



virgin atlantic 

 HOLIDAYS

Securing the DevOps Landscape



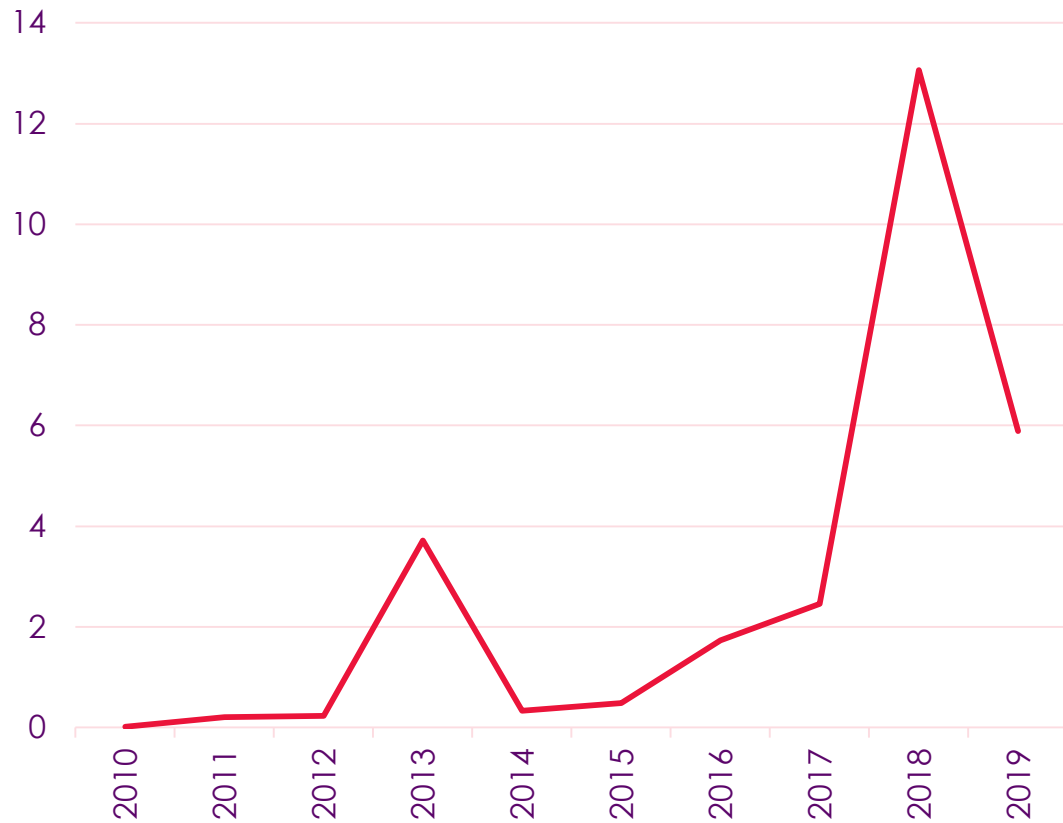
Martyn Coupland
DevOps Technical Lead, Virgin Atlantic

