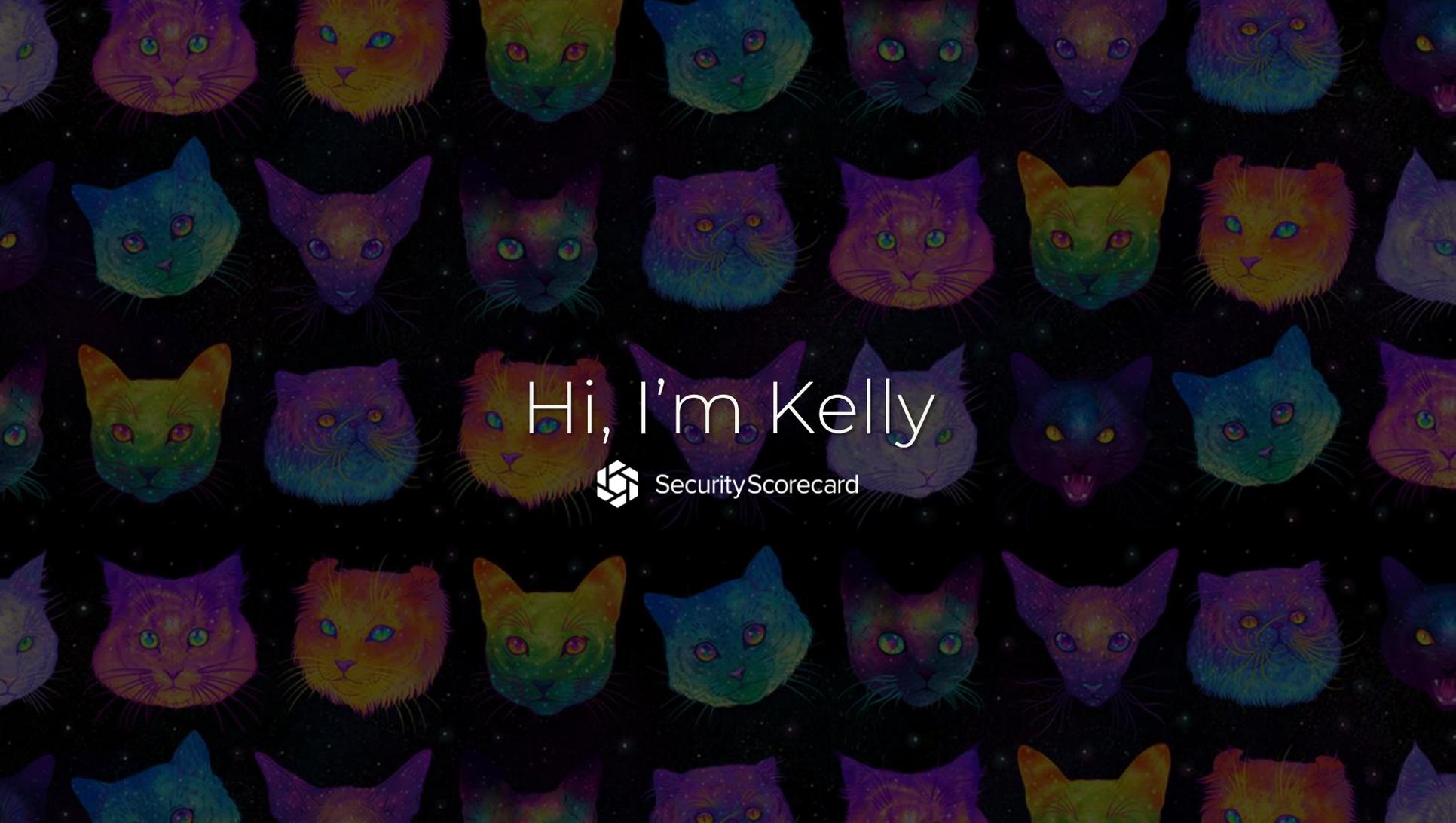


A close-up, slightly blurred photograph of a watercolor palette with various colored wells. The colors include shades of green, yellow, brown, blue, and purple. A paintbrush is visible on the right side, resting on one of the wells. The overall lighting is soft and artistic.

Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda_)

AusCERT 2018



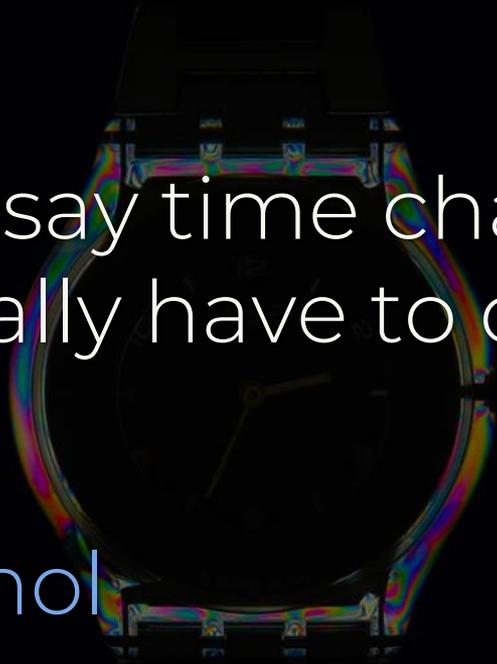
Hi, I'm Kelly

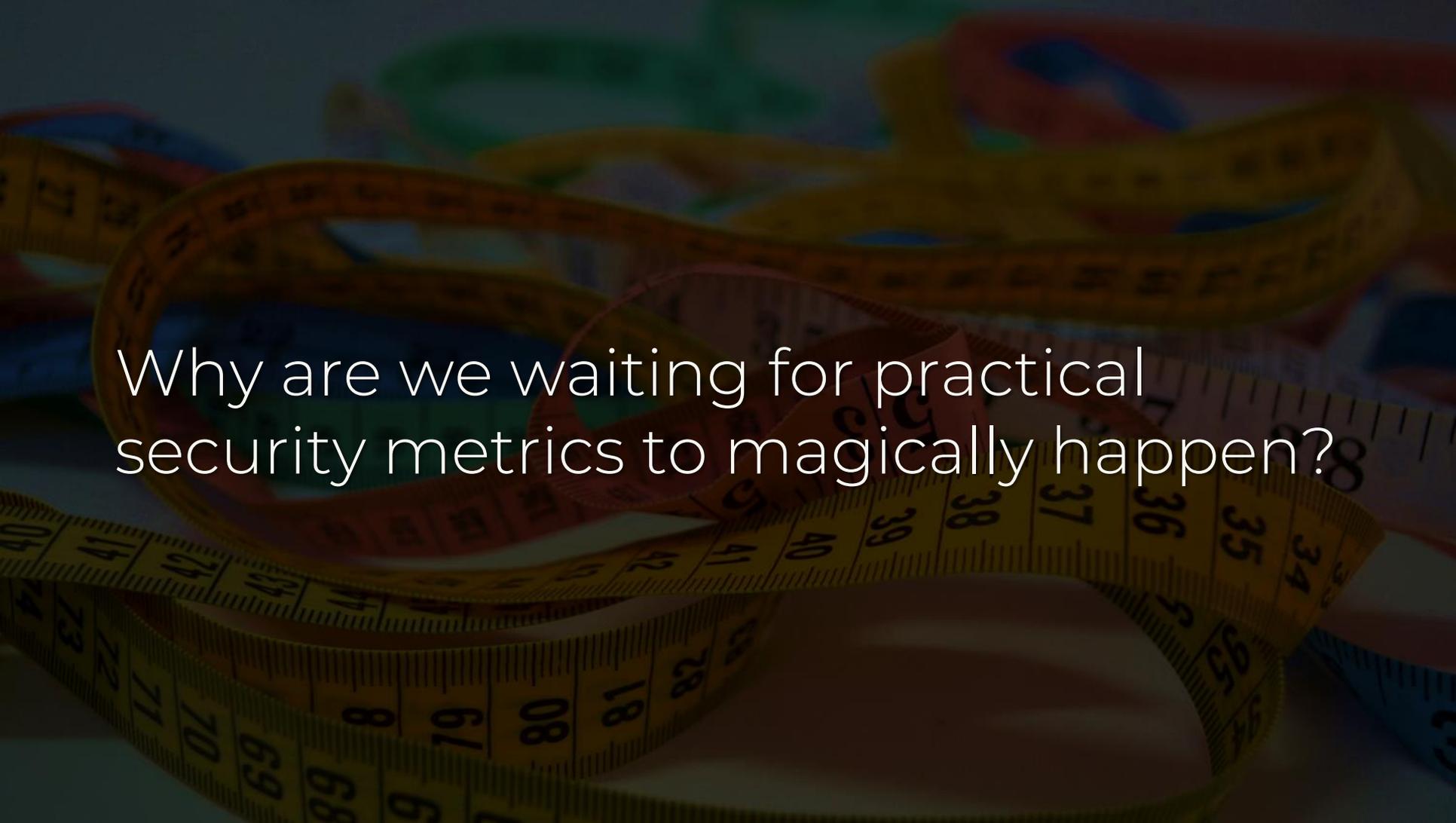


SecurityScorecard

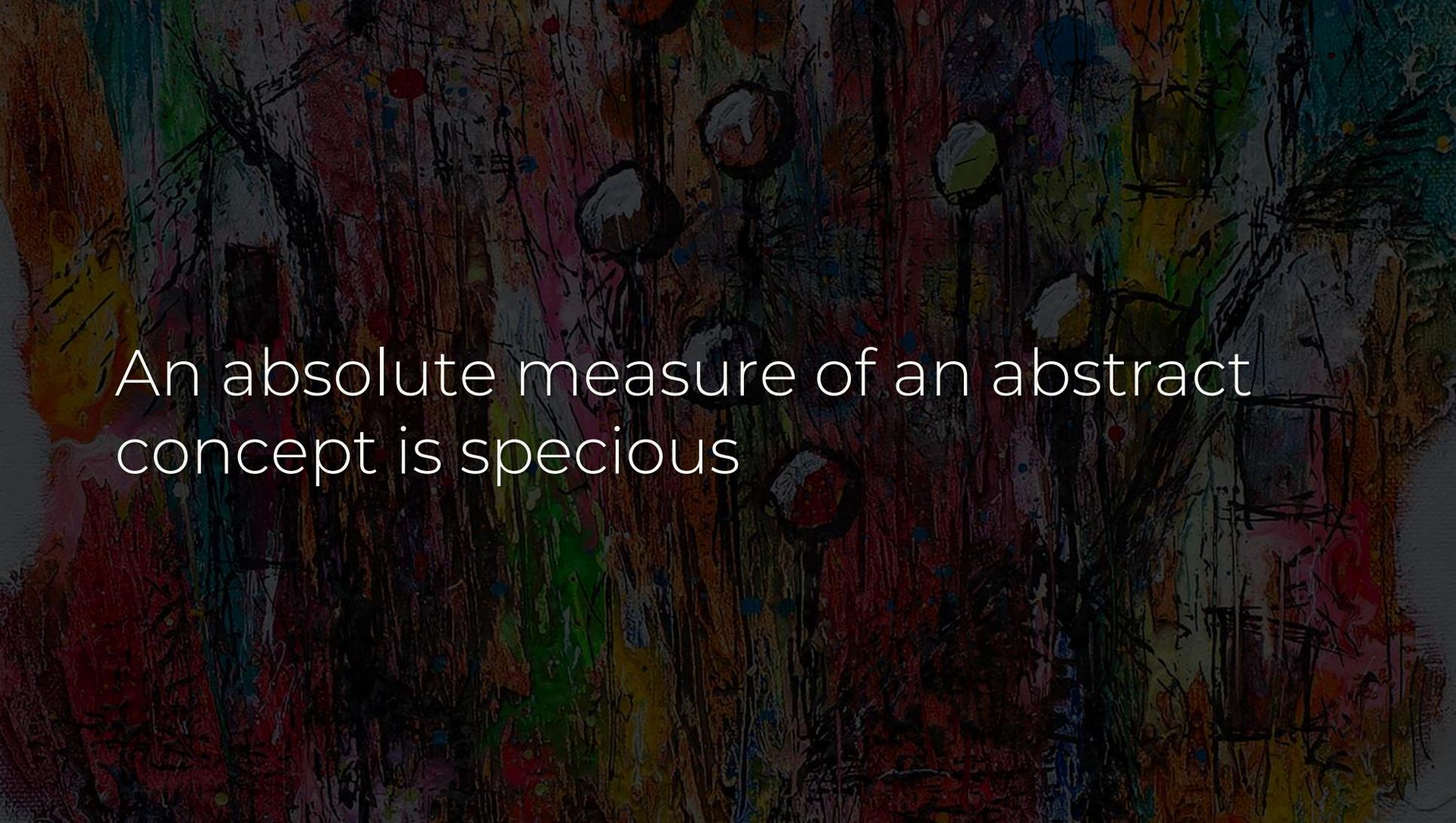
“They always say time changes things,
but you actually have to change them
yourself.”

