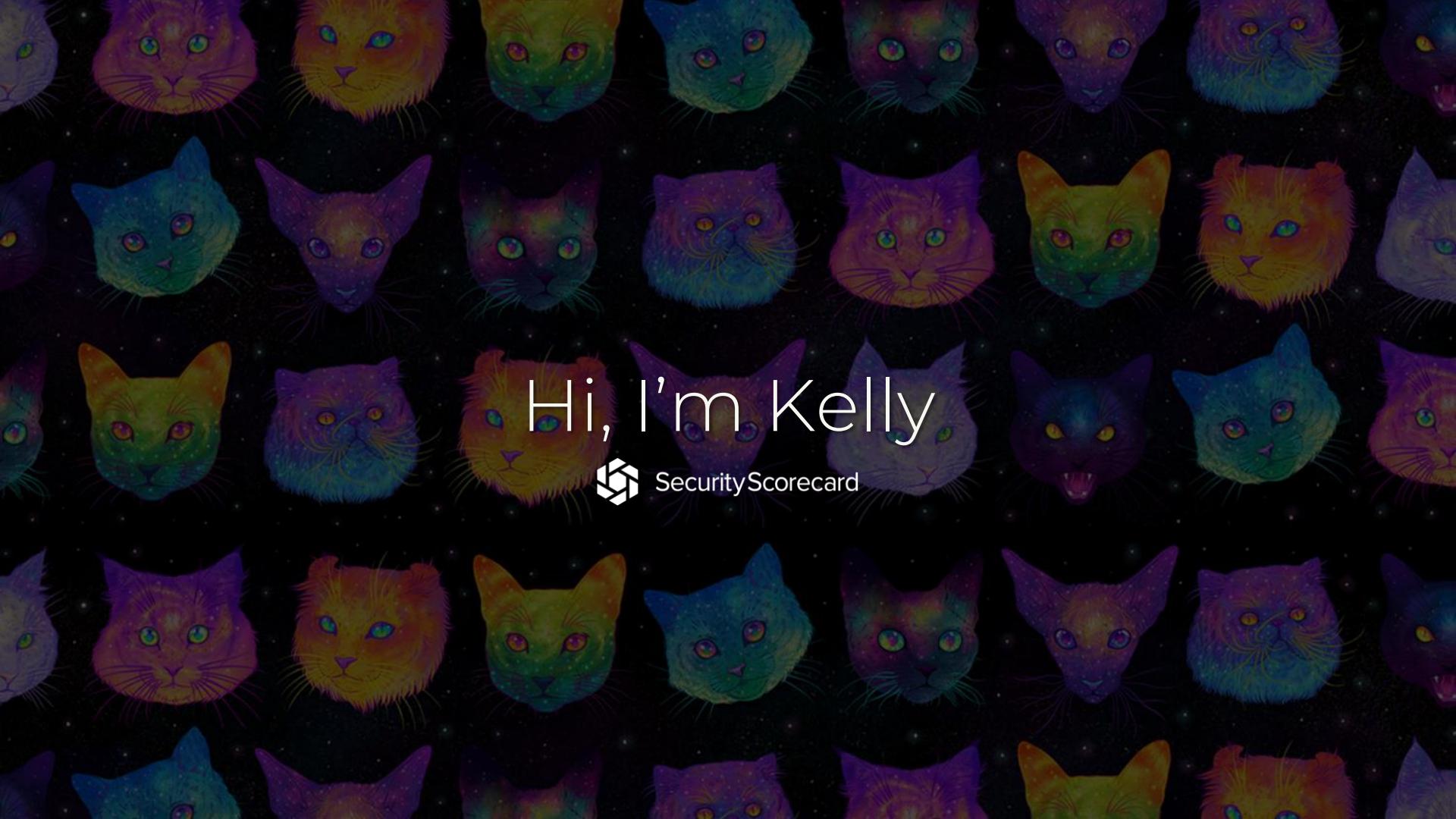


# Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda\_)  
AusCERT 2018



Hi, I'm Kelly

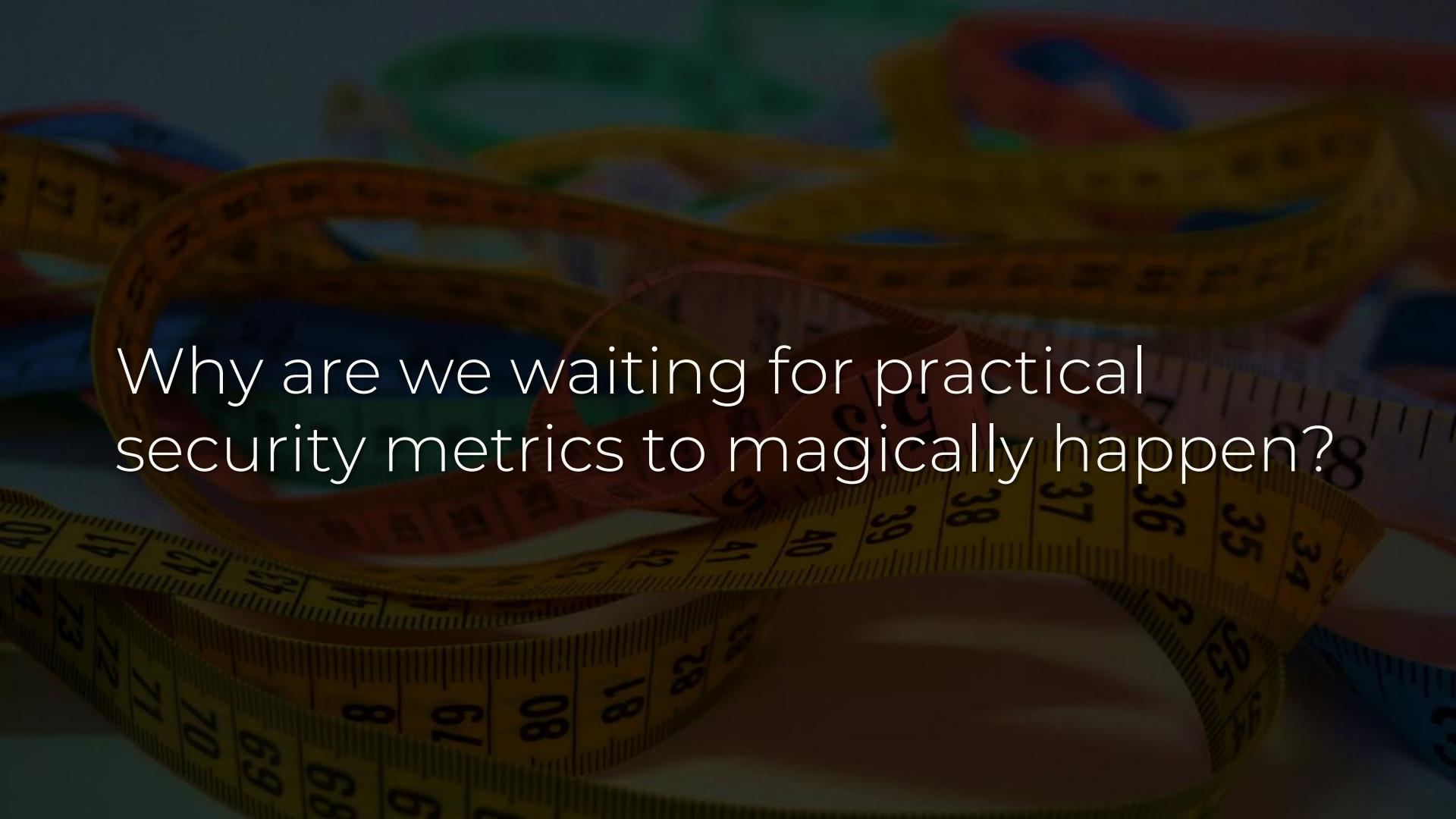


SecurityScorecard

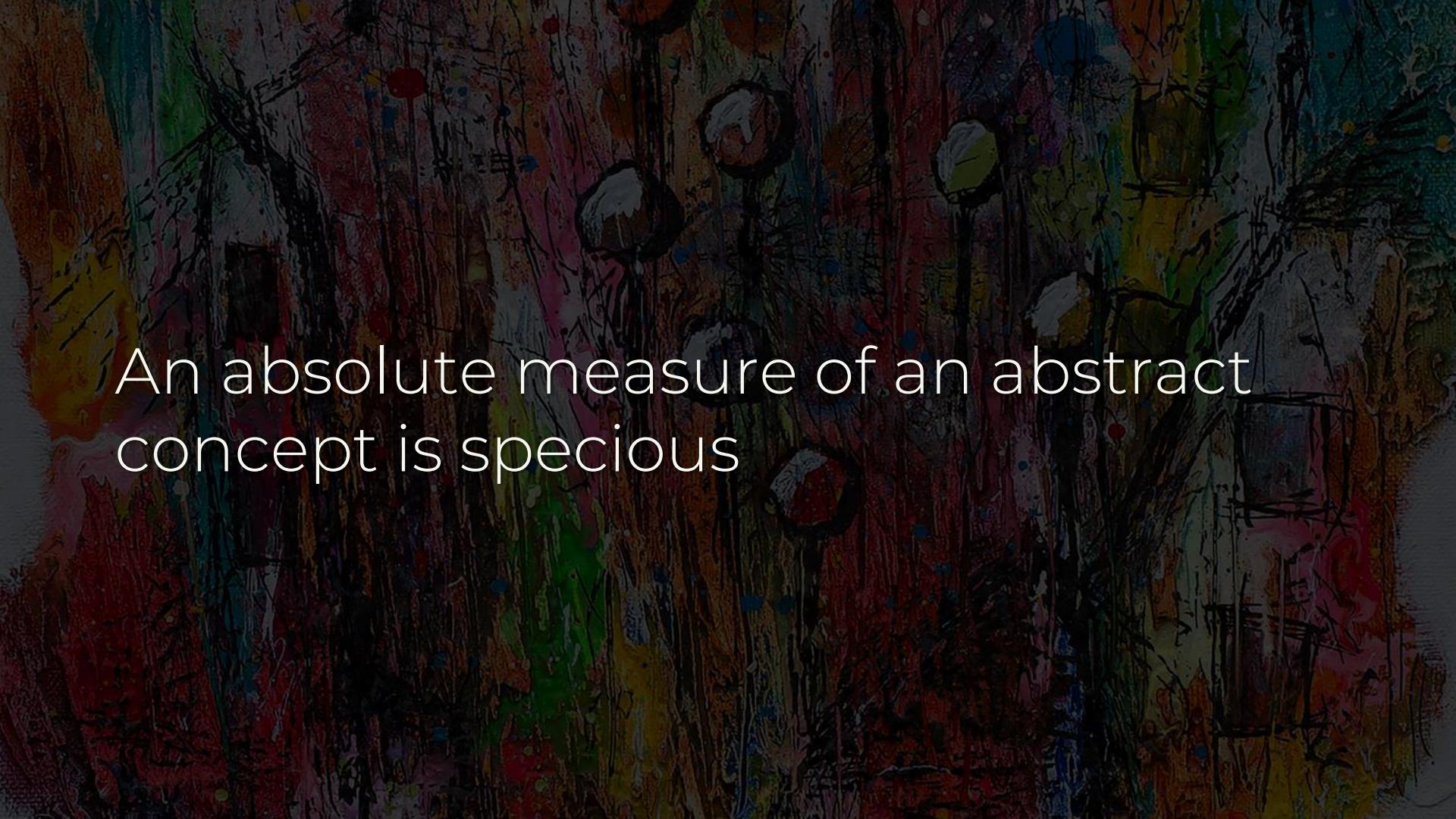


“They always say time changes things,  
but you actually have to change them  
yourself.”