virgin atlantic 

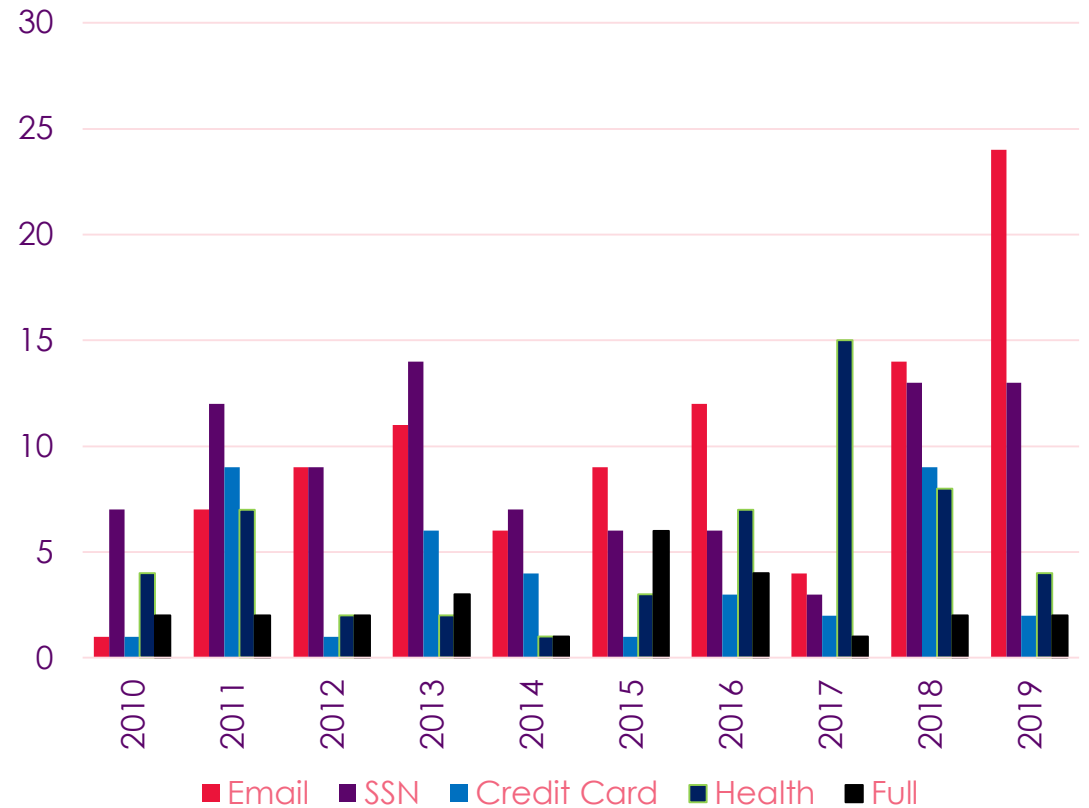
 HOLIDAYS

Reality of data breaches

Records Lost Per Year

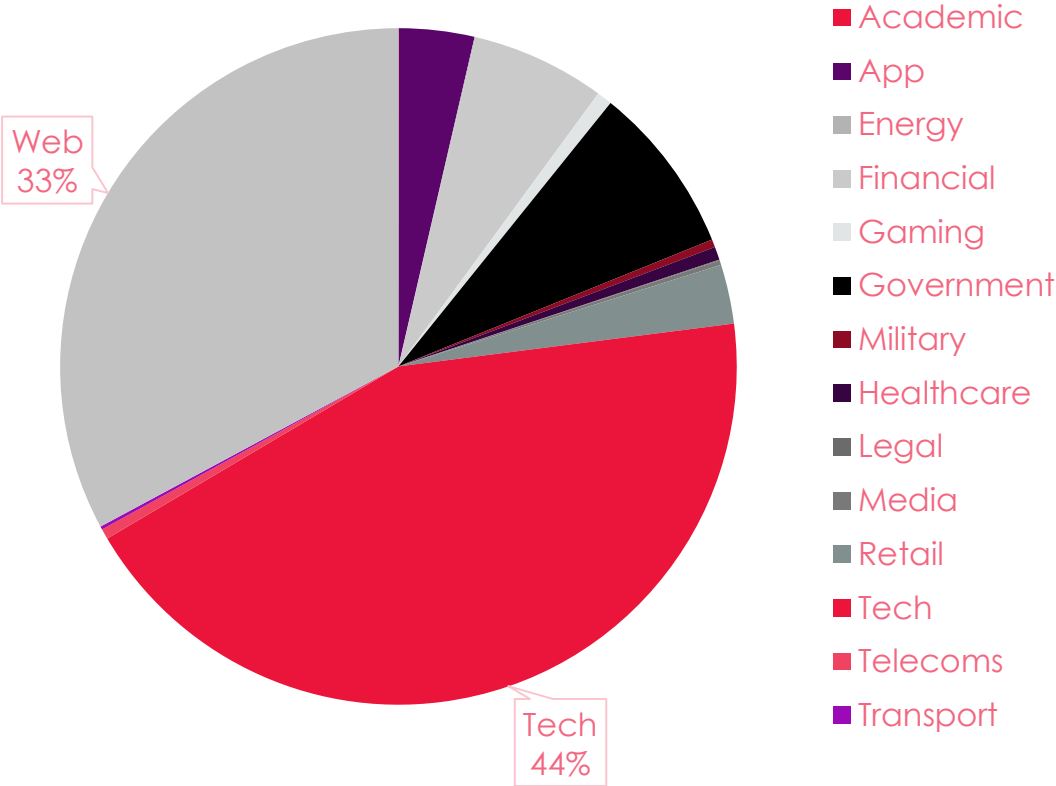


Breaches by Sensitivity

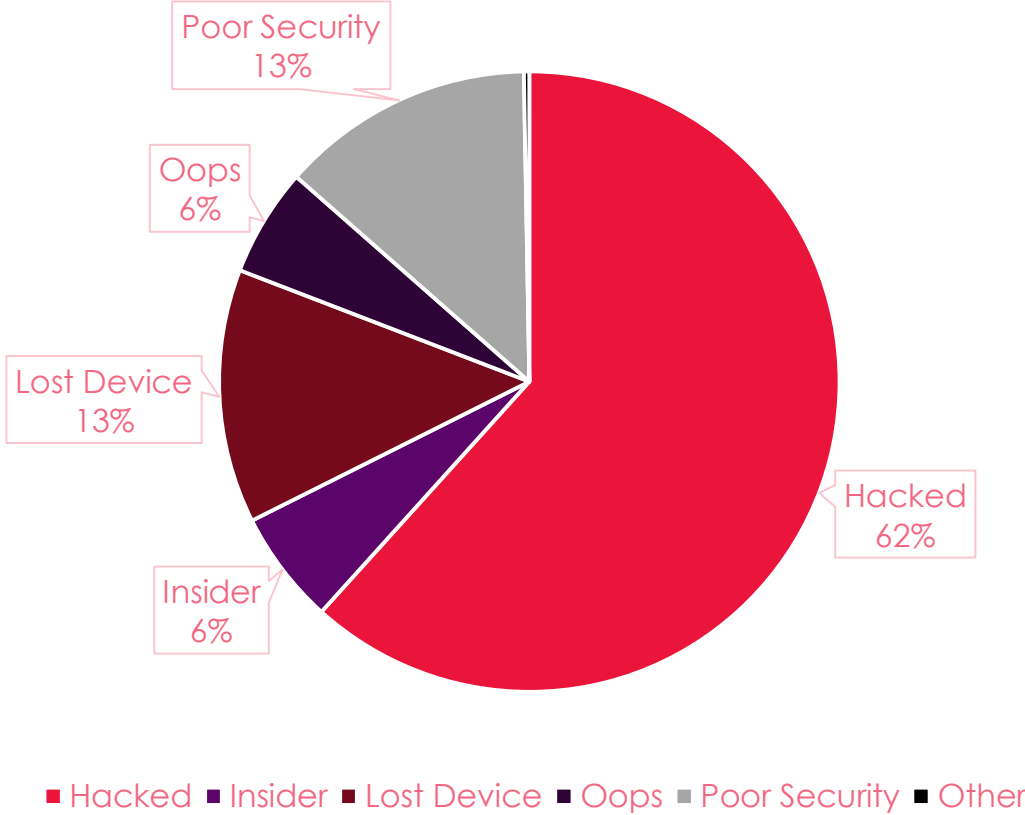


Reality of data breaches

Breaches Per Sector

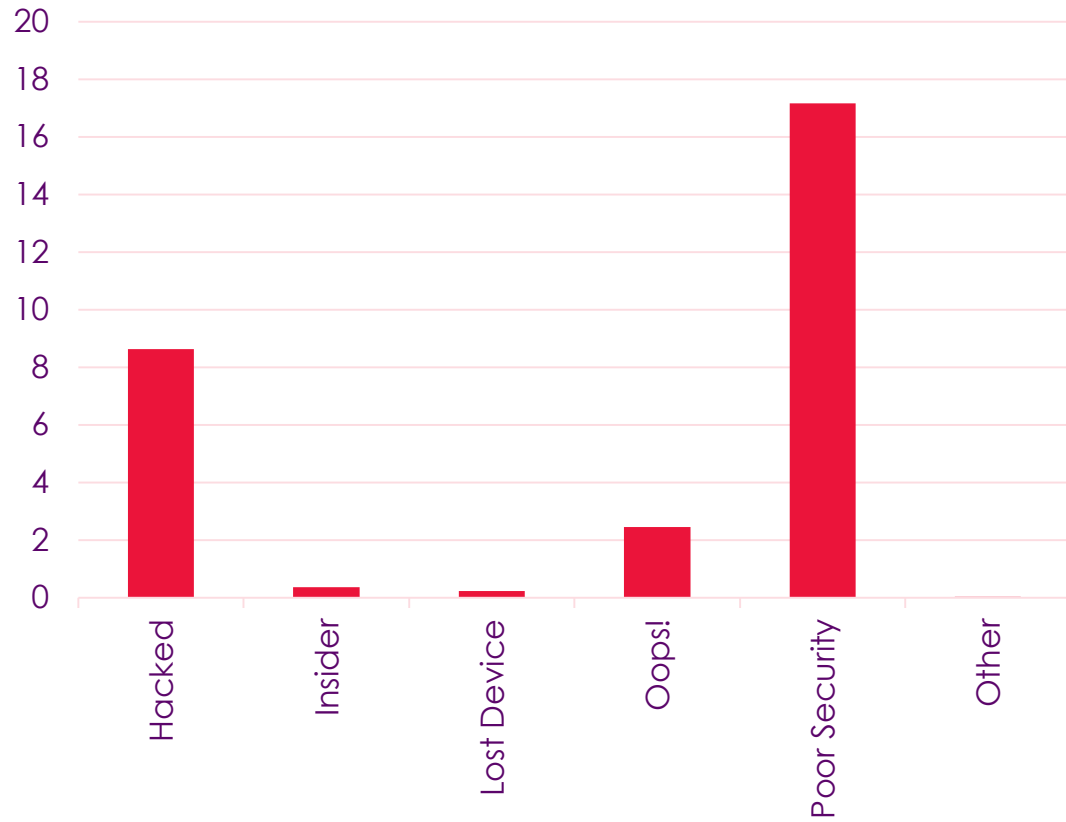


Breaches by Method



Reality of data breaches

Records Lost by Method



What have we learned

Summarising the data

- Number of breaches and records lost per year is generally going up
- **62%** of breaches are due to hacking
- **6%** is due to mistakes
- **6%** is due to insider jobs
- Although hacking accounts for nearly $\frac{2}{3}$ of breaches, half the number of records are stolen compared to poor security
- Lost devices account for **13%** of breaches but only around **1%** of record loss
- Tech firms are most at risk accounting for **44%** of breaches and web based breaches next with **33%**
- **70%** of passwords are in the breaches charted

Security comes first...

Don't be headline news

- Security comes in various forms, think about every angle
- With hacking so prevalent, secure all aspects of your platform, this includes your pipelines
- It should just be DevOps, not DevSecOps, think Security as a Service
- Shift security to the left

Security comes first...



