



When Trust Becomes the Threat

Behavioral Intelligence in an Artificial World

I've been watching you.

Don't worry. Professionally.





I'm not qualified to psychoanalyse all
cyber professionals before dinner.

The assessment: Who are you people?

A very scientific one.

Say yes or no if feels familiar
or resonates, or not.



menti.com
2987 7379





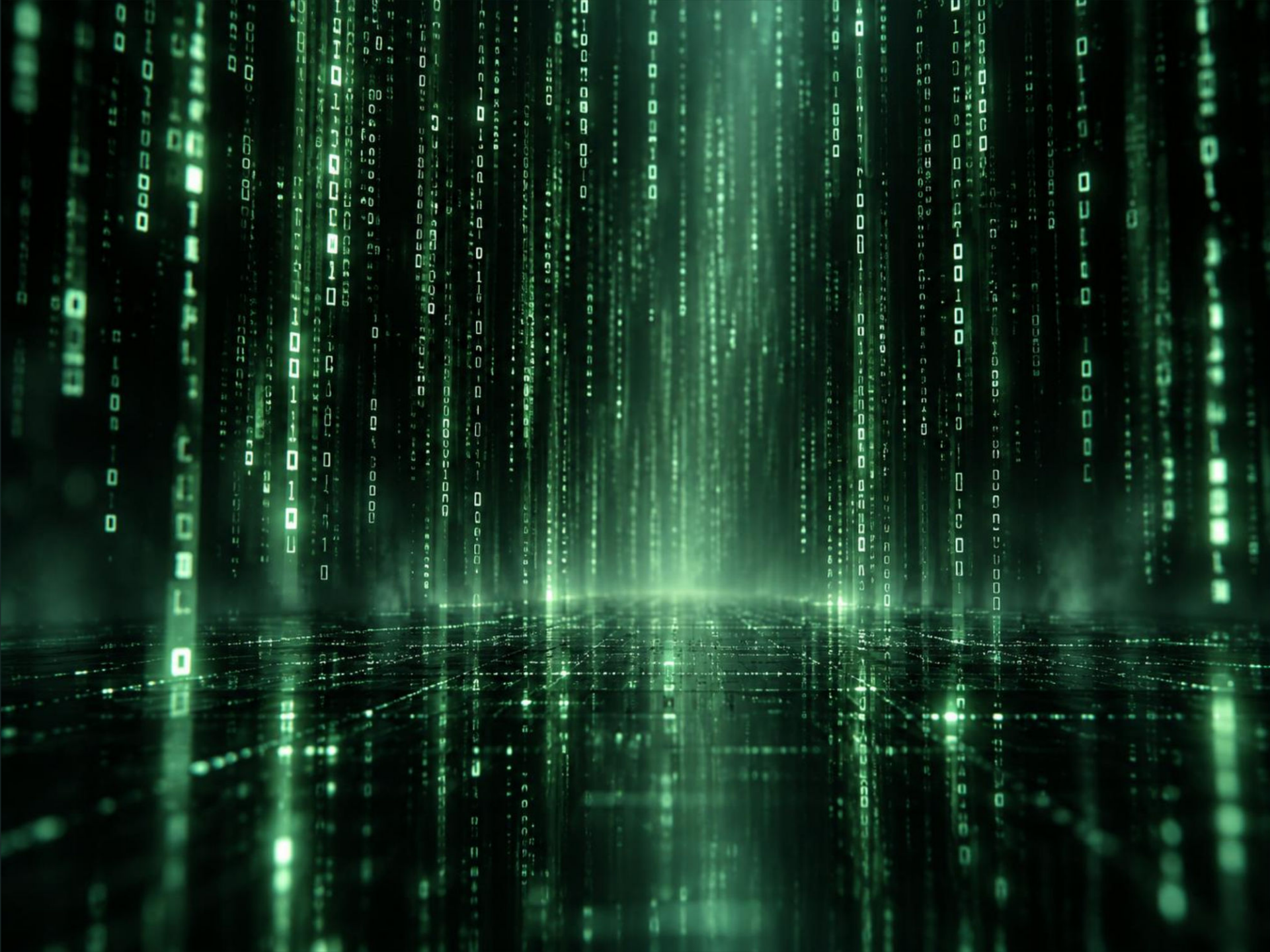
- ① Reproduce
- ② Analyze
- ③ Contain
- ④ Fix
- ⑤ Verify



Threat Hunting
Linux

GOOD
INFRA
BETTER
PEOPLE

DEFEND
OBSERVE
AUTOMATE
REPEAT









Counselor Deanna Troi.

