STM JOURNALS

Journal of
Communication Engineering & Systems

ISSN: 2249-8613 (Online)
ISSN: 2321-5151 (Print)
Volume 14, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoCES

https://journals.stmjournals.com/joces

Review JoCES

Developing a Comprehensive Framework for User and Entity Behavior Analytics (UEBA): Integrating Advanced Machine Learning and Contextual Insights

Garima Sharma[1,*], Ambika Thakur[2], Chetna Tiwari[2]

Abstract

User and Entity Behavior Analytics (UEBA) has emerged as a crucial approach in modern cybersecurity for detecting and mitigating insider threats, compromised accounts, and other malicious activities within organizational networks. However, existing UEBA frameworks often face challenges in scalability, detection accuracy, and response effectiveness. This research work proposes a novel framework for UEBA that aims to address these limitations and enhance threat detection and response capabilities. The framework integrates advanced machine learning algorithms, behavioral analytics techniques, and threat intelligence to establish baseline behaviors, detect anomalies, and prioritize response actions. Key components of the framework include user and entity profiling, behavioral analytics, risk scoring, and incident detection and response mechanisms. In user and entity profiling, comprehensive profiles are created for both users and entities (e.g., devices, applications) within the network, capturing relevant attributes and historical behaviors. Behavioral analytics leverages these profiles to identify deviations from normal behavior patterns, signaling potential security incidents. Risk scoring assigns severity levels to detected anomalies based on their potential impact and likelihood, enabling prioritization of response efforts. Overall, this research contributes to advancing the field of UEBA by providing a comprehensive framework that addresses scalability, accuracy, and effectiveness challenges. It lays the groundwork for developing more robust and adaptive cybersecurity solutions to combat evolving threats effectively, ensuring the security and integrity of organizational networks in an increasingly complex threat landscape.

Keywords: UEBA, cybersecurity, threat detection, security framework, security analysis, behavioral analytics, threat intelligence

INTRODUCTION

The advent of sophisticated cyber threats and the increasing complexity of organizational networks have highlighted the crucial importance of implementing strong cybersecurity measures [1]. In this context, UEBA has emerged as a pivotal approach in identifying and mitigating insider threats, compromised accounts, and other malicious activities [1].

However, existing UEBA frameworks often encounter challenges in scalability, detection accuracy, and response efficiency [2]. To address these limitations, this research work introduces a novel framework for UEBA, aimed at enhancing response to security threats. Leveraging advanced machine learning algorithms, behavioral analytics techniques, and threat intelligence, the proposed framework establishes baseline behaviors, detects anomalies, and prioritizes response actions [3].

***Author for Correspondence**
Garima Sharma
E-mail: garimasharma@ncuindia.edu

[1]Assistant Professor, Department of Computer Science and Engineering, The NorthCap University, Haryana, India
[2]Student, Department of Computer Science and Engineering, The NorthCap University, Haryana, India

Received Date: April 09, 2024
Accepted Date: April 26, 2024
Published Date: June 29, 2024

Citation: Garima Sharma, Ambika Thakur, Chetna Tiwari. Developing a Comprehensive Framework for User and Entity Behavior Analytics (UEBA): Integrating Advanced Machine Learning and Contextual Insights. Journal of Communication Engineering & Systems. 2024; 14(2): 20–32p.

UEBA stands as a pivotal cybersecurity technology aimed at identifying and addressing insider threats, and compromised accounts [1]. UEBA solutions leverage advanced analytics, machine learning, and behavioral modeling techniques to develop a baseline of normal behavior for users, applications, and other entities [4]. Through continuous surveillance and analysis, UEBA systems can identify deviations from normal behavior, or anomalies, that may indicate security threats or risks. This proactive stance enables organizations to swiftly detect and mitigate potential security incidents before they escalate, enhancing their overall cybersecurity posture [1]. The rising importance of UEBA stems from the dynamic nature of cybersecurity threats and the increasingly intricate architecture of organizational networks. Figure 1 illustrates the importance of UEBA [5].