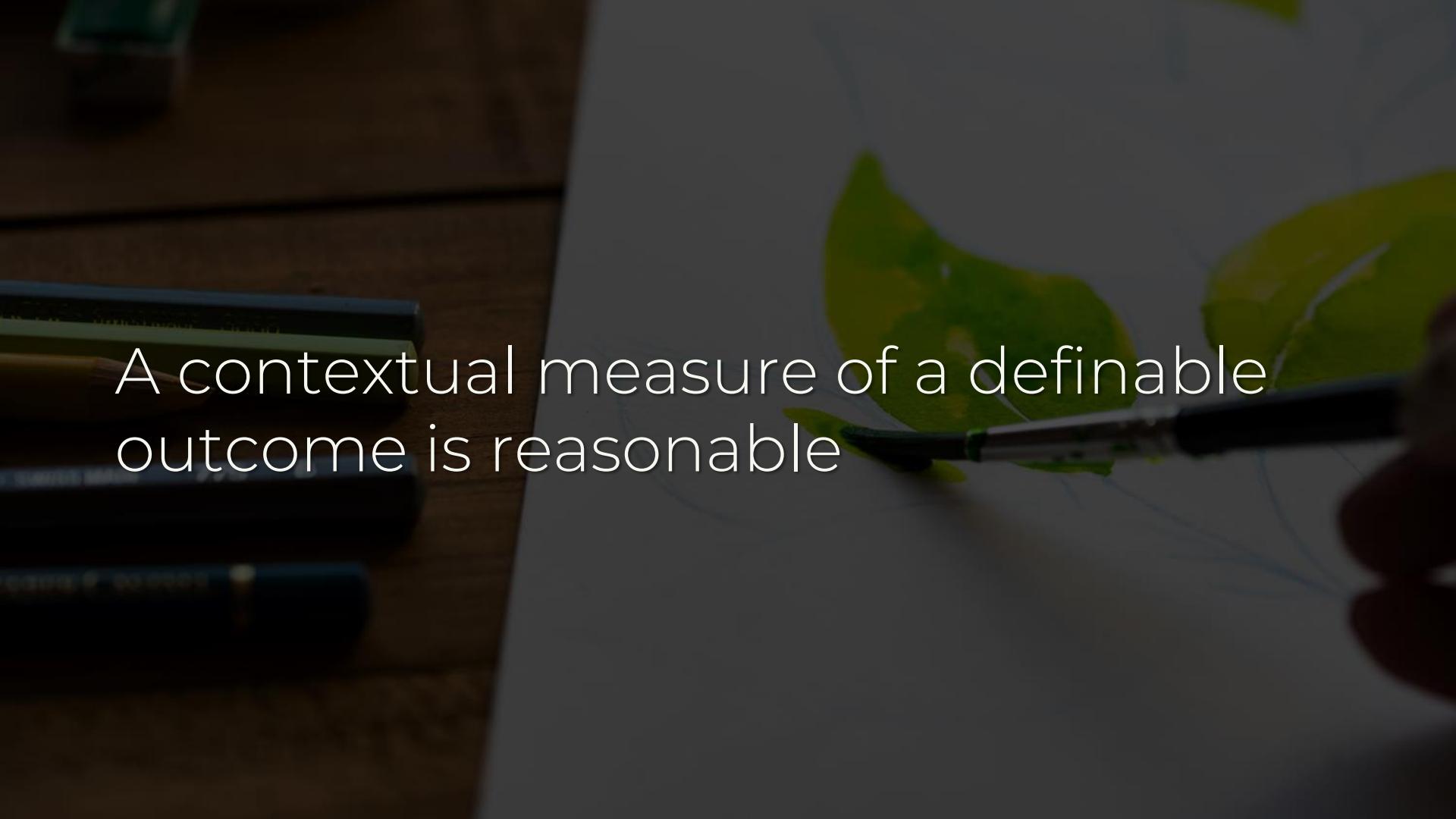
— Andy Warhol



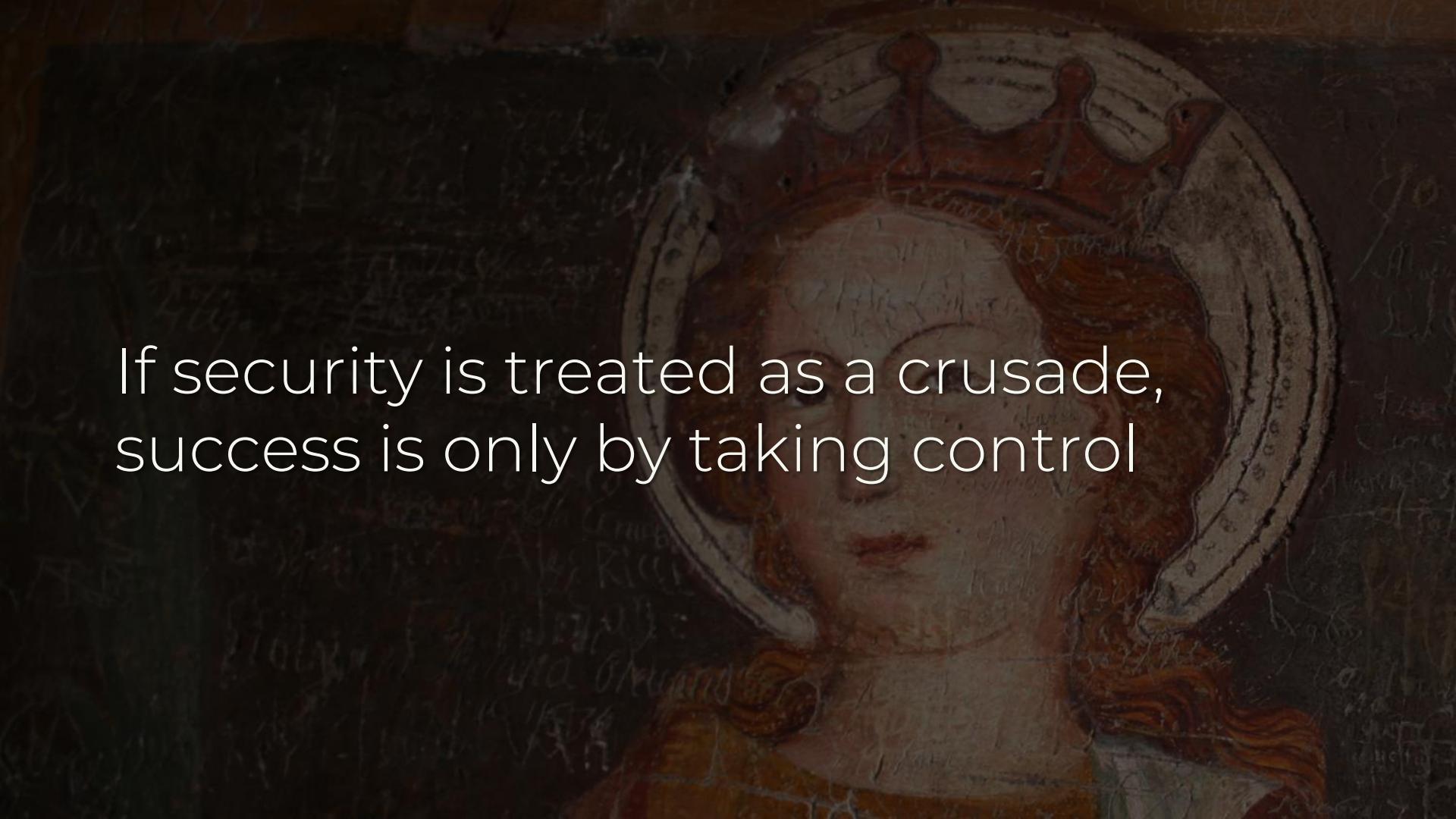
Why are we waiting for practical security metrics to magically happen?

The background of the slide is a vibrant, abstract painting. It features a dense composition of vertical and horizontal brushstrokes in a variety of colors, including shades of red, orange, yellow, green, blue, and purple. Some areas are more saturated than others, creating a dynamic range of tones. The overall effect is one of energetic movement and visual complexity.

An absolute measure of an abstract  
concept is specious

A close-up photograph of a person's hand holding a paintbrush with a green handle and a silver ferrule. The brush is angled downwards, resting on a light-colored surface that has several bright yellow paint splatters on it. The background is dark and out of focus.

A contextual measure of a definable outcome is reasonable



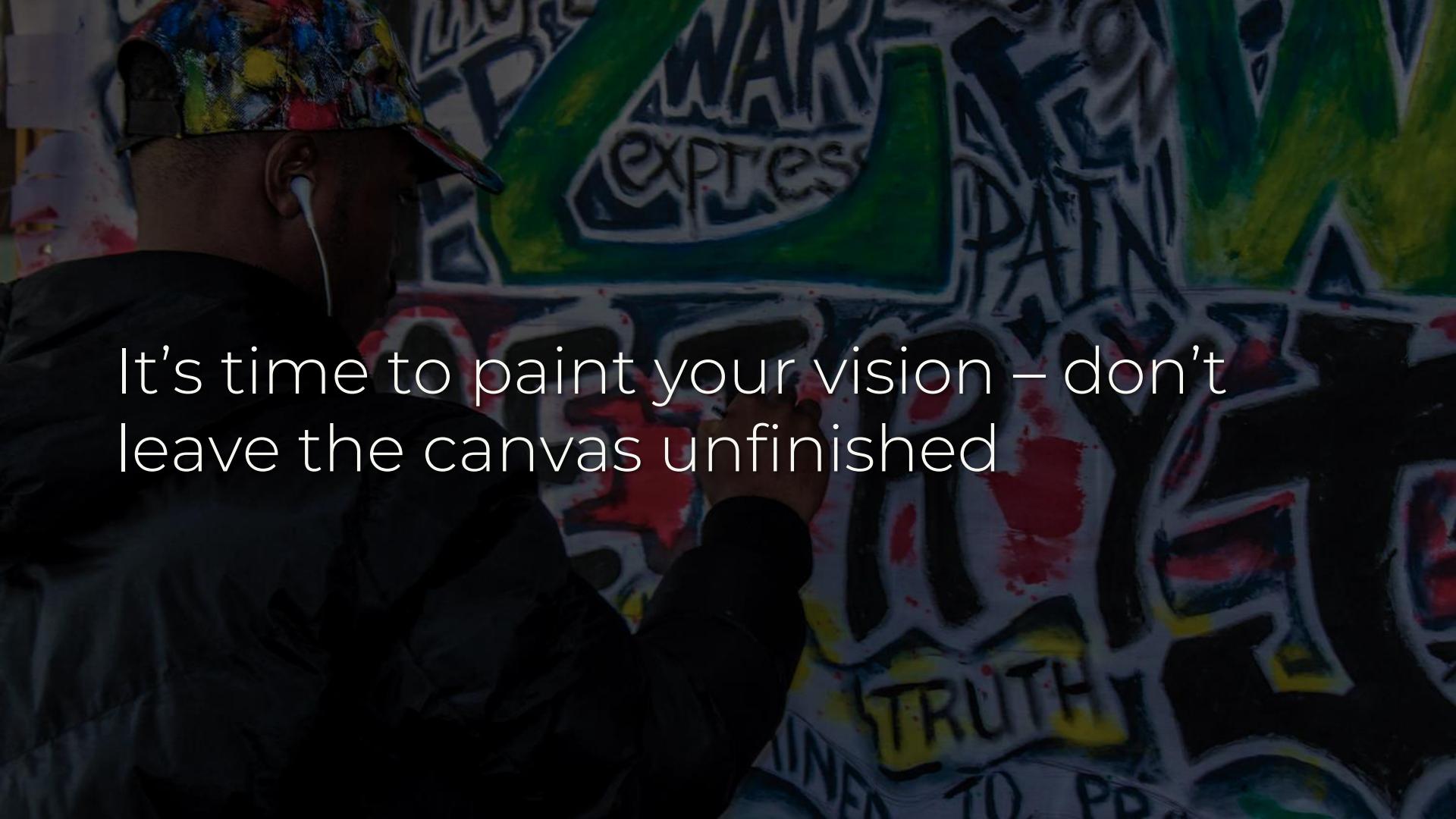
If security is treated as a crusade,  
success is only by taking control



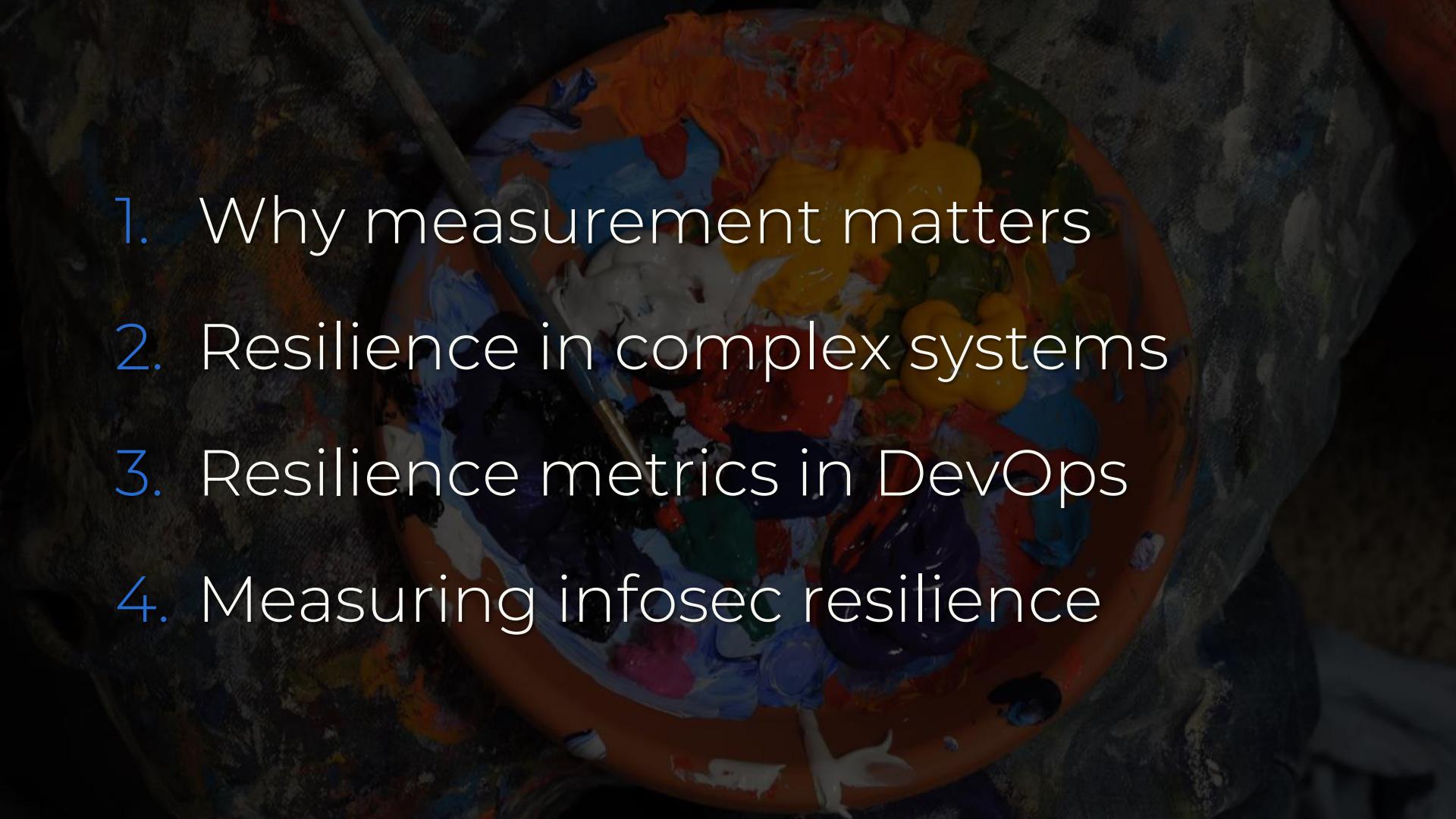
If security is treated as a product,  
success can be defined & measured

“Be a better person” vs. “read 30 mins per day & volunteer 1x per month”



A person wearing a colorful, patterned baseball cap and white headphones is painting a large mural on a wall. The mural features bold, stylized text in various colors like green, blue, red, and yellow. Some words visible in the mural include "MAKE", "express", "TRUTH", and "DREAM". The person is focused on their work, with paint splatters on their shirt and arms.

