

Practical Magic: Behavior-based Safety Design for IoT

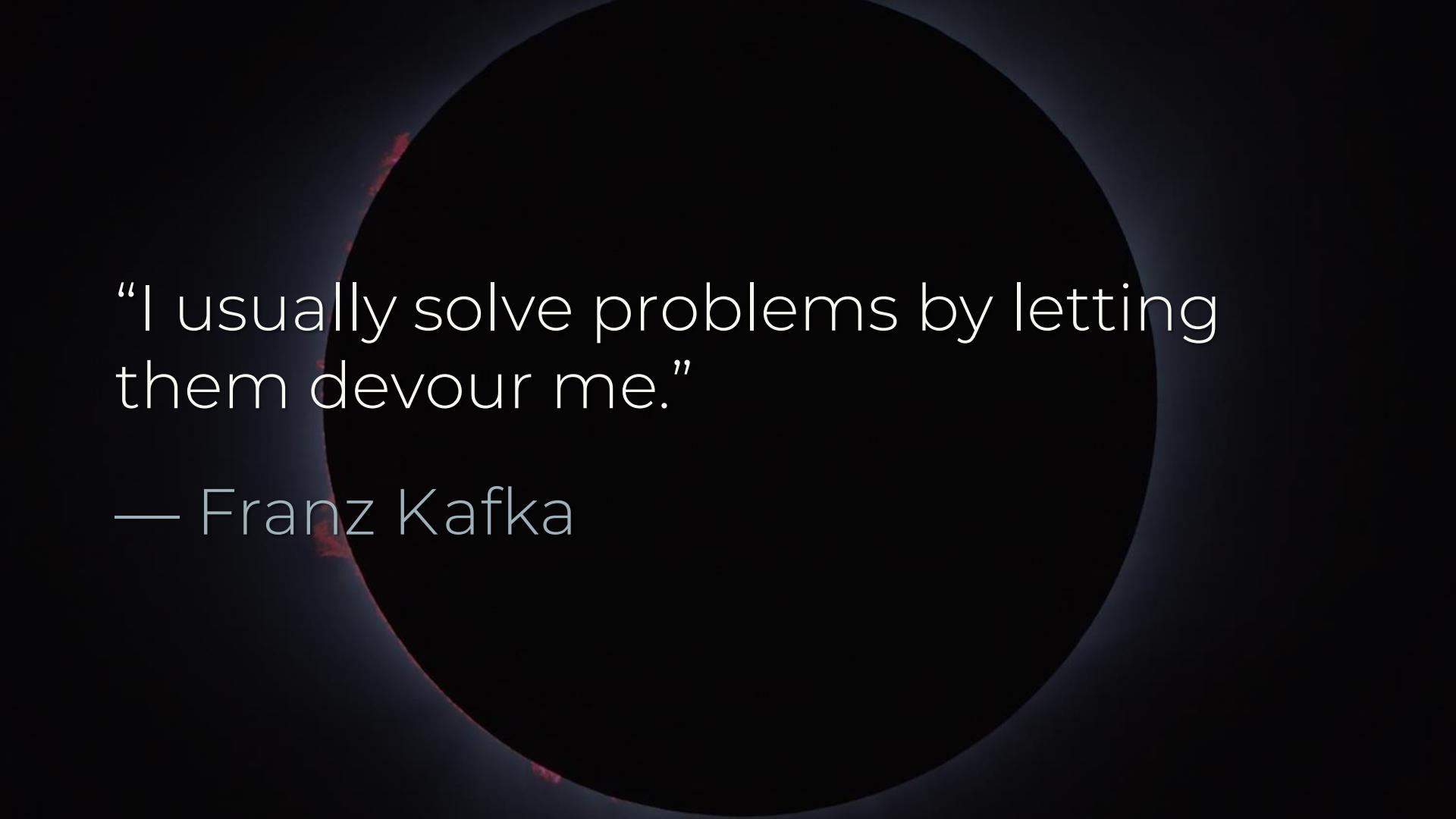
Kelly Shortridge (@swagitda_)
Troopers 2018



Hi, I'm Kelly

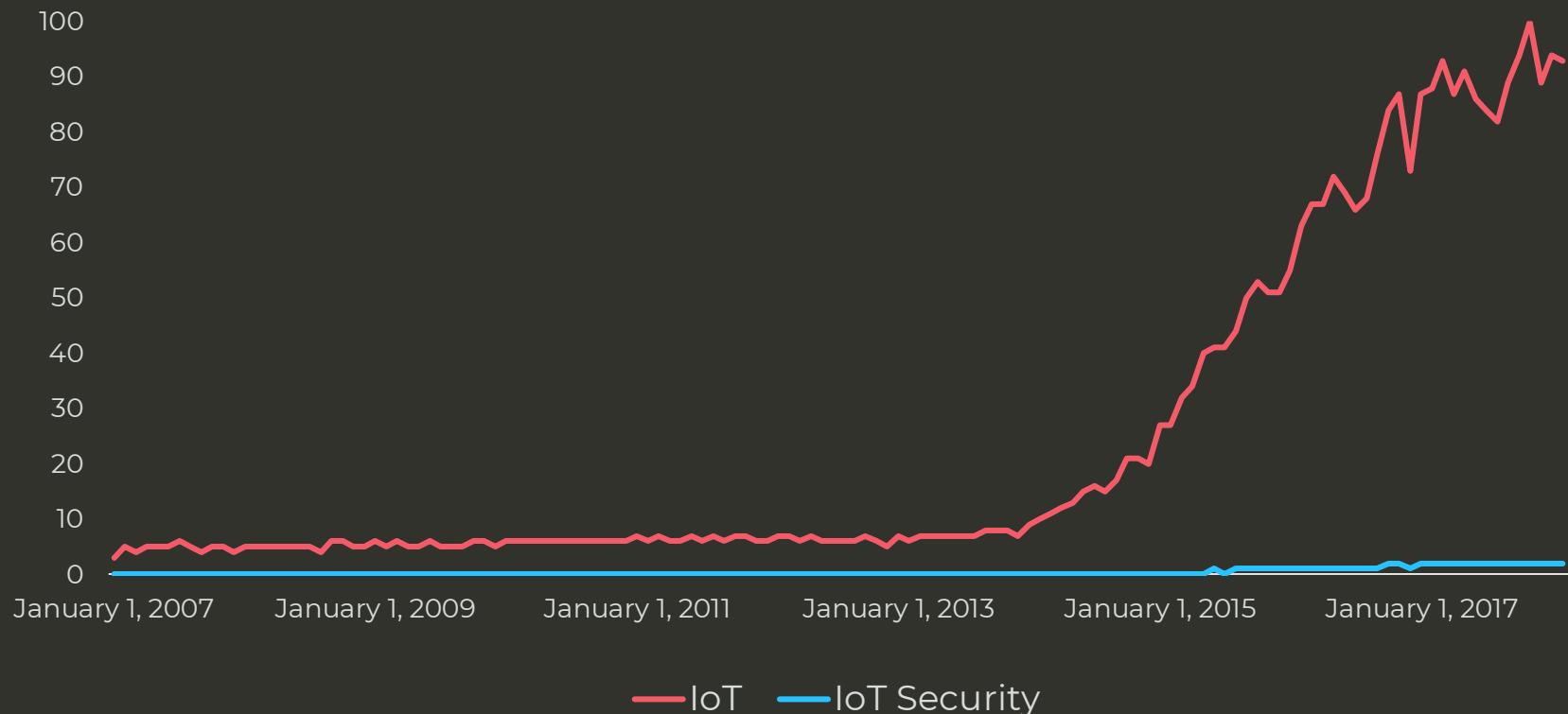


SecurityScorecard



“I usually solve problems by letting them devour me.”

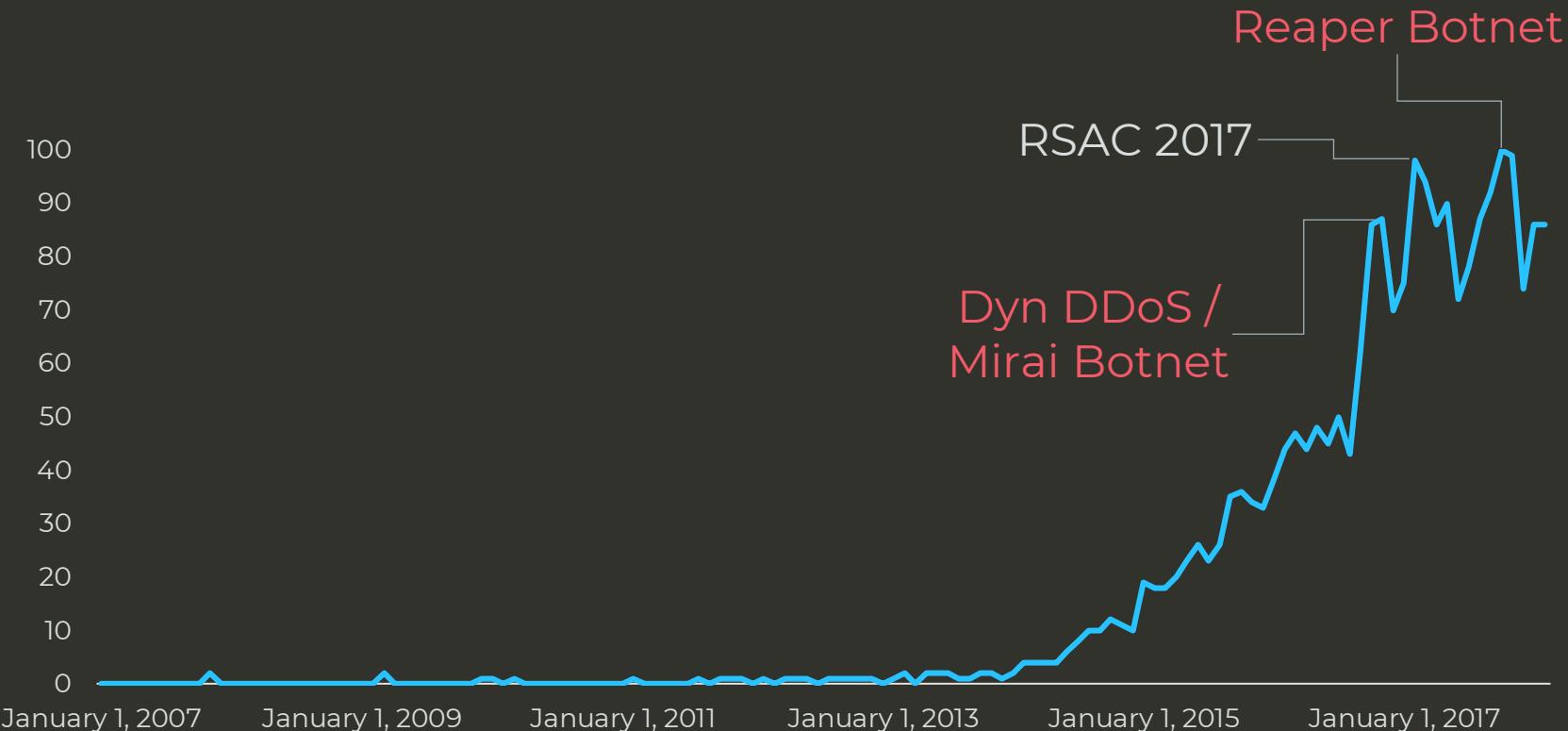
— Franz Kafka



Source: Google Trends

A dark, circular tunnel with diamond-plate floor and walls, leading to a bright light at the end.

