the system-wide nature caused by

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

the increasing number of alarms and resulting in even greater cognitive load for security analysts and leading eventually to the negative consequences such as burning out, lack of vigilance, and decreased detection quality. Tariq et al., however, point out that the three components of the solution to this problem are automation, augmentation, and collaboration between people and artificial intelligence, but the current solutions are still not sufficient. This is explained, among other things, by the traditional approach to classification of false alarms used by SOCs. Thus, Sacher [2] states that grouping various incidents under the label of "false positive" is wrong and even detrimental to the security processes. It is important to distinguish between configurations errors, detection rules mistakes, unannounced administration actions, and actual attacks for getting all the required information about the process of operation. For doing this, Sacher [2] suggests using a special taxonomy built according to the lessons-learned methodology of the NIST 800-61 document.

Insider Threat Detection within SIEM Environment

The most challenging threat faced by an organization is the insider threat simply because in this situation the attacker operates inside, meaning he uses legitimate credentials, knows the systems, and follows normal access procedures to blend into normal organizational operations. Erola et al.
[3] highlight that while considerable academic effort has gone into conceptualizing insider behavior and proposing automated detection systems, the vast majority of these solutions have been tested exclusively on synthetic datasets. Their deployment of the Corporate Insider Threat Detection (CITD) tool across three multinational organizations over six months revealed that real-world behavioral data exhibits significantly higher variance than synthetic equivalents — a finding that calls into question the practical reliability of many previously proposed detection models.
The distinction in the behavior of SIEM systems under laboratory tests and in reality has been thoroughly investigated by Komka et al. [6]. They have shown that the SIEM systems currently being used are unable to detect the danger of an insider attack since they rely on static correlation, which is incapable of recognizing any behavioral change. There has been a definite proof that in order to recognize such threats, dynamic detection mechanism needs to be implemented.

Machine Learning Integration in SIEM

The limitations of rule-based detection have driven growing interest in embedding machine learning directly into SIEM workflows. Komka et al. [6] evaluated two unsupervised models — Isolation Forest and One-Class SVM — against four insider attack scenarios using the CERT Insider Threat Dataset. According to their research, the Isolation Forest was significantly more effective in finding the right balance between detecting malicious behavior and handling false positives, as its F1-score amounted to 0.92 in comparison with the One-Class SVM, which featured quite a large number of false positives.
The next step in the research is associated with the work of Mohamed and Arabo [7]. The researchers proposed the architecture of a calibrated 1D-CNN algorithm that operates in the environment of the Splunk Machine Learning Toolkit. The algorithm uses enterprise logs along with the behavioral biometric data, implementing various

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

approaches to eliminating false positives. It should be noted that the developed dashboard allows for changing the thresholds for alerts without any knowledge of AI systems.

Summary and Research Gap

In this chapter, the literature review will examine the full picture of what goes on in a sector which faces constant structural issues. Although SIEM technology is vital in terms of security processes within an enterprise, it still falls short of three key components – understanding the context of alerts, preventing insider threats, and alert processing over time by personnel. González-Granadillo et al. [4] perfectly describe this concept saying that participants in the market should understand that the new generation of SIEM solutions should incorporate big data, artificial intelligence, and SOAR.

What the existing body of work has not yet produced, however, is an integrated and empirically validated framework that addresses all three dimensions simultaneously — one that combines intelligent alert classification, machine-learning-based behavioral anomaly detection, and analyst-centric false positive management within a single unified SIEM architecture. This gap forms the direct foundation of the present study.

The Research Method

Research Design

This study relies solely on a theoretical/conceptual perspective. The aim here is to put together the knowledge that already exists in order to build a framework aimed at improving the detection of insider threats and solving the false positive problem within Security Operation Centers utilizing SIEM technologies. Unlike gathering data empirically, this study critically analyzes the important aspects of scholarly articles conducted by others to identify the gaps between theory and practice in relation to the problem under investigation. This design is appropriate given that the primary contribution of this research is a framework proposal rather than an experimental outcome.

