International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Unmasking the Shadows: Recognizing and Overcoming Hidden Pitfalls in UEBA

Kumrashan Indranil Iyer

Email: Indranil.iyer[at]gmail.com

Abstract: ***User and Entity Behavior Analytics (UEBA) has revolutionized cybersecurity by enabling dynamic, behavior-based threat detection. By modeling normal behavioral patterns, UEBA identifies insider threats, compromised credentials, and advanced persistent threats (APTs) that traditional signature-based and rule-based systems often overlook. However, several challenges such as data bias, model drift, false positives, and adversarial exploitation, pose significant risks to its efficacy. This paper examines these hidden pitfalls, their symptoms and proposes effective mitigation strategies. By addressing these challenges, organizations can enhance the resilience and accuracy of behavioral analytics, strengthening enterprise security.***

Keywords: User and Entity Behavior Analytics (UEBA), cybersecurity, anomaly detection, machine learning, adversarial attacks, model drift, insider threats

1.Introduction

As cyber threats continue to evolve, the limitations of traditional rule-based cybersecurity solutions have become increasingly evident. The growing dominance of insider threats and sophisticated, stealthy attack techniques has driven organizations to seek advanced detection methods leading to the widespread adoption of User and Entity Behavior Analytics (UEBA). UEBA solutions leverage machine learning (ML) to establish baseline activity patterns and detect deviations that may indicate malicious or anomalous behavior [1]. Compared to static, signature-based, this behavior-based approach enhances the detection of previously unknown threats, accelerates response times, and provides a more holistic view of user and entity interactions.

Despite these advantages, UEBA implementations face several challenges. Hidden vulnerabilities can undermine the effectiveness and reliability of UEBA solutions, exposing organizations to undetected breaches or an overwhelming volume of false positives. Additionally, concerns related to data privacy, regulatory compliance, and computational overhead further complicate large-scale adoption [2]. This research article aims to unmask the hidden pitfalls of UEBA by examining critical challenges such as model drift, data bias, adversarial manipulation, and the complexities of enterprise-scale deployment. This article also concludes with strategic recommendations to mitigate these risks and enhance the resilience of UEBA-driven cybersecurity defenses.

1.1 Research Objectives

1. **Identify** pitfalls that can undermine UEBA's reliability.
2. **Analyze** how these pitfalls manifest in practical deployments.
3. **Propose** tactical and strategic solutions for mitigating these vulnerabilities, preserving UEBA's value proposition.

2.Literature Review

2.1 UEBA Emergence and Core Principles

The concept of baselining normal user and system behavior dates back to early anomaly detection research in network security [3]. As the volume and variety of enterprise data expanded, researchers integrated machine learning algorithms to identify subtle deviations indicative of threats [4]. UEBA expanded from earlier "User Behavior Analytics" to incorporate not just human users but also entities such as networked devices, servers, and service accounts.

This shift provided three main benefits:

1. **Insider Threat Detection:** Identifying privileged users who deviate from their typical access or usage patterns.
2. **Entity Behavior Visibility:** Monitoring servers, endpoints, and machine accounts for abnormal usage or connections.
3. **Adaptive Learning:** Adjusting to changing usage patterns and organizational structures more flexibly than static rules.

2.2 Pitfalls and Hidden Vulnerabilities in UEBA

Despite the growing adoption of UEBA, research has begun to identify several key pitfalls. One major issue is model drift, where evolving data patterns can cause baselines to become outdated [5]. False positives continue to be a significant concern, particularly when employees return from leave or switch roles, triggering unwanted alerts for unusual behavior.

Another challenge is adversarial evasion. Attackers can sometimes mimic legitimate user behavior so skillfully that their actions go undetected [6].

Additionally, data bias in anomaly detection is a crucial factor. If the training data predominantly reflects the behavior of typical office workers while neglecting remote or shift workers, legitimate actions from these groups may be wrongly flagged as suspicious. As organizations increasingly embrace remote and hybrid work models, these biases can lead to alert fatigue, eroding trust in UEBA systems [7].

2.3 Integration and Operational Challenges

UEBA seldom operates as a standalone product, it must integrate seamlessly with SIEM (Security Information and Event Management) tools, UEBA UI and other components of a Security Operations Center (SOC). Log ingestion from various sources introduces complexity in data quality, format normalization, and privacy compliance [8]. When organizations implement UEBA at scale, computational overhead for real-time analysis can be significant, occasionally slowing detection or forcing trade-offs between accuracy and efficiency.