She was there to help interpret the part that wasn't in the data.

Emotion

Intent

Behavior

The meaning behind what people were saying

While you were looking at the screen...
I was looking at you.



FAMILIAR

BELONGING

TRUST

That looked familiar.
That felt like us.
So you trusted it.

*Humans have always used signals to decide what (and whom) to **trust**.*

I collected a lot of behavioral information.

But here's the important part.

I still don't know what any of it means.

OBSERVATION $\neq$ INTERPRETATION

Technology produces information. Humans assign meaning.

THE SIGNAL WAS NEVER THE TRUTH

A voice. A face. A title.
An accent. A logo. A
familiar email address.

Signals do not arrive with
meaning attached.
We attach the meaning.

Trust is efficient.

And that is precisely why it is exploitable.



So what happens when the signal stays familiar,
but its origin changes?

For some of you, a familiar dialect does not only carry information.

It carries belonging.

LOCAL • FAMILIAR • ONE OF US • PROBABLY SAFE



The voice isn't Swiss. It isn't even human.

But your brain still recognises home.

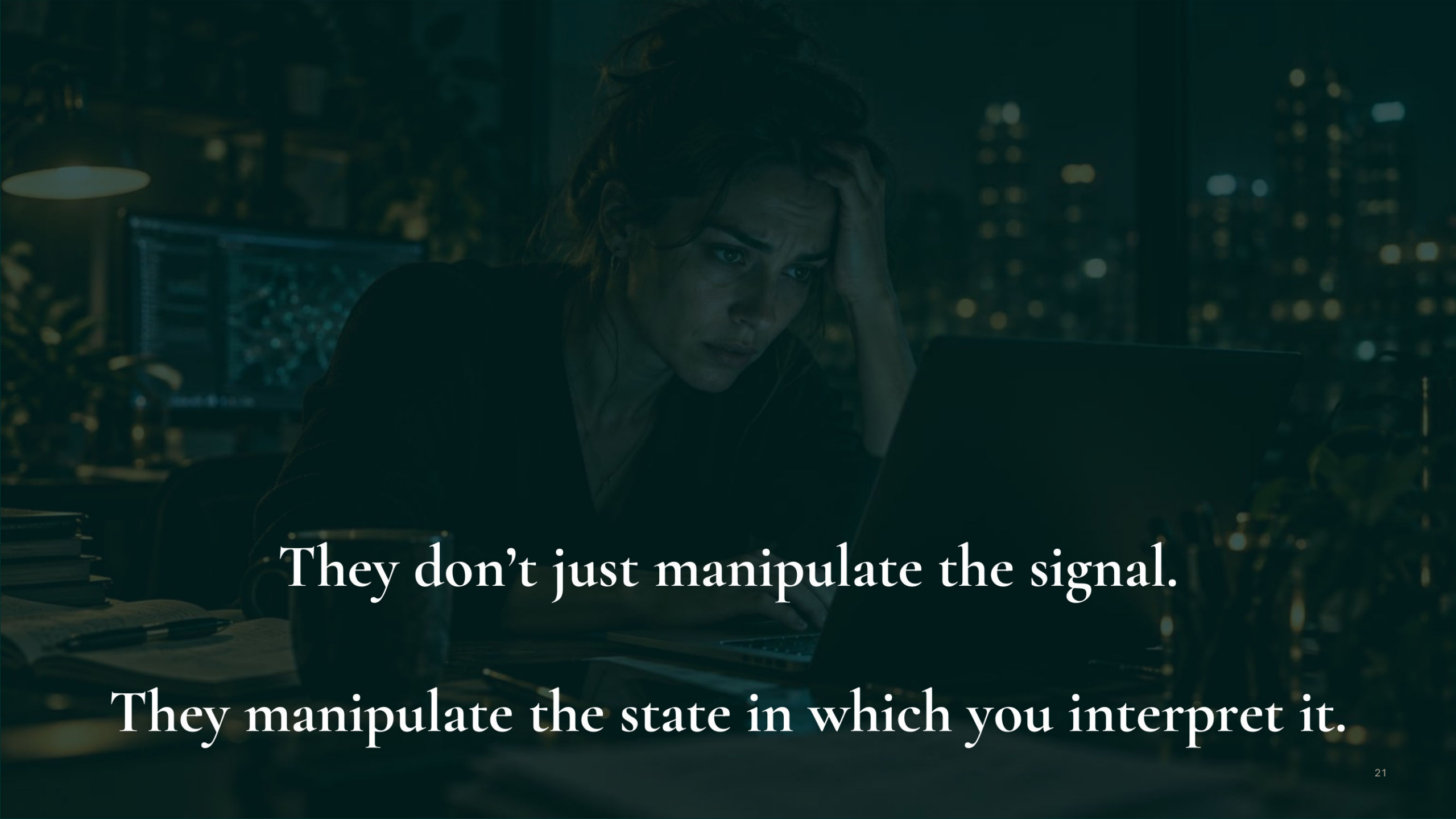
AI changes the reliability of the input our human system receives.