LITERATURE STUDY

The evolution of UEBA has been marked by significant advancements in cybersecurity technology and methodologies. Originating in the early 2000s, UEBA emerged as an organization that recognized the need to analyze user behaviors to detect insider threats and unauthorized activities [5]. Over the years, UEBA has evolved from basic behavioral analysis techniques to sophisticated solutions that leverage machine learning, big data analytics, and automation. Early implementations focused on rule-based anomaly detection, but as cyber threats became more complex, UEBA integrated machine learning algorithms to enhance detection accuracy. The integration of big data analytics capabilities allowed organizations to analyze large volumes of data for comprehensive threat detection [1]. Cloud adoption and scalability became prominent features in the late 2010s, while recent years have seen a shift towards automation, orchestration, and AI-driven approaches. Today, UEBA stands as a core component of modern cybersecurity architectures, providing organizations with the ability to proactively identify and mitigate a wide range of security threats [6]. Figure 2 depicts the evolution of UEBA from the early 2000s to the present time.

While UEBA offers significant advantages in detecting insider threats and malicious activities within organizational networks, it also has its limitations. One limitation is the challenge of accurately establishing baseline behaviors for users and entities, which can lead to false positives or missed detections if not properly calibrated. Additionally, UEBA systems may struggle with the sheer volume and variety of data sources, potentially resulting in incomplete or inconsistent analysis [6]. Furthermore, UEBA solutions may encounter difficulties in detecting sophisticated attacks that involve evasion techniques or manipulation of normal behaviors. Integration and interoperability issues with existing security infrastructure can also pose challenges for UEBA deployment and effectiveness [6]. Now let us investigate UEBA deeply and discuss its core components and functionalities.

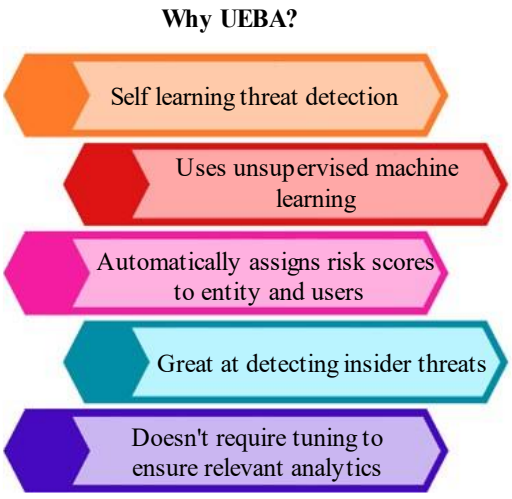

Figure 1. Why prefer UEBA.

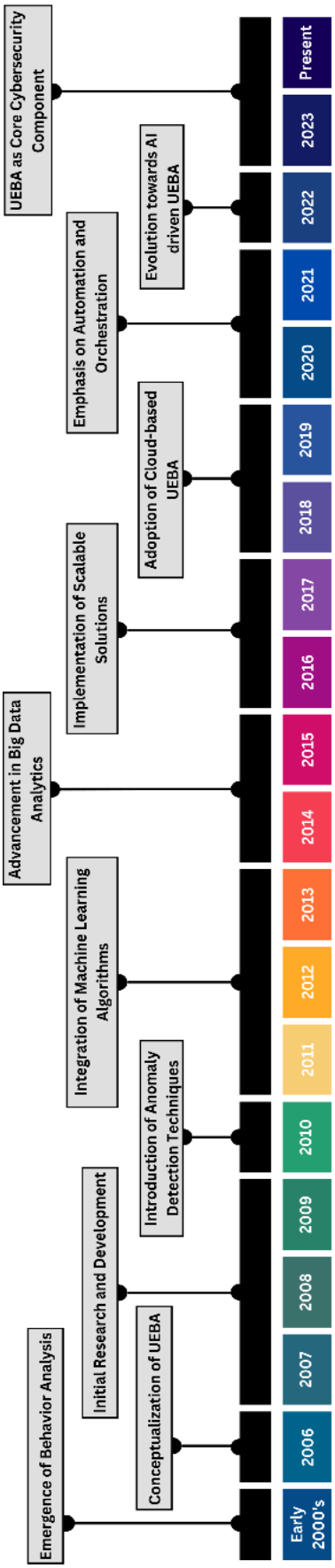

Figure 2. Evolution of UEBA.

USER AND ENTITY BEHAVIOR ANALYTICS

UEBA is a cybersecurity strategy that analyzes the behavior of people and entities on an organization's network or system to discover insider threats, compromised accounts, and various security problems [7]. UEBA systems usually include several key components and features that analyze user and entity behavior inside a corporate's network or system. This section provides a comprehensive explanation of the associated components [8]. The basic terminologies associated with UEBA are discussed as shown in Figure 3.

Data Collection

UEBA systems gather information from a variety of sources on the organization's network, including logs, event streams, user activity records, and endpoint data. The data may include user behavior, network traffic, system activity, and application use.