3.Key Pitfalls, Symptoms, Impacts, Mitigation Strategies in UEBA

3.1 Model Drift and Concept Drift

Model drift (also referred to as concept drift) occurs when the statistical characteristics of user behavior change over time, causing UEBA (User and Entity Behavior Analytics) models to become less accurate. This happens because the "normal" behavioral baseline shifts, leading to a growing mismatch between what the model was trained on and how users actually behave in real-world conditions.

For example, after a sudden shift to remote work, an organization might see an increase in logins from new locations. If the UEBA model was trained on a predominantly on-premises workforce, it may mistakenly flag these logins as anomalies, resulting in false positives. On the other hand, an attacker who understands how the model operates may gradually adapt their behavior to avoid detection, leading to false negatives.

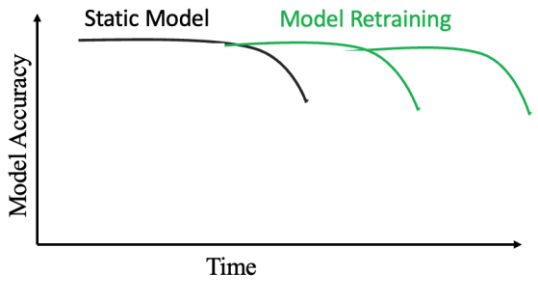

Figure 1: Machine Learning Model Drift Source: Owner's Own Processing

Symptoms

- **Increased False Positives:** The system incorrectly flags normal user activities as suspicious due to outdated baselines.
- **Unexpected False Negatives:** Emerging attack patterns bypass detection because the model has not been retrained on new threats.
- **Post-Change Detection Issues:** Major organizational shifts (e. g., mass adoption of hybrid work, mergers, or policy updates) result in erratic anomaly detection performance.
- **Reduced SOC Confidence:** Security analysts notice UEBA inconsistencies, leading to lower trust in alerts and increased manual review efforts.

Impact

- **Degraded Detection Accuracy:** Outdated models either miss real threats (true positive) or have too many false positives.
- **Operational Inefficiency:** Analysts spend more time investigating irrelevant alerts, delaying real threat responses.
- **Increased Attacker Success Rates:** Advanced threat actors can exploit drift patterns, making attacks stealthier and more persistent.
- **Higher Maintenance Costs:** Frequent manual rule adjustments and model updates increase the operational burden on security teams.

Mitigation Strategies

1. **Automated Model Retraining & Self-Learning Systems**
   - Implement continuous model updates using automated retraining pipelines based on the latest behavioral data.
   - Use adaptive AI techniques that can dynamically adjust baselines without requiring complete model retraining.
2. **Real-Time Baseline Adjustments**
   - Instead of static thresholds, leverage time-sensitive behavioral analytics that gradually adjust anomaly thresholds based on changing patterns.
   - Incorporate seasonality and trend analysis to differentiate between genuine user behavior changes and potential threats.
3. **SOC-Driven Feedback Loops**
   - Allow security analysts (SOC analyst) to label false positives/negatives, feeding this feedback into the UEBA system for continuous fine-tuning.
   - Implement human-in-the-loop decision-making, where analysts verify high-risk anomalies before triggering automated responses.
4. **Hybrid Detection Models**
   - Use a combination of rule-based detection (for stable patterns) and machine learning-based detection (for dynamic changes) to reduce drift-related errors.
   - Incorporate ensemble models that compare multiple anomaly detection approaches to enhance accuracy.
5. **Periodic Model Audits & Testing**
   - Conduct regular performance evaluations to detect signs of drift before it impacts detection accuracy.
   - Simulate real-world cyberattacks and evolving user behaviors (e. g., red team testing) to ensure the model remains effective in dynamic environments.

By proactively detecting and correcting model drift, organizations can enhance UEBA accuracy, reduce false positives, and ensure long-term reliability in identifying insider threats and advanced cyberattacks [9].

3.2 Data Bias and Limited Coverage

UEBA (User and Entity Behavior Analytics) relies on historical data to establish baselines of normal behavior. However, if the training data lacks diversity or fails to

represent certain user groups, it can introduce biases into the system. These biases may cause legitimate activities to be flagged as anomalies while actual threats go unnoticed.