Research Approach

From the outset, deductive approach will serve as the foundation of this research. The corresponding theoretical framework, namely the kill-chain based model of alerts categorization, unsupervised machine learning approaches and incident classification technique has been derived from the literature sources and is utilized systematically for the construction of the research framework. Thus, in such case, the researcher can logically proceed from the known material to the research that has not been solved before by the other scholars.

Research Philosophy

The interpretation theory has been employed in this study as a philosophical framework for the research. It is because this research does not seek to generalize any of its findings. On the contrary, this research seeks to interpret and synthesize diverse theoretical concepts to get deep insights.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Literature-Based Data Collection

Since no primary research was conducted in this study, peer-reviewed literature was used in this study. Selection of the seven empirical and theoretical studies was made in accordance with the process of reviewing the literature. This process of reviewing was based on the consideration of those studies that address issues related to the SIEM limitations, detection of insider threats, alert fatigue, and use of machine learning in the management of SOCs.

Framework Development Process

The theoretical framework of the current study is designed through three stages. The first stage involves the identification of different channeling challenges that have been established in the literature review. These involve lack of context-based alert, failure to detect insiders, and alert fatigue, amongst others. After successful identification of more problems, parts of the proposed solutions that are seen to be the most effective are selected. This involves aspects such as anomaly detection via Isolation Forest approach, alert enrichment based on the Kill Chain approach, and threshold dashboard for the analyst. The final stage of the process entails evaluating the proposed theoretical framework through the provision of answers to the research questions formulated.

Evaluation Criteria

Since this research does not involve experimental testing, the framework is evaluated against three conceptual criteria drawn directly from the literature: detection effectiveness, defined as the theoretical capacity to identify insider threat anomalies with greater accuracy than rule-based systems; false positive reduction, assessed by examining how the proposed categorization model addresses the root causes of alert misclassification identified by Sacher [2] and Tariq et al. [5]; Feasibility of operations has been considered too, which is determined by checking whether the elements present in the proposed framework can be used in the presently available SIEM frameworks without needing any expertise in machine learning.

Ethical Considerations

Given that human subjects are not involved in the research undertaken, there is little risk of ethical issues arising from the research carried out. All sources that have been mentioned and cited in this research are peer-reviewed and publicly available in nature; hence, no confidential information or proprietary data have been employed in this research endeavor. Where the reviewed literature references real organizational deployments — such as the multinational case studies in Erola et al. [3] — this research engages only with the published findings and draws no conclusions beyond what the original authors report..

Research Limitations

The primary limitation of a conceptual research design is the absence of empirical validation. As of now, there is no real-life performance evaluation done for the proposed framework since the framework has not been tested using any practical SIEM data and implemented within the actual SOC environment. In other words,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

there is dependency on the existing literature to support the current scope of research. It would be appropriate to proceed to the stage of testing and implementing the framework in future researches to prove its efficiency in the real-life business environment.

RESEARCH METHODOLOGY

Overview

Within this chapter, I am going to prove the main contribution of my research – the creation of a conceptual framework that includes multiple layers and is focused on overcoming three major shortcomings identified within the literature review, such as the lack of possibility to inform the environment about the threat, the inability to identify the insider threats and the issue of alert fatigue. As opposed to introducing a series of isolated solutions to individual problems, the framework that I am offering includes multiple layers created on the basis of the existing SIEM system and capable of being integrated with it without replacing it.

Framework Architecture

The architecture has been divided into four levels wherein each level depends on the results obtained at the previous level: Level 1: SIEM foundation; Level 2: Kill chain alerts enrichment; Level 3: ML-based anomaly detection; and Level 4: Analyst based response and categorization. The entire framework architecture has been depicted in.

