IAM & SECURITY BRIEFING

IAM & Security Weekly Briefing

WEEK OF May 3, 2026

1. Executive Summary (TL;DR)

- **Identity security trends:** Organizations are facing a crisis of "Identity Dark Matter," where nearly half (46%) of enterprise identity activity occurs outside the visibility of centralized IAM.
- **AI-related risks:** Non-Human Identities (NHIs), including AI agents and bots, have skyrocketed to a 144:1 ratio compared to human identities, creating unseen identity sprawl. Deepfakes and voice cloning are also rendering traditional verification methods obsolete.
- **Major breaches or incidents:** Attackers are heavily exploiting interconnected systems, with supply chain and third-party breaches quadrupling. Incidents involving compromised OAuth tokens (e.g., Drift/Salesloft) highlight indirect access risks.
- **Notable vendor/product changes:** The emergence of Identity Visibility and Intelligence Platforms (IVIP) as Layer 5 in the Identity Fabric framework is gaining traction to address opaque authentication flows and legacy app sprawl.
- **Strategic implications:** Security leaders must treat vulnerability patching and identity hardening as parallel priorities. As unauthenticated exploits account for 56% of tracked vulnerabilities, relying solely on MFA is no longer sufficient without continuous session validation.

2. Top IAM & Security News

Cyberthreats in 2026: North America Targeted, Supply Chain Risks Soar * **Summary:** For the first time in six years, North America became the most attacked region, accounting for 29% of X-Force incident response cases. Furthermore, major supply chain and third-party breaches have quadrupled over five years. * **Why it matters (identity/security impact):** North America's massive cloud footprint and deep reliance on SaaS/identity integrations mean attackers do not need zero-days—they only need valid credentials and patience to cause widespread downstream impact. * **Direct source link:** IBM Think

Shrinking the IAM Attack Surface through Identity Visibility and Intelligence * **Summary:** Enterprise IAM is hitting a breaking point, with 46% of identity activity operating unseen as "Identity Dark Matter" across shadow IT and decentralized teams. * **Why it matters (identity/security impact):** Centralized IAM solutions fall short for unmanaged applications. Organizations are turning to Identity Visibility and Intelligence Platforms (IVIP) to dynamically inspect native authentication logic and reveal opaque pathways. * **Direct source link:** The Hacker News

Exploitation Without Authentication on the Rise * **Summary:** IBM X-Force found that 56% of nearly 40,000 vulnerabilities tracked in 2025 could be exploited without any form of authentication. * **Why it matters (identity/security impact):** Adversaries often find weaknesses that do not rely on user credentials or MFA bypasses. CISOs must prioritize reducing initial access risk via patching while hardening identity controls to limit post-exploitation impact. * **Direct source link:** IBM Think

Traditional Authentication Defeated by Voice Cloning * **Summary:** Highly convincing deepfakes and AI voice cloning are being used to replicate executives to bypass human-centric verification over the phone. * **Why it matters (identity/security impact):** Standard phishing defenses are no longer enough. Security teams must adopt Attribute-Based Access Control (ABAC) and continuous verification, shifting to a true Zero Trust Architecture. * **Direct source link:** Clarity Security

AI Chatbots & Agents Become a Credential Gold Mine * **Summary:** More than 300,000 ChatGPT credentials were listed for sale on the dark web last year, as infostealers increasingly target AI agent platforms and chat tools. * **Why it matters (identity/security impact):** The use of open-source or local AI agent platforms without strict governance introduces significant insider threat potential. Compromised stored credentials within these platforms give attackers the keys to the kingdom. * **Direct source link:** IBM Think

3. AI, Identity & Emerging Tech

Non-Human Identity Explosion * **Summary:** Non-Human Identities (NHIs) such as service accounts, bots, and AI agents have grown by 44%, hitting an astounding 144:1 ratio against human identities. * **Security implications:** This massive scale creates a burden on security teams to govern shadow identities. Unified governance across cloud and on-premise environments is critical to eliminate blind spots. * **Source link:** Clarity Security

AI-Driven Cyber Attacks Increase in Speed & Scale * **Summary:** AI-powered cyber attacks increased 47% globally, allowing attackers to exploit vulnerabilities faster than human defenders can manually respond. * **Security implications:** Security teams must implement automated remediation, drift detection, and Just-In-Time access, rather than relying on manual, ticket-heavy identity governance. * **Source link:** Clarity Security

AI Agents as Identity Dark Matter * **Summary:** Autonomous AI agents are operating with independent identities and permissions that fall outside traditional governance models. * **Security implications:** Secure AI agent adoption requires Zero Trust governance, specifically Human-to-Agent Attribution, where every agent action must map back to a responsible human owner's entitlements. * **Source link:** The Hacker News

