LDX3
By LeadDev

Being Secure-By-Design

Engineer Led Security

Dan Abel : PLEO

LDX3
By LeadDev

Being Secure-By-Design

Engineer Led Security

Dan Abel : PLEO

IT'S OK TO NOT BE A SECURITY EXPERT!

Getting to know you - hands up!

1. Who worries about a bad actor penetrating their systems?
2. Who worries about an official body issuing fines or taking away a license to operate?
3. Who worries that their engineering teams may not be ready to control these risks?

These are reasonable worries.

M&S

These are reasonable worries.

M&S

Challenge

Solution

What we did

Impact

Close

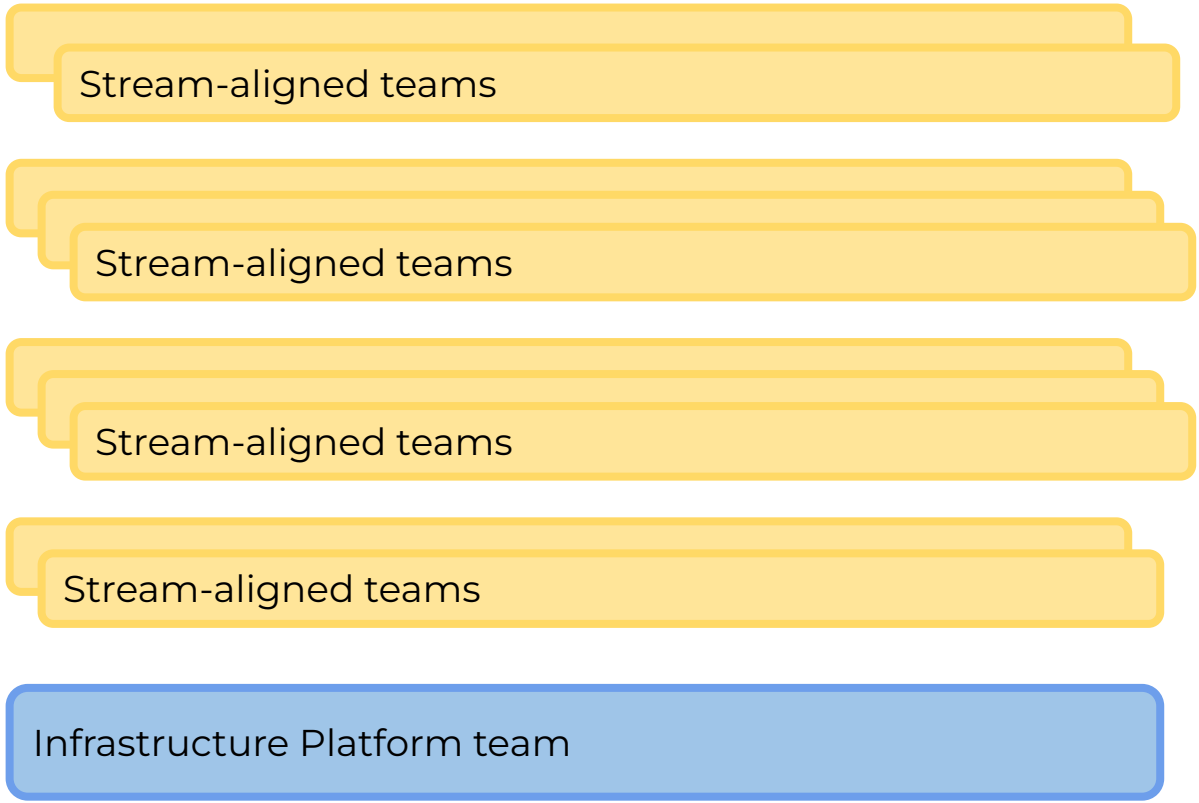
Tes: an 100 year old education company

Becoming Digital

10
teams

50
engineers

140