It's time to paint your vision – don't leave the canvas unfinished

- 
- The background of the slide features a vibrant, abstract painting of a face. The face is composed of various colors including orange, red, yellow, blue, and green, with a prominent crown of flowers on top. The brushstrokes are visible and expressive. The overall mood is artistic and organic.
1. Why measurement matters
  2. Resilience in complex systems
  3. Resilience metrics in DevOps
  4. Measuring infosec resilience



Why is measurement  
important?

Generally we do a thing in order to achieve a certain result

Process: “a series of actions taken in order to achieve a particular end.”

A close-up photograph of a person's hands holding a smartphone. The phone has a vibrant, abstract patterned case featuring shades of orange, yellow, green, and blue. The background is dark and out of focus.

You cannot people or technology  
your way out of bad processes

Define your desired result & what counts as “success”

Vision: reduce the security team's workflow volatility

Success: “In 1 year, my team will spend only 10% - 15% of time on firefighting”

Success: “In 6 months, JIT-pre-GA security reviews will decrease >50%”



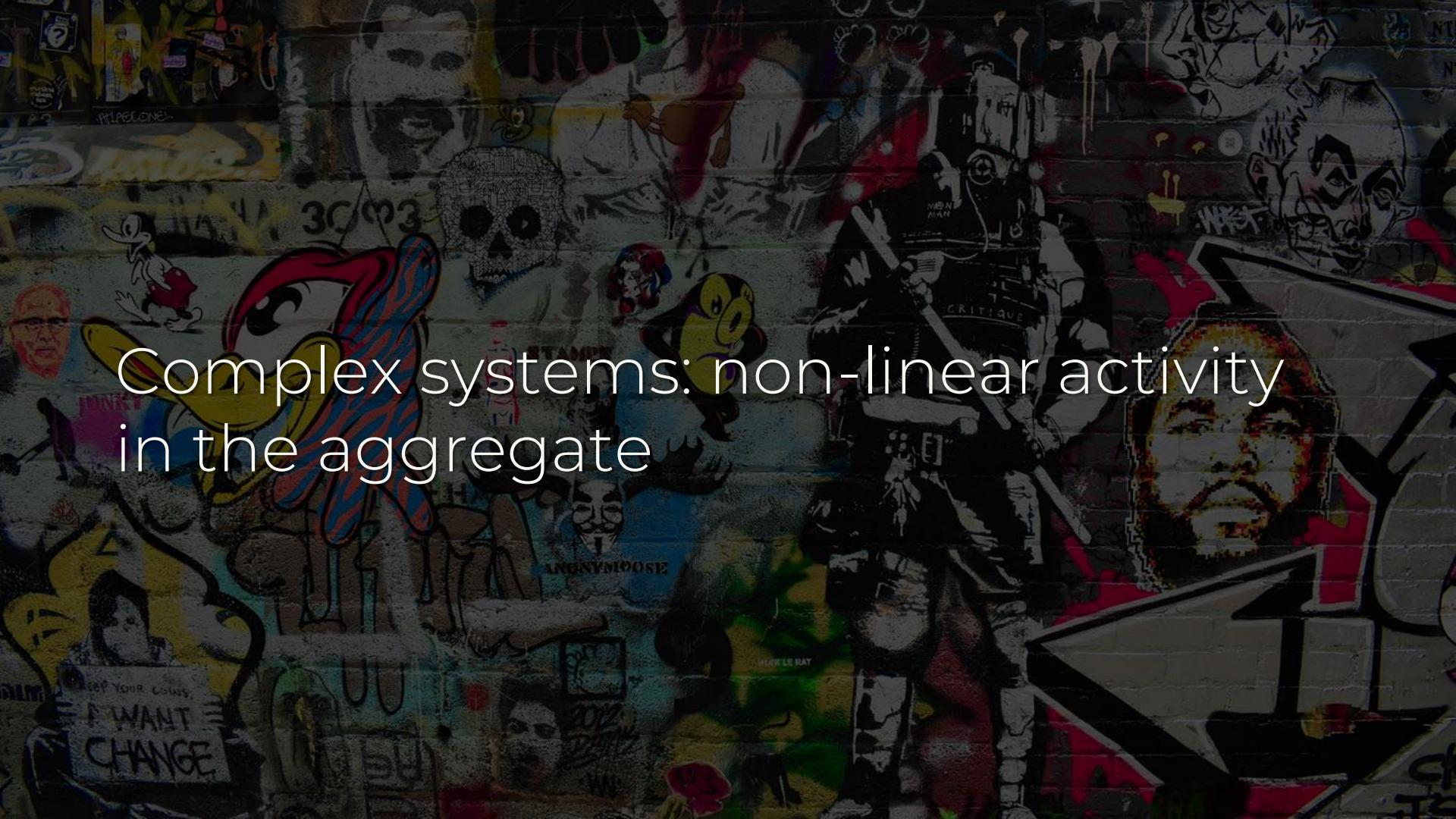
Success metrics create the numbers  
by which you paint your vision

Metrics are quantifiable measures to track & assess status

Your process must reflect a relentless pursuit of continuous improvement

The background of the slide features a vibrant, abstract pattern composed of various colors including red, yellow, green, blue, and purple. These colors are arranged in swirling, organic shapes that resemble a microscopic view of a complex system or perhaps a celestial body like a galaxy. The overall effect is one of depth and intricate interconnectedness.

# Resilience in Complex Systems



Complex systems: non-linear activity  
in the aggregate

Infosec is a complex system.

Defenders, attackers, users,  
governments, vendors, SPs, etc...

Evolutionary resilience: assumes  
complex systems co-evolve

Three central features of resilience:

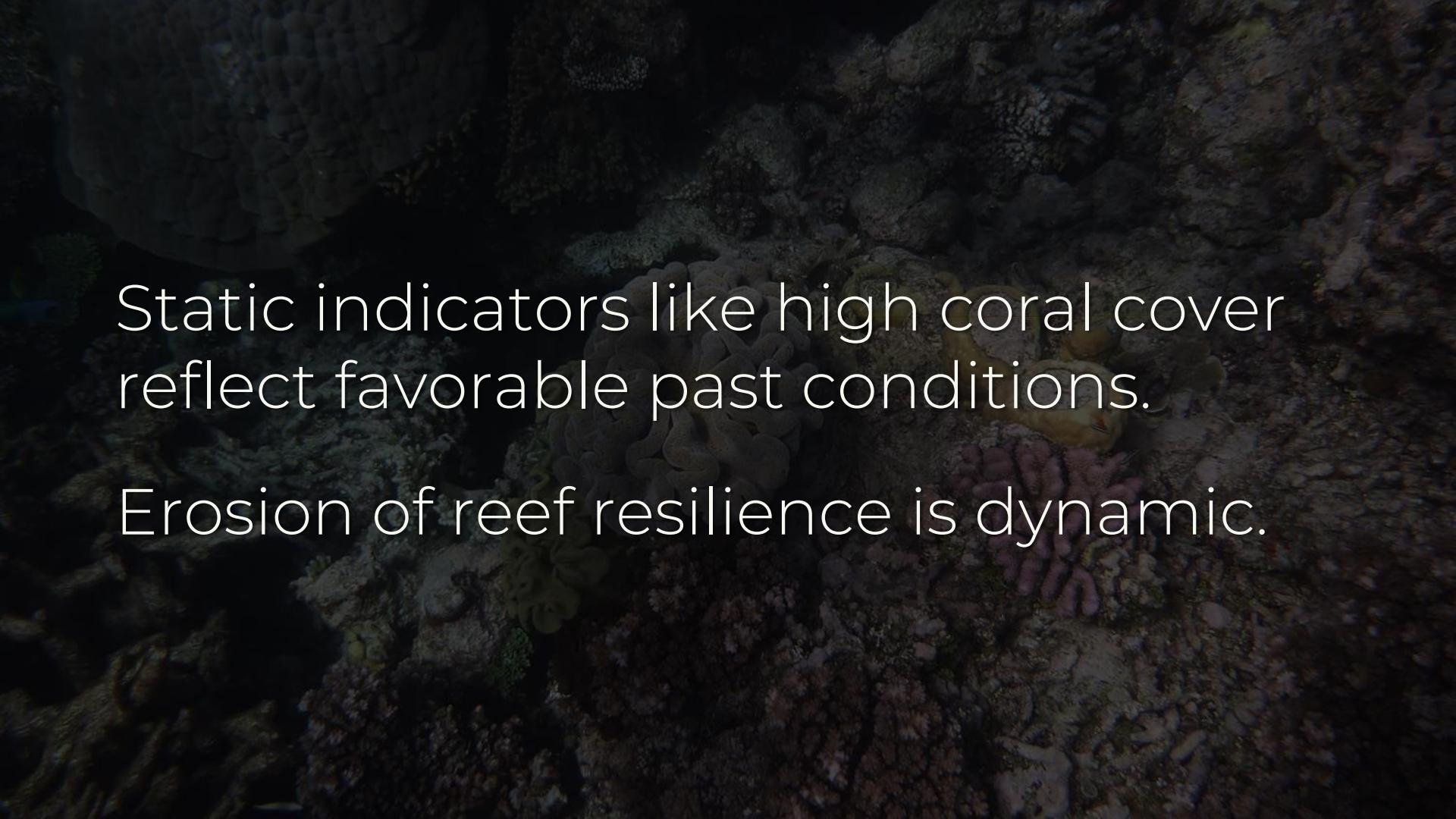
Robustness, Adaptability,  
Transformability

Resilience is a *journey*, not a singular,  
final destination

A dramatic painting depicting a shipwreck at sea. In the foreground, a small boat with several figures is visible, struggling against large, white-capped waves. The sea is depicted with dark, turbulent brushstrokes. In the background, a dark, silhouetted structure, possibly a ruined castle or a distant shore, sits atop a hill under a sky filled with heavy, dark clouds. The overall mood is one of despair and the power of nature.

Natural disaster resilience must  
assume failure of controls

What % of human development is in known at-risk disaster areas?

