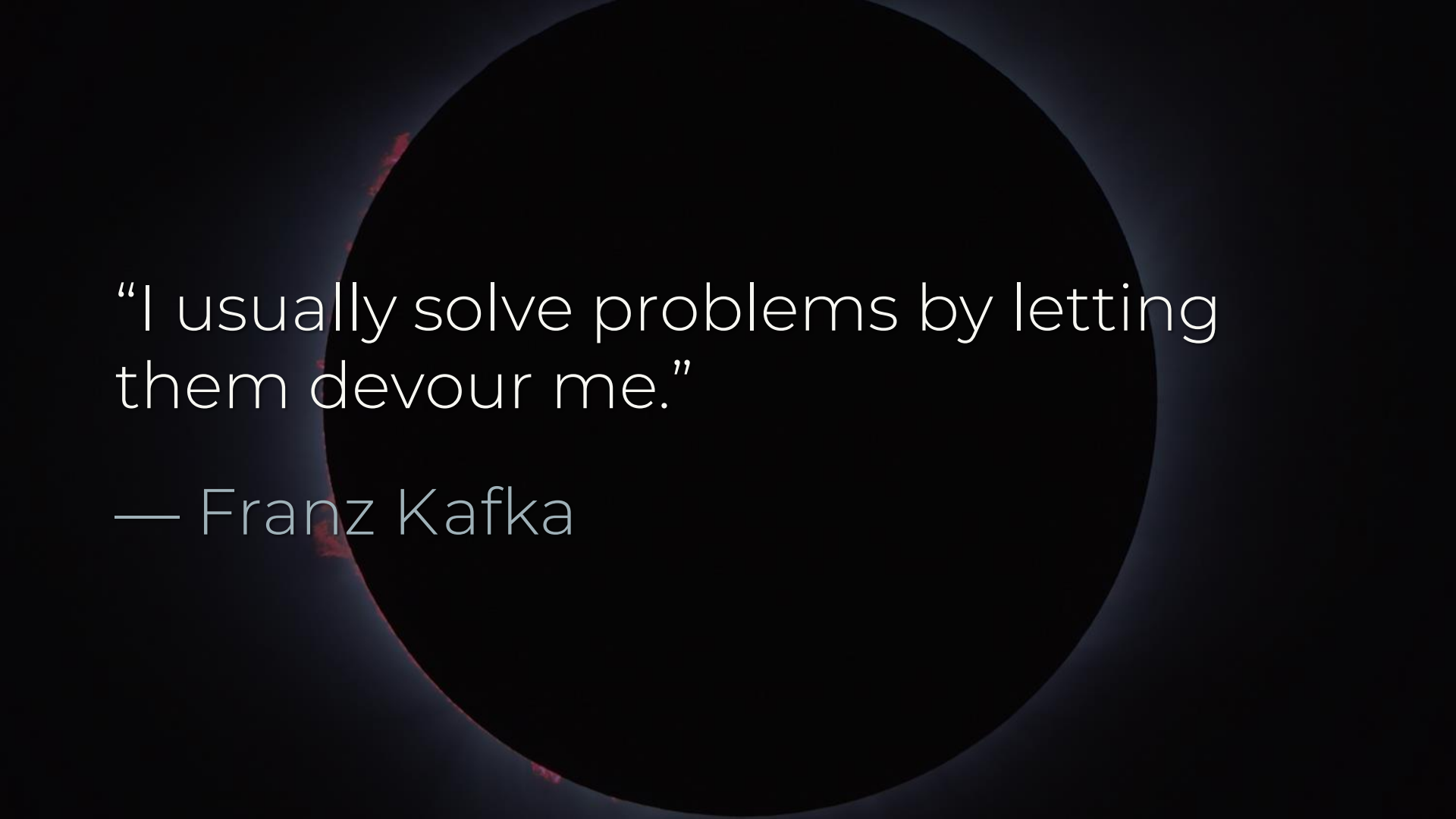
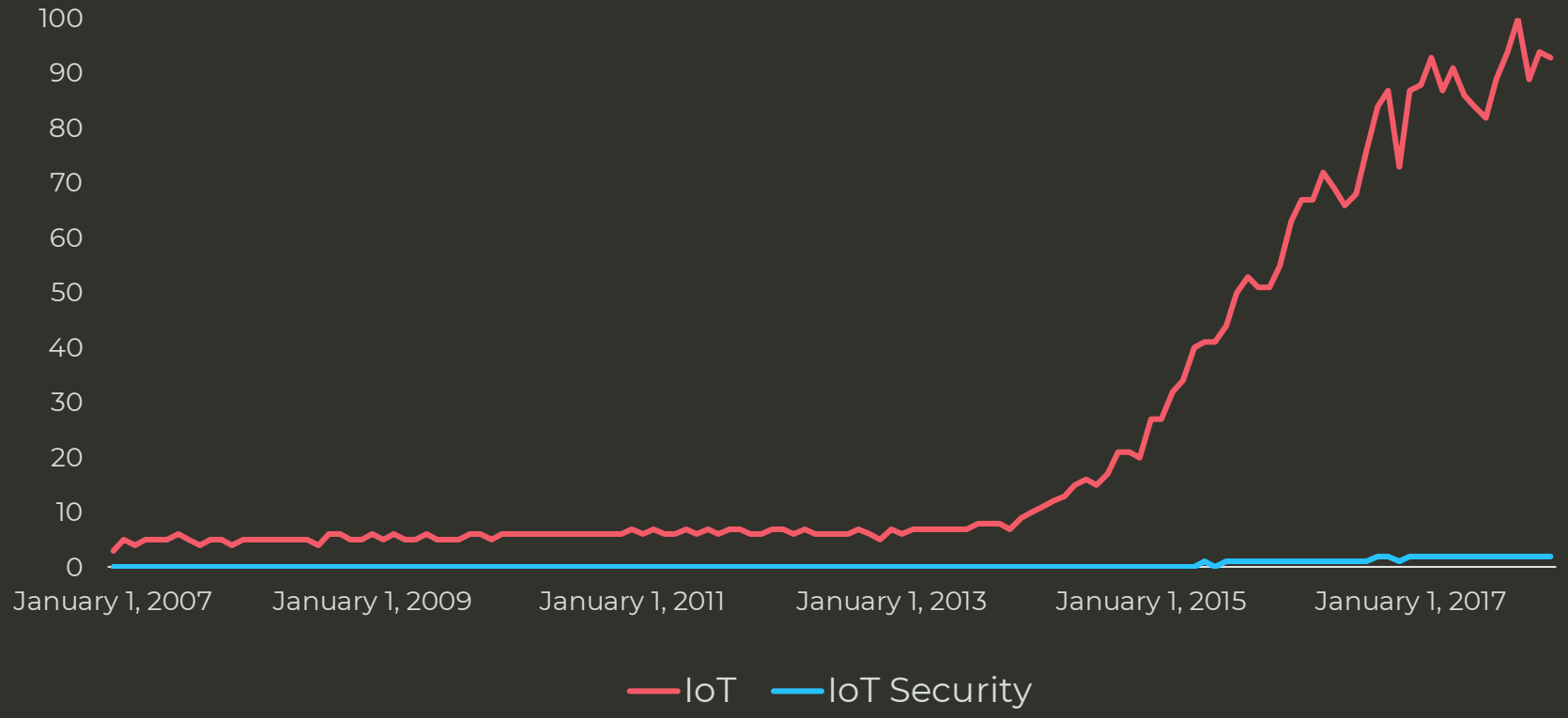
# Practical Magic: Behavior-based Safety Design for IoT

Kelly Shortridge (@swagitda_)