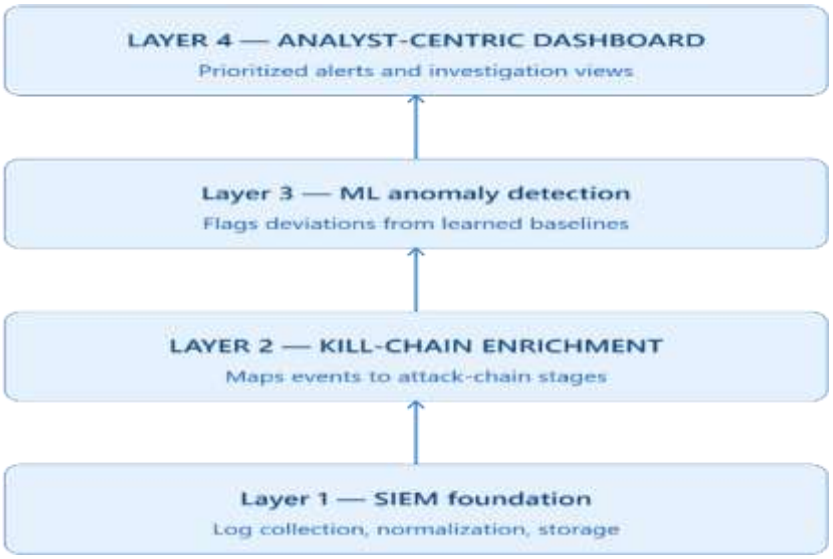

Fig. 1. Proposed four-layer SIEM augmentation framework architecture

Layer 1: SIEM Foundation

The first layer describes the existing SIEM solution of the company and it may be Splunk, IBM QRadar or any other system which operates in common conditions. Logs are collected at this stage from the whole company infrastructure, including network devices, endpoint sensors, and authentication systems and so on. This layer is used solely for the purpose of data collection and normalization; there is no addition

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

of intelligence in this layer at all. It is imperative to mention the fact that this layer of the system has been designed in such a way that it is completely platform independent, which means that this system could be implemented in any SIEM regardless of its architecture.

Layer 2: Kill-Chain Alert Enrichment

Phase two consists of the application to this alerting pipeline of the concept of contextual intelligence in order to correlate the incoming alerts of the SIEM with the phases of the cyber kill chain, namely: information gathering, weaponization, delivery, exploitation phase, installation, command & control phase, and the exfiltration phase. This layer relies on the schema provided by Bryant and Saiedian in their work and which adds more metadata to the alerts in order to classify them according to their relationship with the events of a possible attack. In this way, analysts would not just get a set of random events, but the process of the completion of actions. Enrichment will be used to introduce a score to the alerts according to the phases of the killing chain which was just mentioned

TABLE II illustrates the mapping of kill-chain stages to corresponding SIEM alert types and assigned priority levels.

TABLE 2: KILL-CHAIN STAGE TO ALERT TYPE MAPPING

Kill-Chain Stage	Example SIEM Alert Type	Priority Level
Reconnaissance	Port scanning, DNS enumeration	Low
Weaponization	Malicious file creation, script compilation	Low-Medium
Delivery	Phishing email detection, malicious attachment	Medium
Exploitation	Privilege escalation attempt, buffer overflow	High
Installation	Unauthorized software installation, rootkit detection	High
Command & Control	Unusual outbound traffic, beaconing behavior	Critical
Exfiltration	Large data transfers, unauthorized cloud uploads	Critical

Layer 3: ML-Based Anomaly Detection

The third layer embeds unsupervised machine learning directly into the enriched alert stream, targeting the insider threat detection gap that rule-based SIEM logic cannot close. Based on the comparative findings of Komka et al. [6], Isolation Forest algorithm has been applied in this layer as a primary detection engine due to its ability to detect subtle behavior anomalies. The second layer applied in this case is One-Class SVM algorithm, which is a filtering technique. This technique is applicable only for those alerts which have been detected by Isolation Forest algorithm using medium

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

confidence level. This creates a multi-level detection technique where sensitivity and accuracy is balanced.Along with this, behavioral biometric data, such as data access time, keystrokes and speed of data transfer, has been considered.[7]. These cues offer the user-level behavioral context that raw log data does not provide, greatly enhancing the capability of the model in determining real insider threats from mere behavioral variations. The comparison between the two ML models is shown in **TABLE 3**.