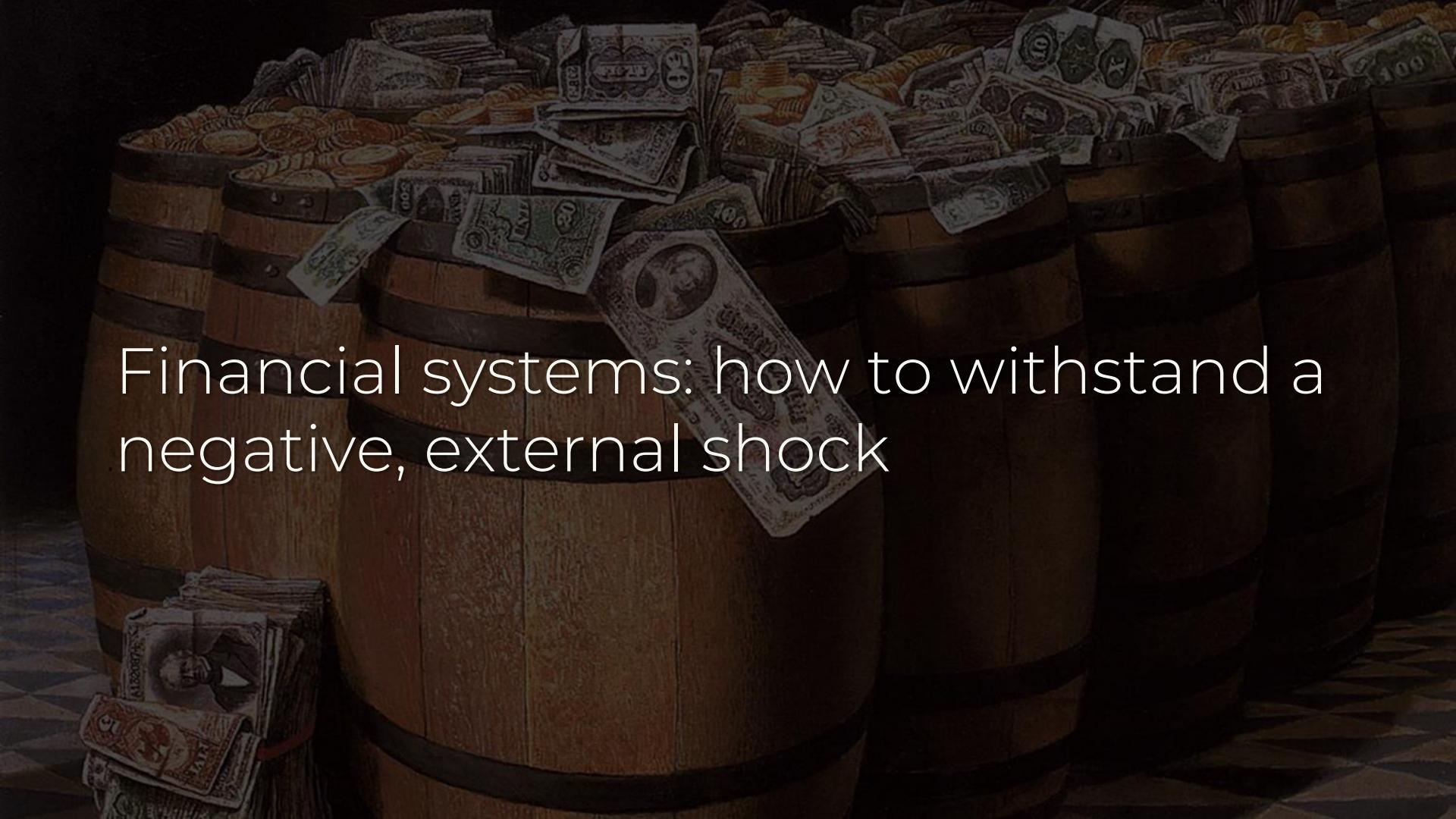
A vibrant underwater scene of a coral reef. The reef structure is complex, featuring various types of coral like Acropora and Pocillopora. Numerous small, colorful fish, possibly damselfish or wrasses, are scattered throughout the frame, swimming near the coral. The water is clear, allowing for a detailed view of the marine life and the intricate textures of the coral.

Static indicators like high coral cover reflect favorable past conditions.

Erosion of reef resilience is dynamic.

Ongoing stress like ocean warming  
makes coral less resilient in the face of  
cyclones or coral bleaching events

How many ongoing stressors exist?  
How frequent are acute stressors?



Financial systems: how to withstand a negative, external shock

In a financial network, at what point does one default lead to a cascade?



High connectivity & large fraction of  
contagious links = riskiest nodes

Interconnectivity helps financial systems... until it hurts.

Not all transactions are equal: some  
create potential insolvency cascades

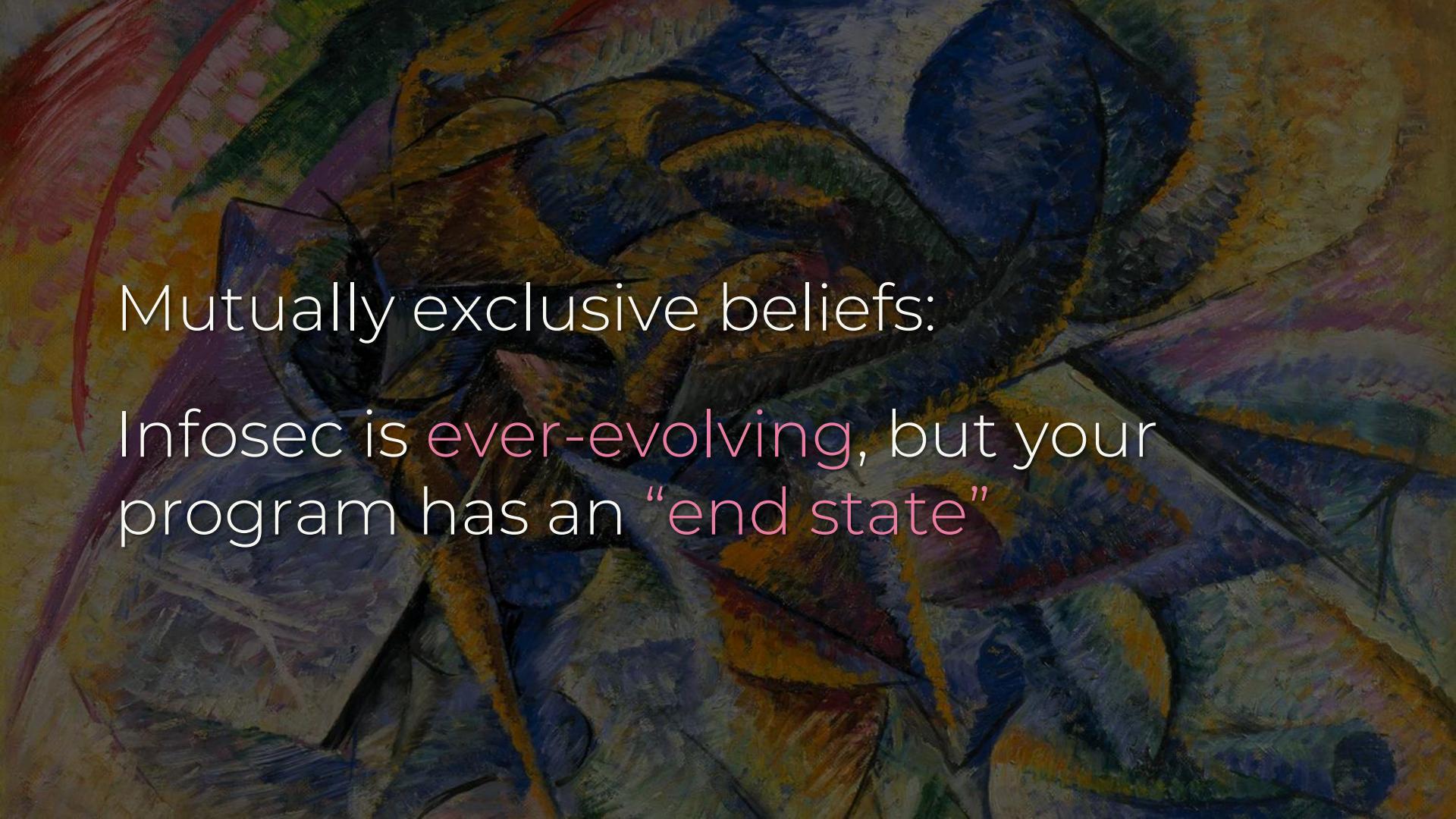
# Systemic Risk Tax (SRT): tax transactions based on systematic risk

Source: "Incentivizing Resilience in Financial Networks," Leduc & Thurner

# Resilience Metrics in DevOps

“Maturity models are for chumps.”

– Dr. Nicole Forsgren @nicolefv

The background of the slide features a vibrant, abstract painting with thick brushstrokes. It consists of various colors including red, yellow, green, blue, and purple, creating a dynamic and textured composition.

Mutually exclusive beliefs:  
Infosec is ever-evolving, but your  
program has an “end state”

*Accelerate:* rigorous data analysis of  
which metrics correlate with success

Successful measures: global (org-level) results & outcomes (vs. outputs)



Global: intra-org teams shouldn't be pitted against each other

Outcomes: what actually helps your org? Lots of things don't

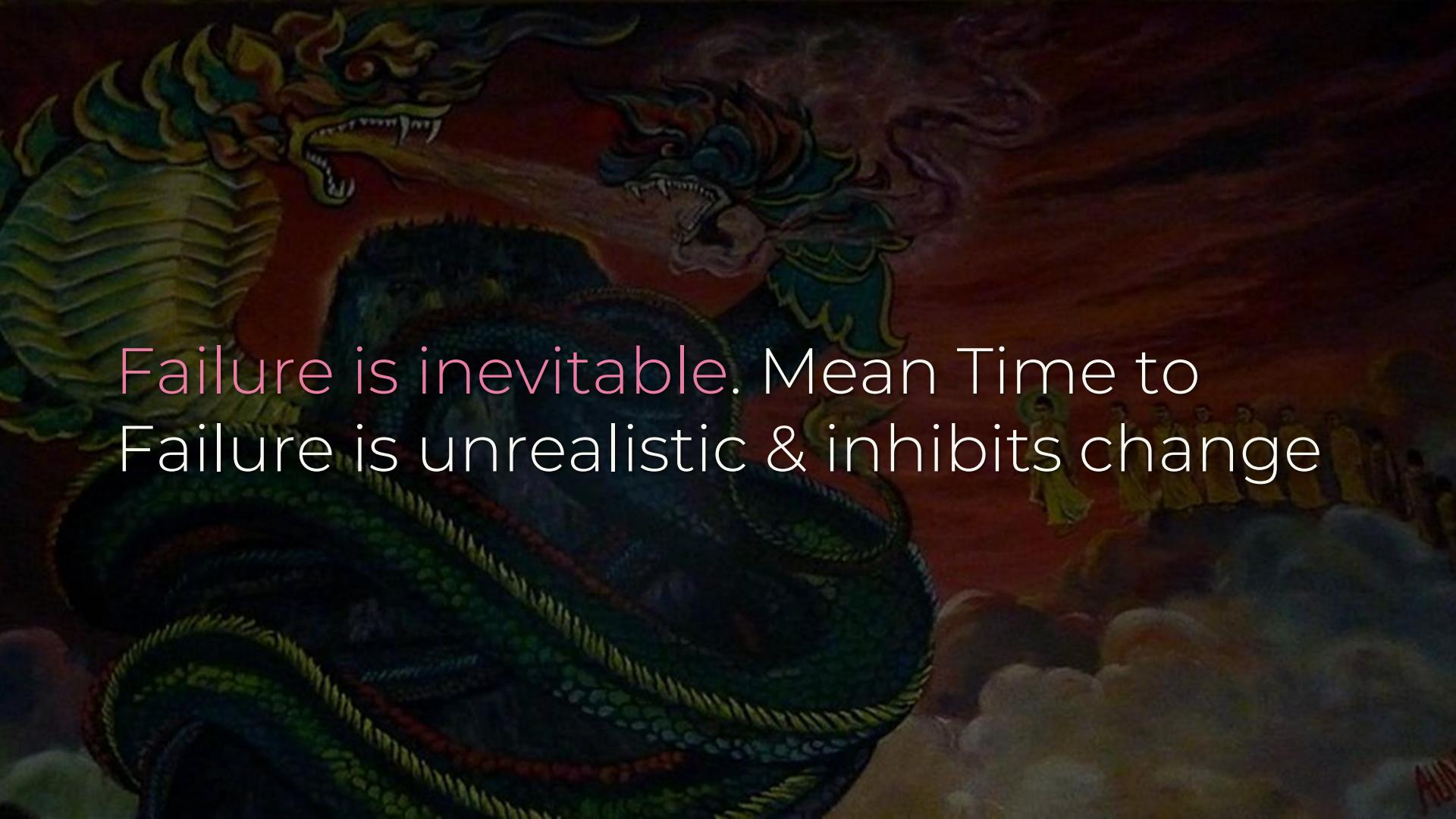
Lead time, release frequency, MTTR



Lead time: time to design a feature +  
time to deliver a feature

Release frequency: proxy for “batch size” (ie amount produced at a time)

Mean Time to Recovery: how quickly  
can service be restored?

A traditional Chinese dragon painting, featuring two heads with sharp fangs and scales, breathing fire or smoke. The dragon's body is long and coiled, with intricate patterns on its scales. The background is dark with swirling clouds.

