STM JOURNALS

Journal of
Operating Systems
Development & Trends

ISSN: 2454-9355
Volume 11, Issue 1, 2024
January–April
DOI (Journal): 10.37591/JoOSDT

https://journals.stmjournals.com/joosdt

Review JoOSDT

Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology

Sania[1,*], Neha Sindhu[2], Yogita Gigras[3], Shilpa Mahajan[4]

Abstract

In the dynamic landscape of cybersecurity, organizations confront increasingly intricate cyber threats that necessitate sophisticated security measures. Conventional systems such as Security Information and Event Management (SIEM) systems face ongoing challenges, they often struggle to effectively detect and mitigate sophisticated attacks within extensive data sets. To address these limitations, the introduction of Gatividhi Guard signifies a paradigm shift in SIEM technology. Gatividhi Guard is an innovative SIEM platform leveraging advanced Artificial Intelligence and Machine Learning (AIML) algorithms. Its primary objective is to empower organizations with enhanced threat detection capabilities and comprehensive user behavior analysis. Through the integration of AIML, Gatividhi Guard excels in swiftly and accurately identifying and neutralizing cyber threats. A distinguishing feature of Gatividhi Guard lies in its ability to track user mouse movements and locations, facilitating the mitigation of insider threats. This proactive approach to monitoring user activity adds a layer of security crucial for safeguarding digital assets. Moreover, Gatividhi Guard offers intuitive dashboards and robust reporting tools, enabling security analysts to gain deeper insights into security events and make informed decisions to mitigate risks effectively. By presenting security data in a user-friendly manner, Gatividhi Guard enhances the efficiency of security operations and strengthens overall cybersecurity posture. This paper elucidates the design and features of the Gatividhi Guard, providing comprehensive guidance on its implementation and setup. By elucidating the significance of the Gatividhi Guard in protecting digital assets, the paper underscores the indispensable role of AI-driven solutions in addressing modern cybersecurity challenges. Gatividhi Guard emerges as a pivotal asset for organizations seeking to fortify their IT systems against emerging threats. Through the strategic integration of AI and comprehensive user behavior analysis, Gatividhi Guard empowers organizations to confront new cybersecurity challenges with confidence, thereby elevating the overall security resilience of their digital infrastructure.

***Author for Correspondence**
Sania
E-mail: sania20csu167@ncuindia.edu

[1,2]Student, Department of Computer Science and Engineering, The NorthCap University, Gurugram, Haryana, India
[3,4]Associate Professor, Department of Computer Science and Engineering, The NorthCap University, Gurugram, Haryana, India

Received Date: April 09, 2024
Accepted Date: April 20, 2024
Published Date: May 03, 2024

Citation: Sania, Neha Sindhu, Yogita Gigras, Shilpa Mahajan. Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. Journal of Operating Systems Development & Trends. 2024; 11(1): 29–44p.

Keywords: SIEM, cybersecurity, AI, machine learning, threat detection, user behavior analysis, insider threats, Gatividhi Guard

INTRODUCTION

In today's highly connected digital world, the need for strong cybersecurity defenses is crucial. As organizations across various industries rely more on digital systems and data-driven processes, the threat of cyberattacks grows significantly. This presents a serious challenge that requires constant attention and innovative solutions. At the core of many organizations' cybersecurity strategies are Security Information and Event Management (SIEM) [1]

systems. Playing a critical role in monitoring, detecting, and responding to security events in digital environments, these systems serve as central hubs, collecting extensive data from various sources such as network devices, servers, applications, and security logs. Leveraging advanced analysis and correlation techniques, SIEM platforms provide valuable insights into potential security incidents, enabling swift response and mitigation efforts. However, with the rapid evolution of the digital threat landscape and the increasing sophistication of cyber adversaries, the limitations of traditional SIEM systems are becoming increasingly apparent. Reliant primarily on rules and signatures, these systems struggle to adapt to the constantly shifting nature of modern cyber threats. Their reactive approach leaves organizations vulnerable to new attack methods and persistent threats that can bypass conventional detection methods [2].

Furthermore, the vast scale and intricate complexity of today's IT environments present significant obstacles for traditional SIEM systems. The immense volume of security data generated by numerous endpoints, applications, and cloud services exceeds the capabilities of older SIEM platforms. This overload of information results in alert fatigue, false alarms, and instances where threats go undetected. Consequently, organizations are faced with the challenging task of sifting through this deluge of data to differentiate between meaningful signals and irrelevant noise, often at the expense of valuable time and resources.

Acknowledging these limitations, there's a rising agreement within the cybersecurity community about the necessity for next-generation SIEM solutions that adopt a proactive, intelligence-driven strategy toward detecting and responding to threats. This is where Gatividhi Guard steps in - a pioneering platform leading the charge in cybersecurity innovation. Gatividhi Guard is set to revolutionize the industry with its integration of cutting-edge AIML technologies.

Gatividhi Guard heralds a significant shift in cybersecurity defense, surpassing the limitations of traditional SIEM systems through seamless integration of AI/ML (Artificial Intelligence and Machine Learning) algorithms and User and Entity Behavior Analysis (UEBA) [3]. By harnessing the capabilities of AI-driven analytics, Gatividhi Guard opens new horizons in threat detection, enabling organizations to proactively identify and thwart emerging threats before they escalate into major breaches. At its core, Gatividhi Guard utilizes AI/ML algorithms to ingest, analyze, and contextualize large numbers of security data in real-time. It identifies patterns, anomalies, and indicators of compromise that may evade human detection. Through continuous learning and adaptation, the platform evolves threat detection capabilities, staying one step ahead of evolving threat actors and their tactics. Furthermore, Gatividhi Guard enhances traditional SIEM functionality with sophisticated User and Entity Behavior Analysis, shedding light on the human aspect of cybersecurity. By scrutinizing user activity and behavior patterns across digital assets, Gatividhi Guard identifies deviations from normal behavior that may indicate insider threat, compromised credentials, or malicious intent. This fortifies the organization's defenses from within, providing a comprehensive approach to cybersecurity.

In the upcoming sections, the paper delves deeply into Gatividhi Guard's architecture, functionalities, and practical implementations. It aims to provide a thorough understanding of how this innovative platform is revolutionizing the cybersecurity field. Through a lens of technological advancement and strategic vision, this study examines the interconnectedness of AI/ML, UEBA, and SIEM, illustrating how their integration signifies a paradigm shift toward proactive threat detection and resilience in challenging circumstances.

