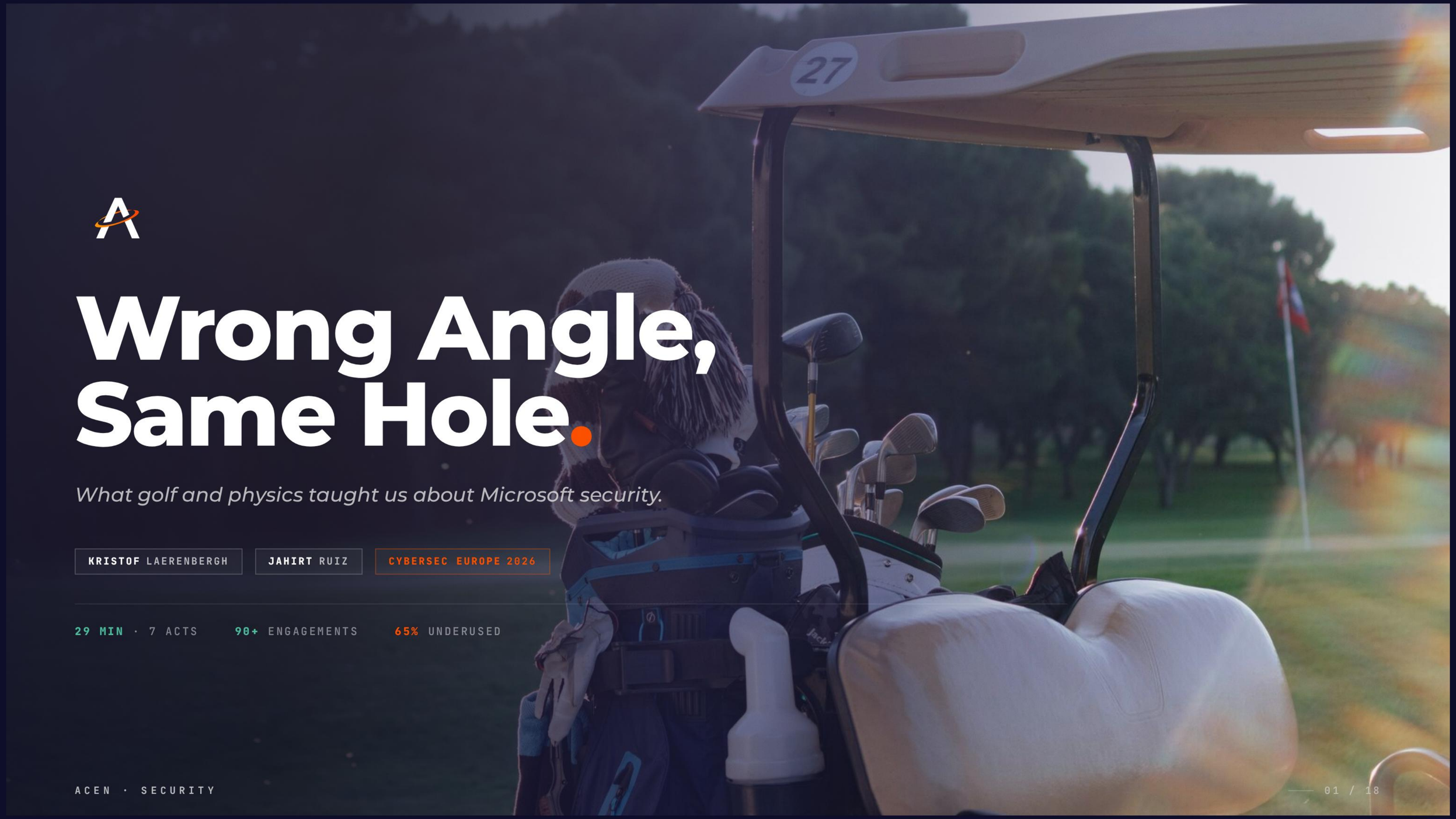


Wrong Angle, Same Hole.

What golf and physics taught us about Microsoft security.

KRISTOF LAERENBERGH

JAHIRT RUIZ

CYBERSEC EUROPE 2026

29 MIN · 7 ACTS **90+** ENGAGEMENTS **65%** UNDERUSED

Every winter I buy a new driver. Every spring I hit the same trees.

OBJECTIVE 01	OBJECTIVE 02	OBJECTIVE 03
✗ break 82	✗ no three-putts	✗ kill the slice

New EDR. Full E5 stack. A management layer.

Still compromised through the same door.

