Технічні науки

UDC 004.056.5:004.89

Dashevskyi Artem
Independent Researcher
(Ukraine, Kryvyi Rih)
Дашевський Артем
незалежний дослідник
(м. Кривий Ріг, Україна)

UEBA AND AI IN BUILDING ADAPTIVE CYBERSECURITY
UEBA ТА ШТУЧНИЙ ІНТЕЛЕКТ У ПОБУДОВІ АДАПТИВНОЇ КІБЕРБЕЗПЕКИ

Summary. *This article explores the application of artificial intelligence and user and entity behavior analytics (UEBA) in building adaptive cybersecurity strategies. It outlines the core components of UEBA systems, including data collection, behavioral modeling, anomaly detection, and automated response mechanisms. Particular attention is given to the role of AI in reducing false positives and detecting novel, non-obvious threats. Practical use cases are discussed, such as compromised account detection, risk scoring, and adaptive authentication. The article also addresses implementation challenges related to data integration, privacy, and cross-functional collaboration. UEBA is presented as a shift from reactive to proactive cybersecurity enabled by intelligent automation.*

Key words: *UEBA, artificial intelligence, user behavior, cyberattack, cybersecurity, threat detection, adaptive defense systems, vulnerability.*

Анотація. *У статті розглянуто застосування штучного інтелекту та аналітики поведінки користувачів (UEBA) для побудови адаптивної стратегії кіберзахисту. Визначено ключові компоненти систем UEBA,*

включаючи збір даних, створення моделей поведінки, виявлення аномалій та механізми реагування. Особливу увагу приділено ролі ІІ у зменшенні кількості хибних спрацювань та виявленні нових, нетипових загроз. Наведено приклади використання UEBA для захисту облікових записів, оцінки ризиків та адаптивної автентифікації. Також проаналізовано виклики впровадження, зокрема питання конфіденційності, інтеграції даних та потребу в міжфункціональній взаємодії. UEBA представлено як перехід від реактивного до проактивного кіберзахисту.

Ключові слова: *UEBA, штучний інтелект, поведінка користувачів, кібератака, кібербезпека, виявлення загроз, адаптивні системи захисту, вразливість.*

Introduction. With the advancement of artificial intelligence, cyberattacks have become more sophisticated, frequent, and destructive—especially considering that threats such as insider attacks and credential theft often bypass traditional security measures. To stay ahead of these threats, innovative approaches to cybersecurity are required, capable of detecting subtle and complex behavioral patterns. This is where User and Entity Behavior Analytics (UEBA) plays a crucial role. UEBA leverages the power of artificial intelligence (AI) to monitor user activities, detect anomalies, and identify potential insider threats. AI has transformed UEBA into an adaptive security strategy, enabling organizations to proactively detect unusual behavior and strengthen their cybersecurity posture.

Threat Landscape and Limitations of Traditional Detection Methods

Cybercriminals are increasingly employing artificial intelligence and machine learning to automate and enhance the effectiveness of their attacks, including AI-powered phishing campaigns and malware that adapts to evade detection. AI enables the scaling and sophistication of attacks, while AI-based tools assist in reconnaissance, target selection, and execution of cyber operations.

Traditionally, conducting cyberattacks required significant technical expertise. Now, generative AI tools can create exploit scripts, phishing emails, and variants of malicious software with the click of a button [3]. This means that even less-skilled individuals can launch highly effective attacks, increasing both the frequency and complexity of cyber threats.

For instance, AI-powered tools can generate highly convincing targeted phishing emails directed at specific individuals, making detection significantly more difficult. Attackers can also create malware that constantly evolves to avoid signature-based detection.

Unlike static, pre-programmed attacks, AI-driven cyber threats can dynamically change tactics. For example, malware may rewrite its own code to evade detection by antivirus software.

Historically, security systems have relied on predefined rules and pattern matching to detect threats. While effective against known threats, these approaches struggle to detect new or well-camouflaged attacks. For example, signature-based systems such as traditional intrusion detection systems (IDS) may fail to identify low-and-slow behavioral threats or attacks utilizing modern AI-driven techniques [7].