OVERVIEW

SIEM (Security Information and Event Management)

In the early 2000s, SIEM became crucial for companies protecting against data breaches and cyberattacks (Figure 1). However, over time, SIEM struggled to keep up with changing security needs. Handling large amounts of diverse data and facing new, advanced threats made SIEM less effective.

Plus, it was costly to set up and maintain SIEM systems, making them inaccessible for many companies. Problems with getting SIEM to work well added to doubts about its usefulness in cybersecurity. However, SIEM bounced back. It evolved to handle various data in complex situations, providing a strong defense against cyberattacks. Now, SIEM is a vital part of organizations, letting them focus on their main tasks without constant worry about security threats. It helps spot and solve security issues to ensure compliance with rules and regulations. SIEM also sends automated alerts about potential intrusions and helps manage defensive systems effectively. With regulations requiring regular IT audits, SIEM has become crucial for checking defensive systems' strength and spotting unauthorized attempts to breach security [4].

The increasing demand for security information and event management systems often stems from clients seeking to fulfill compliance obligations while also ensuring real-time threat detection capabilities. SIEM's popularity stems from its ability to help clients quickly analyze security events, manage threats, and create detailed reports on log data. This makes SIEM a fundamental technology in modern cybersecurity practices.

Merging of Two Domains

SIEM has two parts as shown in Figure 2: SIM (Security Information Management) and SEM (Security Event Management). SIM gathers and analyzes data from various sources, while SEM quickly looks at security events and alerts if something's wrong. Though SIM and SEM used to be separate, now they are part of SIEM, which brings all log data together to find and deal with security threats, making organizations safer [4].

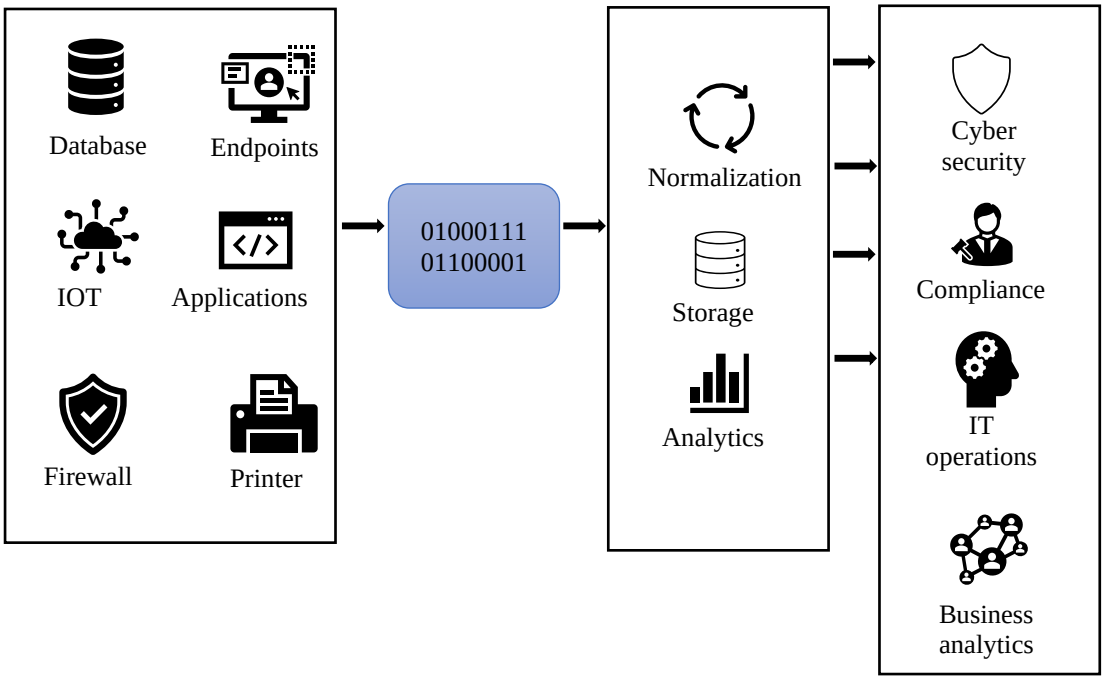

Figure 1. SIEM (Security Information and Event Management).

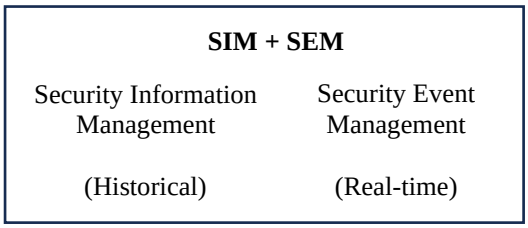

Figure 2. Components of SIEM.

Security Information and Event Management

Security Information and Event Management Process

The SIEM process encompasses four key steps:

1. Collect data from various sources such as network devices, servers, domain controllers, etc.
2. Normalize and aggregate the collected data.
3. Analyze data to identify and uncover potential threats
4. Identify security breaches and assist companies in investigating alerts.

Security Information and Event Management Architecture

The architecture of SIEM focuses on constructing SIEM systems and their essential components. This architecture comprises the following elements (Figure 3):

- Log management
- Log normalization
- Log sources
- SIEM network hosting choices
- Report SIEM products
- Real-time monitoring of SIEM security.

