

GUARDIANS OF THE GALAXY

Architecting a culture of
secure software

LAURA BELL

FOUNDER AND CEO: SAFESTACK

@lady_nerd laura@safestack.io

<https://safestack.io>





In this talk

Everything is not awesome

The reality of our 'threat landscape' and the need for change

Security at speed

Shifting mindsets and adapting to our new environment

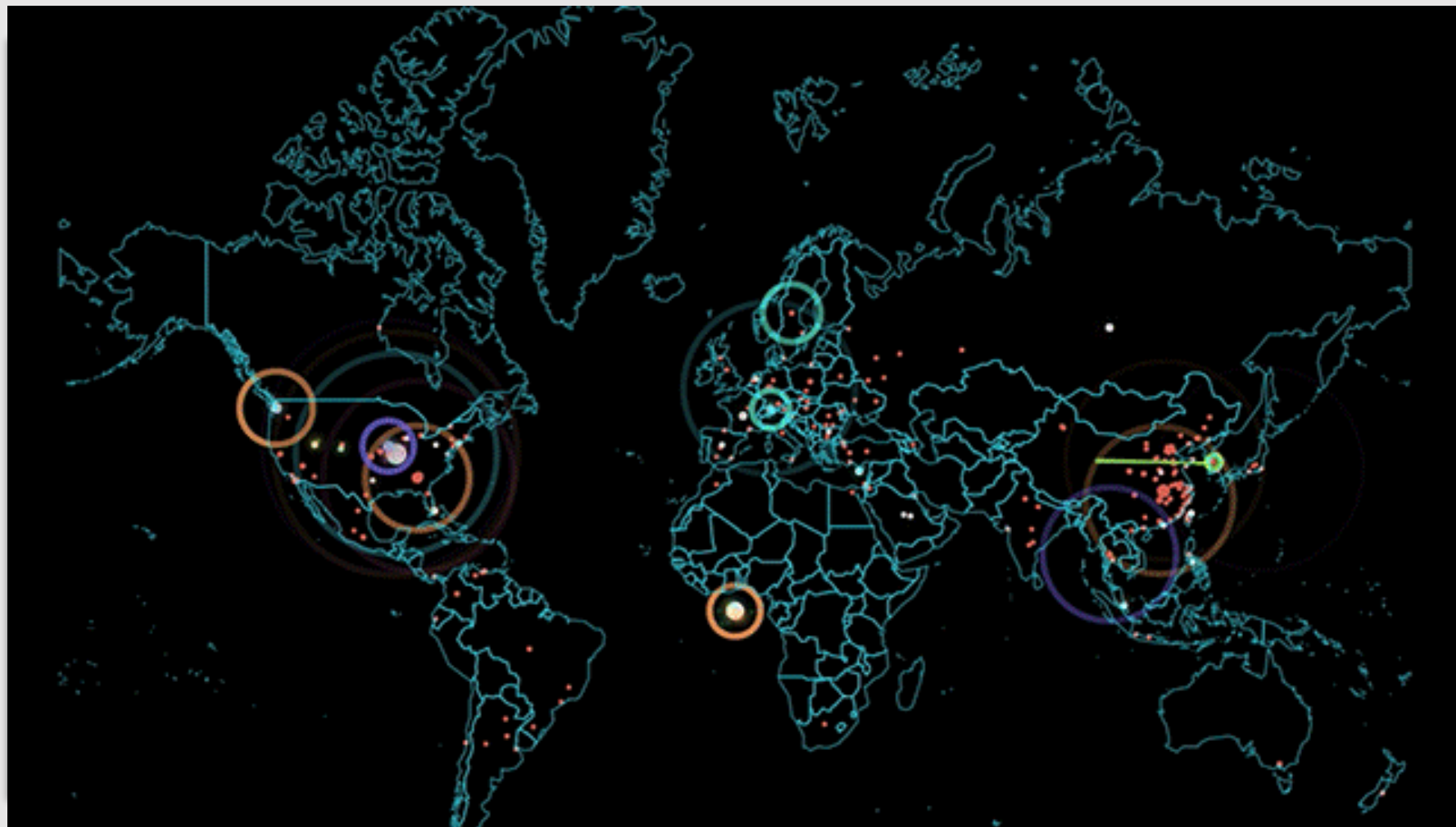
Architecting conscious security culture

Building a security-by-default culture