Troopers 2018

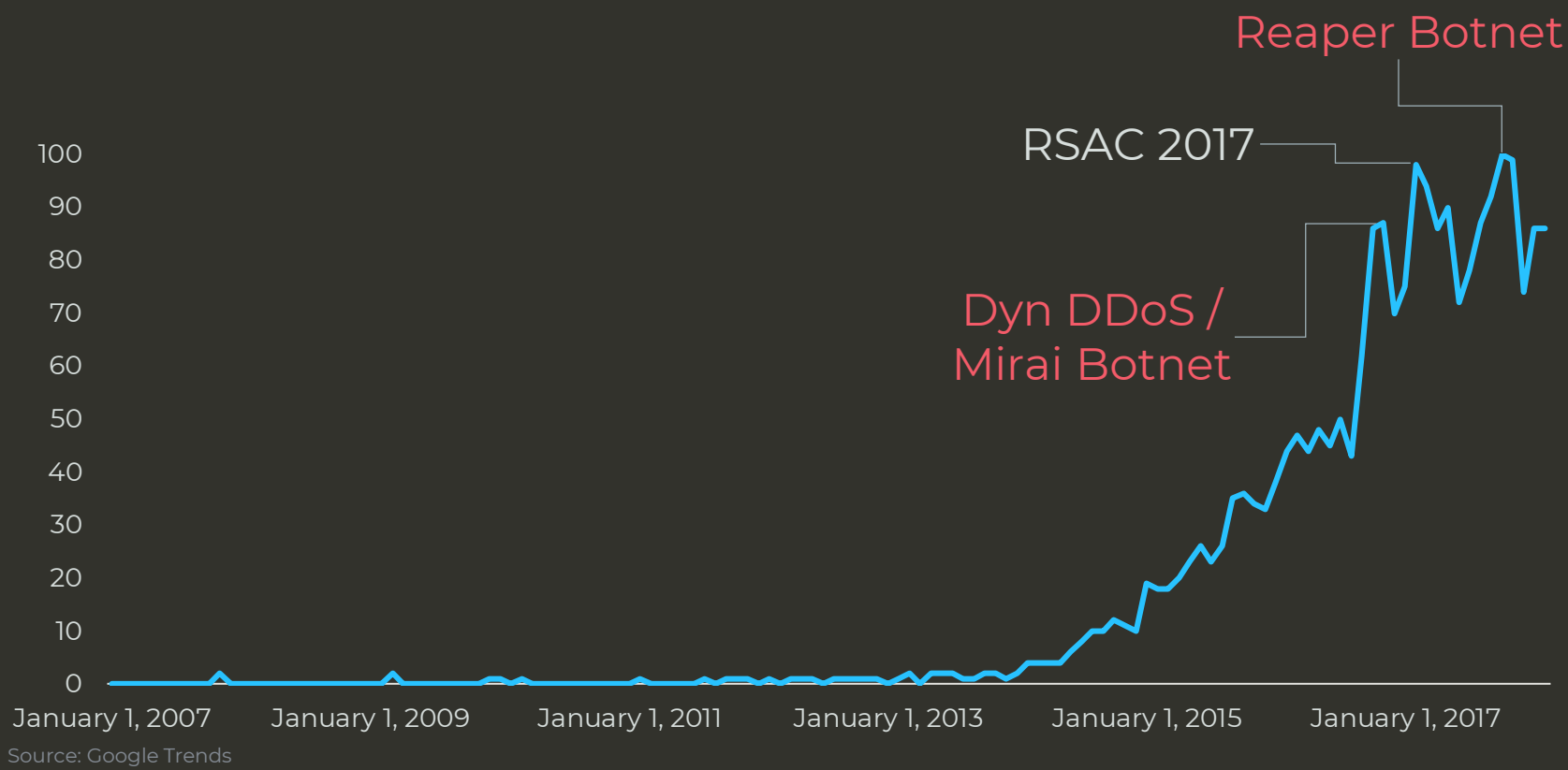

Hi, I'm Kelly
SecurityScorecard


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



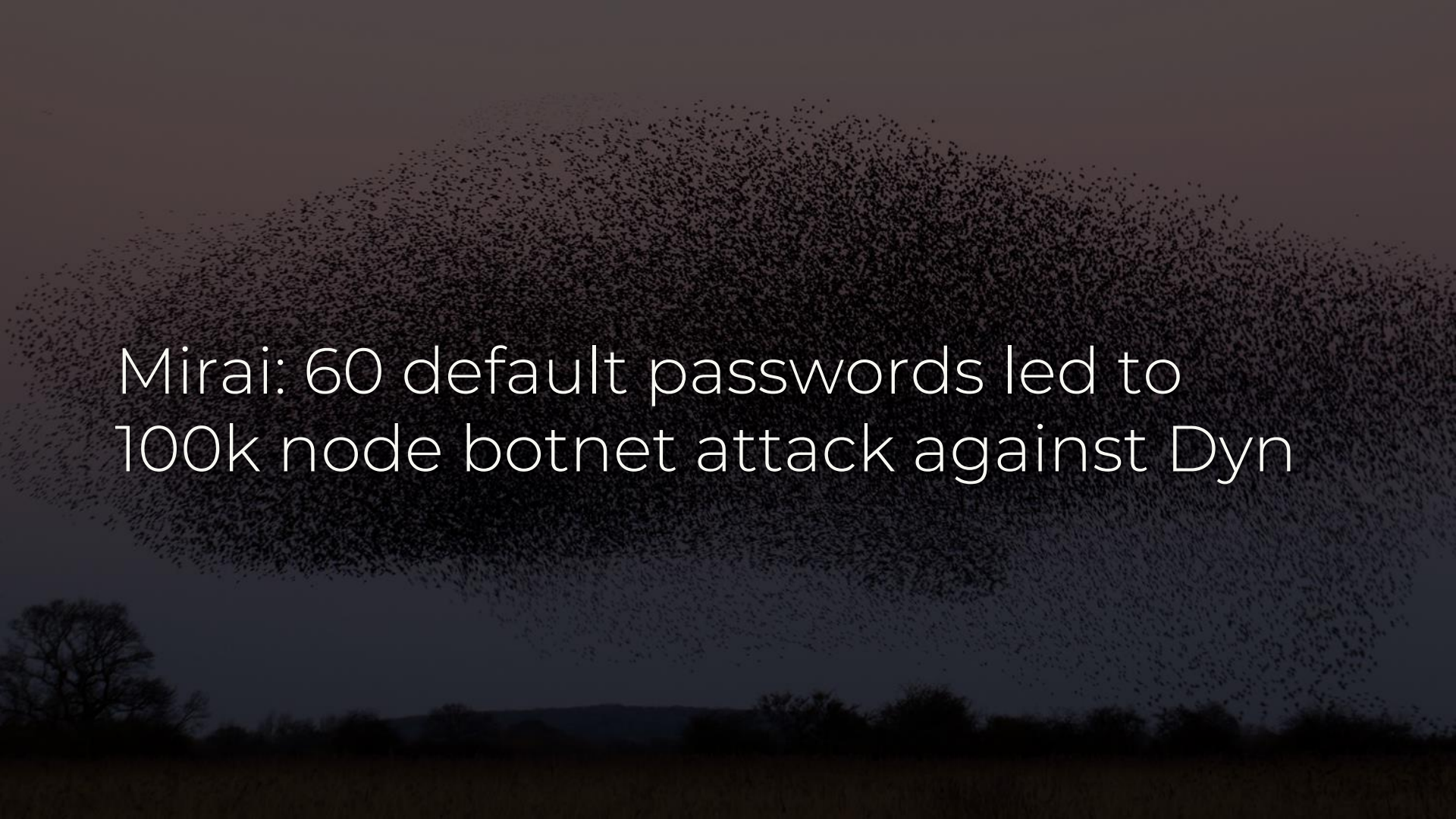

Source: Google Trends


We’re engendering a Kafkaesque paradigm for IoT security

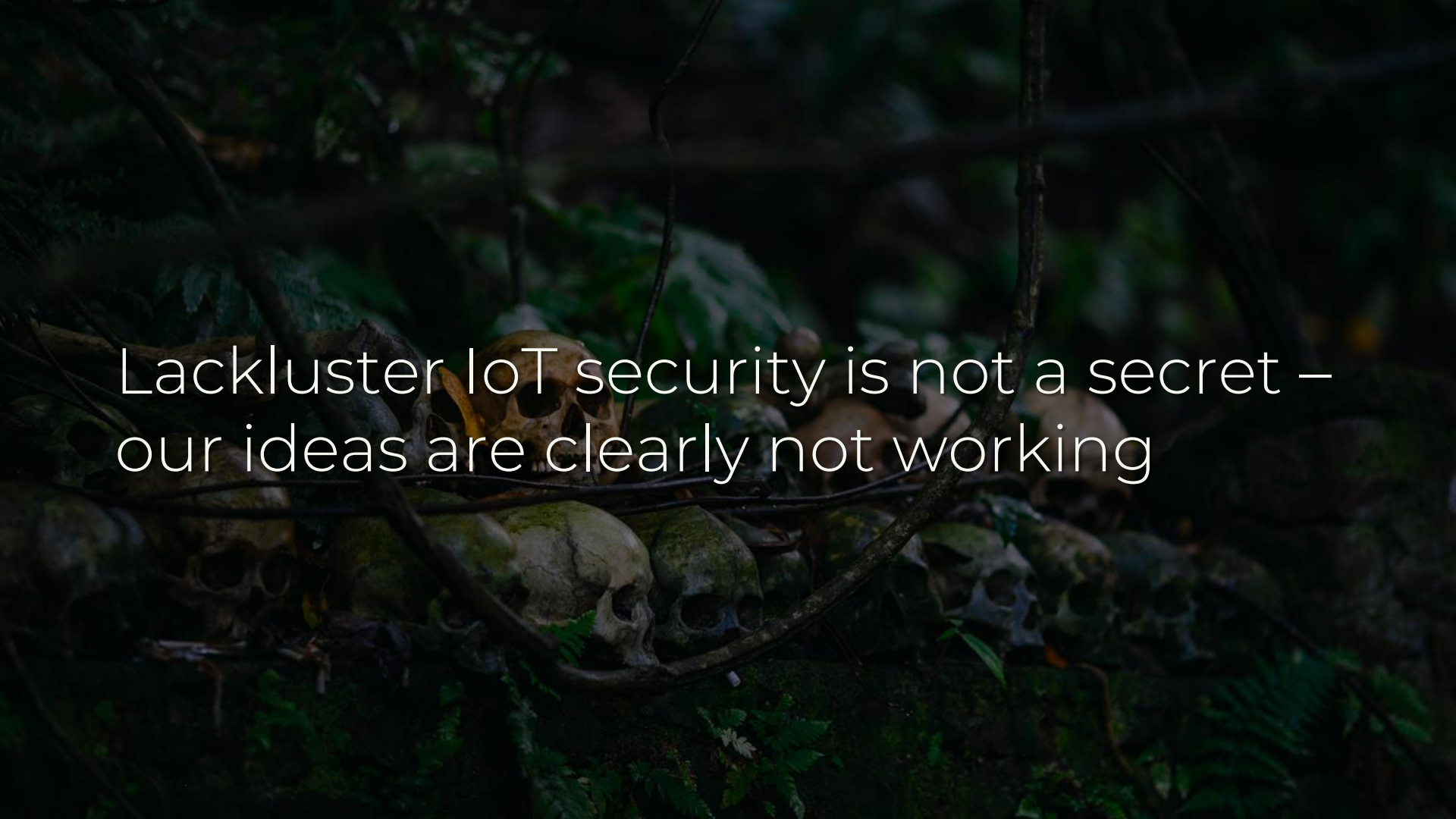



Source: Google Trends


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


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


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!)

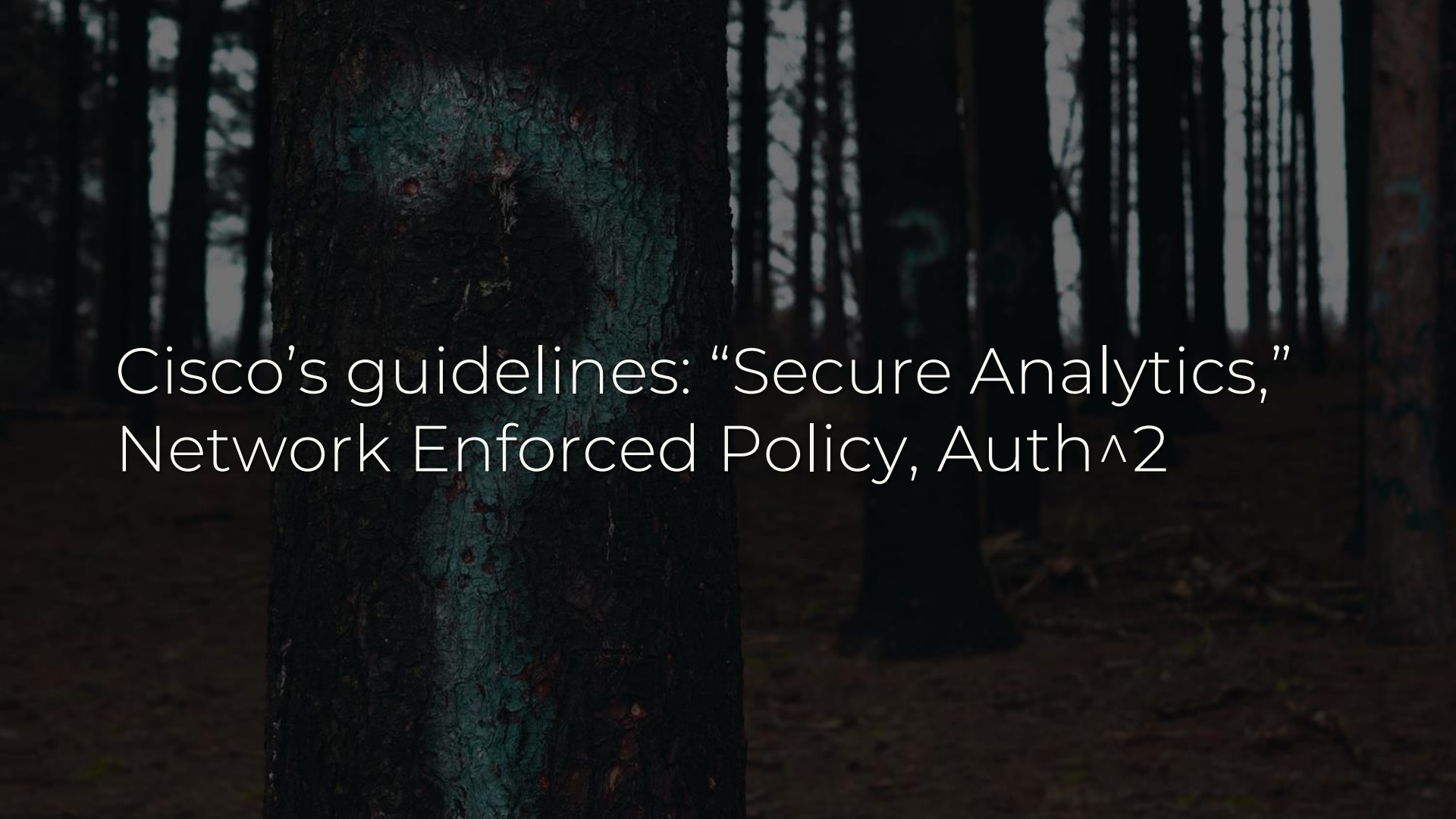
# FDA: Pre- & Post-Market Guidelines (H/T @marasawr)


Pre-market: a lot of documentation &
threat modelling

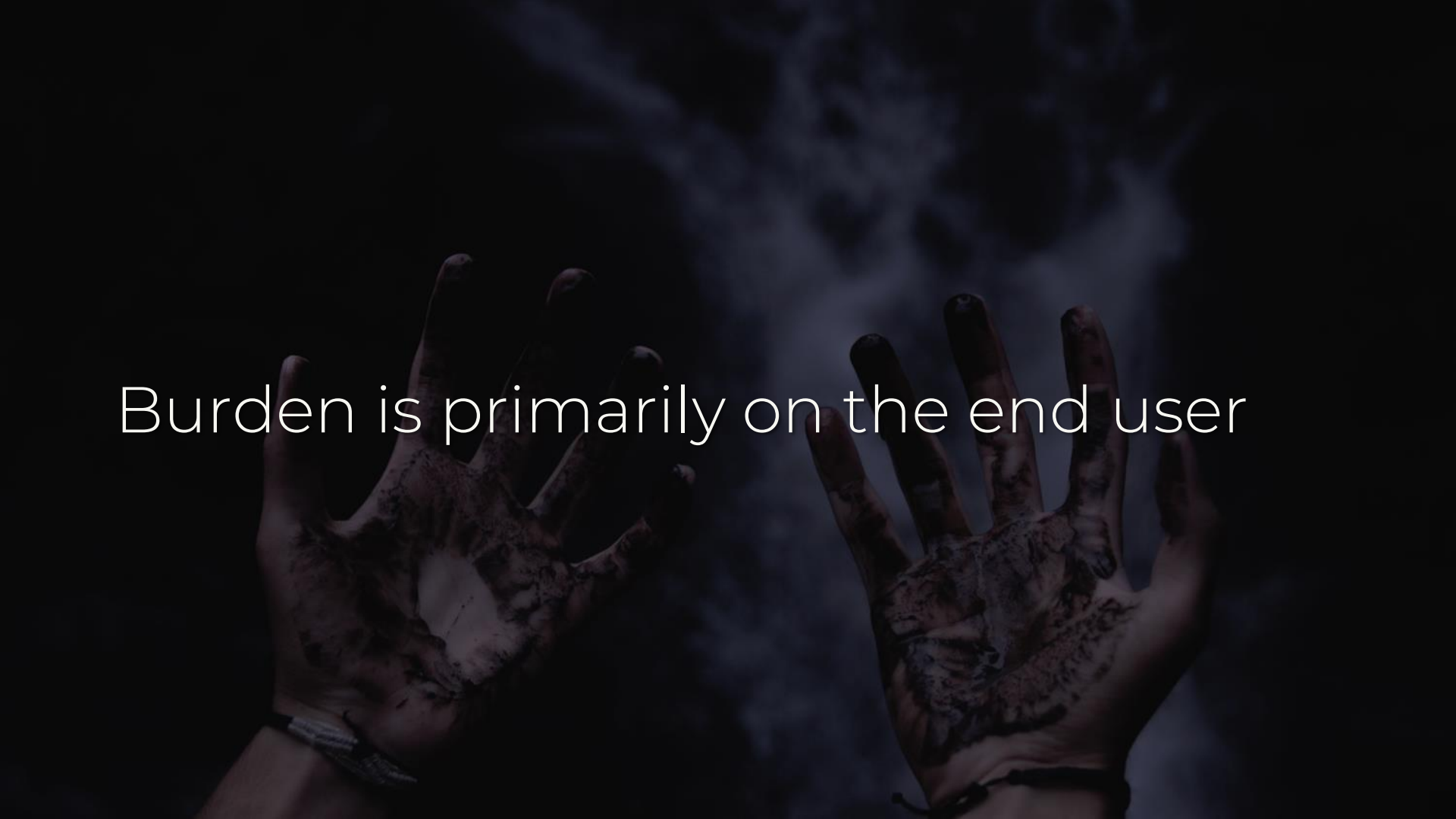
# Post-market: monitoring & a mitigation deployment strategy

