THE IDENTITY UNDERGROUND

Q3 2024

THE IDENTITY UNDERGROUND

Wisdom Report Q3 2024

TABLE OF CONTENTS

INTRODUCTION

Identity security is one of the biggest challenges security and IT leaders face today. It is often a shared responsibility across multiple departments with different goals, or the people who own it don't have the authority to change it.

We created The Identity Underground to transform how organizations understand, develop, and build their identity security programs. We want to change identity security from within.

By mentoring the next generation, we'll empower those who own these programs with the authority and influence to create long-lasting, winning identity security strategies.

The Identity Underground network thrives on its diverse membership.

By connecting security leaders across organizations, we create a platform for sharing insights and addressing shared challenges. This peer network allows members to validate strategies and find support.

These connections empower our community to drive meaningful change in identity security, both within their organizations and across the industry.

Q3 TOPICS AND PRESENTERS

We recently conducted a series of strategic gatherings, comprising three consecutive executive meetings that encompassed our members in the Americas, Europe, Middle East and Africa (EMEA), and Asia-Pacific (APAC) regions. Additionally, we convened a global practitioners' meeting to ensure comprehensive input from all levels.

Jessica Stone, Managing Director at The Identity Underground, led the meetings together with **Rob Larsen,** Executive Advisor at Silverfort and former executive at General Motors.

KEYNOTE SESSIONS

"Stop Saying Humans are the Weakest Link in Security"

- Shift narrative from blaming human behavior
- Bolster identity security through better technology and policies
- Empower people rather than penalize them

"Guarding the Digital Estate" (Case Study)

- Insights on managing IAM to protect digital assets
- Best practices in scaling identity security
- Challenges in large enterprise environments

“Aligning Identity Strategies with Cybersecurity”

Necessity of alignment in light of increasing automation in enterprise environments

“Identity Threat Detection and Response (ITDR)”

- In-depth technical insights on ITDR
- Focus on CAEP & discussion of shared signals

WHAT IS WISDOM?

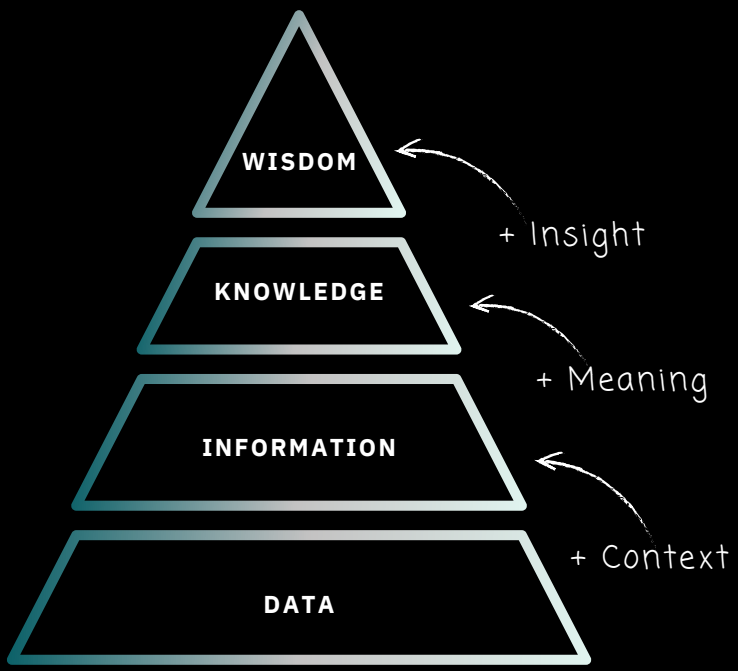
The journey from data to wisdom represents the evolution of understanding in our increasingly complex digital landscape.

At the base lies data, raw and unprocessed, holding potential but lacking meaning. As we add context, data transforms into information, enabling us to see patterns and trends. From there, by applying meaning, information becomes knowledge, empowering us to make informed decisions.

However, it is only through insight – the deep understanding drawn from experience and analysis – that knowledge matures into wisdom.

This is the core objective we strive to achieve at The Identity Underground. Our mission is to transform raw data into actionable wisdom, empowering organizations to navigate the complexities of the digital identity world.

This continuous journey from data to wisdom is at the heart of everything we do, driving innovation and leadership in the identity security space.



EXECUTIVE WISDOM SUMMARY

In today's digital world, identity has become the new security perimeter. With the explosion of digital identities, whether human or machine, each one represents a potential vulnerability. The traditional mindset of trusting users or systems by default is no longer enough. Instead, we must adopt Zero Trust principles, where every identity is continuously verified and access is tightly controlled.

Managing identity is now the cornerstone of security. By integrating dynamic identity governance and real-time monitoring, we ensure access is granted based on context and risk, not just credentials. In this era, securing identities means securing everything, as identity is at the heart of every interaction in the modern digital ecosystem.

These insights highlight the need for a unified approach: cybersecurity and identity management must work together. As the world becomes more interconnected, our security strategies must evolve accordingly, focusing on real-time intelligence, dynamic threat response and strict identity governance.

