The Metrics That Actually Matter

Skip the feel-good metrics, if you want proof you're actually shrinking attacker options, the KPIs that matter are:

- % *of reduction in exploitable exposure on crown jewels*
- *Time-to-contain for top scenarios*
- # *of "prevented" high-confidence intrusions (with evidence)*

A practical tip: define "prevented" clearly so it doesn't become marketing math. Evidence matters.

ACTION BOX

The First 90 Days: Prove it with 2-3 pilots

1 Pick 2–3 high-risk areas to pilot

Good candidates:

- Privileged identity attack paths (most breaches become "identity breaches")
- One critical business app end-to-end (auth → data → admin plane)
- OT/edge (if relevant) where visibility is harder and impact is high

Define upfront:

- The crown jewels in scope
- The top attack paths you're breaking
- The metrics you'll use to show improvement

2 Put deception/moving target where it hurts attackers most

High-impact placements:

- **Privileged identity paths:** decoy admin accounts, honey tokens, instrumented endpoints for admin activity
- **Critical apps:** decoy admin portals, canary data, alerts on suspicious API usage
- **OT/edge (if applicable):** deception for lateral movement and high-signal detection where traditional tooling is limited

3 Tie everything to exposure management

Before/after measurement is the whole game:

- Baseline exploitable exposure on the in-scope crown jewels
- Implement deny/disrupt controls + deception tripwires
- Re-measure: did exploitable paths collapse? did time-to-contain improve?

If you can show a real reduction in viable attack paths, congratulations! you've built a predictive prevention program, not a pile of tools.

DIGITAL ERA