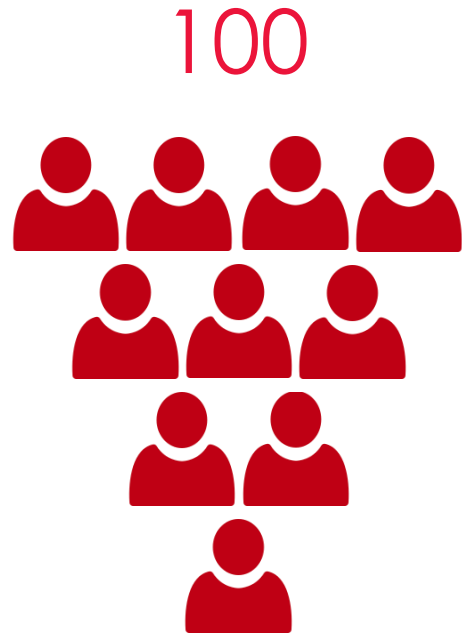
What hinders security innovation?

- Manual processes and culture
- Point in time assessments
- Traditional InfoSec “friction”
- Misunderstanding of context
- Political internal interference
- Fear of failure
- Lack of external thinking

Security is everyone's
responsibility...

The DevOps, Sec ratio

Numbers matter...



DevSecOps

Security
Engineering