Failure is inevitable. Mean Time to  
Failure is unrealistic & inhibits change

No tradeoff between improving performance vs. stability or quality

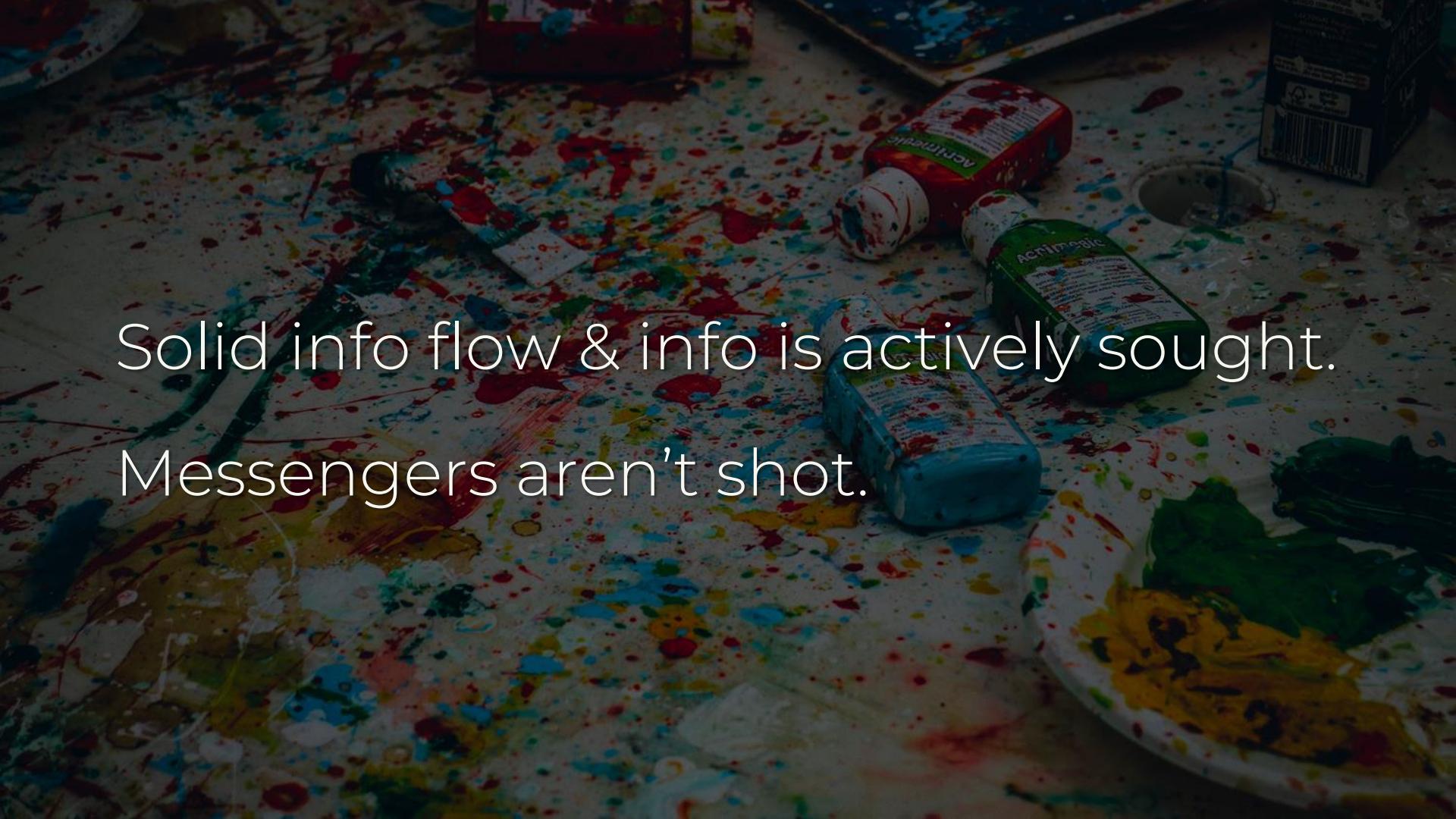
High performers:

Deploy frequency: on-demand

Lead time: <1 hour

MTTR: <1 hour

Westrum model of culture: power-,  
rule-, or mission-oriented

The background of the image shows a floor completely covered in a chaotic, colorful mess of paint splatters in various colors like red, blue, green, and yellow. Scattered across this painted surface are several art supplies, including several plastic containers of acrylic paint in different colors, some with their lids off, and a few paintbrushes. The scene suggests a creative, messy environment.

Solid info flow & info is actively sought.  
Messengers aren't shot.

Responsibilities are shared.

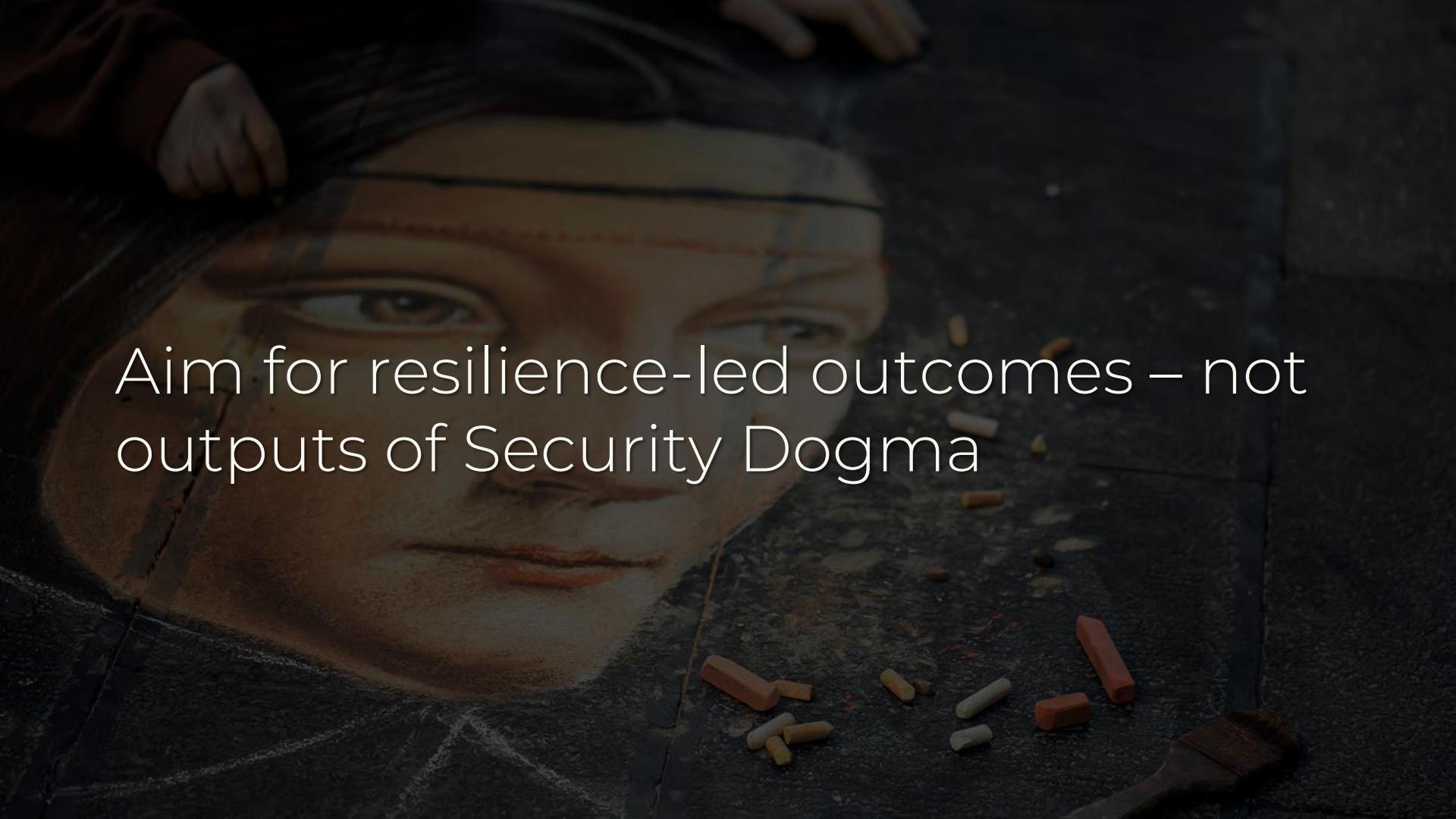
Cross-team collaboration is rewarded.

Failures are treated as learning opportunities for improvement.

How many (or few) of these match  
your infosec culture?

# Measuring InfoSec Programs

Your program's goal isn't maturity –  
it's org-level continuous resilience



Aim for resilience-led outcomes – not outputs of Security Dogma

Infosec resilience means a **flexible**  
system that can **absorb** an attack and  
**reorganize** around the threat.

Flexibility: can your program serve  
your org's needs in the way it needs?

Global results: zealots combatting the  
“unenlightened” is unhealthy

Prioritizing infosec vs. org-level can lead to inhibition of innovation



Measure impact both ways: improved security vs. tighter bottleneck

Positive: reduction in number of security fixes per release

Negative: increase in engineering time spent using security tools

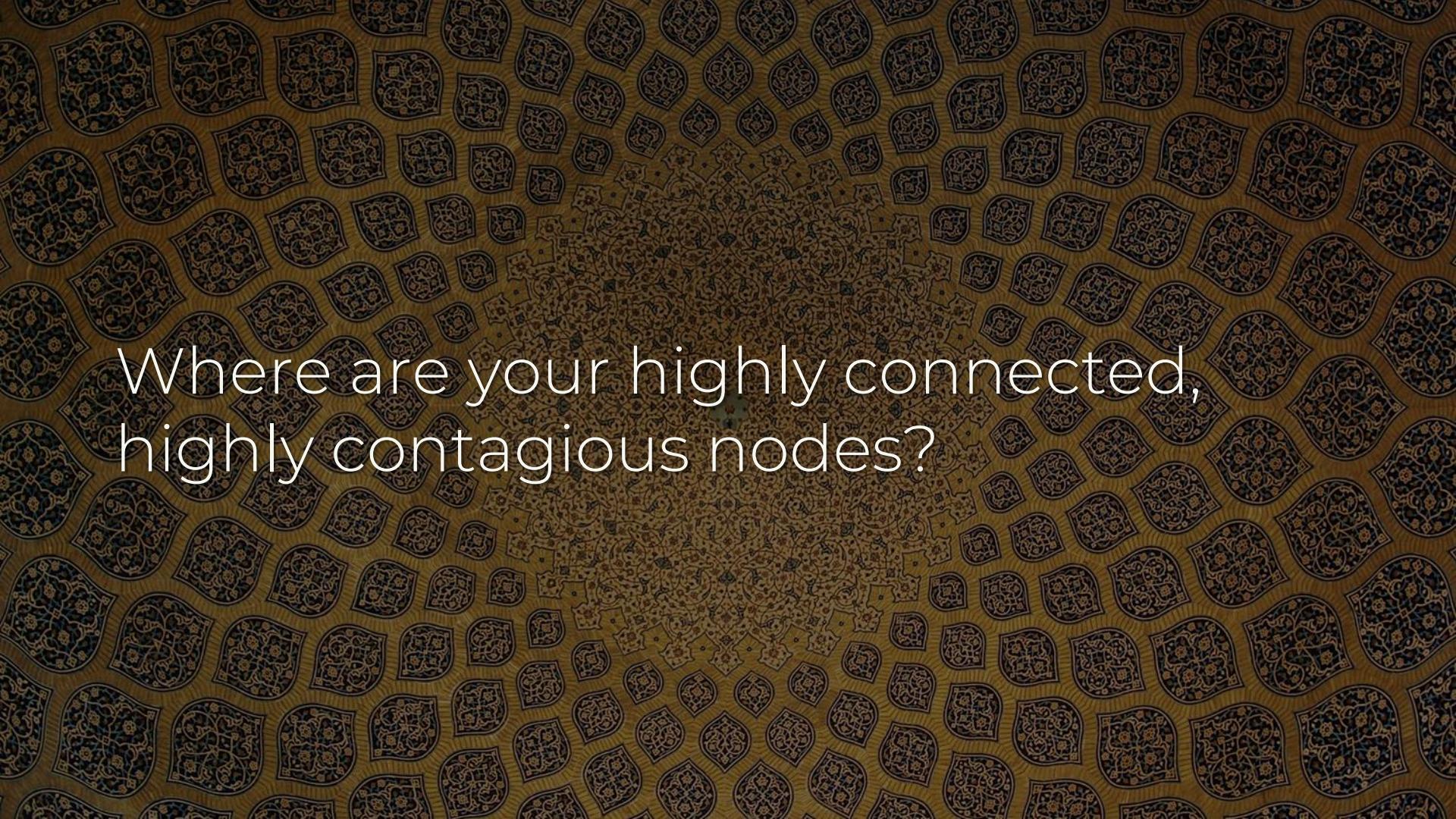
High-performing dev orgs spend 50% less time remediating security issues

Source: *Accelerate* by Forsgren, et al., 2018

Mean Time for Security Reviews

Mean Time for Threat Modelling

Absorbing an attack: reducing  
contagion, adapting efficiently



Where are your highly connected,  
highly contagious nodes?

Measure ongoing amplification ratio:  
pwn of node\_1 leads to X total dmg

Track ongoing stressors like complexity & employee turnover

Impact of a new vuln or breach  
depends on erosion by ongoing stress

Mean Time to Remediation: how quickly do you resolve an incident?