What happens when the signals we learned to
trust can be artificially manufactured?

Human trust isn't a bug.

It is infrastructure.

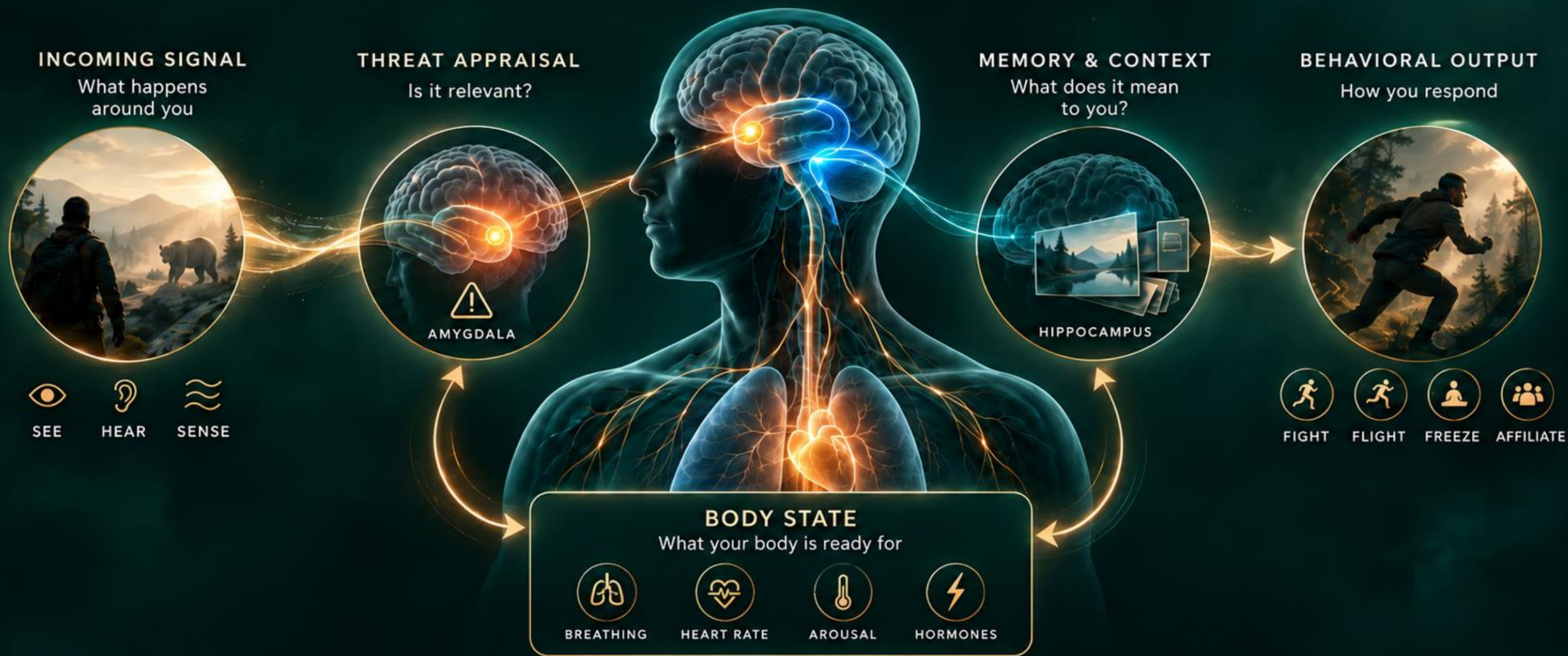
A woman with long, dark hair is sitting at a desk in a dimly lit room at night. She is looking at a laptop screen with a concerned expression, her hand resting on her forehead. The background shows a city skyline with lights visible through a window. The overall mood is one of stress or frustration.