TABLE 3: COMPARISON OF ML MODELS FOR INSIDER THREAT DETECTION

Criteria	Isolation Forest	One-Class SVM
Algorithm Type	Unsupervised	Unsupervised
F1-Score (CERT Dataset)	0.92	Lower
False Positive Rate	Low	Higher
Computational Complexity	Low-Medium	Medium-High
Scalability	High	Moderate
Role in Framework	Primary detection engine	Secondary investigative filter
Source	Komka et al. [6]	Komka et al. [6]

Layer 4: Analyst-Centric

At the highest level, there is a focus on the human side of the system, which entails the interplay between the intelligent detection pipeline and the security analyst who makes the final decision regarding the actions to be taken. From the dashboard seen by the security analyst, the MLscored alerts are shown, and here the analyst can manually set the detection threshold without any knowledge of ML. This principle is concerned with the issues of usability as identified by Mohamed and Arabo [7] and strives towards the wee via this approach, but this time empowering a human analyst rather than alienating him. This level replaces the conventional binary classification scheme of true/falsely positives by the more complex scheme introduced by Sacher [2].Every resolved alert is classified into one of several structured outcome categories rather than being dismissed as a generic false positive. These categorized resolutions feed back into the detection pipeline as structured operational intelligence, enabling continuous improvement of both the kill-chain enrichment rules and the ML model's threshold calibration over time. The proposed granular alert categorization scheme is detailed in TABLE 4.

TABLE 4: PROPOSED GRANULAR ALERT CATEGORIZATION SCHEME.

Category	Definition	Recommended Action
Confirmed Malicious Activity	Alert corresponds to verified attack behavior	Immediate escalation and incident response
Misconfigured Detection	Alert triggered by poorly defined correlation rule	Rule reviewed and updated

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Rule		
Unannounced Administrative Action	Legitimate IT activity not communicated to SOC	Communication protocol enforced
Confirmed Benign Anomaly	Unusual but non-threatening user behavior	Logged for behavioral baseline update
Insufficient Data	Alert cannot be classified due to missing log context	Log coverage reviewed and expanded

Framework Summary

Taken together, the four layers address each of the research questions posed in Chapter 1. The kill-chain enrichment layer responds to RQ1 by providing contextual alert intelligence. The ML anomaly detection layer responds to RQ2 by offering an empirically grounded approach to insider threat identification. For RQ3, the use of the granular classification scheme becomes an alternative to the binary classification scheme, whereas for RQ4, the analyst-focused dashboard enables non-experts of security to manage the system easily. The multi-layered architecture guarantees that all components do not work in isolation but rather complement the performance of the layer above them, thus resulting in an overall enhancement of detection accuracy, false positives handling, and efficiency of analysts that cannot be provided by any other system in existence today.

DISCUSSION

Overview

This chapter is a critical evaluation of the conceptual framework introduced in Chapter 4 relative to the research questions, objectives, and research gaps highlighted in the literature review. While the previous chapter highlights the results from experimental work, this chapter questions the theoretical validity and practical applicability of each level of the conceptual framework based on the literature review. TABLE 5 is an evaluation of the proposed conceptual framework relative to each research question

TABLE 5: FRAMEWORK EVALUATION AGAINST RESEARCH CONTRIBUTIONS

Contribution	Framework Layer	How it is Delivered
C1: Kill-chain alert Enrichment	Layer 2	Alerts mapped to kill-chain stages; priority escalation applied to advanced attack stages
C2: ML model comparative evaluation	Layer 3	Isolation Forest selected as primary engine based on superior F1-score; One-Class

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

		SVM as secondary filter
C3: Granular alert categorization scheme	Layer 4	Five-category outcome scheme replaces binary true/false positive model
C4: Analyst-centric dashboard design Principles	Layer 4	Threshold-adjustable interface designed for non-specialist analysts

Addressing the Contextual Alert Deficiency

The initial and fundamental challenge highlighted from the literature review is that of standard SIEM systems failing to offer context around any generated alerts. Bryant and Saiedian [1] have made the point quite clear that in absence of mapping the alerts to an attack progression framework, the analyst is forced to interpret each individual event in isolation - a process which makes it difficult for them to detect real threats.