We're engendering a Kafkaesque
paradigm for IoT security



Source: Google Trends

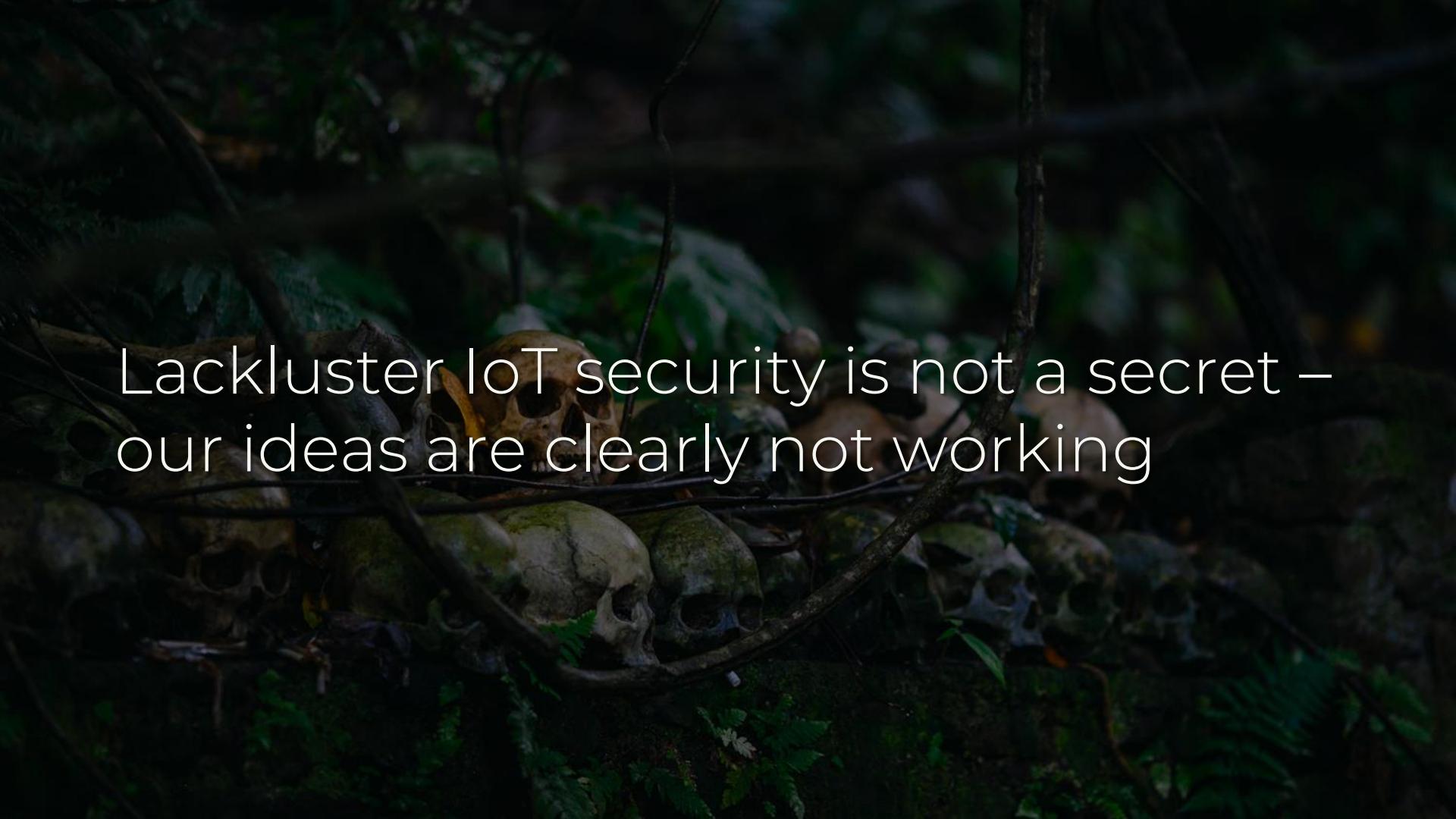


IoT botnets are the first, and ravenous, boss of the IoT security battle

Mirai: 60 default passwords led to
100k node botnet attack against Dyn



But we're promoting complexity & a seemingly endless set of hurdles

A dark, atmospheric photograph showing several human skulls and bones scattered among green ferns and foliage. The scene is dimly lit, with the subjects appearing as dark shapes against a background of deep shadows and muted greens.

Lackluster IoT security is not a secret –
our ideas are clearly not working

A photograph of a person performing a handstand in a forest. The person is wearing a light-colored long-sleeved shirt and dark pants. They are positioned on a fallen log or a low branch, with their body inverted. The background consists of dense trees and foliage, with sunlight filtering through the leaves, creating bright highlights on the person's body and the surrounding environment.

By understanding behavior, we can
guide choice & support secure habits

- 
1. Existing Suggestions
 2. Incentive Problems
 3. Behavior-Based Design
 4. IoT Security Ideas

Existing Suggestions



FTC recommends building-in security
from the beginning (simple as that!)

FDA: Pre- & Post-Market Guidelines (H/T @marasawr)

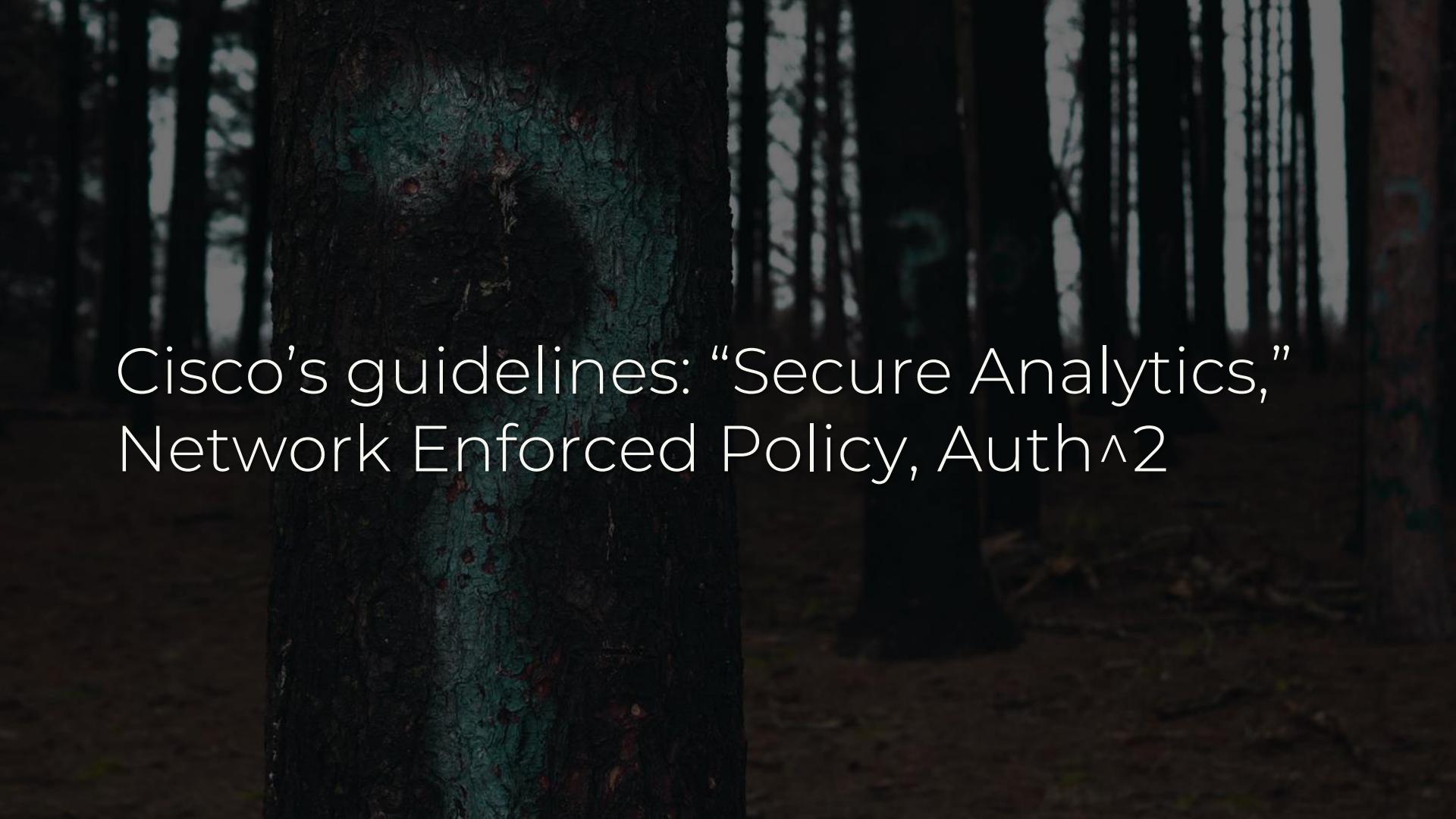
The background of the slide features a close-up, slightly blurred photograph of a stack of antique books. The books are bound in dark, textured leather, showing significant wear, discoloration, and some loss of material at the edges and corners. The spines of the books are visible, with some featuring gold-tooled decorations. The overall lighting is warm and focused on the top few books, creating a scholarly and historical atmosphere.

Pre-market: a lot of documentation & threat modelling

Post-market: monitoring & a
mitigation deployment strategy

OWASP: IoT Testing Guide, IoT Attack Surface Areas, Principles of IoT Sec...

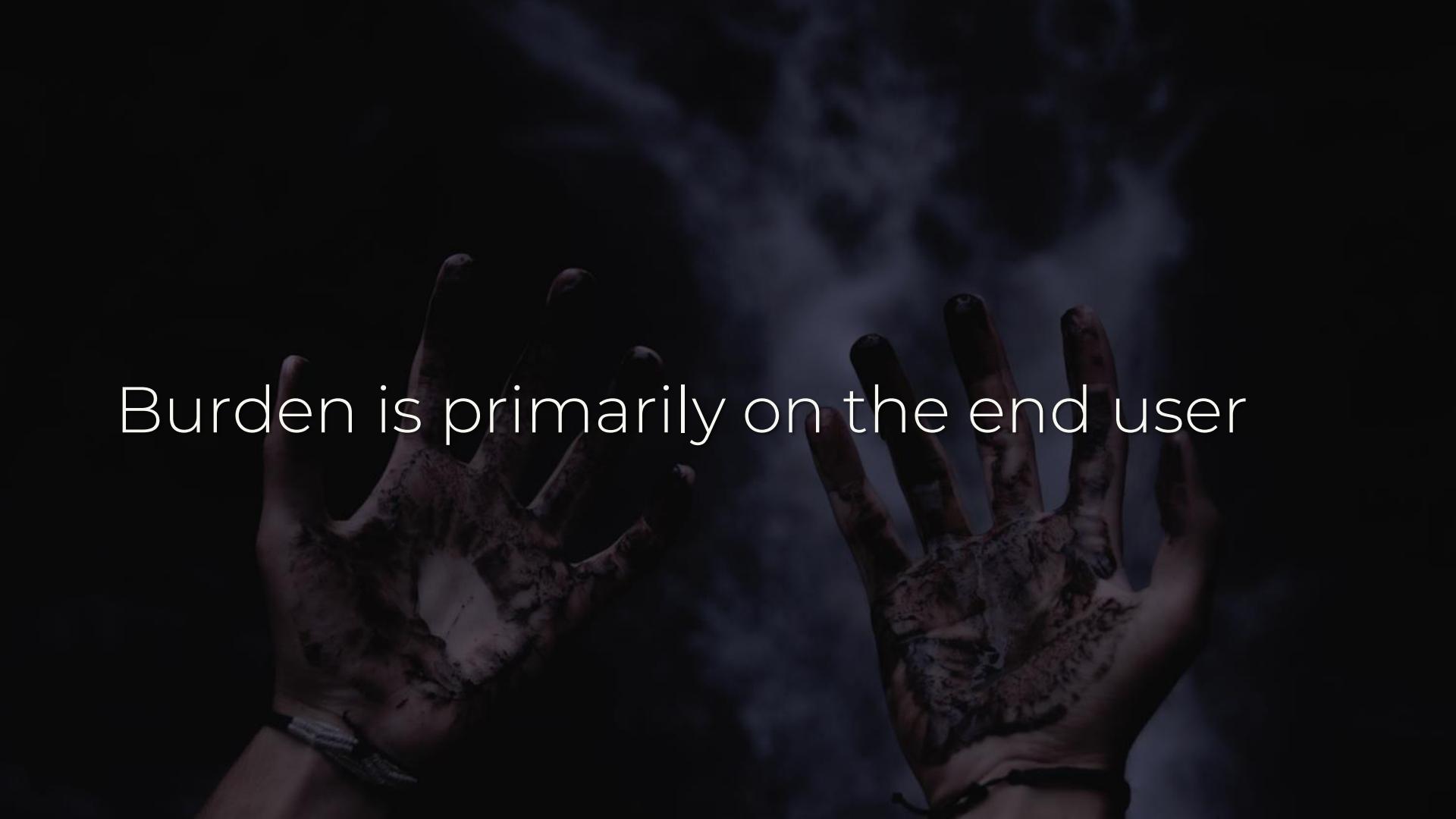
Designed for the penetration tester
user persona – not developers