They don't just manipulate the signal.

They manipulate the state in which you interpret it.

The Threat Response System

FROM PERCEPTION TO PHYSIOLOGY TO BEHAVIOR



Under pressure, people do not just interpret the signal — *they interpret it through their state.*

The AI-generated voiceover of President Zelensky used for educational purposes in behavioral analysis training. Not intended to mislead or impersonate. Created by An Gaiser.



Created on
Riverside

But what happens when we hear too much too

Why are we still designing rational solutions for irrational problems?

Especially when stress changes how people process information.

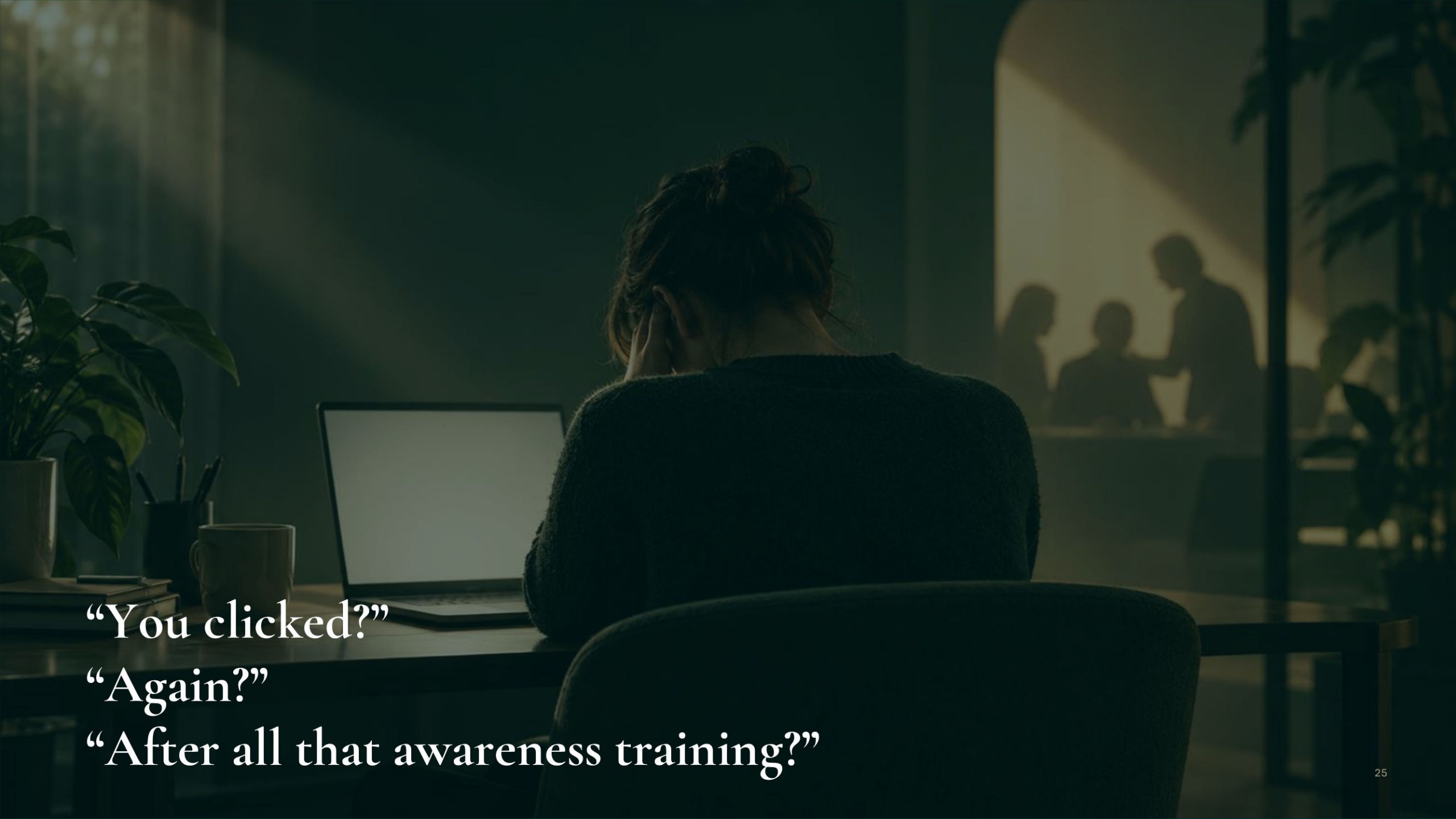


Knowledge doesn't make you immune.

Recognition can give you a window to intervene.

