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?

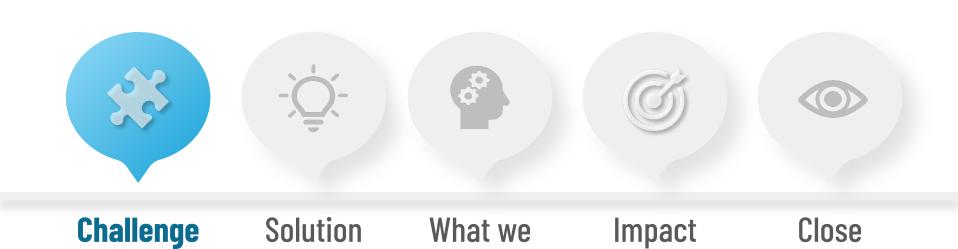3. Who worries that their engineering teams may not be ready to control these risks?

These are reasonable worries.

Challenge   Solution   What we did   Impact   Close

Tes: an 100 year old education company

Becoming Digital

THE TIMES
Educational Supplement

FRIDAY JUNE 27 1986   NUMBER 3652

FIRST PUBLISHED 1910   PRICE 60p

Cabinet urged to agree open-ended powers to fund maths and science push

Baker seeks central control over spending

by Biddy Passmore

Mr Kenneth Baker, the Education Secretary, is pressing his Cabinet colleagues for open-ended powers to control education spending direct from the DES.

He wants to insert an amendment into the Education Bill, now going through Parliament...

DES, had had it ready for some time. The plan is to be discussed within the next few...

All the fun of the festival
Education takes over the Edinburgh Fringe

magazine
Welcome to the chalkface 10-15
New teachers who choose a challenge

the TES

The Times Educational Supplement
Friday August 20, 2010
No 4901 Price £1.50

Elite grade increases university competition as overall pass rate rises for 28th consecutive year

Thousands of pupils exceed A* projection

By William Stewart

tes Essential weekly intelligence for the education prof

tes

Coding: outdated technique for our...

How thinking maps can help pupils navi the world of learning

What today's teacher can learn from da Vinc

The psychometric test helping colleges to improve student suppor

Is mindfulness clouding the issue of teac

10
teams

50
engineers

140
micro-services

Stream-aligned teams

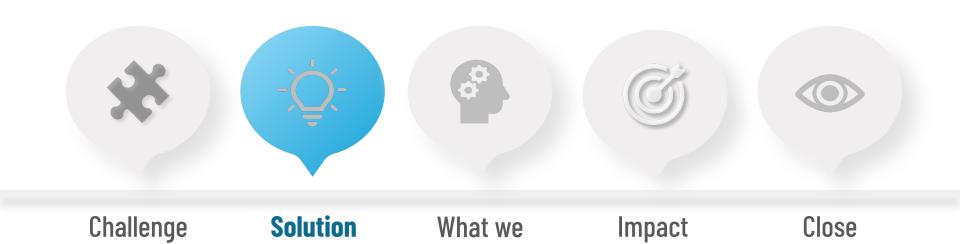Stream-aligned teams

Stream-aligned teams

Stream-aligned teams

Infrastructure Platform team

Concepts from Team Topologies
By Matthew Skelton & Manuel Pais

THE CHALLENGE

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

Risk to
reputation,
operation
and
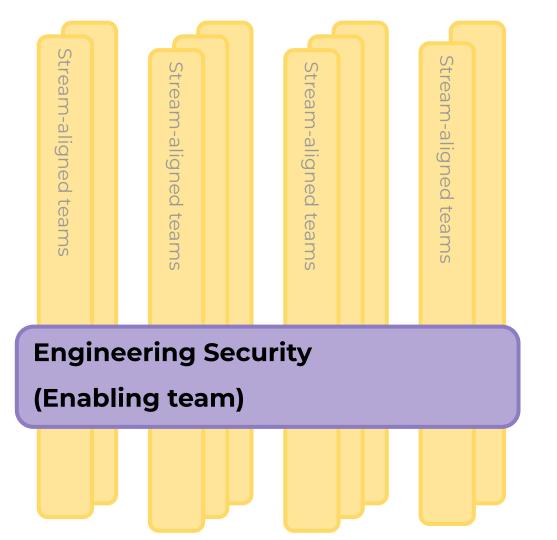**teacher data**

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,
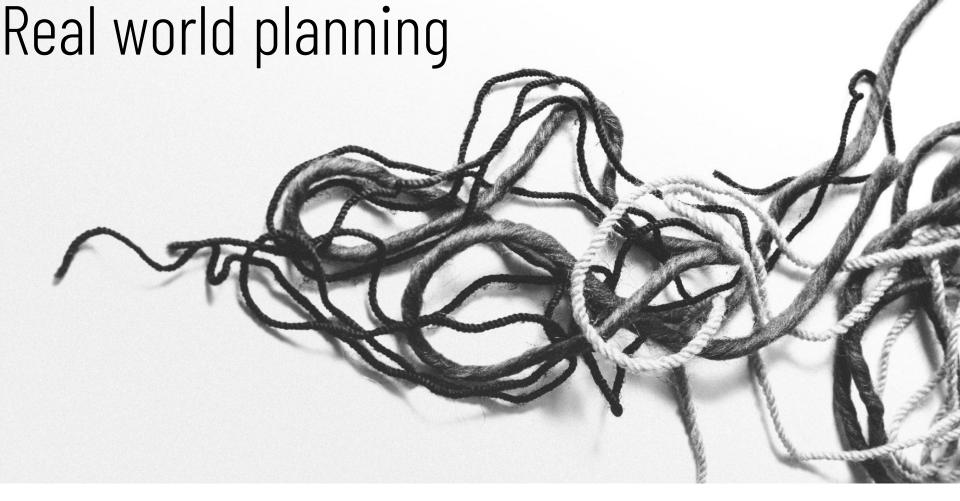a DevSecOps leader