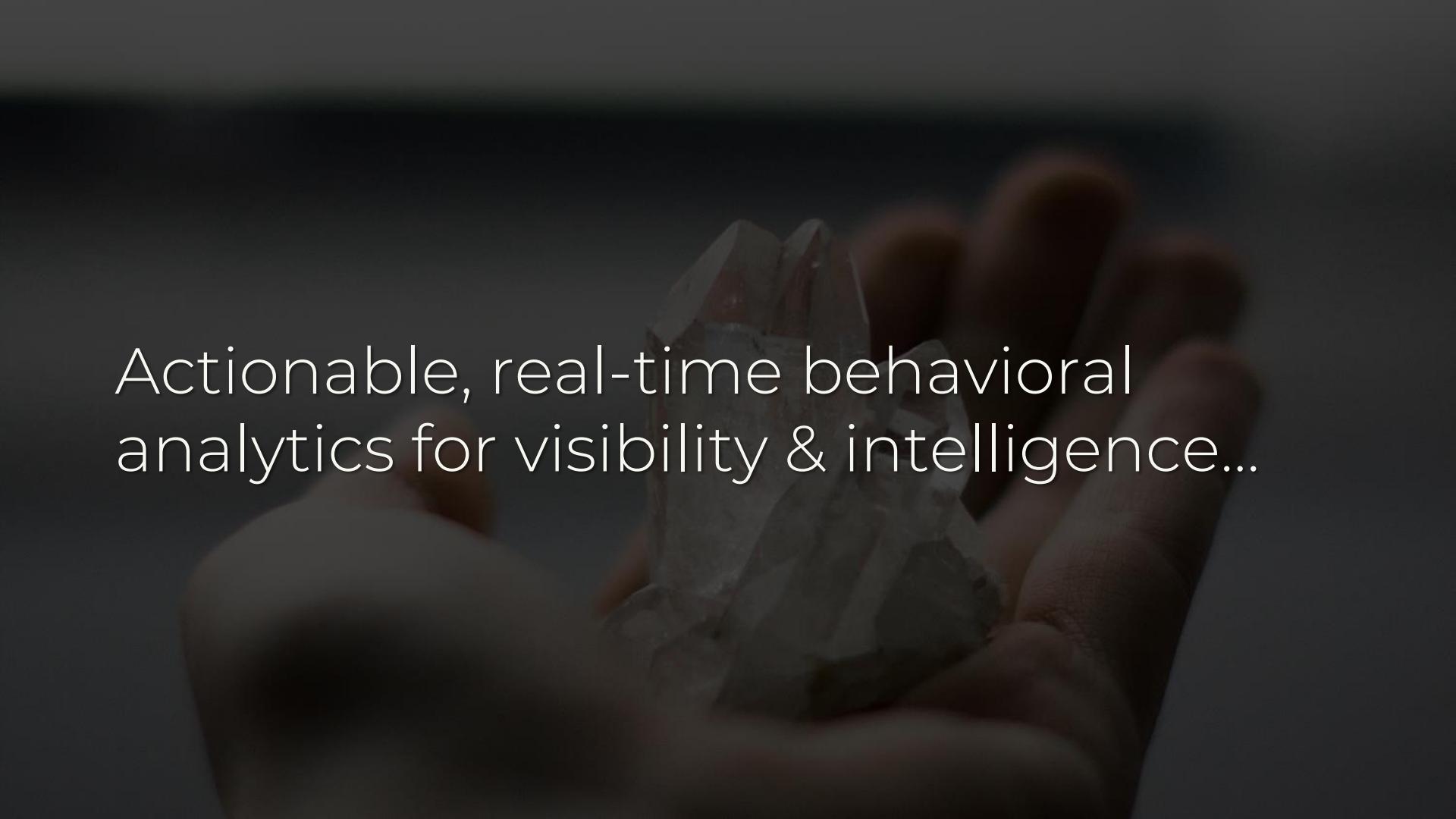
Cisco's guidelines: "Secure Analytics,"
Network Enforced Policy, Auth^2



Compensating Controls: post-market remedies by third parties



Burden is primarily on the end user



Actionable, real-time behavioral
analytics for visibility & intelligence...

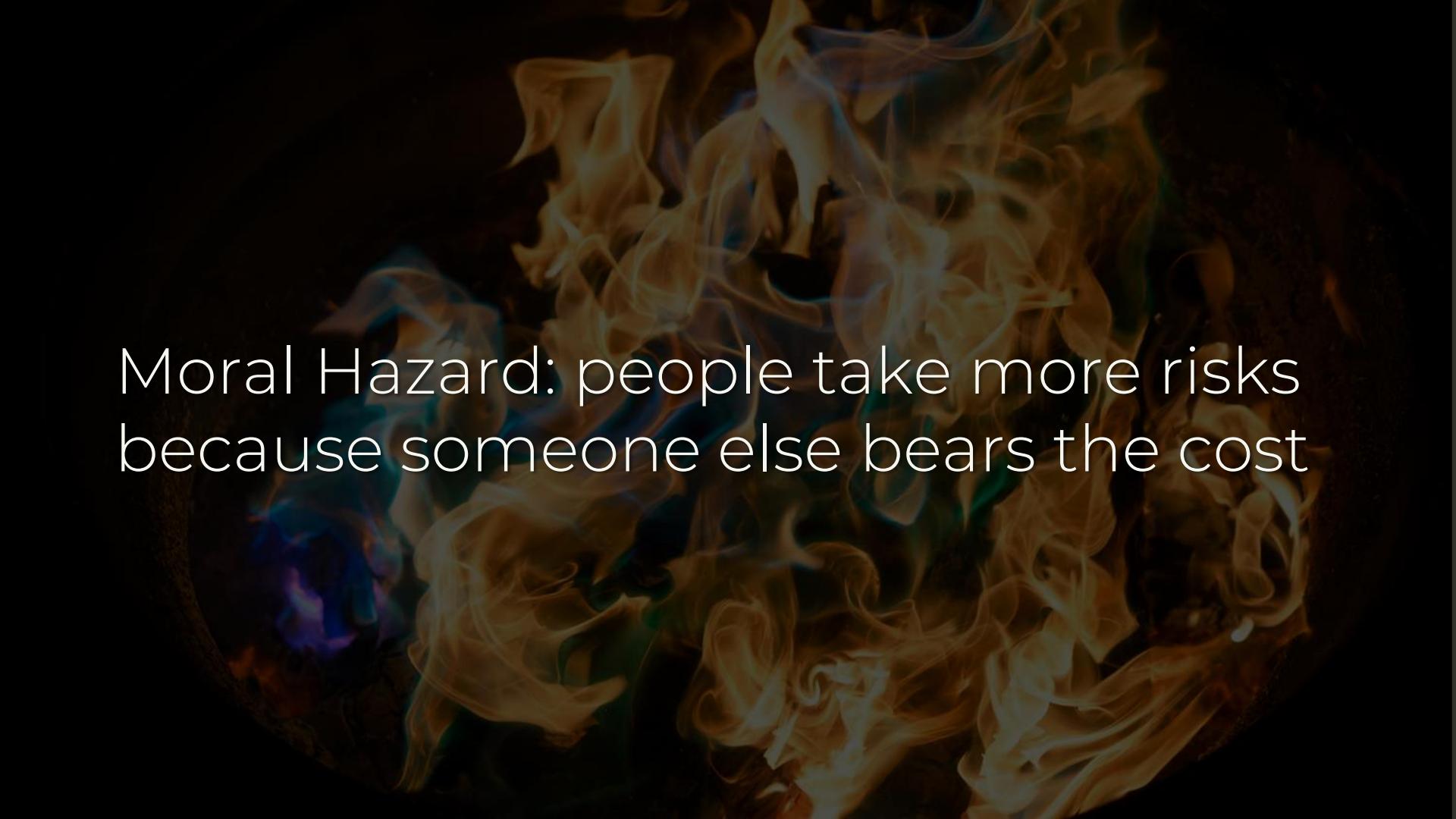
Maybe feasible for enterprises, but
what are consumers to do?

Incentive Problems



Principal-agent problem: someone
else makes the decisions, but you
bear the impact

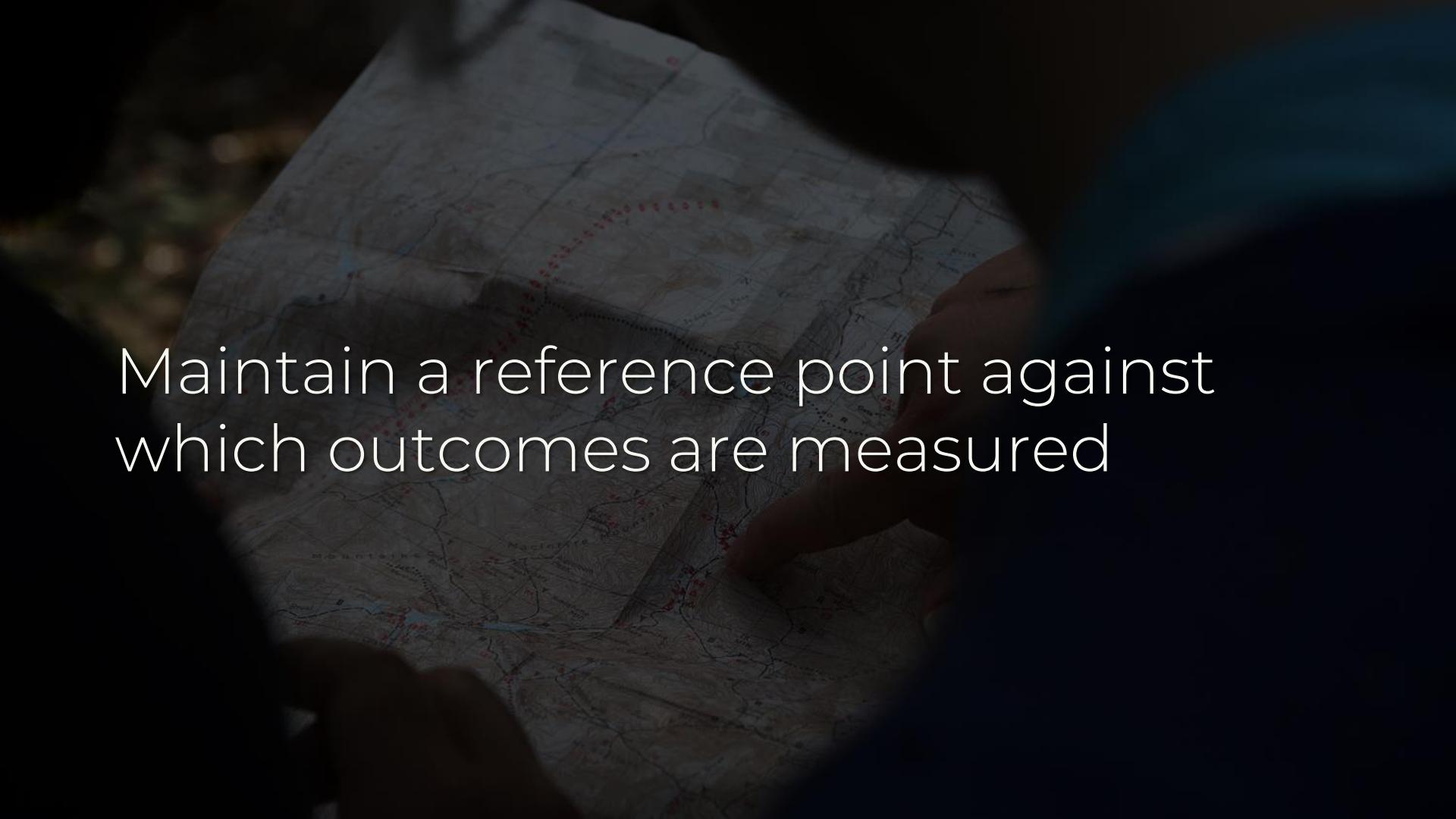
The Agent has their own self-interest.
It's likely not the same as yours.

The background of the slide features a dynamic, abstract pattern of swirling flames. The flames are primarily orange and yellow, with some darker, smoky areas and occasional blue and purple highlights, suggesting a fire or explosion. They are set against a dark, almost black, background which makes the bright colors stand out. The flames appear to be in motion, creating a sense of energy and intensity.