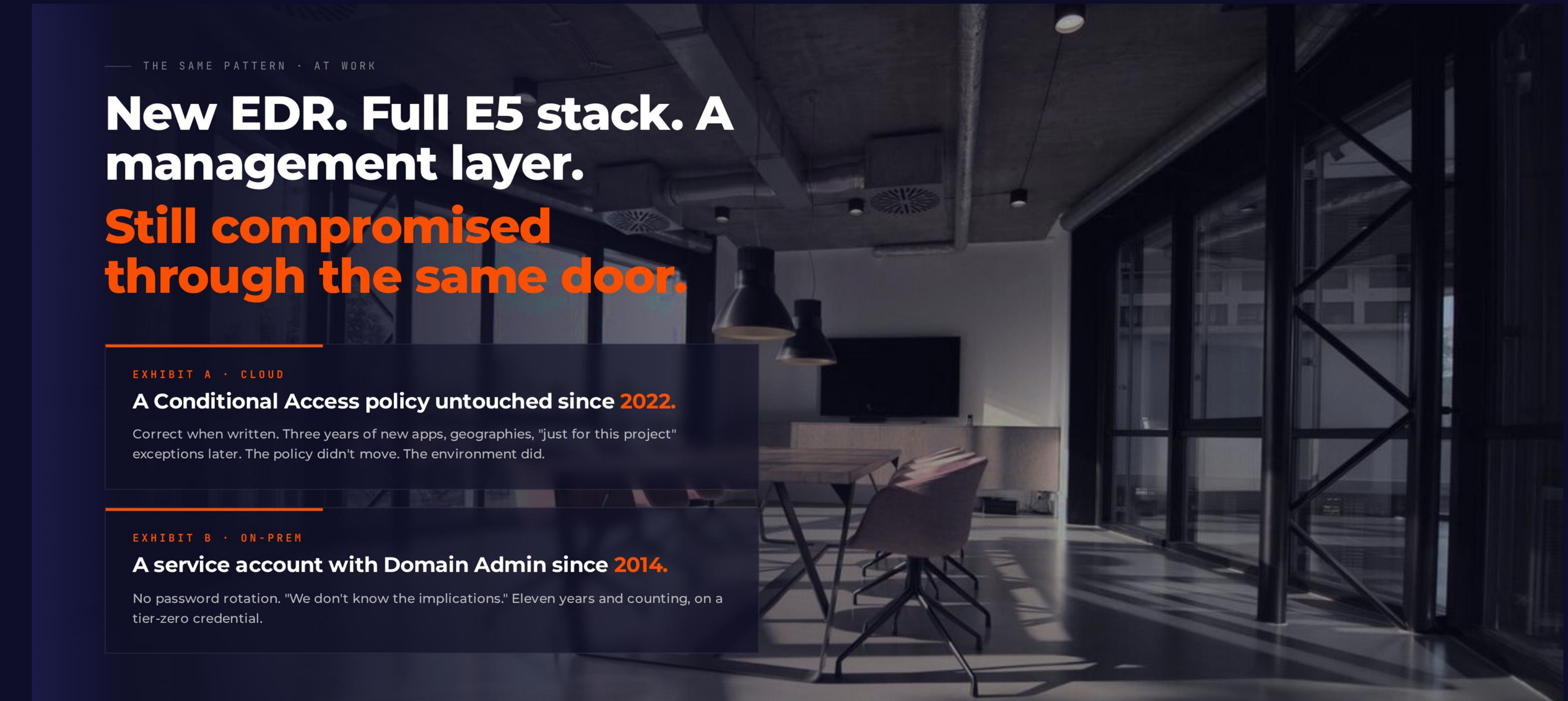


EXHIBIT A · CLOUD

A Conditional Access policy untouched since 2022.

Correct when written. Three years of new apps, geographies, "just for this project" exceptions later. The policy didn't move. The environment did.

EXHIBIT B · ON-PREM

A service account with Domain Admin since 2014.

No password rotation. "We don't know the implications." Eleven years and counting, on a tier-zero credential.

THE THESIS

New clubs.
Same slice.

THAT'S WHAT THIS TALK IS ABOUT

THE NUMBER THAT STARTED THIS TALK

65%

of the Microsoft security stack they're paying for isn't doing its job.