The kill-chain mapping layer used in this framework attempts to address this very challenge. By placing each and every alert in the perspective of a known attack progression phase, this framework helps convert basic data into actionable intelligence. Further, by including the priority escalation component, it also makes sure that those alerts which represent more advanced stages of the attack get processed first. As far as the theory goes, this concept is quite well-founded; however, the challenge for future research will be in assessing how effective this automatic mapping of the kill-chain is in different types of enterprise logs with different types of alert metadata.

Closing the Insider Threat Detection Gap

The most alarming result of the reviewed literature is obtained by Erola et al. [3], who state that insider threat detection algorithms trained and tested on the basis of synthetic data often prove to be ineffective when applied to real organization data. The importance of this statement should not be underestimated, as it refers directly to the ML detection layer of the presented framework, which relies on the results of the CERT Insider Threat Dataset study carried out by Komka et al. [6].

One of the motives for choosing the Isolation Forest method as the main instrument is its ability to give a good performance on high-dimensional behavioral data while producing fewer false alarms than One-Class SVM. Nonetheless, the authors of the considered methodology admit that the true power of the algorithm can only be shown through empirical research using real data of organizations' behavioral logs.[3] The utilization of behavioral biometric variables as additional features according to the paper of Mohamed and Arabo [7] mitigates this problem to some extent

Reforming False Positive Management

Tariq et al. [5] has documented that alert fatigue issues are not just pure technological problem and also include a classification and workflow problem. In this regard,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Sacher [2] also affirms that the use of only the binary model of true positive/fake positive is crucial because organizations are deprived from important learning opportunities when it comes to analyzing their alerts. Any alert, which is turned down as a false one, means lost chances for operational improvement.

The detailed classification mechanism that represents the highest layer of the framework solves this problem. It makes sure that different types of intelligence are being produced constantly, as analysts are required to categorize all resolved alerts based on their outcomes. This model of feedback loop is the most advanced one and means that alert detection system is developed and upgraded all the time

Practical Feasibility and Adoption Considerations

While the idea itself seems perfect theoretically, it would be of no use in practice if the framework is not feasible. Let us consider the following three aspects of feasibility.

First, the framework operates under the assumption that the organization creates logs of appropriate quality and completeness for both kill chain enrichment and machine learning-driven anomaly detection. González-Granadillo et al. [4] find out that the quality and completeness of log information vary greatly in enterprise environments and in particular if the organization uses legacy systems or heterogeneous networks.

Second, the dashboard-oriented approach requires certain level of organizational readiness, that is, the ability of SOC teams to adjust thresholds and classify findings. In cases when there is a lack of staff or other resources in the Security Operations Center (SOC) framework, the most efficient tools may overload the system. It happens due to specific complications associated with security issues and some additional difficulties like budgeting problems. There are no detailed actions for implementing the suggested model. However, it can be viewed as the weakness and strength of the SOC framework since there are no instructions that are important for implementation strategy at the same time

Framework Coherence and Research Objective Alignment

Thus, it can be concluded that the developed framework demonstrates very good theoretical integration. Each layer compensates for some weakness, each design decision is substantiated by literature, and layers are integrated in such a manner that compound benefits are gained rather than standalone ones. However, the most important thing is that the framework meets the main purpose of this research. This is development of a common architecture based on SIEM with machine learning techniques used for detecting insider threats more accurately and avoiding false positive detections and alert fatigue of analysts. No other work analyzed in this paper offered anything like this and, thus, this framework can be called an intellectual contribution indeed.

RESEARCH METHODOLOGY

Summary of the Study

The objective of this work was to offer solutions to a serious, widely reported operational challenge which is being faced by enterprise Security Operations Centers - the simultaneous shortcoming of existing SIEM platforms in providing context-

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

based alert intelligence, accurate detection of insider threats, and dealing with alert volumes in a way acceptable to analysts. This paper engages in systematic analysis of the seven scholarly sources and formation of a four-layer conceptual framework that contributes to the formulation of theoretically grounded solutions to these interrelated challenges.