Data Processing

After collection, the data is preprocessed and normalized to guarantee consistency and compatibility across several data sources. This process entails cleaning, organizing, and structuring raw data for analysis.

Machine Learning Algorithms

UEBA systems use machine learning algorithms to process vast datasets and recognize patterns, abnormalities, and deviations from typical behavior. These algorithms use learned behavior models to detect suspicious behaviors, odd access patterns, and possible security issues.

Behavioral Analytics

Behavioral analytics techniques are used to create baseline behavior profiles for individuals, entities (such as devices, apps, and servers), and the entire system. By monitoring departures from these baselines, UEBA systems may detect unusual behavior that could signal a security breach or insider threat.

Anomaly Detection

UEBA systems use anomaly detection algorithms to alert to odd actions or behaviors that differ considerably from anticipated patterns. This might include odd login times, access to sensitive data, changes in user roles or permissions, and other questionable behavior.

Contextual Analysis

UEBA systems analyze behavior in context, taking into account user roles, access rights, time of day, location, and the criticality of the assets being accessed. Contextual analysis aids in the prioritization and contextualization of security warnings, lowering false positives and increasing threat detection efficacy.

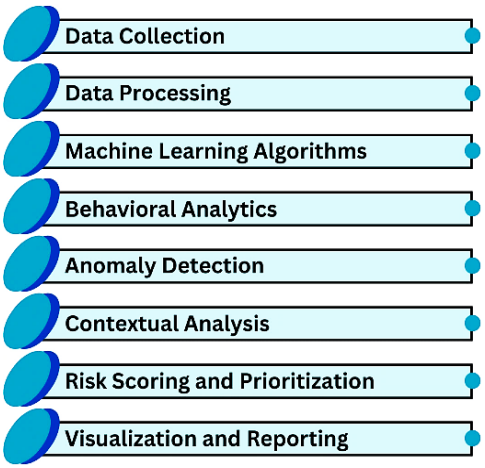

Figure 3. Core components and fundamentals of UEBA.

Risk Scoring and Prioritization

Security anomalies and occurrences are assigned risk ratings based on their severity, possible effect, and likelihood of posing a danger. UEBA systems prioritize warnings and events based on risk scores, enabling security teams to concentrate on the most serious threats first.

Visualization and Reporting

Many UEBA solutions include visualization tools and dashboards that enable security analysts to study data patterns, analyze events, and produce reports. Visualization helps analysts grasp complicated relationships and patterns in data, allowing for better informed decision-making and reaction.

MACHINE LEARNING ALGORITHMS

UEBA systems utilize a variety of machine learning techniques to analyze user and entity behavior patterns and identify abnormalities or possible security vulnerabilities inside an organization's network or system [9]. Some typical machine learning methods used in UEBA are shown in Figure 4 [10].

Unsupervised Learning Algorithms

Unsupervised learning algorithms are commonly used in UEBA to detect patterns and abnormalities in user and entity behavior without the requirement for labeled training data. Clustering methods like k-means clustering, hierarchical clustering, and density-based clustering are used to group similar behavior patterns and detect outliers or anomalies.

Supervised Learning Algorithms

UEBA uses supervised learning algorithms to categorize behavior patterns and forecast whether certain behaviors are suggestive of security vulnerabilities. Classification techniques which include logistic regression, random forests, support vector machines (SVM), decision trees, and neural networks are trained on labeled datasets to discriminate between normal and abnormal behavior and give risk ratings to security incidents.

Deep Learning Models

Deep learning models, particularly deep neural networks (DNNs), are becoming more prevalent in UEBA systems for analyzing intricate and multifaceted data like network traffic logs, user activity logs, and system events. Architectures such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders can grasp intricate patterns and representations from raw data. This enables more accurate identification of abnormal behavior and advanced attack vectors.

Anomaly Detection Algorithms

UEBA uses anomaly detection algorithms, such as Gaussian mixture models (GMM), Isolation Forest, one-class SVM, and robust statistical approaches, to find departures from typical behavior patterns. These algorithms describe the distribution of typical behavior and identify cases that deviate considerably from predicted patterns as potential security issues.