# 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

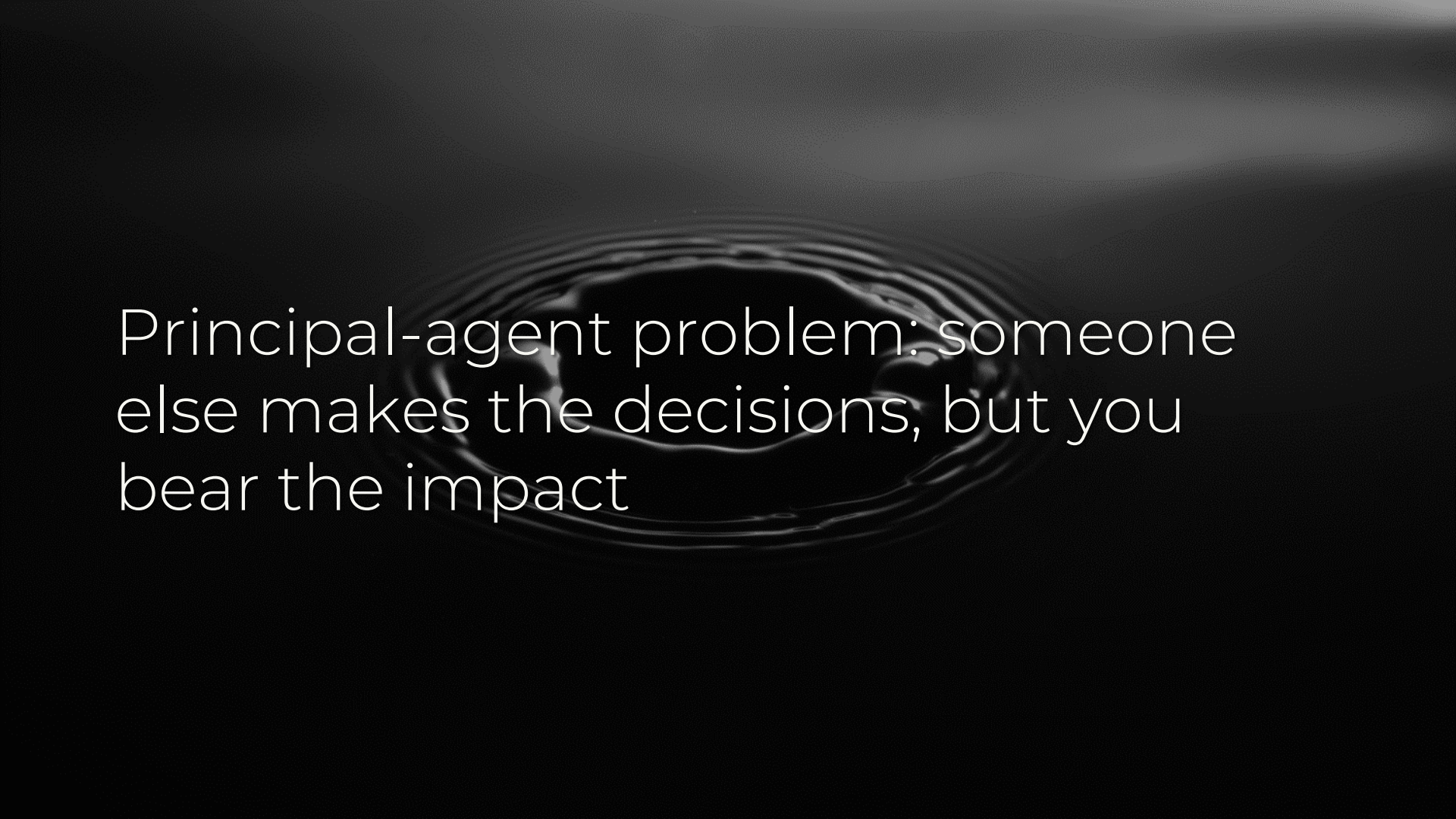
# Compensating Controls: post-market remedies by third parties


Burden is primarily on the end user


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

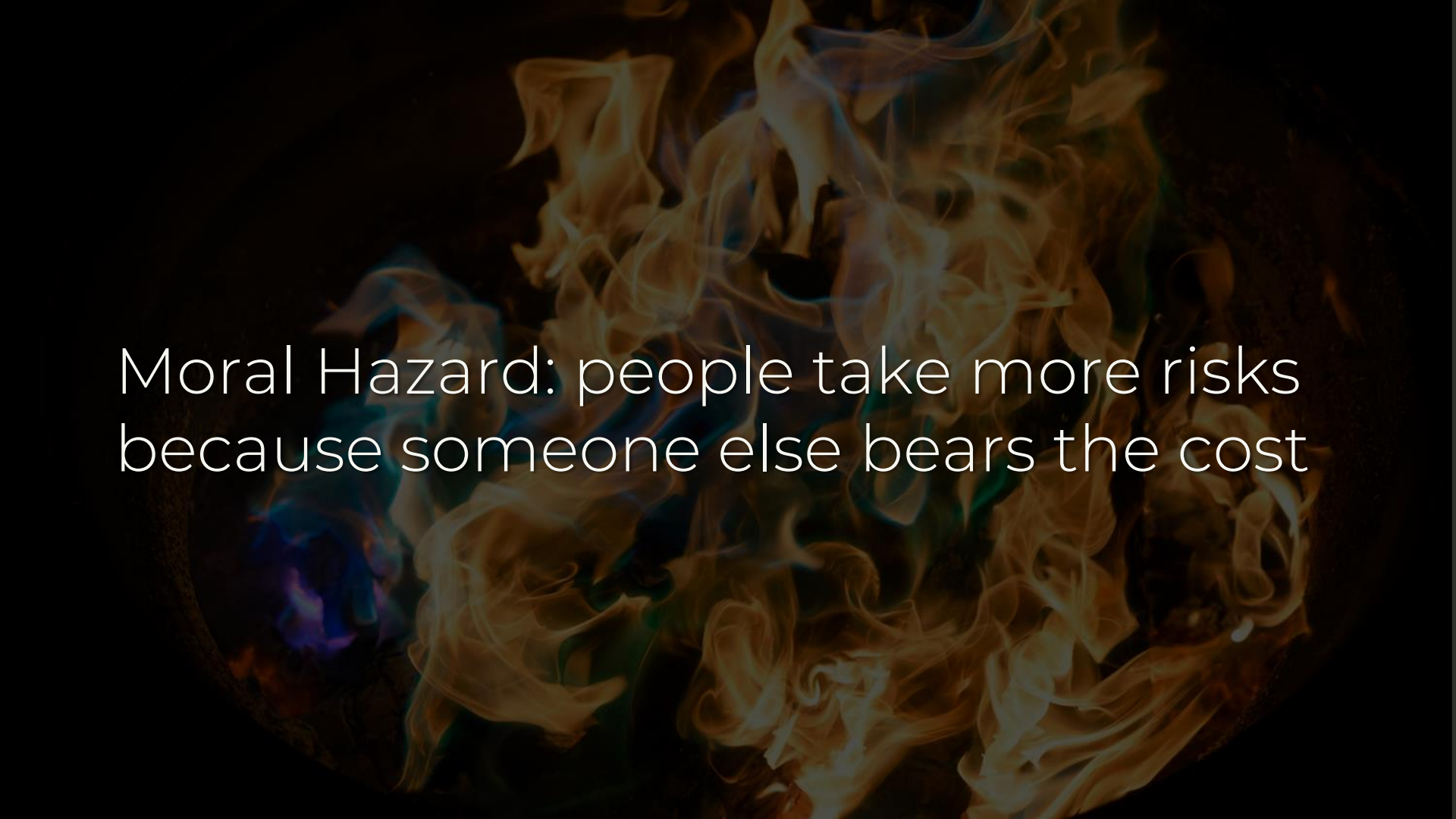
Maybe feasible for enterprises, but what are consumers to do?


# Incentive Problems


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

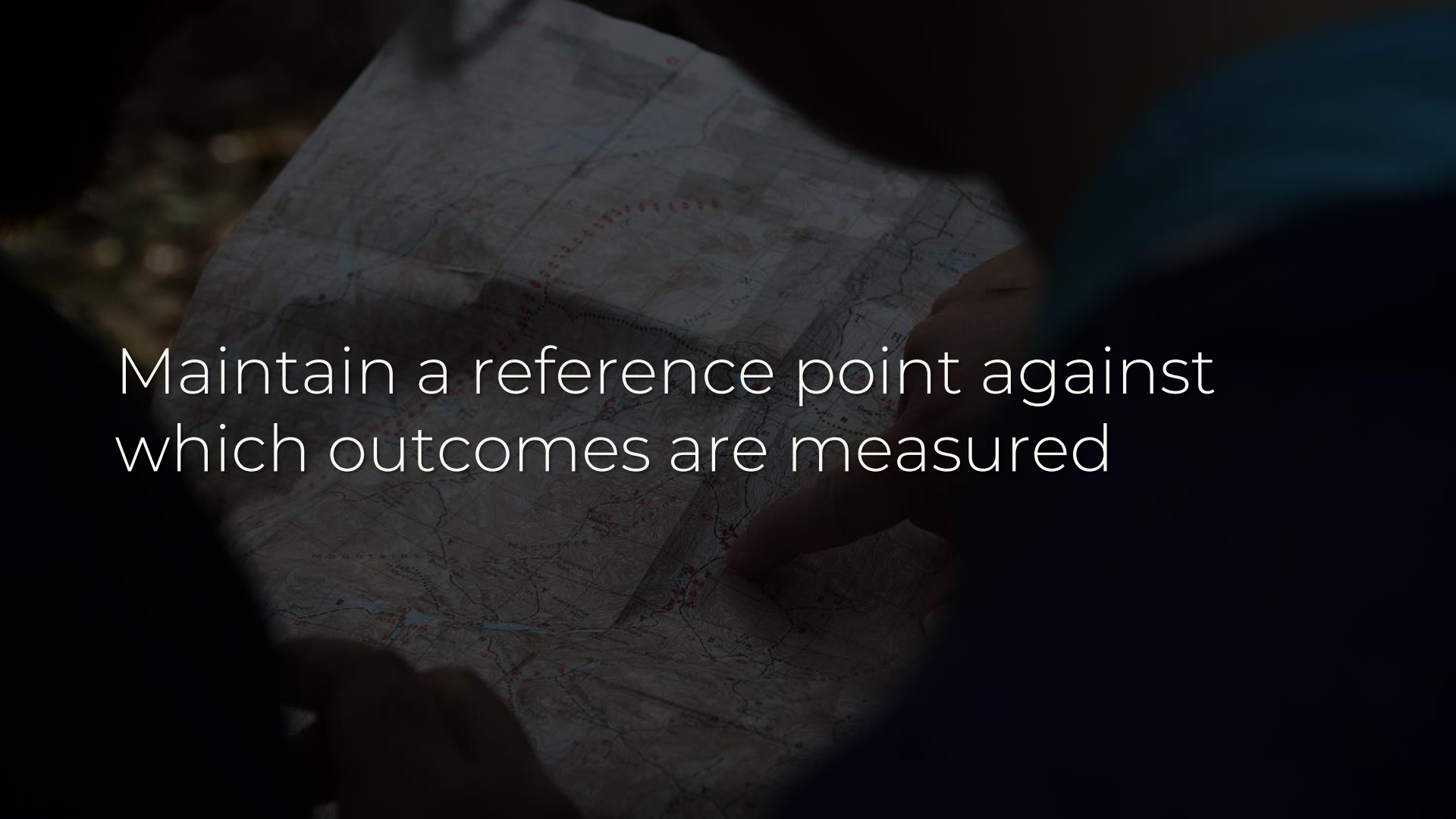
The Agent has their own self-interest.