The analysis of the existing works revealed that these challenges are not independent. Alert fatigue is partly a result of improper contextual classification. As for the detection failure of insider threats, it is exacerbated by excessive reliance on rule-based logic that cannot catch the subtle shifts in behavior. Moreover, the existing true/false positive model hinders continuous improvement of the system capable of solving the two problems simultaneously. The study sought to reveal the described dependence of the layers on each other and to integrate all the layers so that not only the solutions to the respective problems were found but also those of the accompanying issues.

Research Contributions Revisited

All four contributions which were discussed in Chapter 1 have been implemented according to the specified framework. The first contribution, which is known as kill-chain alert enhancement, has been achieved by Layer 2, which showed in theory how the alert contextualization, referring to the phases of attack progression, leads to better prioritization along with reducing noise in investigations. The second contribution was achieved using Layer 3, where the comparison between Isolation Forest and One-Class SVM took place, enabling the analysis which proved that Isolation Forest is the best technique to be used for detection as it displayed the highest F1score, thus proving Komka et al.[6] statements correct. The third contribution, known as the detailed alert categorization system, was presented using Layer 4, where the binary classification model was replaced by a system of structured outcomes, enabling root cause analysis and feedback for further improvements. The last contribution is the design principles, which ensures the dashboard architecture of Layer 4 and enables the threshold adjustments and alerts management for non-expert specialists without requiring any machine learning skills

Contributions of the Study

The contributions of this research study can be divided into two categories. The first category is theoretical contribution, where this research integrates findings from various fields of study, including SIEM system development, insider threat detection, and alert management, to provide a novel schema that has not yet been provided in existing literature. The practical contribution of this research is providing professionals involved in MIS management, SOC authorities, and security officers with a professional guide on how to enhance existing SIEM systems

Limitations

One clear limitation of the current study is the lack of any empirical validation. The model has been only tested and validated on theoretical basis and not practically in terms of how effective the model is and how efficient it is in generating less number of false alarms. It should be noted that the model relies on the findings of the study

Online ISSN 3007-3197
Print ISSN 3007-3189

conducted by Komka. [6] means its ML layer recommendations are bounded by the characteristics of that dataset, which may not fully represent the behavioral complexity of all enterprise environments as cautioned by Erola et al. [3].

Recommendations for Future Research

Three directions for future research emerge directly from this study's limitations.Firstly, the suggested approach needs to be applied in practice and verified within an actual enterprise SIEM environment – preferably in different companies in order to test its resilience and applicability. Secondly, the efficiency of automated mapping needs to be researched as part of the kill-chain enrichment stage aiming to find ways of more effective collaboration with different and inconsistent log sources. Lastly, longitudinal research examining the impact of the feedback loop created with the help of granular categorization on the quality of the threat detection rules and adjustment of machine learning models over a long period of time would immensely improve the process of verification and implementation of the framework.

Closing Remarks

The threat environment within the field of cybersecurity is only expected to increase in terms of its complexity and magnitude. It is true that SIEM solutions are likely to stay central in enterprise-level defense – at least for the time being – but their current state is inadequate. As per the present study, rather than upgrading from the existing platform, it is better to add various layers of context, machine learning, and analyst-driven design to them. Such an effort needs to be studied further and employed in any future empirical studies.

References

[1] B. D. Bryant and H. Saiedian, "Improving SIEM alert metadata aggregation with a novel kill-chain based classification model," Computers & Security, vol. 94, p. 101817, 2020.

[2] D. Sacher, "Fingerpointing false positives: How to better integrate continuous improvementinto security monitoring," Digital Threats: Research and Practice, vol. 1, no. 1, pp. 1–7, 2020. [3] A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, "Insider-threat detection: Lessons from deploying the CITD tool in three multinational organisations," Journal of Information Security and Applications, vol. 67, p. 103167, 2022

[3] A. Erola, I. Agrafiotis, M.Goldsmith, and S. Creese, “Insider-threat detection:Lessons from deploying the CITD tool in three multinational organizations,” Journal of Information Security and Application, vol. 67, p. 103167, 2022.

