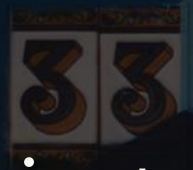
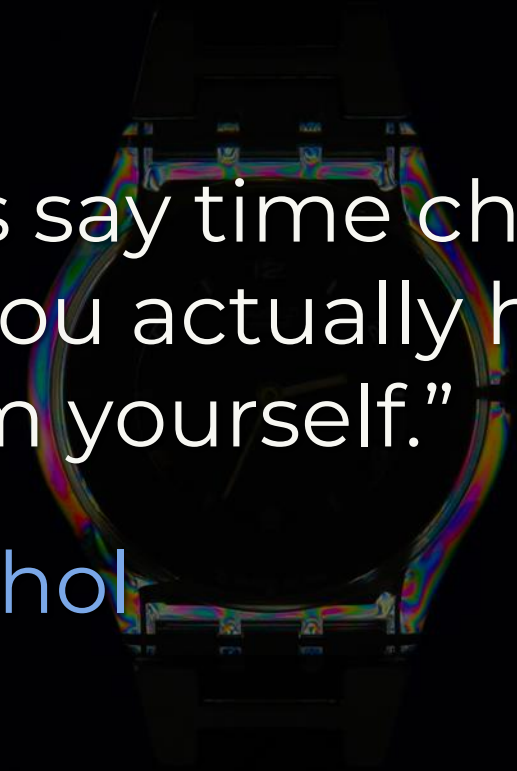


Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda_)

Square R00t 2018


Hi, I’m Kelly



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

— Andy Warhol

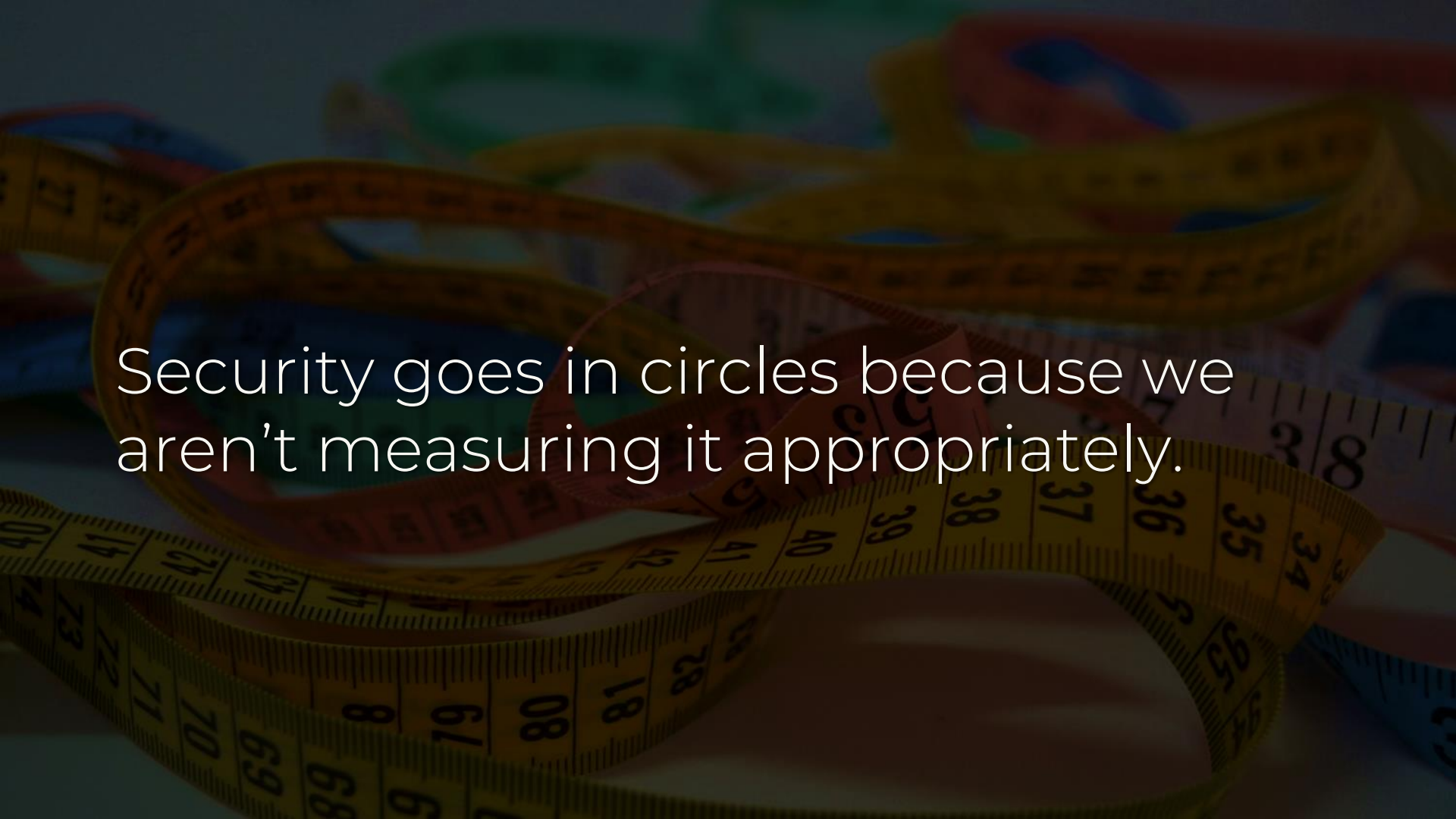
Kelly Shortridge @ #DuraznoConf
@swagitda_

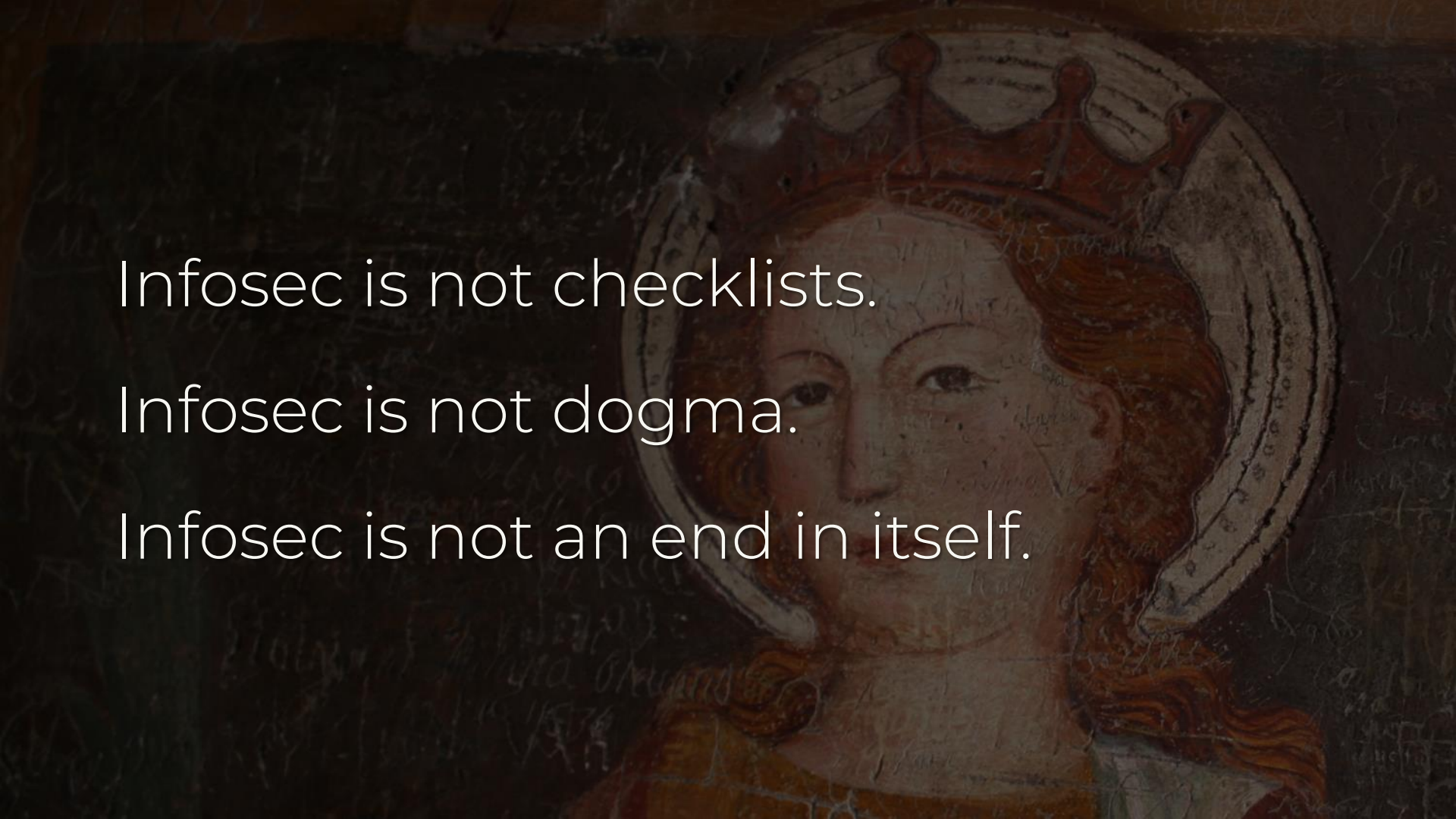
OH: "One thing I love about working in security: I get older, the problems stay the same"