Everything is
not awesome



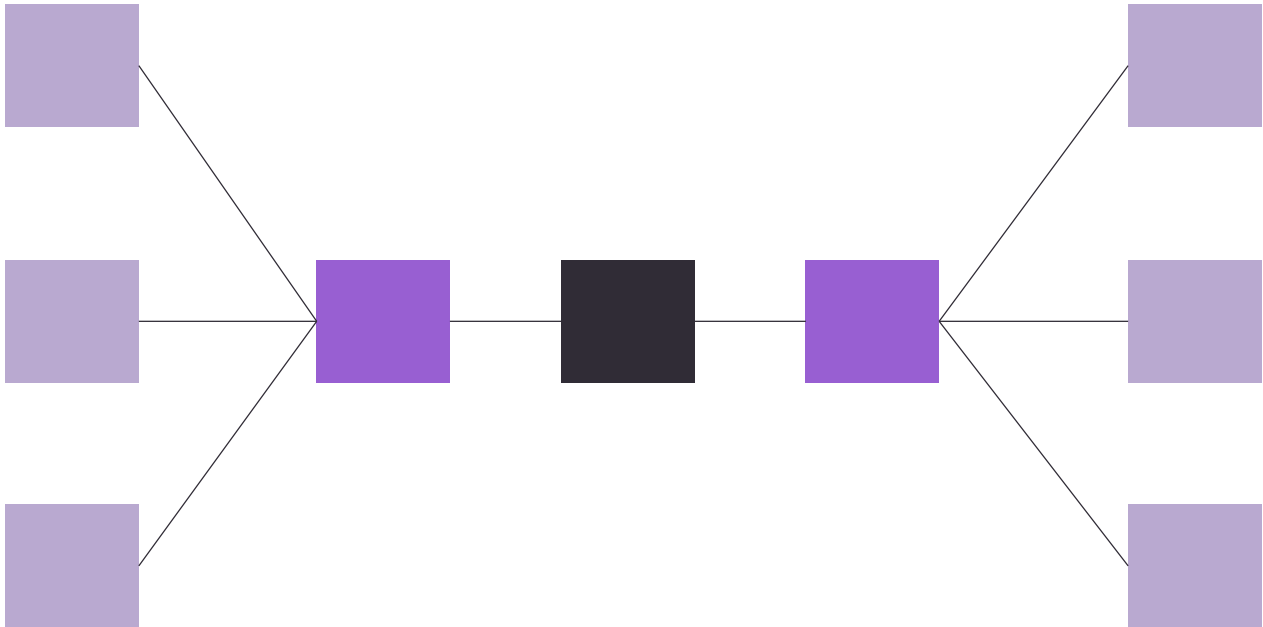




Sidenote

Shiny Pebbles are kind of interesting River rocks that shine under moonlight were often volcanic. Volcanic rocks don't get compromised under high temperatures and shatter.

“Shiny Pebbles” became a highly sought after cooking tool that would be passed between generations and had significant value both culturally and economically in Polynesian cultures.