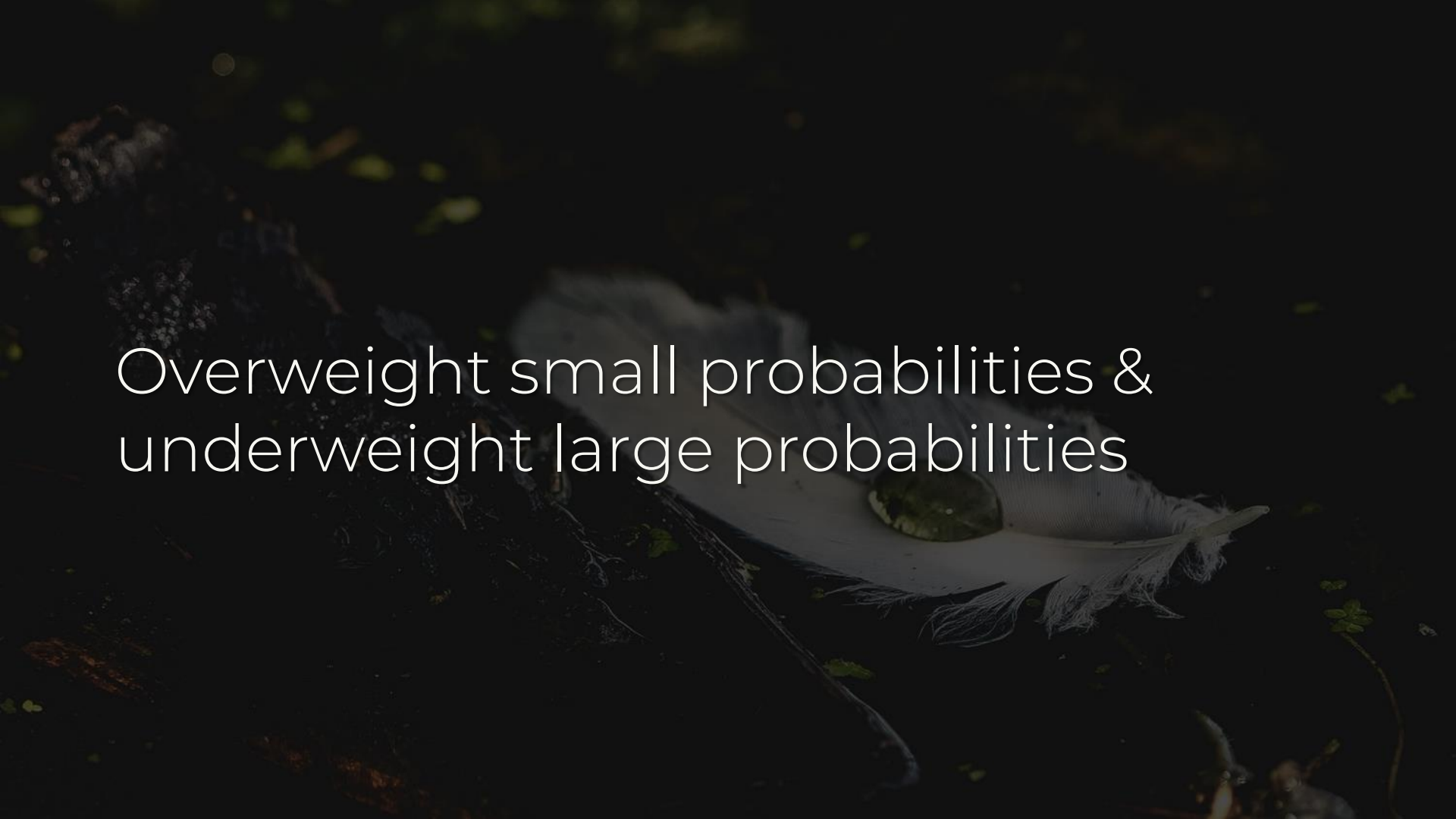
It’s likely not the same as yours.


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

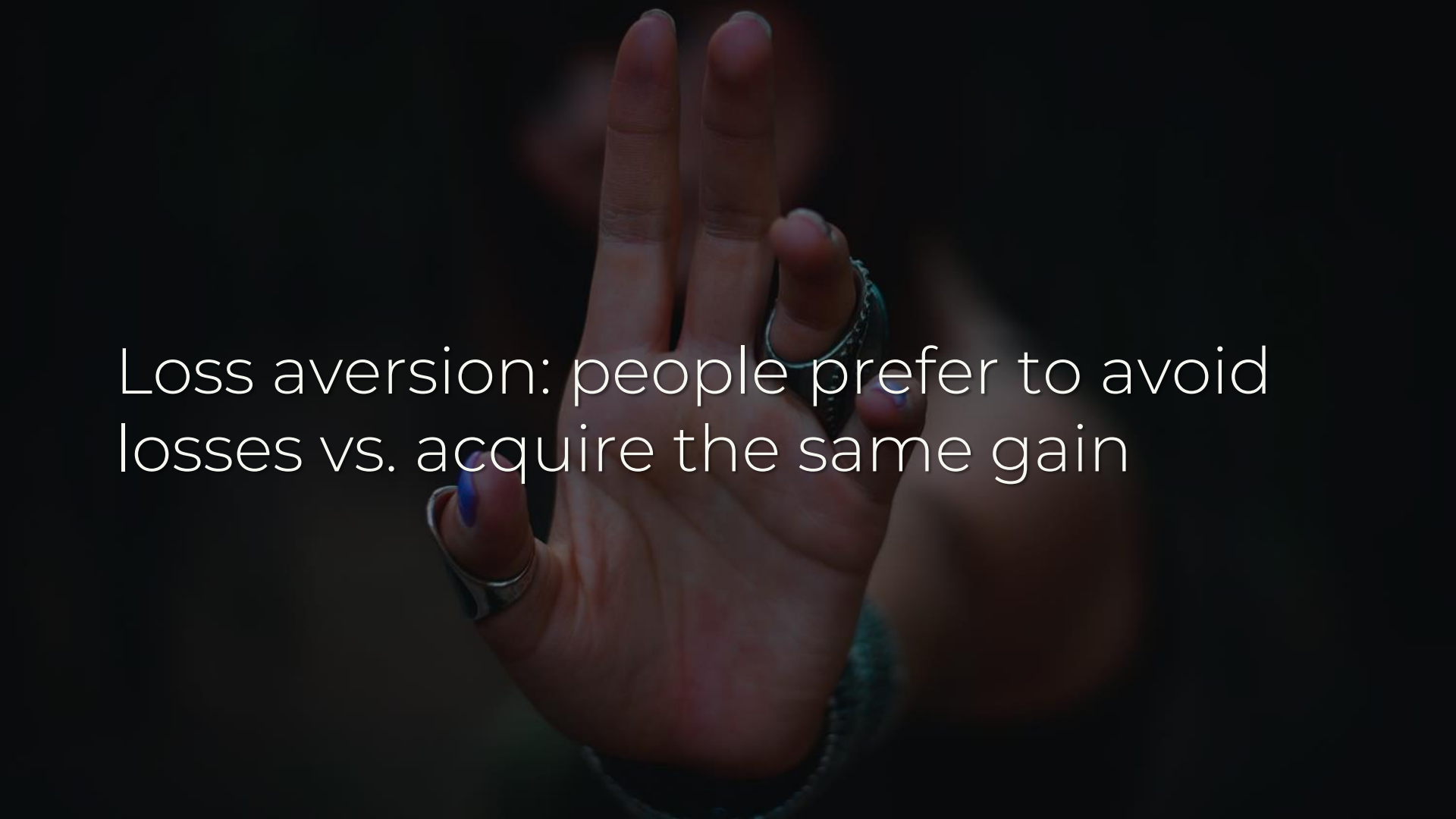
# Next level: Equifax's customers aren't the end users whose data is stored

# Prospect Theory: people care about relative vs. objective outcomes


Maintain a reference point against
which outcomes are measured


Overweight small probabilities &
underweight large probabilities

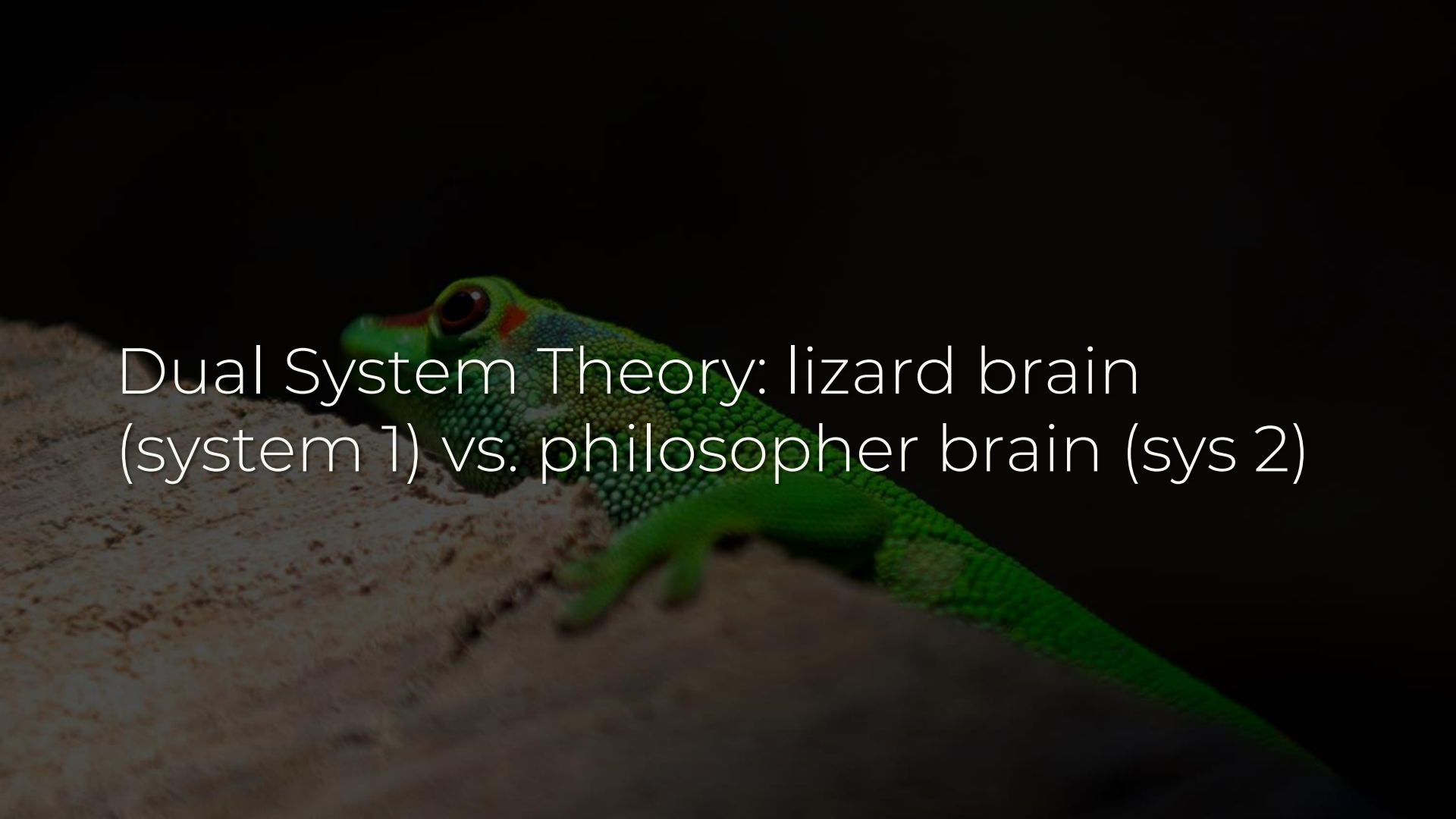
# Overhyping low-probability vuln exploitation vs. default passwords