In this new era, protecting ourselves from cyber threats means taking a holistic approach that treats cyber and identity as two sides of the same coin – an approach that anticipates threats, secures identities and enables us to thrive in an increasingly digital world.

WHAT ARE EXECUTIVES TALKING ABOUT?

INSIGHTS FROM SESSION

IAM consistently ranks as the most cost-effective and outcome-correlated cybersecurity domain across industries and organization sizes, with high-ROI strategies including least privilege controls, privileged access management, and strong HR-security integration.

Cybersecurity strategy should be treated as a data analytics problem, with decision-making based on real-world outcomes and cost-effectiveness rather than just standards or trends, requiring dynamic and regular re-evaluation as threats and technologies evolve.

While certain IAM strategies like least privilege controls and PAM show high ROI, others like enterprise password management tools and large-scale centralized IAM solutions tend to have lower ROI, emphasizing the importance of targeted, data-driven investment in IAM.

WHAT ARE EXECUTIVES TALKING ABOUT?

INSIGHTS FROM SESSION

Identity attacks are increasing dramatically, with Microsoft reporting a four-fold increase in attacks on Azure AD from 2021 to 2023, emphasizing the critical need for robust identity protection.

Zero Trust principles (verify identity, assume breach, least privilege) are foundational to modern cybersecurity strategies, requiring a shift in how we approach security.

Comprehensive visibility into both human and machine identity activity across all contexts is essential, with machine identities potentially outnumbering human identities by 50 to 1 in cloud environments.

Static security measures like traditional MFA are no longer sufficient; continuous adaptive risk models incorporating various signals (device risk, user behavior, etc.) are necessary for real-time policy decisions.

Integration between IAM processes and Security Operations Center (SOC) activities, coupled with automation, is crucial for handling the volume of security data and enabling proactive threat response in modern enterprises.

WHAT ARE EXECUTIVES TALKING ABOUT?

INSIGHTS FROM LECTURE

Security is an Enabler, Not a Barrier | Rethinking Human-Centric Security
Let's talk about making security work for people, not against them.

First up, we need to make security actually help people do their jobs better. Imagine logging in and getting personalized tips on how to tackle your day more efficiently. That's the kind of authentication we should aim for – one that doesn't just check who you are, but helps you out too.

Next, let's borrow a page from behavioral economics. We can design security interfaces that subtly guide people towards safer choices. Picture a dashboard that shows how strong your security choices are, kind of like a fitness tracker for your digital habits. It's not about forcing people, but gently nudging them in the right direction.

Now, here's a cool idea: security that learns and adapts to each person. We could use AI to create security profiles that change based on how someone typically works. If you usually access certain files from your home office on weekends, the system would know that and wouldn't freak out when you do it.

Lastly, let's ditch those routine annual security trainings. Instead, why not turn security awareness into an ongoing game? We could have monthly team challenges where people practice spotting phishing emails or handling security incidents. Add in some friendly competition with leaderboards and real prizes, and suddenly, security becomes something people actually want to engage with.

By putting these ideas into action, we can make security feel less like a chore and more like a natural part of getting work done. It's about making security work with people, not against them.

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

- Prioritize high-ROI IAM initiatives leveraging advanced analytics and machine learning for risk quantification.
- Regularly evaluate and adjust strategies using AI-driven behavioral analysis and adaptive access controls.
- Challenge assumptions through graph-based identity analytics to uncover hidden vulnerabilities in complex ecosystems.

01 **Implement Data-Driven IAM Strategies**

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

- Shift security mindset from perimeter-based to identity-centric by implementing Software-Defined Perimeter (SDP) technologies.
- Implement continuous verification using dynamic risk scoring and just-in-time (JIT) access provisioning.
- Tailor Zero Trust implementation to align with NIST SP 800-207 framework and your organization's unique threat model.

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

- Develop comprehensive monitoring strategies using automated PKI and certificate lifecycle management.
- Implement Hardware Security Modules (HSMs) or cloud-based Key Management Services (KMS) for secure key storage and rotation.
- Collaborate with industry peers to develop API-first strategies for managing machine identities in containerized and serverless environments.

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

- Foster collaboration through Security Orchestration, Automation, and Response (SOAR) platforms for streamlined incident response.
- Implement User and Entity Behavior Analytics (UEBA) to detect anomalous activities in real time.
- Develop custom playbooks for automated threat hunting based on identity analytics and MITRE ATT&CK framework.

05 Embrace Human-Centric Security Design

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

- Implement adaptive Multi-Factor Authentication (MFA) that adjusts based on user context and risk levels.
- Utilize Natural Language Processing (NLP) for developing intuitive, conversational security interfaces.
- Continuously educate employees using simulated phishing exercises and AI-powered training modules.

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

06 Justify Security Investments

- Develop measurable metrics using Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) specific to identity security.
- Allocate resources based on comprehensive cybersecurity ROI models that incorporate both tangible and intangible benefits.
- Utilize advanced threat modeling techniques to prioritize investments based on specific attack vectors and TTPs.