Behavior-Based Security and UEBA Foundations

For many years, security teams have relied on threat intelligence feeds and correlation rules to identify cyber threats. However, these traditional methods have proven insufficient in preventing attacks powered by artificial intelligence.

Threat intelligence gathers information on known indicators of compromise (IOCs), such as malware signatures, suspicious IP addresses, and attack patterns, and alerts security teams when matches are detected [2]. However, this method has a major limitation: AI-generated attacks often lack recognizable IOCs.

Since AI can generate unique, tailored variations of attacks for each target, conventional threat intelligence channels struggle to keep up. Attackers can easily

modify code structure, execution methods, and attack mechanisms, making detection through signature-based defenses nearly impossible.

As a result, traditional defense mechanisms lag behind AI's ability to adapt and generate attacks that do not match any known patterns.

In response, security teams are increasingly turning to behavior-based detection methods, such as User and Entity Behavior Analytics (UEBA), which uses machine learning to detect anomalies in user behavior that may indicate account compromise or other threats [1].

The integration of artificial intelligence and machine learning into security systems has significantly enhanced the effectiveness of UEBA. Techniques such as clustering, classification, and anomaly detection enable UEBA systems to process vast amounts of data and identify subtle behavioral changes that would otherwise go unnoticed by humans or static rules.

Core Components of UEBA Systems

UEBA solutions typically consist of four key components that work together to detect and respond to threats:

1. **Data collection** involves gathering information from various sources, including identity and access management (IAM) systems, security information and event management (SIEM) tools, Active Directory logs, VPN access records, endpoint detection and response (EDR) platforms, cloud service logs, and application or database access logs [10].
2. After collecting data, the system builds baseline models to analyze typical behavior of users and entities, including login habits, application usage, network activity, and device interactions.
3. **Anomaly detection** compares current activity against the baselines using methods such as statistical thresholding, peer group analysis, time-series analysis, and machine learning techniques [4].
4. Finally, **alerting and response mechanisms** correlate anomalies and prioritize them to reduce false positives. These mechanisms are often

integrated with Security Orchestration, Automation, and Response (SOAR) platforms to trigger automated actions such as account lockout, network isolation, or step-up authentication.

The Role of Artificial Intelligence in UEBA:

1. One of AI's key strengths lies in its ability to analyze massive volumes of data and detect patterns that may go unnoticed by human analysts. With UEBA, AI-based systems can establish baselines of normal behavior for users and organizations [6]. Any deviation from these baselines is flagged as an anomaly, indicating potential security risks.
2. AI-powered UEBA systems consider various contextual factors when analyzing behavior. These include the user's role, job responsibilities, location, time of day, and device used — all to determine whether behavior is legitimate or suspicious.
3. AI leverages machine learning models that continuously improve and adapt based on new data. Over time, these models become more accurate, leading to better detection of anomalies and more effective threat identification.
4. AI assigns **risk scores** to various actions based on their severity and the likelihood that they are malicious. This enables security teams to prioritize responses and focus on high-risk behaviors requiring immediate attention.
5. AI creates **behavioral profiles** for each user and entity by learning their typical activity patterns. When an action significantly deviates from these baselines, the AI system generates alerts to assist security teams in investigations.
6. AI's analytical capabilities help **reduce false positives**, allowing security personnel to concentrate on actual threats instead of being overwhelmed by benign anomalies.

By establishing baseline indicators of normal activity and applying machine learning to detect deviations, UEBA enhances detection efficiency

compared to traditional rule-based systems and enables faster and more accurate incident response.

Use Cases and Practical Applications

Thanks to its ability to detect behavioral anomalies in real-time, UEBA supports a wide range of cybersecurity applications.

One of the most critical functions of UEBA is **data protection and identity management**. It can detect unusual data transfers, unauthorized access attempts, and suspicious activities — including covert channels and tunneling [8].

When integrated with Identity and Access Management (IAM), UEBA and AI can provide **real-time behavioral analytics** [10]. By analyzing login data, device usage, and user behavior, the system can tailor authentication responses — enabling seamless access for low-risk users, prompting multi-factor authentication for medium-risk users, or blocking access for high-risk profiles.