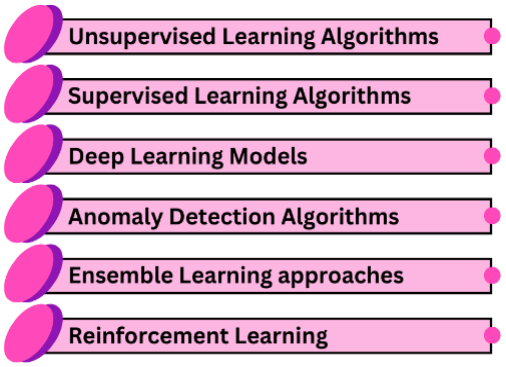

Figure 4. Machine learning algorithms.

Ensemble Learning Approaches

Bagging, boosting, and stacking are common approaches used in UEBA to integrate various machine learning models and increase the overall accuracy and resilience of threat detection. Ensemble approaches reduce the danger of overfitting while increasing the system's capacity to generalize to new and unknown threats.

Reinforcement Learning

Some sophisticated UEBA systems may use reinforcement learning techniques to optimize security rules and response tactics based on environmental feedback. Reinforcement learning algorithms learn to make sequential judgements and update security policies in response to evolving threats and weaknesses.

BEHAVIORAL MODELING TECHNIQUES

Behavioral modeling approaches are critical to UEBA systems because they enable them to create baseline behavior patterns, spot deviations from typical activity, and detect possible security vulnerabilities inside an organization's network or system [11]. Some typical behavioral modeling methodologies used in UEBA are shown in Figure 5.

Profile-Based Modeling

Profile-based modeling is the process of establishing behavioral profiles for individuals, entities (such as devices, apps, and servers), and groups using previous activity data. These profiles document typical behavior patterns, such as login times, access patterns, data transfer volumes, and program usage. Deviations from these patterns might suggest suspicious or unauthorized activities.

Peer Group Analysis

Peer group analysis compares the behavior of individual users or entities to that of their peers within the organization. By combining people or entities with comparable roles, responsibilities, and access rights, UEBA systems may detect anomalies and outliers that depart considerably from the norm in their peer groups.

Sequence Analysis

These approaches look at the sequential patterns of user and entity interactions inside the system. This entails analyzing the sequence of activities and events carried out by individuals or entities over time, such as the sequence of instructions issued during a session, or the series of network connections created by a device. Sequence analysis aids in detecting abnormal sequences of actions that may suggest malevolent behavior or insider threats.

Graph-Based Modeling

Graph structures are used to describe the relationships and activities between users, entities, and assets in a corporate's network. By modeling the network architecture and analyzing the flow of data

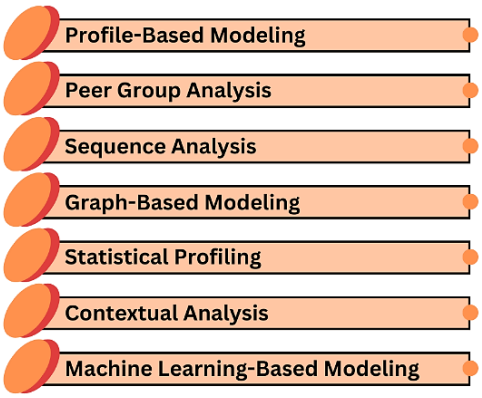

Figure 5. Behavioral modelling methodologies of UEBA.

and access rights across interconnected organizations, UEBA systems can detect anomalous patterns of communication, privilege escalation, or data exfiltration that may indicate security breaches or insider attacks.

Statistical Profiling

Statistical profiling entails examining quantitative measurements and statistical aspects of user and entity behavior, such as frequency, duration, volume, and variation. By using statistical approaches like mean, standard deviation, histograms, and time series analysis to behavioral data, UEBA systems may detect outliers, patterns, and statistical abnormalities that indicate security events or policy breaches.

Contextual Analysis

Contextual analysis evaluates behavior patterns by considering contextual characteristics such as user roles, access entitlements, time of day, location, and the criticality of the assets being accessed. By contextualizing behavior within its relevant environment, UEBA systems can discern between legal and suspect activity, lowering false positives and enhancing threat detection accuracy.

Machine Learning-Based Modeling

Machine learning techniques are critical for modeling and analyzing complicated behavioral patterns in UEBA systems. Supervised, unsupervised, and semi-supervised learning techniques are used to learn from past data, adapt to changing threats, and detect anomalies and security issues in real-time [10].

STATISTICAL ANALYSIS

UEBA relies heavily on statistical analysis to provide quantitative insights into patterns, trends, and anomalies inside an organization's network or system. UEBA solutions employ a variety of statistical methodologies to analyze user and entity behavior data, identify deviations from typical activity, and discover possible security risks [2]. Some important areas of statistical analysis in UEBA are shown in Figure 6 [12].