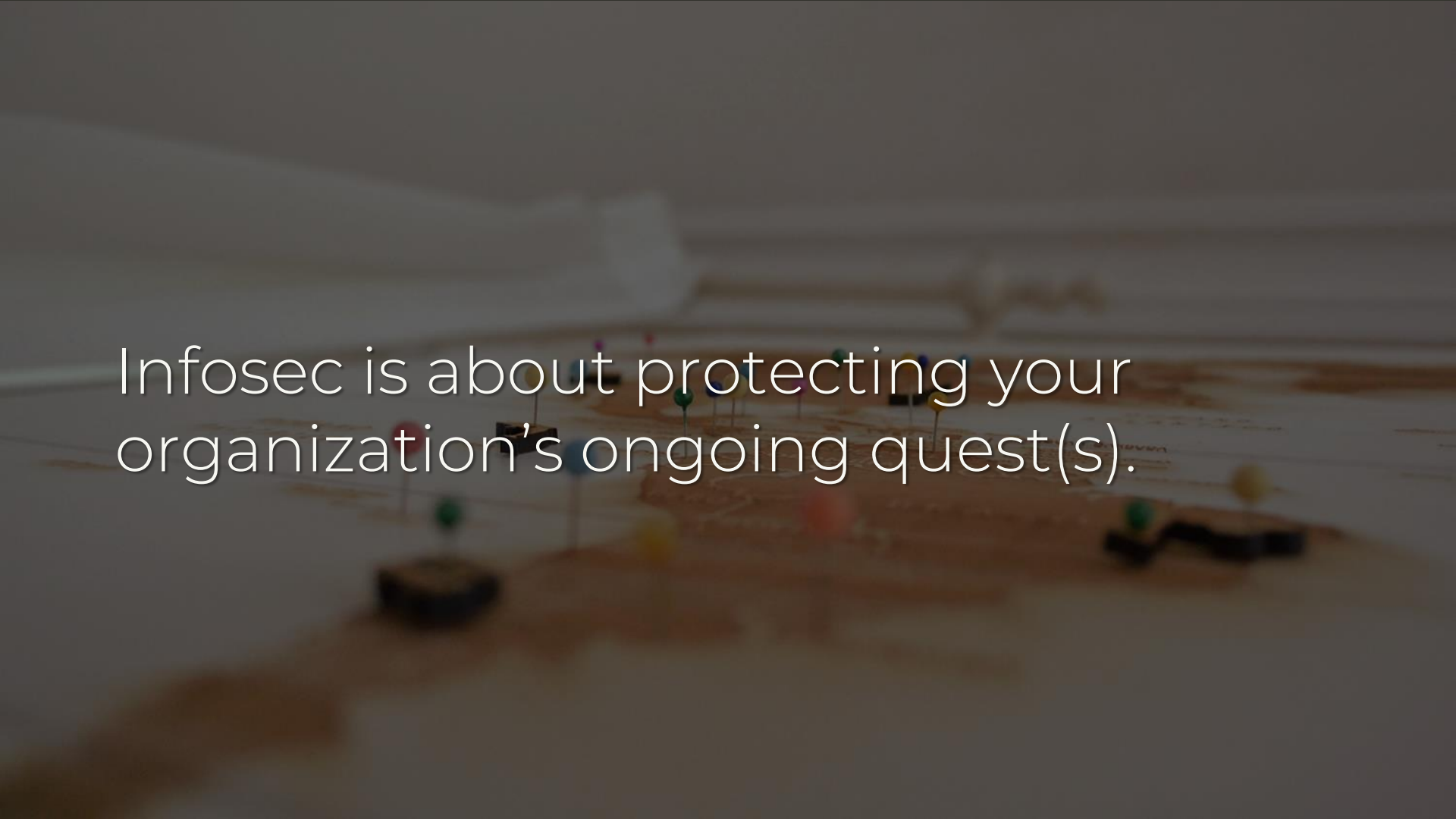
9/21/18, 11:56

View Tweet activity

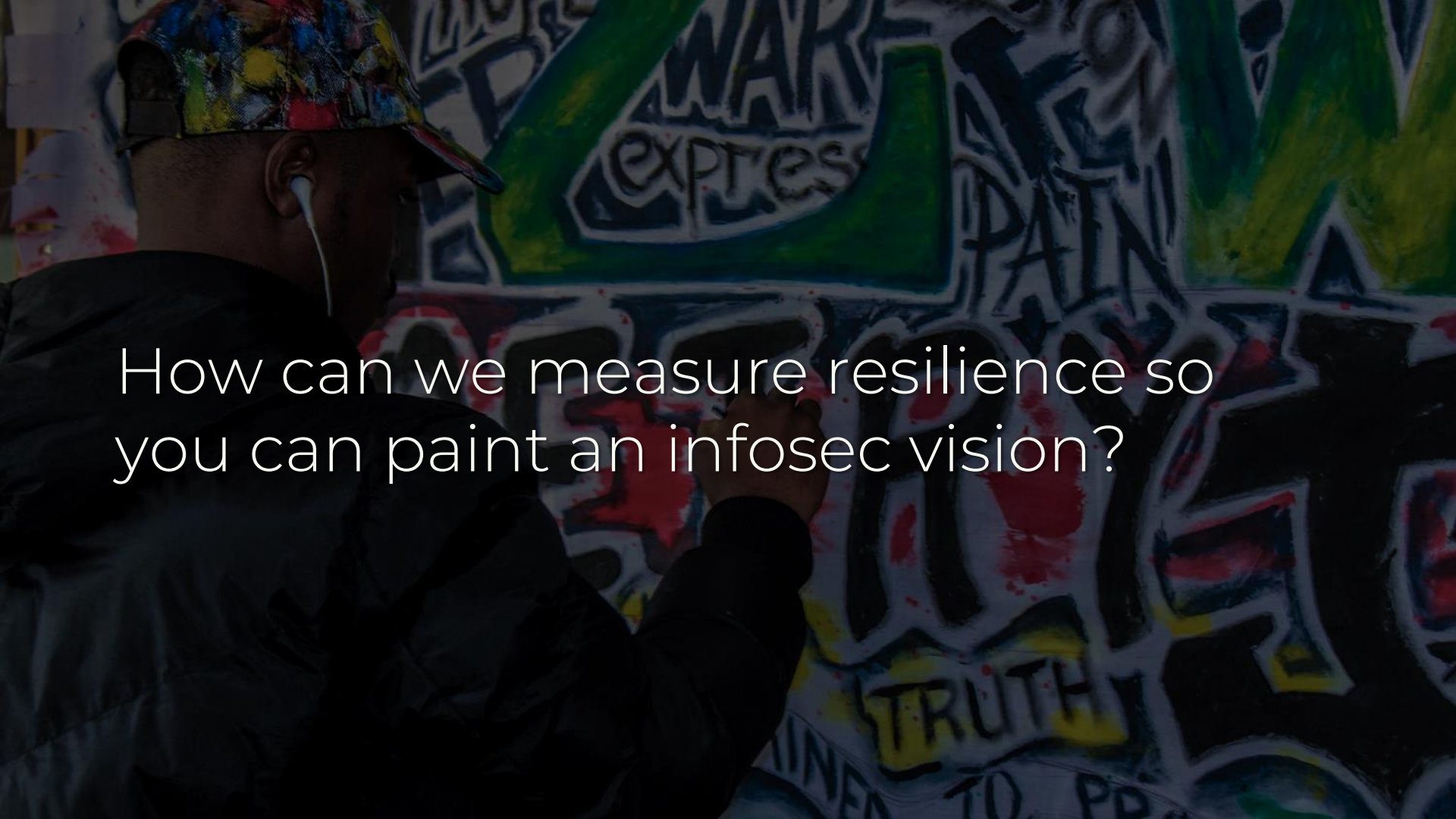
74 Retweets **280** Likes

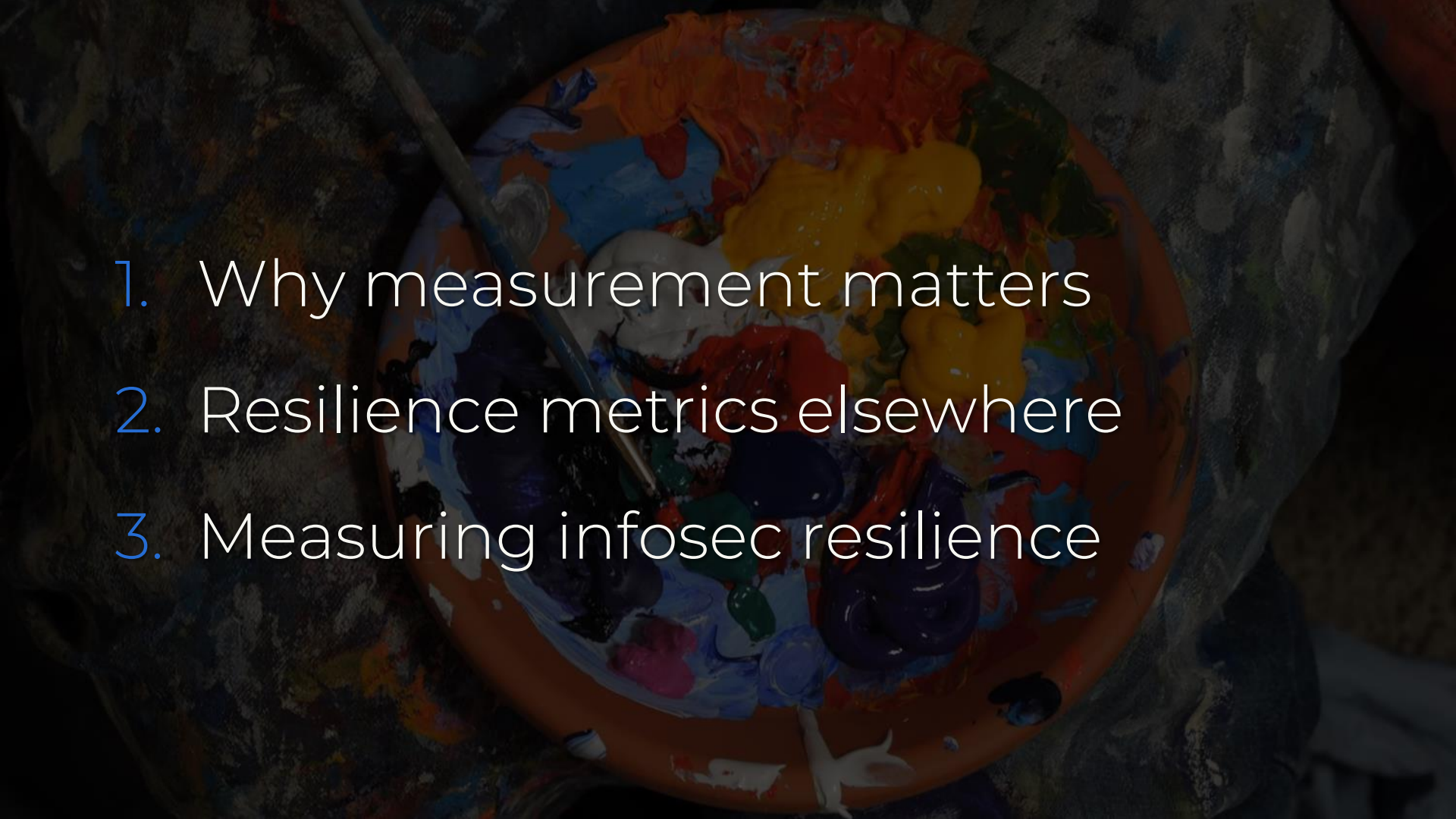

Security goes in circles because we
aren’t measuring it appropriately.


Infosec is not checklists.
Infosec is not dogma.
Infosec is not an end in itself.