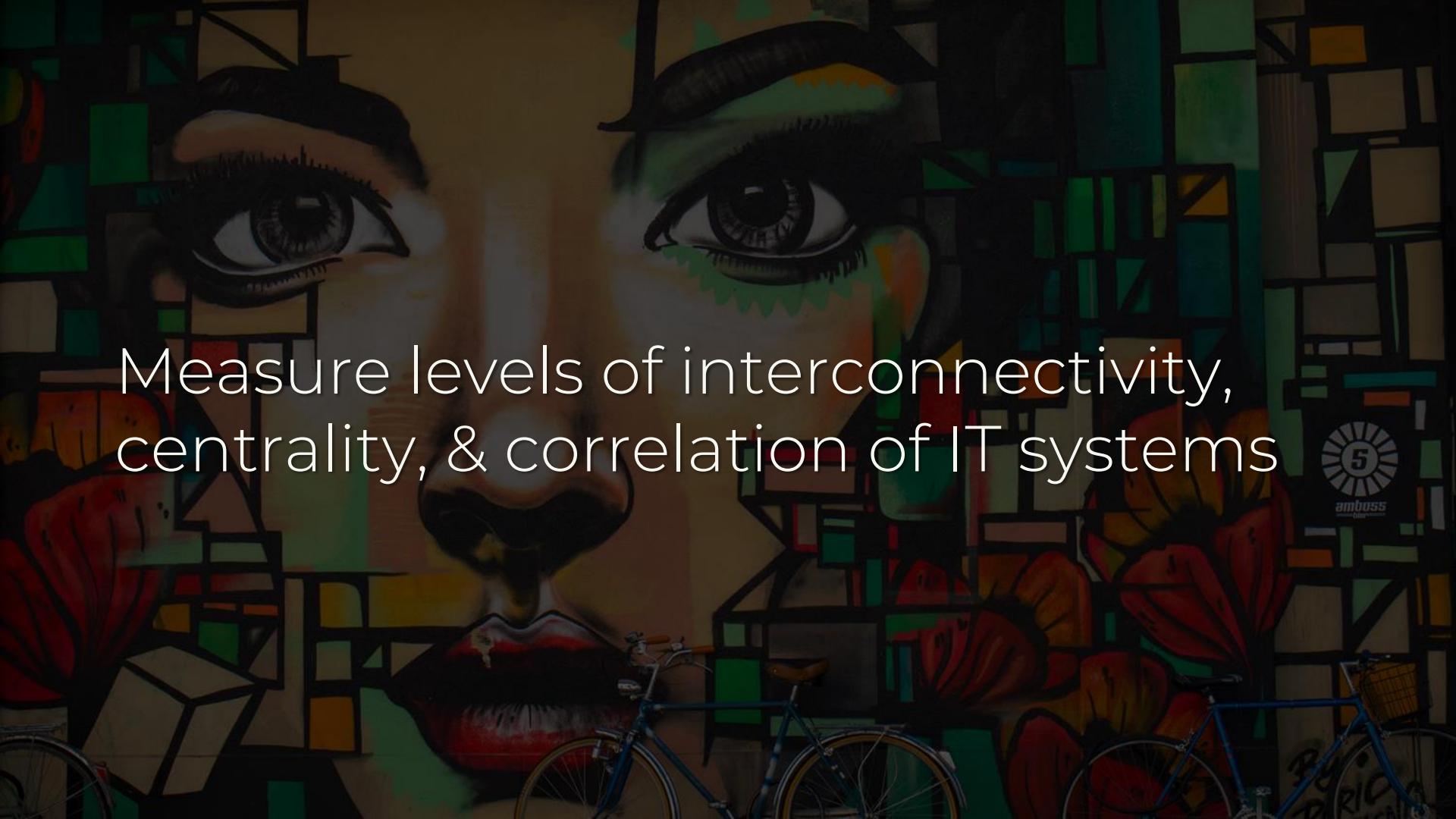
Mean Time to Failure (incident) can prioritize unhealthy stagnation

Deploy frequency of config mgmt  
changes (firewall rules, patches, etc.)

Reorganize around the threat: can you transform & innovate?

SRT for tech: incentivize resiliency by  
throttling cascade-creating nodes

As in both finance & DevOps: there's no single, optimal architecture

A vibrant mural on a building wall depicts a woman's face with large, expressive eyes. The background is filled with geometric shapes, colors, and a blue bicycle in the foreground.

Measure levels of interconnectivity,  
centrality, & correlation of IT systems



5  
amboss

Acute stress \* interconnectivity =  
potential propagation of pwn (PPP)

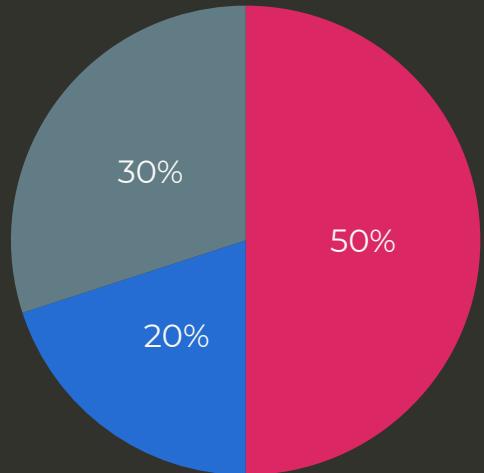
How is your security team's time  
being used?

SIEM maintenance = 30 hrs / month

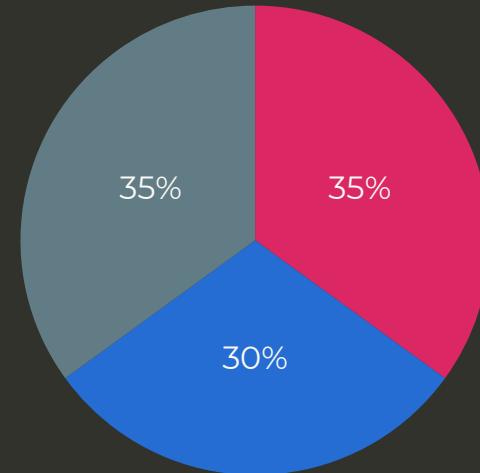
12.5% of work time = \$1k+ / month

Time usage: problem solving,  
firefighting, meetings & maintenance

# Good



# Bad



Security Innovation

Firefighting

Meetings & Maintenance

Suggested figures based on *Accelerate* by Forsgren, et al., 2018

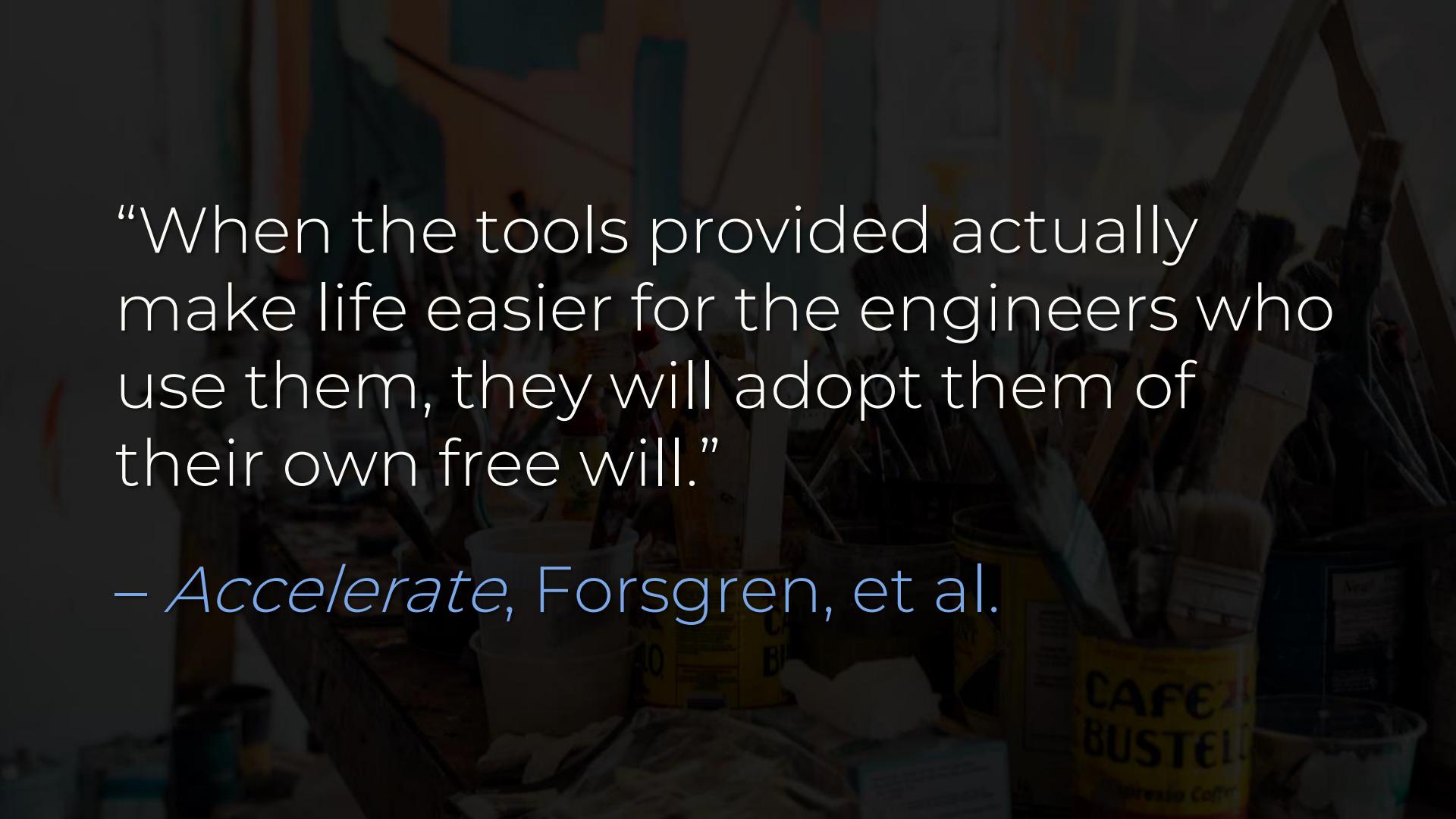
How strong is your culture? Are you actually mission-oriented?

Equifax blamed one person for failing to deploy a patch.

Don't do that.

It is never just one person or variable  
in a complex system

If “the user” or “devs” don’t security well, your infosec program is failing.

A dark, grainy photograph of a cluttered workspace. In the foreground, there are several white plastic containers with lids, some with yellow labels. One container has "CAFE BUSTE" and "Espresso Coffe" printed on it. Behind them, there are more containers, some with blue and red labels, and what appears to be a wooden ladder or scaffolding structure in the background.

“When the tools provided actually make life easier for the engineers who use them, they will adopt them of their own free will.”

– *Accelerate*, Forsgren, et al.