Most importantly, UEBA assists in detecting **compromised accounts** in real time through anomalies such as logins from unusual locations or **impossible travel scenarios**. Combined with threat intelligence, this helps organizations identify known attack tactics.

For example, UEBA can detect when:

- A user logs in from an unusual location at an atypical time.
- A privileged account accesses sensitive files it has not previously interacted with.
- A system begins transmitting unusually large volumes of data to an external service.

By analyzing behavior patterns rather than relying on predefined rules, UEBA can identify **subtle, emerging threats** that other tools may overlook.

Table 1

Evaluation of Cyberattack Threat Detection Strategies

Feature	UEBA (User and Entity Behavior Analytics)	Correlation Rules (Logic Trees)	Threat Intelligence Feeds
Detection of unknown threats	Uses machine learning to detect behavioral anomalies and identify previously unknown attack patterns.	Uses predefined templates and signatures; cannot detect new, unknown attack vectors.	Can only detect threats that have already been identified and published in the threat intelligence community.
Adaptation to AI-driven attacks	Continuously learns and adapts to new behavior patterns, making it ideal for combating evolving AI-driven threats.	Rules must be manually updated; cannot keep up with the rapid evolution of AI-driven attacks.	Relies on detection and dissemination of known threats; does not provide protection against novel AI-based threats.
False positive rate	Context-aware understanding of normal behavior reduces the number of false alerts.	Rigid rules can generate many false positives, overwhelming security teams.	Depends on the accuracy and relevance of aggregated intelligence.
Detection speed	Quickly detects deviations from normal behavior, enabling faster response.	Detection is as fast as the comprehensiveness of the rules; new threats may go unnoticed.	Dependent on external updates, which may delay detection of emerging threats.
Resource efficiency	Automates detection processes, reducing the need for constant manual oversight.	Requires constant rule creation and tuning, which is resource-intensive.	Easy to collect information, but lacks autonomous threat detection capabilities.
Detection of complex attacks	Detects subtle, sophisticated attacks that mimic normal behavior.	Cannot detect complex attacks that fall outside existing rule logic.	Can only identify known complex threats; fails to detect zero-day or novel attacks.
Scalability	Effectively handles large datasets and diverse environments.	Becomes unmanageable as rule complexity increases.	Scales with volume of shared intelligence but lacks proactive detection capabilities.
Resistance to AI evasion tactics	Difficult for attackers to accurately mimic normal behavior to evade detection.	AI-driven attacks can easily bypass rigid rules by exploiting their inflexibility.	Attackers can change tactics faster than threat data can be updated.

Advanced AI Techniques in Cybersecurity

Machine Learning (ML) is a branch of artificial intelligence that enables systems to learn from data and improve their performance without being explicitly programmed [5]. In the field of cybersecurity, a common application of ML is **User and Entity Behavior Analytics (UEBA)**, which detects threats by analyzing patterns and behaviors. Machine learning excels at tasks such as identifying anomalies in network traffic and preventing attacks by recognizing abnormal behavior before it escalates.

Deep learning, a subtype of machine learning, uses neural networks to analyze complex datasets and is particularly effective at identifying sophisticated cybersecurity threats, such as emerging strains of malware [7]. In cybersecurity, deep learning is applied to detect **polymorphic malware**, which continuously alters its code to evade traditional detection techniques.

Deep learning models are capable of processing massive amounts of data and detecting behavioral patterns in malware—even when the code differs. For instance, deep learning can identify anomalies in how files interact with a system and signal malicious intent, even if the malware has not been previously encountered [1].

This ability to learn from subtle behavioral patterns significantly reduces detection and response times to previously unknown threats, making deep learning essential for staying ahead of sophisticated cyberattacks.

Neural networks are AI models inspired by the human brain. Within these networks, nodes process data using weighted inputs. Each node evaluates the input and adjusts the weights to improve accuracy. The final output is based on the sum of these evaluations. In cybersecurity, neural networks help analyze vast datasets—such as firewall logs—to identify patterns and predict potential threats, making them a powerful tool for threat detection.