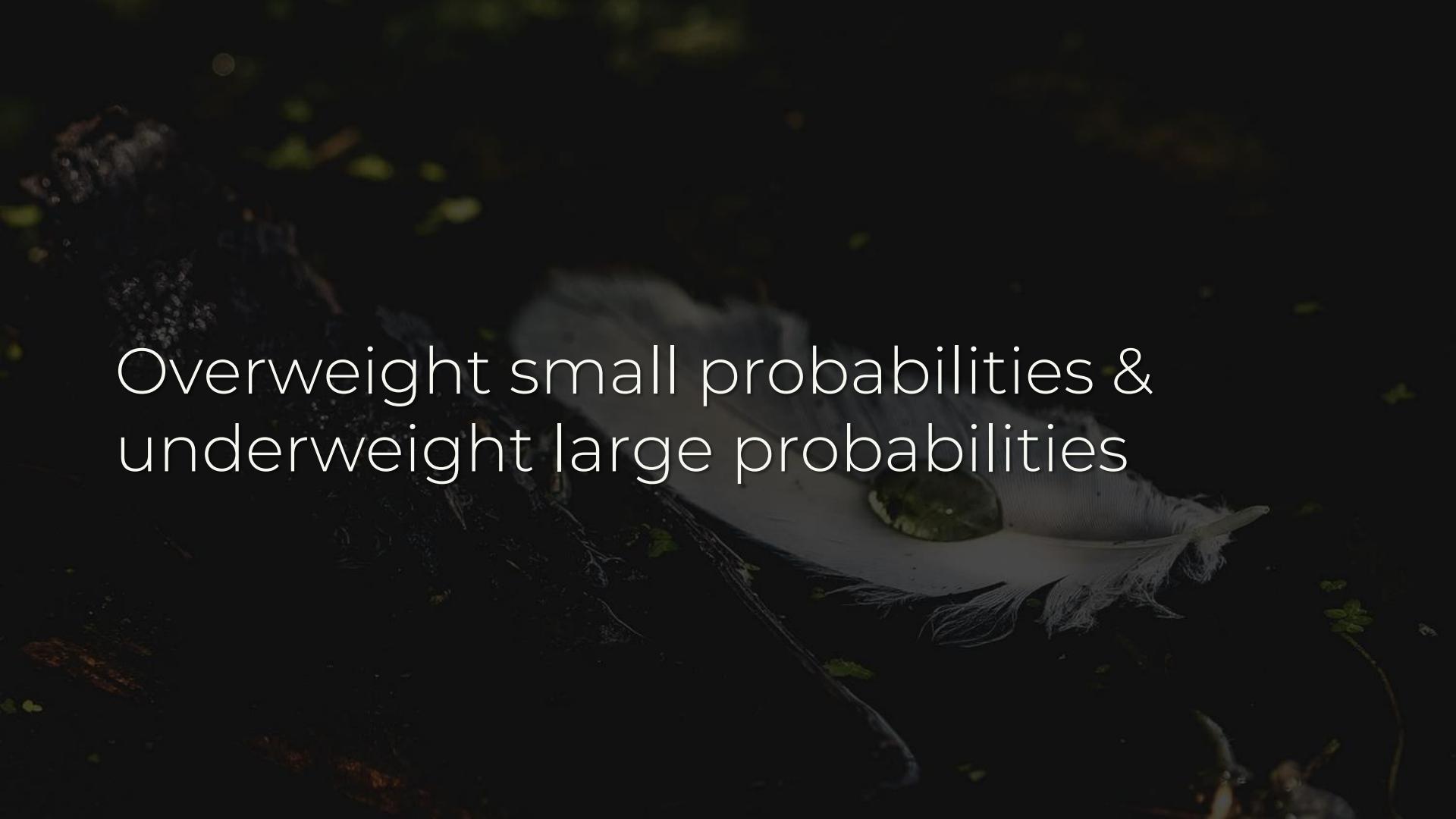
Moral Hazard: people take more risks
because someone else bears the cost

Next level: Equifax's customers aren't
the end users whose data is stored

Prospect Theory: people care about relative vs. objective outcomes

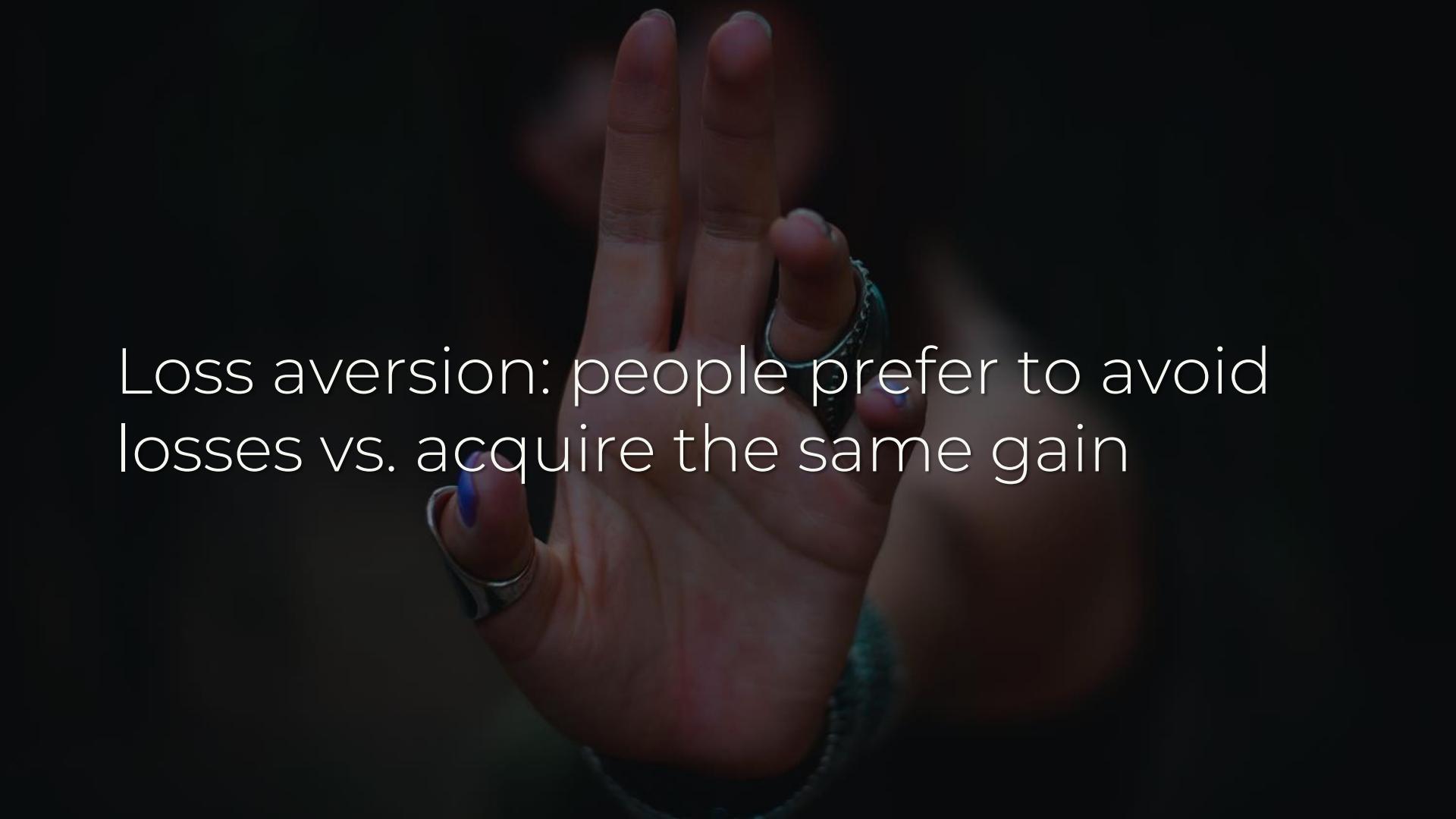
A close-up photograph of a person's hands holding an open map. A red dashed line is drawn across the map, likely representing a path or route. The map shows various geographical features like roads and terrain. The hands are visible at the top and bottom edges of the map.

Maintain a reference point against
which outcomes are measured



Overweight small probabilities &
underweight large probabilities

Overhyping low-probability vuln
exploitation vs. default passwords



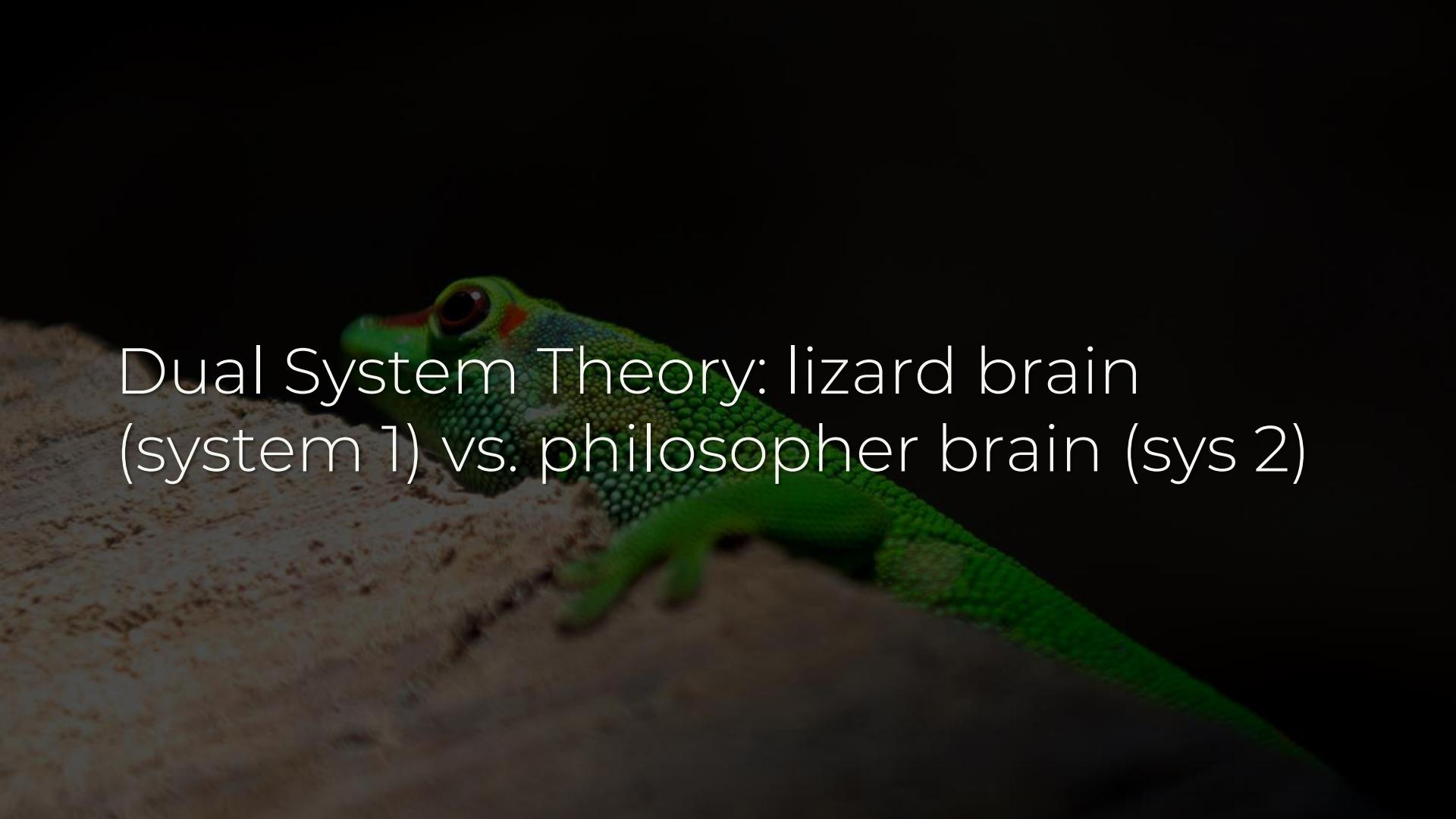
Loss aversion: people prefer to avoid losses vs. acquire the same gain