07 Foster Continuous Learning and Adaptation

NEXT STEPS AND RECOMMENDATIONS

To drive effective identity security strategies, executives should focus on:

01 Implement Data-Driven IAM Strategies

02 Adopt Zero Trust Principles

03 Enhance Visibility of Machine Identities

04 Integrate IAM with SOC

05 Embrace Human-Centric Security Design

06 Justify Security Investments

07 Foster Continuous Learning and Adaptation

- Implement a Cyber Range for simulated attack scenarios focused on identity-based attacks.
- Encourage ongoing education through bug bounty programs and capture-the-flag (CTF) exercises tailored to IAM challenges.
- Develop an internal threat intelligence capability, focusing on emerging identity-related threats and attack methodologies.

CONCLUSION

This Executive Wisdom Briefing highlights the critical role of identity in modern cybersecurity strategies. By focusing on data-driven decisions, embracing Zero Trust, fostering a human-centric approach to security, and adapting to the interconnected nature of the cybersecurity ecosystem, organizations can build resilient defenses against evolving threats.

Remember, effective identity security is not just about technology – it's about creating a culture where security becomes an intuitive part of every digital interaction.

As leaders, your role is to drive this cultural shift, ensuring identity security is woven into the fabric of your organization's digital transformation journey.

Continuously evolve your strategy, leveraging both technological advancements and human insights. Justify investments through measurable outcomes, and foster collaboration within your organization and across the industry to build collective resilience. Security is a dynamic journey, not a static destination. Embrace the challenge, lead with vision.

WHAT ARE PRACTITIONERS TALKING ABOUT?

This report offers unique insights into cutting-edge identity management techniques recently debated within The Identity Underground Network.

Shared in-depth technical insights on Identity Threat Detection and Response (ITDR), focusing on CAEP (Continuous Access and Evaluation Profile) and shared signals.

These discussions centered around practical implementation challenges, especially when integrating these concepts into existing IAM systems.

TECHNICAL DEEP DIVE

ITDR with CAEP and Shared Signals
Sean O'Dell presented how CAEP (Continuous Access and Evaluation Profile) can be leveraged to build robust ITDR systems. CAEP allows real-time identity threat detection by analyzing contextual data and adjusting security policies dynamically.

By incorporating shared signals, multiple identity systems can communicate and adjust access controls in response to emerging threats, effectively coordinating security actions across platforms.

Technical Insight: CAEP requires tight integration with signal-sharing frameworks to ensure real-time, adaptive risk scoring. The challenge is maintaining the balance between response accuracy and system performance without overwhelming existing access controls.

Signal Plane Architecture
The signal plane, a new addition to identity architectures, enables real-time monitoring and event signaling across multi-cloud environments. It unifies identity events, offering a comprehensive view of potential threats.

Technical Insight: Implementing the signal plane requires a low-latency, fault-tolerant messaging system for real-time event processing. The challenge lies in developing robust event-streaming technologies that can integrate across distributed environments without bottlenecks.

Overcoming Integration Challenges with Legacy Systems
A common concern among practitioners was how to introduce ITDR frameworks like CAEP and the signal plane into their current, often outdated, identity management systems.
Many organizations are not prepared for a complete system overhaul, which makes the idea of phased, incremental implementation appealing.

Technical Insight: A hybrid integration approach is essential. This involves modularizing CAEP and other ITDR components so that they can be deployed gradually, minimizing disruption to existing IAM systems. The focus should be on high-risk user populations first, before scaling ITDR across the entire organization.

PRACTITIONER WISDOM

NEXT STEPS AND RECOMMENDATIONS

To effectively implement the significant advancements in identity management offered by CAEP, shared signals, and the signal plane, organizations should focus on:

- Developing Advanced Event Processing Pipelines: Build high-performance message brokers capable of processing large volumes of identity data with minimal latency. This is essential for deploying the signal plane, which provides a unified layer for managing real-time identity events.

- Implementing Context-Aware Policy Engines: Modify risk engines and access control layers to incorporate CAEP technology. This enables dynamic adjustment of identity risk based on shared signals across systems, representing a fundamental shift in traditional IAM approaches.

- Adopting a Hybrid, Incremental Approach: To address integration challenges without overwhelming existing systems, take a modular approach. Allow ITDR frameworks to coexist with legacy architectures, gradually incorporating these innovations while rethinking traditional IAM systems.

This strategy acknowledges the leap forward in identity management while addressing the serious integration challenges posed by these new technologies.

CONCLUSION

This Practitioner Wisdom offers exclusive, highly technical insights into the cutting edge of Identity Access Management.

The innovations around CAEP, shared signals, and the signal plane represent the future of ITDR but come with significant implementation challenges.

Practitioners are advised to take an incremental, strategic approach to integrating these technologies, ensuring alignment with both immediate needs and long-term goals.

THE
IDENTITY
UNDERGROUND