OBSERVEID

Enhancing Security with User Behavior Analysis (UBA) and Automation

WHITEPAPER PREPARED BY:

Sperry Bilyea

Table of Contents

UBA + IAM Automation Industry Facts

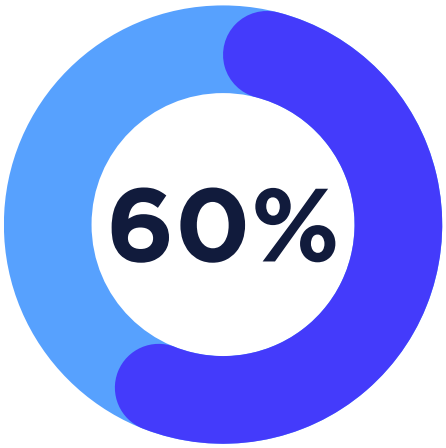
UBA/UBEA DEFINITION

First defined by the analyst firm Gartner in 2015, user and entity behavior analytics (UEBA) is a class of security tools that evolved from UBA. "'U' is a must," but "going beyond 'U' to other 'E' is not.

VALID CREDENTIALS USED TO ACCESS ORGANIZATION

Sixty percent of interactive intrusions observed by OverWatch involved the use of valid credentials, which continue to be abused by adversaries to facilitate initial access and lateral movement.

- Garter



$24B

IAM Market Growth is expected to increase from $16.1 Billion in 2023 to $24.9 Billion in 2027

- Garter

Enhancing Security with User Behavior Analysis and Automation

Introduction

In today's digital age, where cyber threats are evolving at an unprecedented pace, traditional security measures are no longer sufficient. Organizations must adopt advanced techniques to safeguard their assets, data, and operations. One such approach is the integration of User Behavior Analysis (UBA) and automation into Identity and Access Management (IAM) systems. This white paper explores the significance of UBA and automation, their benefits, and best practices for implementation.

Understanding User Behavior Analysis (UBA)

What is User Behavior Analysis?

User Behavior Analysis involves monitoring and analyzing the actions of users within a system to detect abnormal or suspicious behavior. By establishing a baseline of normal behavior, UBA can identify deviations that may indicate potential security threats, such as insider threats, compromised accounts, or fraudulent activities.

UEBA add entities (such as devices, applications, servers, etc.) in a network to the above definition

Key Components of UBA

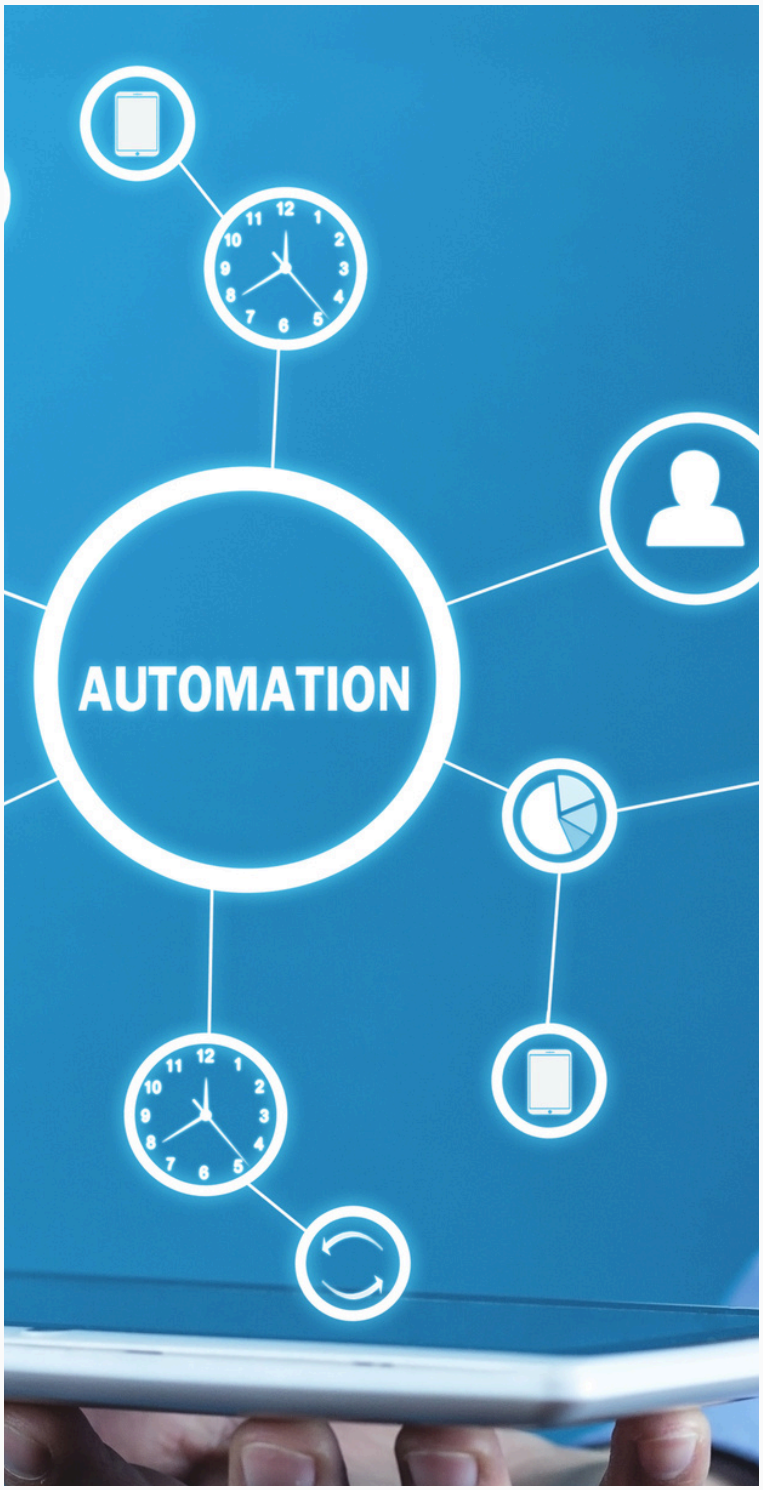
Data Collection: Gathering data from various sources, including login records, access logs, application usage, and network traffic.