Framing security as a time & cost sink
facilitates natural resistance



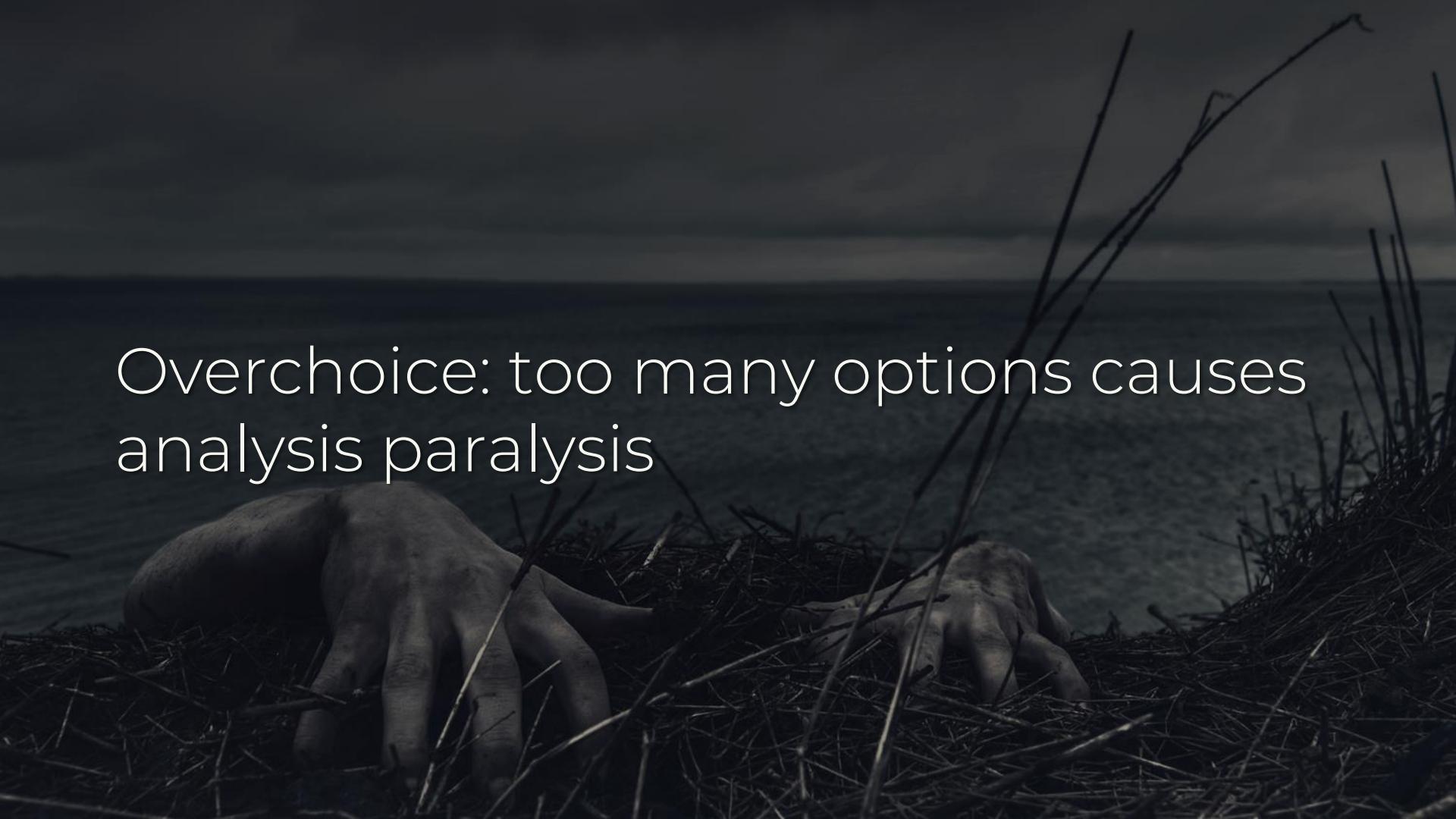
Hyperbolic discounting: future rewards are discounted vs. present

Many security initiatives are
“investments” with long-term benefits



Dual System Theory: lizard brain
(system 1) vs. philosopher brain (sys 2)

Most policies work on System 2 – we
need to work with System 1 instead

A dark, moody photograph of a person lying face down in tall grass, looking out over a body of water under a cloudy sky.

Overchoice: too many options causes analysis paralysis

Which of the 100 items do devs tackle
1st in a 10-page IoT attack surface doc?

We have to work with how people think, not against it

Behavior-based Design





What is choice architecture?

Design presentation of choices to promote improved decision-making

Example: MINDSPACE framework for behavioral design

A dark, atmospheric landscape featuring a rocky shoreline in the foreground. A small, clear glass bottle with a cork is nestled among the rocks. In the background, a body of water reflects a dark, hilly shoreline under a cloudy sky.

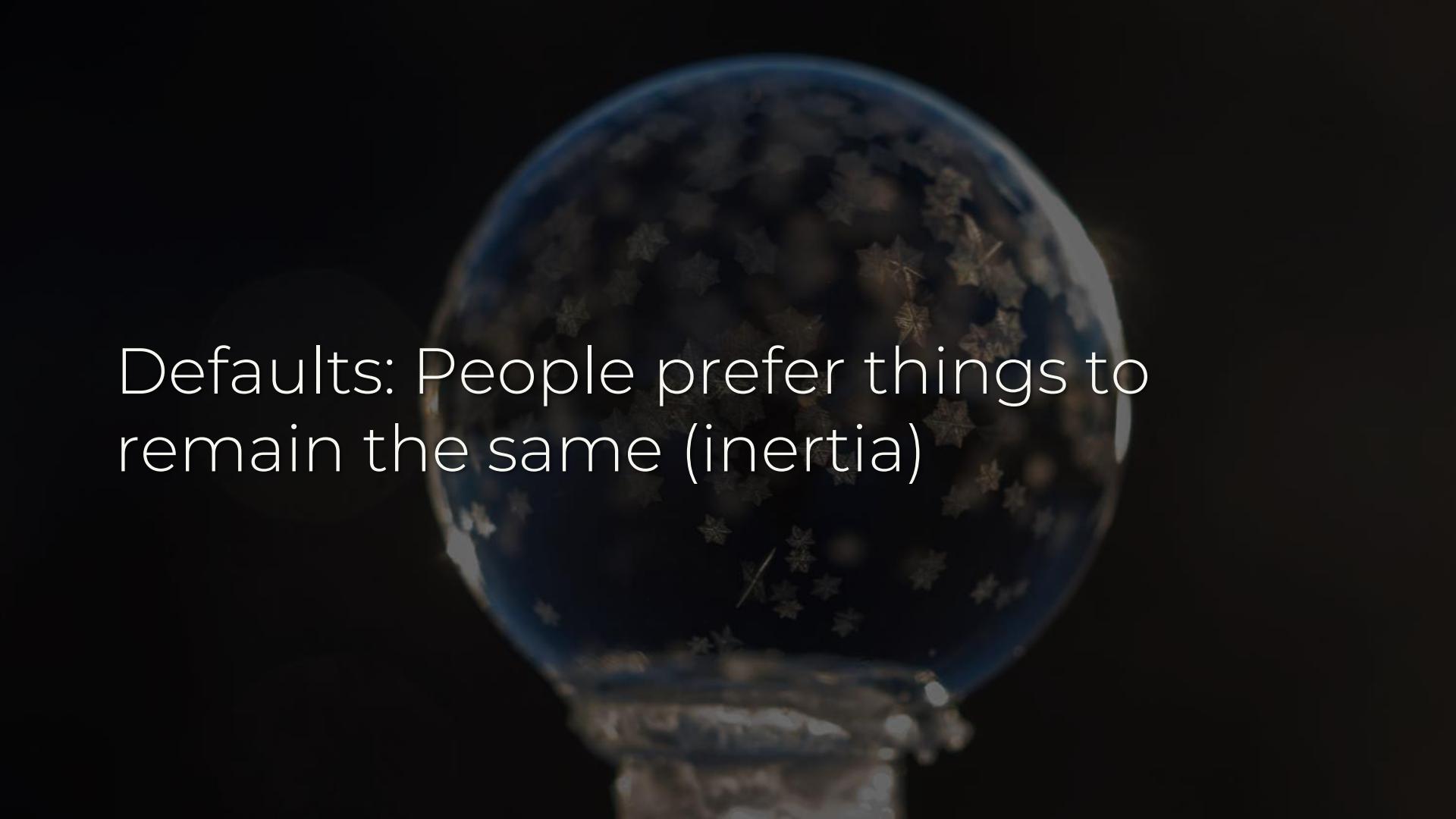
Messenger: people dismiss info from
sources they don't like / respect

A photograph of a person's hand reaching upwards against a dark background. The hand is positioned palm-up, fingers spread, reaching towards a bright, glowing light source at the top of the frame. The light creates a strong lens flare and illuminates the fingers and the back of the hand. The overall mood is one of aspiration, motivation, or reaching for something.

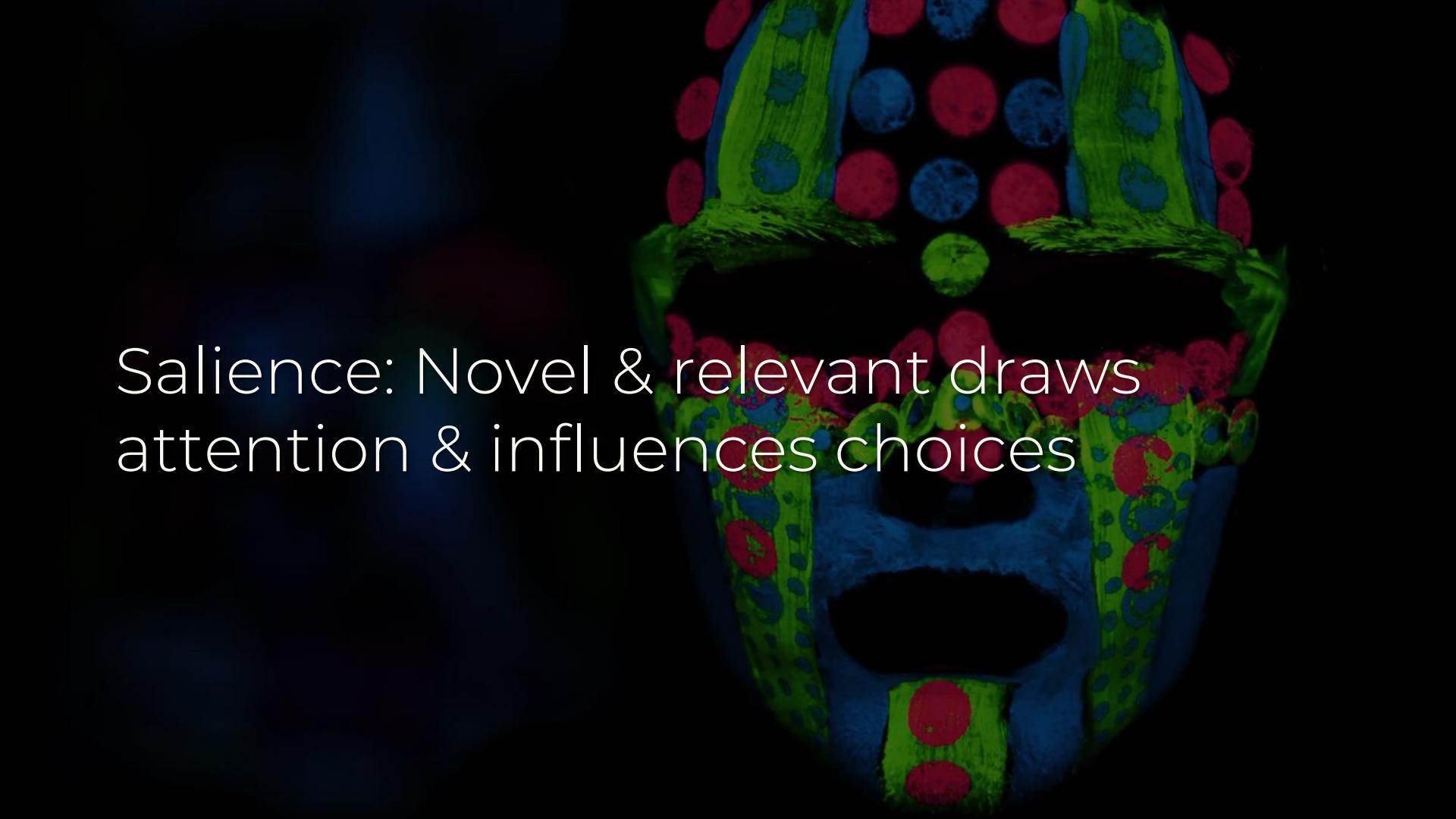
Incentives: losses can be more
motivating than rewards



