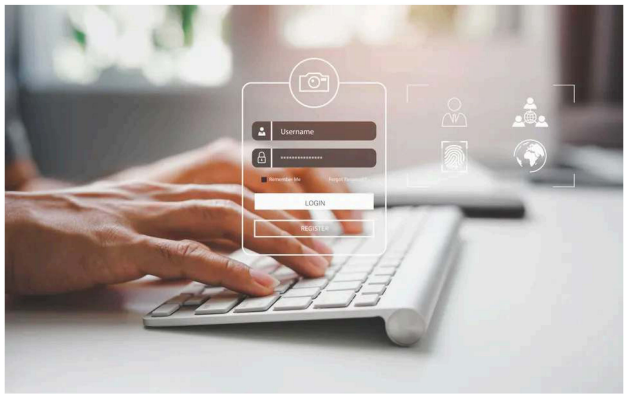
INNOVATION

Cybersecurity Awareness Isn't Enough: Championing Prevention By Design

By **Federico Simonetti,** Forbes Councils Member.

Xiid's CTO, Federico Simonetti, is a security expert with a background in ethical hacking, law enforcement and academia.



For too long, Cybersecurity Awareness Month has served as an annual pep rally for security teams, inspiring a flurry of posters, phishing simulations and optimistic PowerPoint presentations. But if a decade of headlines has proven anything, it's this: Awareness doesn't equal safety.

Deep down, CISOs and technology leaders know that, myself included. Breaches keep accelerating. Thanks to AI, adversaries adapt faster than human training can keep pace, and attackers count on human error as part of their toolkit.

So, let me be blunt: making teams "aware" is not a defense strategy. But prevention by design is. It's time to start rewiring our organizations at the architectural level, where awareness is a feature, not the backbone. Let's take a look at my blueprint for turning awareness into tangible, deterministic controls.

Deterministic Controls Are Prevention That Doesn't Blink

Most security programs are built on a foundation of probabilistic controls: "Hopefully, users spot the phish." "Maybe our monitoring will catch the intrusion in time." That's dice-rolling. In contrast, deterministic controls eliminate chance. The control either blocks the action, or it isn't allowed to happen.

Why do deterministic models sweep the board? Because they don't rely on wishful thinking. A locked door can't be "forgetfully" left open by a distracted employee, and a process segmented from all systems makes it impossible for malware to move laterally, no matter how slick the attacker.

This is the bedrock of what we call prevention by design: security certainty, not best effort.

The Easy Button: Shrink The Attack Surface Everywhere

Security need not be complicated to be impenetrable. Here's a direct model for the real world:

• **Applications:** Make them out of range—not on the open network, not directly reachable, not visible to port scans and certainly not presenting static, internet-facing endpoints. If your critical apps aren't discoverable, they're not on the menu for easy exploitation.

• **Identities:** Ditch static credentials. Eliminate shared secrets entirely. Credentials don't exist to be stolen if they never traverse the wire. Credential-less, zero-knowledge authentication isn't just a buzzword; it's what stops attackers from turning a leaked password or token into a breach.

• **Data And Pipelines:** Expect that someone in your organization will slip up one day. Building controls like pico segmentation (cutting privilege and access at the process or microservice level, not "perimeter" or "network") means even a successfully compromised session can't go on a spree.

This model doesn't require the resources of a Fortune 50. It just requires that "never trust, always verify." This means zero open doors—outbound-only connections, credential-less authentication and controls that cannot be bypassed by human mistake or optimistic policy exceptions.

Training Matters, But Assume The Worst

Awareness campaigns, tabletop exercises and user education aren't going away. They're necessary, but not sufficient. 2025's breaches, just like last year's, increasingly begin with a human, whether phished, misled or simply overwhelmed by alerts and etiquette. Attackers are hiring social engineers and using AI to bring phishing and vishing to unprecedented scale and effectiveness.

Design your security stack assuming every user will click one day, every developer will eventually leak a token and someone will misclassify a critical asset. Great architecture recognizes user fallibility and makes compromise non-catastrophic, not just "less likely."

A Four-Week Plan To Go From Posters To Policy That Sticks

Talking about prevention by design is easy; the sticking point is always action. Here's a four-week plan to convert awareness into architecture:

• **Week 1:** Audit what's routable, visible or reachable from outside. List all open ports, public IPs, exposed credentials in code and SaaS integrations.

• **Week 2:** Begin closing what doesn't need to be open. Move to outbound-only connections for CICD, RDP and admin tools. If a resource doesn't require inbound access, make it non-addressable. Deploy credential-less authentication for privileged access.

• **Week 3:** Segment at the smallest practical unit—pico segmentation. Use process-to-process tunnels instead of flat network trust, so compromise gets contained to a single asset or service.

• **Week 4:** Lock policy, log exceptions and run red team exercises. Refactor your policies so the

"check engine" light comes on the minute someone tries to re-open a port or reintroduce addressable resources.

Don't Settle For Average: Lead With Prevention By Design

If CISOs and C-suite leaders take away one message, make it this: Awareness is only the first mile. Deterministic, prevention-by-design controls are the last. Security isn't a matter of luck, prayer or hoping your users stay vigilant around the clock. It's engineering risk out of the architecture—a relentless shrinking of what is reachable, what is collectible and what is usable when, not if, something breaks.

Don't settle for a security program anyone can "see" or "probe." Move everything critical out of range, minimize mistakes to nuisance status and be the leader who turns slogans into substance.

Forbes Technology Council is an invitation-only community for world-class CIOs, CTOs and technology executives. *Do I qualify?*

By Federico Simonetti, COUNCIL POST | Membership (fee-based). Xiid's CTO, Federico Simonetti, is a security expert with a background in ethical hacking, law enforcement and academia. Read Federico Simonetti's full executive profile here.
Find Federico Simonetti on LinkedIn. Visit Federico's website.