— Andy Warhol

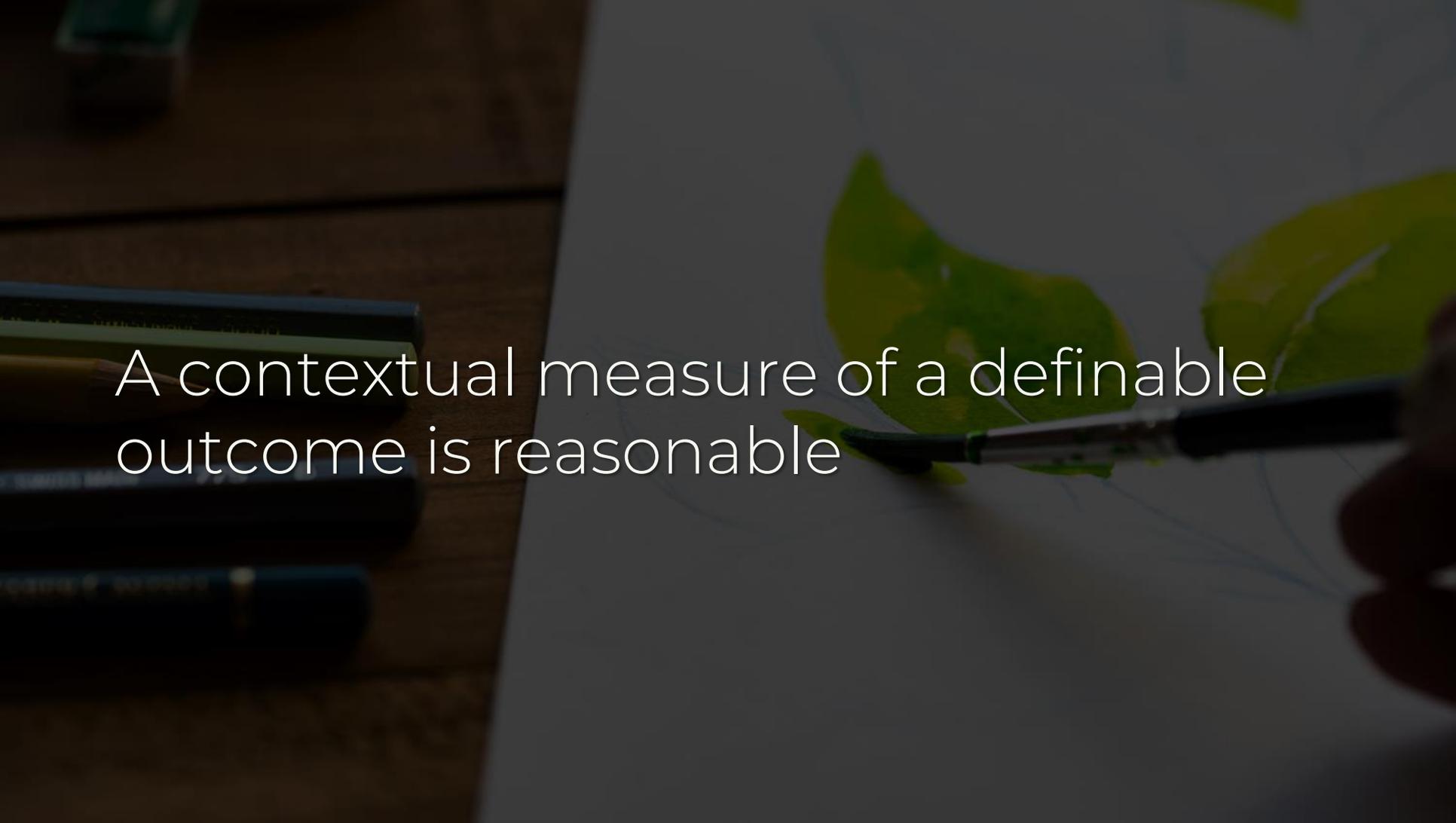




Why are we waiting for practical security metrics to magically happen?

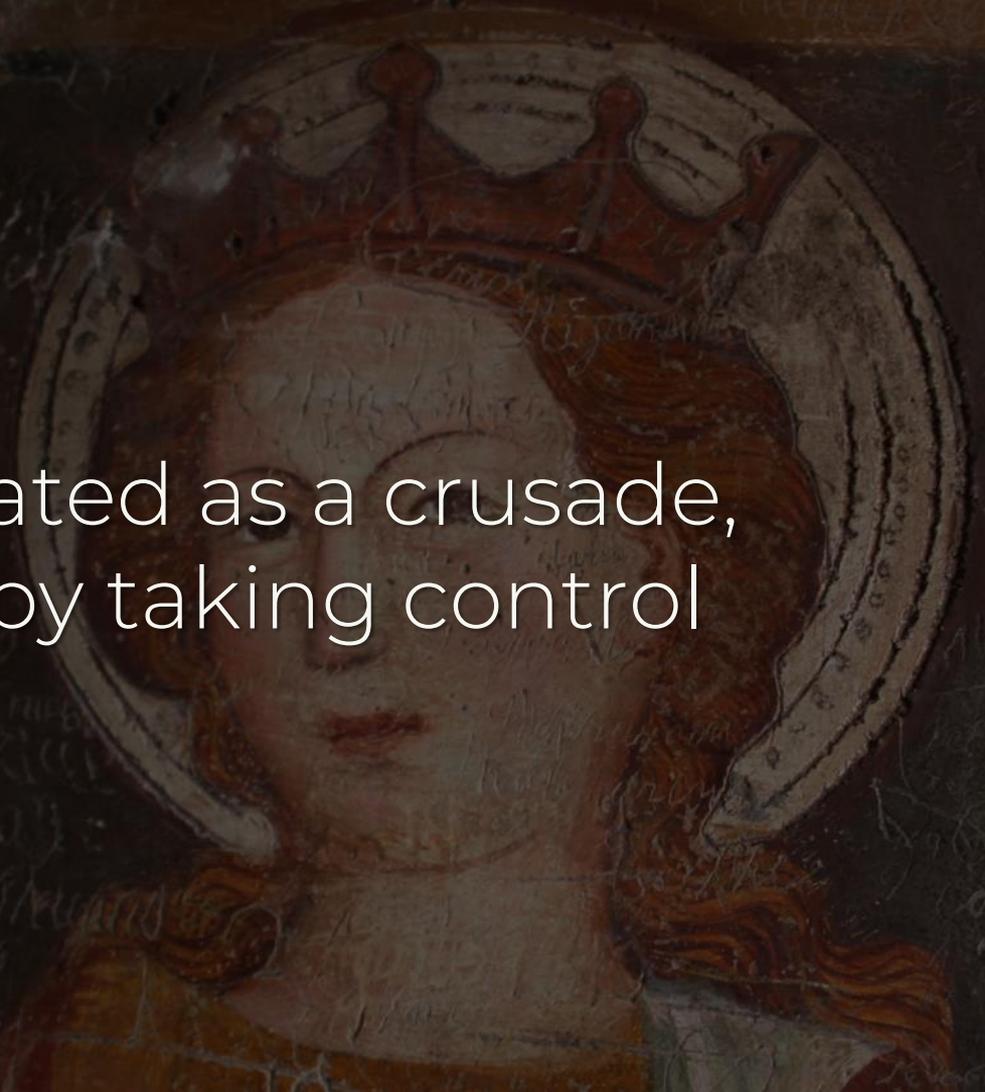
An abstract painting with a dark, textured background. The composition is filled with vertical, expressive brushstrokes in various colors including red, green, yellow, and blue. Several dark, circular shapes are scattered across the canvas, some appearing to be painted over or integrated into the existing strokes. The overall effect is one of dynamic energy and complex layering.

An absolute measure of an abstract
concept is specious



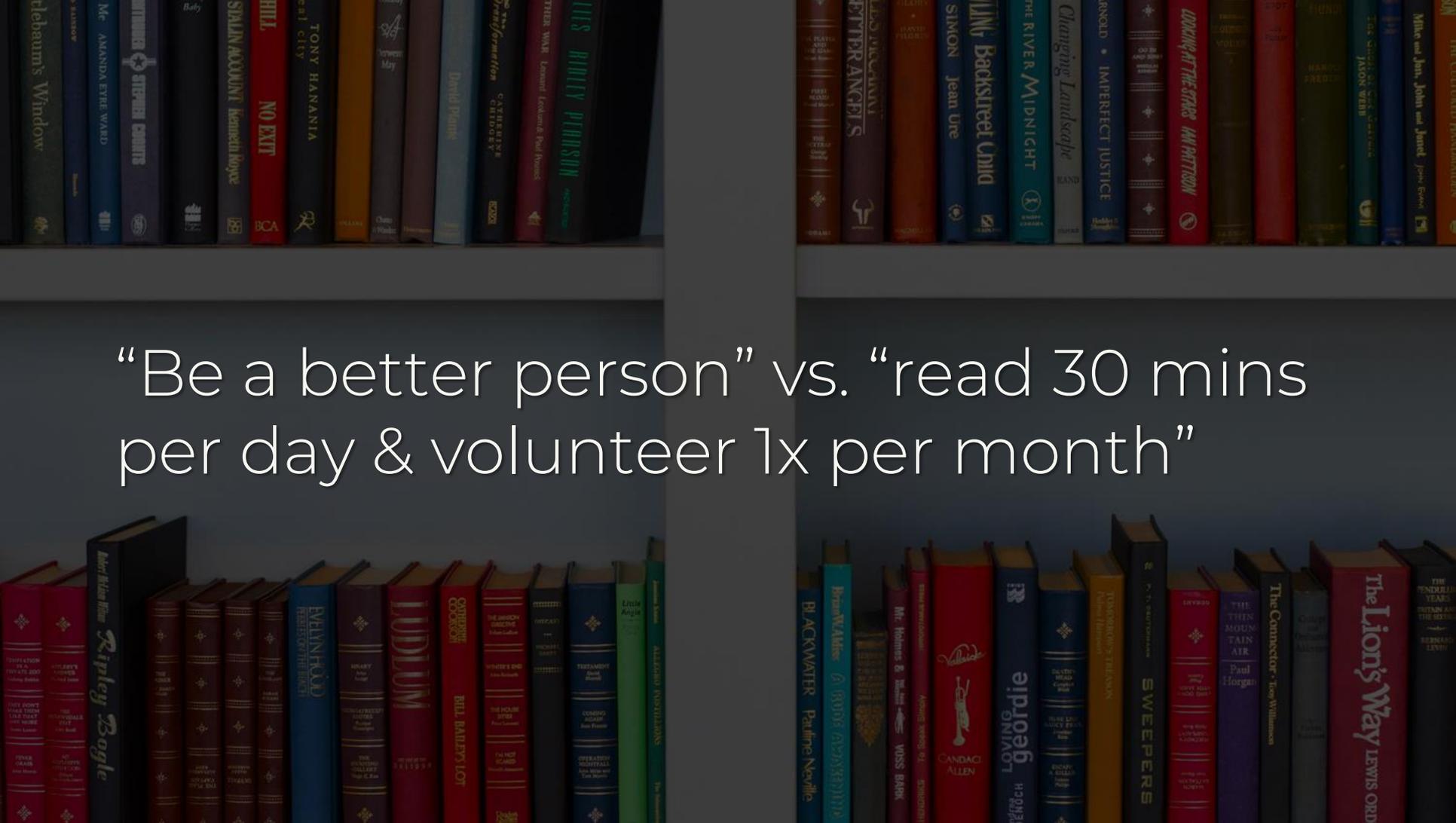
A contextual measure of a definable
outcome is reasonable