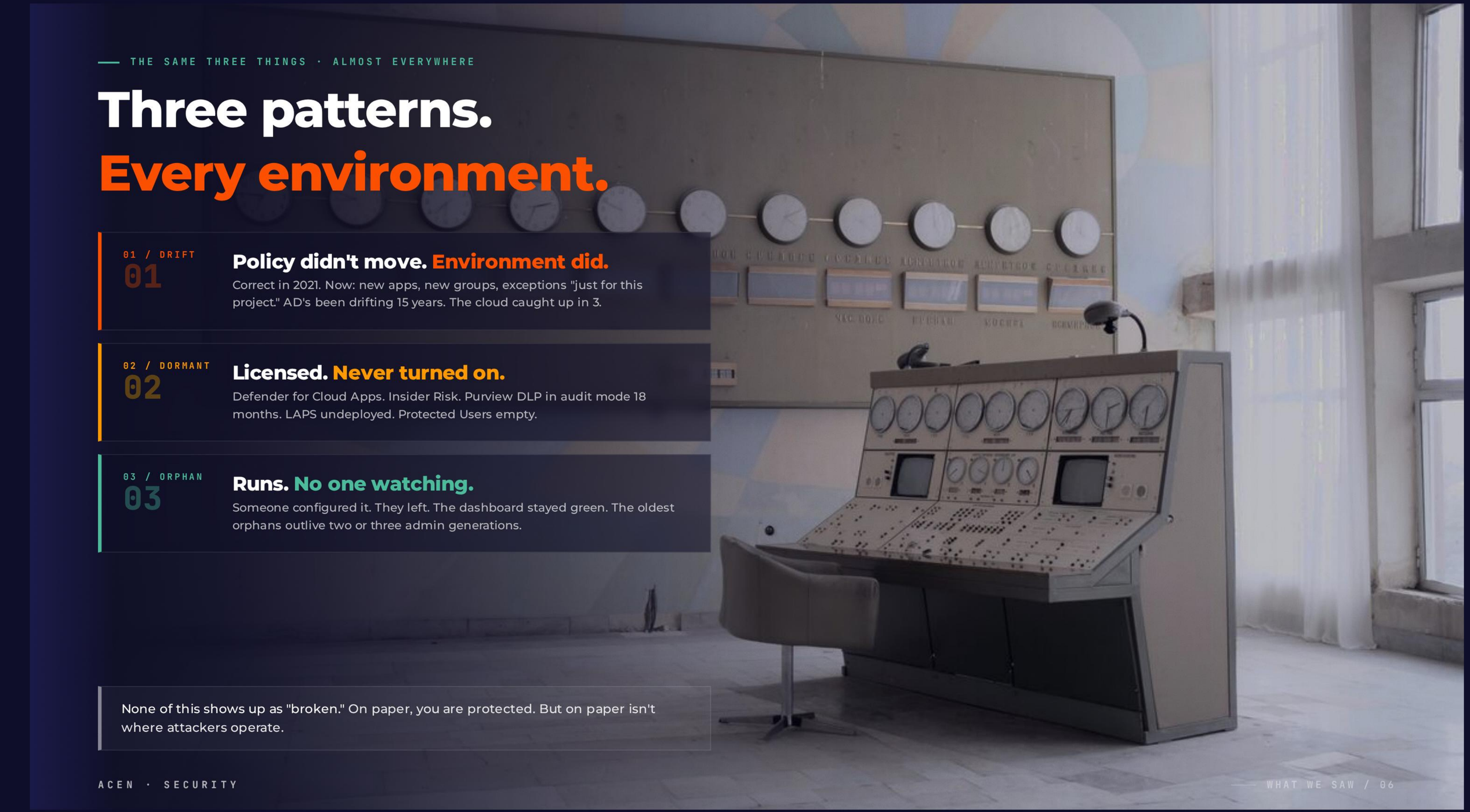
Underused. Misconfigured. Or both. Not small companies. Mature IT teams with real budgets. And in hybrid? The pattern is worse: two aging systems and a sync layer between them that almost nobody fully understands.

90+
ENGAGEMENTS

3
PATTERNS, EVERYWHERE

2
SIDES OF EVERY ESTATE

Three patterns.
Every environment.



01 / DRIFT
01

Policy didn't move. Environment did.

Correct in 2021. Now: new apps, new groups, exceptions "just for this project." AD's been drifting 15 years. The cloud caught up in 3.

02 / DORMANT
02

Licensed. Never turned on.

Defender for Cloud Apps. Insider Risk. Purview DLP in audit mode 18 months. LAPS undeployed. Protected Users empty.

03 / ORPHAN
03

Runs. No one watching.

Someone configured it. They left. The dashboard stayed green. The oldest orphans outlive two or three admin generations.

None of this shows up as "broken." On paper, you are protected. But on paper isn't where attackers operate.

Buy a management layer. Never fix what it was managing.

Customers keep buying solutions that sit on top of their existing stack. A new dashboard. Another orchestrator. Another pane of glass.

But the stack underneath was never aligned to best practice, or set up once years ago, and never maintained.