4. Cyber Threats & Attack Trends

AI-Assisted Attacks at Scale * **Attack description:** Attackers are leveraging AI-assisted phishing and infostealer malware to harvest credentials from AI chatbots and workflow agents. * **How identity was exploited:** Stealing stored credentials within agent platforms or chatbots to breach organizational infrastructure. * **Techniques used:** Credential harvesting, infostealer malware. * **Real-world example:** The sale of over 300,000 ChatGPT credentials on the dark web in 2025. * **Source link:** IBM Think

OAuth Token Abuse in Third-Party SaaS * **Attack description:** Supply chain attacks exploiting compromised third-party integrations and public-facing applications. * **How identity was exploited:** Bypassing front doors by exploiting a trusted third party's access. * **Techniques used:** Token hijacking, indirect access exploitation. * **Real-world example:** Compromised Drift OAuth tokens used to access customer Salesforce environments. * **Source link:** IBM Think

Deepfake Social Engineering * **Attack description:** Voice cloning attacks imitating executives over synchronous communications (e.g., phone calls). * **How identity was exploited:** Using high-fidelity AI voice cloning to bypass human verification and authorize data transfers. * **Techniques used:** Vishing (voice phishing), AI voice cloning. * **Real-world example:** Fake calls from simulated executives designed to trick employees. * **Source link:** Clarity Security

5. Product Updates & Vendor News

Note: Missing data. No major product updates from the requested vendors (Microsoft, Okta, AWS IAM, Google Cloud Identity, Ping Identity, RSA, CyberArk, Duo, Auth0) were found in the monitored sources this week.

6. Notable Research & Reports

X-Force Threat Intelligence Index 2026 * **Key findings:** North America accounts for 29% of cases; 56% of vulnerabilities can be exploited unauthenticated; supply chain breaches quadrupled. * **Statistics:** 44% year-over-year increase in the exploitation of public-facing applications. * **Strategic implications:** Foundational security hygiene and continuous exposure management are crucial; attackers are relying on valid account abuse over complex zero-days. * **Source:** IBM Think

Orchid Security: The Fragmented State of Enterprise Identity * **Key findings:** 46% of enterprise identity activity sits outside centralized IAM visibility; 85% of applications contain accounts from legacy/external domains; 70% of applications grant excessive privileges. * **Statistics:** 40% of all accounts are orphaned (up to 60% in legacy environments). * **Strategic implications:** Enterprises must implement an Identity Visibility and Intelligence Platform (IVIP) layer to discover the true state of their application estate and identity risk. * **Source:** The Hacker News

7. Practical Security Takeaways

1. **Enforce phishing-resistant MFA:** Go beyond basic MFA; adopt continuous session validation to guard against deepfakes and AI-powered phishing.
2. **Audit non-human identities:** Consolidate governance of human and non-human identities (bots, agents) into one unified platform.
3. **Perform deep entitlement reviews:** Execute nested reviews to identify hidden access points that are commonly attached to NHIs.
4. **Implement automated drift detection:** Set up real-time alerts to detect and remediate new identities or privilege escalation instantly.
5. **Treat patching and identity hardening as parallel tracks:** Unauthenticated vulnerabilities require rapid patching, while robust identity controls limit lateral movement post-breach.
6. **Enforce human-to-agent attribution:** Ensure every autonomous AI agent action maps back to a responsible human owner's privileges.
7. **Establish strict out-of-band verification:** Define clear policies for handling sensitive data requests to counteract highly convincing deepfake phone calls.

8. Trends to Watch

- **Explosion of Machine Identities:** The ratio of NHIs to human identities will continue to skew drastically as organizations rush to deploy autonomous AI agents.
- **Identity Dark Matter:** Security teams will increasingly discover that their centralized IAM tools lack visibility into significant portions of custom apps, legacy systems, and shadow IT.
- **From Authentication to Continuous Verification:** Legacy password and static biometric checks are giving way to real-time Attribute-Based Access Control (ABAC) and behavior models.

- **AI as an Insider Threat:** AI chatbot platforms and local agents hold massive amounts of data and API access, making them primary targets for infostealers.

9. Tool / Resource of the Week (Optional)

Identity Visibility and Intelligence Platforms (IVIP) * **What it does:** Gartner's Layer 5 of the Identity Fabric; ingests and unifies IAM data, leveraging AI to provide a single window into identity events across both managed and unmanaged systems. * **Why it's useful:** Helps solve the "Identity Dark Matter" problem by moving from inference-based access policies to evidence-driven identity intelligence at the application level. * **Link:** The Hacker News Analysis

10. Sources

- Cybersecurity Trends 2026 - IBM — https://www.ibm.com/think/insights/more-2026-cyberthreat-trends
- 5 IAM Trends to Watch in 2026 | Clarity Security — https://claritysecurity.com/clarity-blog/5-iam-trends-to-watch-in-2026/
- Shrinking the IAM Attack Surface through Identity Visibility and Intelligence Platforms (IVIP) - The Hacker News — https://thehackernews.com/2026/04/shrinking-iam-attack-surface-through.html