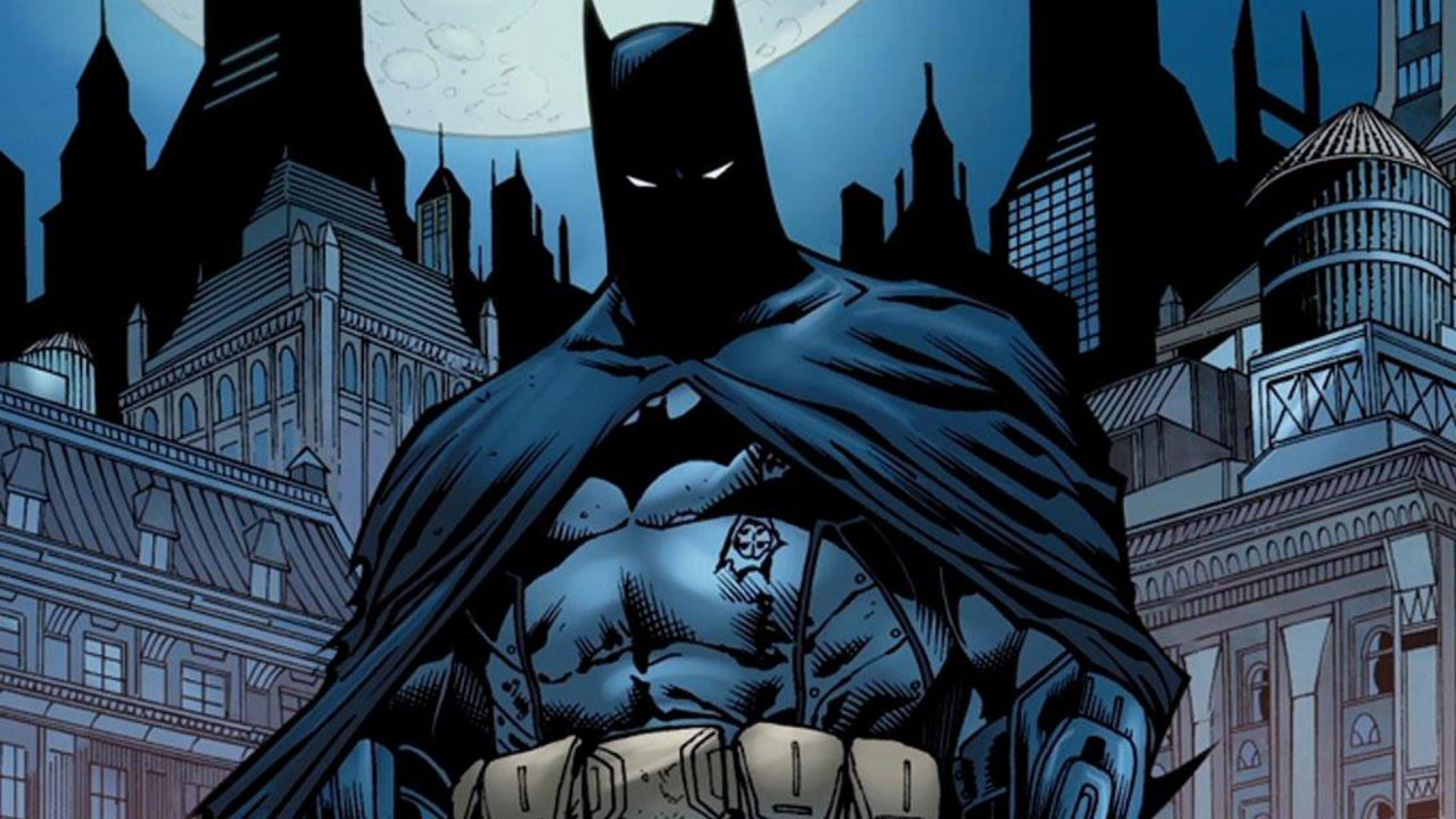
Knights

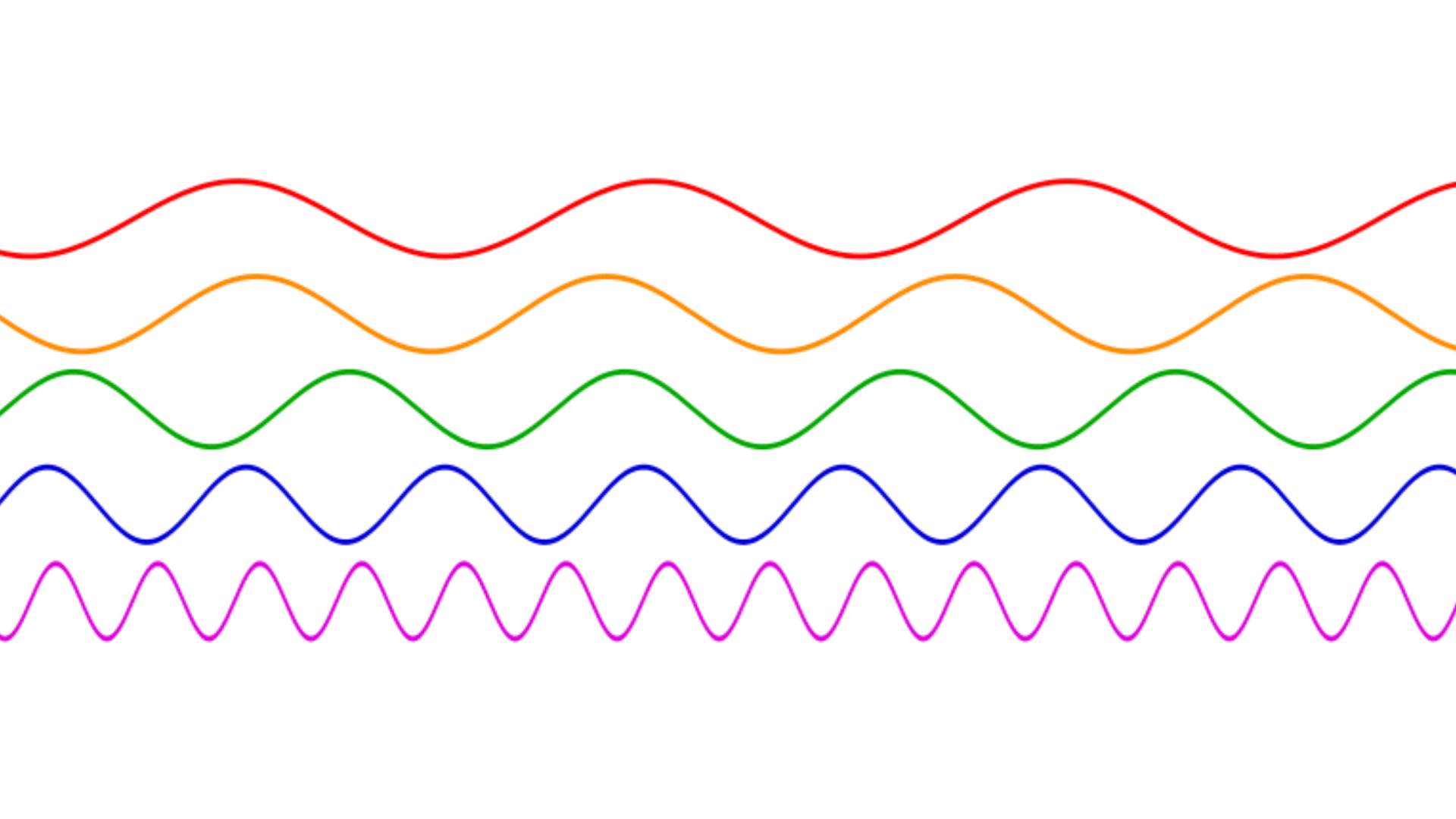
Warriors

Armies

Law Enforcement

Security Managers





Hire more security people!



DC
JUSTICE LEAGUE

Everyone expects your security team to be a team....