AWARENESS $\neq$ IMMUNITY

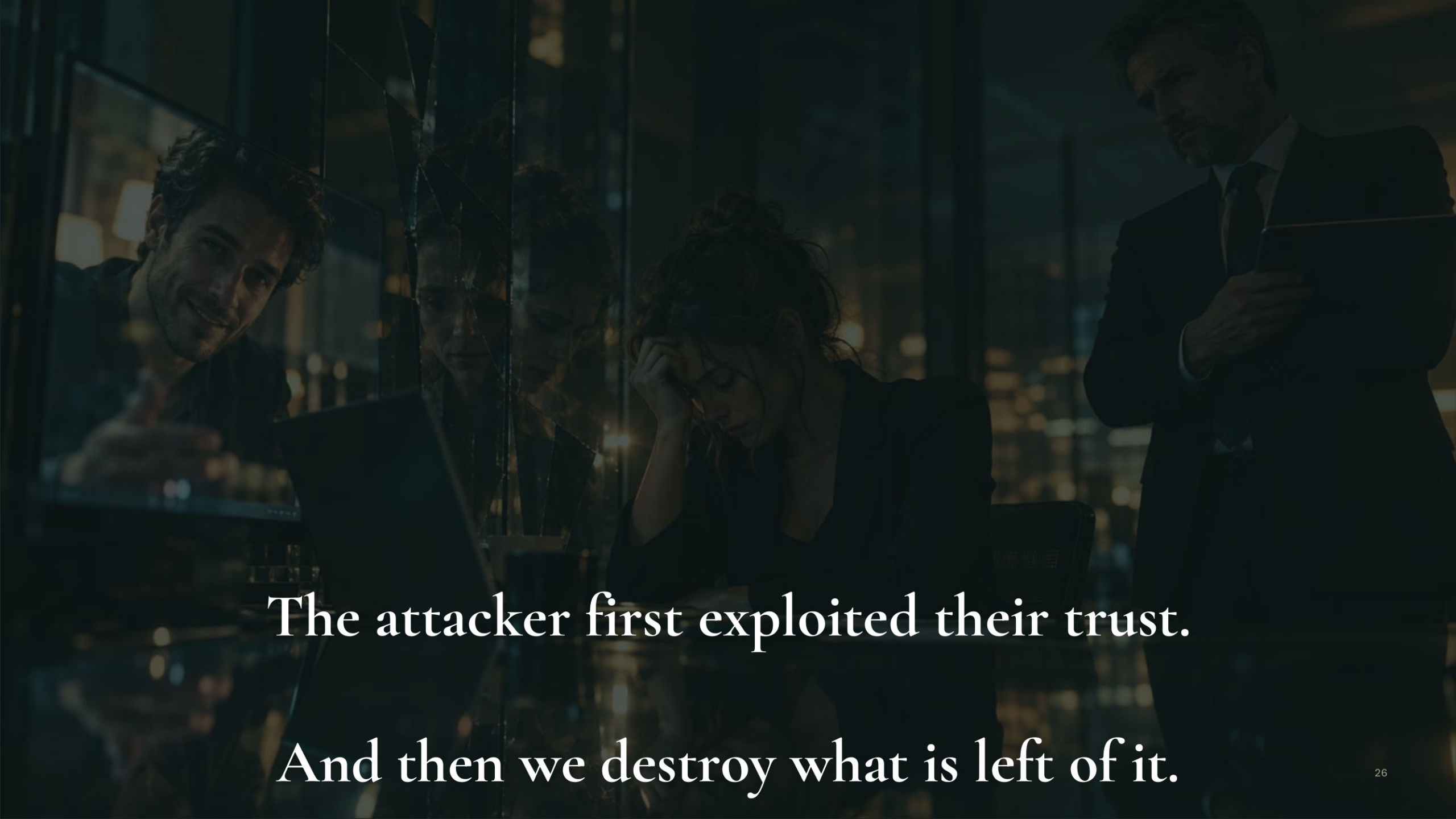
Awareness = earlier recognition

A person with dark hair tied in a bun is seen from behind, sitting at a desk in a dimly lit office. They are holding a phone to their ear. On the desk, there is a laptop with a blank screen, a mug, and some papers. To the left, there is a potted plant. In the background, through a glass partition, the silhouettes of other people working at desks are visible. The overall atmosphere is quiet and focused.

“You clicked?”

“Again?”

“After all that awareness training?”



The attacker first exploited their trust.
And then we destroy what is left of it.

If you treat the people you are trying to protect as the weakest link,
why would they ever trust you enough to tell you when the link has
broken?

Security culture is not what people know about
security.

It is what people dare to tell you when security
has already gone wrong.

Can we trust the user?

Can the user trust us?

Trust determines whether critical information moves ...
or gets hidden.

The image is a composite. On the left, a digital, wireframe hand made of glowing green lines and points reaches out. On the right, a real human hand reaches out towards it. The two hands are just inches apart, with a small glow of light between them. In the background, there is a blurred crowd of people, suggesting a public space or a large gathering. The overall color palette is dark with green and yellow highlights from the digital elements and the light between the hands.

We have spent decades teaching humans
to behave more like security systems.

Maybe it's time we design security systems
that understand how humans actually behave.

Trust needs both culture and clarity.

HEALTHY CULTURE ENABLES PEOPLE. CLEAR THREAT LOGIC SHOWS WHAT TO PROTECT.



CULTURE
SHAPES
BEHAVIOR.

THREAT
LOGIC
CLARIFIES
EXPOSURE.



When someone gets fooled, don't start by asking
what is wrong with them.

Start by asking what the attacker understood
about them that you didn't.

WHOM CAN I TRUST?

AM I WORTHY OF TRUST?