LAYER 03 · NEW PURCHASE
Management orchestrator €€€

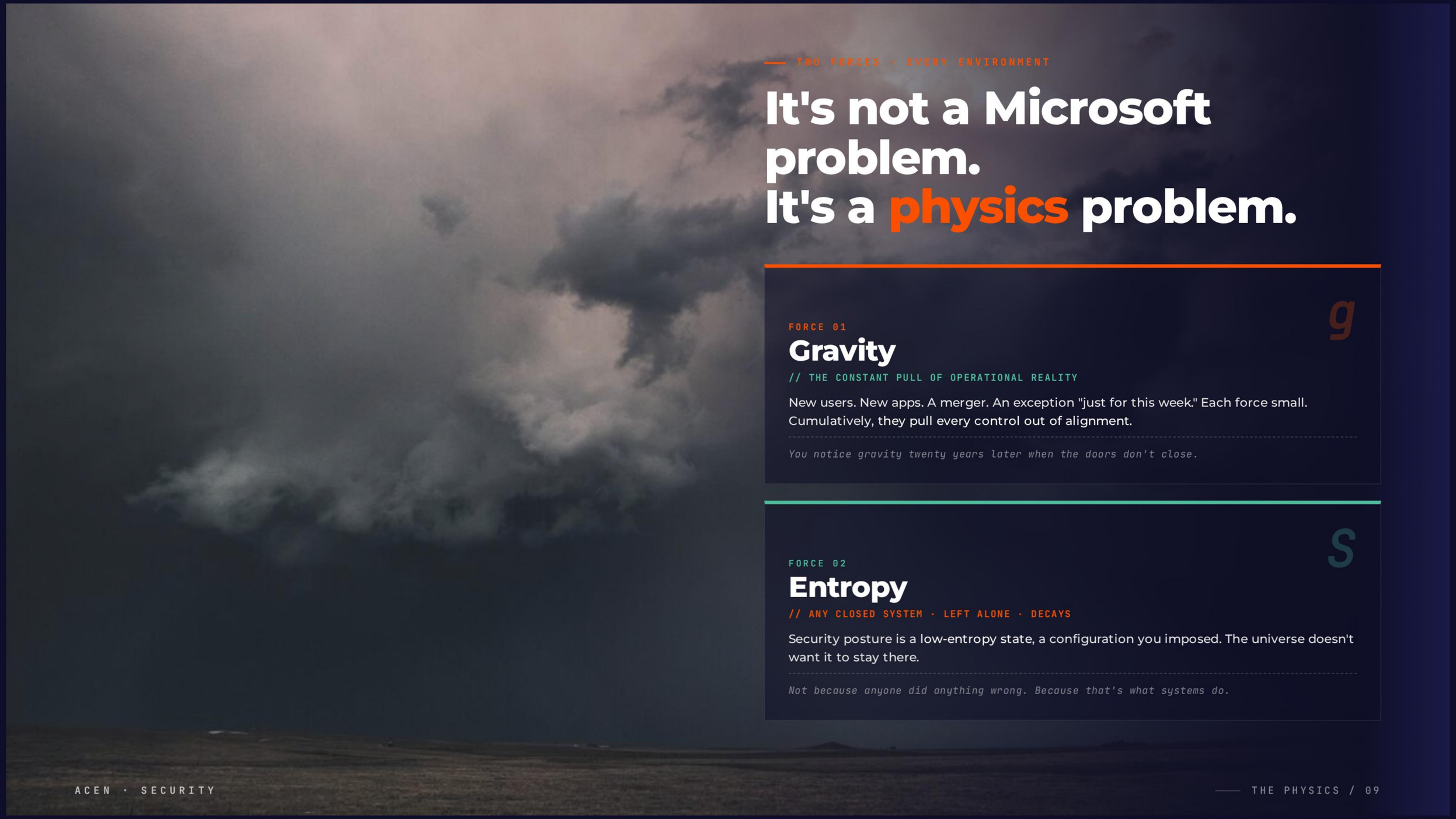
↓

LAYER 02 · EXISTING TOOLS
Defender · Entra · Purview · M365E5

↓

LAYER 01 · NEVER MAINTAINED
Misconfigured baseline ✗
// where the breach actually starts


ON PAPER
You are protected.
But on paper isn't where attackers operate.
LICENSE ACTIVE
POLICY EXISTS
TOOL DEPLOYED
DOOR OPEN



TWO FORCES · EVERY ENVIRONMENT

It's not a Microsoft problem. It's a physics problem.

FORCE 01

Gravity

// THE CONSTANT PULL OF OPERATIONAL REALITY

New users. New apps. A merger. An exception "just for this week." Each force small. Cumulatively, they pull every control out of alignment.

You notice gravity twenty years later when the doors don't close.