For example, if a UEBA system is primarily trained on standard office employees working from headquarters, it may struggle to correctly interpret behavior from remote workers, third-party contractors, or shift-based employees. As organizations expand globally and adopt hybrid work models, biased data can lead to misclassification of users and increased false positives [10].

Symptoms

- **Disproportionate False Positives**: Routine activities from remote employees, consultants, or non-traditional roles (e. g., IT administrators, executives) frequently get flagged as suspicious.
- **Overlooked Insider Threats**: The system may struggle to identify anomalies from privileged users, as their access patterns are often atypical and underrepresented in the training data. [11].
- **Unfair Security Scrutiny**: Certain employee groups may be flagged more frequently, leading to unnecessary investigations and eroding trust in UEBA.
- **Alert Fatigue & Inefficiency**: SOC analysts spend excessive time investigating benign alerts, reducing focus on real threats.

Impact

- **Reduced Detection Accuracy**: UEBA may generate an imbalance between false positives (flagging normal users) and false negatives (missing real threats).
- **Operational Bottlenecks**: Increased investigations strain SOC resources, slowing down threat response.
- **Compliance & Ethical Concerns**: Biased UEBA decisions may create legal and ethical risks, particularly in sectors with strict regulatory oversight (e. g., finance, healthcare).
- **Loss of Confidence in Security Analytics**: If UEBA repeatedly misclassifies users, organizations may disable alerts or ignore findings, reducing its overall effectiveness.

Mitigation Strategies

1. **Diverse and Representative Training Data**
   - Ensure UEBA models are trained on a wide range of user behaviors, including:
     - Remote/hybrid employees
     - Contractors and third-party vendors
     - Privileged users (admins, C-suite executives)
     - Shift-based workers (e. g., healthcare, manufacturing, SOC analysts)
   - Regularly audit datasets to identify and correct underrepresented groups.
2. **Context-Aware Anomaly Detection**
   - Implement role-based behavioral baselines, where UEBA understands different work patterns based on job function, location, and access levels.
   - Incorporate geo-behavioral analytics, ensuring that users in different time zones or regions are not incorrectly flagged.
3. **Hybrid Detection Models**
   - Use a combination of rule-based detection and AI-driven UEBA to reduce bias in anomaly detection.
   - Implement adaptive learning mechanisms that allow security teams to adjust anomaly thresholds dynamically.
4. **Analyst Feedback & Continuous Model Tuning**
   - Enable SOC analysts to flag false positives and retrain models with this feedback to improve accuracy.
   - Incorporate human-in-the-loop validation, where security teams provide their feedback before enforcing automated decisions.
5. **Bias Auditing & Compliance Monitoring**
   - Regularly conduct bias audits on UEBA models to ensure fairness and accuracy across different user demographics.
   - Align UEBA analytics with regulatory frameworks (e. g., GDPR, HIPAA, NIST AI Risk Management Framework) to minimize privacy and discrimination risks.

By ensuring representative training data, adaptive detection mechanisms, and human oversight, organizations can reduce bias in UEBA, improving both detection accuracy and trust in security analytics.

3.3 Alert Overload and False Positives

Alert overload occurs when UEBA (User and Entity Behavior Analytics) generates an excessive volume of security alerts, many of which turn out to be false positives. Since UEBA models detect deviations from "normal" behavior, they can sometimes misinterpret legitimate actions as suspicious, particularly in dynamic work environments where roles and responsibilities frequently change [12].

False positives overwhelm Security Operations Center (SOC) analysts, making it difficult to identify real threats between the noise. If too many benign alerts flood the system, critical security incidents may be missed or delayed, reducing overall incident response efficiency [13].

Symptoms

- **SOC Fatigue**: Security teams become overwhelmed by hundreds or thousands of alerts per day, leading to delayed investigations.
- **Frequent False Alarms**: Routine activities such as an employee accessing a new system, logging in from a different location, or working late, get flagged as anomalies [12].
- **Decreased Trust in UEBA**: If analysts repeatedly encounter false positives, they may start ignoring or dismissing alerts, creating blind spots for real threats.
- **Escalation Bottlenecks**: High alert volume slows down triage, escalation, and response, allowing real security incidents to go undetected for longer periods [13].

Impact

- **Missed Critical Threats**: Excessive noise reduces visibility into real insider threats and cyberattacks.