Behavior Profiling: Creating profiles for individual users based on their typical behavior patterns.

Anomaly Detection: Using statistical models and machine learning algorithms to detect deviations from established behavior patterns.

Alerting and Reporting: Generating alerts for security teams to investigate and providing detailed reports for audit and compliance purposes.

What is Automation in IAM?



Automation in IAM refers to the use of automated processes and tools to manage identities and access rights efficiently. This includes provisioning and de-provisioning user accounts, managing entitlements, and ensuring compliance with security policies.

Benefits of Automation

- **Efficiency and Speed:** Automating routine IAM tasks reduces the time and effort required for manual processes, allowing IT teams to focus on strategic initiatives.
- **Consistency and Accuracy**: Automated processes ensure that IAM tasks are performed consistently and accurately, reducing the risk of human error.
- **Scalability:** Automation enables organizations to scale their IAM operations to handle a growing number of users and applications without increasing administrative overhead.
- **Enhanced Security:** Automated IAM processes help enforce security policies and ensure timely de-provisioning of access rights, reducing the risk of unauthorized access.

Integrating UBA and Automation in IAM

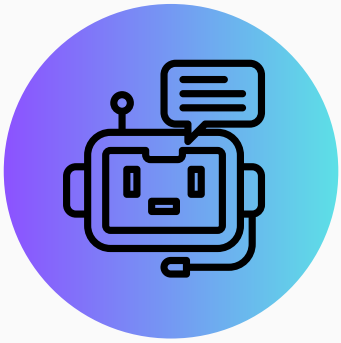
How UBA and Automation Complement Each Other

The integration of UBA and automation in IAM creates a robust security framework that enhances an organization's ability to detect, respond to, and prevent security threats.

Here's how they work together:

Proactive Threat Detection

UBA continuously monitors user behavior to detect anomalies in real time. When suspicious activity is identified, automated workflows can trigger immediate actions, such as locking accounts or requiring multi-factor authentication (MFA) for verification.



Real-time Automated Response

Automation can be used to execute predefined actions in response to detected anomalies, such as revoking access, initiating incident response procedures, or notifying security teams.

Continuous Improvement

Data collected from UBA can be fed into machine learning models to continuously improve the accuracy of behavior profiling and anomaly detection. Automated processes can be updated based on the latest insights to enhance security measures.

Enhanced Behavioral Visibility

UEBA offers a thorough understanding of user and entity behavior across the network, detailing who accesses which resources, when, where, how, and why.

Cost Reduction

By automating threat detection and analysis, UEBA reduces security operational costs, alleviates security analyst workload and alert fatigue, and minimizes the impact of breaches.