Many hats not many people



OC-CIS-VS AB ORI-GINE M-VN-DI

Fear
Vulnerability
Shame
Isolation
Uncertainty



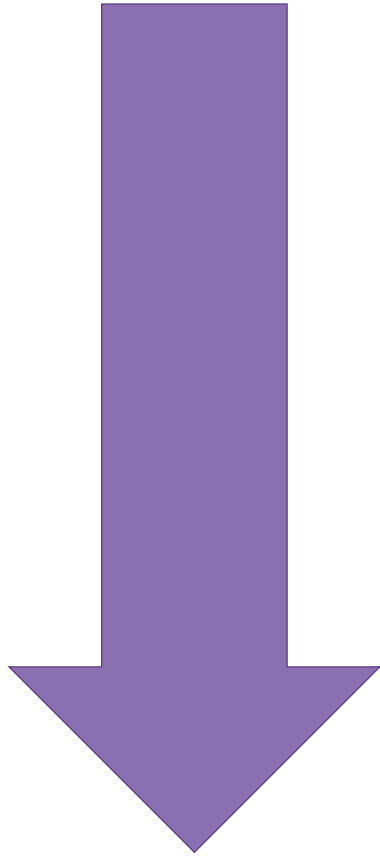
4 million people
35 penetration testers
450 security professionals
1.2 per security team