micro-services



Concepts from Team Topologies
By Matthew Skelton & Manuel Pais

THE CHALLENGE

Many **precious** things to **protect**

Risk to
reputation,
operation
and
teacher data

Risk to our
autonomous
& **high trust**
teams

Challenge | **Solution** | What we did | Impact | Close

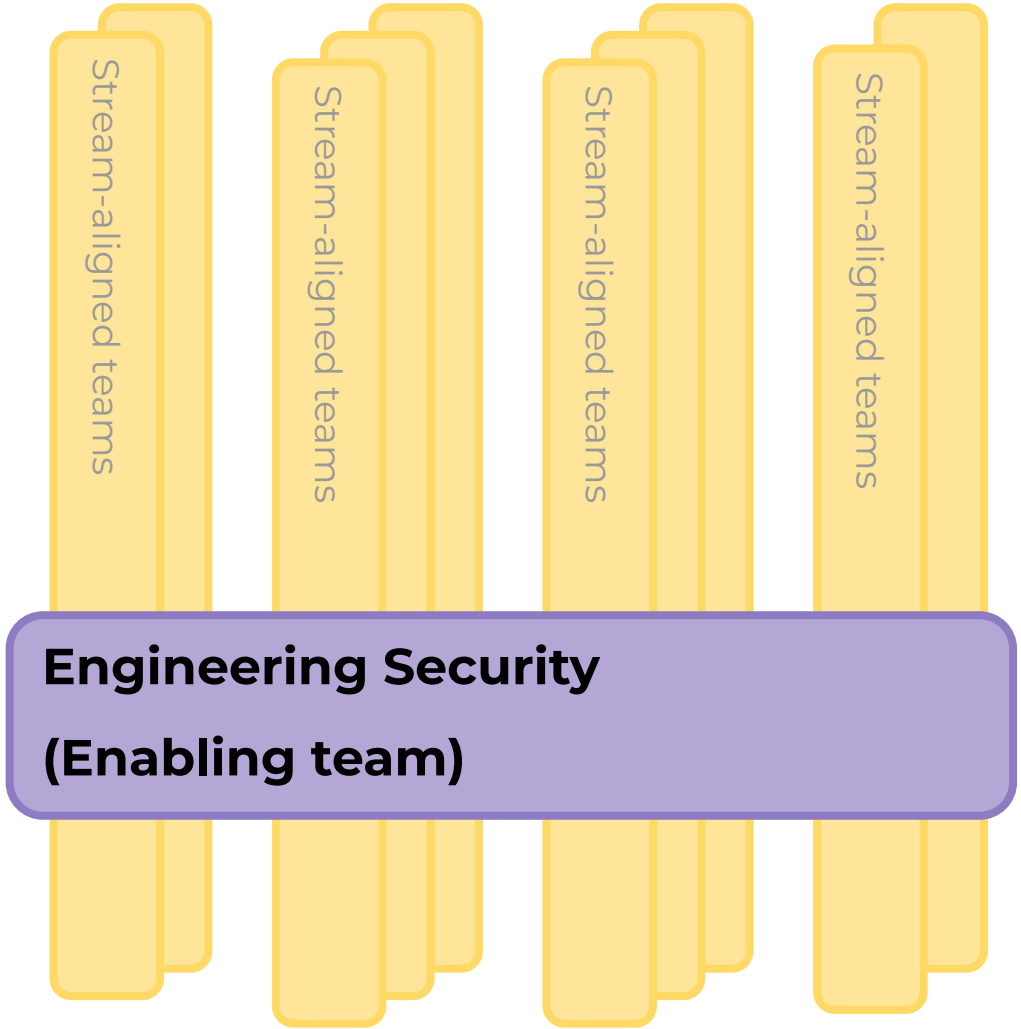
OUR SOLUTION

Engineer-Led Security

Why did we think this was possible?

We were inspired by
Shannon Lietz,
a DevSecOps leader

(GOTO 2015 • The Road To Being Rugged)


Stream-aligned teams
Stream-aligned teams
Stream-aligned teams
Stream-aligned teams
Engineering Security
(Enabling team)

SPOILERS!

It worked

Challenge | **Solution** | What we did | Impact | Close

The eng-sec team

And then...