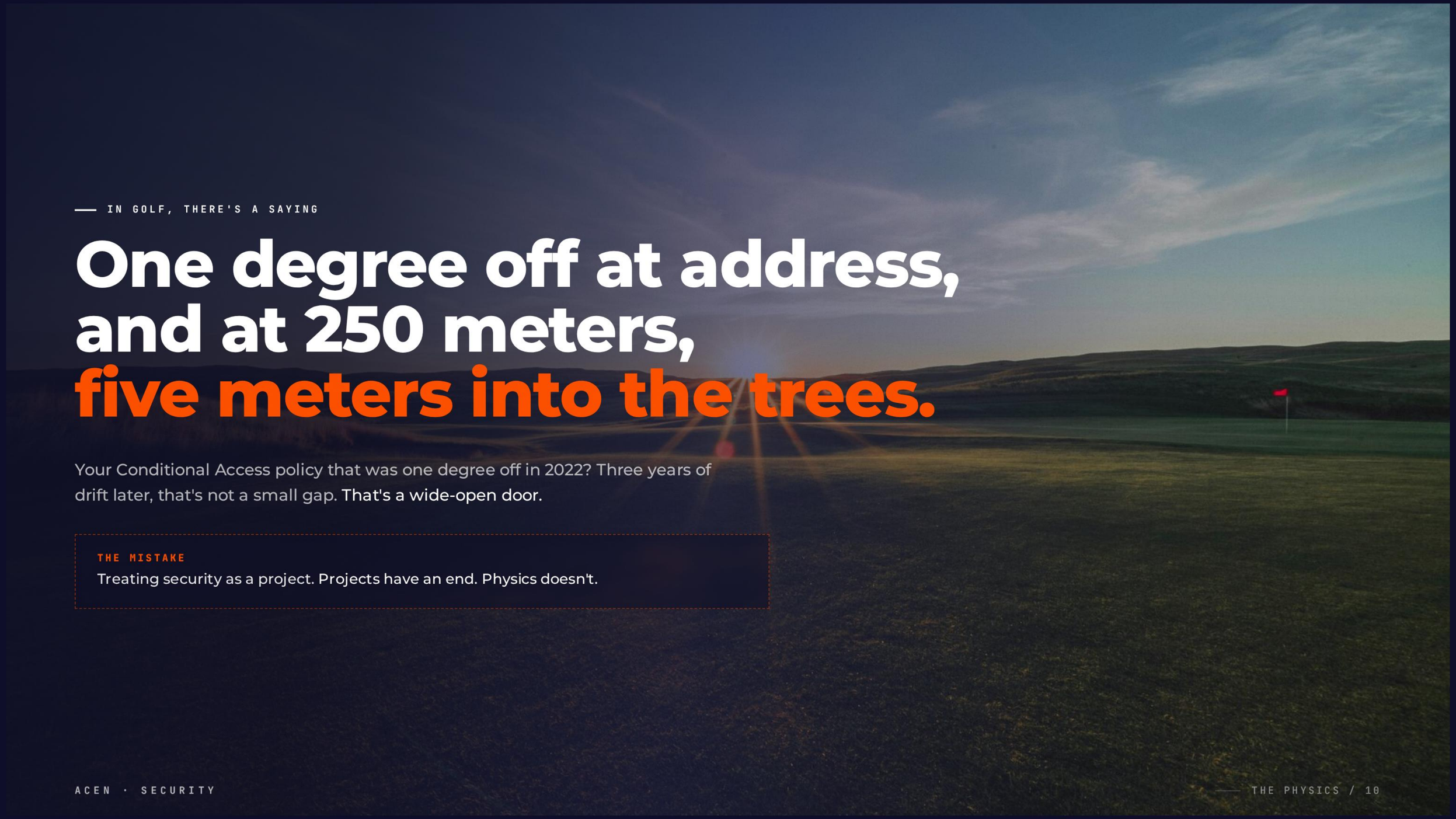
FORCE 02

Entropy

// ANY CLOSED SYSTEM · LEFT ALONE · DECAYS

Security posture is a low-entropy state, a configuration you imposed. The universe doesn't want it to stay there.

Not because anyone did anything wrong. Because that's what systems do.



— IN GOLF, THERE'S A SAYING

One degree off at address, and at 250 meters, five meters into the trees.

Your Conditional Access policy that was one degree off in 2022? Three years of drift later, that's not a small gap. That's a wide-open door.

THE MISTAKE

Treating security as a project. Projects have an end. Physics doesn't.

HOLE 16 · PAR 4 · 10 OVER THROUGH 15

Pull left. Hero shot. Plugged in the bunker.

SHOT 01 TEE · PULL LEFT | **SHOT 02** HERO · BUNKER | **SHOTS 03-06** STILL IN SAND | **SCORE 8 ON PAR 4**

A best round of my life, ruined on one hole. Except: the disaster wasn't where I thought it was.

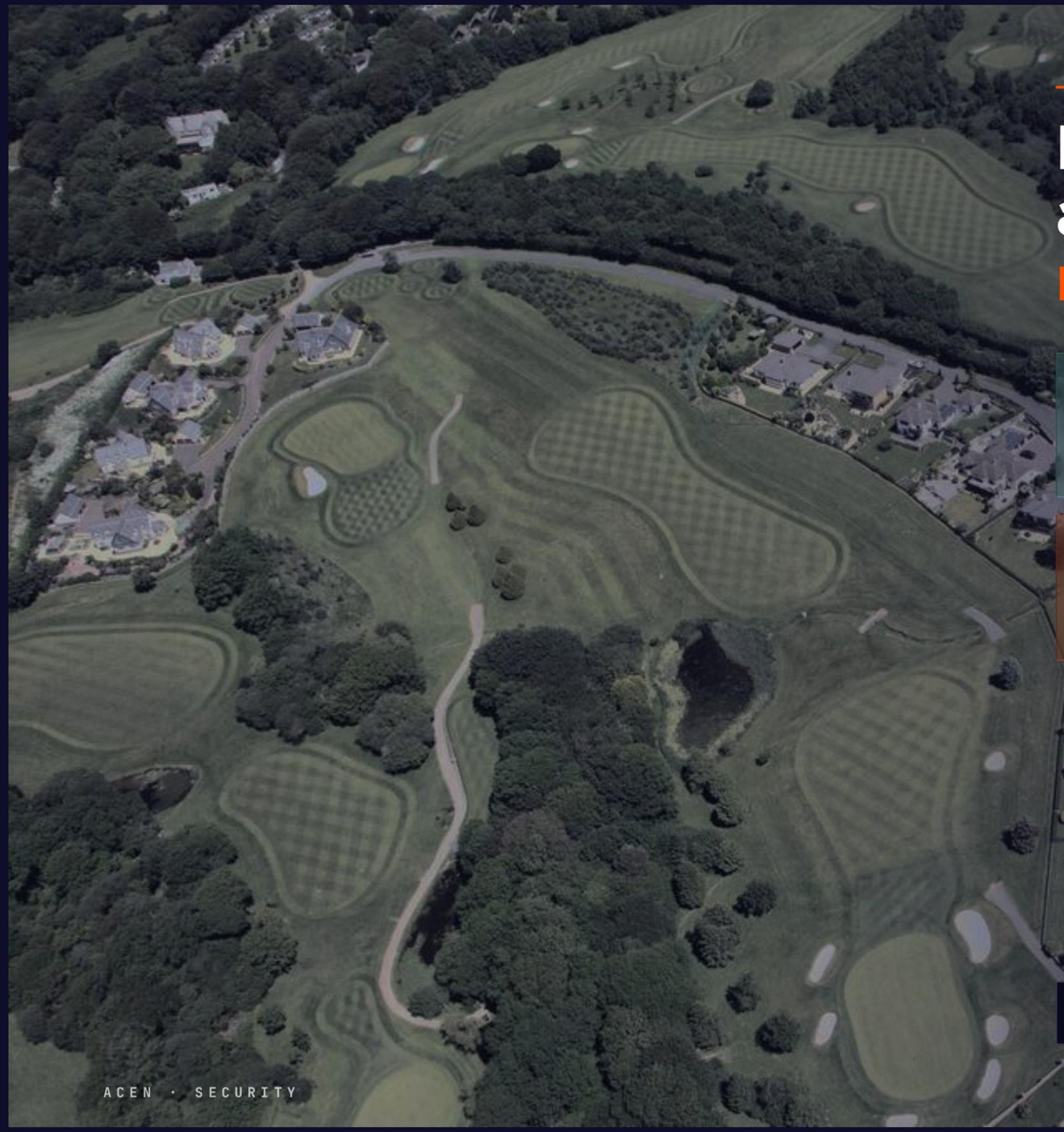
The disaster didn't happen on 16. It happened months earlier.