Infosec is about protecting your
organization’s ongoing quest(s).


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


How can we measure resilience so you can paint an infosec vision?



1. Why measurement matters
2. Resilience metrics elsewhere
3. Measuring infosec resilience

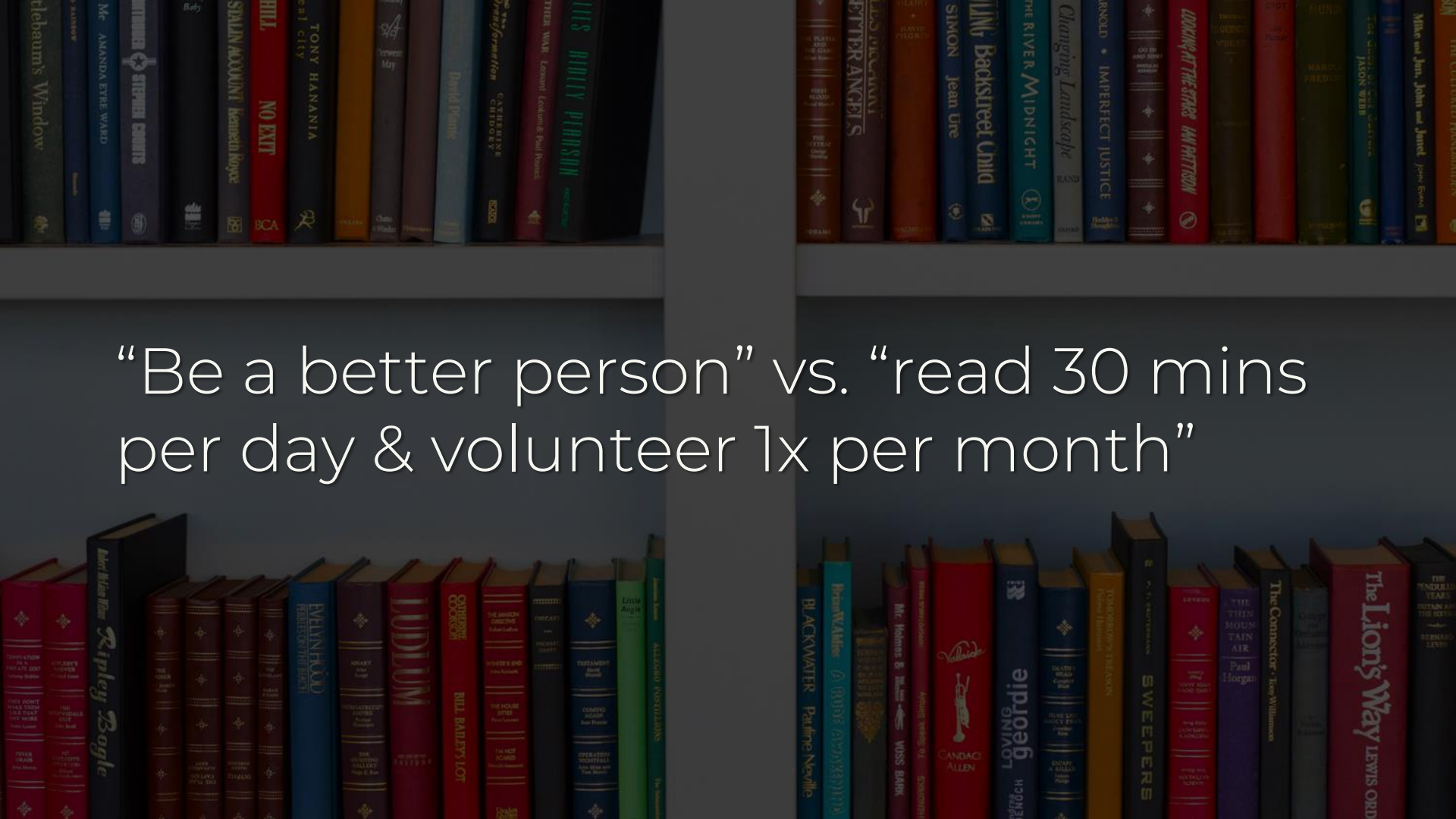

Why is measurement
important?