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

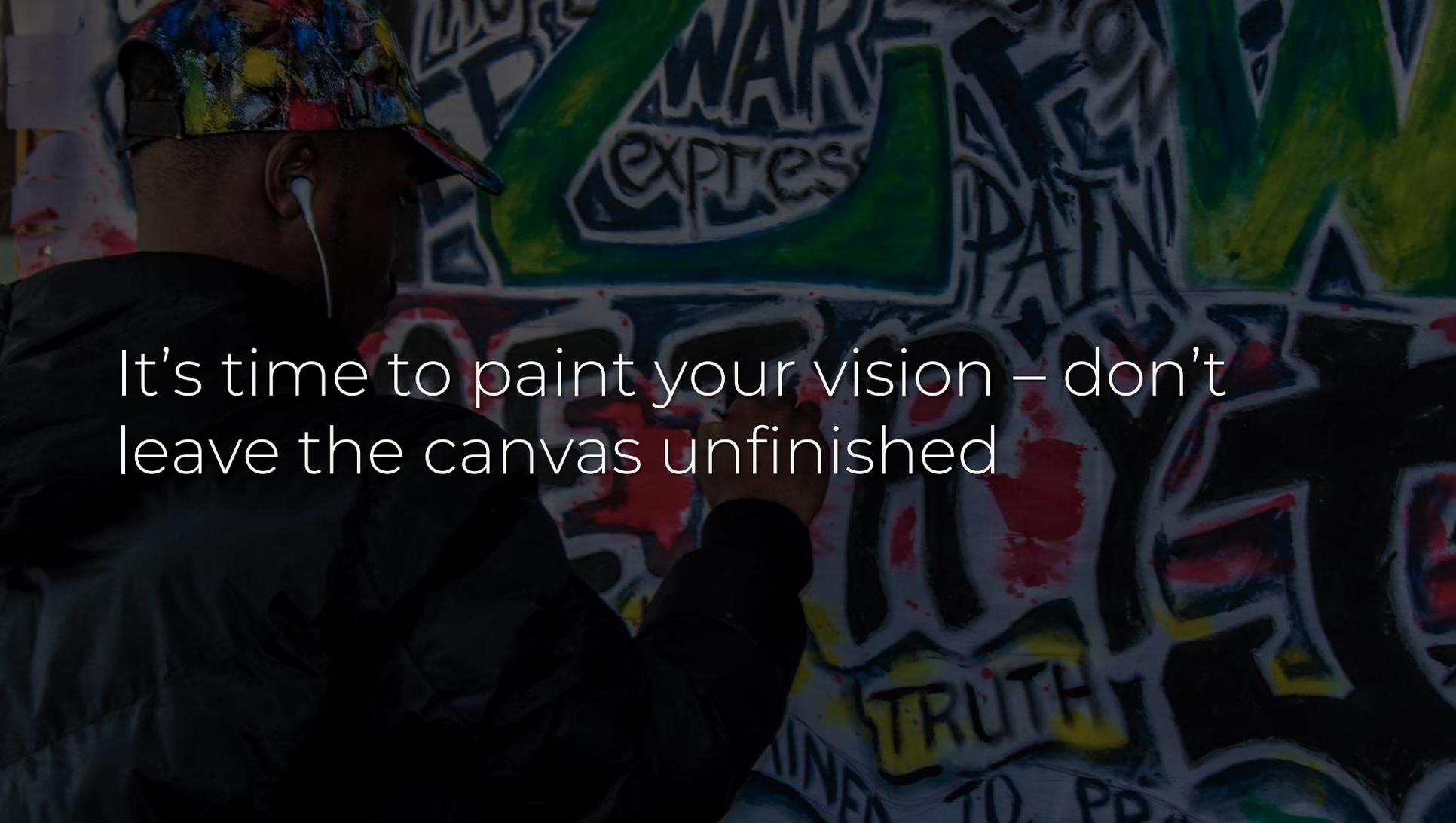




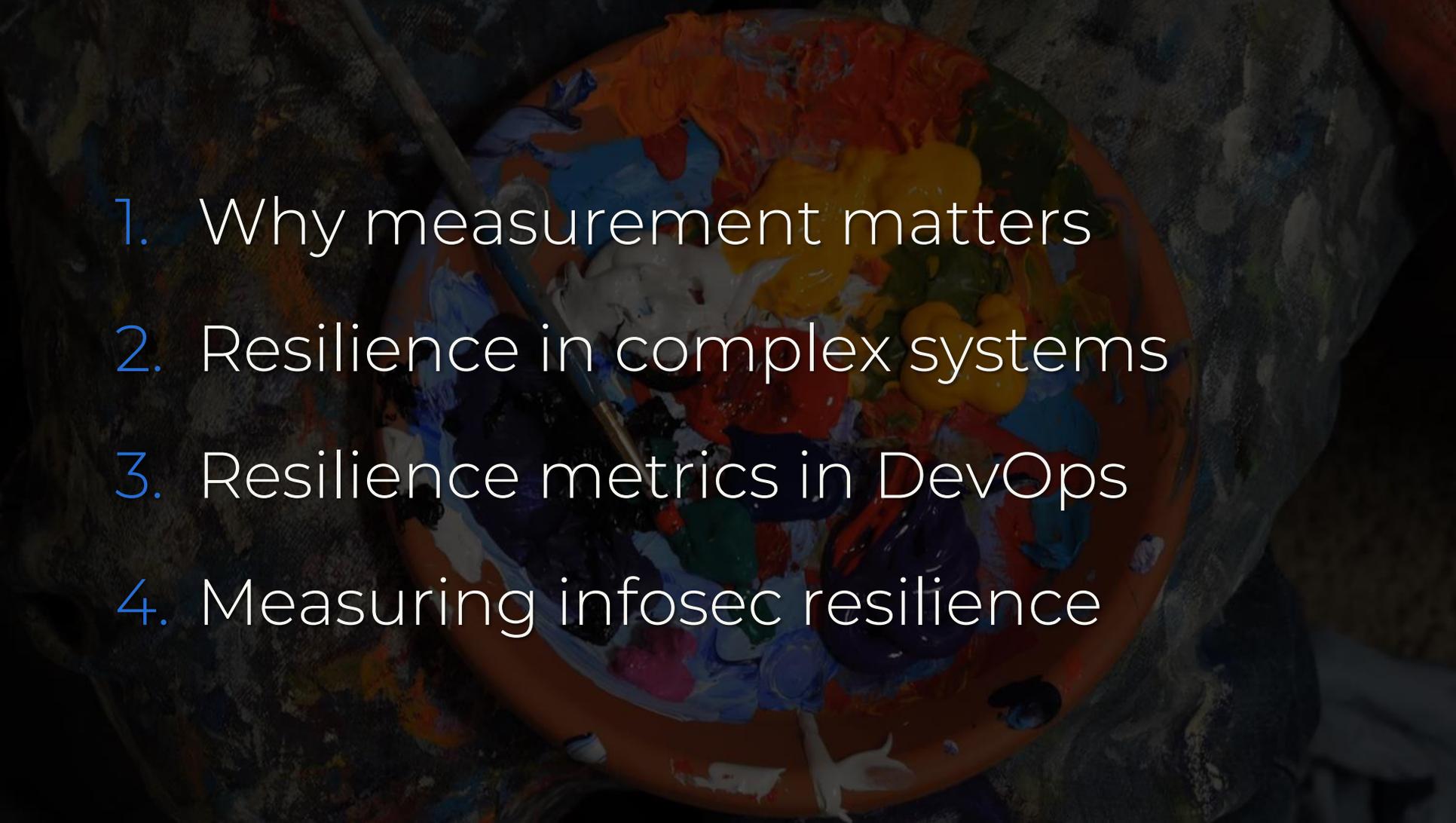
If security is treated as a product,
success can be defined & measured



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

A person wearing a colorful, paint-splattered cap and a dark jacket is painting graffiti on a wall. The wall is covered in various graffiti tags and words, including "WAK", "EXPTIES", "TRUTH", and "WINNER TO PR". The person is using a spray can to apply paint to the wall. The overall scene is dimly lit, with the person's face and hands illuminated by a light source.

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

- 
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.”



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%”

A collection of colored pencils is arranged in a row at the top of the image. Below them is a spiral-bound notebook. The notebook's cover features a detailed black and white line drawing of a rabbit surrounded by floral and leaf patterns. The notebook is open to a page with a calendar or schedule, showing dates and text such as "Good Friday (Western)", "Passover* Easter Sunday (Australia - except T&A, WA)", and "Easter (Western)". The entire scene is overlaid with a semi-transparent dark grey filter.

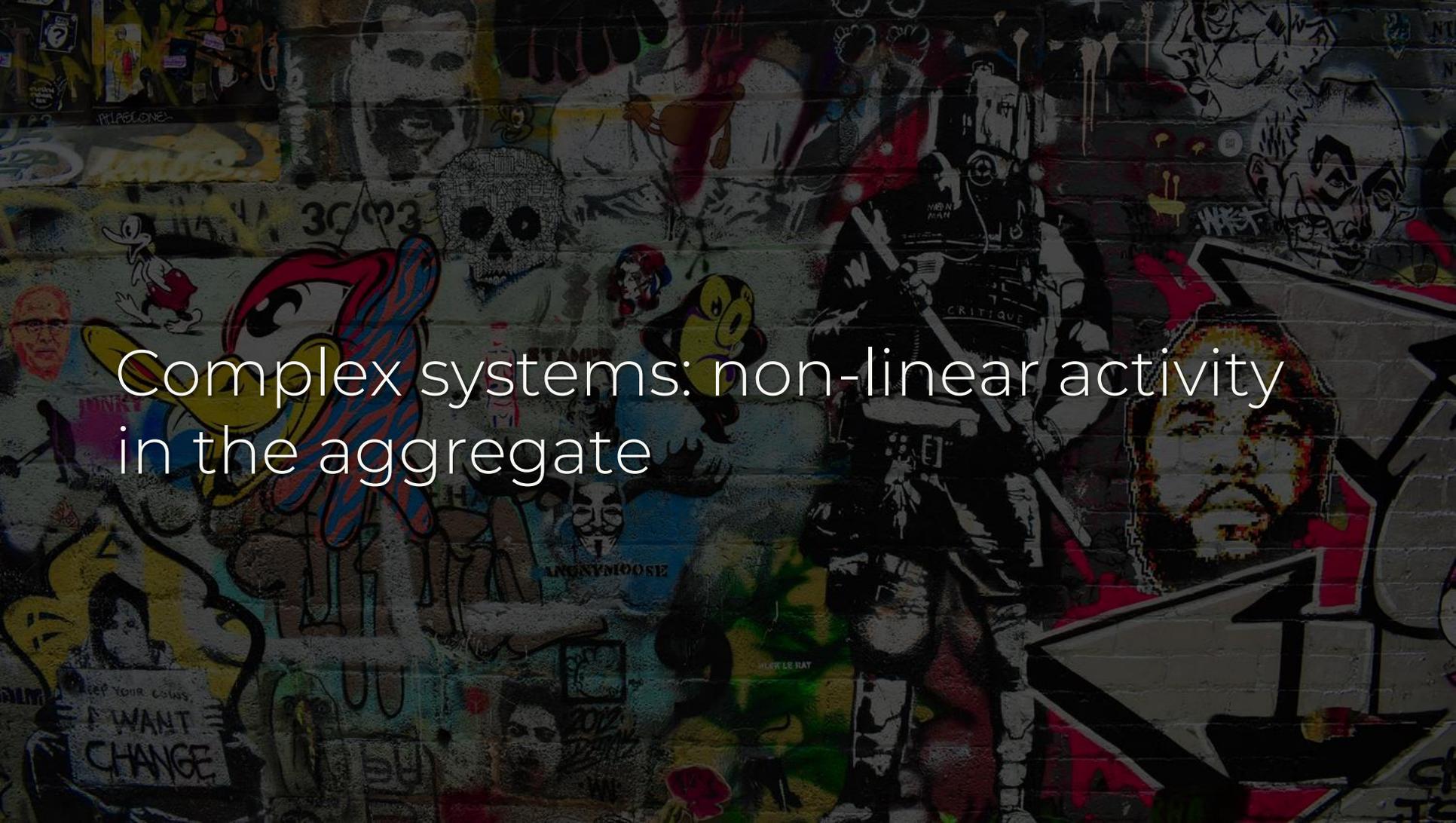
Success metrics create the numbers
by which you paint your vision

Metrics are quantifiable measures to track & assess status

Your process must reflect a relentless pursuit of continuous improvement



Resilience in Complex Systems

A dense, multi-layered graffiti wall. The background is a complex collage of various styles and subjects. In the upper left, there's a tag 'MILFELONEL' and a date '30/03'. A large, stylized skull is prominent in the center. To the right, a figure in a black jacket with 'CRITIQUE' written on it is depicted. Below that, a tag 'ANONYMOOSE' is visible. In the bottom left, a sign reads 'KEEP YOUR COINS I WANT CHANGE'. Other elements include a cartoon character resembling Daffy Duck, a portrait of a man, and various abstract shapes and colors. The overall aesthetic is chaotic and expressive, typical of street art.

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**

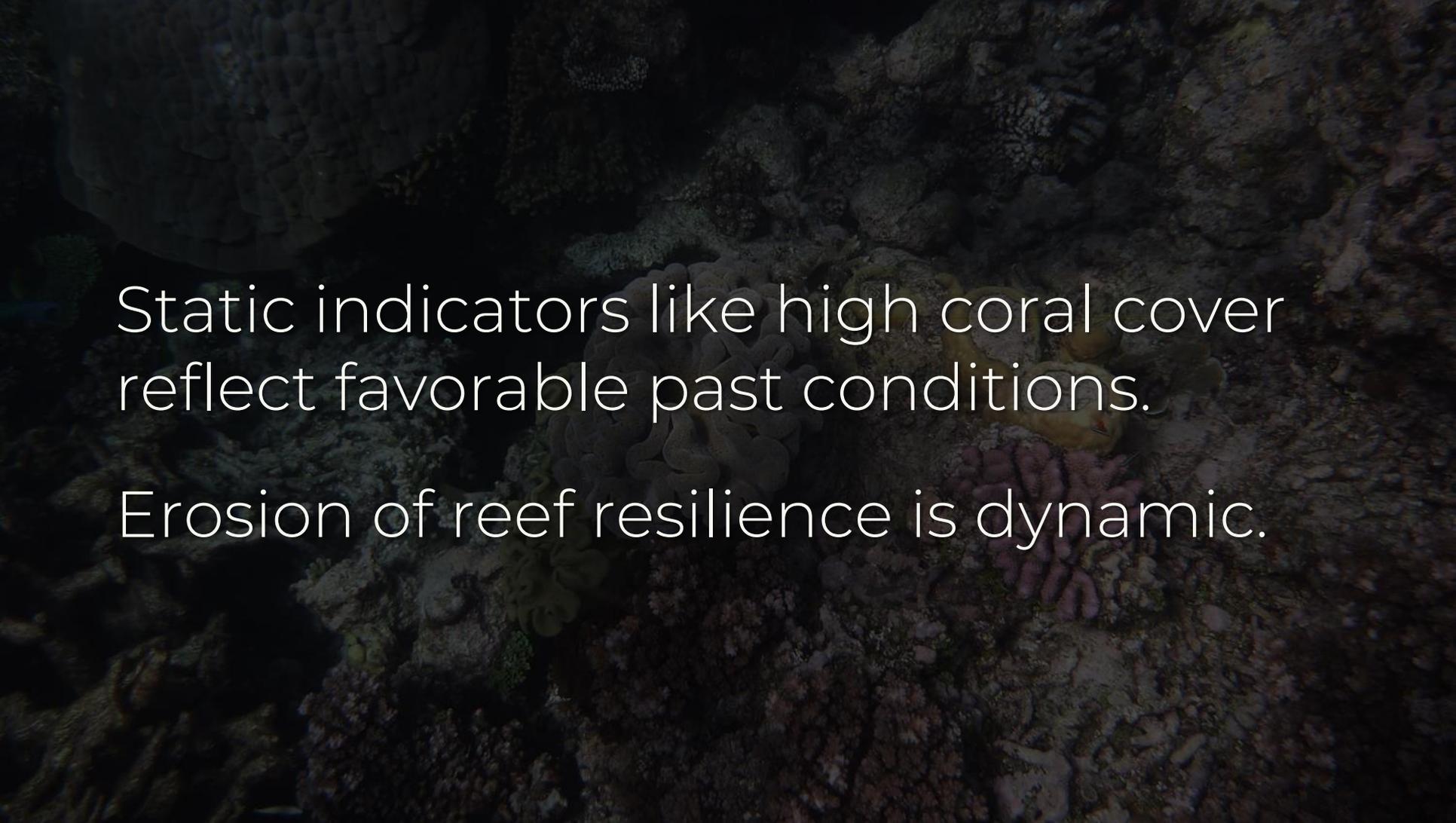
Three central features of resilience:
Robustness, Adaptability,
Transformability

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

A dramatic, dark landscape painting. In the foreground, a small boat with a single sail is caught in turbulent, dark water, struggling against a massive wave. The middle ground shows a coastal town with buildings and a prominent tower or castle on a cliffside, partially obscured by the dark, swirling water and mist. The background features a vast, dark sea under a heavy, overcast sky with dark, swirling clouds. The overall mood is one of intense natural power and peril.