P.S we are hiring



Security at speed





absent

ad-hoc

gated

agile

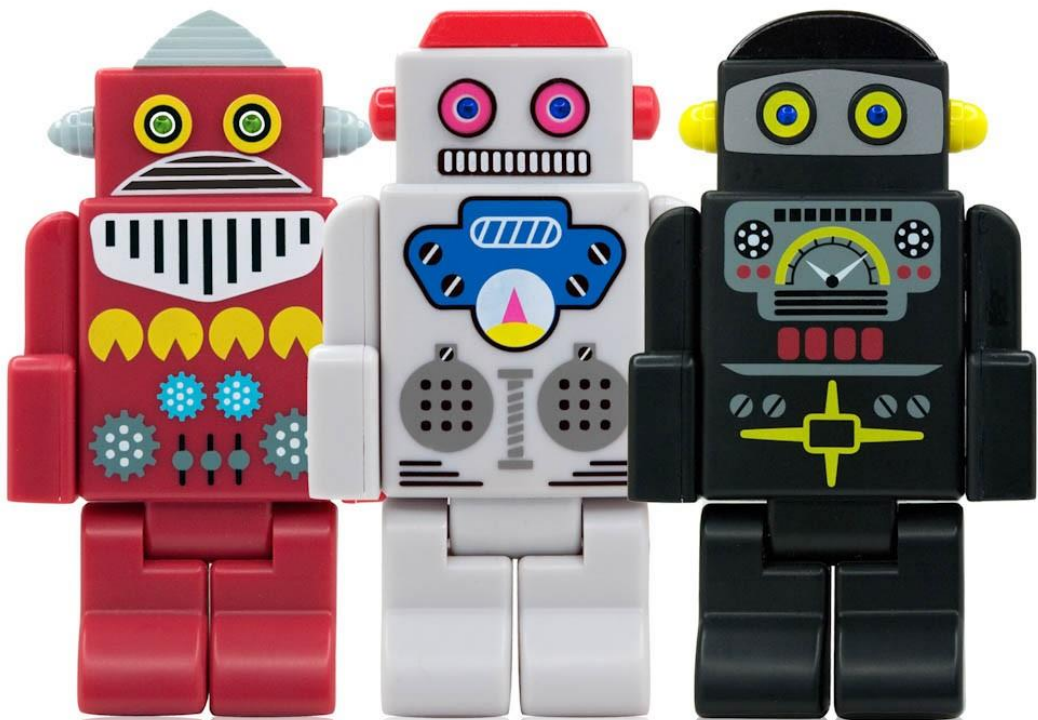
continuous

continuous security is

**automated
autonomous
integrated
repeatable
scalable
measurable
respectful**

“the best technical people I know work
really hard to make themselves redundant”

automated



Deployment

Provisioning

Testing

Static analysis

Vulnerability mgmt

“no bottlenecks, breakdowns or ripples”

autonomous



Skills
Authority
Accountability



every team

“bite-sized security that works with every step
of your lifecycle”