Generally we do something 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

Metrics are quantifiable measures to track & assess status



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

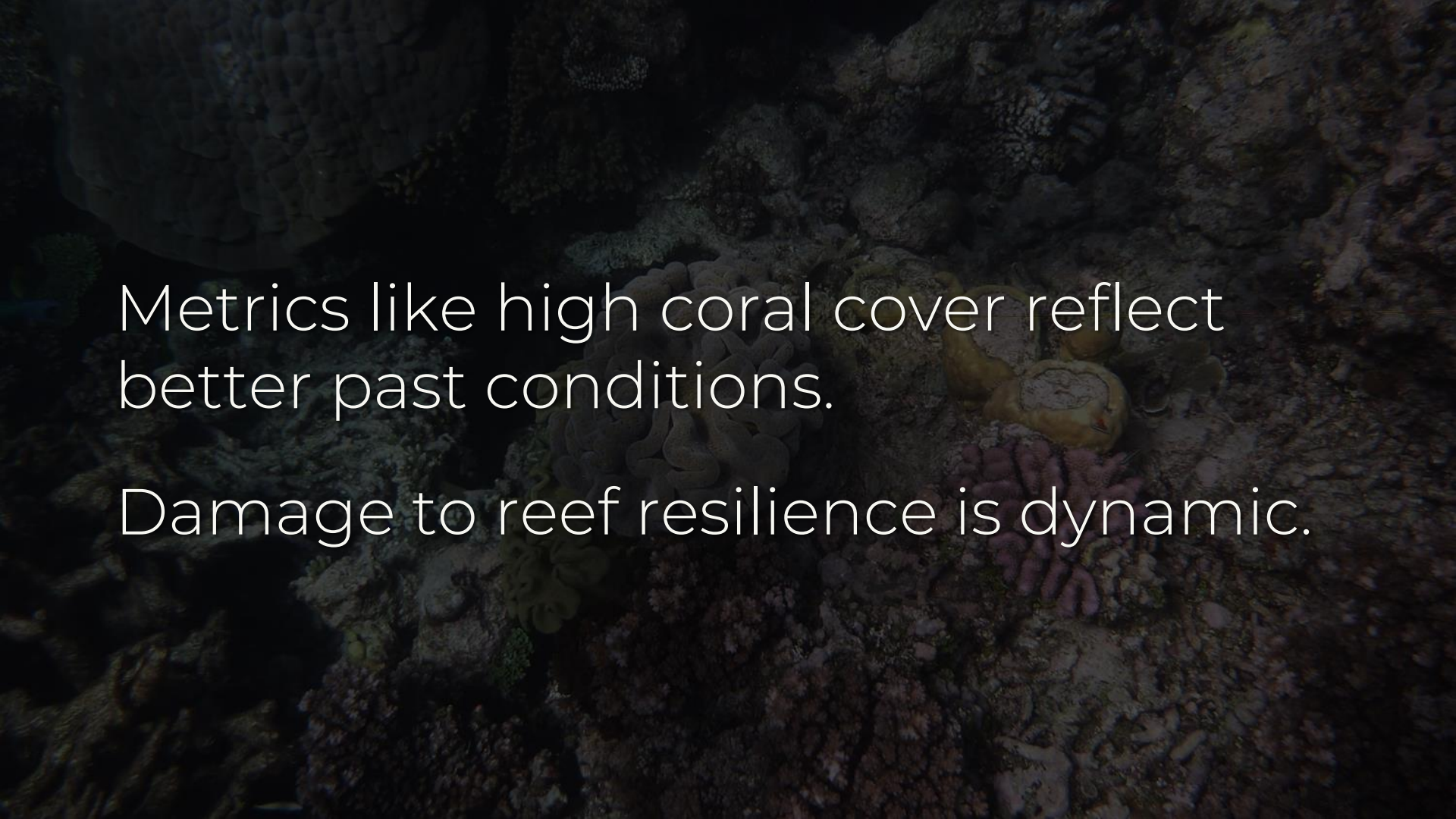

Success metrics create the numbers
by which you paint your vision


Resilience Metrics
Elsewhere

Resilience is a journey, not a singular, final destination

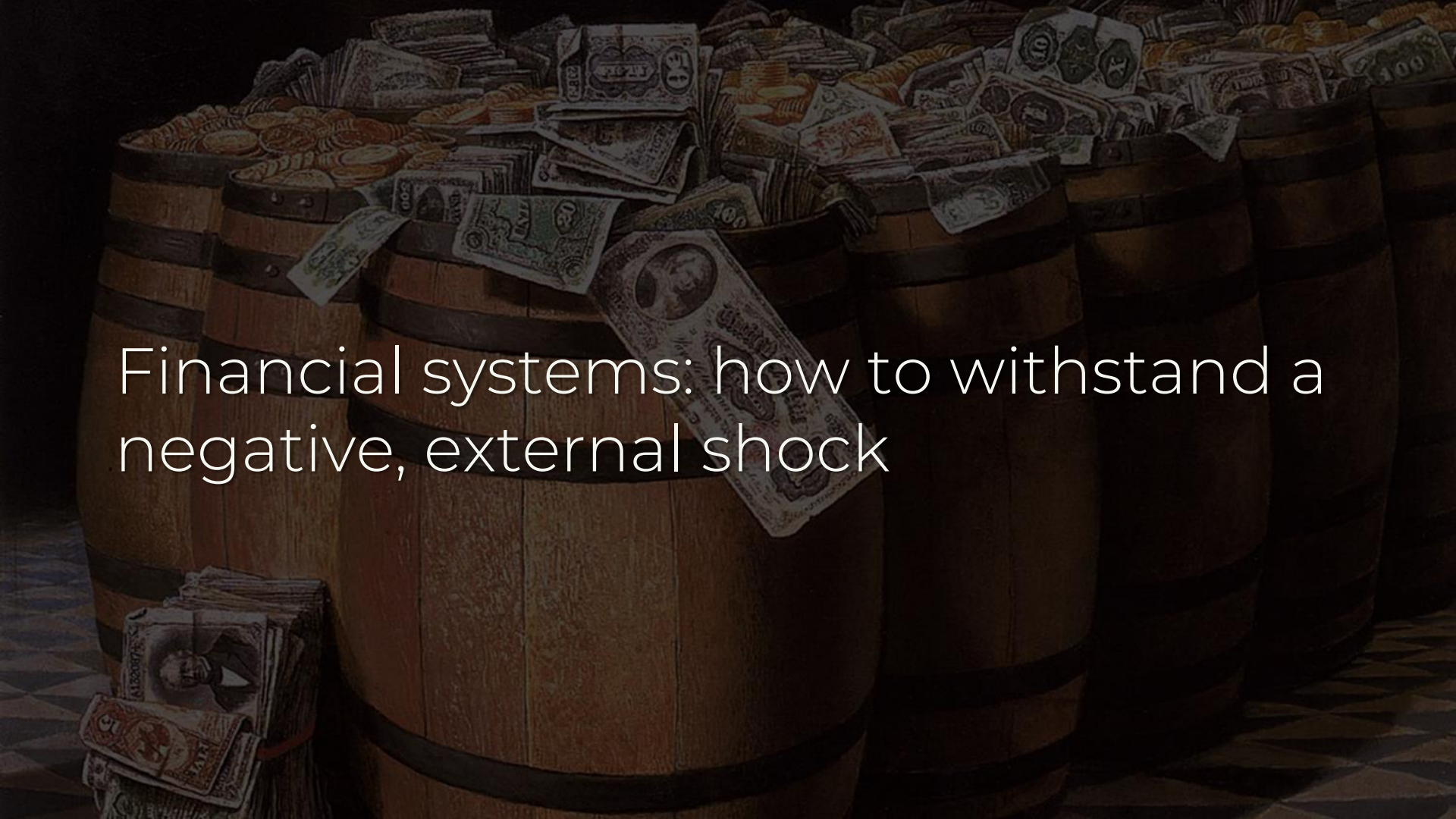

Natural disaster resilience must
assume failure of controls

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


Metrics like high coral cover reflect better past conditions.
Damage to reef resilience is dynamic.