- **Analyst Burnout & Resource Drain**: Overloaded security teams struggle to prioritize alerts, increasing workload stress and turnover rates.
- **Reduced SOC Efficiency**: Excessive false positives lead to longer response times, delaying the containment of actual breaches.
- **Higher Operational Costs**: Organizations may need to expand SOC teams or invest in automation to handle the surge in alerts.

Mitigation Strategies

1. **Refined Risk Scoring & Contextual Analysis**
   - Implement risk-based alert scoring, where alerts are prioritized based on severity, confidence level, and contextual factors [12].
   - Use behavioral baselining with dynamic thresholds, reducing false positives caused by natural variations in user activity.
2. **Integration with Other Security Tools**
   - Correlate UEBA alerts with SIEM, EDR (Endpoint Detection and Response), and threat intelligence feeds to verify risks before escalating incidents.
   - Leverage cross-tool analytics to validate anomalies against multiple security data sources (e. g., network traffic, IAM logs, and geolocation data).
3. **Adaptive Machine Learning & Continuous Tuning**
   - Train models using high-quality, diverse datasets that reflect different work environments (e. g., remote, hybrid, and shift-based employees).
   - Enable semi-supervised learning, where security teams provide feedback on false positives to improve model accuracy over time.
   - Use adversarial testing to simulate real-world attack patterns and minimize unnecessary detections.
4. **Human-in-the-Loop & Threat Intelligence Augmentation**
   - Implement SOC analyst feedback loops, allowing security teams to adjust detection parameters dynamically.
   - Incorporate external threat intelligence feeds to validate whether flagged anomalies align with known attack behaviors [13].
5. **Automated Response & Alert Suppression**
   - Deploy automated response workflows that handle low-risk alerts without human intervention.
   - Implement alert suppression rules to reduce noise, ensuring that repetitive benign activities (e. g., periodic remote logins) do not continuously trigger alarms.

By refining UEBA detection mechanisms, leveraging automation, and integrating human expertise, organizations can reduce false positives, improve threat detection accuracy, and enhance SOC efficiency—ensuring that real cyber threats do not get lost in the noise.

3.4 Adversarial Exploitation

Adversarial exploitation occurs when threat actors manipulate or evade UEBA (User and Entity Behavior Analytics) systems by carefully adjusting their behavior to remain undetected. Since UEBA relies on pattern recognition and anomaly detection, attackers can study normal activity baselines and modify their actions to blend in [14]. This tactic, known as adversarial mimicry, allows cybercriminals to avoid triggering alerts while executing insider threats, lateral movement, or data exfiltration.

Advanced persistent threats (APTs) and sophisticated adversaries increasingly employ adversarial machine learning techniques to bypass behavioral defenses, making UEBA susceptible to evasion and poisoning attacks if not properly safeguarded [14].

Symptoms

- **Subtle Credential Misuse**: Attackers escalate privileges gradually, avoiding large deviations that might be flagged as anomalies.
- **Mimicked Work Patterns**: Threat actors operate during normal working hours and replicate login behaviors to evade detection [15].
- **Data Exfiltration via Normal Channels**: Instead of using obvious bulk transfers, attackers slowly (in chunks or at different time intervals) exfiltrate sensitive data using standard business applications (e. g., email, cloud storage, or messaging tools).
- **Machine Learning (ML) Evasion**: Attackers manipulate system inputs, such as introducing synthetic "normal" behaviors into training data, to degrade UEBA effectiveness [14].

Impact

- **Stealthy Threat Persistence**: Advanced attackers can maintain unauthorized access for extended periods without triggering security alerts.
- **Undermined Detection Capabilities**: UEBA models may fail to distinguish between genuine users and adversarial behaviors, reducing the system's ability to detect threats.
- **Data Breaches & Insider Threats**: Sophisticated adversaries can exfiltrate critical business information without detection, leading to financial and reputational damage [15].
- **Increased False Negatives**: As attackers refine their evasion tactics, UEBA systems may fail to flag legitimate threats, giving organizations a false sense of security.