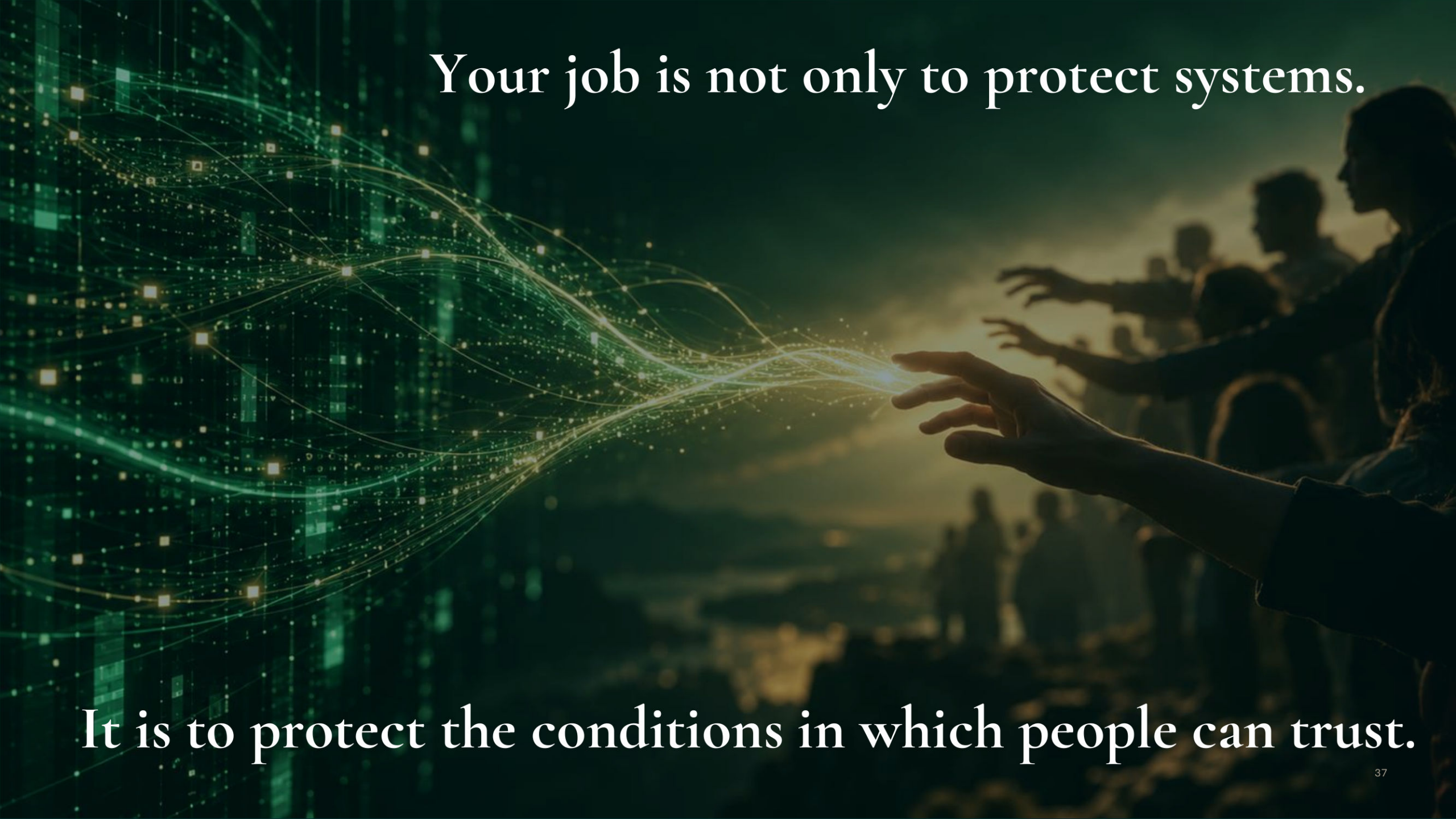
In an artificial world, cybersecurity is no longer only
about deciding what is real.

It is about understanding why humans trust what they trust,
and becoming worthy of that trust ourselves.

Why did you choose this work?

Maybe it was never really about the technology.

Maybe it was about protecting something.



Your job is not only to protect systems.

It is to protect the conditions in which people can trust.

Whatever brought you into this work...

Don't lose that.

NOTICE MORE.

ASSUME LESS.

DECIDE BETTER.

NOTICE MORE.

ASSUME LESS.

BE WORTHY OF TRUST...

DECIDE BETTER.

Thank You!

www.angaiser.com

info@angaiser.com

English book “Hidden Signals” coming soon!

De kunst
van timing en
invloed in
gesprekken

AN GAISER

VERBORGEN SIGNALEN

Dit is het boek dat ik had willen hebben toen ik FBI-agent werd – een absolute aanrader.
Joe Navarro, voormalig FBI-agent, internationaal bestsellerauteur en spreker