Ongoing stress like ocean warming makes coral less resilient to cyclones

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

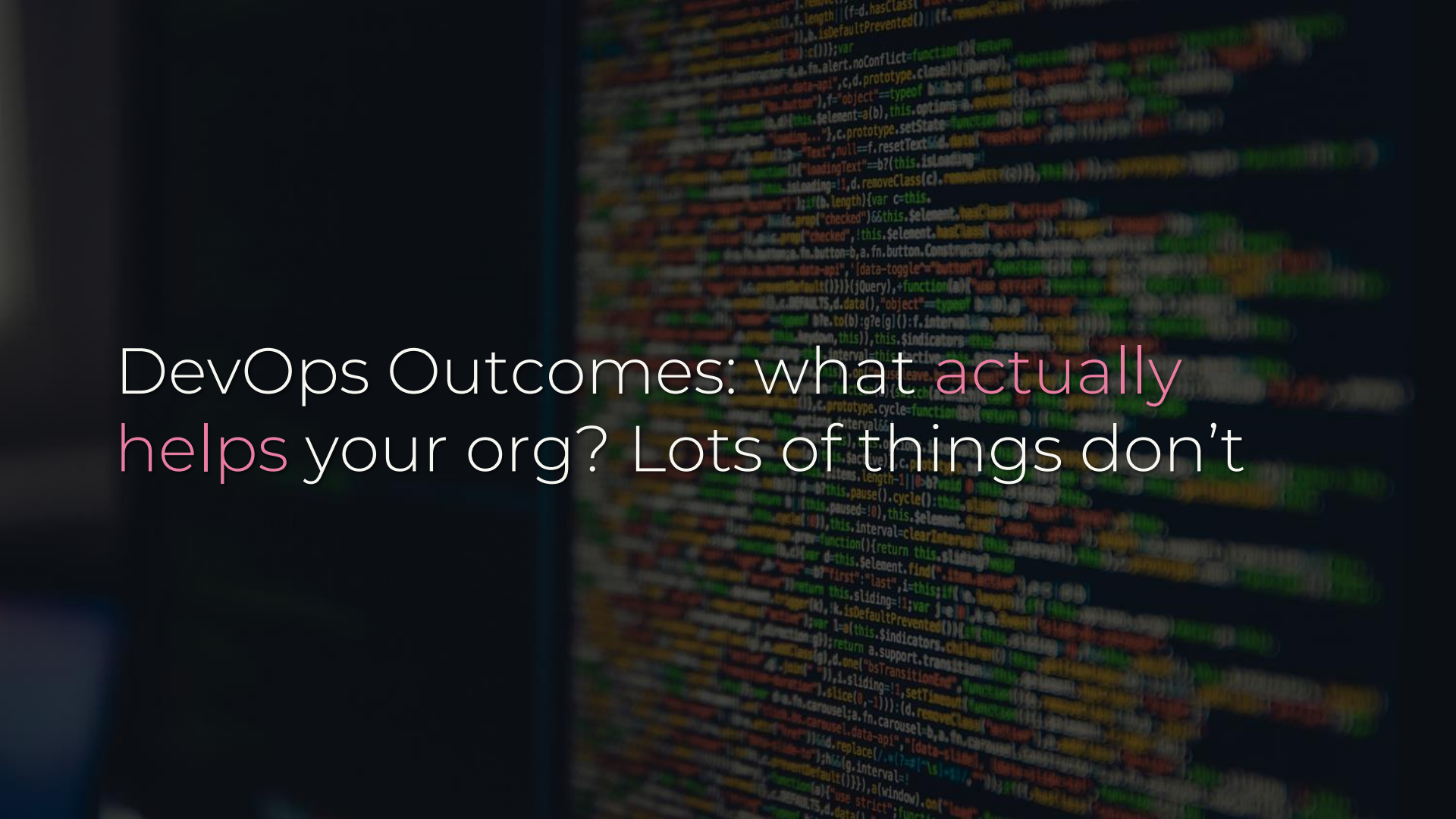


Financial systems: how to withstand a negative, external shock

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.


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

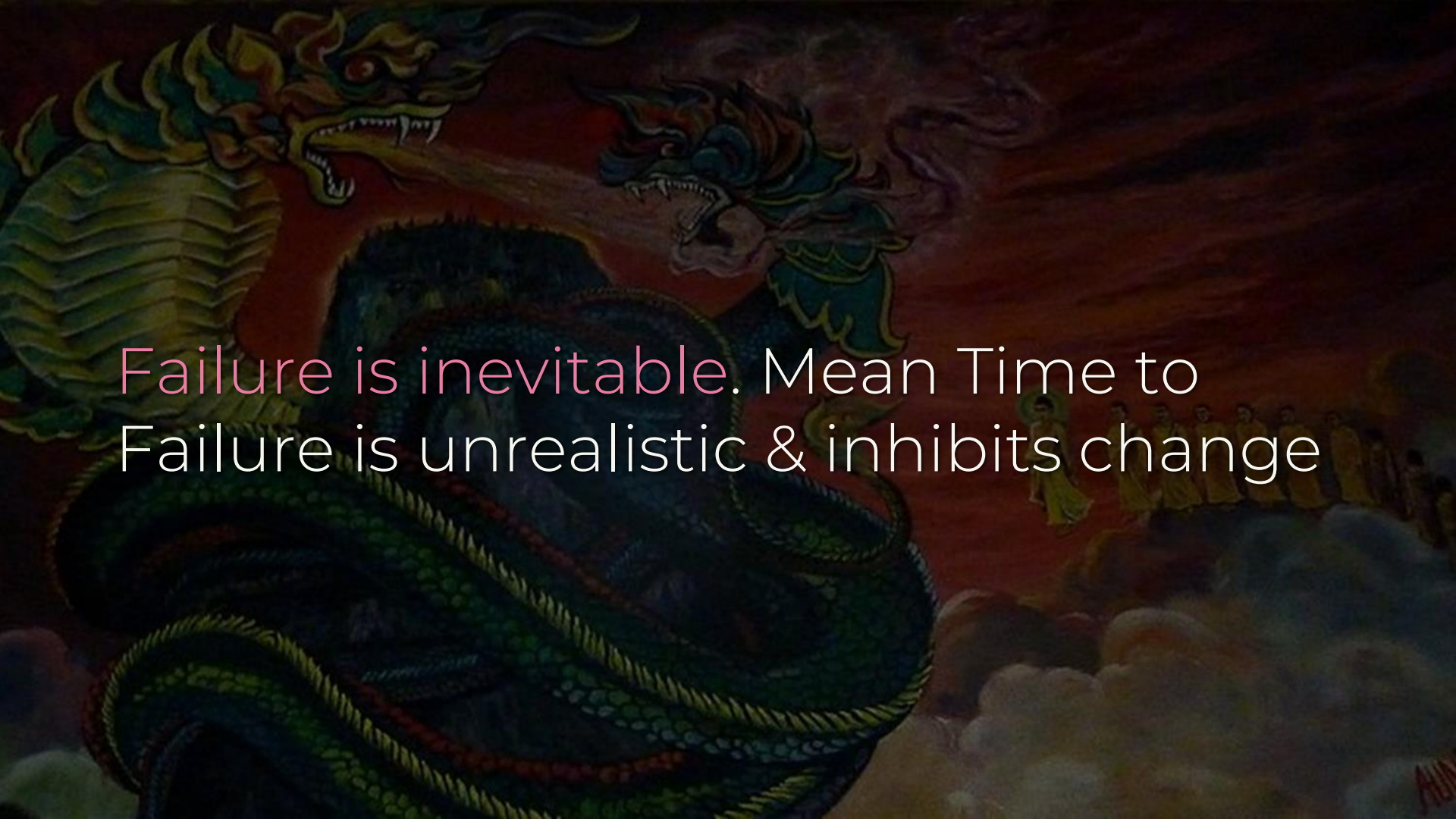
Elite DevOps performers:

Deploy frequency: on-demand

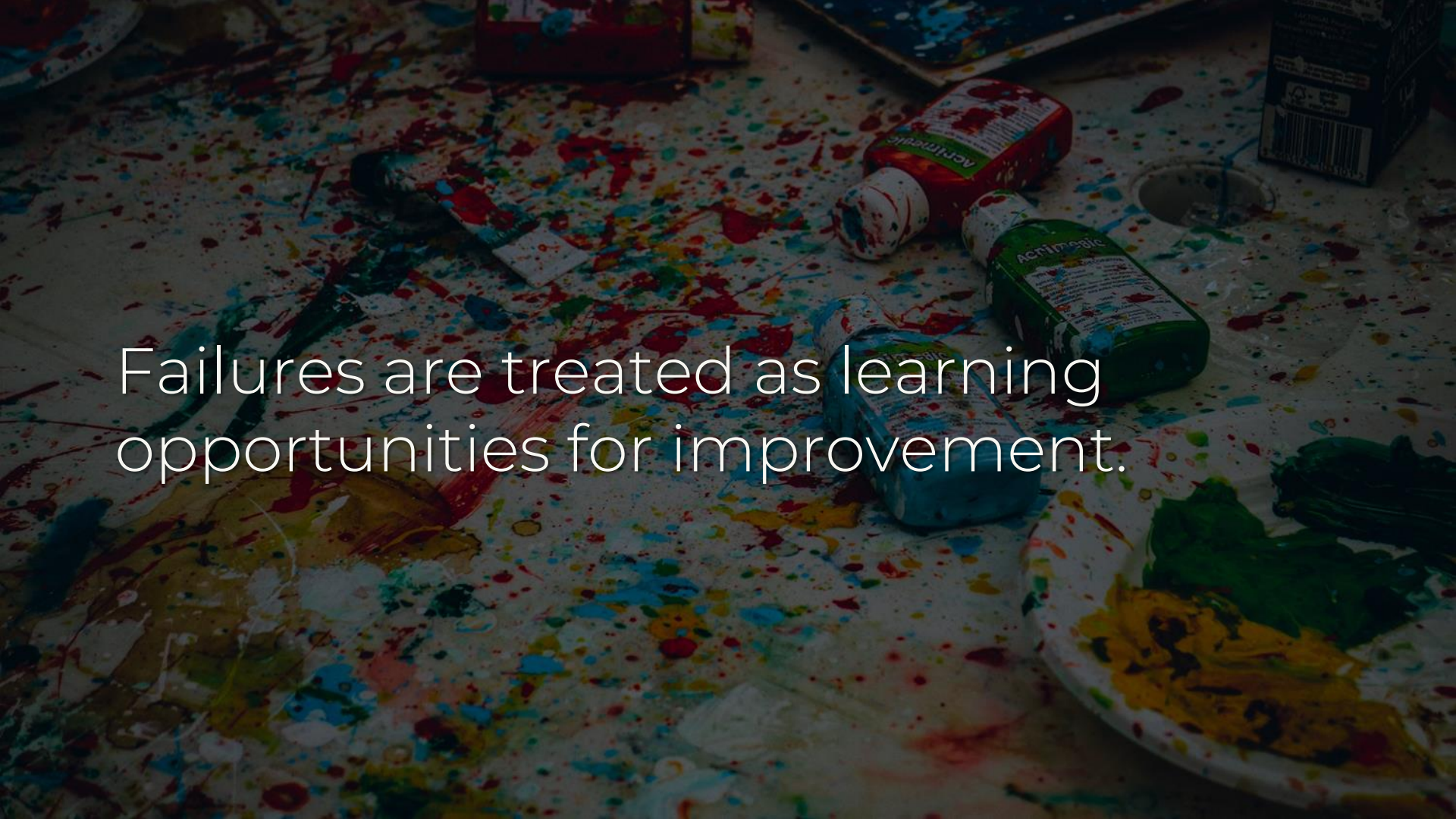
Lead time: <1 hour

MTTR: <1 hour

"Accelerate: State of DevOps 2018" report by DORA., 2018

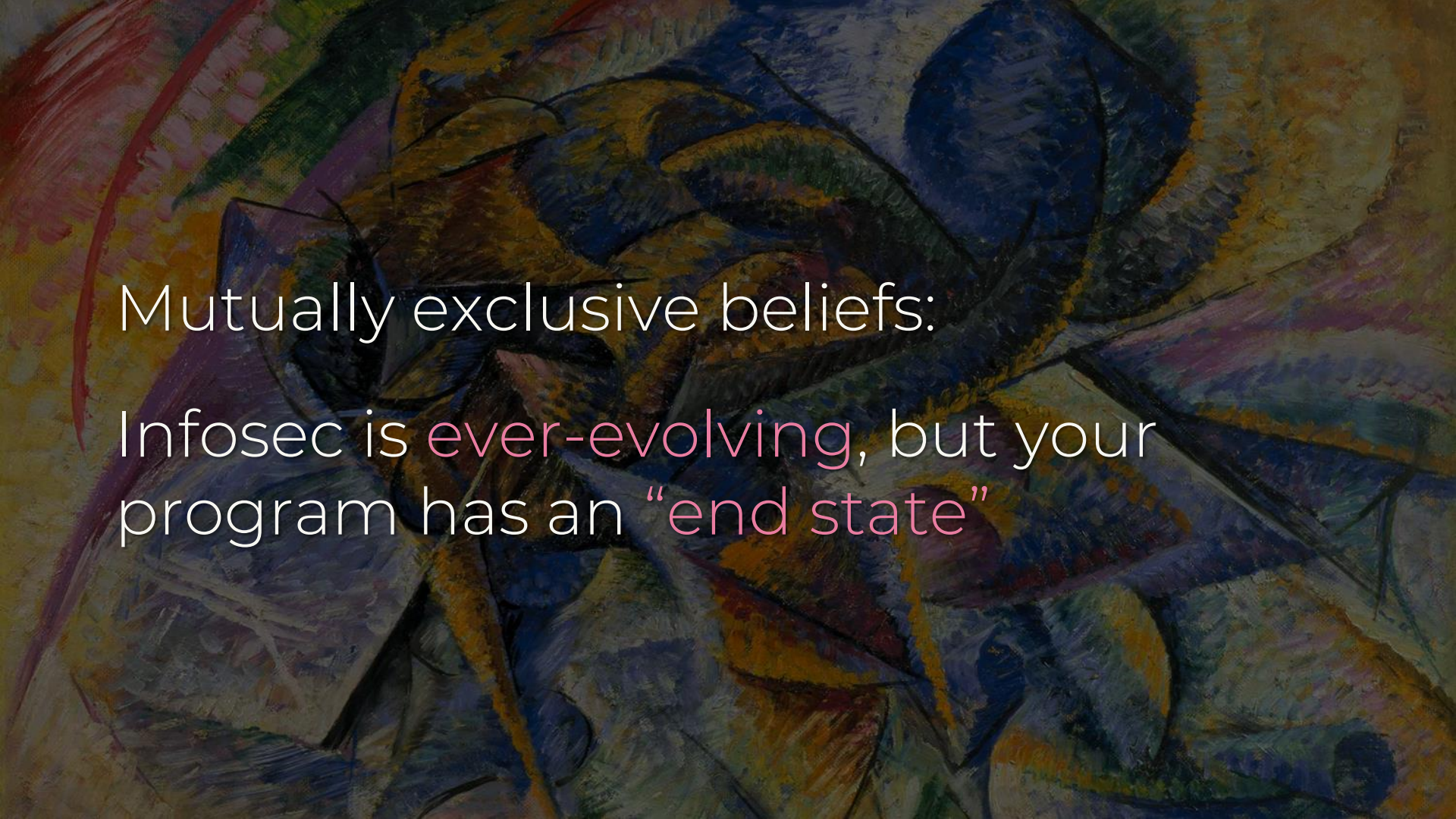

Failure is inevitable. Mean Time to
Failure is unrealistic & inhibits change

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


Failures are treated as learning
opportunities for improvement.

What resilience metrics can we take from this to use in infosec programs?