Large language models such as GPT-4 represent another significant AI technology in the field of cybersecurity. These models specialize in processing and understanding human language, making them highly useful for automating

threat analysis and improving the effectiveness of security measures [8]. They can analyze vast volumes of textual data—such as threat reports, logs, and documentation—to identify potential risks and patterns that may indicate an attack.

Language models also assist with tasks such as phishing detection, generating human-readable threat reports, and automating incident response. By understanding context, they enhance cybersecurity tools, enabling faster and more accurate decision-making.

While the implementation of UEBA enables effective threat detection, it also presents several challenges.

Organizations may face data integration issues, as UEBA requires large volumes of data from diverse sources such as network logs, authentication systems, endpoints, and cloud services [2]. Consolidating and normalizing this data, especially in fragmented or legacy environments, can be complex and resource-intensive.

It is also important for organizations to establish baselines of normal behavior, since UEBA systems operate by recognizing deviations from typical user activity. This can be particularly difficult in dynamic environments where roles or behaviors frequently change. Limited historical data or inconsistent patterns may result in false positives or false negatives, undermining trust in alerts during the early stages of deployment.

Privacy concerns and regulatory compliance may also impact implementation. Detailed user monitoring via UEBA can raise privacy issues [5]. To ensure legal and ethical compliance, organizations must implement proper governance, data anonymization, and transparency.

Finally, effective use of UEBA requires expertise in machine learning, behavioral analytics, and cybersecurity—skills that small organizations often lack. The financial burden of acquiring, deploying, and maintaining UEBA tools, along with ongoing tuning and incident response, can be prohibitive.

To address these challenges, organizations need a strategic, phased approach that includes effective data management, cross-functional collaboration, and investment in skill development and technology [8].

Conclusion. AI has transformed UEBA from a reactive cybersecurity approach into a proactive and adaptive defense strategy. By leveraging AI's capabilities in data analysis, pattern recognition, and machine learning, organizations can detect unusual behavior, identify insider threats, and enhance overall cybersecurity. As UEBA continues to evolve, it is becoming a powerful tool that enables organizations to stay one step ahead of cybercriminals.

References

1. Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Review. *Computer Communications*, 170, 19–41.

2. Alotaibi, A., & Rassam, M. A. (2023). Adversarial Machine Learning Attacks on Intrusion Detection Systems: A Review of Strategies and Defenses. *Future Internet*, 15(62).

3. Gkinko, L., & Elbanna, A. (2023). Appropriation of Conversational AI in the Workplace: A Taxonomy of AI Chatbot Users. *International Journal of Information Management*, 69.

4. Dewis, M., & Viana, T. (2022). Phish Responder: A Hybrid Machine Learning Method for Detecting Phishing and Spam Emails. *Applied System Innovation*, 5(4), 73.

5. Kamara Amadou Sara. (2024). The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems. *Security Issues*, 1. Retrieved from https://cyberleninka.ru/article/n/the-role-of-cognitive-information-technologies-in-cybersecurity-threat-detection-and-adaptive-defense-systems (accessed: 04.07.2025).

6. Kandhro, I. A., Alanzi, S. M., Ali, F., et al. (2023). Real-Time Detection of Malicious Intrusions and Attacks in IoT-Enabled Cybersecure Infrastructures. *IEEE Access*, 11, 9136–9148.

7. Mughaid, A., AlZu'bi, S., Hnaif, A., et al. (2022). An Intelligent Phishing Detection System in Cybersecurity Using Deep Learning Techniques. *Cluster Computing*, 25, 3819–3828.

8. Rizvi, W. (2023). Strengthening Cybersecurity: The Power of Artificial Intelligence in Threat Detection and Prevention. *International Journal of Advanced Engineering and Research Science (IJAERS)*, 10(5).

9. Juanes-Martino, F., Alaiz-Rodriguez, R., Gonzalez-Castro, V., et al. (2023). Email Spam Detection: An Analysis of Spammer Strategies and Dataset Shift Challenges. *Artificial Intelligence Review*, 56, 1145–1173.

10. Chio, C., & Freeman, D. (2018). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. 1st ed., O'Reilly Media, pp. 25–45.