Natural disaster resilience must
assume failure of controls

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

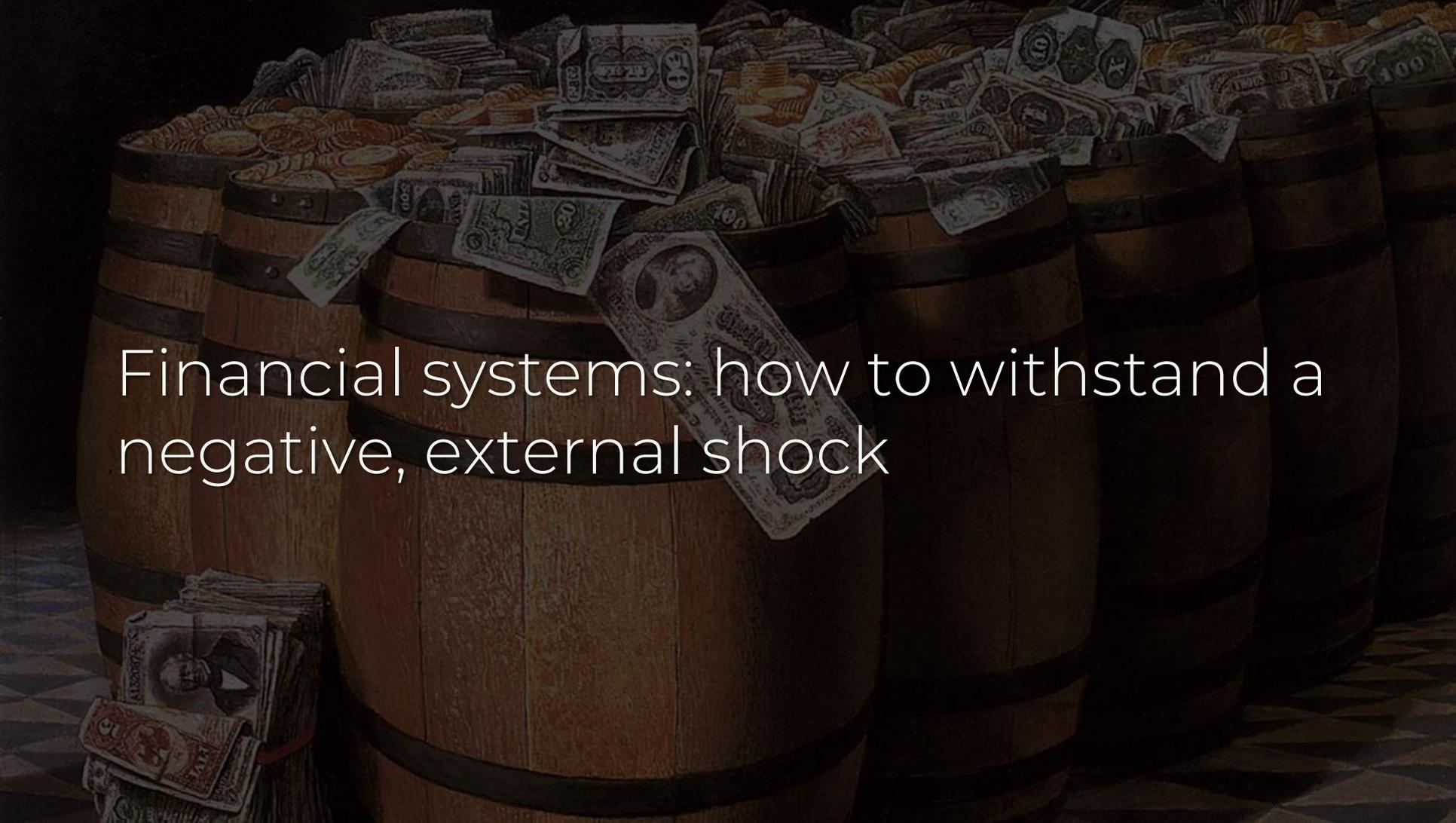
An underwater photograph of a coral reef. The scene is dimly lit, showing various types of coral and rocky structures. The text is overlaid in white, sans-serif font. The background shows a mix of dark and light patches, likely due to the depth and the presence of different coral species and rocks.

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?

A row of wooden barrels overflowing with stacks of various banknotes and coins, including US dollars and Euro coins. The barrels are arranged in a line, and the money is piled high, spilling over the tops. The scene is dimly lit, with a checkered floor visible in the foreground.

Financial systems: how to withstand a negative, external shock

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



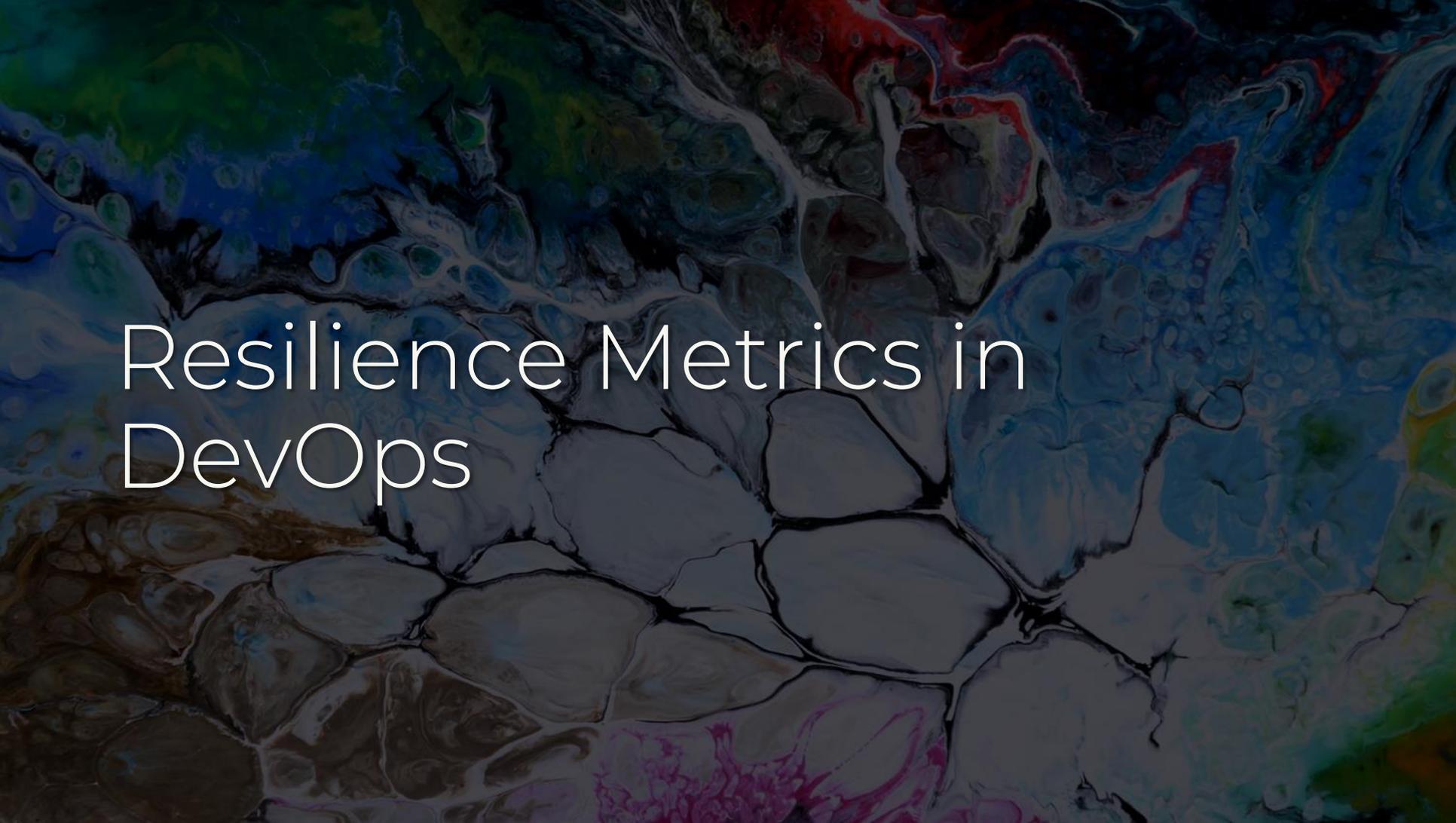
High connectivity & large fraction of contagious links = riskiest nodes

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

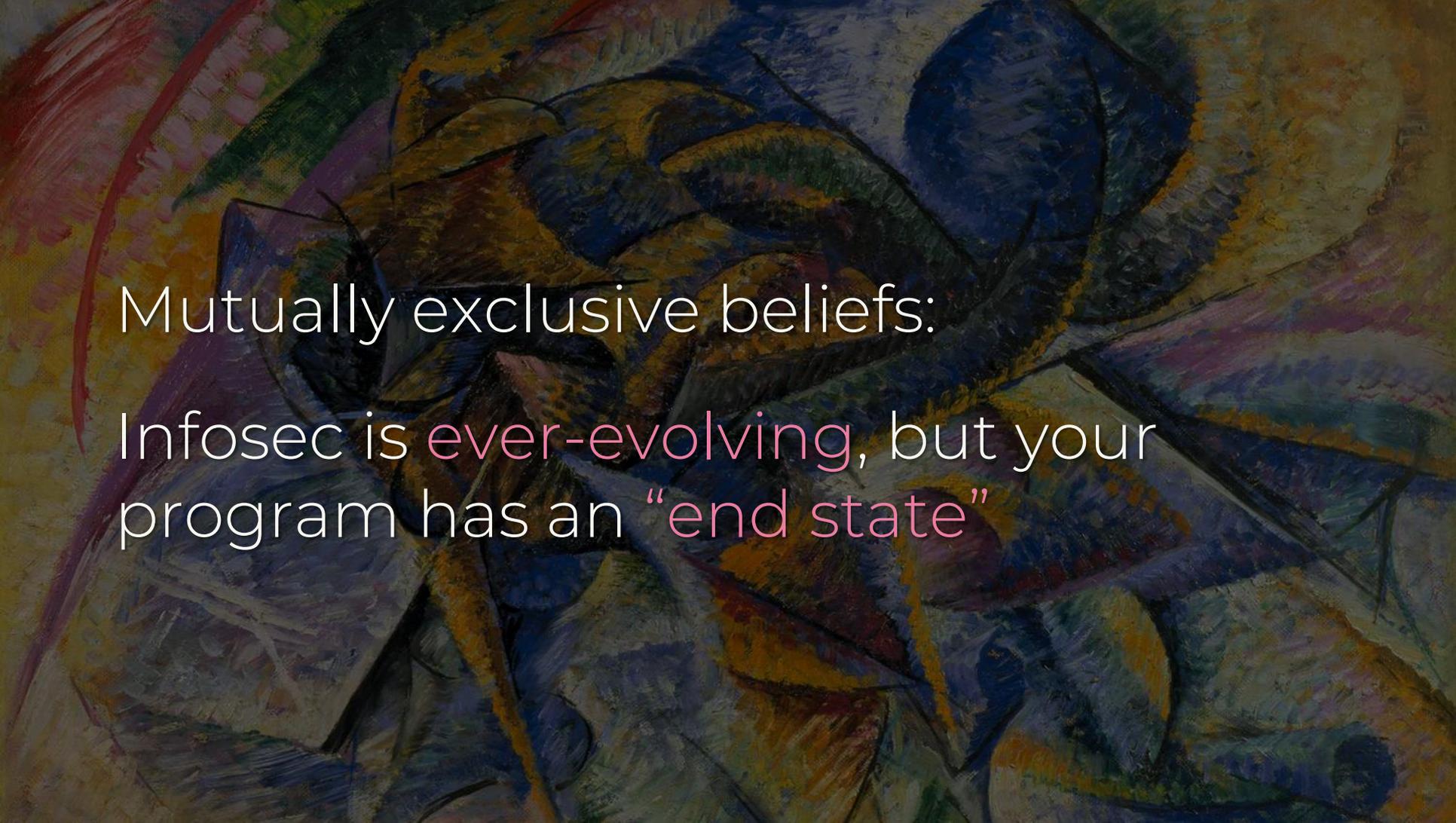
Source: "Incentivizing Resilience in Financial Networks," Leduc & Thurner

The background is a piece of marbled paper with a complex, organic pattern of swirling colors including deep blues, greens, reds, and greys. A semi-transparent dark grey or black overlay covers the entire image, making the colors appear muted and providing a high-contrast background for the white text.

Resilience Metrics in DevOps

“Maturity models are for chumps.”