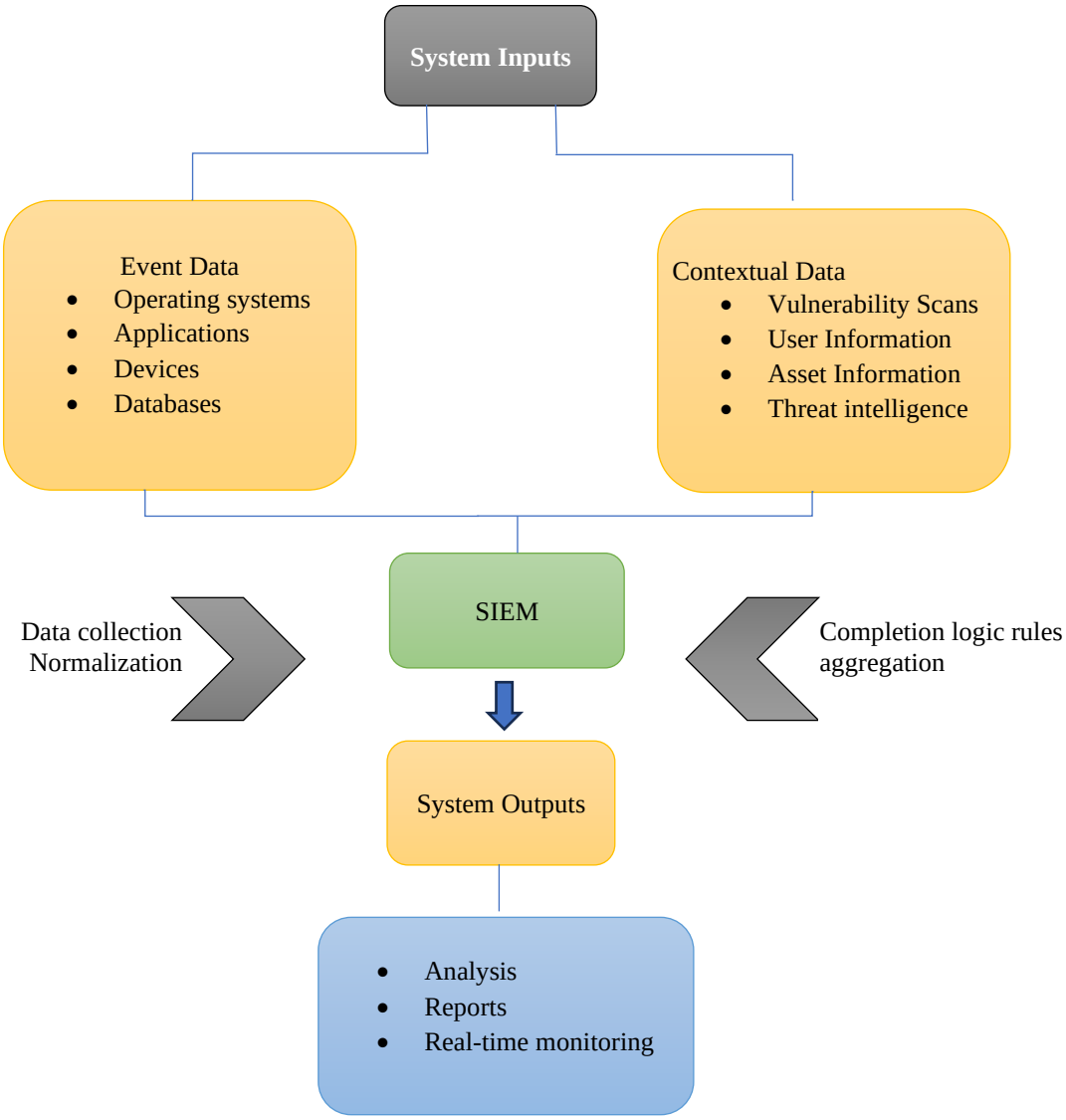

Figure 3. The architecture of SIEM.

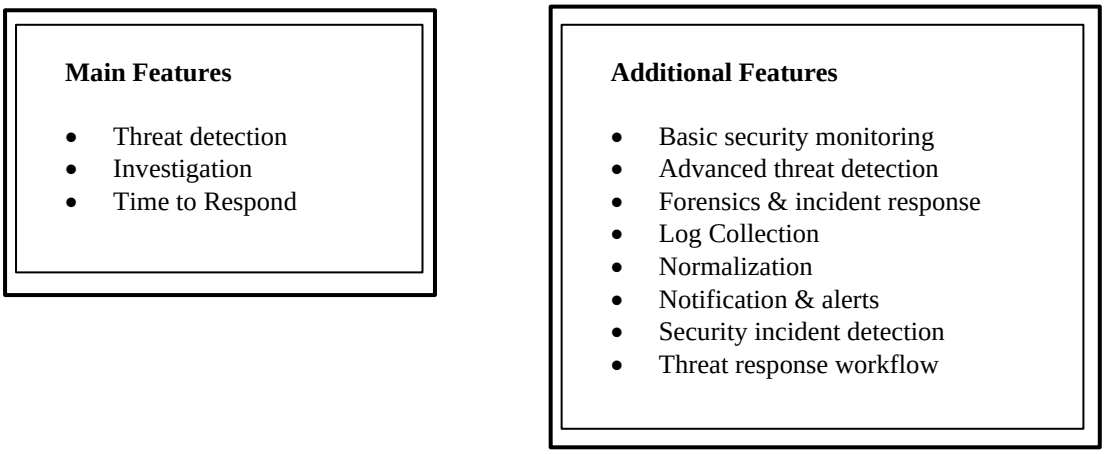

Figure 4. SIEM critical and additional capabilities.

How does SIEM Work?

Security Information and Event Management software is vital in modern cybersecurity. It gathers, organizes, and analyzes large amounts of data logs from various sources like network devices, servers, and applications. Once data is collected, SIEM uses advanced log analytics to find patterns, anomalies, and possible security issues. It sorts through log data, detects security events, and categorizes them by severity. By applying rules, SIEM can tell the difference between normal network activity and suspicious behavior. SIEM has two main goals: improving security and helping with compliance. It generates detailed reports on security events, which are useful for audits, regulations, and internal assessments. It also sends real-time alerts when it detects potential threats or policy violations. These alerts are customizable based on the organization's specific security needs. When something triggers an alert, security teams can investigate and respond quickly.

SIEM Capabilities

The security Information and Event Management system encompasses three pivotal capabilities as depicted in Figure 4:

- Detect threat
- Investigate
- Respond time.

These functions are crucial for strengthening cybersecurity measures by quickly identifying potential threats within an organization's network infrastructure. The threat detection capability allows SIEM to continuously monitor and analyze incoming data streams, promptly flagging any suspicious activities or anomalies that could indicate a security breach. Subsequently, the investigation feature empowers cybersecurity analysts to investigate detected incidents thoroughly, assessing the nature and severity of the threat [5]. Finally, the time to respond aspect underscores the importance of a rapid and effective response strategy. This enables security teams to promptly implement mitigation measures and contain the impact of security breaches, thereby protecting the organization’s confidential data and critical assets.

SIEM CAPABILITIES

Figure 5 outlines essential features of SIEM, such as log collection, log analysis, event correlation, log forensics, IT compliance, application log monitoring, object access auditing, real-time monitoring, user activity monitoring, dashboard, reporting, file integrity monitoring, system and device log monitoring, and log retention [5]. These features enable organizations to manage cybersecurity effectively by gathering, analyzing, correlating, and monitoring security events, and logging from various sources in real-time. They also aid in regulatory compliance, incident investigation, and proactive threat detection, thus improving the total security posture of an organization.