Me
(lead)

+

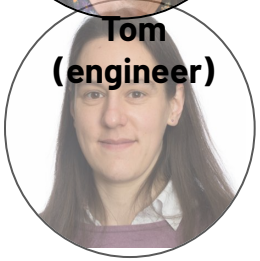
Tom
(engineer)

&

George
(engineer)

Me
(lead)

+



Amélie
(engineer)

&

Charlotte
(engineer)

Real world planning

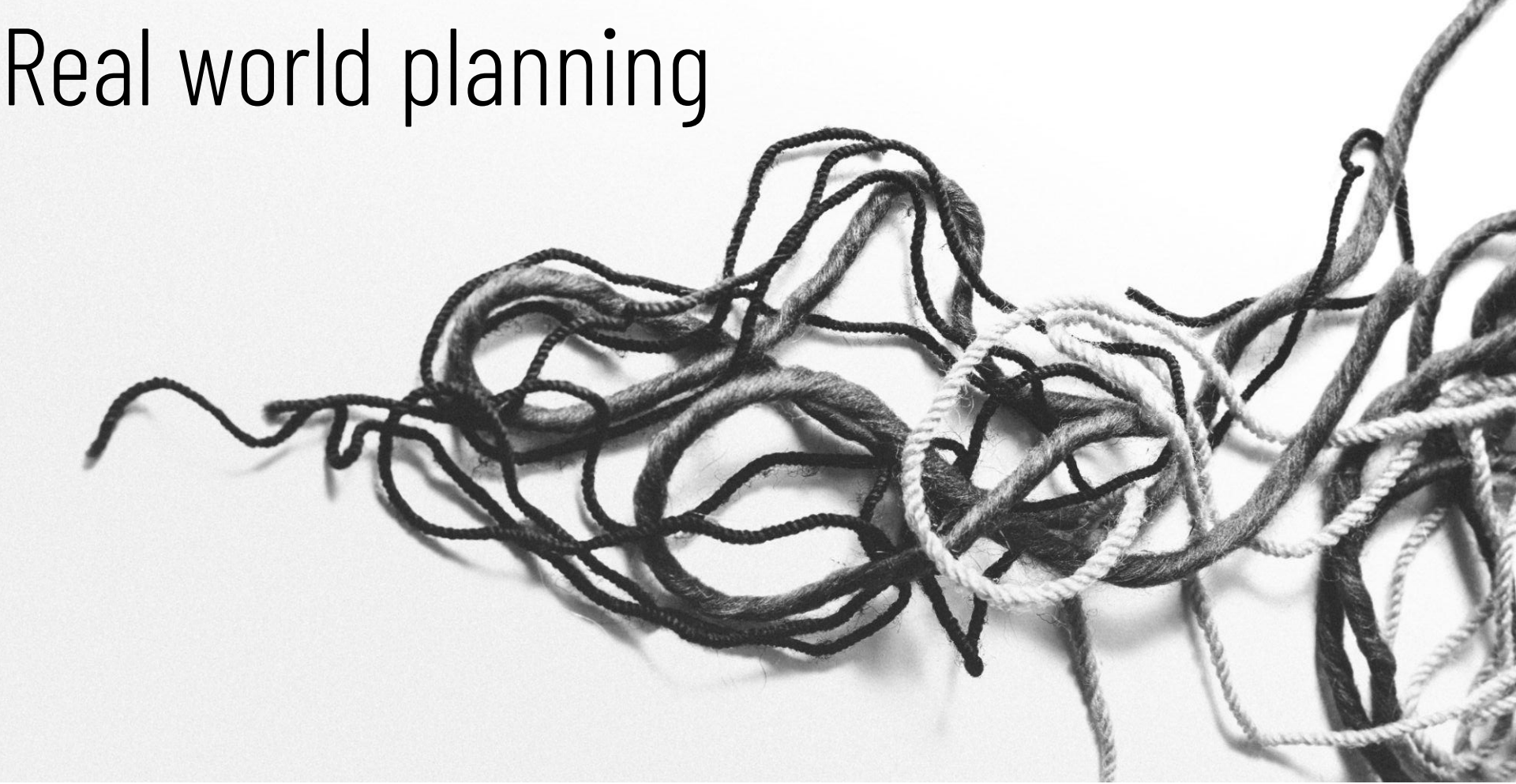
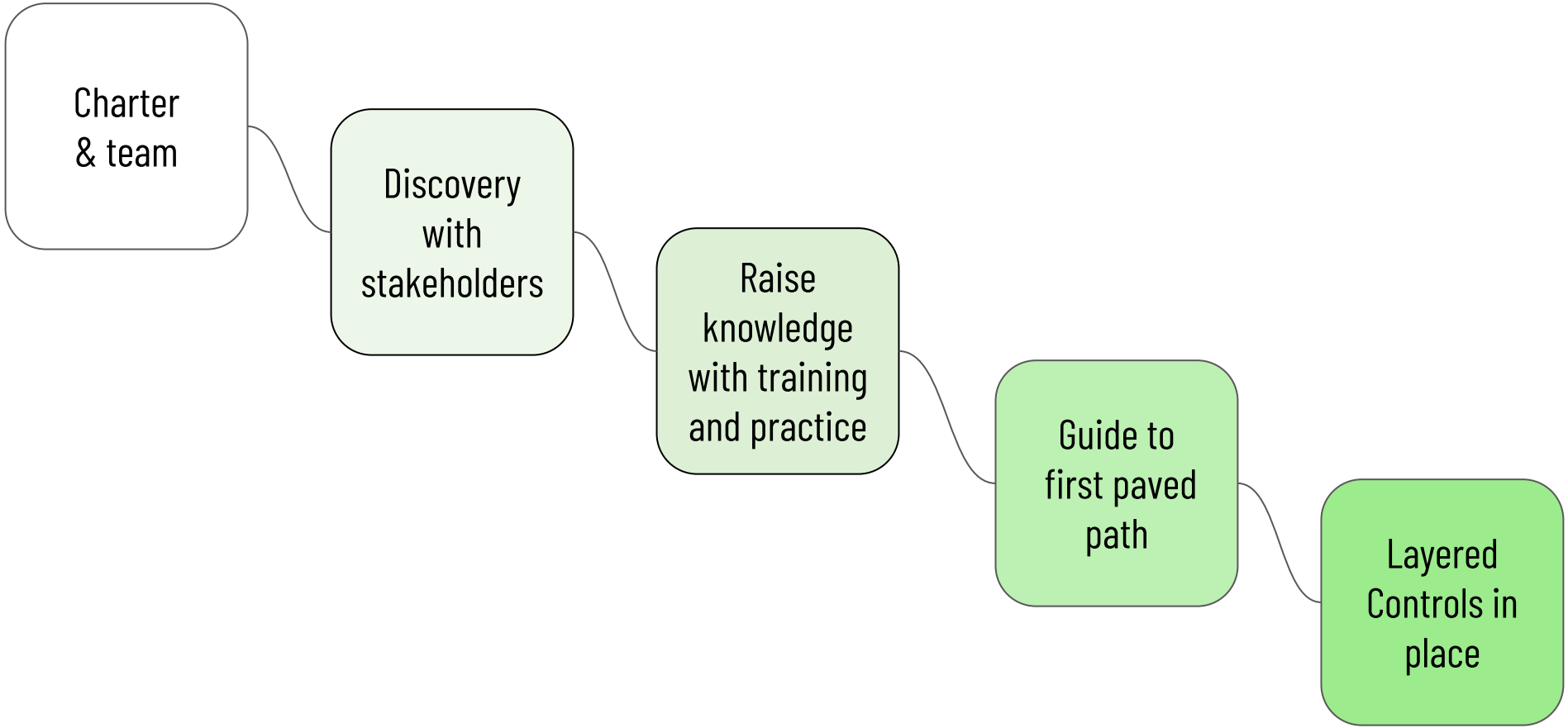