01 · MONTHS EARLIER	**A service account with a weak password** *"temporarily."*
02 · MONTHS EARLIER	**MFA rolled out to 95% of users** *"done next sprint."*
03 · MONTHS EARLIER	**An admin role granted for a project** *"only for now."*

∴ By the time the alert fires, the real mistake is already old.

You don't get good at bunker shots during a tournament.

You don't get good at incident response during a breach.



SAME SCORECARD · TWO DIFFERENT COURSES

Every organisation has a front nine and a back nine.

FRONT NINE

M365 · Entra · Cloud

9

Open, links-style. Where everyone is looking. The new estate. Audited. Visible.

BACK NINE

Active Directory · On-prem

9

Tree-lined. Narrow. Trees you planted fifteen years ago and forgot. Forgotten.

RULE You can't govern one and ignore the other. The attacker plays all eighteen.

The yardage book is an asset inventory.

Translate the discipline of a professional caddie into the work most security teams have never been given time for.

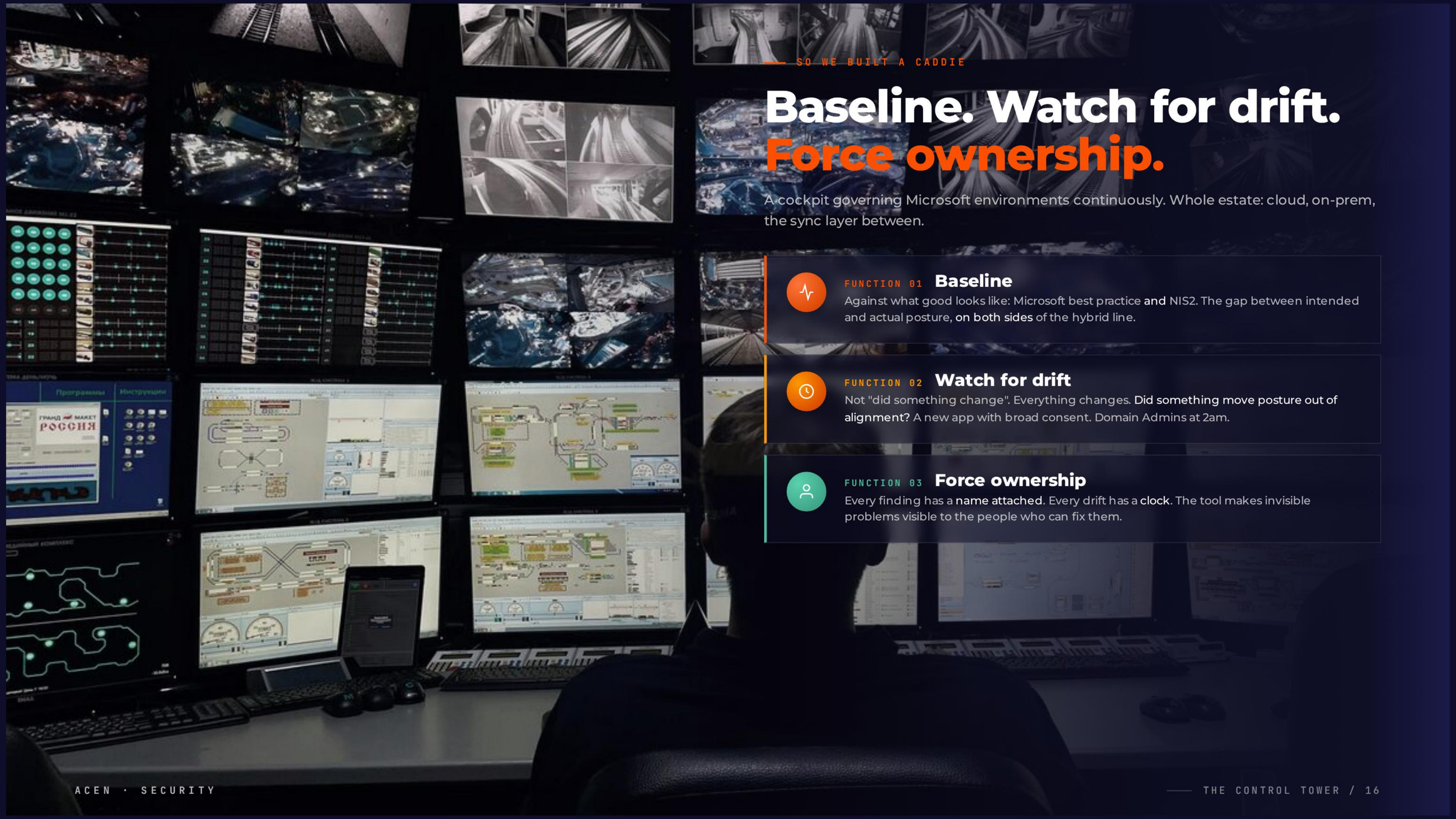
YARDAGE BOOK = Asset inventory
What's in your tenant? Which apps have which permissions?