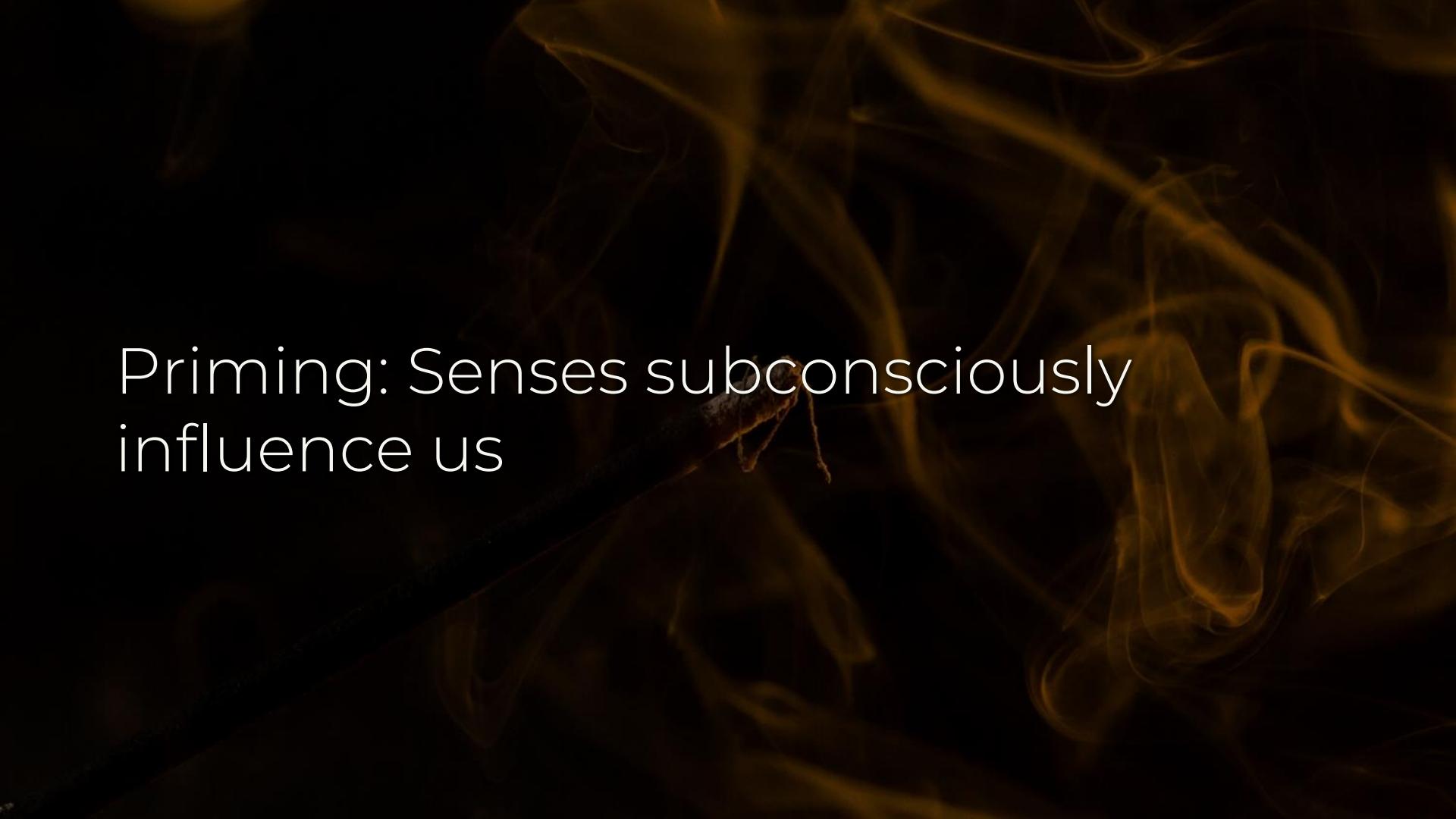
Norms: People follow social standards,
(even when counterproductive)



Defaults: People prefer things to remain the same (inertia)

A close-up, low-angle view of a face, possibly a mask or a painted portrait. The face is primarily black, with vibrant green and blue brushstrokes creating a textured, layered effect. Red circular patterns, resembling polka dots or eyes, are scattered across the surface. The lighting is dramatic, highlighting the contours and the interplay between the colors.

Salience: Novel & relevant draws
attention & influences choices

The background of the slide features a dark, moody atmosphere with wispy, glowing orange lines that resemble smoke or light rays. These lines are more concentrated on the right side of the frame, creating a sense of depth and movement.

Priming: Senses subconsciously
influence us



Affect: Emotional reactions are our brains' first responders

Commitments: Judgements made in advance to create “automatic” actions

A dark, moody photograph of a person from the chest up. They are holding a large, round magnifying glass in front of their face, centered on their eyes. The magnifying glass reflects some light, creating a bright spot in the center. The person's hands are visible, gripping the handle of the magnifying glass. The background is dark and indistinct.

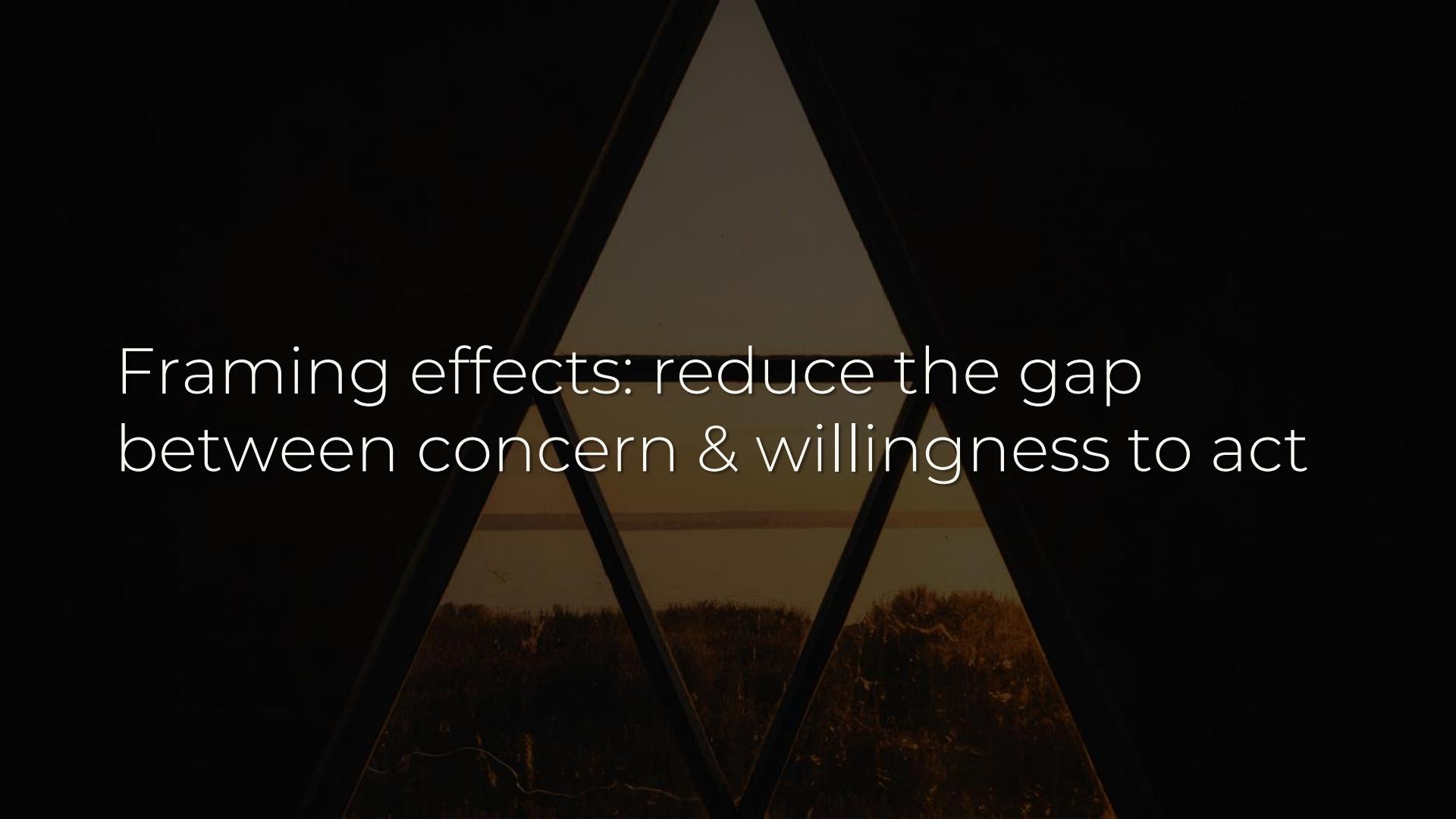
Ego: People like to feel better about themselves & preserve self-image

Reinforcement mechanisms:
consequences to guide behavior

Pay-for-performance lacks empirical evidence for fixing moral hazard

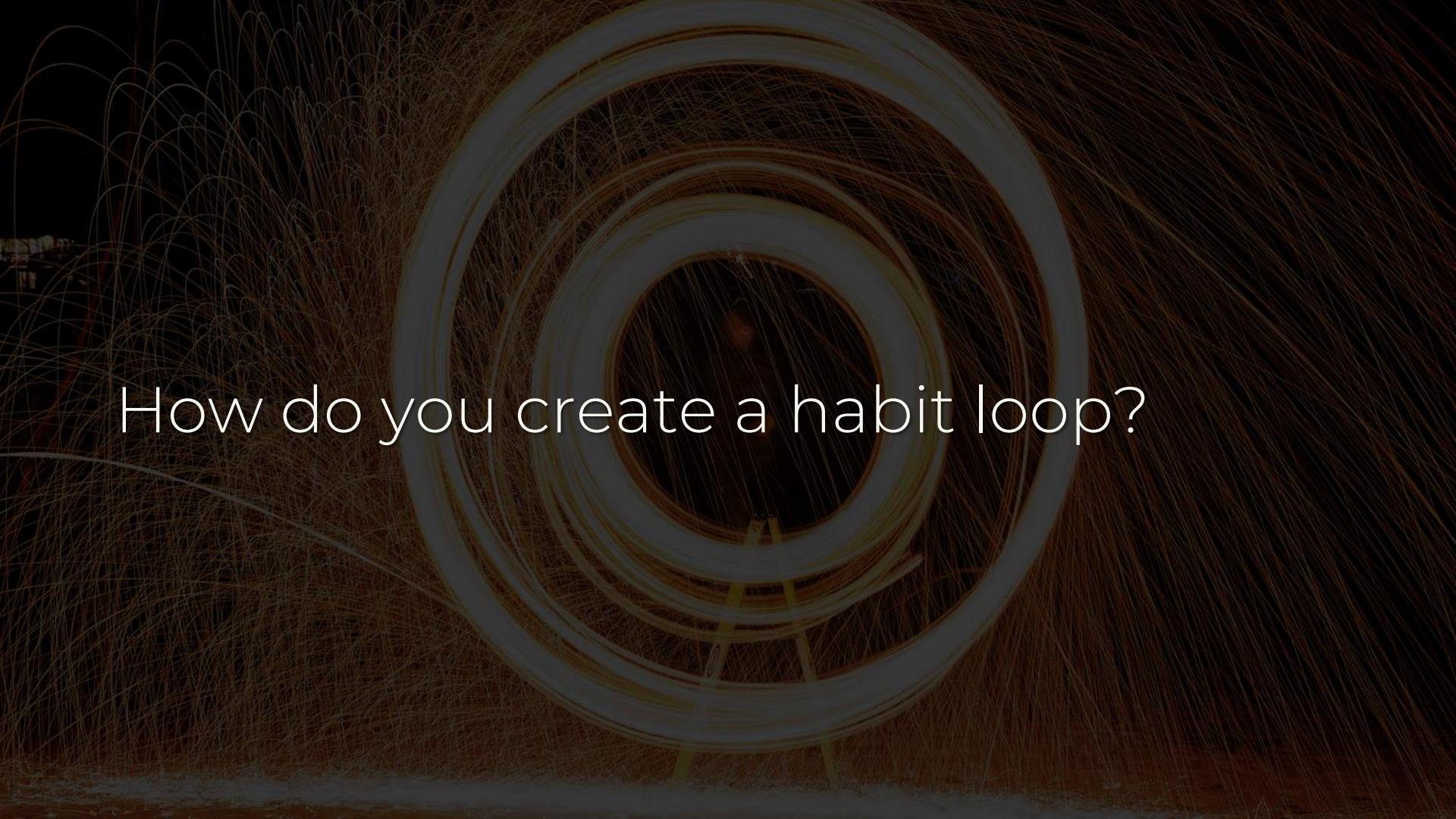
Set clear, achievable goals – “fix all the bugs” is neither

Goal setting must be matched with feedback, ideally immediate



Framing effects: reduce the gap
between concern & willingness to act

Focus on leveraging system 1 to your advantage by altering habits

The background of the slide features a circular track, likely a running track or velodrome, with several concentric lanes. The track is illuminated from above, casting a warm glow on the lanes. The surrounding area is dark, with tall, dry grass visible in the foreground and sides. The overall atmosphere is nighttime.

How do you create a habit loop?

A white ceramic cup filled with dark coffee is centered in the frame. The coffee has a rich, dark brown color with a thin layer of light-colored foam on top. The cup is positioned on a dark, textured surface, possibly a marble or stone counter. The lighting is dramatic, coming from the side to highlight the texture of the coffee and the rim of the cup.