Mitigation Strategies

1. **Adversarial Machine Learning Defense**
   - Implement robust adversarial training by continuously testing UEBA models against simulated evasion techniques to enhance resilience [14].
   - Deploy ensembling and anomaly-resistant algorithms to reduce susceptibility to adversarial manipulation.
2. **Deception Technologies**
   - Introduce honey accounts, decoy files, and deceptive network paths to lure attackers into revealing themselves [15].
   - Use behavioral traps, such as fake privileged access credentials, to detect unauthorized activity in real time.
3. **Layered Security & Contextual Analysis**
   - Combine UEBA with Zero Trust Architecture (ZTA), endpoint detection and response (EDR), and deception-based detection to create multiple detection barriers.

- Use contextual risk scoring to correlate UEBA alerts with other security signals (e. g., impossible travel activity, geolocation anomalies, and abnormal access requests).

4. **Continuous Model Adaptation & Threat Intelligence**
   - Ensure ongoing model retraining using fresh data to counter adversarial drift.
   - Leverage threat intelligence feeds to update detection mechanisms with emerging attack patterns and known evasion techniques [14].
5. **Human-in-the-Loop Approach**
   - Engage SOC analysts and threat hunters to provide manual oversight for high-risk activities that UEBA might miss.
   - Enable adaptive alert triage, where security teams can validate, refine, and adjust UEBA detection thresholds dynamically.

By integrating these proactive defense strategies, organizations can fortify UEBA against adversarial exploitation, ensuring that behavioral analytics remains a robust and reliable security layer.

3.5 Privacy and Regulatory Challenges

User and Entity Behavior Analytics (UEBA) relies on extensive behavioral data collection to detect anomalies, which raises privacy and regulatory concerns under laws such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA) [16]. These regulations impose strict guidelines on data collection, processing, and storage, specifically regarding personally identifiable information (PII) and sensitive user behavior data.

As UEBA systems expand their reach, organizations must navigate challenges related to data minimization, user consent, cross-border data transfers, and retention policies to ensure compliance while maintaining cybersecurity effectiveness.

Symptoms

- **Excessive Data Collection**: UEBA systems may collect more behavioral data than necessary, conflicting with GDPR's data minimization principle, which mandates that organizations only gather data essential for specific security purposes [16].
- **Lack of Transparency**: Employees and users may not fully understand how their behavioral data is being collected, stored, and used, leading to compliance risks.
- **Cross-Border Data Transfer Restrictions**: Laws such as GDPR and China's Personal Information Protection Law (PIPL) impose restrictions on transferring user behavior data outside specific geographic regions. This poses challenges for multinational organizations using cloud-based UEBA solutions.
- **Data Retention Conflicts**: Privacy regulations often require that user data be deleted once it is no longer necessary. However, UEBA systems may rely on long-term historical data to establish behavioral baselines and detect anomalies over time [16].

Impact

- **Legal and Financial Liabilities**: Non-compliance with data privacy laws can lead to severe financial penalties. GDPR violations, for example, can result in fines of up to €20 million or 4% of an organization's global annual revenue, whichever is higher [17].
- **Reputational Damage**: Mishandling user behavior data or a privacy breach in a UEBA system could lead to a loss of customer trust, negative publicity, and regulatory scrutiny.
- **Operational Constraints**: Privacy laws may limit the ability to collect and analyze necessary security data, potentially reducing the effectiveness of UEBA in detecting insider threats and anomalies.

Mitigation Strategies

1. **Data Minimization & Anonymization**
   - Collect only the minimum necessary data for security analysis, ensuring that excess behavioral details are not stored.
   - Apply anonymization and pseudonymization techniques to de-identify user behavior while maintaining detection capabilities [16].
2. **Regulatory Compliance Frameworks**
   - Align UEBA implementations with industry standards like the NIST Privacy Framework, ISO/IEC 27701, and CIS Critical Security Controls to build compliance into security analytics from the outset.
   - Conduct Data Protection Impact Assessments (DPIAs) before deploying UEBA to evaluate potential privacy risks and regulatory challenges [16].
3. **Consent Management & Transparency**
   - Provide clear privacy policies explaining what data is collected, how it is used, and how long it is retained.
   - Implement opt-in/opt-out mechanisms for users where required by law, ensuring compliance with regulations like CCPA.
4. **Data Retention & Secure Storage**
   - Define and enforce strict data retention policies, ensuring that stored behavioral logs do not exceed the legally permitted timeframe [17].
   - Utilize privacy-enhancing technologies (PETs) such as homomorphic encryption and differential privacy to secure stored data while preserving analytical value.
5. **Cross-Border Data Governance**
   - Implement geo-fencing and regional data storage to ensure compliance with data localization laws [16].
   - Where international data transfers are necessary, organizations should use legally approved mechanisms such as Standard Contractual Clauses (SCCs) under GDPR.