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

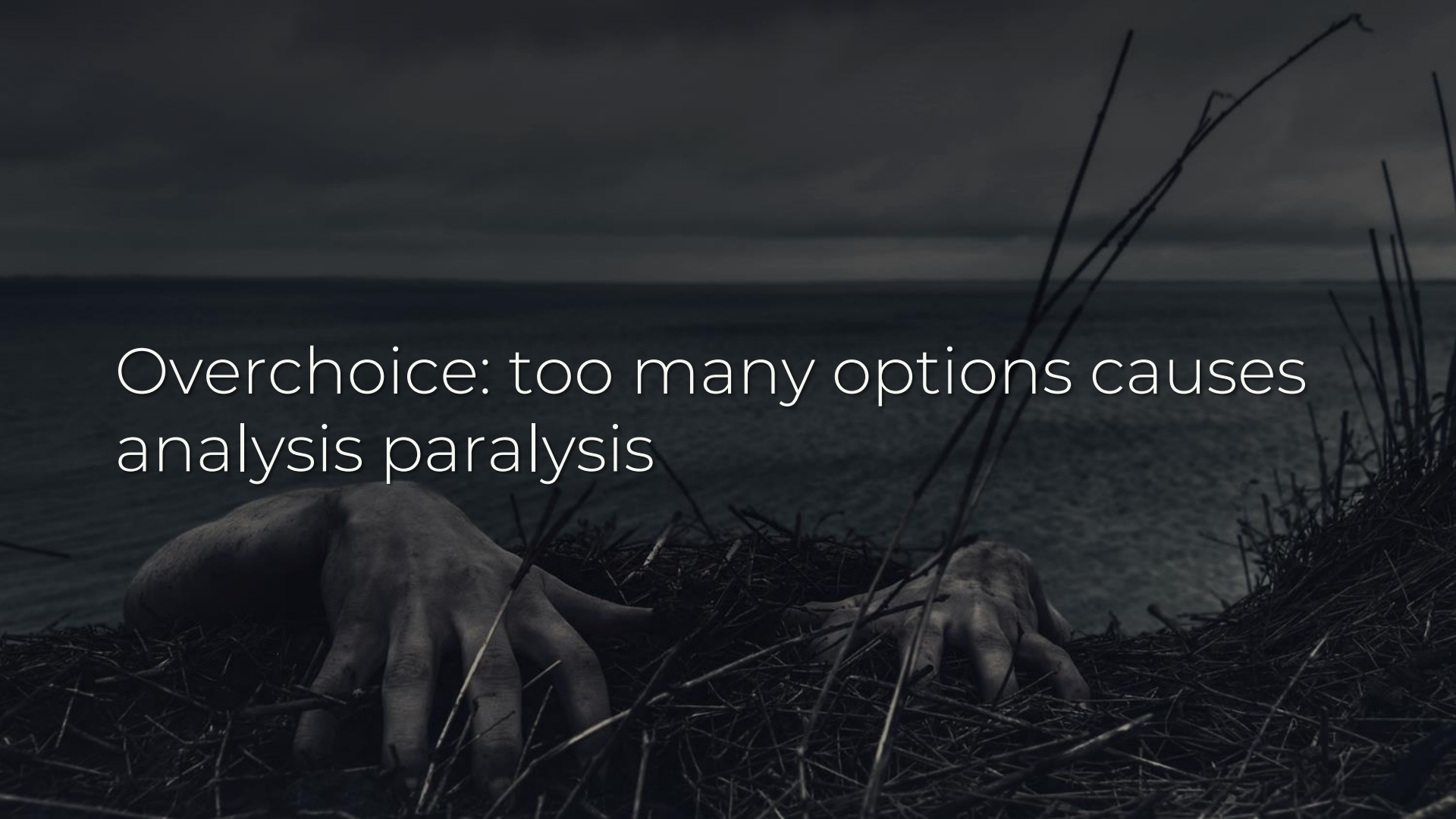
# Framing security as a time & cost sink facilitates natural resistance

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


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?

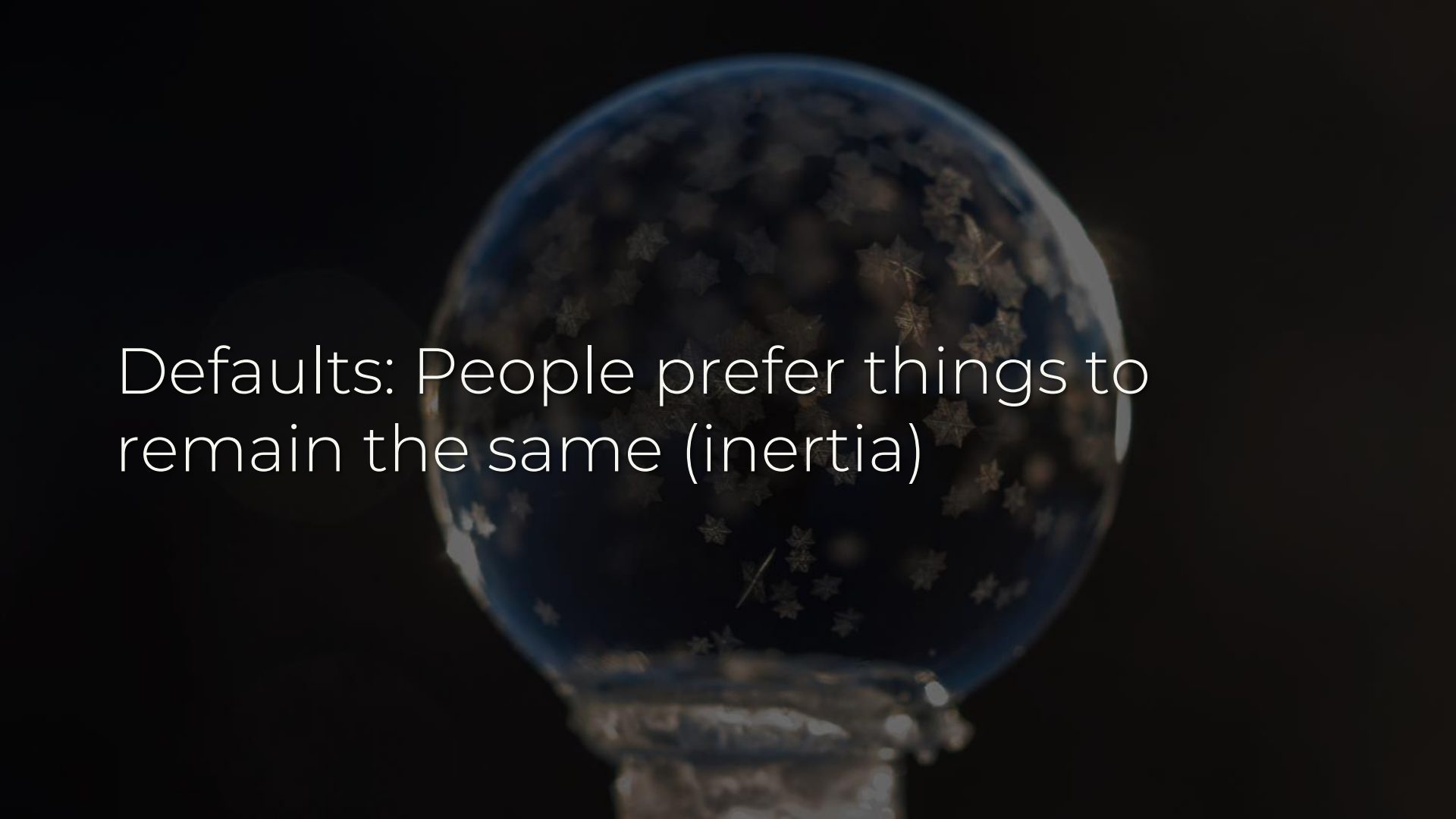
# Design presentation of choices to promote improved decision-making

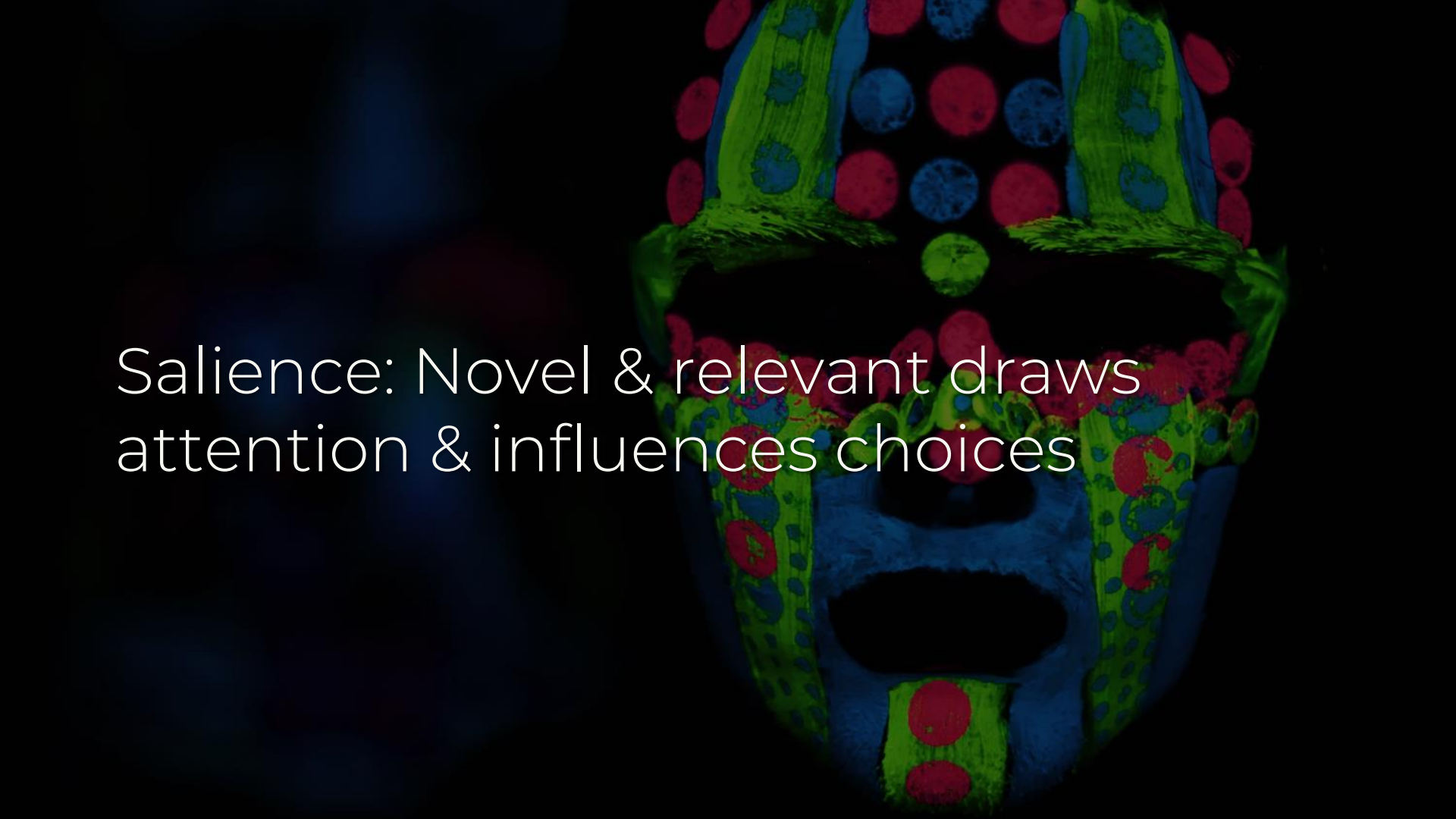
# Example: MINDSPACE framework for behavioral design