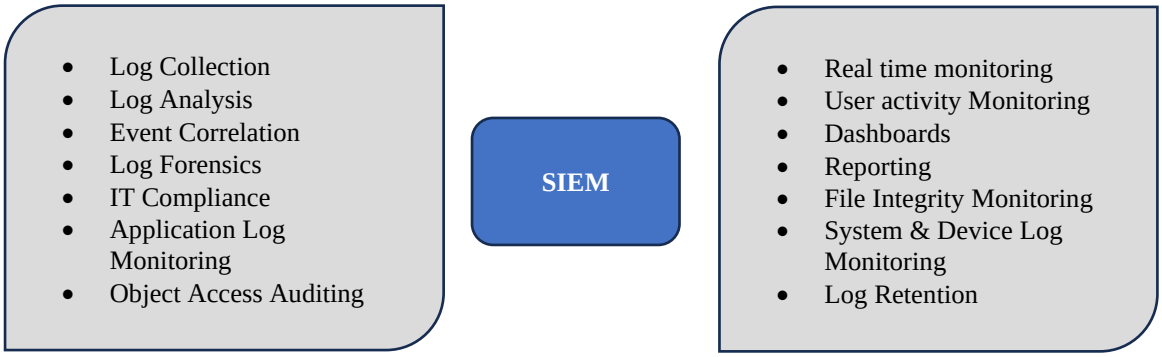

Figure 5. Features of Security Information and Event Management.

User and Entity Behavior Analysis

UEBA is a cybersecurity approach that utilizes ML techniques to monitor and analyze the behavior of users and entities within a network. This includes devices, applications, servers, and more. UEBA systems are skilled at quickly detecting abnormal or potentially malicious activities in real time, promptly alerting security teams, or triggering automated responses. These solutions can seamlessly work alongside or integrate with contemporary security infrastructure, like SIEM systems, to enhance overall security with a more comprehensive and proactive approach. UEBA plays a critical role in strengthening organizations against various threats, such as data breaches, insider risks, fraudulent activities, compromised accounts, and diverse cyberattacks. It achieves this by rapidly identifying and mitigating deviations from standard behavior patterns.

How Does User and Entity Behavior Analysis Work?

UEBA is instrumental in threat detection by flagging activity that diverges from established norms. Its utility extends to monitoring and identifying unusual traffic patterns, unauthorized data access, and suspicious or malicious behavior across computer networks or endpoints [6]. UEBA solutions leverage machine learning algorithms to analyze activity from diverse sources such as network users, hosts, applications, and network traffic, both in real-time and historically, establishing a baseline of typical behavior. Once this baseline is established, UEBA solutions employ diverse analytics methods like simple statistics, pattern matching, and signature rules to pinpoint anomalies indicative of potential threats or malicious activity.

For UEBA solutions to effectively conduct behavioral analytics, organizations must first possess a comprehensive and integrated dataset for their machine learning tools. UEBA systems excel in detecting insider threats, malware, and advanced attacks by harnessing ML and behavioral analytics to scrutinize user behavior, machine activity, as well as entity interactions. They furnish insights to identify malicious activity in real-time, offering investigative insights for analysts to promptly verify and mitigate threats before they escalate and inflict further damage.

UEBA Architecture and Components

The architecture of UEBA adopts an "outside-in" approach, drawing inspiration from Gartner's paradigm for UEBA solutions [7]. This architecture is structured around three key frames of reference: use cases, data sources, and analytics as depicted in Figure 6.

Use Cases

- User and Entity Behavior Analytics solutions provide information on the behavior of users and other entities within the corporate network.
- They monitor, detect, and alert anomalies.
- Unlike specialized tools for specific use cases (such as employee monitoring or fraud detection), UEBA solutions are versatile and applicable across multiple scenarios [8].

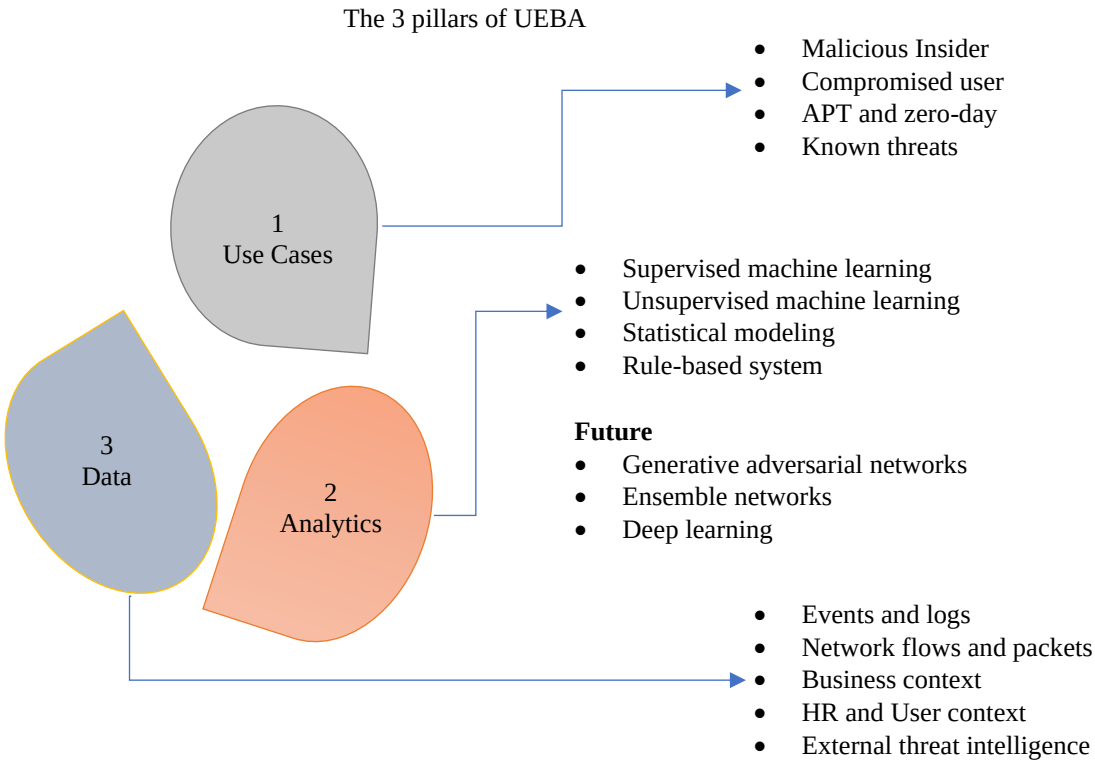

Figure 6. Pillars of UEBA

Data Sources

- User and Entity Behavior Analytics solutions ingest data from various sources, such as a general data repository (like a data lake or data warehouse) or through an SIEM.
- Do not deploy agents directly into the IT environment for collection of data.

Analytics

- User and Entity Behavior Analytics solutions detect anomalies using a variety of analytics approaches Statistical models, Machine learning, Rules, Threat signatures, and more.