– Dr. Nicole Forsgren @nicolefv

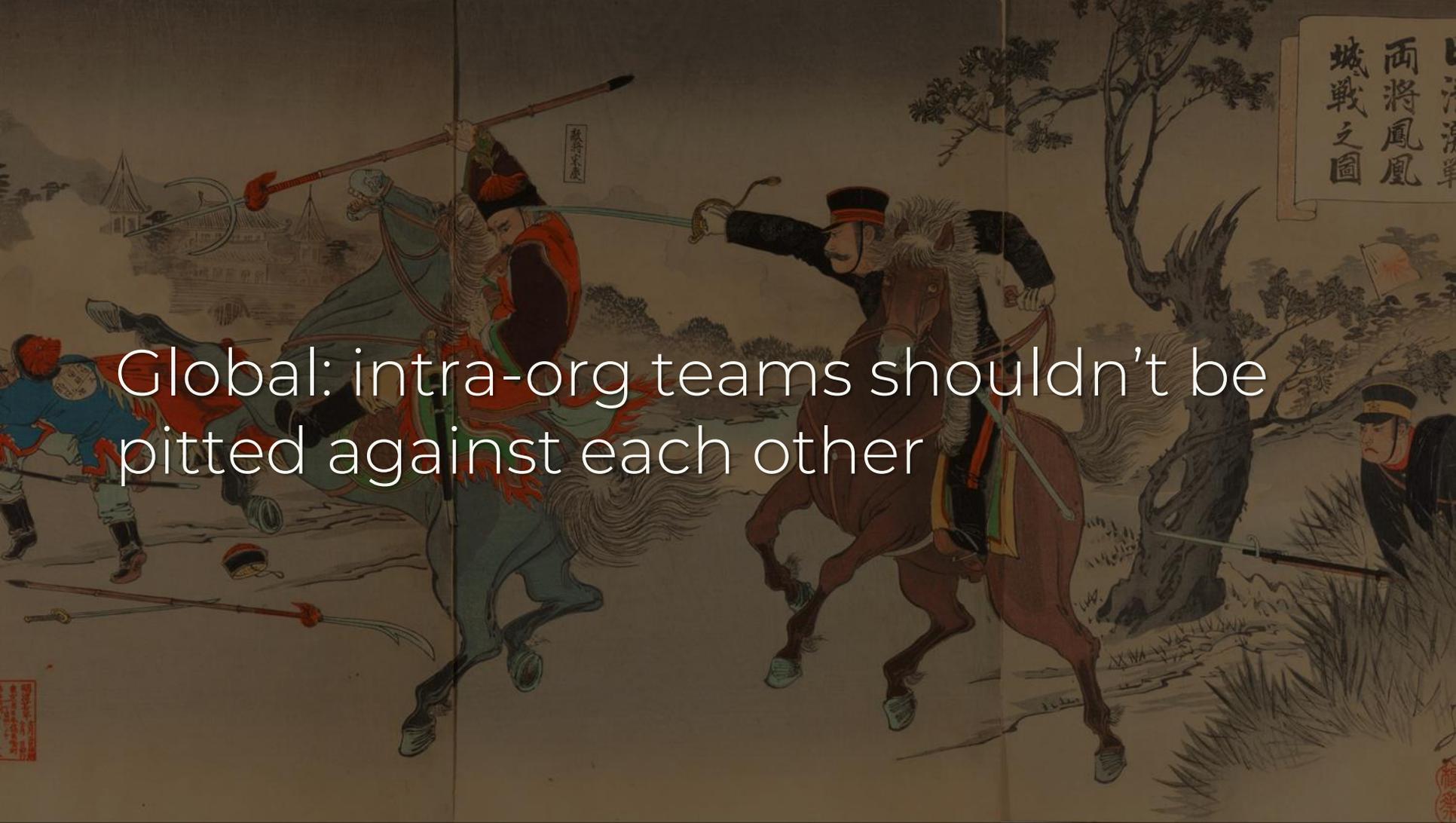
An abstract painting with a complex, layered composition. The background is a dense mix of colors including deep blues, purples, greens, and yellows, with visible brushstrokes and textures. The overall effect is one of depth and movement.

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

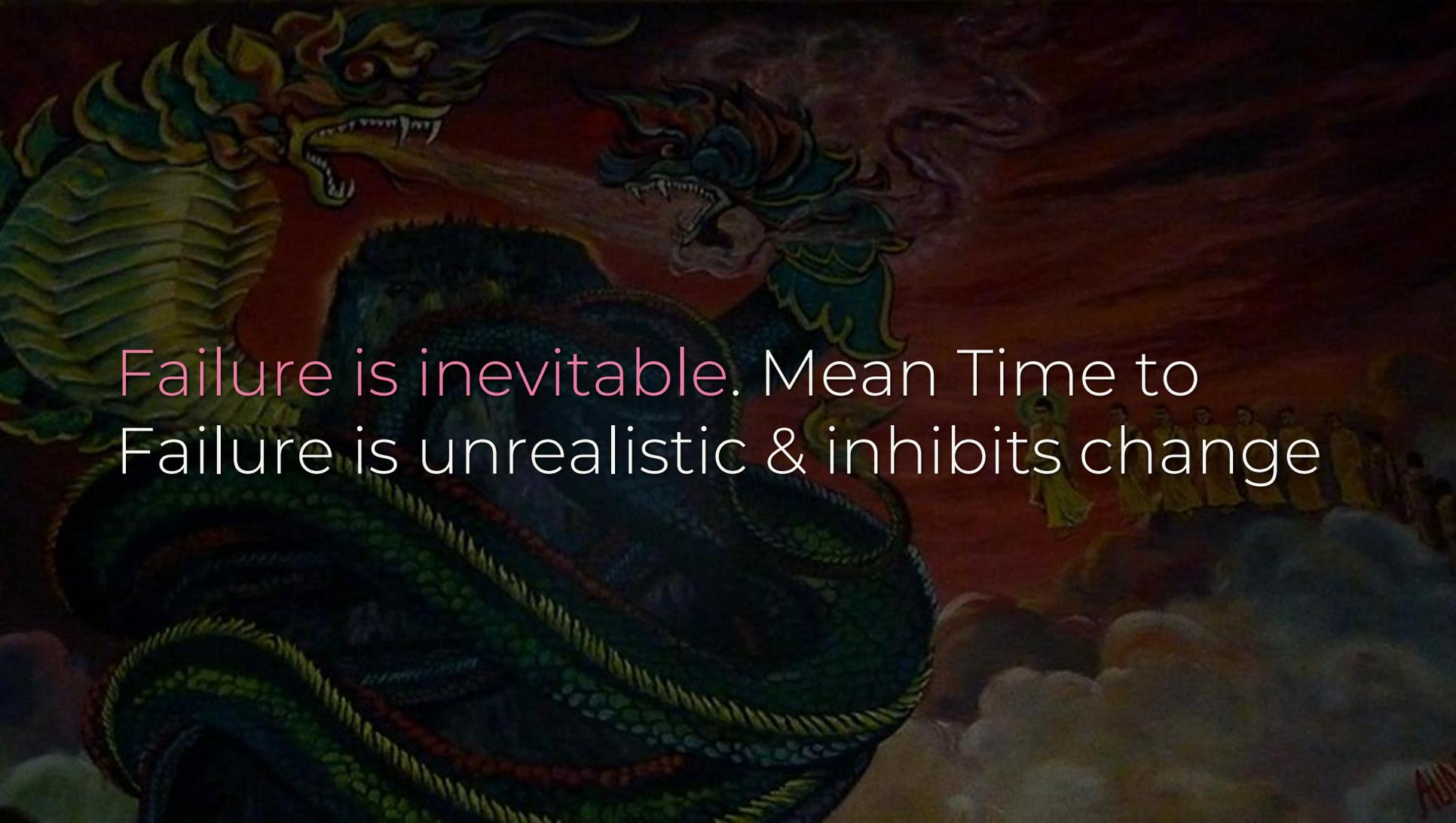
Lead time, release frequency, MTTR

A grayscale photograph of a person's hands drawing a bird on a piece of paper. The person is wearing a striped shirt. The drawing is in progress, with the pen tip touching the paper. There are other drawings of birds and flowers on the paper. The text is overlaid on the image.

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 painting depicting two dragons breathing fire. The dragons are rendered in vibrant green and blue scales, with fierce expressions and open mouths. The background is a dark, reddish-brown sky. In the lower right, a group of people in yellow robes stands on a white, cloud-like base. The overall style is characteristic of traditional Chinese ink and wash painting with a focus on bold colors and dynamic composition.

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

No tradeoff between improving performance vs. stability or quality

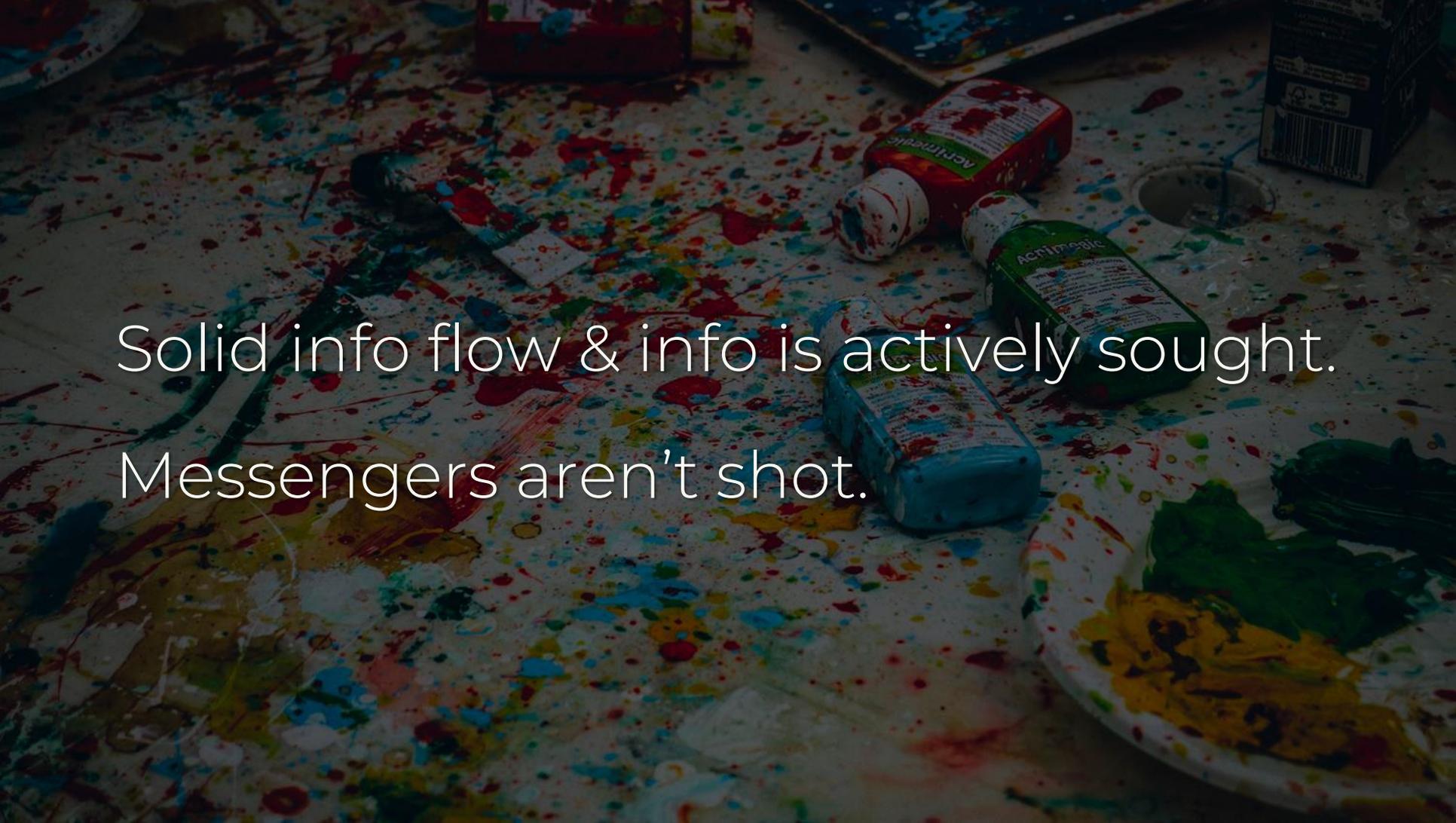
High performers:

Deploy frequency: on-demand

Lead time: <1 hour

MTTR: <1 hour

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

A photograph of a messy art studio floor. The floor is covered in a chaotic pattern of colorful paint splatters in red, blue, yellow, and green. Several tubes of acrylic paint are scattered across the surface, some lying on their sides. A paint palette with yellow and green paint is visible in the bottom right corner. A dark box with a barcode is in the top right. The overall scene is one of creative chaos.

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

Responsibilities are shared.

Cross-team collaboration is rewarded.