[4] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and eventmanagement (SIEM): Analysis, trends, and usage in critical infrastructures," Sensors, vol. 21, no.

[5] S. Tariq, M. Baruwal Chhetri, S. Nepal, and C. Paris, "Alert fatigue in security

Online ISSN 3007-3197
Print ISSN 3007-3189

operationscentres: Research challenges and opportunities," ACM Computing Surveys, vol. 57, no. 9, pp. 1– 38, 2025.

[6] K. M. Cincinsoko, A. K. Ademuwagun, S. Abdullahi, and F. Ifeanyi, "Proactive insider threatdetection in cloud environment using machine learning," Nature Journal of Emerging Sciences Technologies and Innovations, vol. 8, no. 4, pp. 397–410, 2026.

[7] M. S. Mohamed and A. Arabo, "A SIEM-integrated cybersecurity prototype for insider threatanomaly detection using enterprise logs and behavioural biometrics," Electronics, vol. 15, no. 1, p. 248, 2026.

[8] M. Aljumaily, H. Abd, and E. Majeed, "Enhancing user and entity behavior analytics in SIEM systems using AI-powered anomaly detection: A data-driven simulation approach," International Journal of Mechatronics, Robotics, and Artificial Intelligence, vol. 1, no. 2, pp. 82–93, 202.

[9] K. M. Cincinsoko, A. K. Ademuwagun, S. Abdullahi, and F. Ifeanyi, "Proactive insider threat detection in cloud environment using machine learning," Nature Journal of Emerging Sciences Technologies and Innovations, vol. 8, no. 4, pp. 397–410, 2026.

[10] J. M. López Velásquez, S. M. Martínez Monterrubio, L. E. Sánchez Crespo, and D. Garcia Rosado, "Systematic review of SIEM technology: SIEM-SC birth," International Journal of Information Security, vol. 22, no. 3, pp. 691–711, 2023

[11] M. Sheeraz, M. A. Paracha, M. U. Haque, M. H. Durad, S. M. Mohsin, S. S. Band, and A. Mosavi, "Effective security monitoring using efficient SIEM architecture," Human-Centric Computing and Information Sciences, vol. 13, no. 1, pp. 1–15, 2023.

[12] O. Podzins and A. Romanovs, "Why SIEM is irreplaceable in a secure IT environment?," in 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), Apr. 2019, pp. 1–5.

[13] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," IEEE Security & Privacy, vol. 12, no. 5, pp. 35–41, 2014.

[14] M. Vielberth and G. Pernul, "A security information and event management pattern," 2018.

[15] S. Koumourou, A. Peratikou, E. Stavrou, S. Theodoulou, and S. Stavrou, "Reducing SOC analysts alert fatigue via real-time CTI correlation and deduplication," in International Conference on Critical Information Infrastructures Security, Cham: Springer Nature Switzerland, Oct. 2025, pp. 20–35.

[16] M. Shashanka, M. Y. Shen, and J. Wang, "User and entity behavior analytics for enterprise security," in 2016 IEEE International Conference on Big Data (Big Data), Dec. 2016, pp. 1867–1874.

Online ISSN 3007-3197
Print ISSN 3007-3189

[17] N. Okika, O. F. Okoh, and E. E. Etuk, "Mitigating insider threats and social engineering tactics in advanced persistent threat operations through behavioral analytics and cybersecurity training," International Journal of Advance Research Publication and Reviews, vol. 2, no. 3, pp. 11–27, 2025.

[18] S. Phanireddy, "Leveraging SIEM and AI for enhanced web attack detection and prevention," 2022.