% of dev teams using appsec testing

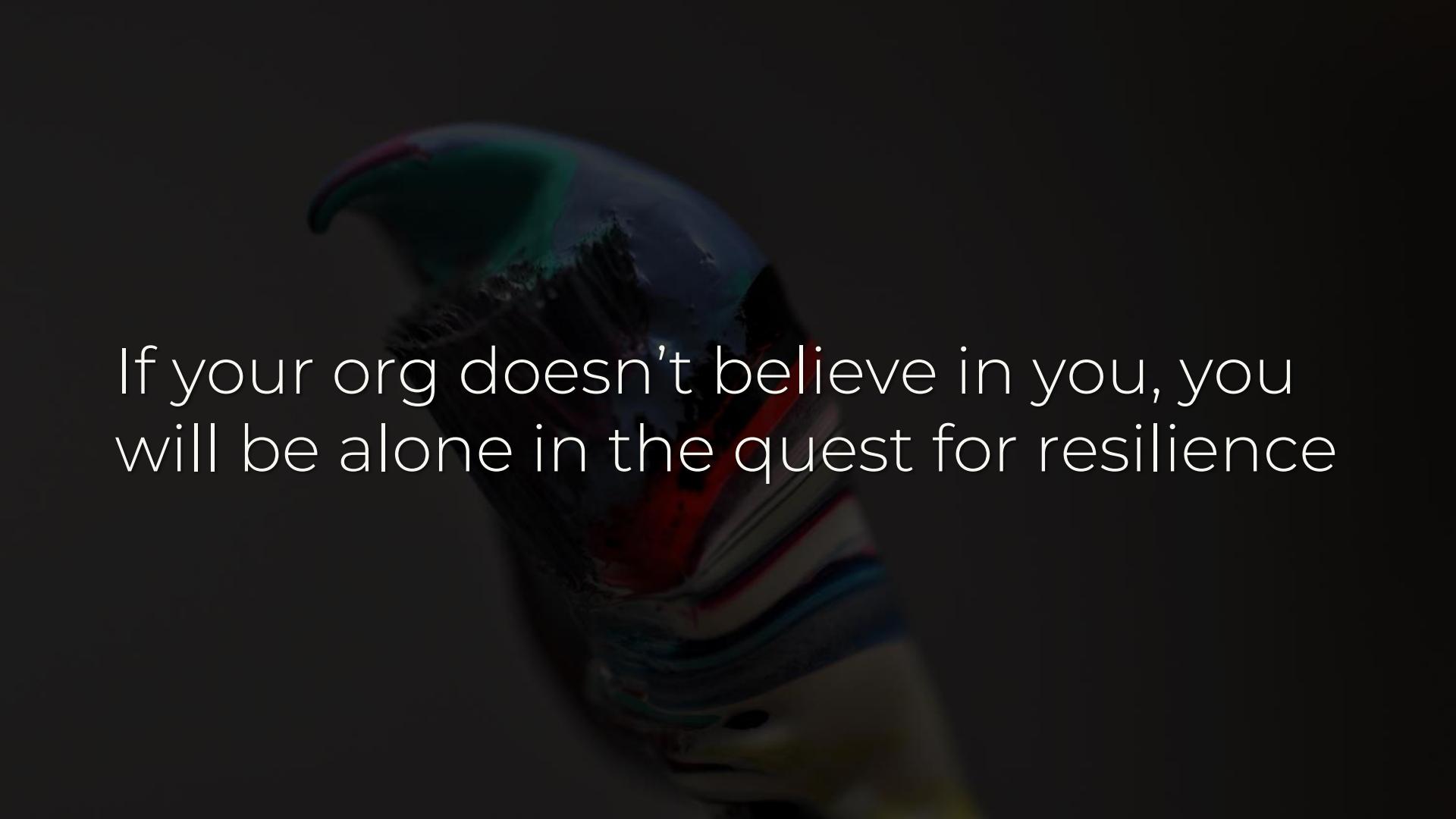
% 2FA usage across departments

# of security support tickets filed

Net Promoter Score (NPS):  
Mathematical calc of satisfaction

Measure NPS among your colleagues  
& teams with whom you work

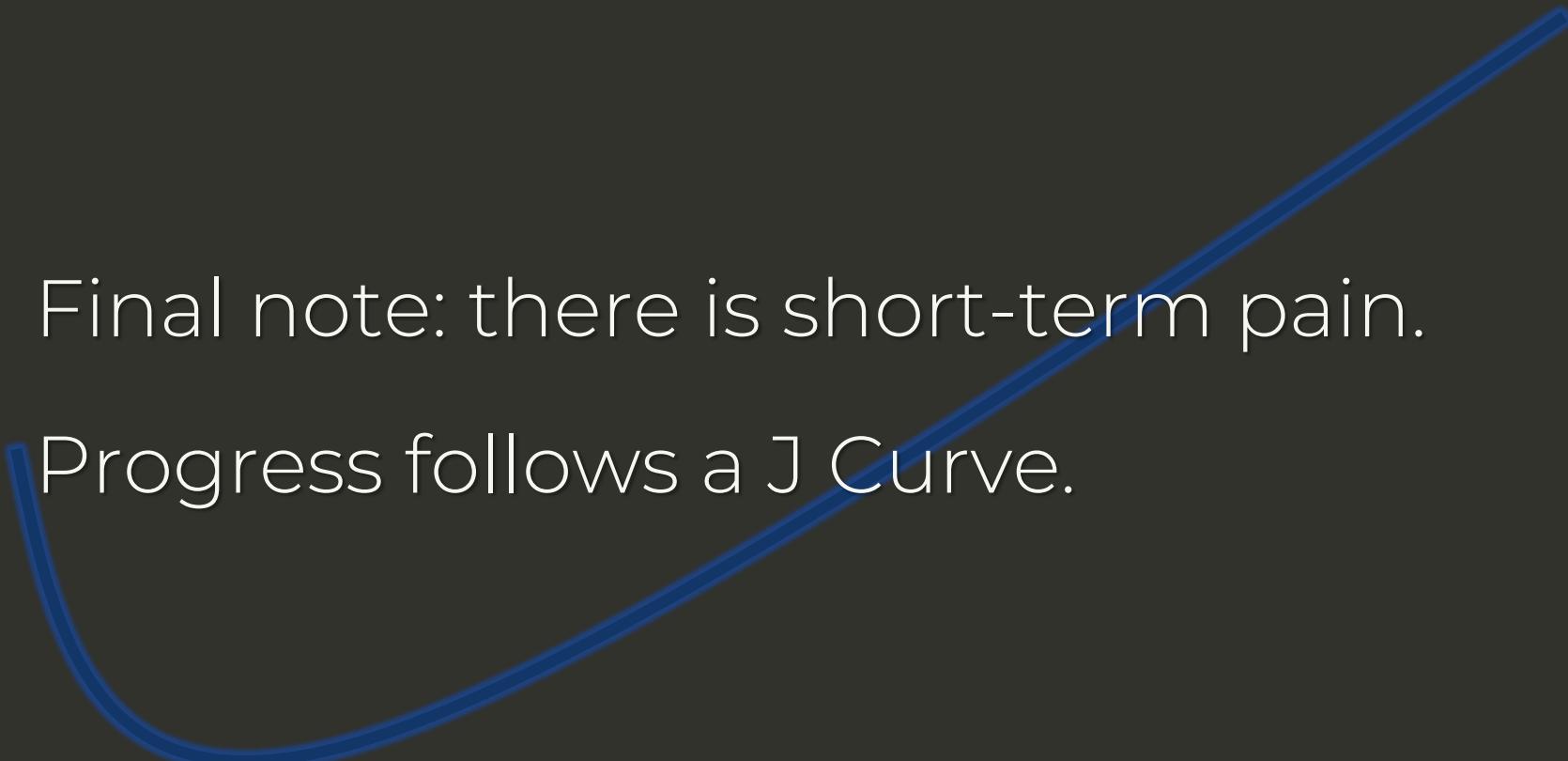
“How likely are you to recommend our security program to a friend?”

A close-up photograph of a person's head and shoulders. They are wearing a vibrant, multi-colored headband with a distinct green, blue, and red pattern. The person has dark hair and is looking downwards with a neutral expression. The background is dark and out of focus.

If your org doesn't believe in you, you  
will be alone in the quest for resilience

# Diversity: enhances adversarial analysis (true red teaming)

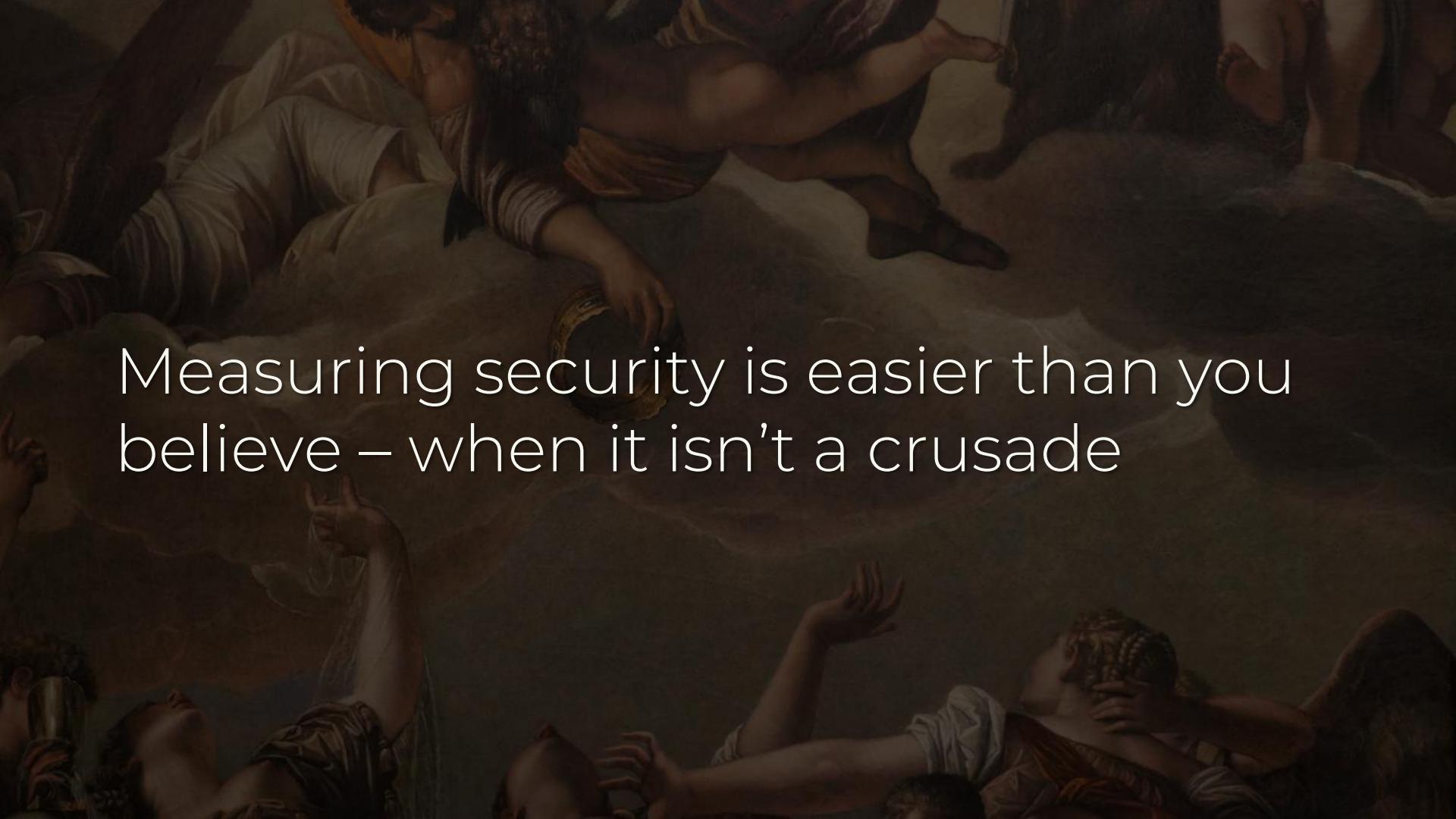
See “Red teaming probably isn’t for you” by Toby Kohlenberg



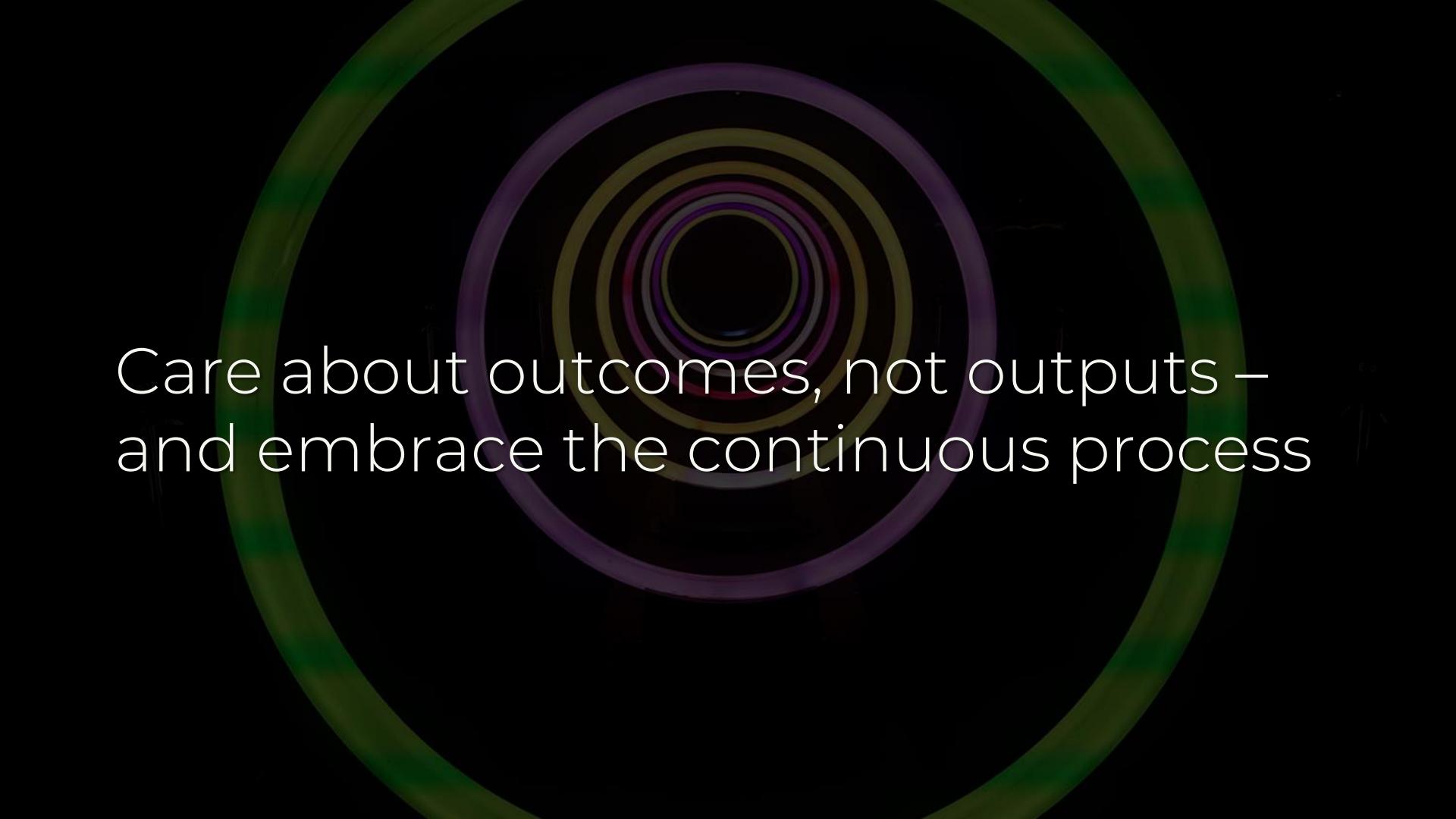
Final note: there is short-term pain.

Progress follows a J Curve.

# Conclusion

A dark, dramatic painting depicting a scene of conflict or death, possibly a crusade, with figures in traditional attire and a horse.