(GOTO 2015 • The Road To Being Rugged)

Stream-aligned teams
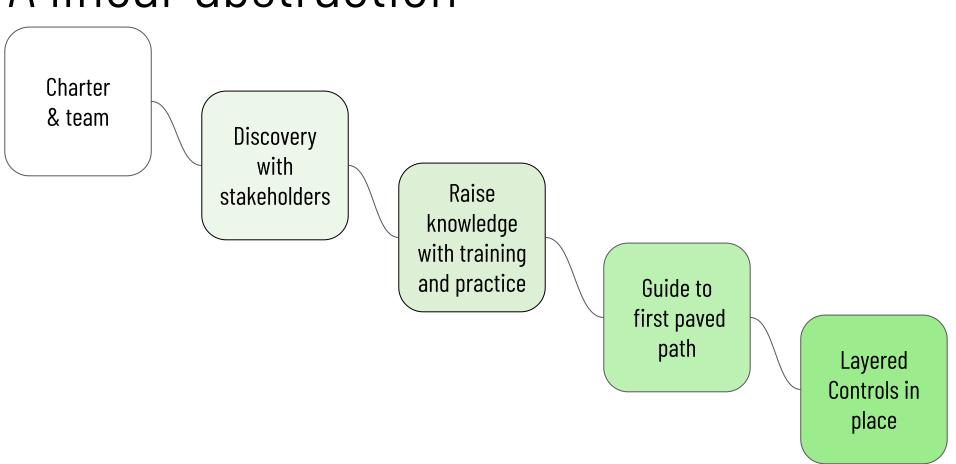
Stream-aligned teams
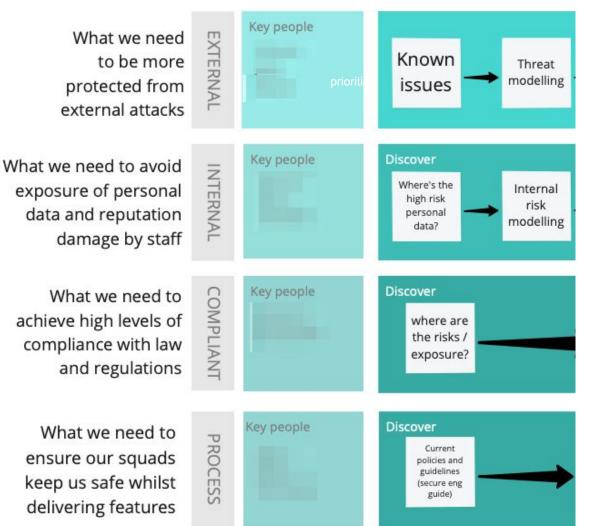
Stream-aligned teams

Stream-aligned teams

Engineering Security

(Enabling team)

SPOILERS!

It worked

Challenge

Solution

What we did

Impact

Close

The eng-sec team

Me
(lead)

+

Tom
(engineer)

&

George
(engineer)

And then...

Me
(lead)

+

Amélie
(engineer)

&

Charlotte
(engineer)

Real world planning

A linear abstraction

Charter & team → Discovery with stakeholders → Raise knowledge with training and practice → Guide to first paved path → Layered Controls in place

To avoid
getting lost

Identify
stakeholders
and the **stakes**

Many rivers to cross

		Key people	
What we need to be more protected from external attacks	EXTERNAL	prioriti	Known issues → Threat modelling
What we need to avoid exposure of personal data and reputation damage by staff	INTERNAL	Key people	**Discover** — Where's the high risk personal data? → Internal risk modelling
What we need to achieve high levels of compliance with law and regulations	COMPLIANT	Key people	**Discover** — where are the risks / exposure?
What we need to ensure our squads keep us safe whilst delivering features	PROCESS	Key people	**Discover** — Current policies and guidelines (secure eng guide)

Begin to fix **security** gap

With the first **Paved path**

🛥️🛥️🛥️ and make

knowledge a **rising** tide

⛵⛵⛵

Meet
Stan

tes

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?

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

ITERATE

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

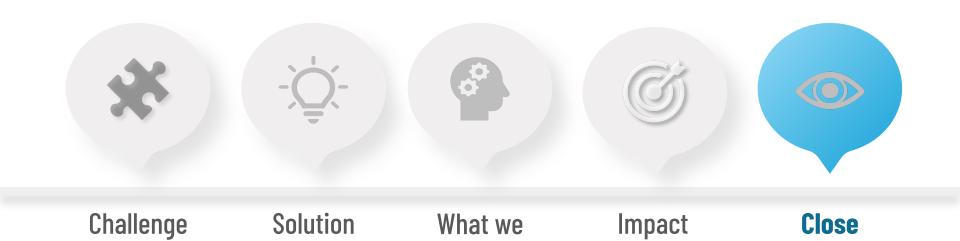**Fixed:** Authentication app occasionally placed user's password in cookie.

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

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**