WALKING THE COURSE = Threat modeling
Who has standing admin access right now, today, this minute?

IDENTIFYING HAZARDS = Configuration baseline
Which Conditional Access policies overlap? Which contradict?

SOFT VS HARD SAND = Real vs theatre
Who's in Domain Admins? Which trusts did you forget you had?

The honest answer: no. Because nobody gave them a caddie.



SO WE BUILT A CADDIE

Baseline. Watch for drift. Force ownership.

A cockpit governing Microsoft environments continuously. Whole estate: cloud, on-prem, the sync layer between.

FUNCTION 01 **Baseline**

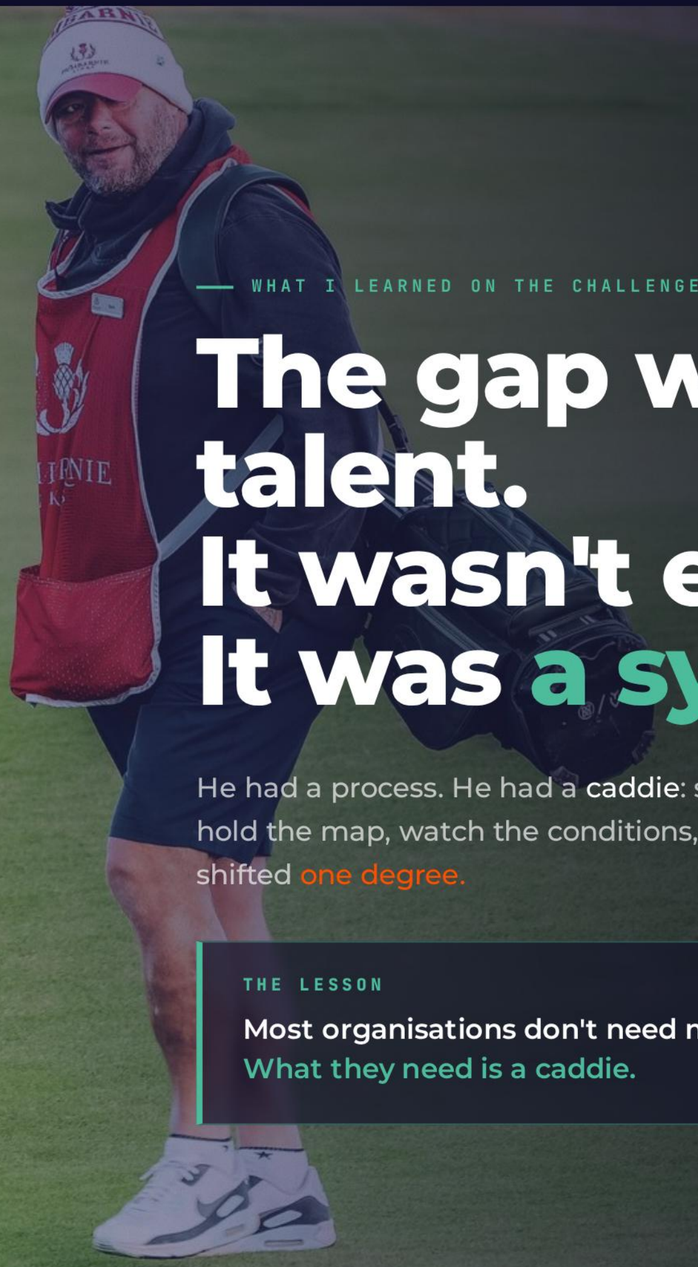
Against what good looks like: Microsoft best practice and NIS2. The gap between intended and actual posture, on both sides of the hybrid line.