Descriptive Statistics

It summarizes and characterizes the features of user and entity behavior data. Descriptive statistics commonly use measures of central tendency (e.g., mean, median, mode), dispersion (e.g., standard deviation, variance), and distribution (e.g., skewness, kurtosis). Analysts can use descriptive statistics to understand the normal behavior patterns and activity distribution inside the system [13].

Frequency Analysis

Investigates the frequency and distribution of certain occurrences or activities over time. UEBA systems can detect anomalous spikes or trends in logins, access attempts, data transfers, and other activities. Frequency analysis is useful for prioritizing security warnings and focusing on high-impact threats.

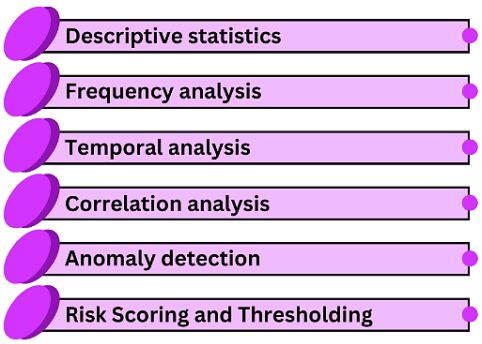

Figure 6. Statistical analysis in UEBA.

Temporal Analysis

Examines user and entity behavior patterns over various time intervals, such as hours, days, weeks, or months. By studying temporal trends and seasonality in activity data, UEBA systems can discover patterns of behavior that may change depending on the time of day, day of the week, or other factors. Temporal analysis identifies unusual activity patterns and detects possible risks in real time.

Correlation Analysis

Investigates the correlations and dependencies among various variables or qualities in user and entity behavior data. UEBA systems can find connections between user behaviors, access patterns, system events, and security issues by using correlation coefficients and covariance matrices. Correlation analysis can reveal hidden links and dependencies that could imply coordinated assaults or insider threats.

Anomaly Detection

Approaches employ statistical methods to find deviations from regular behavior patterns and detect unexpected or suspicious activity inside the system. Statistical models such as Gaussian mixture models (GMM), z-score analysis, and time series analysis are used to detect outliers, anomalies, and statistical abnormalities in behavioral data. Anomaly detection helps to identify possible security issues and prioritize investigative efforts [3].

Risk Scoring and Thresholding

Statistical analysis is used to give risk ratings to security events and set threshold levels that activate security alarms. Risk scoring algorithms take into account a variety of parameters, including the severity, effect, frequency, and chance of security events, using statistical metrics and historical data. Thresholding approaches assist evaluate the amount of risk tolerance and create actionable thresholds for responding to security threats.

PROPOSED FRAMEWORK

This study proposes a novel framework by combining Splunk User Behavior Analytics (UBA) [14] and Securonix Security Analytics Platform [15] framework to create a new framework that will have the qualities of both frameworks and have strong security features. Combining Splunk UBA with Securonix Security Analytics Platform improves cybersecurity by collecting data from several sources, analyzing behavior patterns, and identifying abnormalities. Integration allows for enhanced analytics, contextual awareness, real-time alerts, and compliance reporting. Together, they enable full visibility, accurate threat detection, and proactive incident response throughout the IT ecosystem.

The key components of the proposed framework are discussed as follows:

1. *Behavioral Analysis Engine:* Advanced analytics capabilities, such as machine learning algorithms, behavioral modeling, and statistical analysis, are used to establish baseline behaviors, detect anomalies, and identify patterns of suspicious behavior across the network.
2. *Correlation and Integration Layer:* Components facilitating the integration, correlation, and normalization of security events, alerts, and anomalies detected by both Splunk UBA and Securonix Security Analytics Platform. This layer enables centralized visibility and correlation of security-related activities and events across the network.
3. *Risk Scoring and Prioritization Module:* Components responsible for assigning risk scores to identified threats and anomalies based on the severity and likelihood of security risks. This module prioritizes alerts and incidents based on risk scores to focus response efforts on the most critical threats.
4. *Automated Response and Orchestration Module:* Components offering automated response capabilities to mitigate security threats and incidents promptly. This module may include predefined response actions, playbooks, and workflows for incident response and mitigation.

5. *Incident Investigation and Forensic Analysis Module:* Components providing incident investigation features, including forensic analysis, threat hunting, timeline reconstruction, and evidence-gathering capabilities. This module assists security teams in investigating and responding to security incidents effectively.