Risk Mitigation

Implementing UEBA enhances an organization's security posture and resilience, thereby lowering the risk of data breaches, compliance violations, reputational harm, and financial losses.

Best Practices for Implementation

IAM jumped from 8th place to 2nd in this year's investment priorities ranking, reflecting increasing market concerns about identity security in multicloud tech stacks. (venturebeat, 2023)

1. **Define Clear Objectives**: Establish clear objectives for integrating UBA and automation into your IAM strategy. Identify specific security challenges you aim to address and set measurable goals.
2. **Choose the Right Tools**: Select converged IAM solutions that offer robust UBA and automation capabilities. Ensure that these tools can seamlessly integrate with your entire existing IT infrastructure.
3. **Data Privacy and Compliance**: Ensure that data collection and analysis processes comply with relevant data privacy regulations. Implement measures to protect sensitive user data.
4. **Continuous Monitoring and Tuning**: Regularly monitor the performance of UBA and automation processes. Continuously tune algorithms and workflows to adapt to evolving threats and changing user behavior.
5. **User Education and Awareness**: Educate users about the importance of security and the role of UBA and automation in protecting organizational assets. Promote a culture of security awareness.

Case Study:ObserveID's Implementation of UBA and Automation

Background

ObserveID, a leading IAM solution provider, implemented UBA and automation to enhance its security framework and improve operational efficiency for its clients.

Implementation Process

1. Data Integration: ObserveID integrated data from various sources, including login records, application logs, and network traffic, into its UBA module.

2. Behavior Profiling: Machine learning algorithms were used to create behavior profiles for individual users, establishing baselines for normal behavior.

3. Anomaly Detection: Advanced statistical models were employed to detect deviations from normal behavior patterns in real-time.

4. Automated Response: Automated workflows were configured to respond to detected anomalies, including account lockouts, MFA prompts, and alert generation.