Measuring InfoSec
Programs



Mutually exclusive beliefs:

Infosec is ever-evolving, but your program has an “end state”

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

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


Measure impact both ways: improved security vs. more friction

Positive: reduction in number of security fixes per project

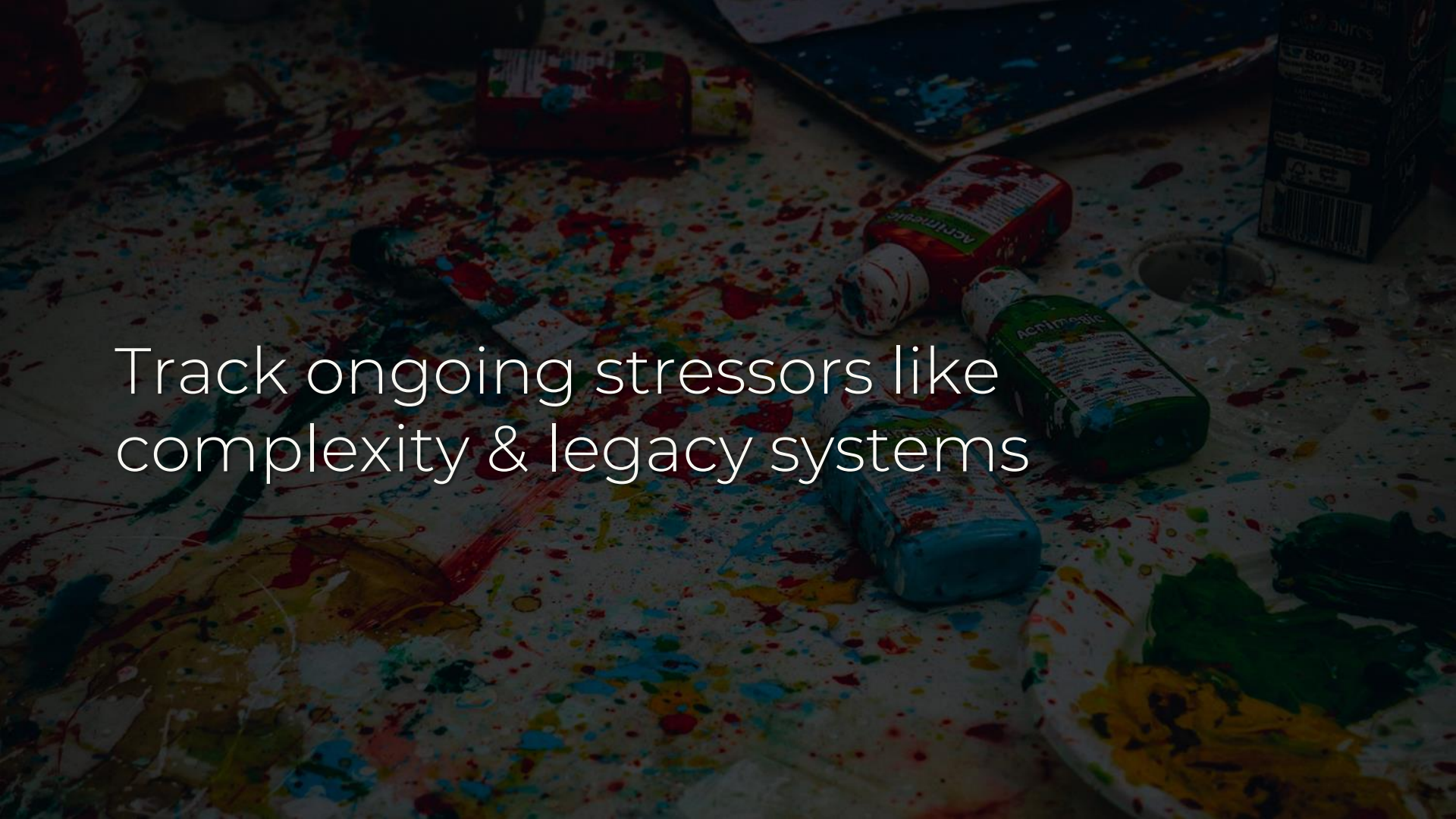
Negative: increase in employee time spent using security tools

“Elite performers build security in and can conduct security reviews & complete changes in just days.”

– State of Dev Ops 2018

Absorbing an attack: can you adapt efficiently?

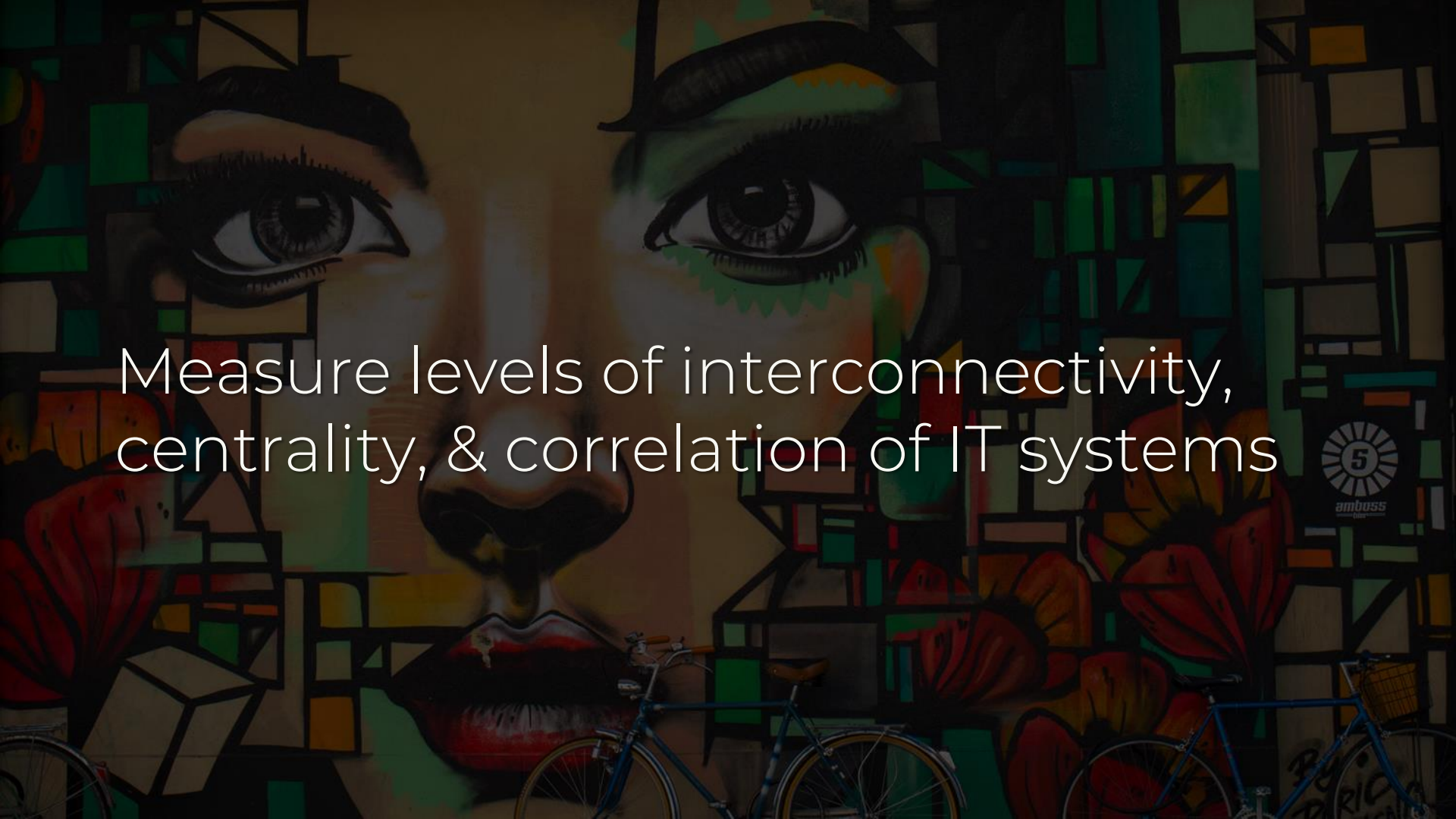
Impact of a new vulnerability depends on erosion by ongoing stress


Track ongoing stressors like
complexity & legacy systems

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

Deploy frequency of security changes (patches, access control rules, etc.)

Reorganize around the threat: can you transform & innovate?