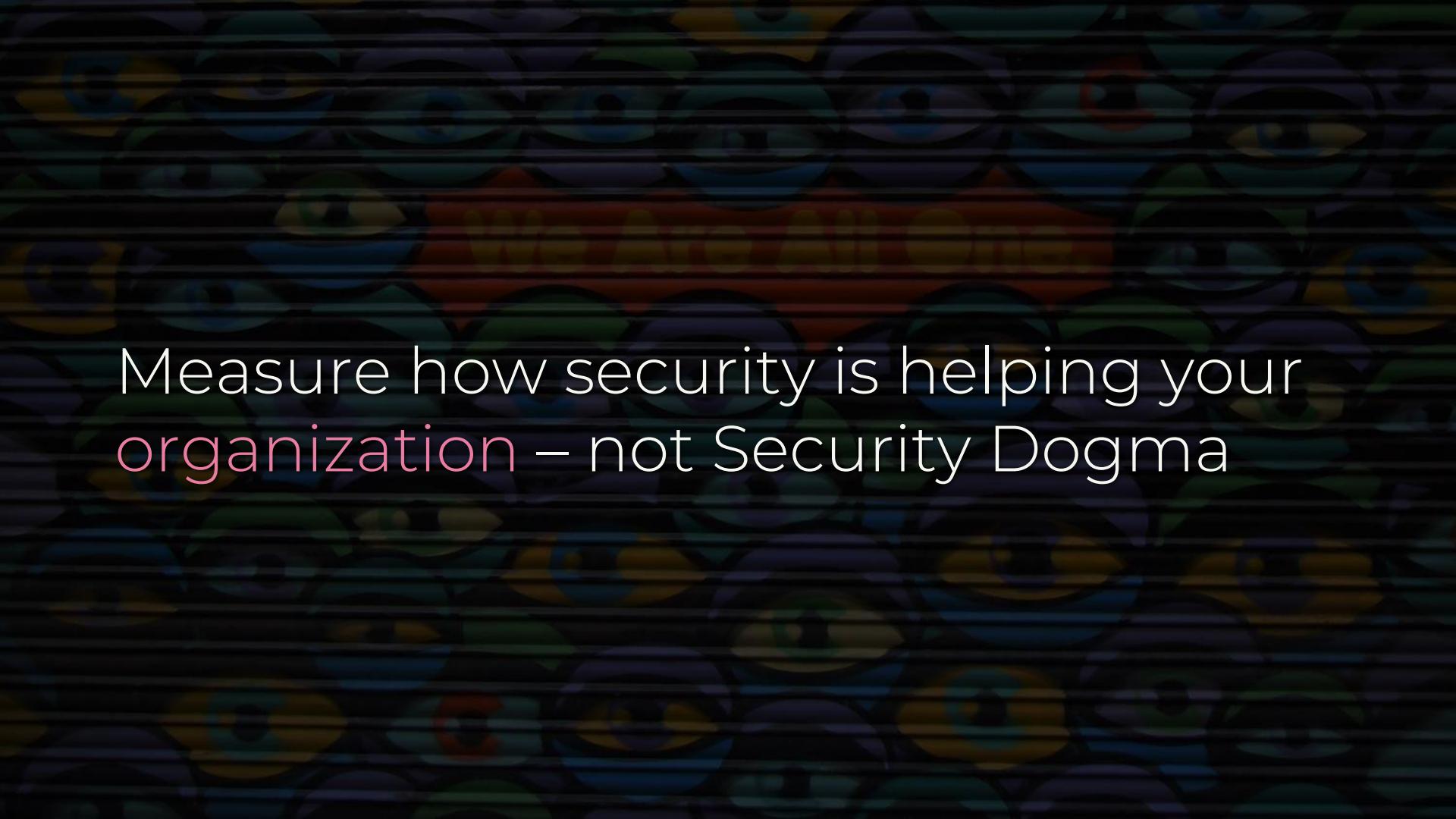
Measuring security is easier than you  
believe – when it isn't a crusade

The background of the slide features a dark, semi-transparent overlay with a series of concentric, glowing circles. These circles are composed of multiple thin, overlapping rings in shades of purple, blue, and green, creating a sense of depth and motion. They are centered in the upper half of the slide.

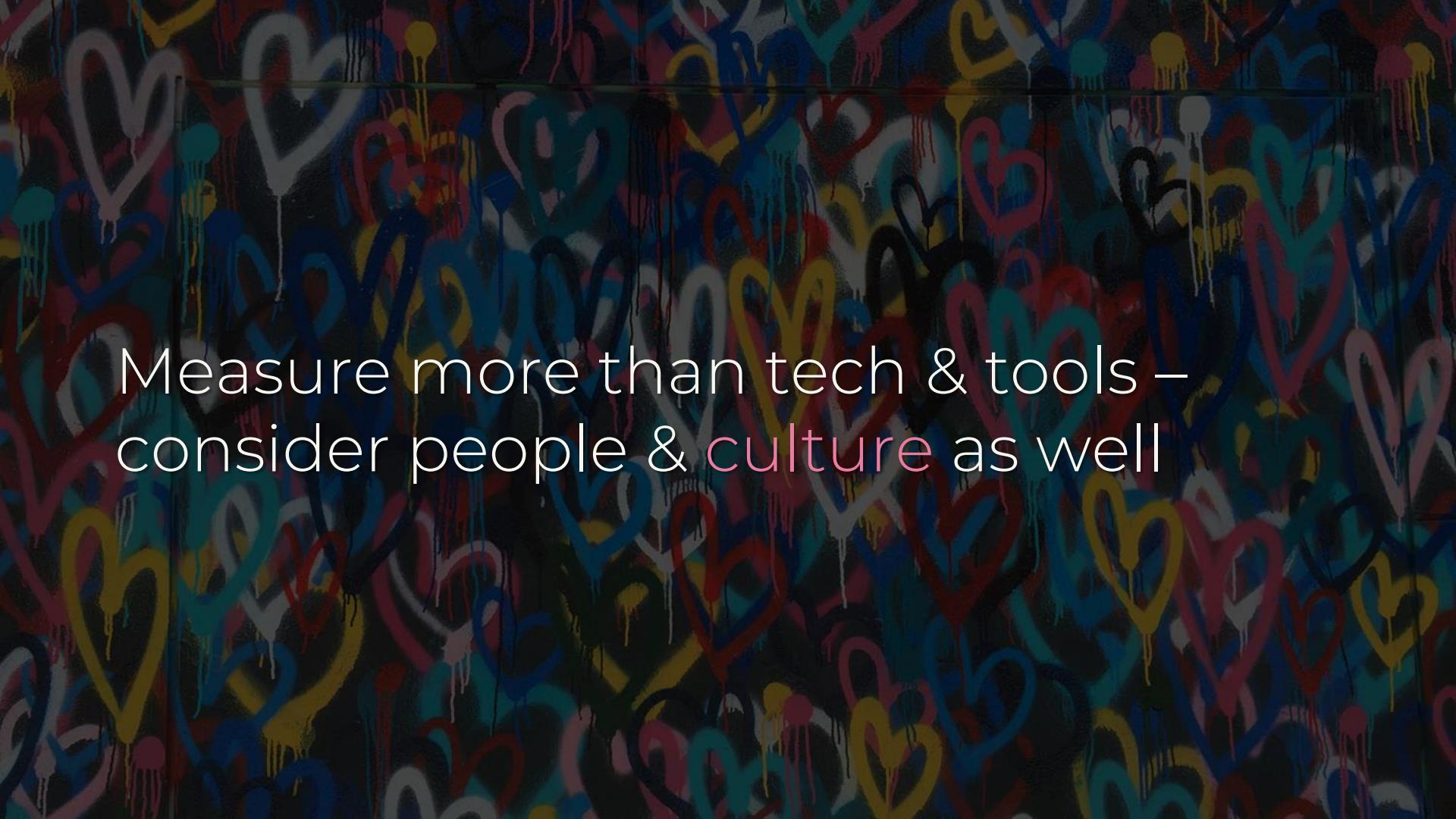
Care about outcomes, not outputs –  
and embrace the continuous process



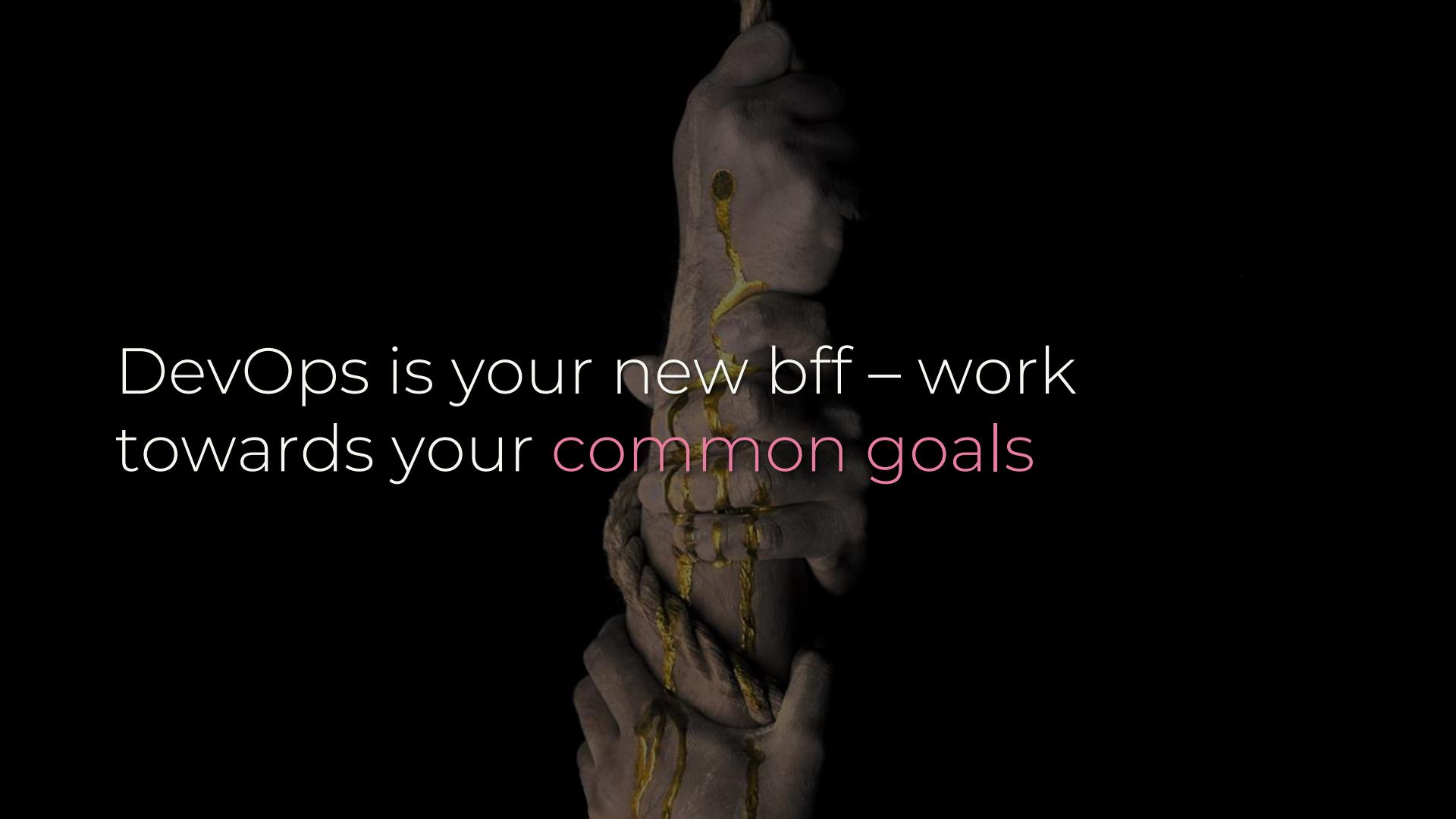
Measure resilience – flexibility,  
adaptability, transformability



Measure how security is helping your organization – not Security Dogma



Measure more than tech & tools –  
consider people & culture as well

A close-up photograph of two hands clasped together. A thick, yellowish liquid, resembling paint or oil, is dripping down the fingers and pooling between them. The hands are set against a dark, neutral background.

DevOps is your new bff – work  
towards your common goals



“Have no fear of perfection – you'll never reach it.”

– Salvador Dalí



@swagitda\_



/in/kellyshortridge



kelly@greywire.net

# Suggested Reading

- [Accelerate](#) by Forsgren, et al., 2018
- ["Are We There Yet? Signposts On Your Journey to Awesome,"](#) Forsgren, 2017
- "Incentivizing Resilience in Financial Networks," Leduc & Thurner, 2016
- ["It's Not Just Semantics: Managing Outcomes Vs. Outputs," HBR,](#) 2012
- "Operationalizing resilience for adaptive coral reef management under global environmental change," Anthony, et al., 2015
- ["Red Pill of Resilience,"](#) Shortridge, 2017
- ["Red teaming probably isn't for you,"](#) Kohlenberg, 2017
- "Resilience to Contagion in Financial Networks," Amini, et al., 2013
- "A strategy-based framework for assessing the flood resilience of cities: a Hamburg case study," Restemeyer, et al., 2015
- "Systemic Risk and Stability in Financial Networks," Acemoglu, et al., 2015