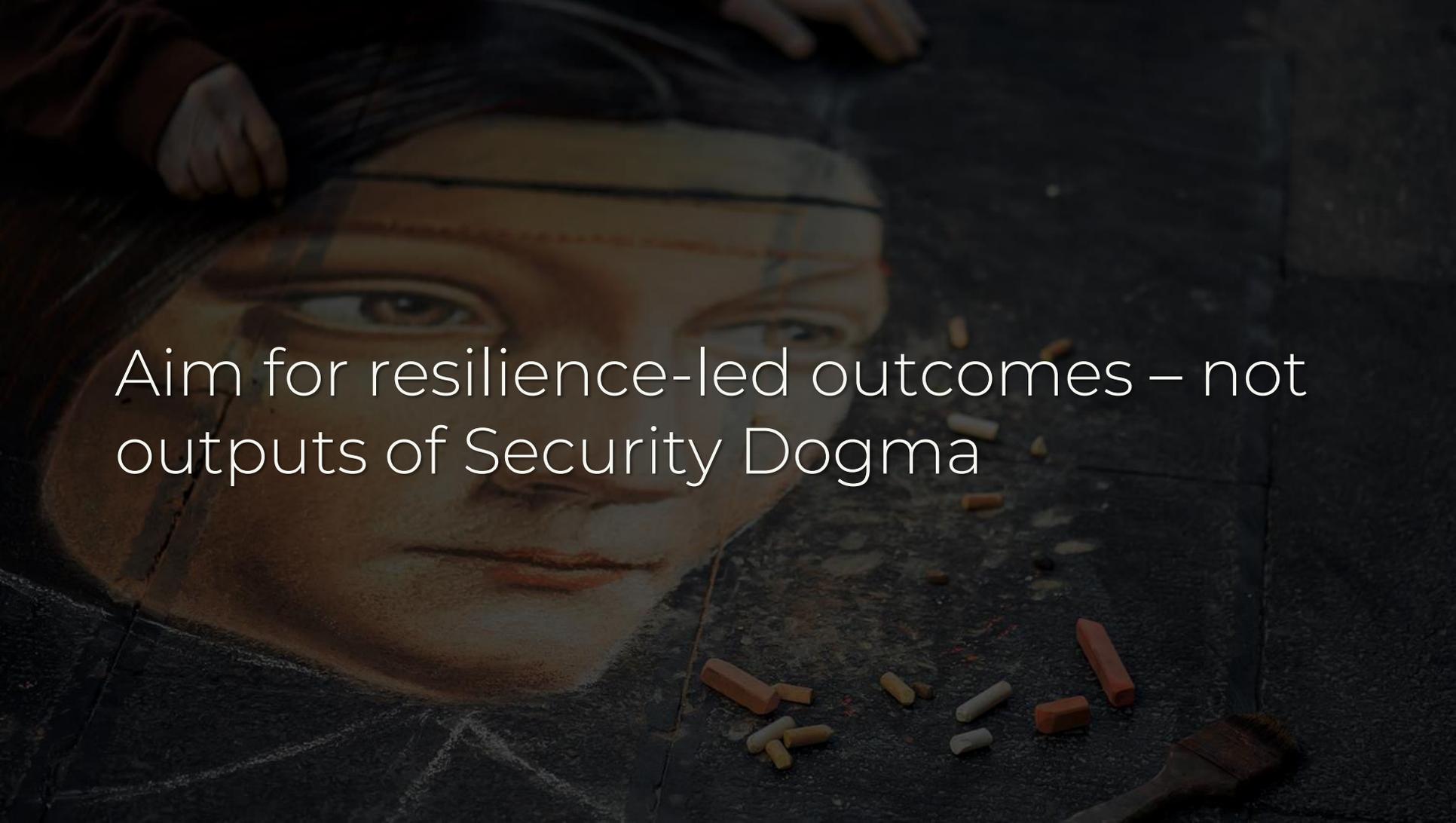
Failures are treated as learning opportunities for improvement.

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

The background of the slide is a piece of marbled paper with a complex, organic pattern of colors including shades of purple, blue, green, orange, and pink. A dark, semi-transparent grey overlay covers the entire image, creating a moody atmosphere. The text is centered in the middle of the slide.

Measuring InfoSec Programs

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

A chalk drawing of a woman's face is the central focus, rendered on a dark, textured pavement. The drawing is detailed, showing the woman's eyes, nose, and lips. To the right of the drawing, several pieces of orange and white chalk are scattered on the ground, along with a small brush. The overall scene is dimly lit, with a dark, moody atmosphere. The text is overlaid on the left side of the image, centered vertically.

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

The background is a dark, textured image, possibly a painting or a photograph with a grainy, painterly quality. It features a central figure wearing a blue robe, standing in a dimly lit environment. To the right, there is a green plant with large leaves. The overall color palette is dominated by dark blues, greys, and browns, with some highlights in blue and green.

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

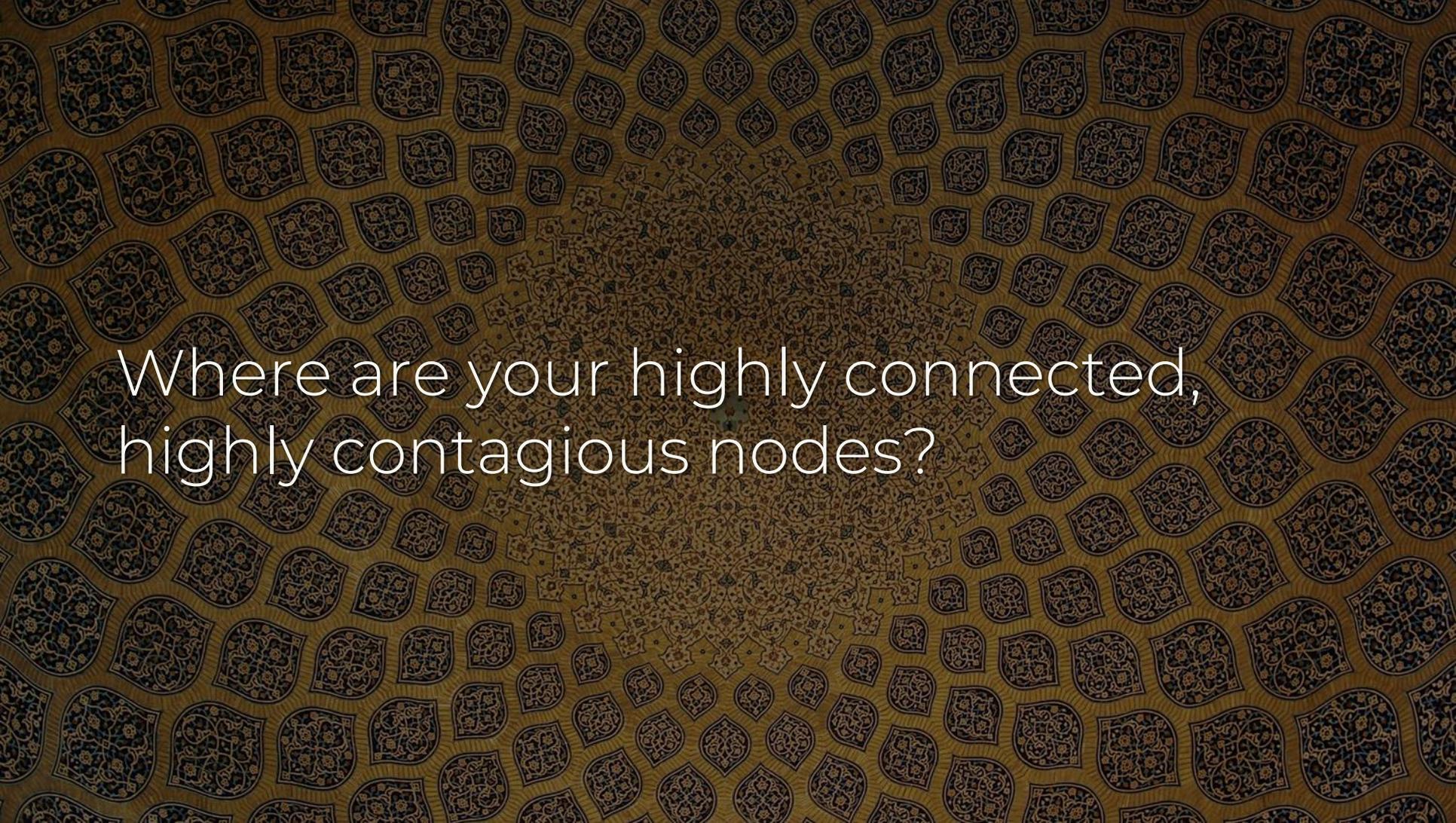
High-performing dev orgs spend 50%
less time remediating security issues

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?

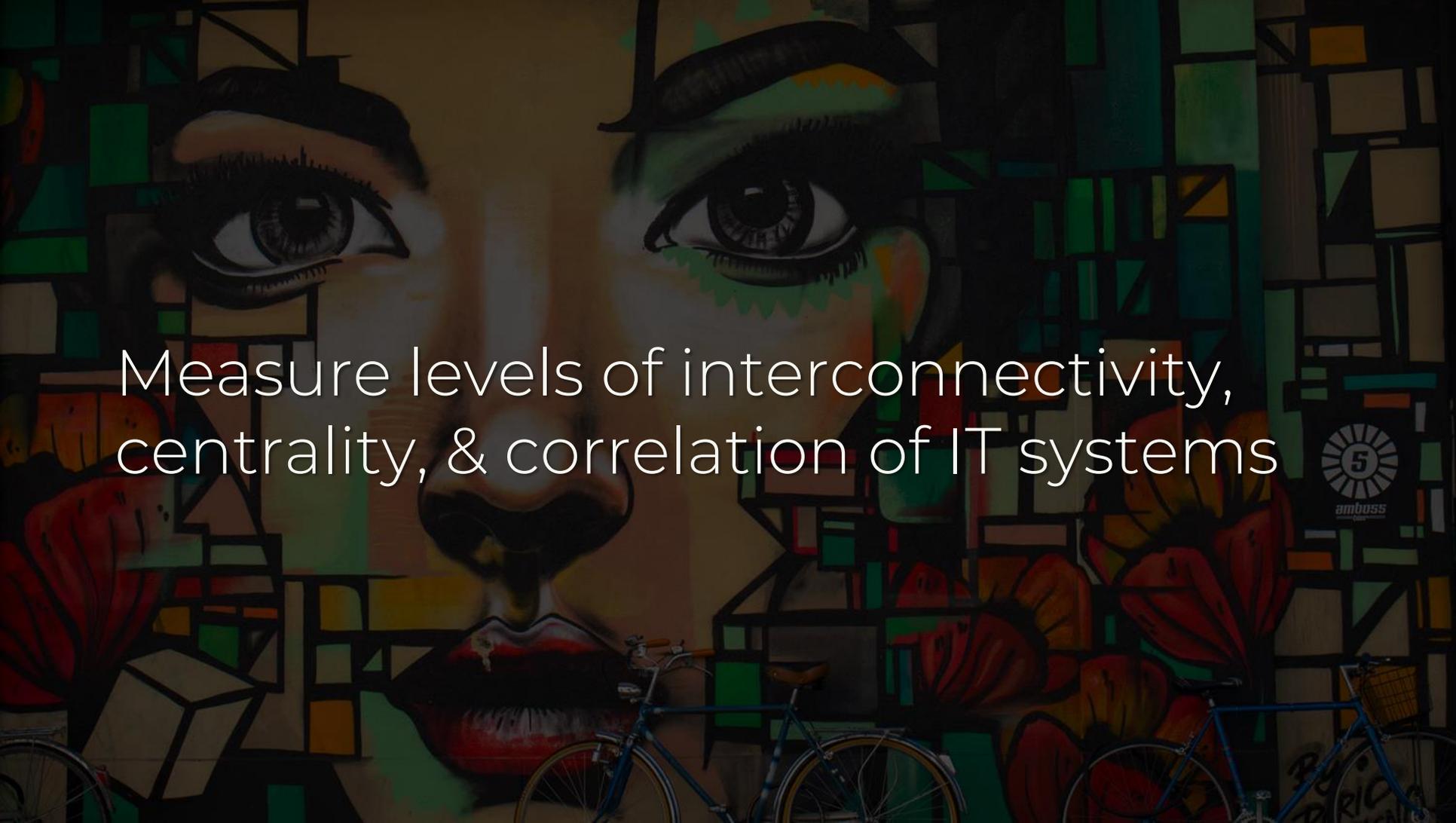
Mean Time to Failure (incident) can
prioritize unhealthy stagnation

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



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



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

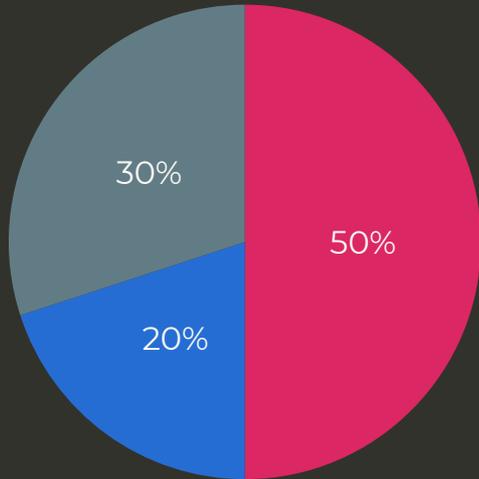
How is your security team's time being used?