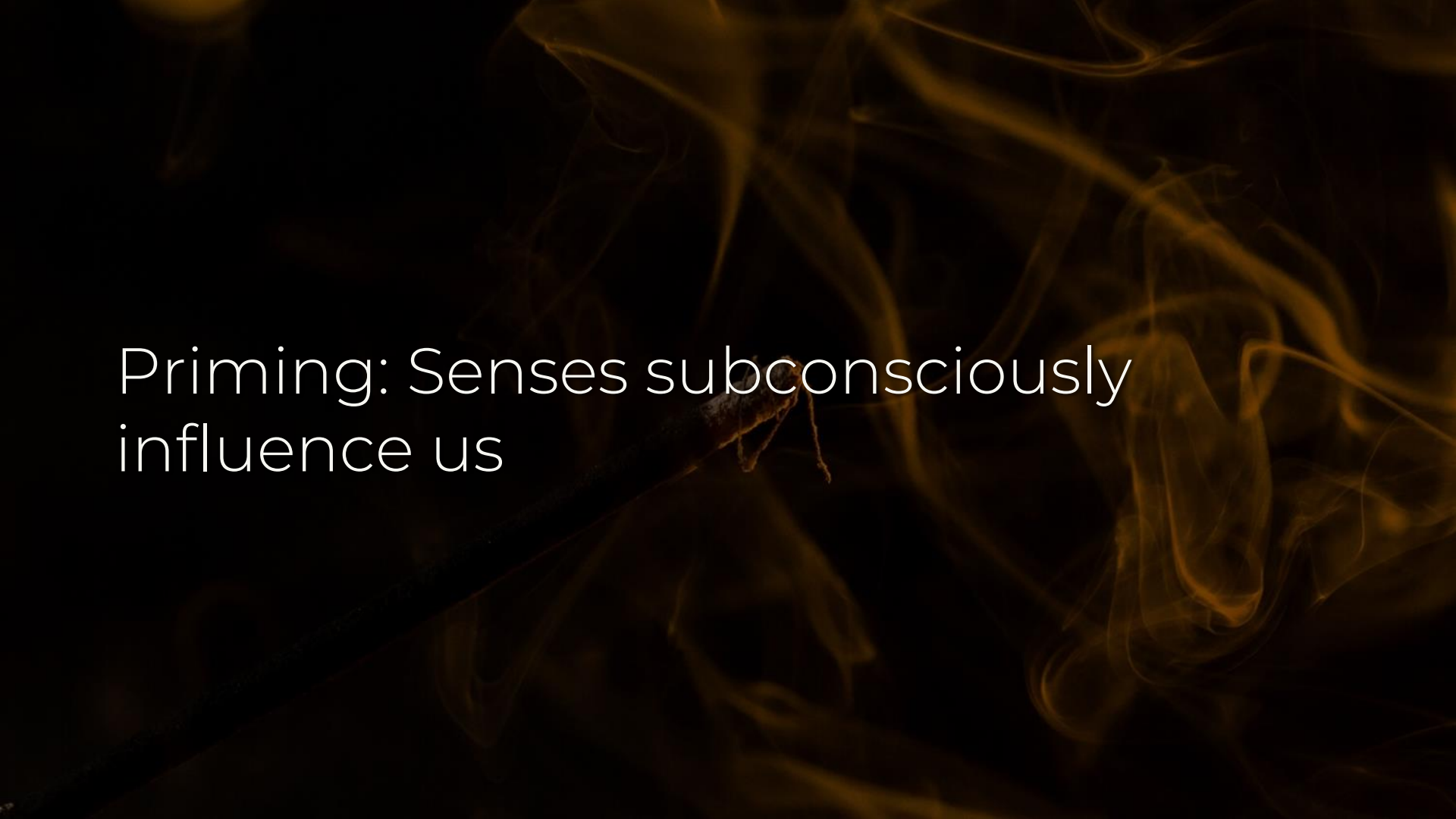

Messenger: people dismiss info from sources they don’t like / respect


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)


Salience: Novel & relevant draws
attention & influences choices


Priming: Senses subconsciously
influence us


Affect: Emotional reactions are our brains’ first responders

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

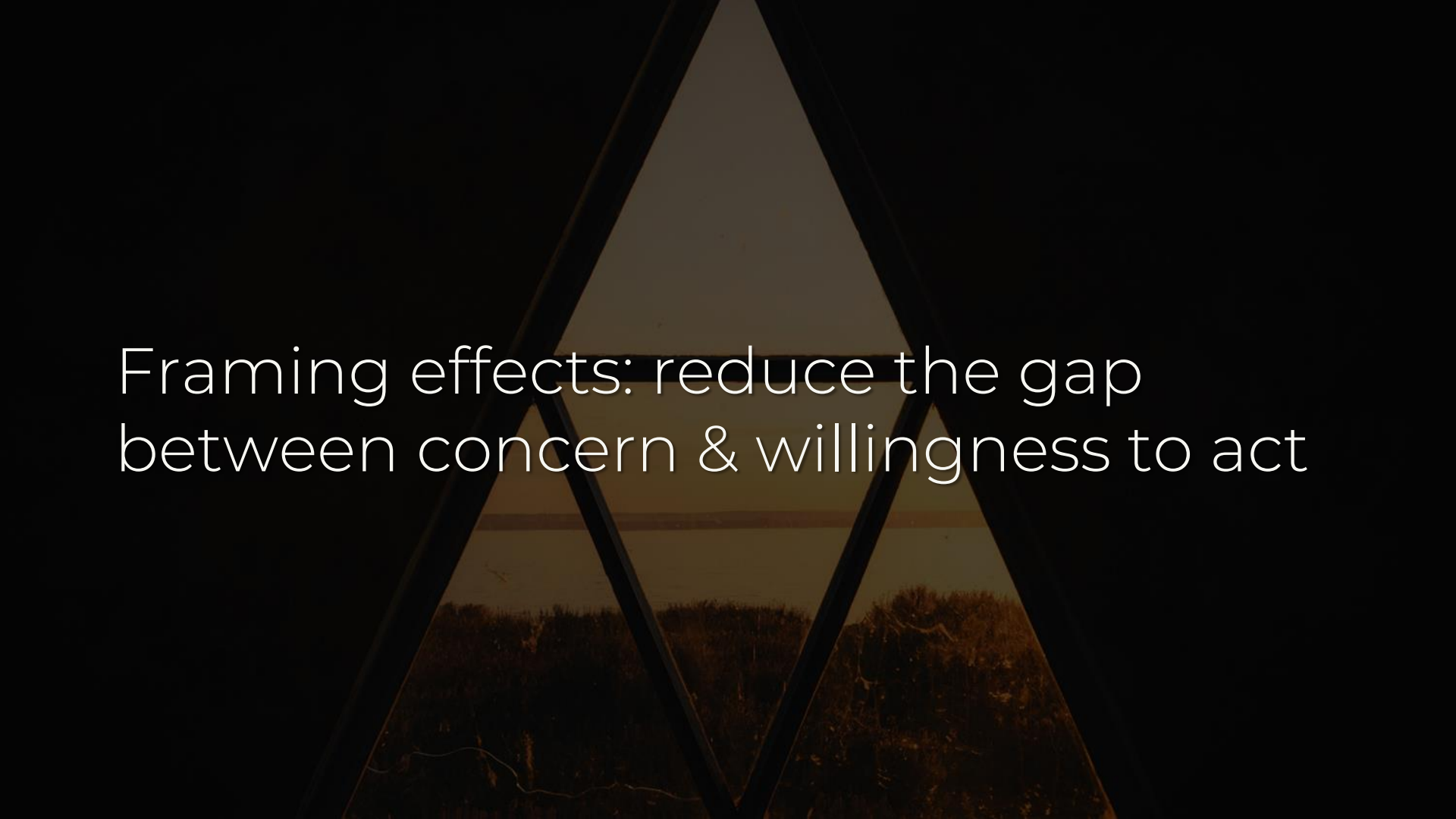

Ego: People like to feel better about themselves & preserve self-image

# Reinforcement mechanisms: consequences to guide behavior

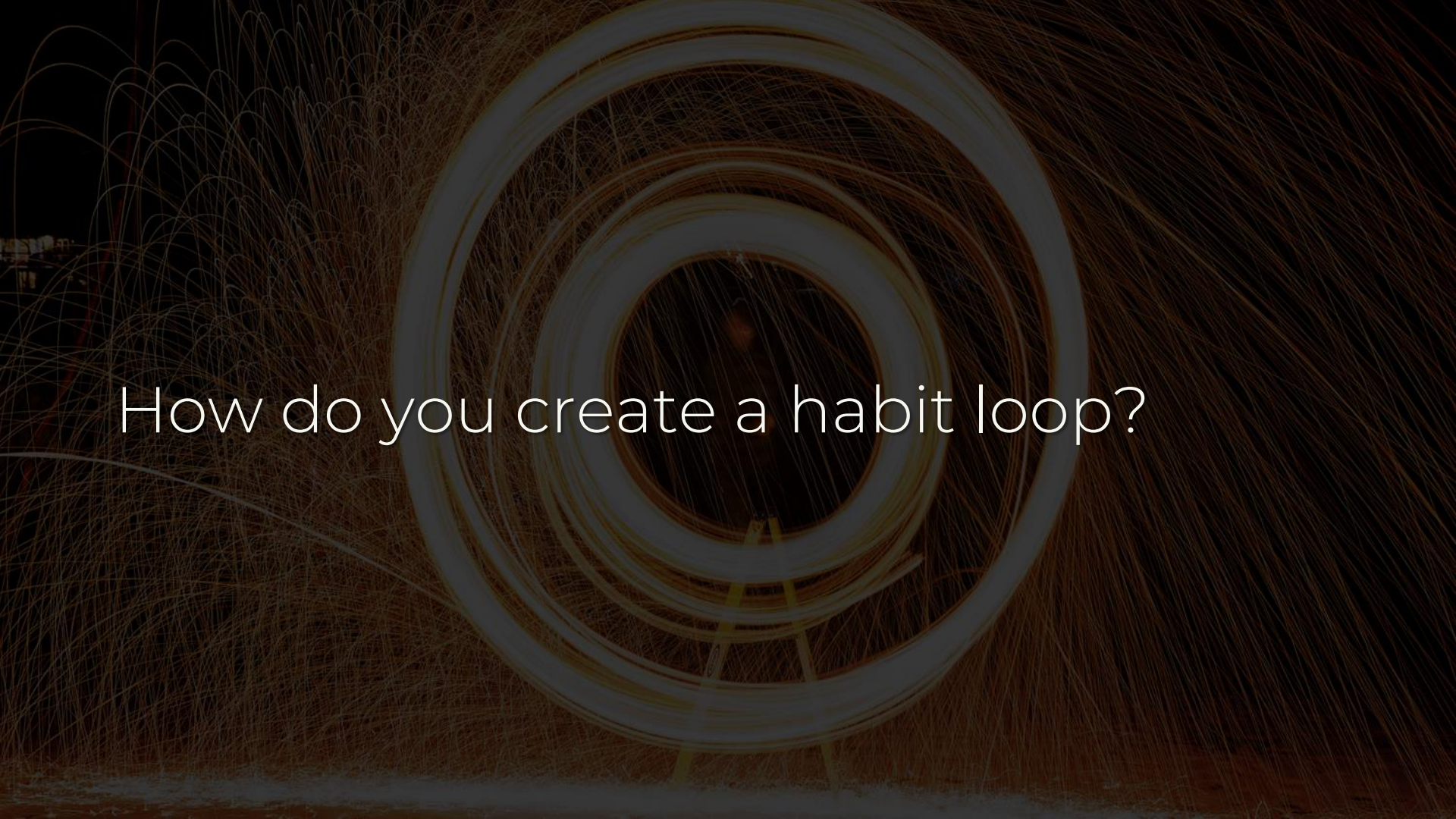
# Pay-for-performance lacks empirical evidence for fixing moral hazard

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


How do you create a habit loop?