LITERATURE REVIEW

SIEM systems serve as the cornerstone of cybersecurity operations, enabling organizations to collect, analyze, and correlate security events from various sources. The proliferation of SIEM vendors, including HP, ArcSight, Symantec, and others, underscores the significance of these platforms in modern cybersecurity strategies. However, traditional SIEM solutions frequently fail to adequately detect emerging threats and recognize abnormal user behavior, underscoring the need for the creation of more sophisticated and proactive strategies. Cybersecurity threats continue to pose significant challenges to organizations worldwide, with increasingly sophisticated attacks targeting sensitive data and critical infrastructure. A comprehensive review of existing literature highlights the evolving nature of cybersecurity threats and the pressing need for robust defense mechanisms. Various studies such as Smith et al. (2021) [9] underscore the escalating frequency and complexity of cyber threats, ranging from malware and phishing attacks to ransomware and insider threats [10].

The evolution of SIEM technology has played a vital role in addressing cyber security challenges. Early SIEM solutions focused on log management and event correlation, offering organizations insights into security events and policy enforcement. However, the effectiveness of traditional SIEM systems in threat detection has been called into question due to their inability to keep pace with the dynamic threat landscape. Notable contributions by Johnson (2018) [11] and Brown and Smith (2017) [12] delve into

the evolution of SIEM technology and its role in detecting cyber threats, highlighting the need for advanced solutions to combat emerging threats effectively.

Despite their utility, traditional SIEM systems exhibit limitations in detecting sophisticated threats, particularly those leveraging advanced evasion techniques. Studies by Chen et al. (2019) [13] and Wang and Zhang (2020) [14] shed light on the shortcomings of traditional SIEM systems in detecting polymorphic malware, insider threats, and zero-day attacks. These limitations underscore the necessity of augmenting SIEM capabilities with advanced technologies like AIML algorithms, as well as User Behavior Analytics (UBA), to enhance threat detection capabilities.

Previous research on the application of artificial intelligence and machine learning algorithms and UBA in cybersecurity has yielded promising results. Studies by Kim et al. (2021) [15] and Gupta and Sharma (2024) [16] explore the efficacy of AI-driven approaches in detecting and mitigating cyber threats, emphasizing the role of ML algorithms in identifying anomalous behavior and patterns indicative of potential security breaches. Furthermore, research by Li and Chen (2023) [17] and Patel et al. (2021) [18] underscores the importance of UBA in enhancing threat intelligence by analyzing user behavior patterns and detecting insider threats.

A comprehensive review of existing literature underscores the escalating nature of cybersecurity threats and the critical role of SIEM technology in threat detection. However, the limitations of traditional SIEM systems necessitate the integration of AI/ML algorithms and UBA to bolster cybersecurity defenses effectively.

Exploring the Constraints of SIEM and UEBA Collaboration

Constraints of SIEM

1. *Lack of contextual information:* SIEM security applications often fall short in providing extensive contextual information tailored to specific organizational needs, which may limit their effectiveness in accurately assessing security events.
2. *Blind spot for unstructured data:* SIEM tools may have blind spots when it comes to handling unstructured data, which can be prevalent in modern IT environments. This limitation could result in overlooking critical security events hidden within unstructured data sources.
3. *Inability to differentiate sensitive data:* Its applications may struggle in the middle of sensitive and non-sensitive data, leading to challenges in distinguishing between legitimate file activities and suspicious actions. This limitation poses risks to data security and intellectual property protection.
4. *Complexity of security event research:* Researching and diagnosing security events within SIEM environments can be labor-intensive and challenging, often requiring extensive time and expertise to uncover and address potential threats effectively.

Constraints of UEBA

1. *Data and processing demand:* UEBA requires substantial volumes of data and processing power to build accurate behavioral models, posing challenges for organizations with limited resources or infrastructure constraints.
2. *Time to establish baseline behavior:* UEBA implementations often require significant time to demonstrate a baseline of normal behavior for users and entities, delaying the detection of abnormal activities and potential threats.
3. *Vulnerability to behavioral changes:* UEBA systems may be susceptible to changes in user behavior or network conditions, leading to potential inaccuracies in threat detection and increased false positives [19].
4. *Privacy and ethical implications:* The implementation of UEBA raises privacy concerns, as it involves monitoring and analyzing user behavior. Organizations must navigate moral considerations and compliance requirements to verify the responsible use of UEBA technologies.

Collaboration Between SIEM and UEBA

Integrating SIEM with UEBA brings together the strengths of both systems to improve overall threat detection. SIEM collects and analyzes logs comprehensively, while UEBA focuses on analyzing user behavior. By combining them, organizations get a more complete view of cybersecurity. SIEM provides a wealth of data for UEBA to analyze user behavior and spot unusual activities. UEBA's ability to recognize patterns and deviations works well with SIEM's event monitoring, allowing for proactive threat detection. This collaboration helps organizations tackle traditional security challenges better, offering insights into both external and insider threats. By using AI/ML algorithms, organizations can refine threat detection further, separate normal from suspicious activities, and prioritize responses. It is a big step forward in cybersecurity, giving organizations a solid defense against evolving threats.

Overview: Gatividhi Guard

The Gatividhi Guard heralds a new era in SIEM technology, revolutionizing cybersecurity defense with its cutting-edge features and capabilities. At its core, the Gatividhi Guard represents a paradigm shift, seamlessly integrating advanced AI and machine learning algorithms to provide real-time analysis of security events. This next-generation SIEM platform is meticulously crafted to address the evolving cybersecurity landscape, offering a comprehensive suite of functionalities designed to fortify organizational defenses. Gatividhi Guard stands out by effectively addressing the constraints encountered in traditional SIEM systems and UEBA collaboration. One of the key challenges faced by organizations is the overwhelming volume of security logs monitored by network analysts, often leading to fatigue and oversight of critical security events. However, the Gatividhi Guard tackles this issue head-on with its innovative AIML algorithms. These algorithms are meticulously trained to differentiate between cyberattacks, normal logs, and false positives, significantly reducing the burden on network analysts and enhancing overall operational efficiency.

Moreover, the Gatividhi Guard goes beyond conventional SIEM capabilities by incorporating advanced features in user behavior analysis modules. In addition to analyzing typical user behavior patterns, the Gatividhi Guard captures intricate details such as mouse movements and user locations, enabling proactive detection of insider threats and abnormal activities. By implementing these advanced functionalities, organizations can effectively identify and mitigate potential security risks, safeguarding against cyber threats in a proactive manner. Furthermore, the collaboration between SIEM and UEBA within the Gatividhi Guard empowers organizations to overcome the limitations of traditional security approaches. By leveraging SIEM's robust infrastructure for log collection and storage, combined with UEBA behavioral analytics, Gatividhi Guard offers enhanced visibility into both external and insider threats [20]. The integration of AI/ML algorithms further augments threat detection capabilities, enabling organizations to differentiate between legitimate and suspicious activities and prioritize security events for prompt response and mitigation.