integrated

Dependency checkers

Static analysis and code review

Integrate security into your pipeline

Vulnerability scanners

Threat assessment tools

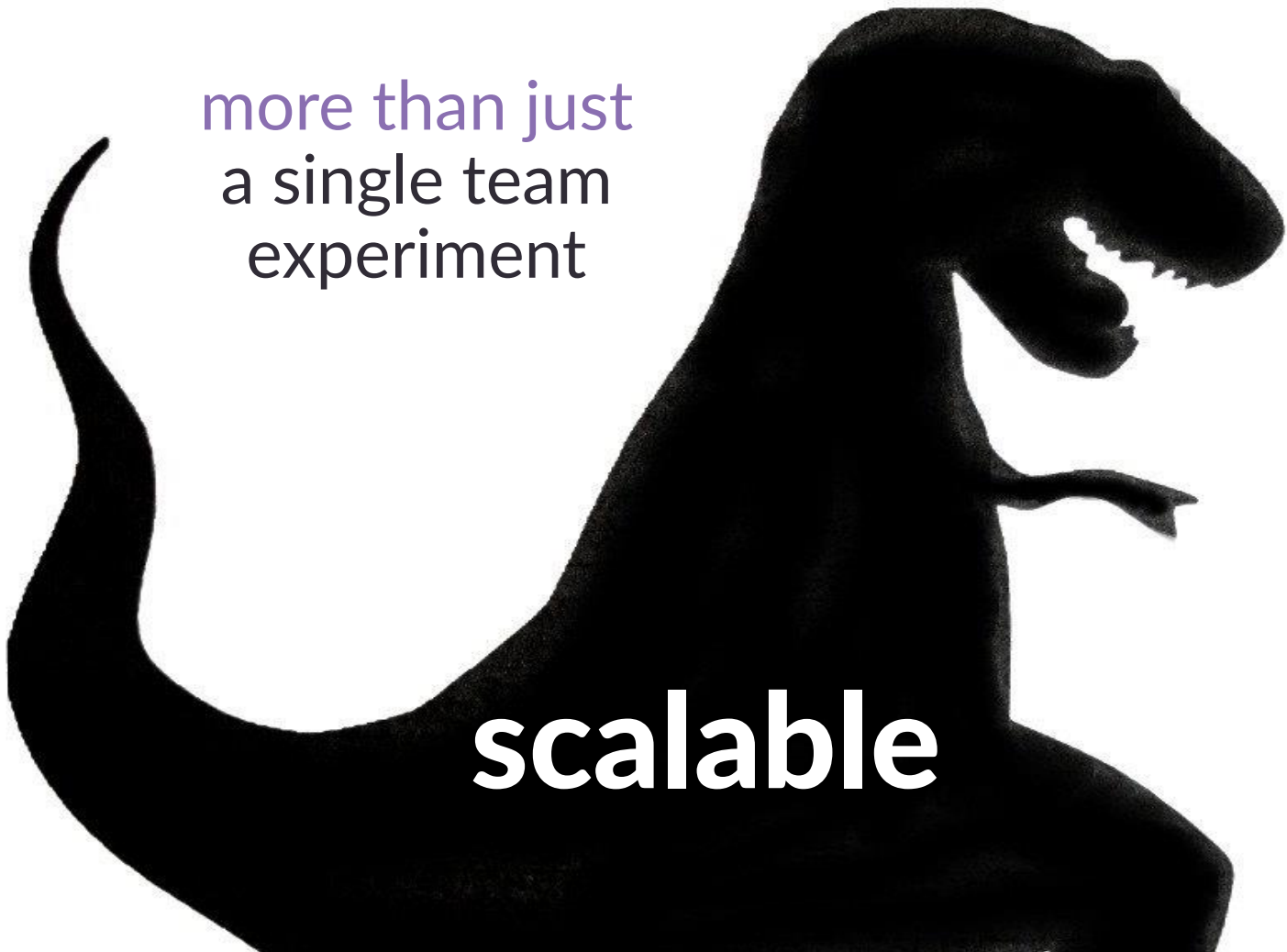
Requirements generators

Woven in to keep you going

Respected enough to stop you

“security fails when it’s a special event”

repeatable

A black silhouette of a T-Rex dinosaur, shown in profile facing right. The dinosaur's mouth is open, revealing its teeth. The tail is long and curved downwards. The overall shape is solid black against a white background.

more than just
a single team
experiment

scalable

if you can't measure it, how do you know you
made things better?

measurable

every action has a cost, value the time and resource needed to complete an action

respectful

Architecting conscious security culture





hire good people

“learn what good means for your organisation”

keep good people

money isn't normally the only factor

skills, authority, accountability
increase effectiveness in role

Agency
Incentivization
Acknowledgement

increase loyalty to role

blameless (fearless)

extend blameless culture to security

Use understanding attack and risk as problem solving,
creative, lateral thinking

You shouldn't feel naughty

You shouldn't feel sad

data driven security

take out the emotion, measure and respond

Patch adoption

Upgrade rates

User profiles (technology and usage)

Device patterns

Browser patterns

Chronological and location patterns

Error rates

Query times

Query data set size and complexity

language matters

consistent, concise, inclusive

sustainability and stamina

save crisis responses and stress for special
occasions

TL;DR

Everything is not awesome

The reality of our 'threat landscape' and the need for change

Security at speed

Shifting mindsets and adapting to our new environment

Architecting conscious security culture

Building a security-by-default culture



QUESTIONS

LAURA BELL

FOUNDER AND CEO: SAFESTACK

@lady_nerd laura@safestack.io

<https://safestack.io>