Photo by Kier in Sight Archives on Unsplash

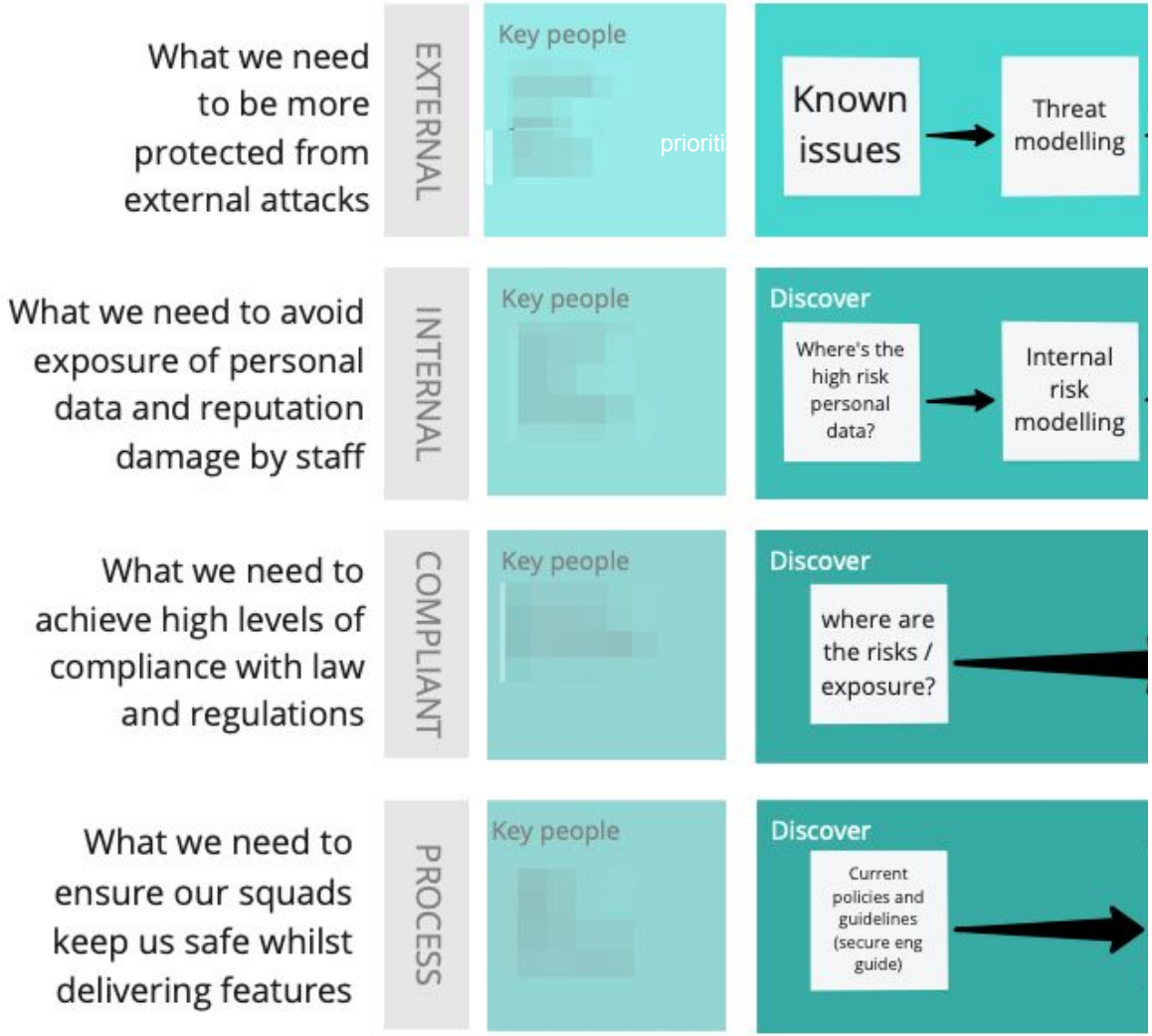
A linear abstraction



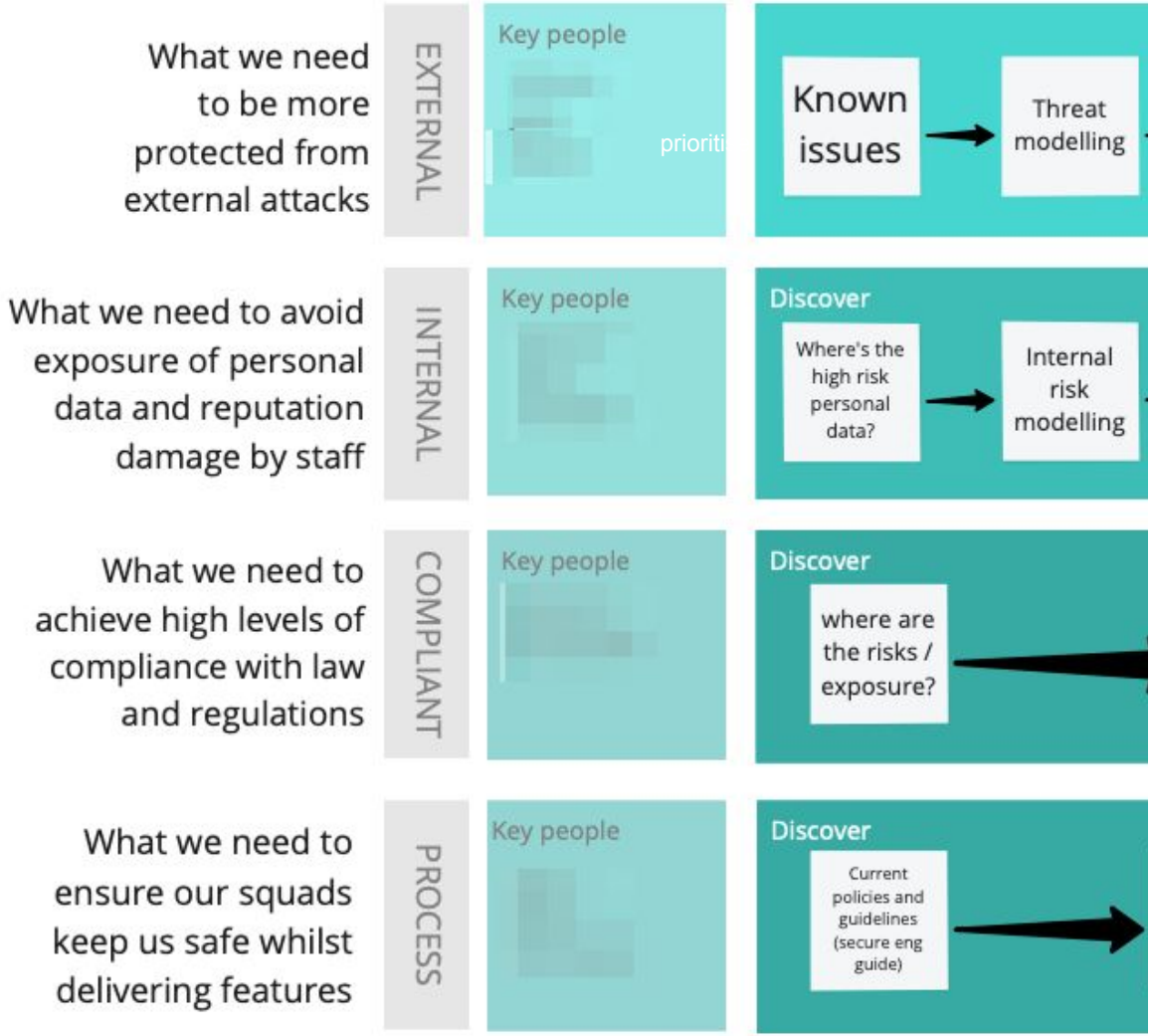
To avoid
getting lost

Identify
stakeholders
and the **stakes**

Many rivers to cross



Many rivers to cross



Begin to fix

security

gap

With the first

Paved path

and make

knowledge a

rising tide

Begin to fix

security

gap

With the first

Paved path

and make

knowledge a

rising tide

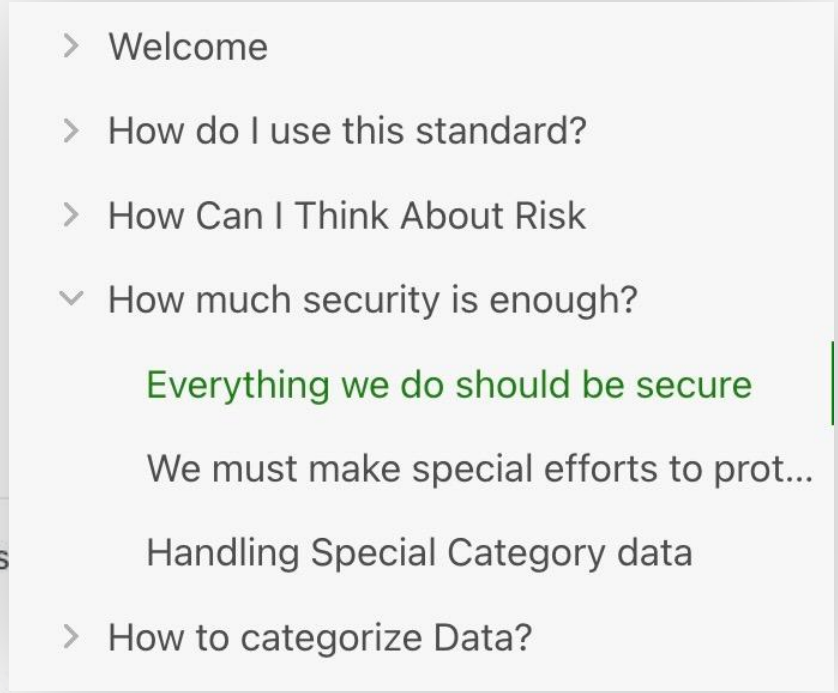
Meet **Stan**


tes
How do I use this standard?
Secure Engineering Standard
Secure by default and design
WITH GREAT POWER COMES GREAT RESPONSIBILITY — STAN LEE
Let's go!

Meet **Stan**


tes
How do I use this standard?
Secure Engineering Standard
Secure by default and design
WITH GREAT POWER COMES GREAT RESPONSIBILITY — STAN LEE
Let's go!

Meet **Stan**



'Secure by Default' Directives

Our working model at Tes is to operate as 'Secure by Default'. You s
software for Tes.

- Protect your data: find the right places for your data and code.
- Manage service credentials safely and do not share them
- Follow the principle of least privilege
- By default APIs should be internal. If public, consider if they should be secured by user or role access.
- Follow the engineer behaviour guidelines
- Avoid key known attack vectors (OWASP top 10) using Tes standard practices

Meet **Stan**

PRACTICES

- Avoid injection via JavaScript
- Implement Access Control
- Avoid CSRF Attacks
- Avoid XSS attacks
- Avoid broken authentication
- Avoid modules with known vulnerabilities
- Secure Code Review
- Avoid Credentials Leakage