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

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

Unpatched databases without authentication = high PPP

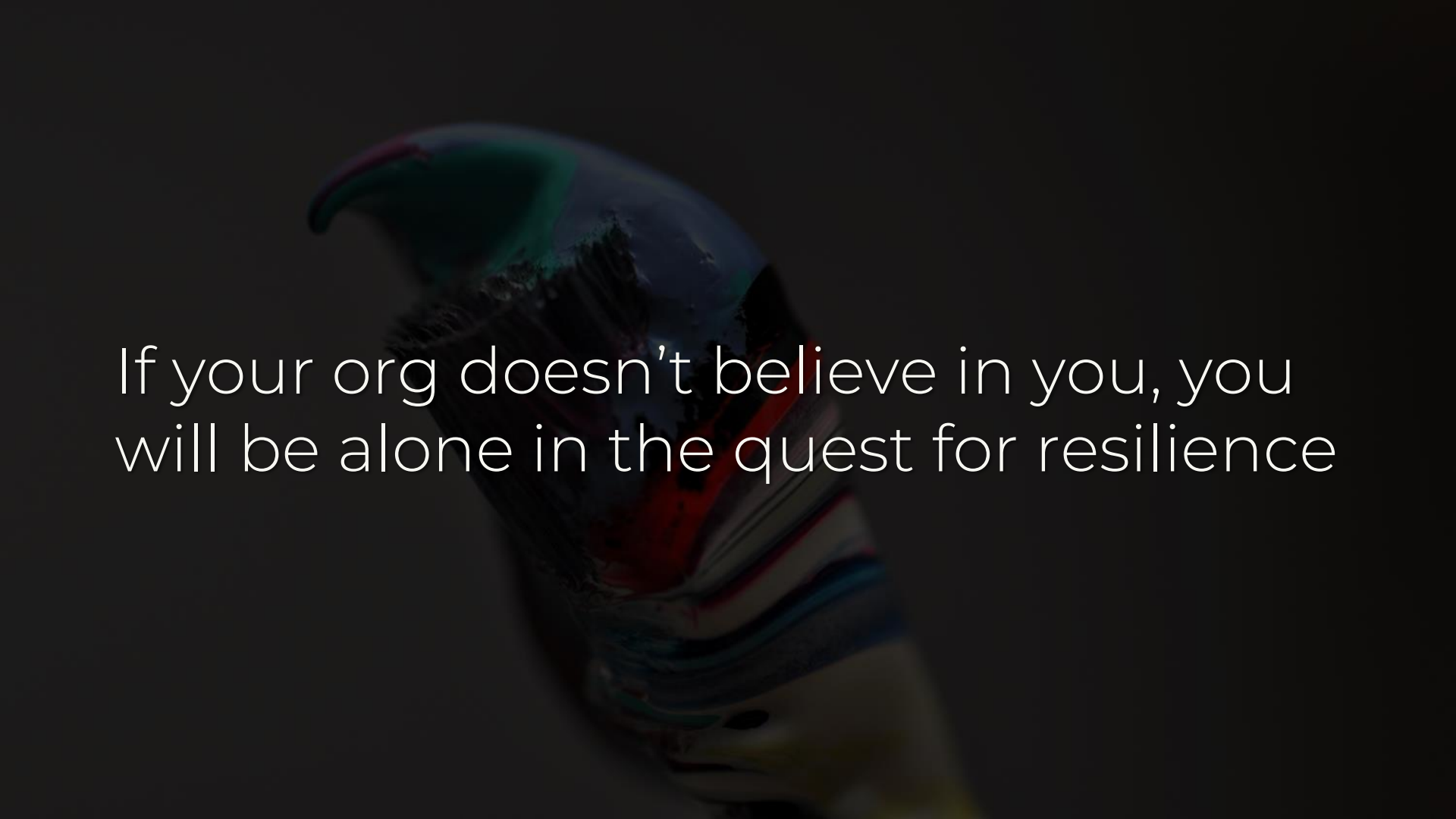

How strong is your culture? Are you actually mission-oriented?

Equifax blamed one person for failing to deploy a patch.

Don’t do that.

Net Promoter Score (NPS): Mathematical calc of satisfaction

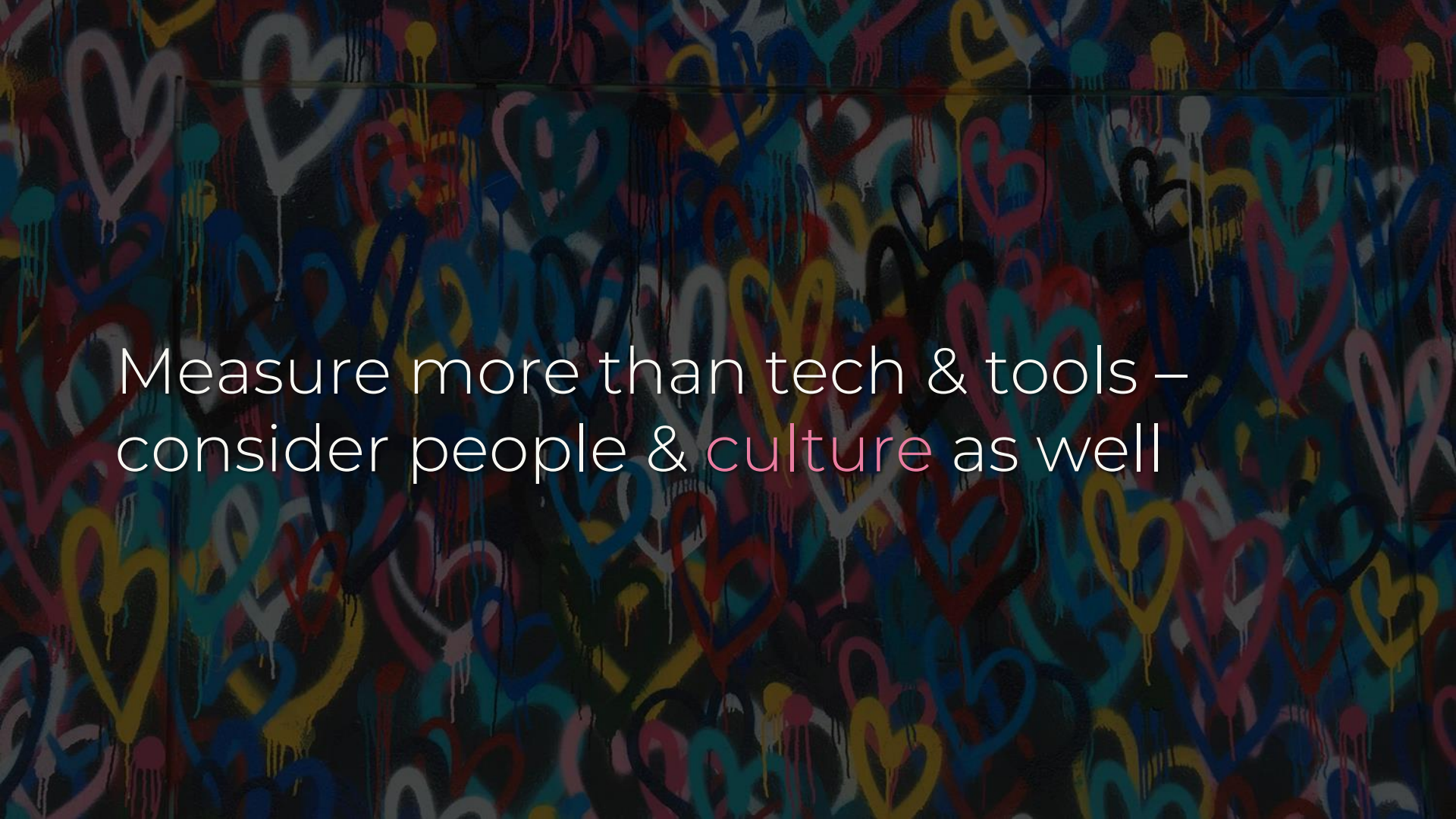
Measure NPS among your colleagues & teams with whom you work


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


Conclusion


Measure resilience – flexibility,
adaptability, transformability

Measure how security is helping your organization & protecting its goals


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


“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
- "Accelerate: State of Dev Ops 2018," DORA, 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