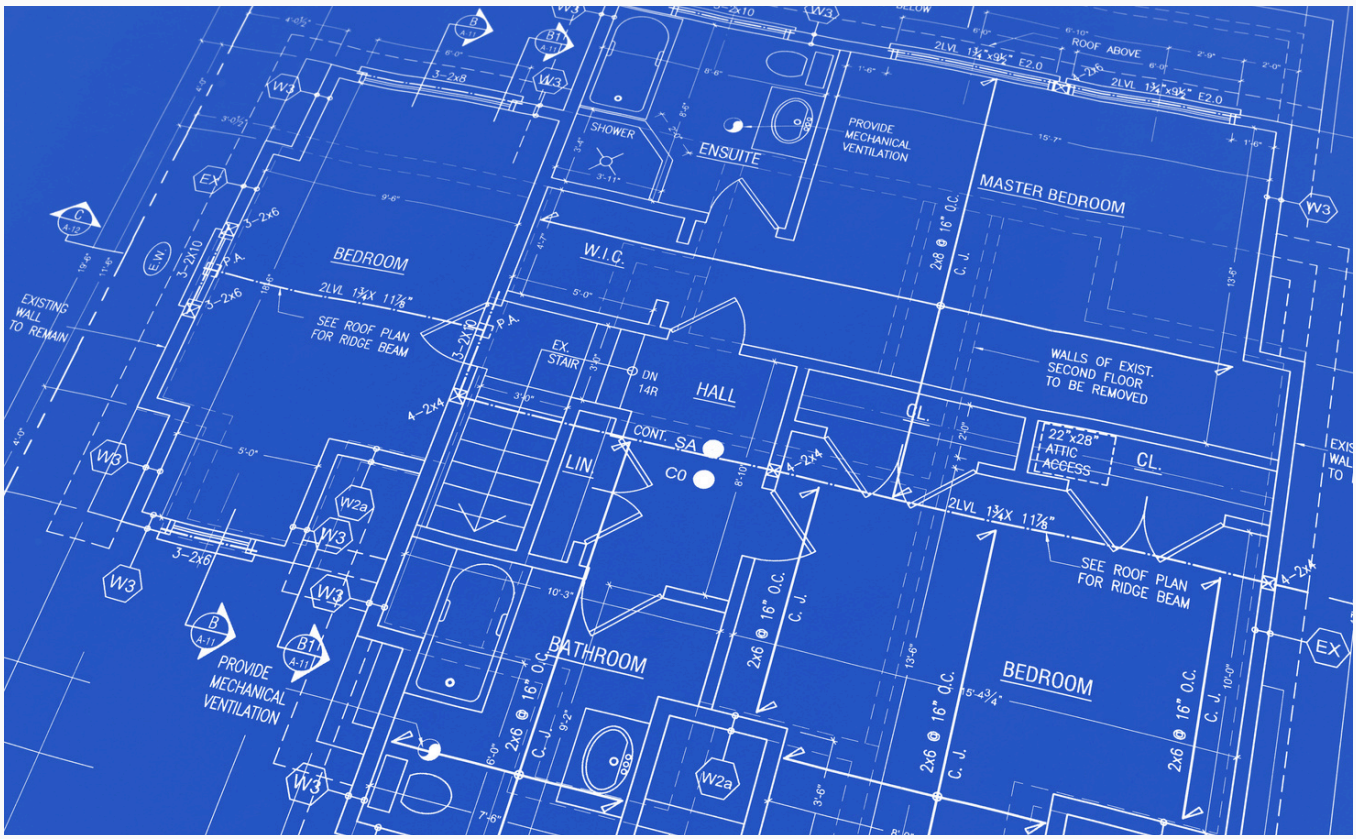
Results

Improved Threat Detection: ObserveID's clients reported a significant increase in the detection of insider threats and compromised accounts.

Operational Efficiency: The automation of IAM tasks reduced the time and effort required for manual processes, allowing IT teams to focus on strategic initiatives.

Enhanced Security Posture: The integration of UBA and automation improved the overall security posture of ObserveID's clients, reducing the risk of unauthorized access and data breaches.

Conclusion



User Behavior Analysis and automation are essential components of a modern IAM strategy. By integrating these capabilities, organizations can enhance their security posture, improve operational efficiency, and ensure compliance with regulatory requirements. ObserveID's successful implementation of UBA and automation demonstrates the tangible benefits of this approach, providing a blueprint for other organizations to follow.

For more Info:

For more information on how ObserveID can help your organization implement UBA and automation, please contact us at **confidence@observeid.com**

References

1. Gartner. (2021). Market Guide for Identity Governance and Administration.
2. Forrester. (2020). The Forrester Wave™: Identity Management and Governance.
3. NIST. (2020). NIST Special Publication 800-63B: Digital Identity Guidelines.
4. Venture Beat (2023) . How generative AI is defining the future of identity access management.

Why we launched ObserveID

It boils down to one key word: confidence.

With over 100+ years between us in cybersecurity and identity access management, we've seen it all—from working with legacy software to tackling all sorts of behind-the-scenes implementations and projects.

But here's the thing—we saw a gap. The way multicloud and on-prem legacy IT infrastructures were being managed was anything but nimble. Companies were not keeping pace with the fast-moving needs of today's hybrid working organizations.

So, we had a lightbulb moment: what if we could bring everything together, linking the IT infrastructure efficiently unifying all the identities, entitlements and resources into one single plane?

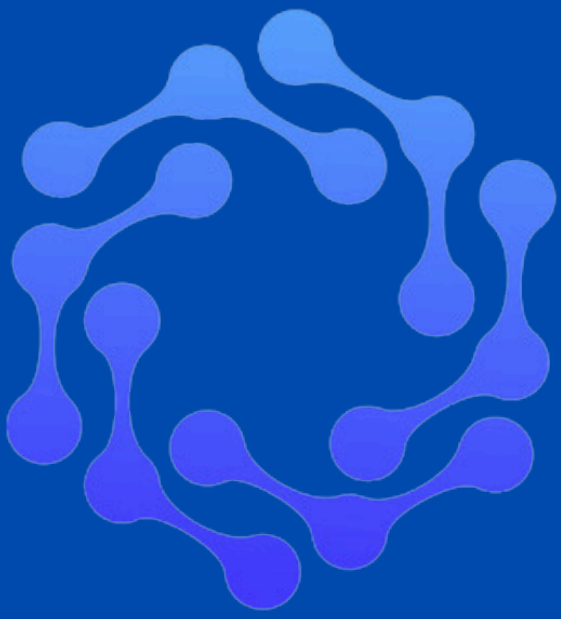
Imagine the boost in confidence for an organization when they know their data is solid, their security risk is under control, and they've got a cost-effective, agile IT infrastructure.

And the real kicker? Ensuring that the right people have the right access to the right information at just the right time.

That's the heart of ObserveID. It's all about giving you that rock-solid confidence in every aspect of your IT environment.

CONFIDENCE

Contact Us



ObserveID

(949) 534-4854
Phone

info@observeid.com
Email

www.observeid.com
Website

California, USA
Address