- Intentional design & Threat Modelling

Trust, but **verify**

Done?

Original by Hello I'm Nik from Unsplash

Everything we do should be secure

To protect the business and all our users, all data should be held securely. It could be damaging if control of it is lost. Additionally, we hold a lot of Higher Risk personal and payment data and it's critical we protect this data.

If your service does not process high risk data then you must follow the 'Secure by Default' directives.

We must make special efforts to protect Higher Risk data

When a service is holding and processing Higher Risk data extra focus is needed to ensure we protect this data.

If your service processes Higher Risk data you should follow the Higher Risk data directives to ensure that this data is protected.

Handling Special Category data

Special Category Data is very sensitive data. We are not allowed to process this data unless it is held to a higher level of compliance.

Gearing through graded paved paths

Everything we do should be secure

To protect the business and all our users, all data should be held securely. It could be damaging if control of it is lost. Additionally, we hold a lot of Higher Risk personal and payment data and it's critical we protect this data.

If your service does not process high risk data then you must follow the 'Secure by Default' directives.

We must make special efforts to protect Higher Risk data

When a service is holding and processing Higher Risk data extra focus is needed to ensure we protect this data.

If your service processes Higher Risk data you should follow the Higher Risk data directives to ensure that this data is protected.

Handling Special Category data

Special Category Data is very sensitive data. We are not allowed to process this data unless it is held to a higher level of compliance.

Gearing through graded paved paths

Whilst avoiding **siloing**

Build **connection**

Guide, don't police.

Only **brake** as last resort

Challenge | Solution | What we did | **Impact** | Close

Scaled Impact

Operations: *"It changed a lot of mindsets, and moved from security being an afterthought"*

Risk: *"Brought the most valuable assets engineering has into security"*

Engineer: *"Everyone knows where to go and engineers are empowered to use secure by design in everyday work"*

Unplanned gains

Fixed: Authentication app occasionally placed user's password in cookie.

Fixed: Hacker games led to engineers patching holes next day.

Protected: Higher risk data moved to safer stores

Protected: Sensitive data encrypted in Message Queues.

Prevented: Standardising security mitigated Credential Stuffing attack.

Awareness: Board level queries and interest

Challenge | Solution | What we did | Impact | **Close**

(1) Security threats are only going to increase

(2) Engineering is optimised for a purpose

(3) There is so much to do and so little time

Photo by Jan Kopřiva on Unsplash

Photo by Nathan Bartlett on Unsplash

How to start

1. Charter a team to solve the problem
2. Connect them up to what's important
3. Set a standard that helps delivery
4. Focus on community not correctness

Takeaways

https://**engineeringandcareering.co.uk/ldx3**

EXTRAS