Step 1: Routine

Make it stable, frictionless, & fit into
existing context

Minimize perceived effort & number
of decisions the user has to make



Step 2: Triggers & Rewards

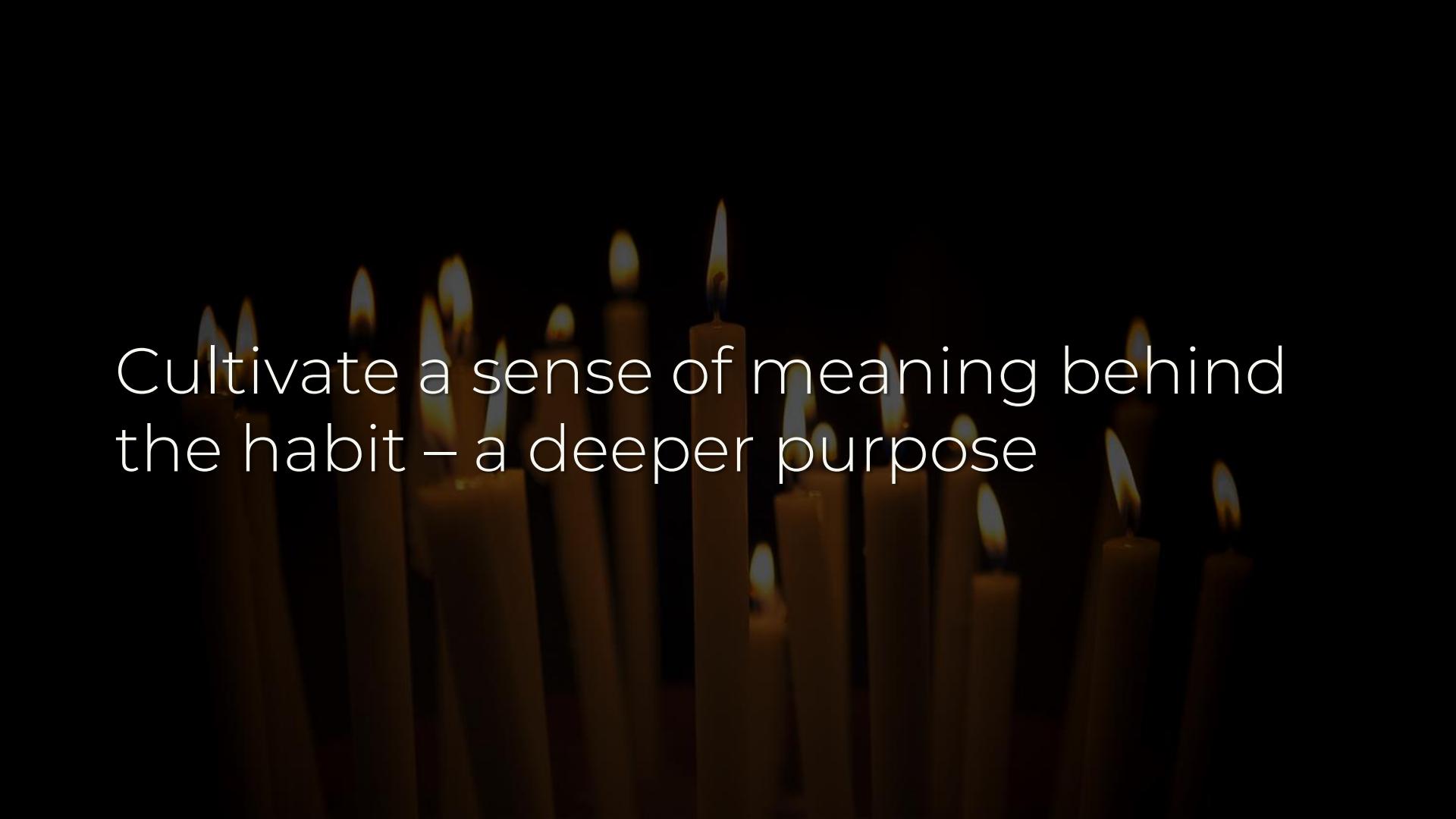
Contextual cues: “If X, do Y”

Magical brew of rewards: mix of short-term & accumulated long-term ones

A close-up photograph showing a person's hand gripping a dark, textured pestle. The pestle is positioned above a grey stone mortar. Inside the mortar, there is a small amount of a yellowish, granular substance, possibly a spice or herb. The background is dark and out of focus.

Step 3: Ingrain

Foster ample opportunities for
practice & interaction

The background of the slide is a dark, almost black, space. In the center, there are several lit candles. Their flames are bright yellow and orange, casting a warm glow. The candles are of various heights and are positioned in a way that creates a sense of depth and focus on the text in the foreground.

Cultivate a sense of meaning behind
the habit – a deeper purpose

People don't like feeling like habit machines; play into self-identity

A close-up photograph of a person's hand holding a small, clear plastic bottle with a yellow cap. The hand is pouring a dark liquid, likely oil, from the bottle into a greyish-green mortar. A dark grey pestle is resting inside the mortar. The background is dark and out of focus.

Ideas for IoT Sec

The background of the slide features a dramatic, dark sky filled with large, white, billowing cumulus clouds. The lighting is low, creating a somber and contemplative atmosphere.

Set concrete goals: “build-in security”
is too nebulous

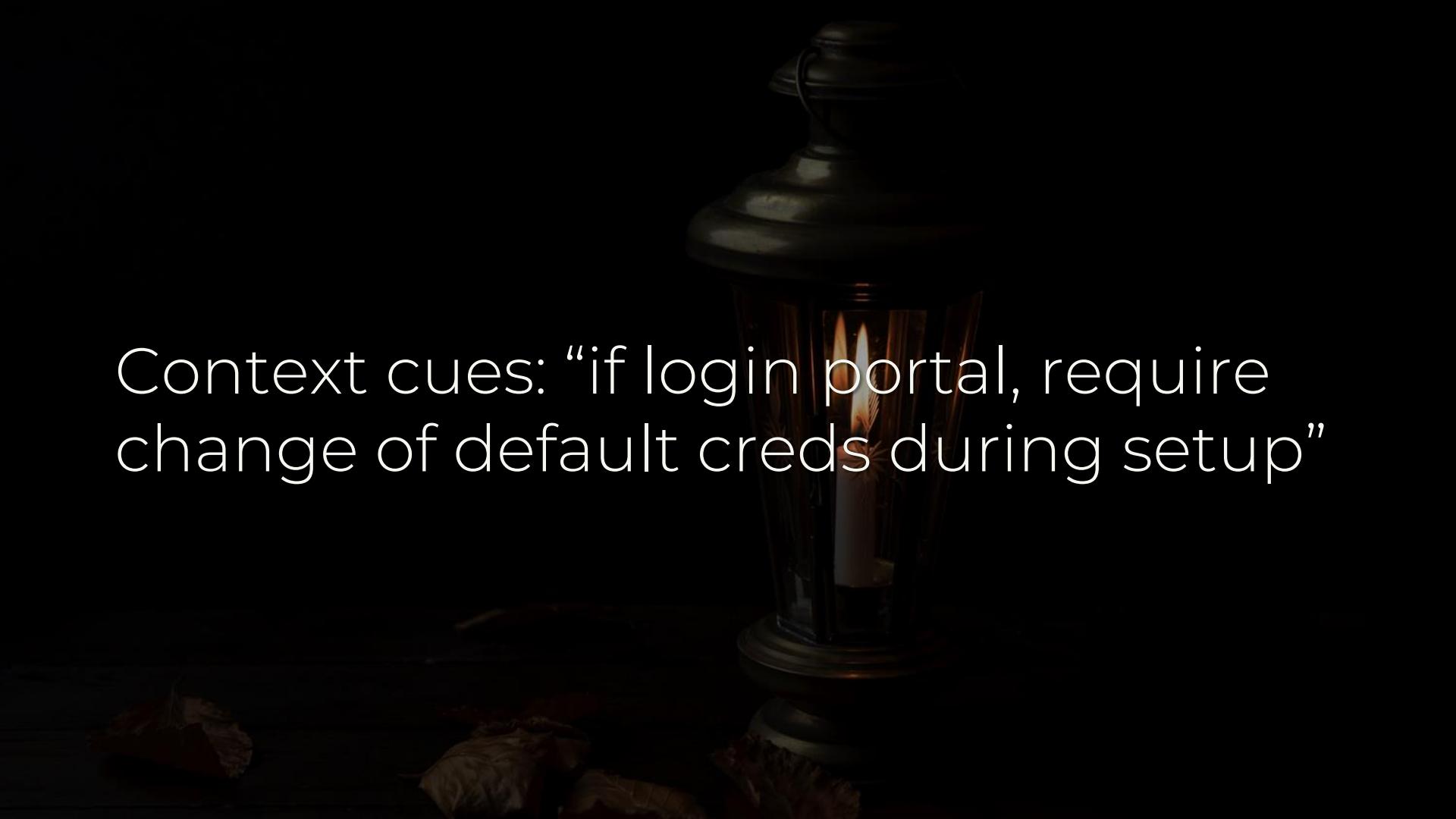
“Ensure each feature release uses a 10-point checklist” is a clear ask

Value should consider maximum security benefit at minimum cost

How to turn security into a habit?



Teams should have a regular, brief time & space to review security goals

A dark, atmospheric photograph featuring a single lit candle in a glass lantern. The lantern has a dark, textured top and sits on a dark, reflective surface. In front of the lantern, several dried, brownish-orange leaves are scattered. The candle's flame is bright and visible through the glass. The background is completely black, making the light from the candle stand out.

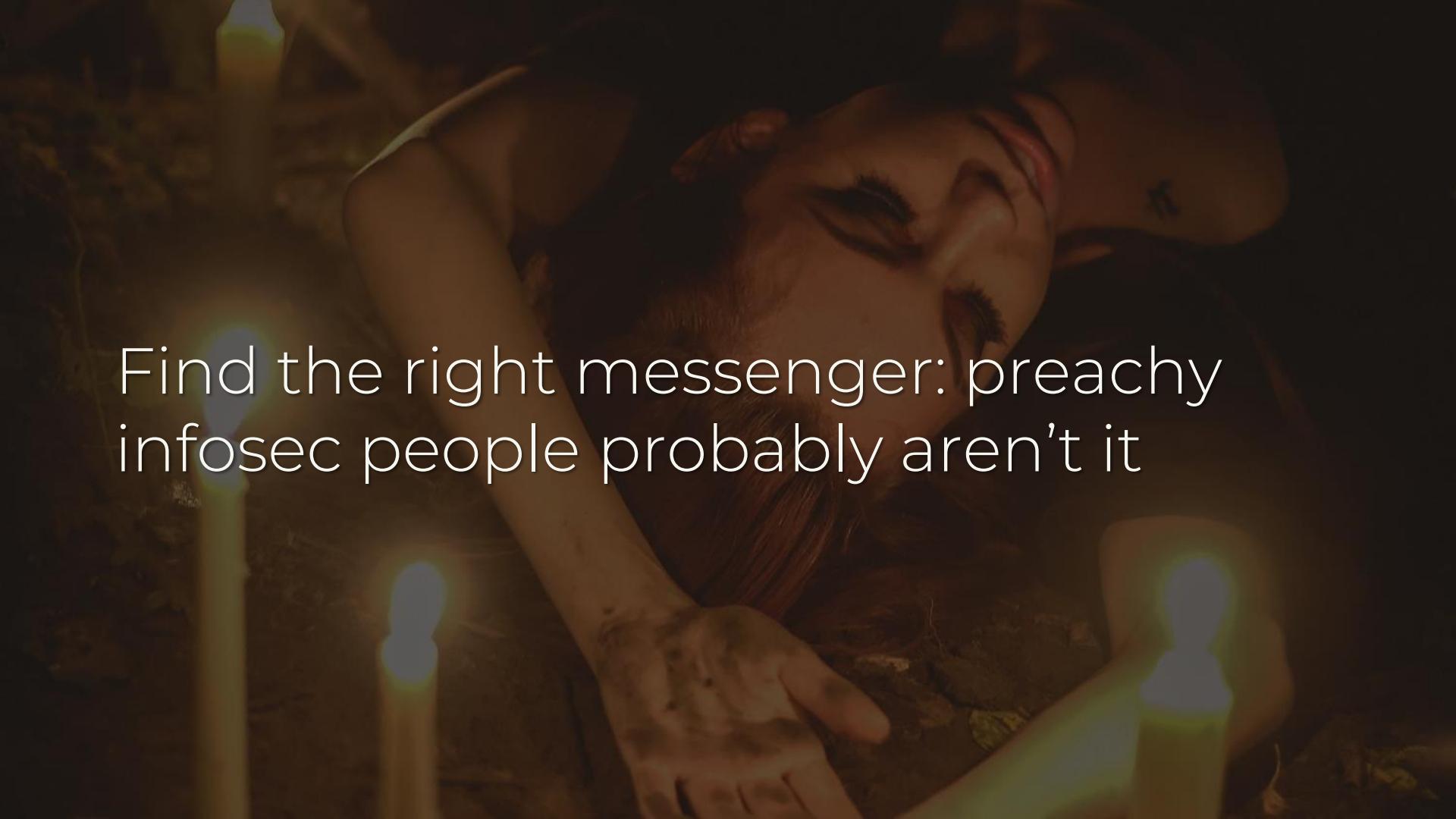
Context cues: “if login portal, require
change of default creds during setup”

Specify attainable steps with minimal complexity, like a checklist

Security suitably serves as a deeper purpose – frame it as a noble cause

A hand reaches towards a glowing plasma sphere, symbolizing interaction with complex, dynamic systems.