By combining the strengths of Splunk UBA and Securonix Security Analytics Platform, organizations can create a unified framework for UEBA that enhances threat detection, response, and overall cybersecurity posture. The integration between the two platforms enables organizations to leverage their complementary capabilities and achieve greater visibility, control, and resilience against evolving security threats. When Splunk User Behavior Analytics (UBA) and Securonix Security Analytics Platform are integrated to create a unified framework, the following stepwise working process outline is shown in Figure 7.

Step 1: Data Collection

Splunk UBA gathers logs, events, and security-related information from a multitude of network sources, such as endpoints, servers, applications, and network devices. Similarly, Securonix Security Analytics Platform compiles data from various origins like logs, network traffic, and user activity records, forming an extensive dataset for thorough analysis.

Step 2: Data Ingestion and Processing

Splunk UBA collects the acquired data and proceeds to analyze it within its platform, employing sophisticated analytics tools including machine learning algorithms and behavioral analysis methods to pinpoint behavior patterns and identify irregularities. Similarly, the Securonix Security Analytics Platform undertakes analogous data ingestion and processing responsibilities, utilizing its unique array of machine learning algorithms, behavioral analytics, and threat intelligence to scrutinize both user and entity behaviors, ultimately discerning potential security threats.

Step 3: Behavioral Analysis and Anomaly Detection

Both Splunk UBA and Securonix Security Analytics Platform perform behavioral analysis to establish baseline behaviors for users, devices, and applications within the network. They utilize advanced analytics techniques to identify deviations from normal behavior, anomalies, and suspicious activities, which could potentially indicate security threats, insider threats, or malicious behavior.

Figure 7. Working process of integrated framework.

Table 1. Comparison between existing and new hybrid framework.

Features	Exabeam Security Management Platform	LogRhythm NextGen SIEM Platform	Splunk UBA	Securonix Security Analytics Platform	Hybrid Framework (Splunk UBA + Securonix
Data Collection	Gathers and evaluates log data, network traffic, and user activity to identify potential security threats.	The system ingests and analyzes a variety of data sources, including log data, network traffic, and user activity, to detect potential security threats.	It collects and analyzes security-related information from a range of sources, such as logs and endpoints, for further processing.	Collects information from various origins, encompassing logs, network traffic, and records of user activities.	Integrates data ingestion from multiple sources, including logs, events, and user activity records.
Behavioral Analytics	Utilizes ML algorithms to detect anomalies and identify insider threats.	Applies behavioral analysis techniques to establish baseline behaviors and detect anomalies.	Leverages ML and behavioral analytics for detecting abnormal behavior patterns.	Employs ML algorithms and behavioral modelling for behavior analysis and anomaly detection.	Utilizes advanced ML algorithms for accurate behavior analysis and anomaly detection.
Integration with SIEM	Integrates with SIEM solutions for centralized security monitoring and incident response.	Provides SIEM capabilities for log management, correlation, and security event monitoring.	Offers integration with SIEM platforms for centralized visibility and correlation of security events.	Seamlessly integrates with Splunk Enterprise Security or other SIEM solution.	Seamlessly integrates with Splunk Enterprise Security or other SIEM solutions.
Automated Response	Offers automated response capabilities for incident mitigation and response orchestration.	Provides automated response features for threat containment and incident remediation.	Offers limited automated response capabilities for incident mitigation and remediation.	Provides enhanced automated response features for prompt threat mitigation and incident containment.	Provides enhanced automated response features for prompt threat mitigation and incident containment.
Incident Investigation	Provides incident investigation features, including forensic analysis and threat hunting capabilities.	Offers incident investigation capabilities, including forensic analysis and timeline reconstruction.	Provides basic incident investigation capabilities for analyzing security events and anomalies.	Enhances incident investigation with forensic analysis, threat hunting, and evidence gathering functionalities.	Enhances incident investigation with forensic analysis, threat hunting, and evidence gathering functionalities.
Reporting and Visualization	Provides advanced reporting and visualization features for presenting security insights and trends.	Offers customizable dashboards, reports, and visualization for analyzing security data and trends.	Offers basic reporting and visualization features for presenting insights and trends.	Provides advanced reporting and visualization capabilities for clear and actionable insights into security incidents.	Provides advanced reporting and visualization capabilities for clear and actionable insights into security incidents and trends.
Scalability and Flexibility	Offers scalability and flexibility to handle large-scale deployments and diverse use cases.	Scalable platform capable of handling large volumes of data and supporting diverse environments.	Varies in scalability and flexibility based on the capabilities and architecture of the solution.	Offers scalability and flexibility to meet organizational requirements and support divers use cases.	Offers scalability and flexibility to handle large volumes of data and support diverse use cases and environments.