Security
Operations

Compliance
Operations

Security
Science

Experiment,
Automate,
Test

Hunt, Detect,
Contain

Respond,
Manage, Train

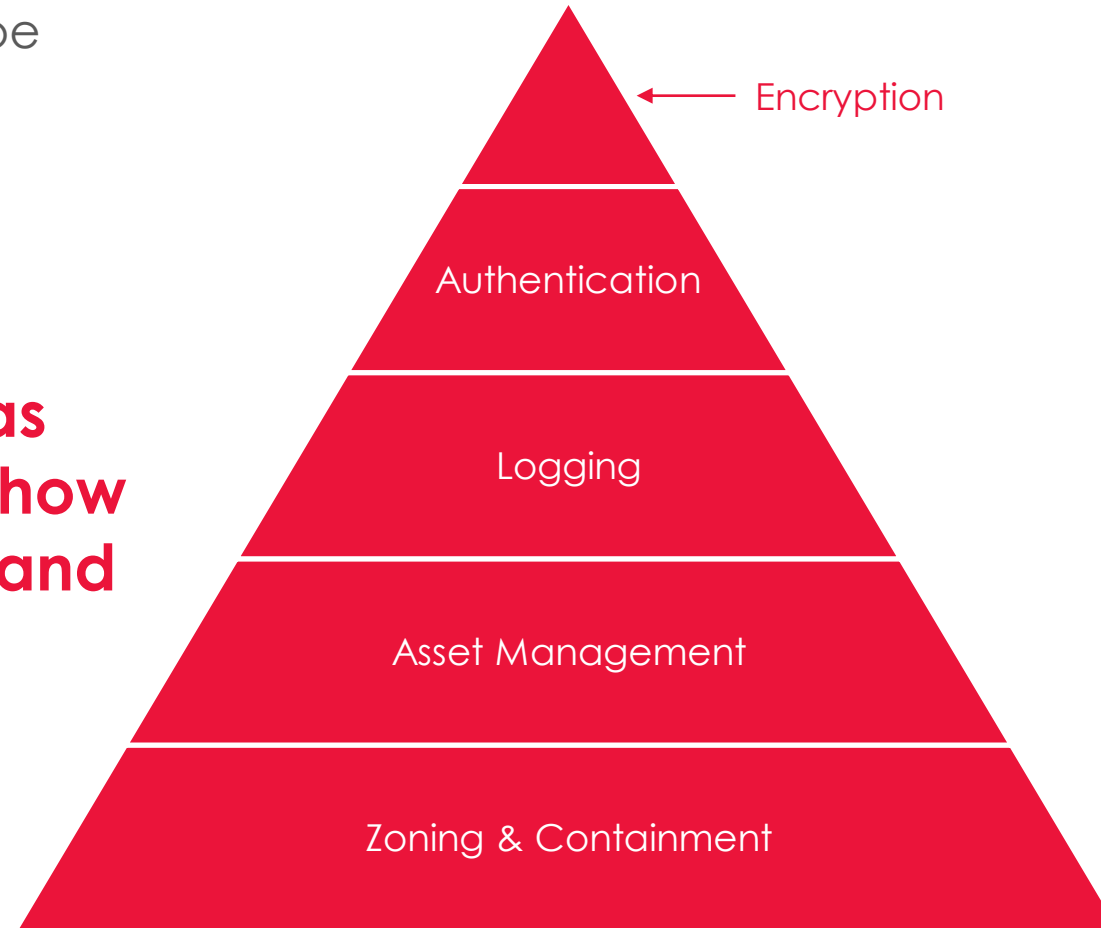
Learn,
Measure,
Forecast

Security is and always has been a design constraint

It must be built-in to be effective

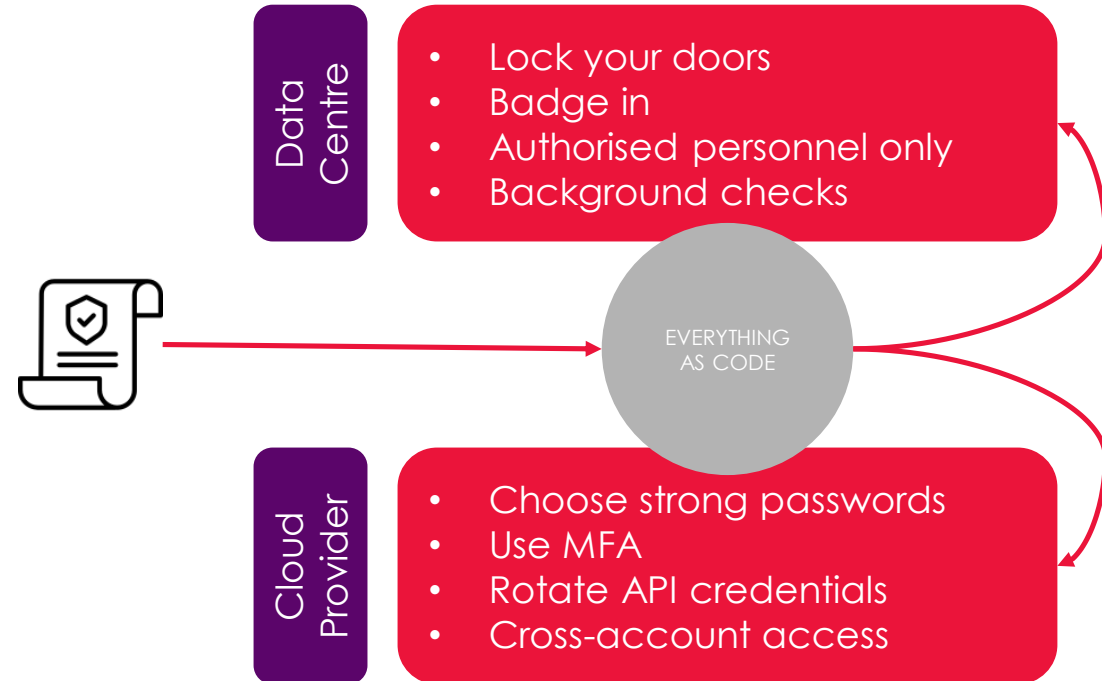
If you can remember five things, let it be these...