Step 1: Routine

# Make it stable, frictionless, & fit into existing context

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

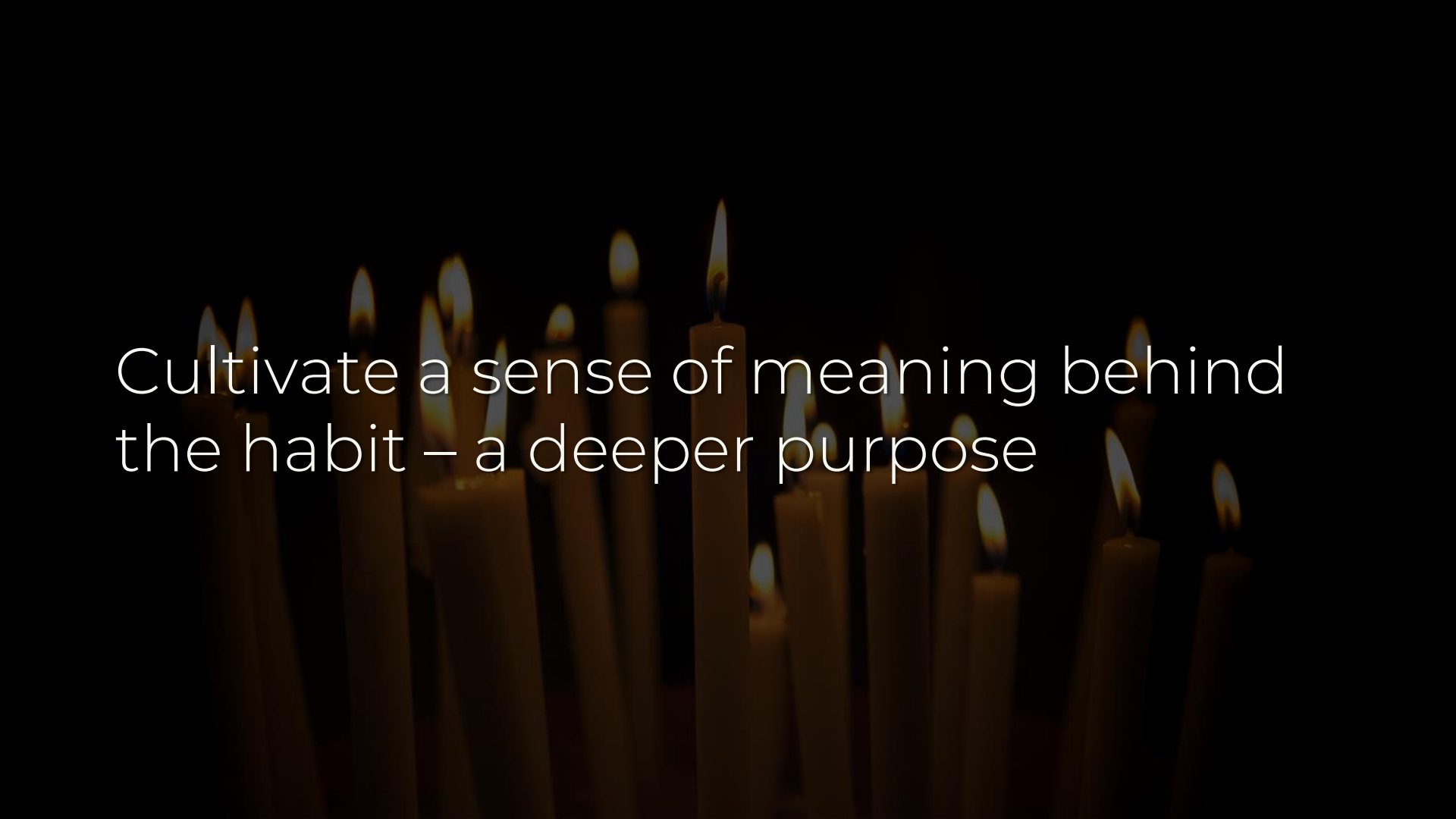
# Step 2: Triggers & Rewards

# Contextual cues: “If X, do Y”

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

# Step 3: Ingrain

# Foster ample opportunities for practice & interaction


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

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


Ideas for IoT Sec

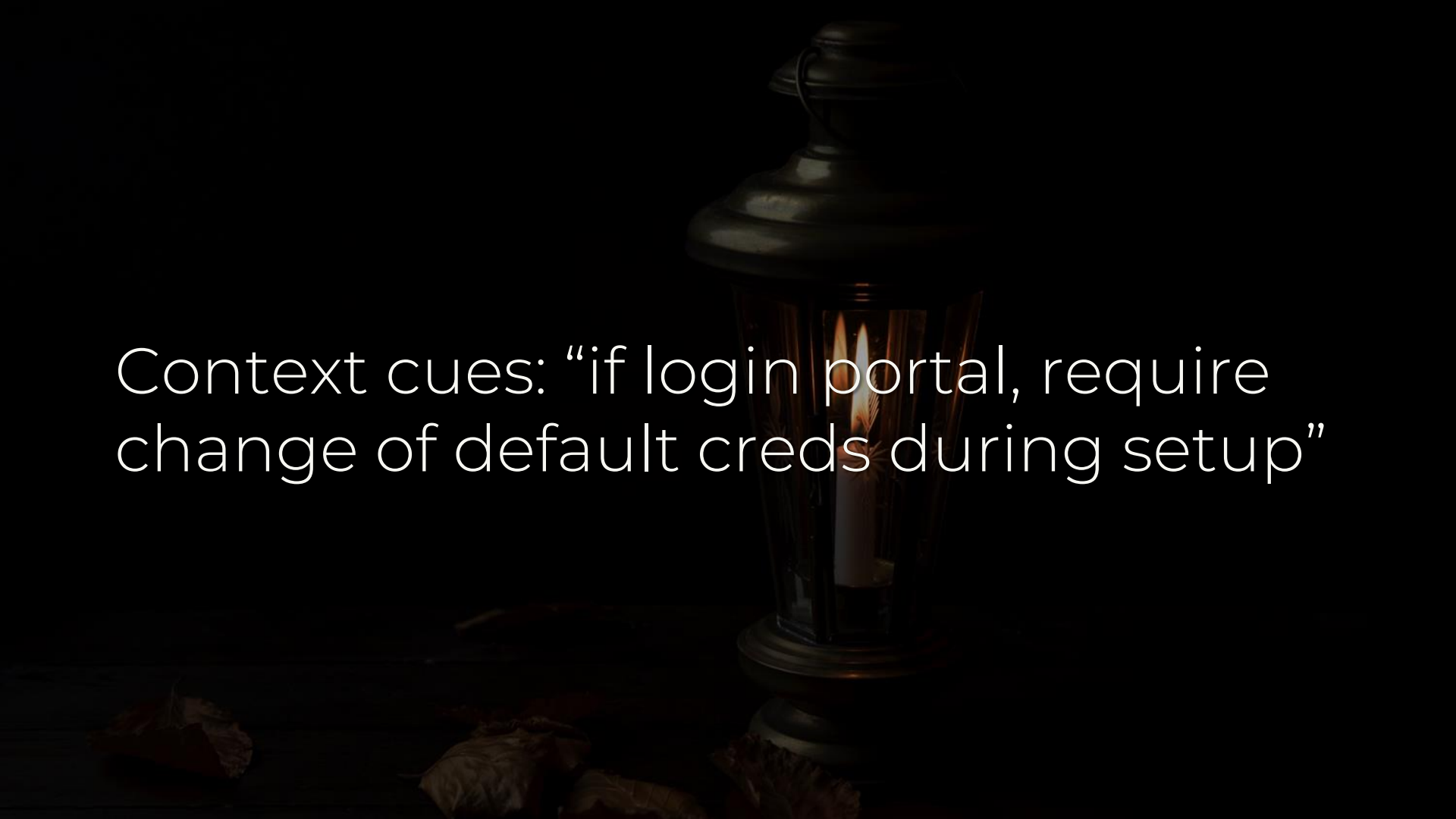

Set concrete goals: “build-in security”
is too nebulous

“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?

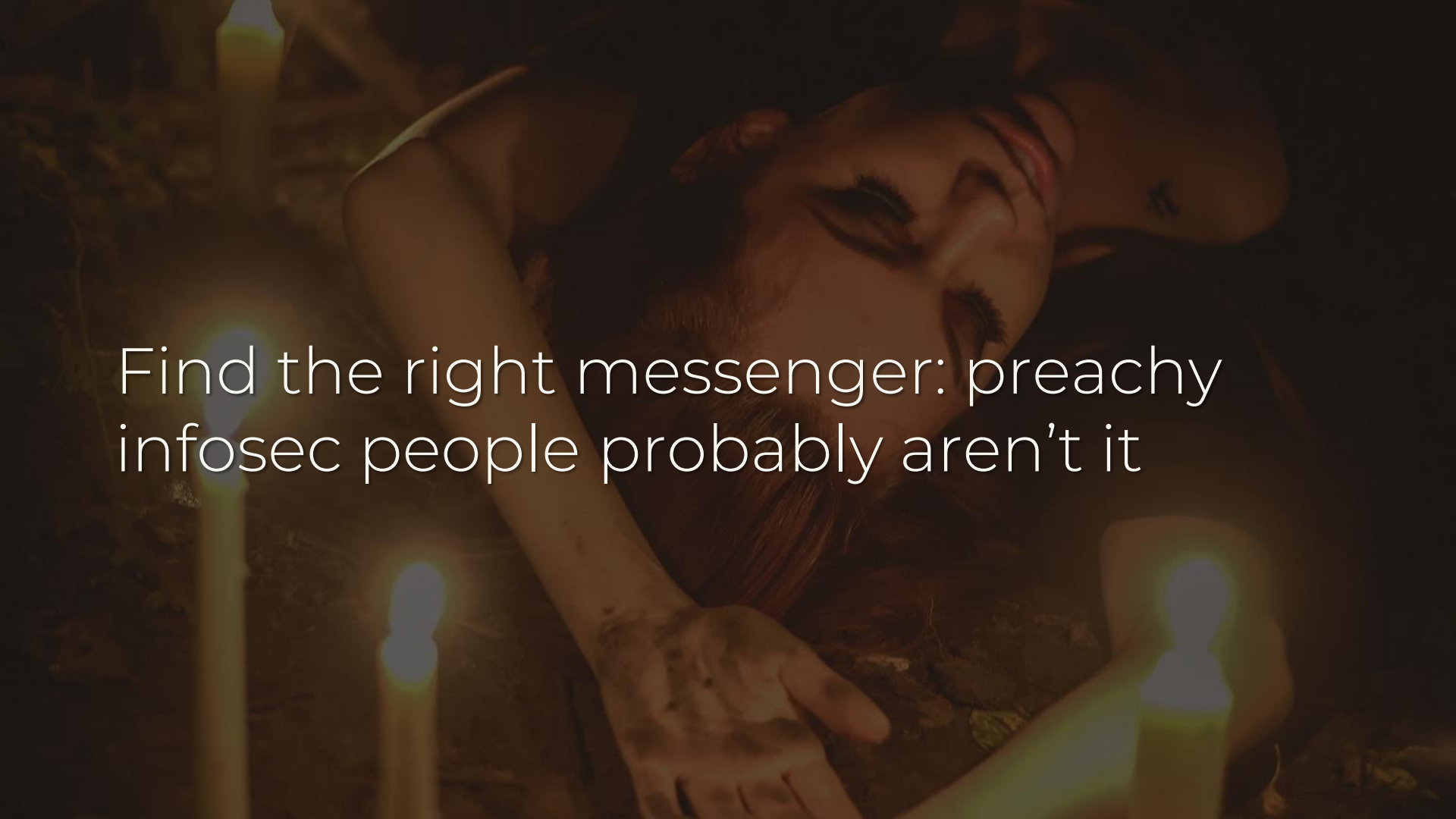
Teams should have a regular, brief time & space to review security goals


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

# How can we leverage MINDSPACE for IoT security?


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

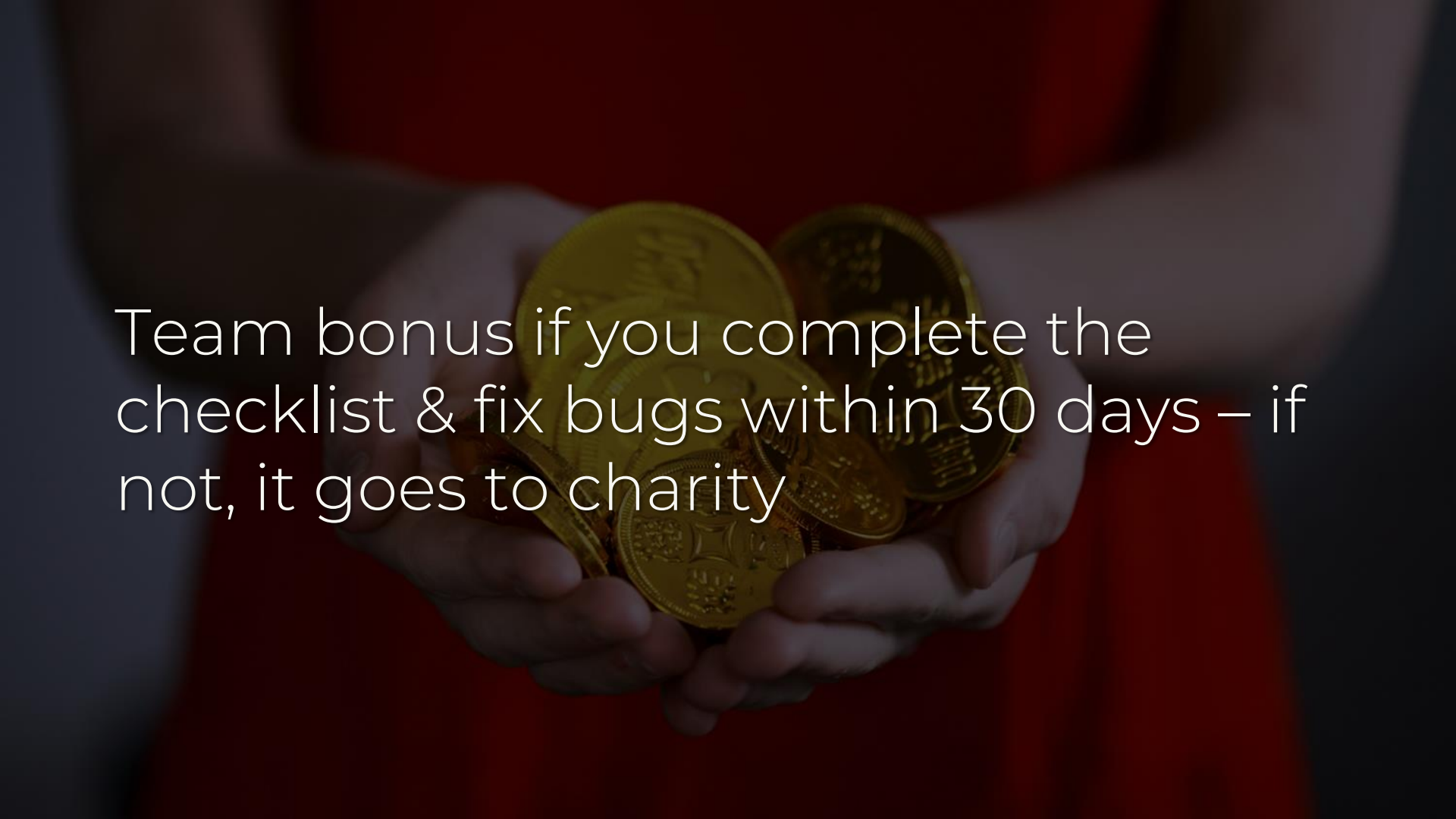
“Gift” budget that is eroded if security goals aren’t met (loss aversion)