Step 4: Integration and Correlation

Both seamlessly integrate to correlate security events, alerts, and anomalies identified by both solutions. This integration offers centralized visibility into security-related activities, empowering security teams to correlate and analyze data from various sources for comprehensive threat detection and response.

Step 5: Risk Scoring and Prioritization

Both platforms assign risk scores to identified threats and anomalies based on the severity of security risks. They prioritize alerts and incidents based on risk scores, allowing security teams to focus their response efforts on the most critical threats and vulnerabilities.

Step 6: Automated Response and Incident Investigation

Splunk UBA and Securonix Security Analytics Platform offer automated response capabilities to mitigate security threats and incidents promptly. They provide incident investigation features, including forensic analysis, threat hunting, and timeline reconstruction, to help security teams investigate and respond to security incidents effectively.

Step 7: Reporting and Visualization

Both platforms offer reporting and visualization capabilities to present insights, trends, and security incidents in a clear and actionable format. They provide dashboards, reports, and visualizations to help security analysts and stakeholders understand and communicate security-related information effectively.

COMPARISON WITH EXISTING FRAMEWORKS

This section provides a comprehensive comparison of the proposed framework with the other similar systems available in the literature. The presented comparative analysis provides an understanding of the distinctive features and advantages of the proposed framework, including its advanced behavioral analysis engine, integration layer, risk scoring, automated response capabilities, and incident investigation modules [16]. This comparison underscores how the integration of Splunk UBA and Securonix Security Analytics Platform enhances cybersecurity by offering full visibility, accurate threat detection, and proactive incident response throughout the IT ecosystem. Table 1 shows a detailed comparison between the existing frameworks and the framework.

CONCLUSION AND FUTURE WORK

This research underscores the crucial significance of incorporating advanced machine learning methodologies and contextual insights to augment the efficiency of UEBA (User and Entity Behavior Analytics) solutions. By integrating sophisticated analytical algorithms alongside contextual factors like user roles, access permissions, and environmental variables, organizations can significantly enhance their capacity to identify, scrutinize, and address security threats and irregular activities. The comprehensive framework delineated in this study offers a holistic perspective on UEBA, presenting a robust amalgamation of behavioral analysis, anomaly detection, risk assessment, and automated response functionalities. In light of the escalating complexity and sophistication of cyber threats, it becomes imperative for organizations to embrace innovative strategies, as outlined in this study, to proactively safeguard their critical assets and data. The industries or sectors where such a hybrid implementation can be useful are shown in Figure 8.

Financial Services Industry

A large bank can integrate Splunk UBA and Securonix Security Analytics Platform to detect insider threats, fraudulent activities, and unauthorized access attempts, enhancing cybersecurity and safeguarding sensitive customer data and financial assets.

Healthcare Sector

A healthcare organization can integrate Splunk UBA and Securonix Security Analytics Platform to monitor network behavior, detect anomalies, and ensure compliance with regulatory standards, safeguarding patient data and privacy.

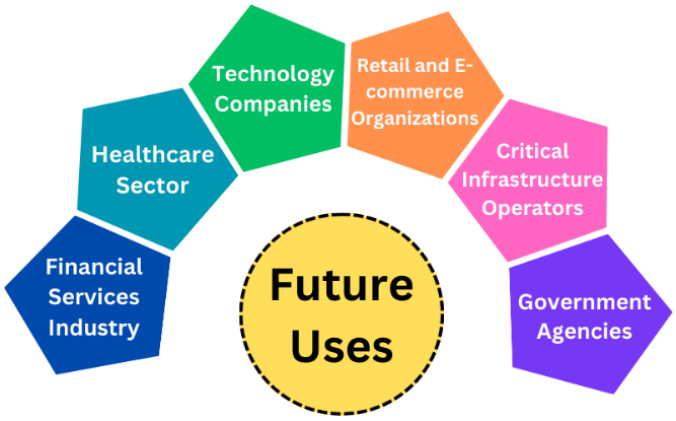

Figure 8. Future uses of the hybrid framework.