SIEM maintenance = 30 hrs / month

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

Time usage: problem solving,
firefighting, meetings & maintenance

Good



Security Innovation

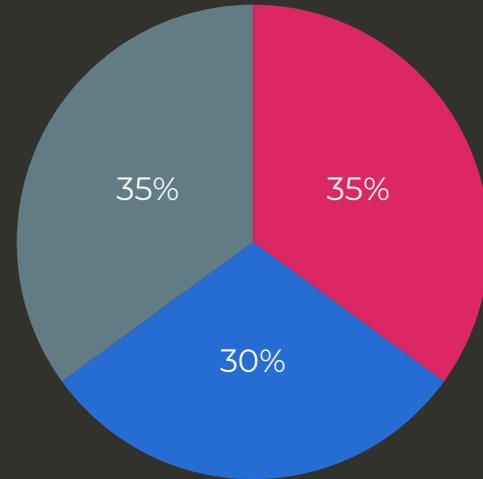


Firefighting



Meetings & Maintenance

Bad



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

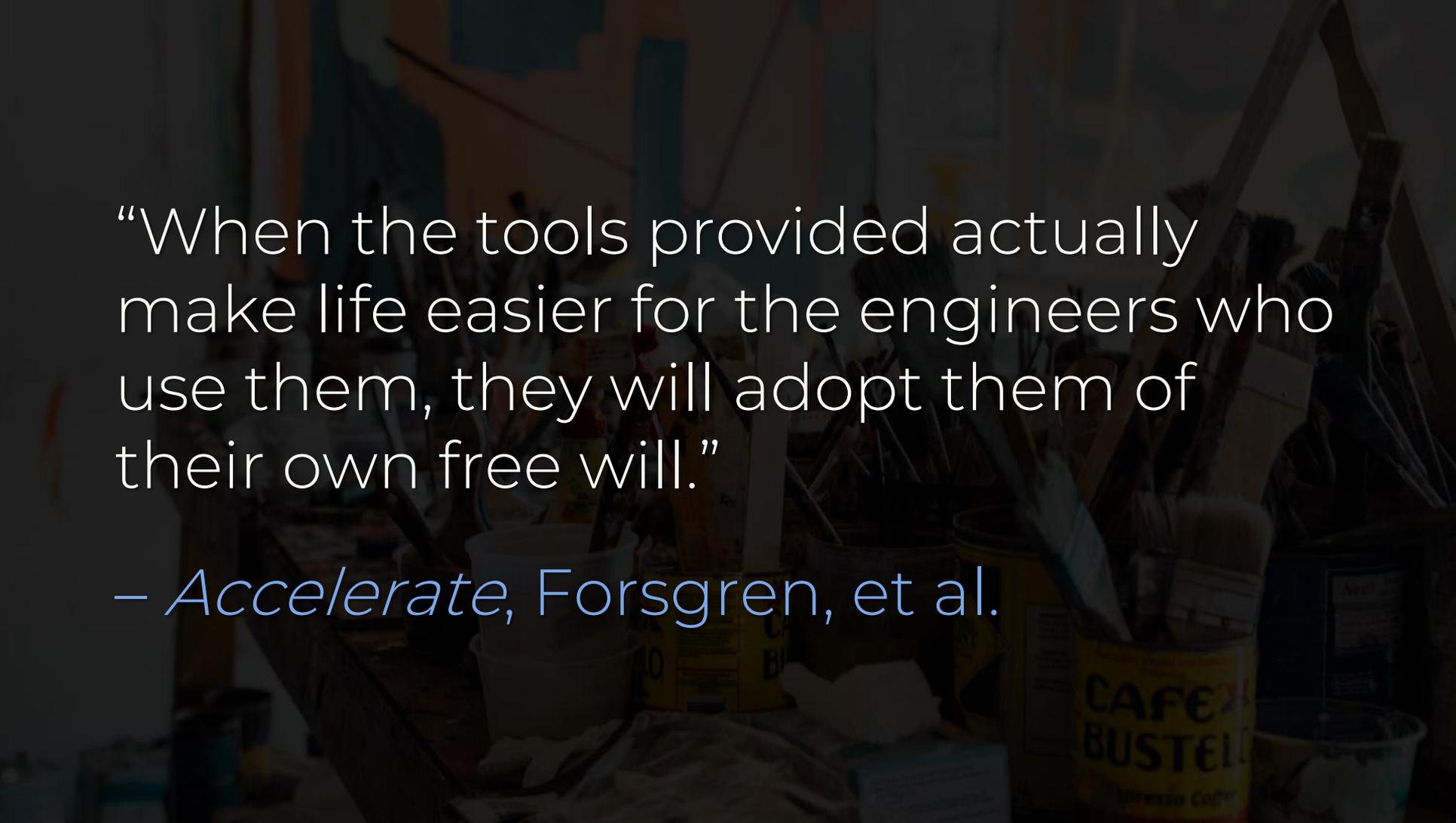
How strong is your culture? Are you actually mission-oriented?

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.



“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

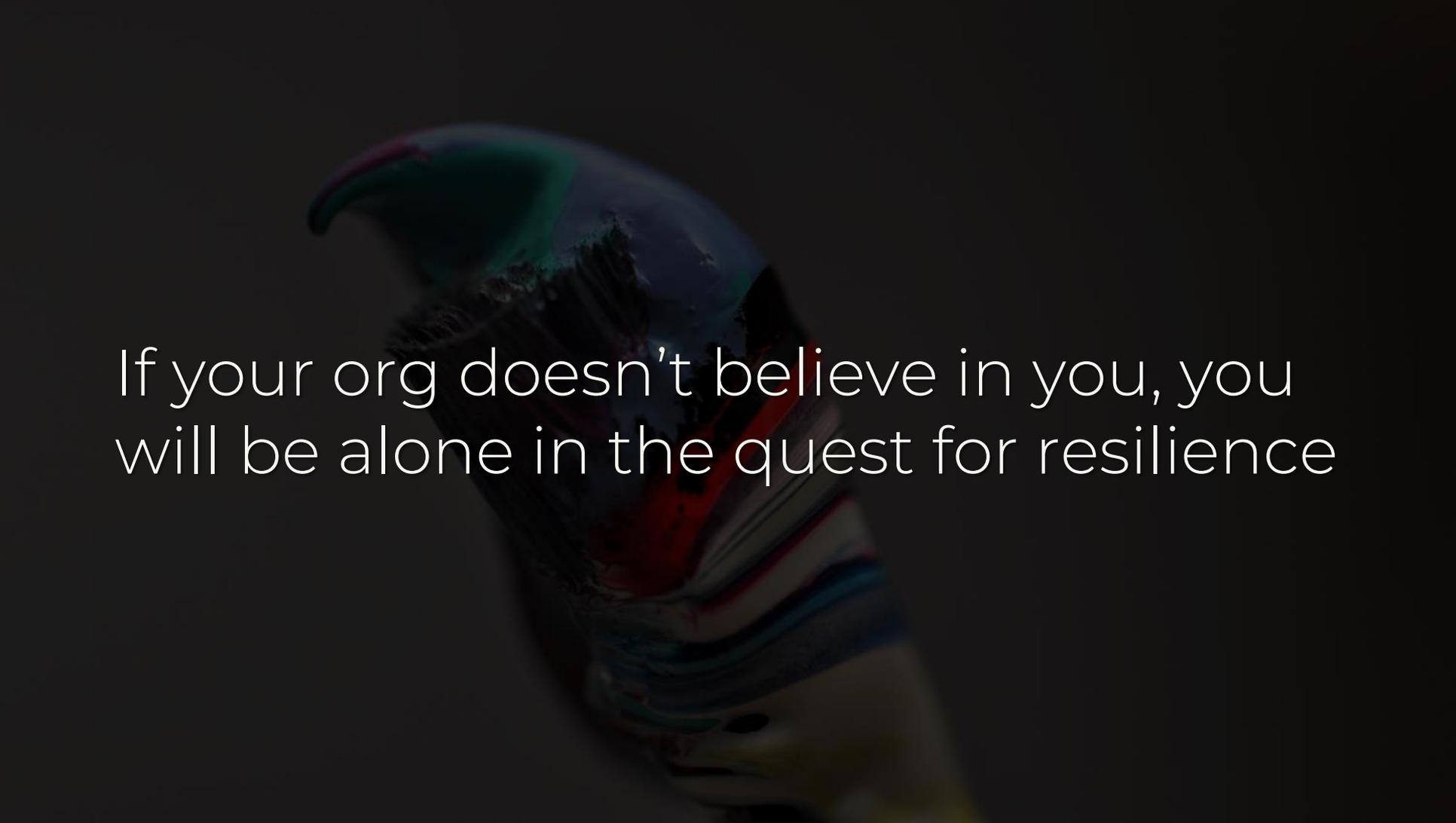
% 2FA usage across departments

of security support tickets filed

Net Promoter Score (NPS):
Mathematical calc of satisfaction

Measure NPS among your colleagues
& teams with whom you work

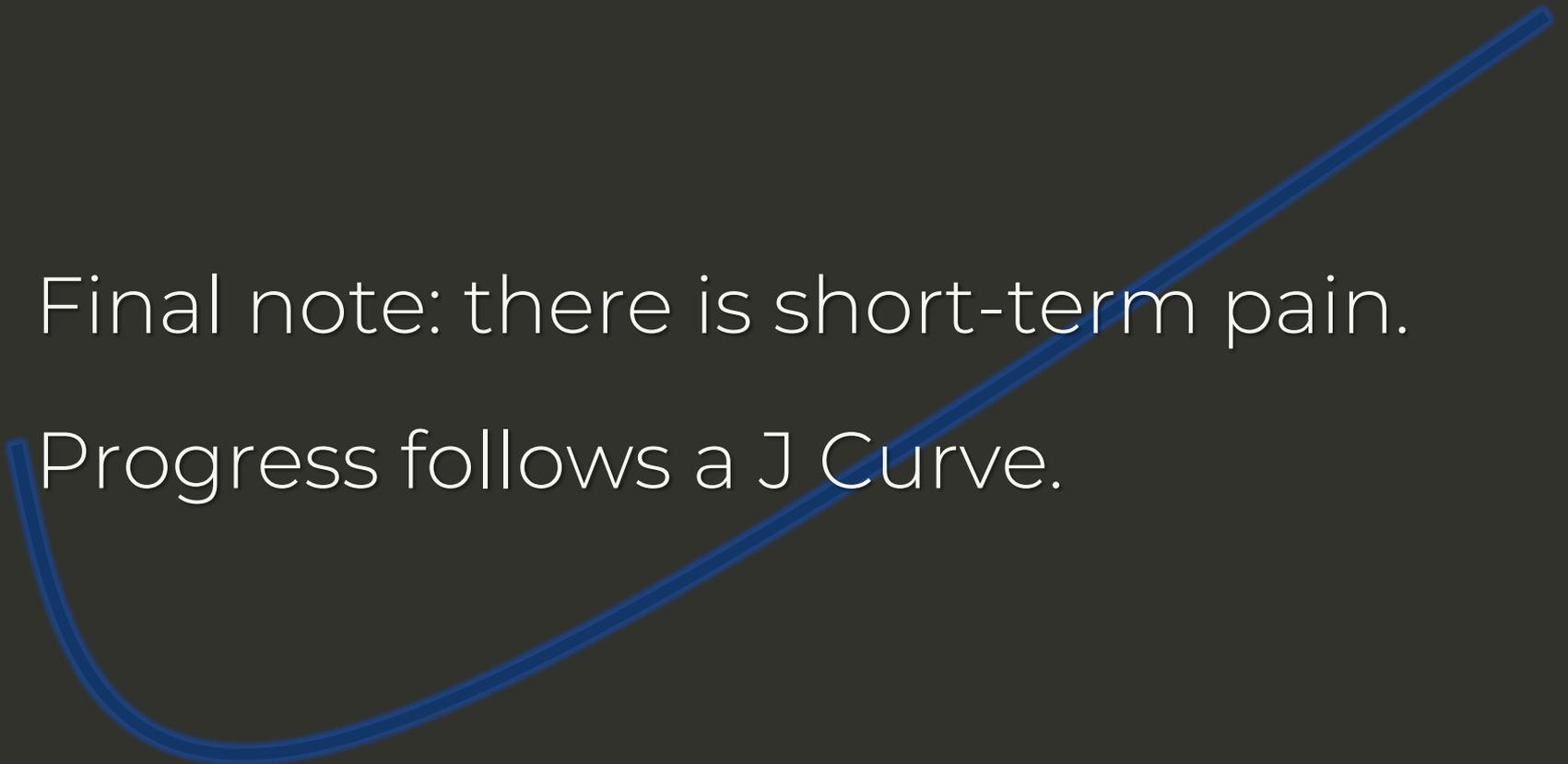
“How likely are you to recommend our security program to a friend?”

A close-up, low-angle shot of a colorful parrot, possibly a cockatiel, looking upwards. The parrot's head is the central focus, showing its vibrant blue, red, and yellow feathers. A clear reflection of a dense forest with tall trees is visible on the top of its head, as if it were a mirror. 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

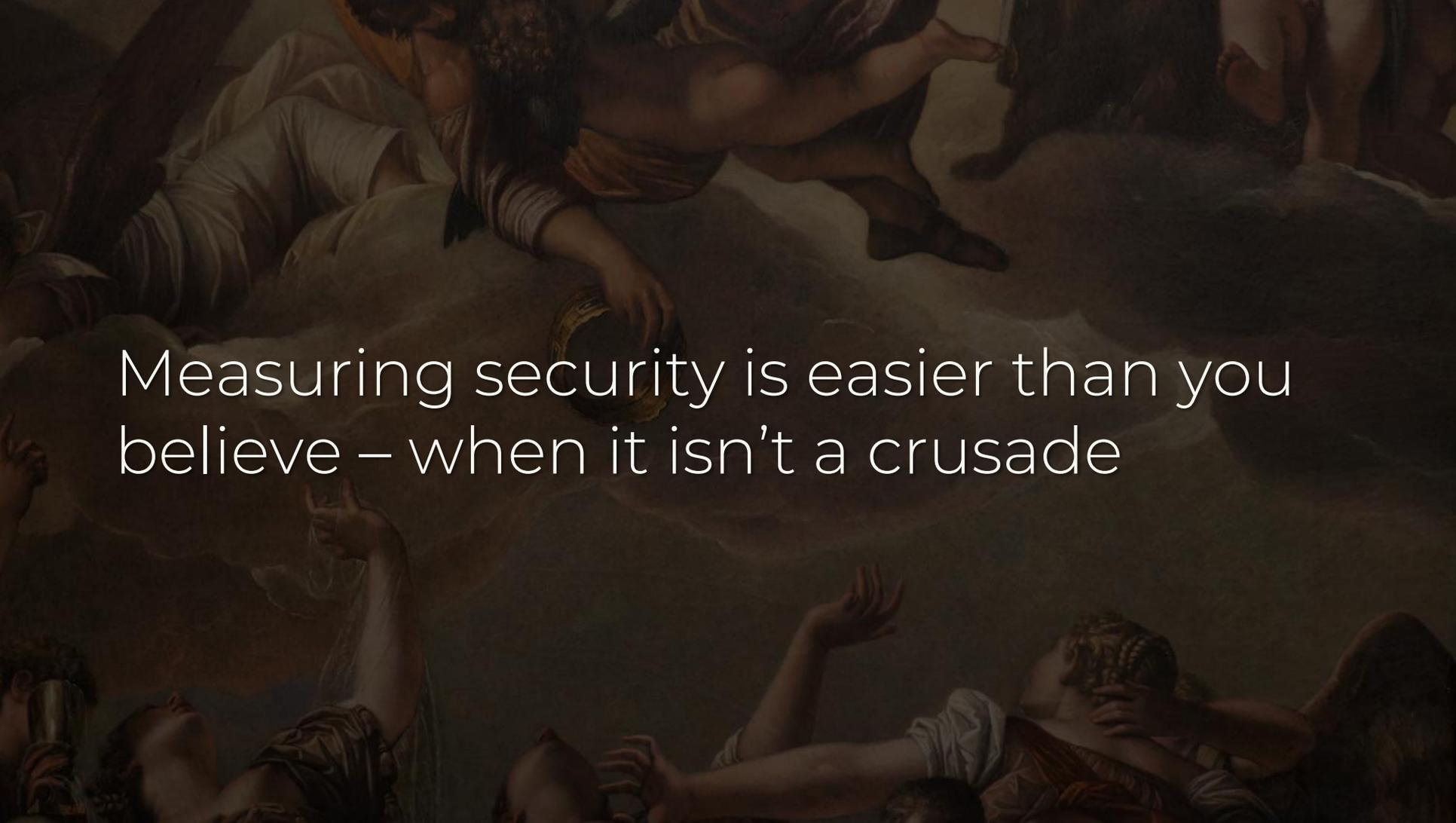


Final note: there is short-term pain.