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

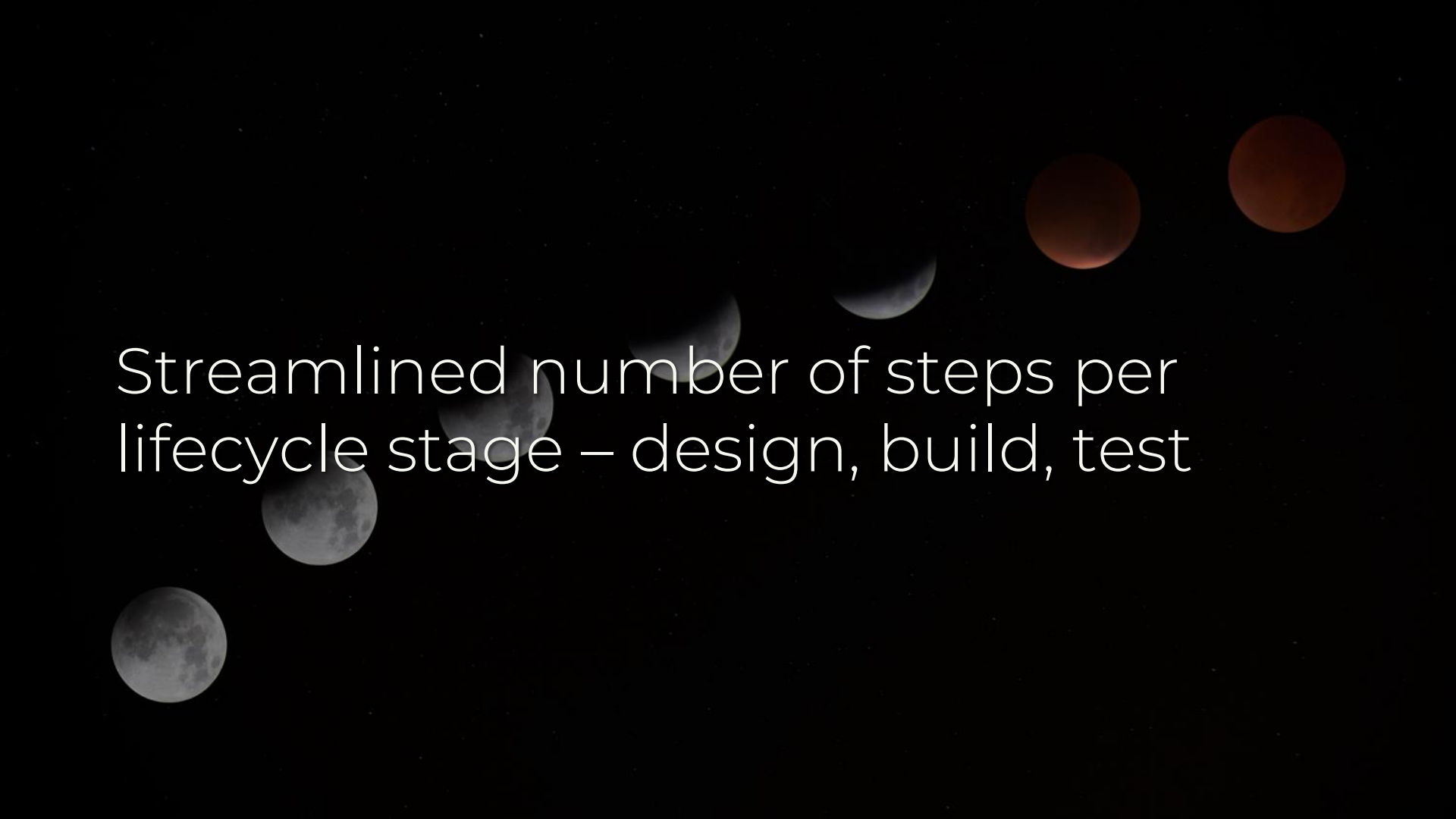
# Control instincts to security issues – slow down via threat modelling


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

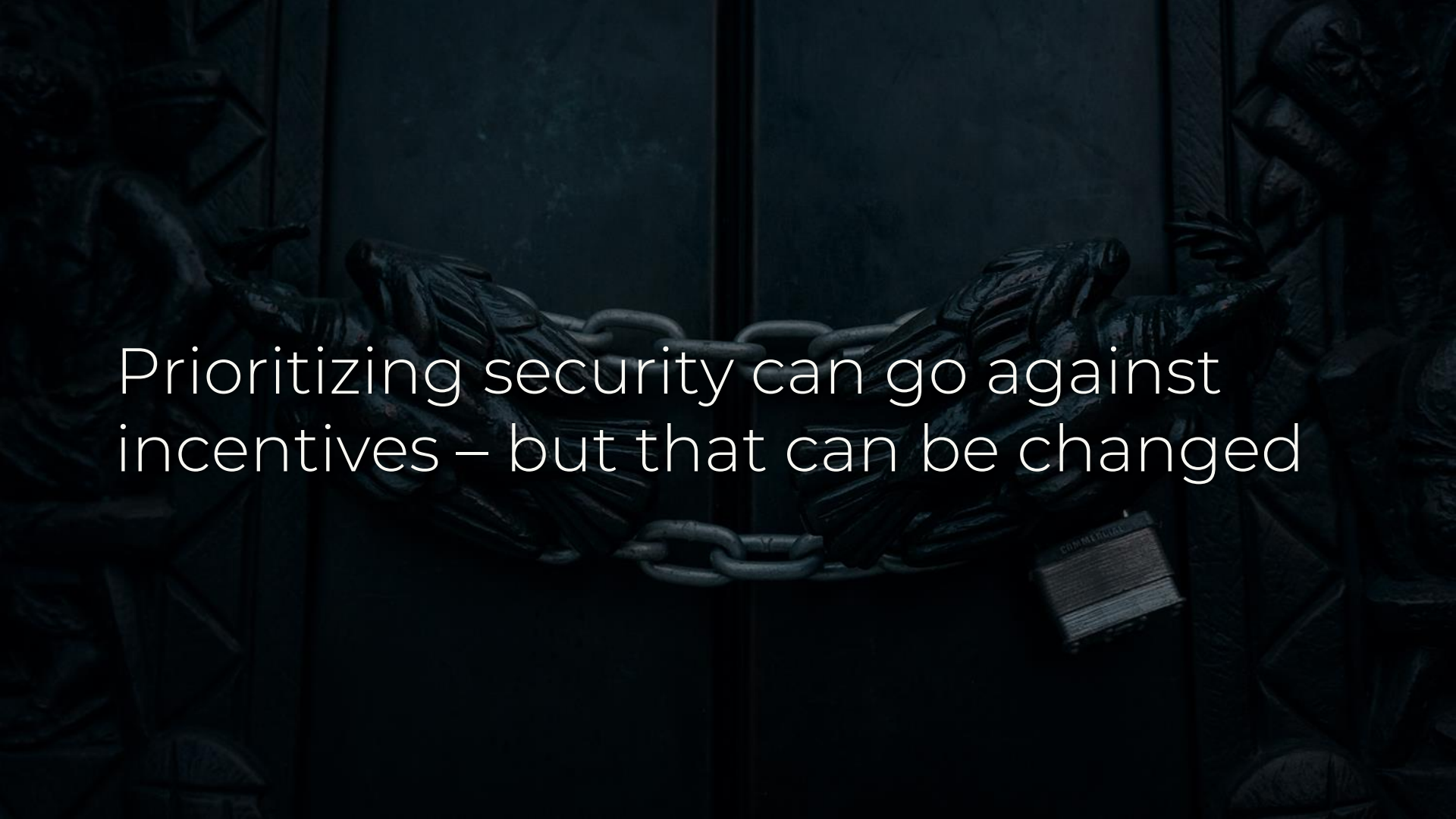
- Share essential information concerning security steps with the team
- Confirm each team member understands the security requirements
- Have any new features been added since design that require review? (ie interfacing w/ the internet, collecting user data)
- Anticipated Security Events
  - What are 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


IoT security ideas must treat devs as
time-constrained humans

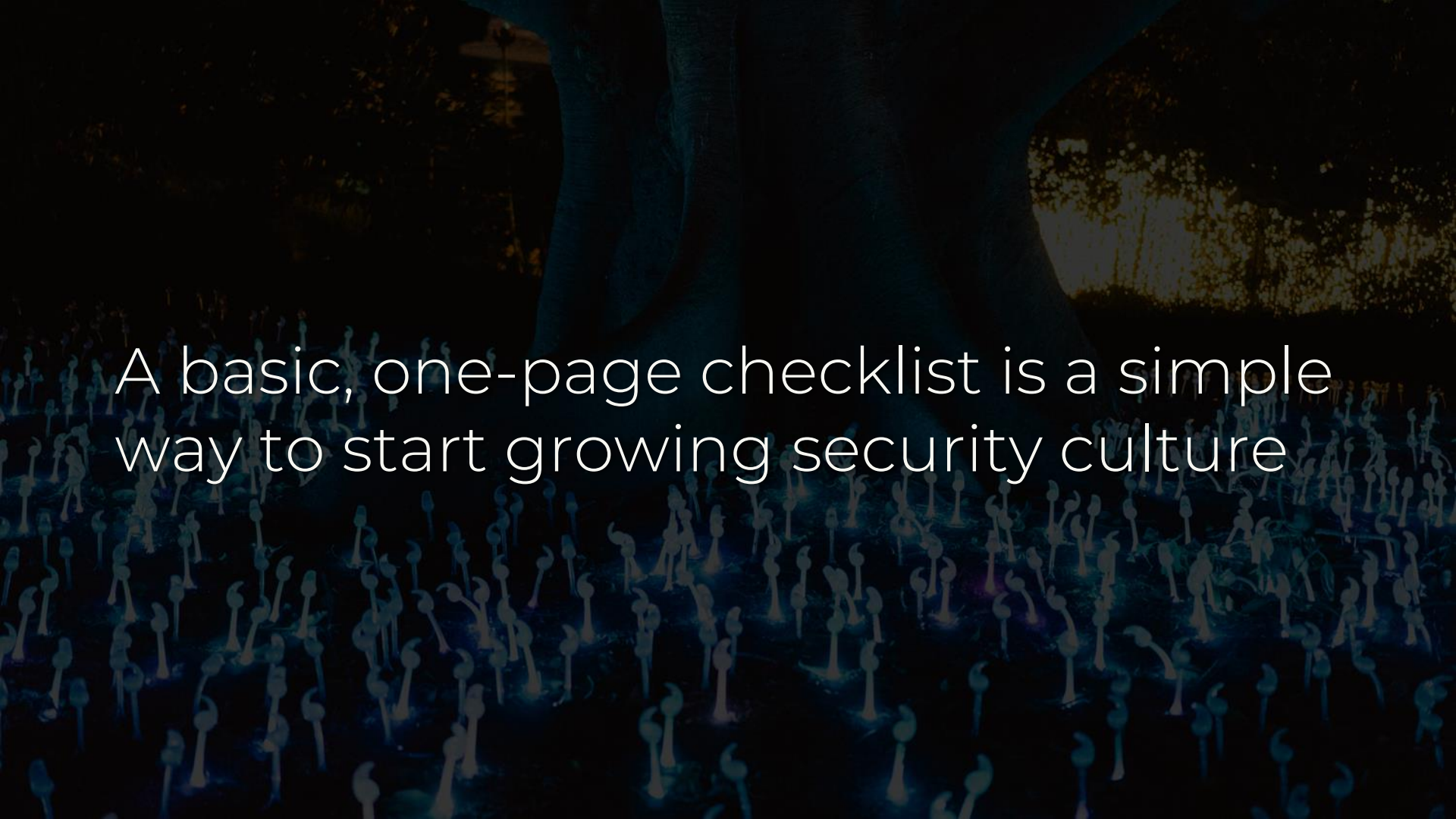

Prioritizing security can go against incentives – but that can be changed


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


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


But practical magic using behavioral
design can improve decision making


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


“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 mindspace 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


110

@swagitda_

/in/kellyshortridge

kelly@greywire.net