FUNCTION 02 **Watch for drift**

Not "did something change". Everything changes. Did something move posture out of alignment? A new app with broad consent. Domain Admins at 2am.

FUNCTION 03 **Force ownership**

Every finding has a name attached. Every drift has a clock. The tool makes invisible problems visible to the people who can fix them.



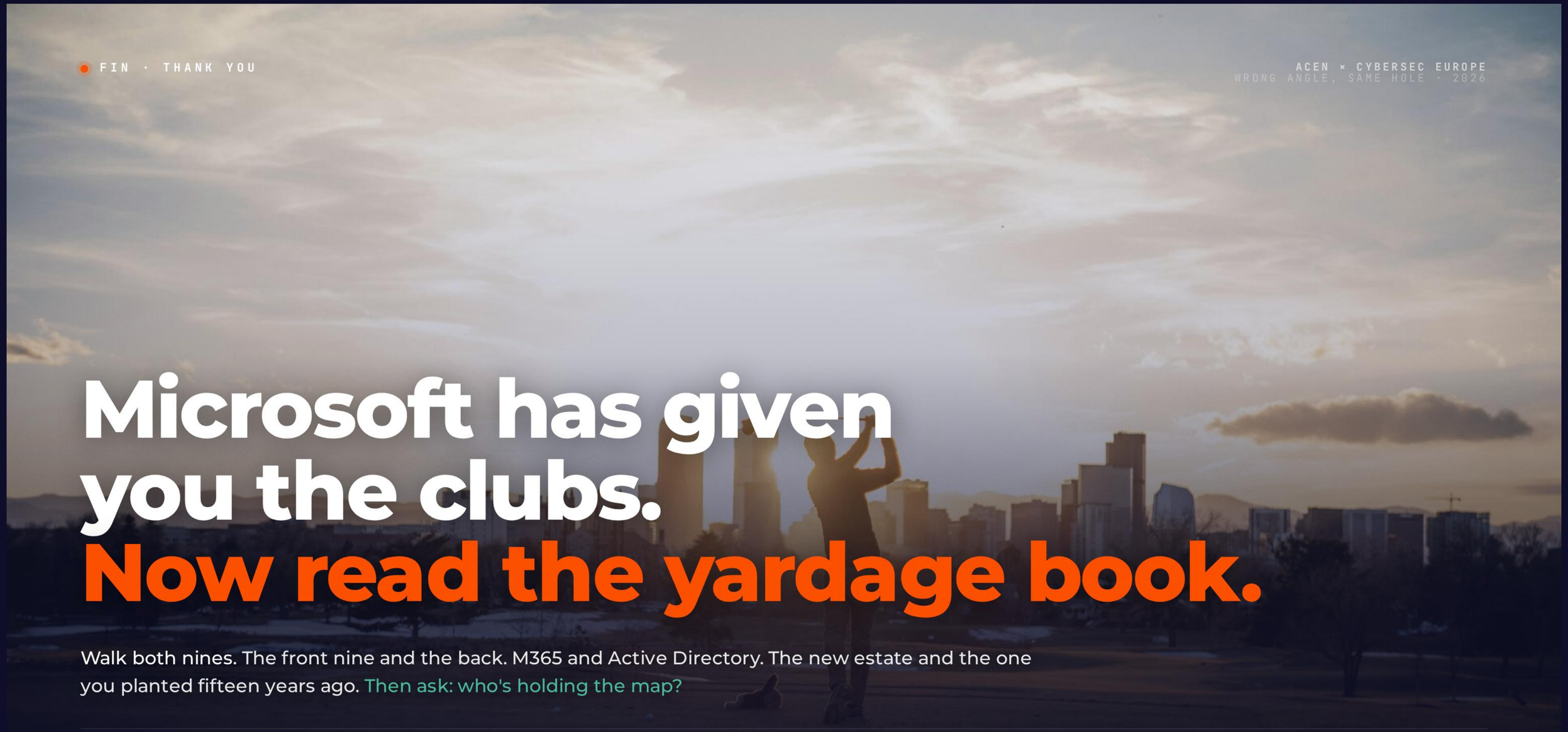
WHAT I LEARNED ON THE CHALLENGE TOUR

The gap wasn't talent. It wasn't equipment. It was a system.

He had a process. He had a **caddie**: someone whose entire job was to hold the map, watch the conditions, and tell him when the wind had shifted one degree.

THE LESSON

Most organisations don't need more security tools. They have enough. What they need is a caddie.



Microsoft has given you the clubs. Now read the yardage book.

Walk both nines. The front nine and the back. M365 and Active Directory. The new estate and the one you planted fifteen years ago. Then ask: who's holding the map?

ACEN HQ

Veldkant 33a · 2550 Kontich · Belgium
acen.eu · kristof.laerenbergh@acen.eu · jahirt.ruiz@acen.eu