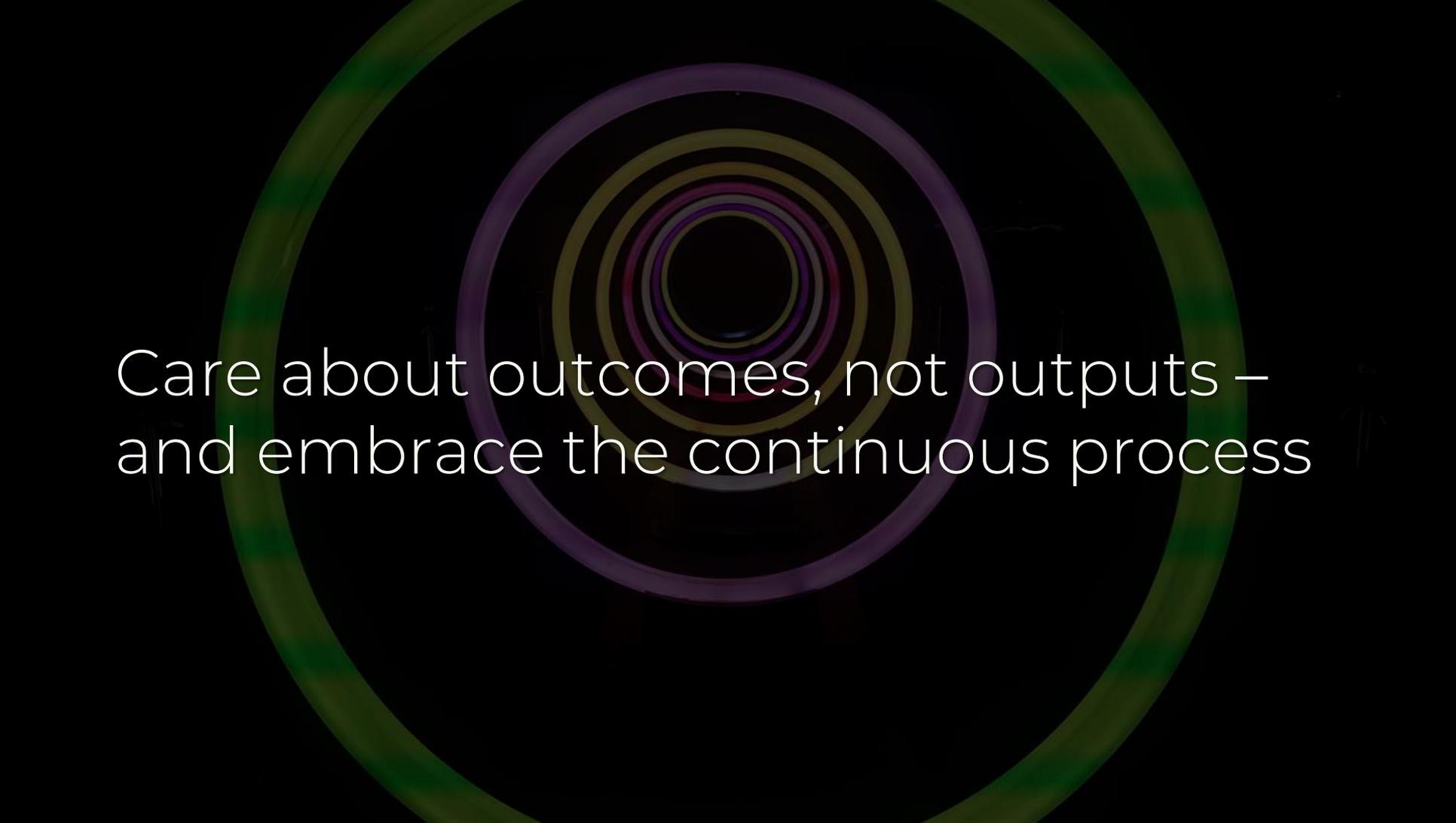
Progress follows a J Curve.



Conclusion

The background is a dark, atmospheric painting. It depicts a scene of suffering or a crusade. In the upper center, a figure with a long, dark beard and a purple and gold robe is shown from the waist down, holding a golden bowl. Below this figure, several other figures are visible in various states of distress. One figure in the lower left is looking upwards with an open mouth, while another in the lower right is lying down with their head resting on their hand. The overall tone is somber and dramatic, with strong contrasts between light and shadow.

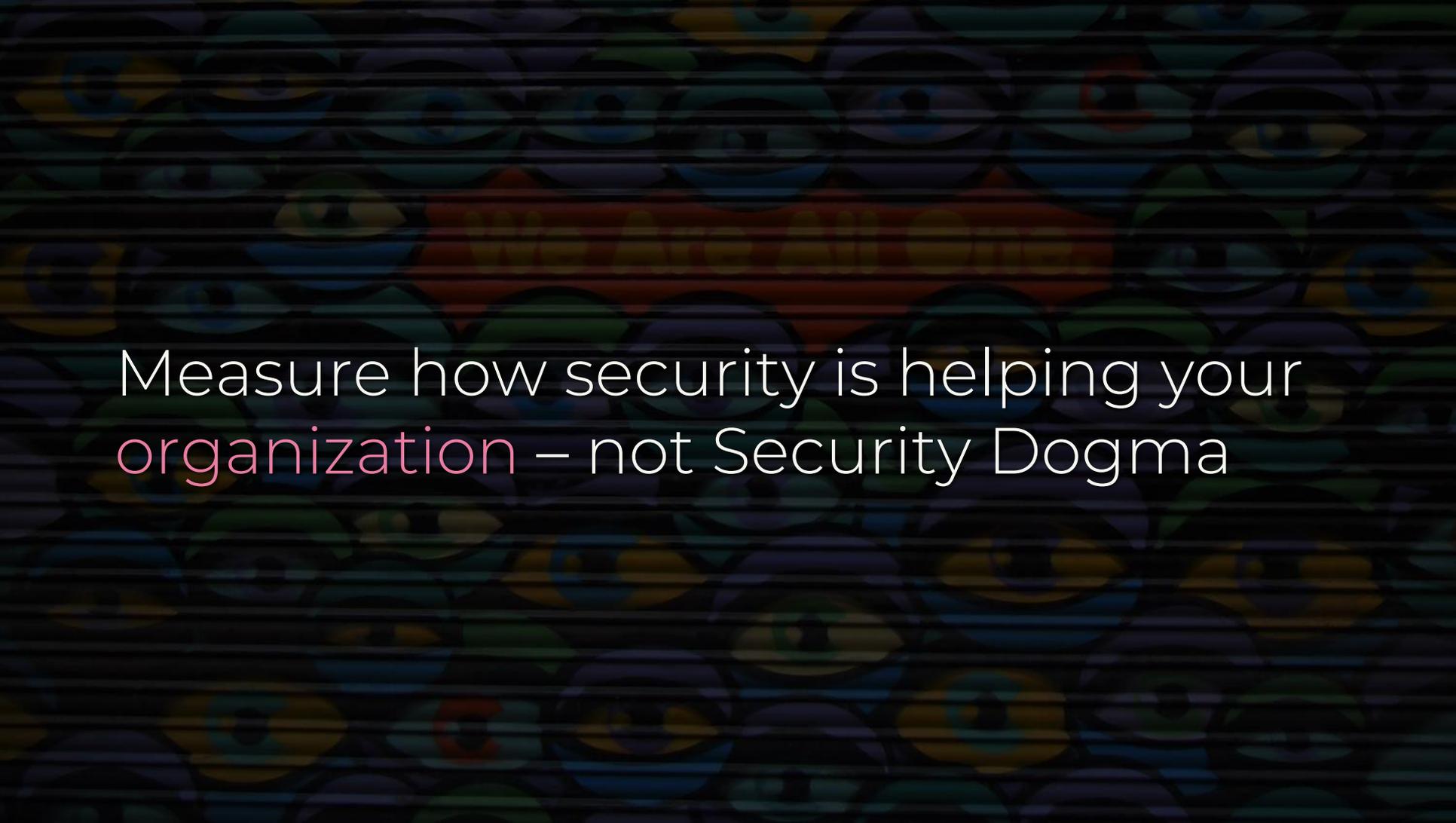
Measuring security is easier than you believe – when it isn't a crusade

The background features a series of concentric circles. The outermost circle is a thick, vibrant green. Inside it is a thinner purple circle, followed by several more thin circles in alternating shades of green and purple, creating a tunnel-like effect that draws the eye towards the center. The text is centered horizontally and vertically over this graphic.

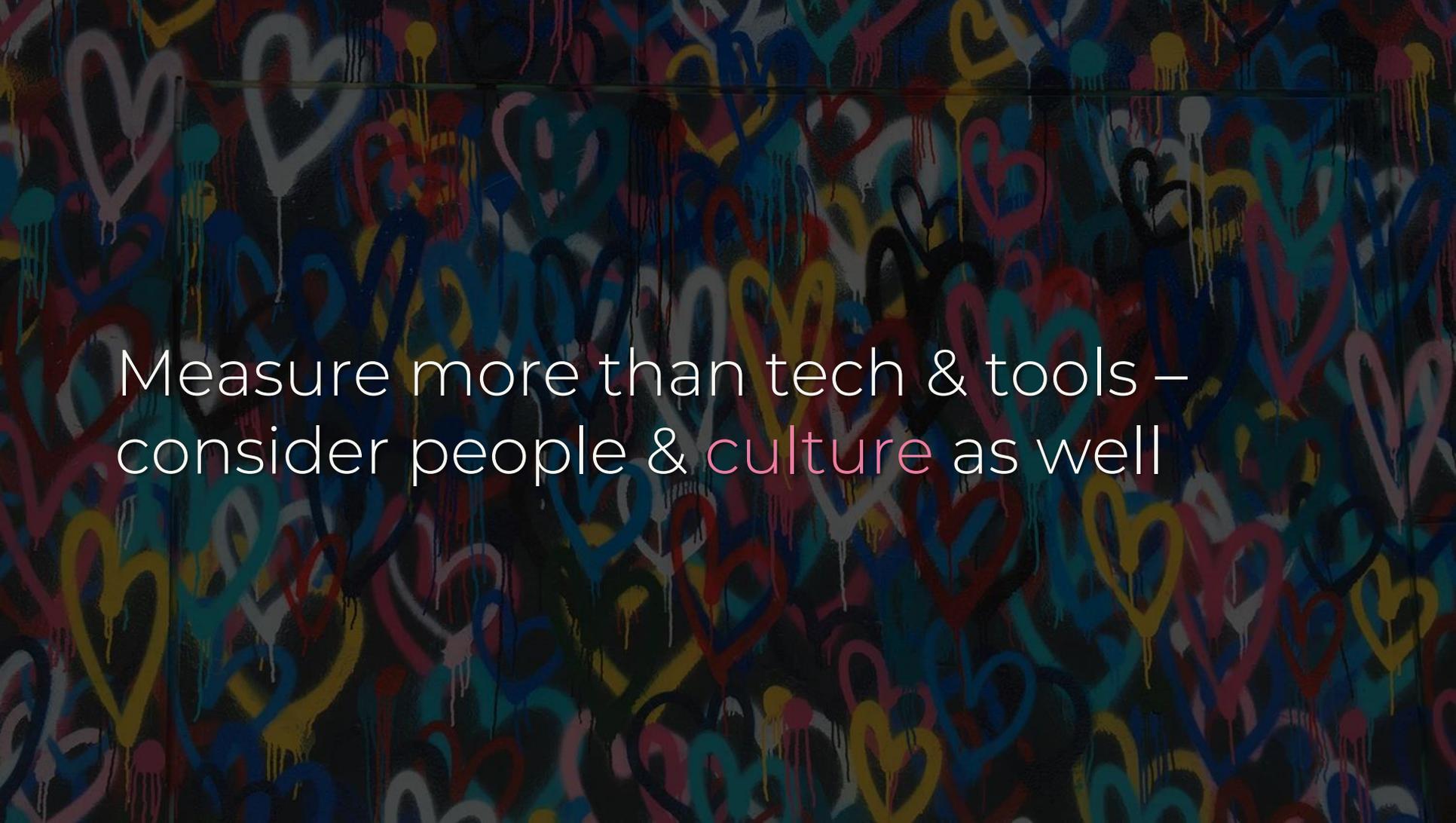
Care about outcomes, not outputs –
and embrace the continuous process



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 vertical image of a hand holding a rope. The hand is rendered in a light, almost white, color with a glowing yellow vein running through it. The rope is thick and textured, and the background is dark. The text is overlaid on the left side of the image.

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