Gatividhi Guard represents a groundbreaking advancement in cybersecurity defense, offering organizations a comprehensive solution to combat evolving cyber threats. With its innovative features and capabilities, Gatividhi Guard sets a new standard for SIEM technology, enabling organizations to take proactive measures to protect their digital assets and infrastructure.

Benefits of Gatividhi Guard

Advanced Threat Detection

Gatividhi Guard excels in advanced threat detection by leveraging AI-driven algorithms. It identifies and prioritizes security events based on severity and potential impact, detecting unusual patterns or deviations from baseline behavior to proactively mitigate emerging threats.

Sophisticated User Behavior Analysis

Gatividhi Guard incorporates sophisticated user behavior analysis modules, capturing mouse movements and tracking user locations to detect insider threats or compromised accounts. By correlating user activities with security events, it provides actionable insights for timely mitigation measures.

Real-time Monitoring and Analysis

The platform offers real-time monitoring and analysis, promptly identifying and responding to security threats as they occur. By continuously analyzing security events and user behavior patterns, it provides timely alerts and notifications for proactive threat mitigation.

Utilization of Advanced AI/ML Algorithms

Gatividhi Guard harnesses advanced AI/ML algorithms to differentiate normal and suspicious activities, reducing false positives and optimizing threat detection accuracy. It continuously learns from new data and evolving threat landscapes to ensure effective defense mechanisms.

Additional Functionality

Gatividhi Guard introduces extra functionalities like capturing mouse movements and tracking user locations, enhancing insider threat detection. By incorporating these features, it offers a comprehensive solution to cybersecurity challenges and improves overall security posture.

Enhanced Scalability and Flexibility

Gatividhi Guard provides enhanced scalability and flexibility with its modular architecture and cloud-based deployment options, ensuring adaptability to changing data volumes and business needs.

Comprehensive Compliance Management

The platform facilitates comprehensive compliance management by centralizing log data and generating detailed compliance reports, ensuring adherence to regulatory mandates and mitigating compliance risks.

Streamlined Incident Response Workflow

Gatividhi Guard streamlines incident response with integrated incident management capabilities, automating detection, investigation, and remediation processes to minimize response times and reduce data breach risks.

Continuous Threat Intelligence Integration

The platform merges threat intelligence feed to strengthen threat detection capabilities, staying updated on emerging threats and enabling proactive identification and mitigation of cybersecurity risks.

Cost-Effective Security Operations

Gatividhi Guard offers cost-effective security operations by automating routine tasks and optimizing resource utilization, reducing manual workload, and increasing operational efficiency for improved security posture.

Reduced Workload on Network Analysts

By automating repetitive tasks and streamlining security operations, Gatividhi Guard significantly reduces the workload on network analysts. This allows them to focus on high-priority tasks and critical security incidents, improving overall security responsiveness.

IMPLEMENTATION AND DEPLOYMENT OF GATIVIDHI GUARD

Architecture Design

Gatividhi Guard's architecture is tailored to handle the intricacies of modern cybersecurity threats, ensuring scalability, reliability, and efficiency. The architecture consists of interconnected modules, each serving distinct roles in threat detection and user behavior analysis.

Log Collection Module

Responsible for gathering logs from diverse sources like network devices, servers, applications, etc., in real-time for prompt detection and response to security events.

Parsing and Normalization Module

Standardizes the format and structure of collected logs to ensure consistency and compatibility across different sources, facilitating seamless integration and analysis**.**

Rule Engine

Defines and enforces security policies and detection rules. Evaluate incoming logs against predefined criteria to identify security events and trigger appropriate actions such as generating alerts or initiating incident response procedures.

AI/ML Algorithms

Utilizes advanced Artificial Intelligence and Machine Learning algorithms to enhance traditional rule-based detection with intelligent, data-driven analysis. Learns from historical log data and adapts to evolving threats for proactive threat detection and mitigation.

Behavior Analysis Module

Monitors and analyzes user activities across the organization's digital environment. Captures various behaviors like mouse movements, keystrokes, and application usage to detect anomalies indicative of insider threats or compromised accounts.

Event Monitoring Dashboard

Provides security analysts with a centralized interface for monitoring security events, investigating incidents, and managing alerts. Presents actionable insights derived from log analysis, AI/ML algorithms, and user behavior profiling to enable informed decision-making and effective incident response.

Deployment Strategy

Deploying Gatividhi Guard involves a systematic approach to ensure seamless integration with existing IT infrastructure and optimal performance in diverse environments as shown in Figure 7.

Infrastructure Assessment

Developed an assessment of the organization's IT infrastructure to identify requirements, dependencies, and compatibility considerations for Gatividhi Guard's deployment.

Installation and Configuration

Install and configure Gatividhi Guard according to the organization's needs and preferences, setting up platform components, integrating with existing systems, and establishing communication channels for log collection and analysis.

Integration with Existing Systems

Seamlessly integrate Gatividhi Guard with existing security systems and tools, ensuring interoperability and data exchange for holistic threat detection and response capabilities.

Training AI/ML Models

Train AI/ML models using historical log data to enhance accuracy in detecting and mitigating cyber threats, iteratively refining algorithms based on feedback and performance metrics.

Testing and Validation

Conduct rigorous testing and validation procedures, including simulating threat scenarios and measuring response capabilities under different conditions, along with user acceptance testing (UAT) to address usability and functionality issues.

Deployment Rollout

Deploy Gatividhi Guard in a phased approach, starting with pilot deployments to validate functionality before expanding to full deployment across the organization. Continuously monitor and optimize throughout the rollout process.