[19] M. N. Aktar, M. N. Sakib, A. Hossain, A. Ullah, K. H. Robin, K. M. Rahman, et al., "Enhancing false positive alert detection in security information and event management system using recurrent neural network," in 2024 27th International Conference on Computer and Information Technology (ICCIT), Dec. 2024, pp. 2794–2799.

[20] X. I. D. Armendariz, "Managing false positives in SOC operations: Solutions and best practices," M.S. thesis, 2025. [Online]. Available: https://upcommons.upc.edu/bitstream/handle/2117/424635/tfg-memoria-final.pdf

[21] B A. R. Zope and D. R. Ingle, "Event correlation in network security to reduce false positive," International Journal of Computer Science & Communication Networks, vol. 3, no. 3, p. 182, 2013.

[22] G. Mozalbat, "Reducing false-positive alerts in SIEM systems using TF-IDF."

[23] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, vol. 104, p. 102221, 2021..

[24] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," IEEE Access, vol. 12, pp. 30907–30927, 2024.

[25] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. Yassin, A. Hassan, K. H. Abdulkareem, et al., "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," Applied Sciences, vol. 10, no. 15, p. 5208, 2020.

[26] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: Anomaly detection and diagnosis from system logs through deep learning," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Oct. 2017, pp. 1285–1298.

[27] S. Huang, Y. Liu, C. Fung, R. He, Y. Zhao, H. Yang, and Z. Luan, "HitAnomaly: Hierarchical transformers for anomaly detection in system log," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2064–2076, 2020.

[28] R. B. Yadav, P. S. Kumar, and S. V. Dhavale, "A survey on log anomaly detection using deep learning," in 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Jun. 2020, pp. 1215–1220.

Online ISSN 3007-3197
Print ISSN 3007-3189

[29] X. Zhang, Y. Xu, Q. Lin, B. Qiao, H. Zhang, Y. Dang, et al., "Robust log-based anomaly detection on unstable log data," in Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Aug. 2019, pp. 807–817.

[30] Q. Hu, B. Tang, and D. Lin, "Anomalous user activity detection in enterprise multi-source logs," in 2017 IEEE International Conference on Data Mining Workshops (ICDMW), Nov. 2017, pp. 797–803.

[31] N. Wijesinghe and H. Hemmati, "Log-based anomaly detection of enterprise software: An empirical study," in 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security (QRS), Oct. 2023, pp. 12–23.

[32] 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, p. e0301183, 2024.

[33] S. M. Zeinali, "Analysis of security information and event management (SIEM) evasion and detection methods," M.S. thesis, Tallinn Univ. of Technology, Tallinn, Estonia, 2016.

[34] I. D. Mail, "The future of SIEM in a machine learning-driven cybersecurity landscape," Turkish Journal of Computer and Mathematics Education, vol. 14, no. 3, pp. 1309–1314, 2023.

[35] M. Hadded, G. Lauras, J. Letailleur, Y. Petiot, and A. Dubois, "An assessment platform of cybersecurity attacks against the MQTT protocol using SIEM," in 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Sep. 2022, pp. 1–6.

[36] S. Mahajan, "The role of SIEM in modern cybersecurity: A comprehensive analysis," in Cybersecurity and Privacy in the Era of Smart Technologies, IGI Global Scientific Publishing, 2026, pp. 301–324.

[37] P. Radoglou-Grammatikis, "SecureCyber: An SDN-enabled SIEM for enhanced cybersecurity in the industrial internet of things," MMTC Communications-Frontiers, vol. 18, no. 2, pp. 16–21, 2023.

[38] O. J. Ojugo, "Enhanced threat intelligence and response in college cybersecurity through SIEM and SOC strategies," Journal of Artificial Intelligence General Science (JAIGS), vol. 7, no. 1, pp. 367–380, 2024.

[39] J. S. Suroso and C. P. Prastya, "Cyber security system with SIEM and honeypot in higher education," IOP Conference Series: Materials Science and Engineering, vol. 874, no. 1, p. 012008, Jun. 2020.

[40] N. Jansen, "Enhancing cybersecurity threat prevention through information security event management (SIEM) and policy deployment effectiveness," 2023.