Cybersecurity Readiness Podcast Series

Episode Title: Identity Defense in the Age of AI

Host: Dave Chatterjee, Ph.D. — https://dchatte.com

Guest: Jasson Casey, CEO and Co-Founder of Beyond Identity

Summary Pitch

In this episode, Dr. Dave Chatterjee sits down with Jasson Casey, a seasoned innovator in enterprise security, to dissect the growing threat of identity-based attacks, which now account for nearly 80% of breaches. Casey explains how adversaries increasingly “log in” instead of breaking in, leveraging techniques such as MFA fatigue, session hijacking, and phishing kits. He shares lessons from his professional journey—ranging from building telco networks to advising the U.S. Government and launching Beyond Identity—and explains how his team's identity defense solution eliminates root causes of credential theft while reducing SOC workloads.

The discussion also addresses why traditional human training cannot withstand adversaries armed with deepfakes and agentic AI, underscoring the need for technology to carry the defensive burden. Together, Chatterjee and Casey explore the double-edged role of AI, strategies for phased deployments (“ring deployments”), and the importance of embedding identity defense into board-level governance through the Commitment–Preparedness–Discipline (CPD) framework.

Discussion Highlights

- Defining Identity-Based Attacks: Credential theft, MFA fatigue, push bombing, phishing kits, and session hijacking.

- Passwordless vs. Phishing-Resistant: The danger of convenience-driven solutions vs. secure, hardware-backed authentication.

- Case Studies: Organizations overwhelmed by credential theft reduced incidents to near zero after adopting immovable credentials.
- Human Training Limitations: Employees cannot reliably outwit AI-enhanced adversaries; systems must be resilient even when users 'do the wrong thing.'
- AI's Dual Role: Attackers exploit deepfakes and generative AI, while defenders must enable tamper-proof verification and session integrity.
- Deployment Lessons: Start with IT teams, then executives, before wider rollout; tailor solutions for kiosk and mobile use cases.
- Governance Lens: Identity defense as a strategic imperative, aligned with the CPD framework—commitment from leadership, preparedness through testing, and discipline in continuous monitoring.

Actionable Recommendations

- Move beyond weak passwordless systems; adopt phishing-resistant, hardware-backed authentication.
- Continuously monitor devices and sessions, not just initial logins.
- Validate defenses with Red Team exercises and nation-state-level adversary scenarios.
- Reduce reliance on employees to spot phishing or AI-driven impersonations.
- Apply the CPD framework to guide identity defense strategy and sustain resilience.

Time Stamps

- 0:49 — Guest background and career journey
- 4:22 — Defining identity-based attacks
- 6:42 — Passwordless convenience vs. true security

- 10:21 — Guidance for CISOs evaluating authentication solutions
- 13:13 — Customer case study: reducing push-bombing and phishing
- 17:35 — Why human training falls short in the AI era
- 24:21 — Deployment lessons and ring rollouts
- 28:02 — The role of AI in identity security and agent authorization
- 33:38 — Key takeaways and closing thoughts

Memorable Quotes

- “Over the last five years, attackers don’t break in—they log in.” — Jason Casey
- “If users can always do the wrong thing and the adversary still can’t create an incident, you know you have identity defense.” — Jason Casey
- “Technology must take the stress off people; we can’t just keep blaming them for clicking links.” — Dr. Dave Chatterjee
- “Phishing-resistant authentication isn’t about convenience—it’s about eliminating root causes of identity breaches.” — Jason Casey