Technology Companies

A technology company can utilize the hybrid framework of Splunk UBA and Securonix Security Analytics Platform to bolster security operations, detecting and mitigating insider threats, cyber-attacks, and intellectual property theft, safeguarding valuable assets and proprietary information.

Government Agencies

A government agency can use Splunk UBA and Securonix Security Analytics Platform to monitor and analyze user behavior and entity activity across its network infrastructure. The hybrid solution assists in detecting and responding to security incidents, protecting critical infrastructure and sensitive government information from cyber threats.

Retail and E-commerce Organizations

A retail or e-commerce company can adopt the hybrid framework of Splunk UBA and Securonix Security Analytics Platform to monitor user activity, detect fraudulent transactions, and prevent account takeover attempts. The integrated solution helps protect customer data, prevent financial losses, and maintain trust in the brand.

Critical Infrastructure Operators

Operators of critical infrastructure, such as energy, utilities, and transportation companies, can implement the hybrid solution of Splunk UBA and Securonix Security Analytics Platform to monitor and secure their operational technology (OT) networks. The integrated solution assists in detecting and mitigating cyber threats targeting industrial control systems (ICS) and ensuring the reliability and resilience of critical infrastructure assets.

REFERENCES

1. Khaliq S, Tariq ZU, Masood A. Role of user and entity behavior analytics in detecting insider attacks. In 2020 IEEE International Conference on Cyber Warfare and Security (ICCWS). 2020 Oct 20; 1–6.
2. Khan MZ, Khan MM, Arshad J. Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). In 2022 IEEE 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS). 2022 Dec 14; 1–9.
3. Rengarajan R, Babu S. Anomaly detection using user entity behavior analytics and data visualization. In 2021 IEEE 8th International Conference on Computing for Sustainable Global Development (INDIACom). 2021 Mar 17; 842–847.
4. Martín AG, Fernández-Isabel A, Martín de Diego I, Beltrán M. A survey for user behavior analysis based on machine learning techniques: current models and applications. Appl Intell. 2021 Aug; 51(8): 6029–55.

5. Exabeam. (2023). What Is UEBA and Why It Should Be an Essential Part of Your Incident Response. [Online]. Available from: https://www.exabeam.com/explainers/ueba/what-is-ueba-and-why-it-should-be-an-essential-part-of-your-incident-response/
6. Logsign. (2023). UEBA Trends - What's New & What's Next. [Online]. Available from: https://www.logsign.com/blog/ueba-trends-whats-new-whats-next/
7. Martín AG, Beltrán M, Fernández-Isabel A, de Diego IM. An approach to detect user behaviour anomalies within identity federations. Comput Secur. 2021 Sep 1; 108: 102356.
8. Exabeam. (2023). UEBA Tools: Key Capabilities and 7 Tools You Should Know. [Online]. Available from: https://www.exabeam.com/explainers/ueba/ueba-tools-key-capabilities-and-7-tools-you-should-know/
9. Ranjan R, Kumar SS. User behaviour analysis using data analytics and machine learning to predict malicious user versus legitimate user. High-Confid Comput. 2022 Mar 1; 2(1): 100034.
10. Gurucul Admin. (2019). ABCs of UEBA: M is for Machine Learning. [Online]. Gurucul UEBA. Available from: https://gurucul.com/blog/abcs-of-ueba-m-is-for-machine-learning/
11. Salitin MA, Zolait AH. The role of User Entity Behavior Analytics to detect network attacks in real time. In 2018 IEEE international conference on innovation and intelligence for informatics, computing, and technologies (3ICT). 2018 Nov 18; 1–5.
12. Exabeam. (2024). What Is UEBA (User and Entity Behavior Analytics)? [Online]. Available from: https://www.exabeam.com/explainers/ueba/what-ueba-stands-for-and-a-5-minute-ueba-primer/
13. Investopedia. (2024). Descriptive Statistics: Definition, Overview, Types, and Example. [Online]. Available from: https://www.investopedia.com/terms/d/descriptive_statistics.asp
14. Splunk. (2024). User Behavior Analytics (UBA). [Online]. Splunk. Available from: https://www.splunk.com/en_us/products/user-behavior-analytics.html
15. Securonix. (2022). Delivering Security Analytics at Cloud Scale. [Online]. Securonix. Available from: https://www.securonix.com/resources/securonix-delivering-security-analytics-at-cloud-scale/
16. Yousef R, Jazzar M. Measuring the effectiveness of user and entity behavior analytics for the prevention of insider threats. J Xi'an Univ Arch & Technol. 2021; 13(10): 175–81.