By embedding these privacy safeguards into UEBA solutions, organizations can balance security effectiveness and regulatory compliance, ensuring that behavioral analytics does not come at the cost of legal risk or user trust.

4.Conclusion

While User and Entity Behavior Analytics (UEBA) has emerged as a powerful tool for detecting insider threats, credential abuse, and advanced cyberattacks, its effectiveness

depends on how well organizations navigate its hidden challenges. Unchecked model drift, data bias, alert overload, adversarial exploitation, and privacy concerns can significantly undermine UEBA's reliability, leading to operational inefficiencies.

To maximize UEBA's potential, security teams must implement countermeasures mentioned below:

- **Continuous Model Management** – Regular retraining and adaptation to shifting behavioral patterns.
- **Holistic Data Collection** – Ensuring diverse user roles, access patterns, and work environments are accounted for to minimize bias.
- **Intelligent Alert Filtering** – Prioritizing anomalies based on risk context to reduce false positives and analyst fatigue.
- **Multi-Layered Defenses** – Combining UEBA insights with SIEM**,** deception techniques, and threat intelligence for stronger detection capabilities.
- **Privacy-Conscious Implementation** – Enforcing data protection, access controls, and compliance with GDPR, CCPA, and industry-specific regulations.

As cyber threats evolve, future research should focus on enhancing UEBA models to incorporate context-aware machine learning, adaptive risk scoring, and industry-wide frameworks for responsible UEBA deployment. By striking a balance between security and user privacy, organizations can ensure UEBA remains a resilient and trusted cornerstone of modern threat detection.

References

[1] Gartner, "Market Guide for User and Entity Behavior Analytics", Gartner, 2015. [Online]. Available: https://www.gartner.com.
[2] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing", U. S. Department of Commerce, 2020. [Online]. Available: https://csrc.nist.gov/publications.
[3] S. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection", *IEEE Trans. Inf. Forensics Security*, vol.5, no.3, pp.1–14, 2010.
[4] A. Brown, J. Smith, and X. Zhang, "Integrating machine learning for anomaly detection in cybersecurity", *J. Cybersecurity Res. *, vol.12, no.2, pp.145–160, 2018.
[5] Z. Zhang and Z. Chen, "Model drift in anomaly detection systems", *J. Cybersecurity*, vol.15, no.3, pp.112–124, 2019.
[6] Y. Huang, W. Lee, and X. Zhang, "Adversarial evasion in behavioral analytics systems", in *Proc.2011 IEEE Symp. Security Privacy*, 2011.
[7] A. Brown, L. Davis, and M. Green, "Impact of data bias on UEBA in remote and hybrid work environments", *Cybersecurity J. *, vol.10, no.2, pp.89–102, 2018.
[8] ISO, "Information security management systems—requirements", *ISO/IEC 27001: 2021*, Int. Org. for Standardization, 2021.
[9] Y. Zhang and X. Chen, "Adaptive UEBA: Handling Concept Drift in Anomaly Detection Systems", *IEEE Security Privacy*, 2019.
[10] T. Brown et al., "Mitigating Bias in AI-Based Anomaly Detection Systems", *IEEE Trans. Inf. Security*, 2018.
[11] Y. Zhang and X. Chen, "Context-Aware UEBA: Reducing Bias in Behavioral Analytics", *IEEE Security Privacy*, 2019.
[12] Y. Zhang and X. Chen, "Reducing False Positives in UEBA Systems with Risk-Based Prioritization", *IEEE Security Privacy*, 2019.
[13] T. Brown et al., "Optimizing SOC Operations: The Impact of Alert Overload on Threat Detection", *IEEE Trans. Inf. Security*, 2018.
[14] Y. Huang, A. D. Joseph, and B. Nelson, "Adversarial Machine Learning Attacks Against Behavioral Detection Systems", *IEEE Security Privacy*, 2011.
[15] T. Brown et al., "Deception-Based Cybersecurity Strategies for Insider Threat Detection", *IEEE Trans. Inf. Forensics*, 2018.
[16] European Union, "General Data Protection Regulation (GDPR)", 2018.
[17] European Data Protection Board, "Guidelines on administrative fines under GDPR", 2022