How can we leverage MINDSPACE for
IoT security?

A dark, moody photograph of a person wearing a mask and a tattooed arm, holding a small animal. The scene is set against a dark background with some glowing elements.

Find the right messenger: preachy
infosec people probably aren't it

“Gift” budget that is eroded if security goals aren’t met (loss aversion)

A close-up photograph of a large cluster of monarch butterflies (Danaus plexippus) roosting on a dark, textured surface, likely a tree branch. The butterflies are densely packed, their wings showing the characteristic orange color with black veins and white spots. The lighting is low, creating a moody, almost abstract effect.

Treat security habits as norms: “90% of our developers fix bugs within 3 days”

Show long-term expenses of options
to highlight ROI of proactive security



Transparency around quality & cost:
easiest measures with highest impact

Control instincts to security issues –
slow down via threat modelling

A close-up photograph of a person's hands holding several shiny gold coins. The coins are stacked in a loose pile, with one prominent coin showing intricate patterns on its reverse side. The background is dark and out of focus.

Team bonus if you complete the
checklist & fix bugs within 30 days – if
not, it goes to charity

Black Girls Code, Calyx Institute, IFF
Diversity & Inclusion Fund, Mozilla
Foundation, Signal Foundation

Public lists of IoT vendors allowing
default cred changes (like the Two
Factor Auth List)



One-page checklist to ensure &
document IoT security basics



Streamlined number of steps per lifecycle stage – design, build, test

1. Design UX workflow to change
default passwords (everywhere)

2. Spoof headers to look like most common web servers

3. Encrypt data in transit with SSL or
TLS

4. Don't call bash scripts from the web interface

5. Don't use custom API protocols –
just use REST or SOAP

Design

- Does the device use:
 - A login portal?
 - Yes, and we allow the change of default creds
 - No
 - User Data
 - Yes, & we encrypt data w/ SSL or TLS
 - No
 - Web Interface
 - Yes, and we do not call bash scripts or use custom API protocols
 - No

If internet-connected, spoof headers to appear “normal”

Cross-checking by teams of critical measures to be taken

Build

- Share essential information concerning security steps with the team
- Confirm each team member understands the security requirements
- Have any new features been added since design that require review? (ie interfacing w/ the internet, collecting user data)
- Anticipated Security Events
 - What are the critical or non-routine security controls required?
 - How long will implementation of controls take?
 - What are the anticipated impacts of the controls?

Test

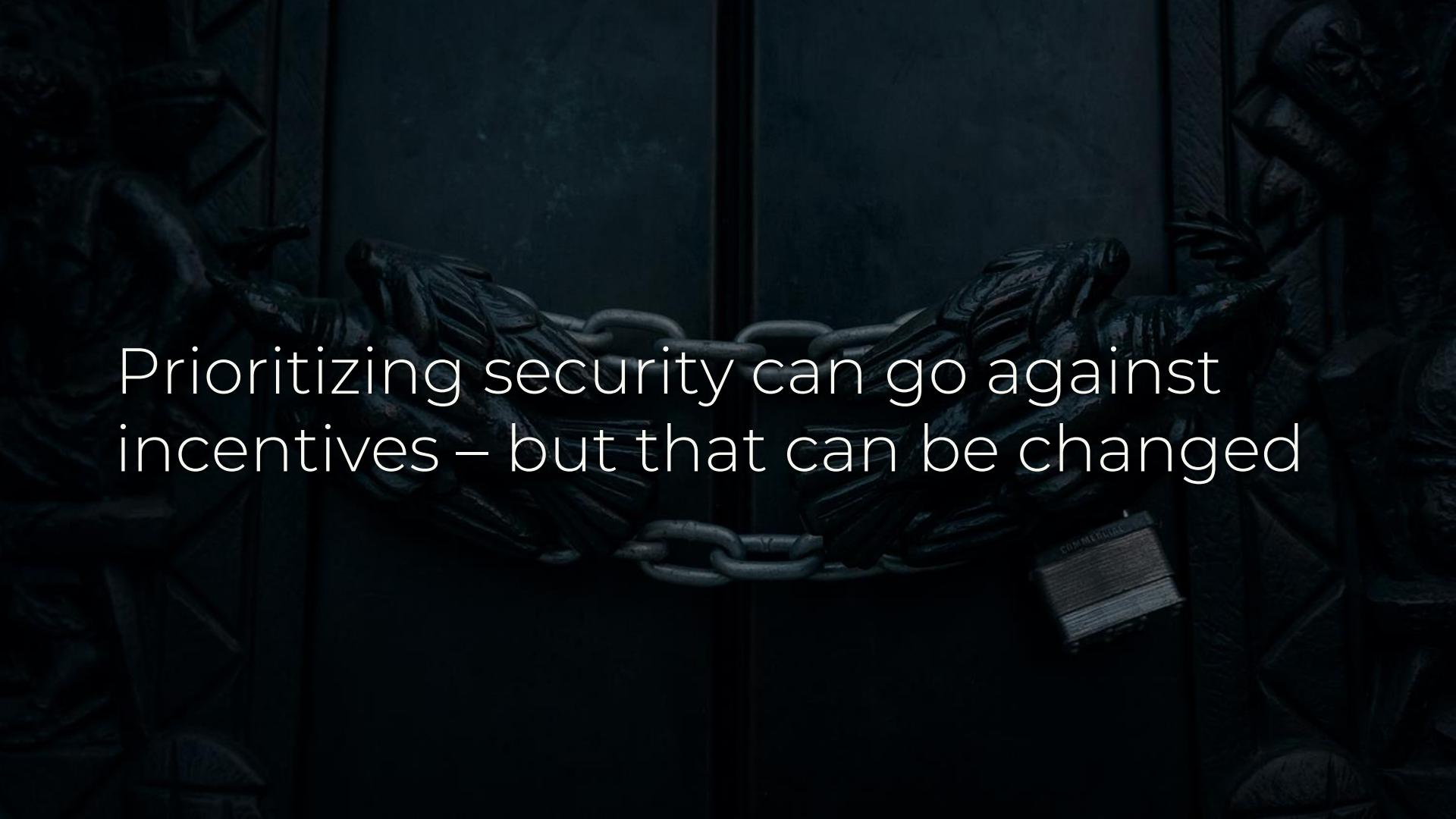
- Tester to confirm:
 - Completion of account controls (default credential alerts, lockouts, 2FA)
 - List of data used by the device, and labelling of user data
 - Whether there are any vulnerabilities to be addressed
- For builders:
 - What are the key concerns around management going forward and any future security concerns?
 - Instructions for immediate post-testing security management are drawn up together

Conclusion



A dark hourglass sits on a pile of sand, symbolizing time constraints.

IoT security ideas must treat devs as
time-constrained humans

A dark, atmospheric background. In the center, a thick metal chain is draped across the frame. To the right of the chain, a stack of papers or files is visible, with the word "CONFIDENTIAL" printed in capital letters on the top document. The lighting is low, creating deep shadows and highlighting the metallic texture of the chain and the paper.

Prioritizing security can go against
incentives – but that can be changed



Our complex, “endgame-level”
solutions are too formidable

A close-up photograph of a person's hand holding a teal-colored pillar candle. The candle is lit, with a thin wick visible and a small amount of smoke or steam rising from the base. The background is dark, making the teal color of the candle stand out.

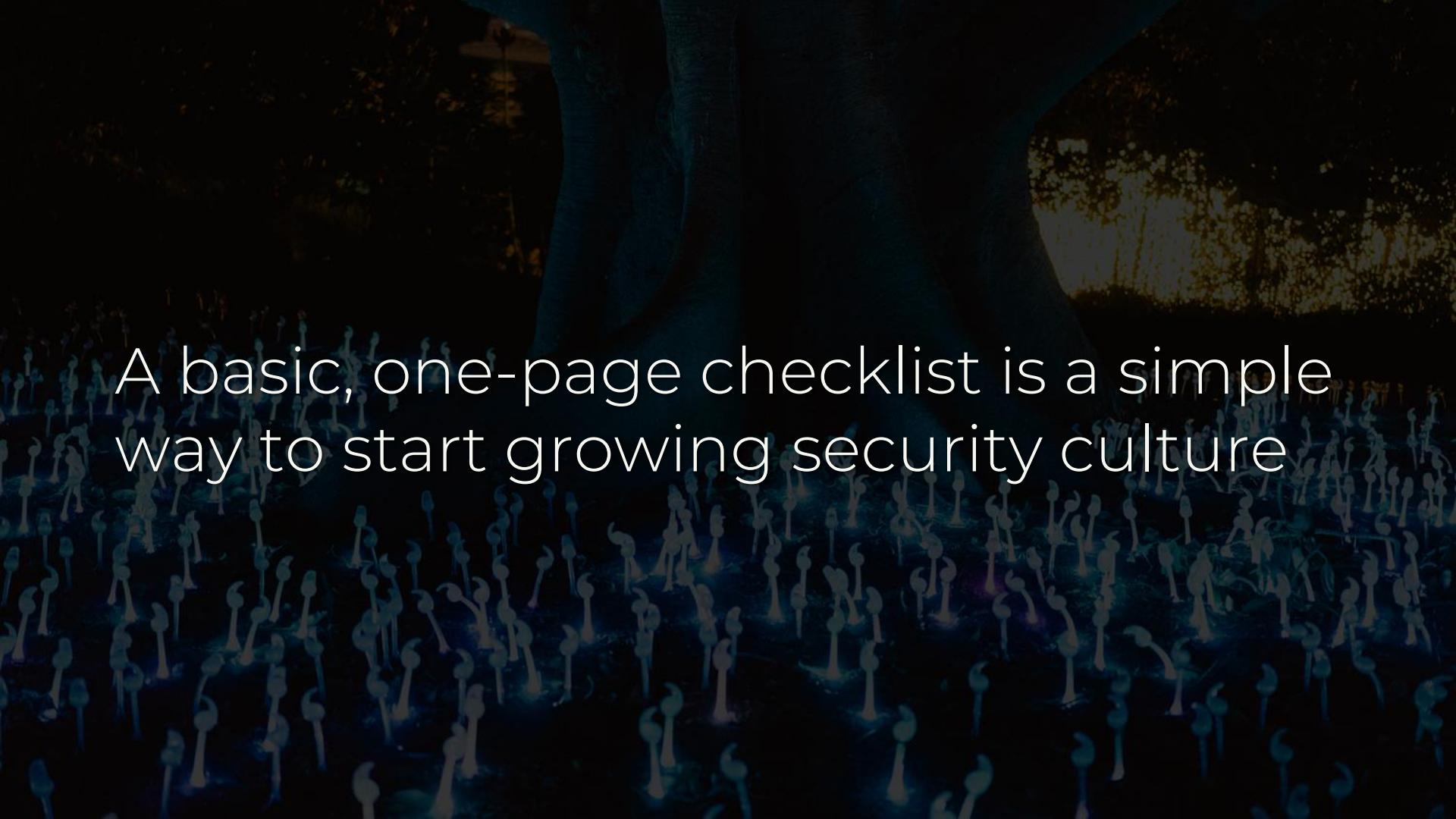
Compensating controls aren't enough
– we can't expect magic post-hoc



But practical magic using behavioral
design can improve decision making

A photograph of a traditional Japanese garden path. The path is paved with dark stones and leads through a series of red torii gates. A small, traditional lantern hangs from one of the gates. The scene is dimly lit, suggesting it might be dusk or dawn.

Goal: straightforward ways to erode
risky habits & promote security habits



A basic, one-page checklist is a simple way to start growing security culture



We cannot wallow in sermonizing –
we can't let the problem devour us

A close-up, low-angle shot of a dark blue globe. Gold-colored latitude and longitude lines are visible, creating a grid pattern. The globe is set against a dark, textured background.

“Good enough is good enough. Good enough always beats perfect.”

– Dan Geer

Suggested reading

- “Approaches based on behavioral economics could help nudge patients and providers toward lower health spending growth,” A. Darzi, F. Greaves, D. King, I. Vlaev
- “Behavior-based Safety Guide,” Ireland Health & Safety Authority
- “Farmer Behaviour, Agricultural Management and Climate Change,” OECD
- “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices,” FDA
- “Influencing behaviour: The mindscape way,” P. Dolan, et al.
- “Postmarket Management of Cybersecurity in Medical Devices,” FDA
- “A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population,” Alex B. Haynes, et al.
- “The Theory of Value-Based Payment Incentives and Their Application to Health Care,” Conrad DA



@swagitda_



/in/kellyshortridge



kelly@greywire.net