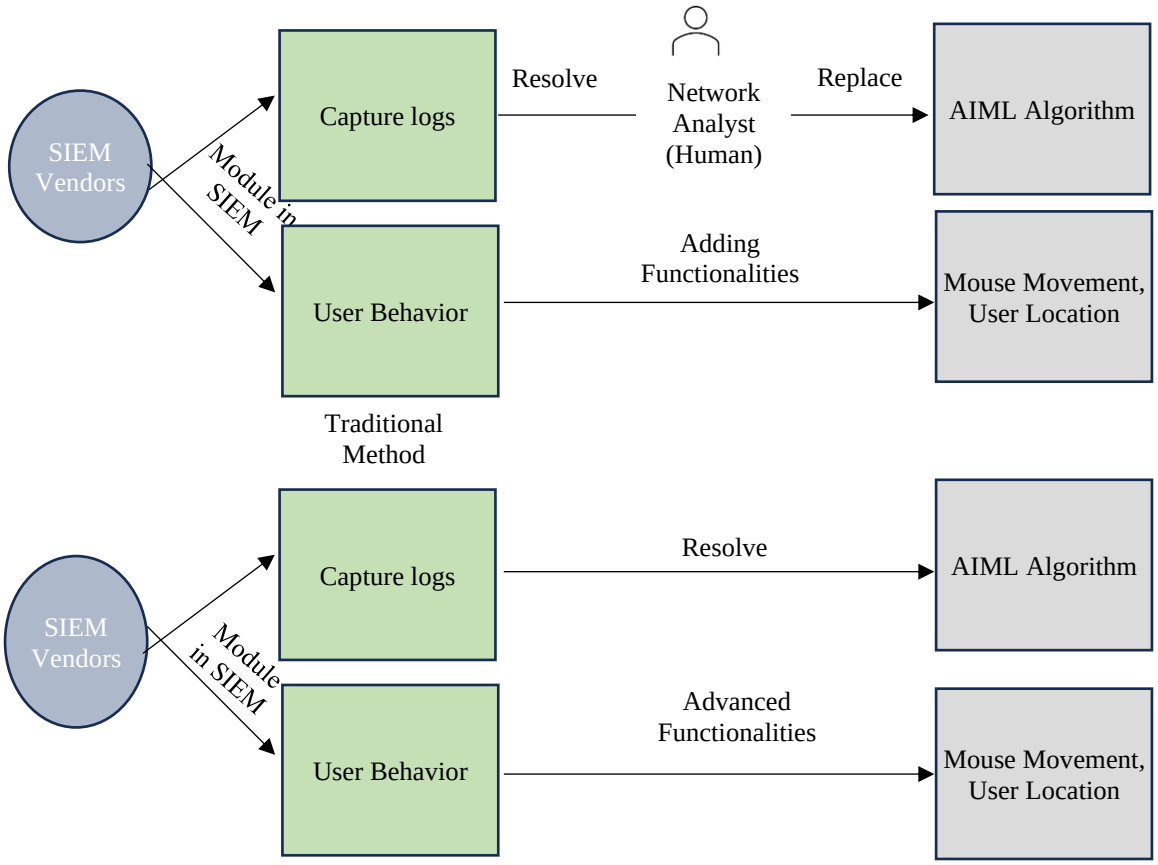

Figure 7. Deployment of Gatividhi Guard.

Gatividhi Guard prioritizes scalability, flexibility, and adaptability in its implementation and deployment strategy to address modern organizations' evolving cybersecurity needs. By integrating advanced AI/ML algorithms with comprehensive user behavior analysis, Gatividhi Guard enables proactive threat detection, mitigation, and prevention.

Pseudocode for Threat Detection Algorithm

```
function detect Threats(logs):
 for log in logs:
 if is Potential Threat(log):
 analyze Log(log)
 if is Attack(log):
 alert Security Team(log)
function is Potential Threat(log):
 return contains Suspicious Activity(log)
function analyze Log(log):
function is Attack(log):
 return log Matches Attack Pattern(log)
function alert Security Team(log):
```

This pseudocode outlines a basic threat detection algorithm for an SIEM system. It iterates through logs, checking for potential threats based on suspicious activity. If a potential threat is found, the log is

analyzed further to determine if it matches known attack patterns. If an attack is detected, the security team is alerted. The pseudocode emphasizes the importance of identifying and responding to security events efficiently within an organization's IT infrastructure.

Pseudocode for User Behavior Analysis Algorithm

```
function analyze User Behavior(logs):
 for log in logs:
 if is User Activity(log):
 analyze User(log)
 if is Suspicious Behavior(log):
 flag As Potential Threat(log)
function is User Activity(log):
 return is User Log(log)
function analyze User(log):
function is Suspicious Behavior(log):
 return has Suspicious Patterns(log)
function flag As Potential Threat(log):
```

This pseudocode outlines a user behavior analysis algorithm within an SIEM system. It iterates through logs, focusing on user activities and analyzing them for suspicious behavior. If suspicious behavior is detected, the log is flagged as a potential threat. The algorithm emphasizes the importance of monitoring user actions to identify anomalous behavior indicative of security risks within an organization's digital environment.

RESULTS

After the implementation and deployment of the Gtividhi Guard, several significant results in the cybersecurity posture.

Enhanced Threat Detection

- Utilizes advanced AI and machine learning algorithms for enhanced threat detection.
- Analyzes security events in real-time to proactively identify potential cyber threats.
- Accurately differentiates between normal logs, false positives, and genuine security incidents, reducing false alarms.

Improved Incident Response

- Empowers organizations with timely and actionable insights into security events.
- Provides a centralized event monitoring dashboard for swift and effective incident response.
- Facilitates seamless incident coordination and response through integration with existing security systems.

Comprehensive User Behavior Analysis

- Captures and analyzes user activities across the digital environment.
- Detects anomalous or suspicious activities indicative of insider threats or compromised accounts.
- Strengthens overall cybersecurity defenses by mitigating insider threats effectively.

Scalability and Flexibility

- Highly scalable and adaptable architecture suitable for diverse organizational environments.
- Offers deployment options in on-premises or cloud environments to meet varying needs.

- Easy integration with contemporary IT infrastructure and security system for customization and expansion.

Proactive Cybersecurity Defense

- Adopts a proactive approach to cyber security by merging advanced threat detection and user behavior analysis.
- Identifies and mitigates cyber threats before they escalate, minimizing the risk of data breaches and financial losses.
- Empowers organizations to identify and prevent insider threat attacks, further strengthening cybersecurity defenses.

Pseudocode Algorithm Results

- Threat Detection Algorithm:
- Enhances detection accuracy by effectively identifying potential threats.
- Triggers timely alerts to the security team for swift response and mitigation.
- Reduces false alarms through advanced analysis techniques and machine learning models.

User Behavior Analysis Algorithm

- Provides comprehensive insights into user activities across the digital environment.
- Detects insider threats and suspicious activities for proactive threat mitigation.
- Enables proactive identification of anomalous user behavior for preventive measures.

CONCLUSION

This research paper has shed light on the critical role of NextGen. Security Information and Event Management systems, exemplified by Gatividhi Guard, in fortifying cybersecurity defenses against evolving threats. Through an in-depth exploration of Gatividhi Guard's architecture, capabilities, and deployment strategies, several key findings have emerged.