“Apps and data are as safe as where you put it, what’s in it, how you inspect it, who talks to it and how it’s protected”

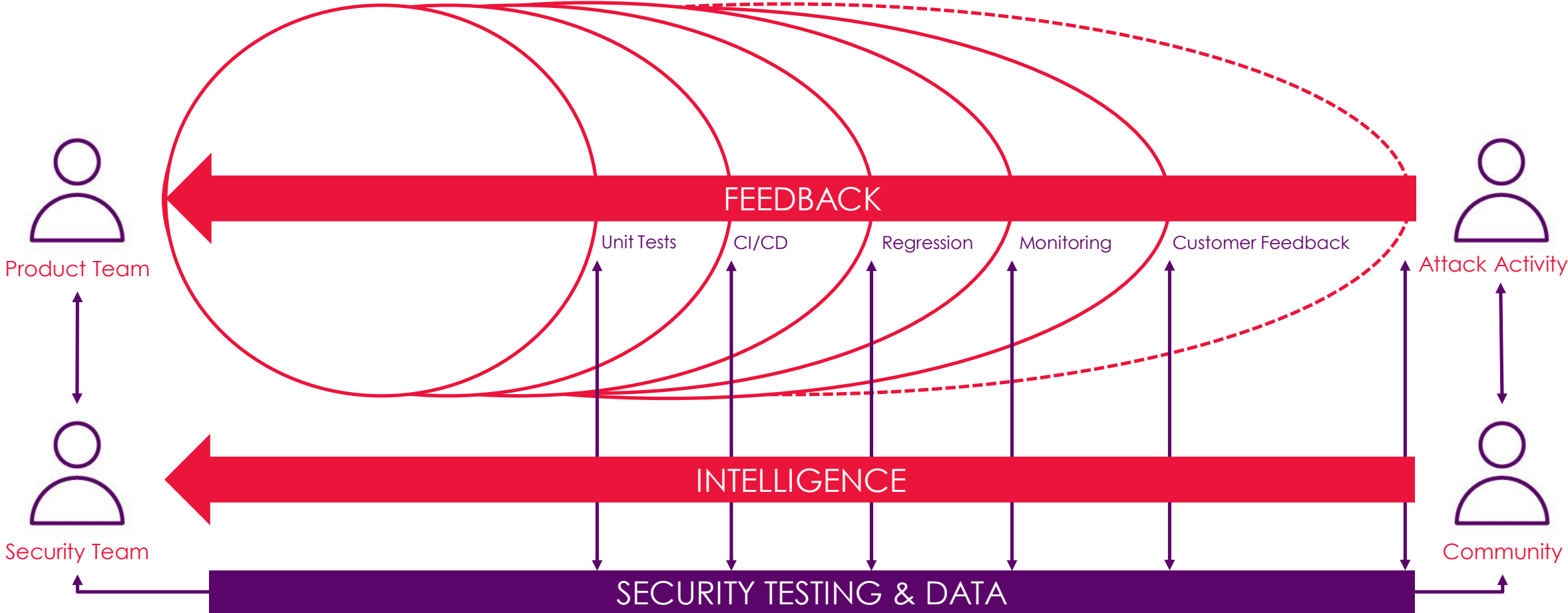


Security as code

- Paper policies do not stand up to constant cloud evolution and lessons learned
- Translation from paper to code and back lead to serious mistakes
- Traditional policies do not translate to full stack deployments



Continuous feedback



Fact check

Great information, but does it work?

- Teams focusing on testing, detection and measuring progress have **30% fewer** defects in production
- MTTR is **5x faster** than other teams
- Average of **98% CI/CD** success

Five foundations

- **Don't measure at a team level, measure globally**
Security's goal is to help the business achieve goals, avoid siloed thinking
- **Measure outcomes vs outputs**
Measuring work is not tied to tangible outcomes
- **“Maturity Threshold”**
Forget it, prioritise resilience over a notion of maturity
- **Don't miss the forest for the trees**
Focusing on components too much can mean missing the bigger picture
- **Don't try to measure failure**
Failure is inevitable, incentivizing failure avoidance is unrealistic at best



virgin atlantic 

 HOLIDAYS