Firstly, the collaboration of advanced AIML algorithms into SIEM platforms such as Gatividhi Guard represents a transformative shift in cybersecurity defense. By harnessing the power of AI-driven analytics, organizations can proactively identify and prevent cyber threat attacks, enhancing overall security posture and resilience. Secondly, the incorporation of UBA modules within SIEM systems adds an extra layer of defense against insider threats and malicious activities. Features such as capturing mouse movements and tracking user locations enable organizations to identify anomalous behavior patterns indicative of potential security risks, empowering them to take proactive measures to safeguard their digital assets.

The significance of adopting next-generation SIEM technologies like Gatividhi Guard cannot be overstated. For organizations seeking to enhance their cybersecurity defenses, it is imperative to embrace innovative solutions that leverage advanced AIML algorithms and UBA capabilities. By investing in such technologies, organizations can exceed emerging threats and prevent cybersecurity risks effectively. Looking ahead, future research and development in the field of SIEM should focus on further refining AI/ML algorithms and enhancing UBA functionalities to keep pace with evolving cyber threats. Additionally, there is a need for continued collaboration between industry researchers, cybersecurity experts, stakeholders, etc., to drive innovation and address emerging challenges in cybersecurity defense.

In conclusion, the deployment of next-generation SIEM systems like Gatividhi Guard offers organizations a proactive approach to cybersecurity, enabling them to detect, mitigate, and prevent cyber threats effectively. By embracing advanced AIML algorithms and UBA capabilities, organizations can empower their cyber security defenses and safeguard digital assets in today's dynamic threat landscape.

Declaration of Interest

The authors declare that there is no conflict of interest for the publication of this paper. Our professional judgment concerns the validity of the work presented in this paper has not been influenced by any secondary interest, including financial gain.

Acknowledgment

We would extend our gratitude to individuals who contributed to the completion of this paper. Special thanks to Dr. Yogita Gigras and Dr. Shilpa Mahajan for their valuable guidance and support throughout the research process. Their knowledge and support have played a crucial role in influencing the content of this paper.

Additionally, we extend our appreciation to Mazars, our organization, for their continuous support and provision of resources, which facilitated the completion of this work.

REFERENCES

1. Williams A. Security information and event management technologies. Siliconindia. 2006;10: 34–35.
2. Arora K, Mahajan S. Detecting denial-of-service attack using dendritic cell approach. In: Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020. Springer: Singapore; 2021. pp. 509–516.
3. Liu H. (Vol. 1994, No. 1, p. 012021) A insider threat detection system based on user and entity behavior analysis. In: Journal of Physics: Conference Series. IOP Publishing; 2021.
4. Roohparvar R. (2019). What is SIEM software? How it works and how to choose the right tool? - Cyber Security Solutions, Compliance, and Consulting Services - IT Security. [online] Cyber Security Solutions, Compliance, and Consulting Services - IT Security - We offer It security management, data, network, & Information security services for protecting information & mitigating security risks to your organization. Available from: https://www.infoguardsecurity.com/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool/.
5. Abidar R, Moummadi K, Moutaouakkil F, Medromi H. Intelligent and pervasive supervising platform for information system security based on multi-agent systems. International Review on Computers and Software. 2015;10:44–51. DOI: 10.15866/irecos.v10i1.4699.
6. Gates C, Taylor C. Challenging the anomaly detection paradigm: A provocative discussion. In: Proceedings of the 2006 Workshop on New Security Paradigms 2006 Sep. 19. 2006. pp. 21–29. DOI: 10.1145/1278940.1278945.
7. Quadrant M. Magic quadrant for security information and event management. Magic Quadrant. 2014:1–16.
8. Customize anomaly scoring rules – splunk documentation. Splunk.com. Available from: https://docs.splunk.com/Documentation/UBA/5.0.5.1/Admin/ScoringRules.
9. Salehi V, Veitch B, Smith D. Modeling complex socio-technical systems using the FRAM: A literature review. Human Factors and Ergonomics in Manufacturing and Service Industries. 2021;31:118–142. DOI: 10.1002/hfm.20874.
10. Fan CI, Tseng YF, Su HP, Hsu RH, Kikuchi H. Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks. International Journal of Information Security. 2020;19:245–255. DOI: 10.1007/s10207-019-00476-5.
11. Johnson A. CCNA Cybersecurity Operations Companion Guide. Cisco Press; 2018.
12. Yang IA, Brown JL, George J, Jenkins S, McDonald CF, McDonald VM, et al. COPD-X Australian and New Zealand guidelines for the diagnosis and management of chronic obstructive pulmonary disease: 2017 update. Medical Journal of Australia. 2017;207:436–442. DOI: 10.5694/mja17.00 686.
13. Najafi P, Mühle A, Pünter W, Cheng F, Meinel C. MalRank: A measure of maliciousness in SIEM-based knowledge graphs. In: Proceedings of the 35th Annual Computer Security Applications Conference. 2019. pp. 417–429. DOI: 10.1145/3359789.3359791.

14. Inderwildi O, Zhang C, Wang X, Kraft M. The impact of intelligent cyber-physical systems on the decarbonization of energy. Energy and Environmental Science. 2020;13:744–771. DOI: 10.1039/C9EE01919G.
15. Ali S, DiPaola D, Lee I, Sindato V, Kim G, Blumofe R, et al. Children as creators, thinkers and citizens in an AI-driven future. Computers and education. Artificial Intelligence. 2021;2:100040.
16. Singh S, Gupta H, Sharma P, Sahi S. Advances in artificial intelligence (AI)-assisted approaches in drug screening. Artificial Intelligence Chemistry. 2024;2:100039. DOI: 10.1016/j.aichem.2023.100039.
17. Li H, Chen W, Tan X, Tan X. Back analysis of geomechanical parameters for rock mass under complex geological conditions using a novel algorithm. Tunnelling and Underground Space Technology. 2023;136:105099. DOI: 10.1016/j.tust.2023.105099.
18. Patel N, Corbett B, Mhaskar P. Model predictive control using subspace model identification. Computers and Chemical Engineering. 2021;149:107276. DOI: 10.1016/j.compchemeng.2021.107276.
19. Sharma S, Mahajan S. Design and implementation of a security scheme for detecting system vulnerabilities. International Journal of Computer Network and Information Security. 2017;9:24–32. DOI: 10.5815/ijcnis.2017.10.03.
20. Amos Z. Combine machine learning and UEBA for advanced threat detection. Isa.org. Available from: https://gca.isa.org/blog/combine-machine-learning-and-ueba-for-advanced-threat-detection.

