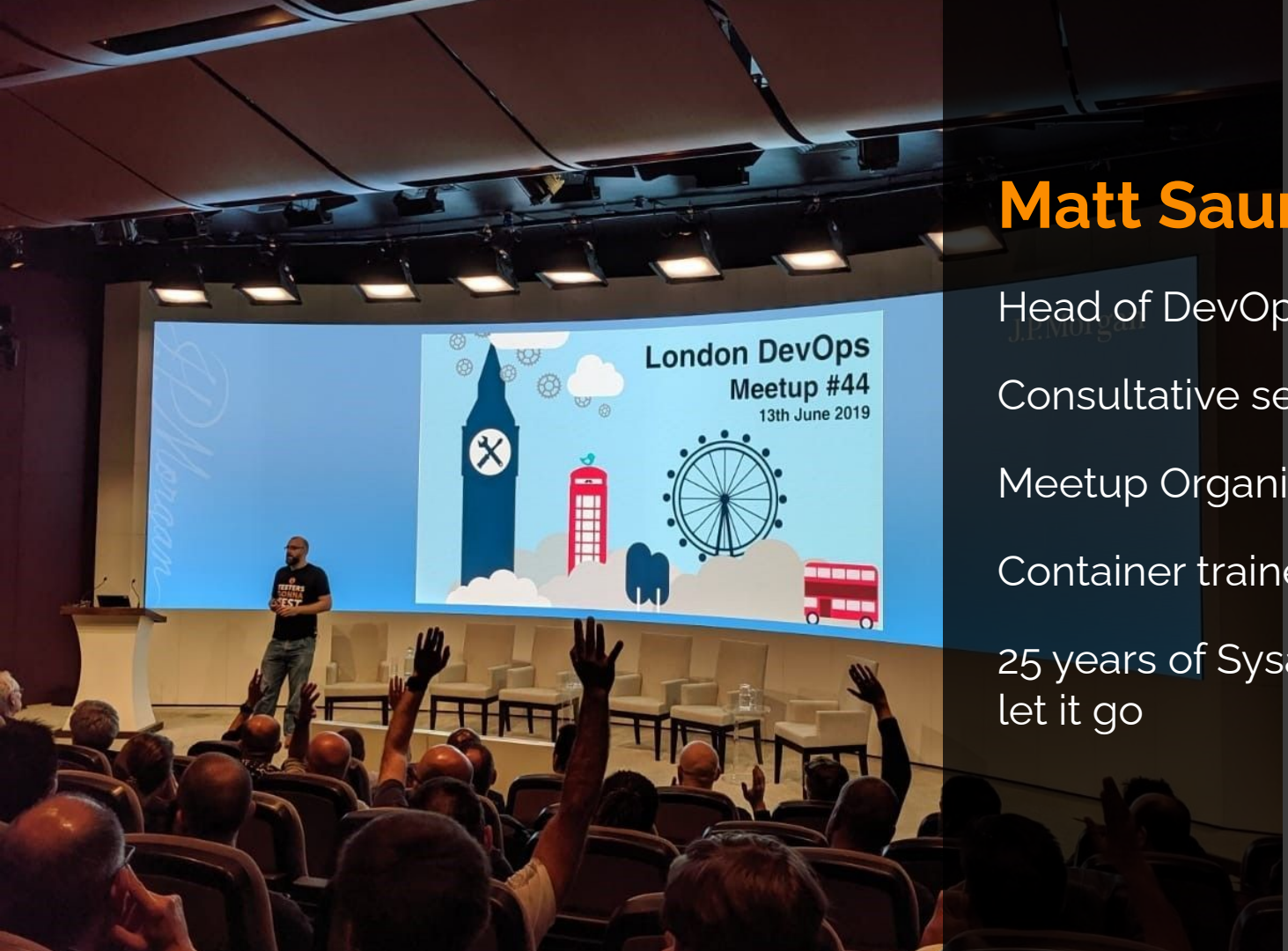
DevSecOps and the Fight against Friction

Matt Saunders



Matt Saunders

Head of DevOps & DevEx

Consultative servant leader

Meetup Organiser

Container trainer since 2014

25 years of Sysadmin, can't let it go

Adaptavist

Platinum Solution Partner ENTERPRISE

slack OFFICIAL PARTNER

Platinum Top Vendor

Agenda

Intro to Dev(Sec)Ops
Just Add Security
Repelling Friction
Takeaways

Intro to Dev(Sec)Ops

Just Add Security

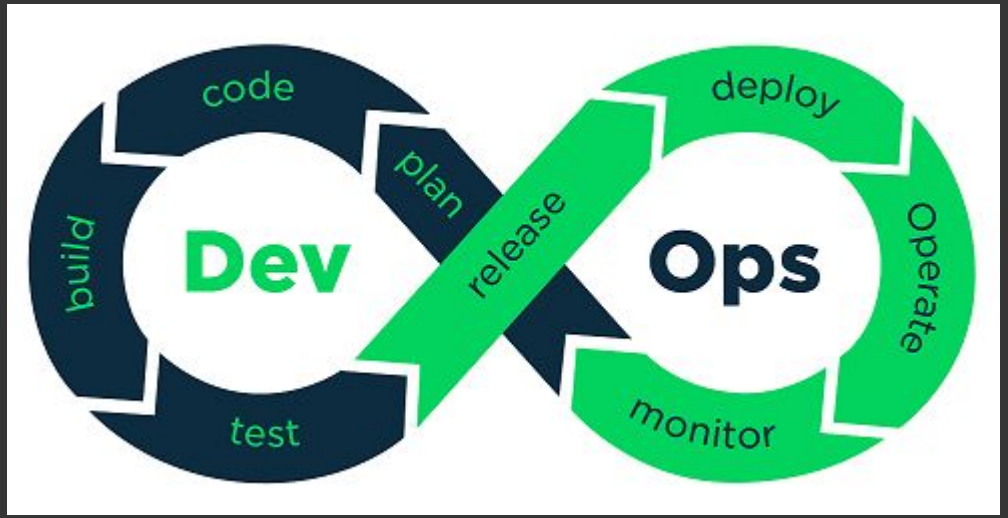
Repelling Friction

Takeaways

WARNING

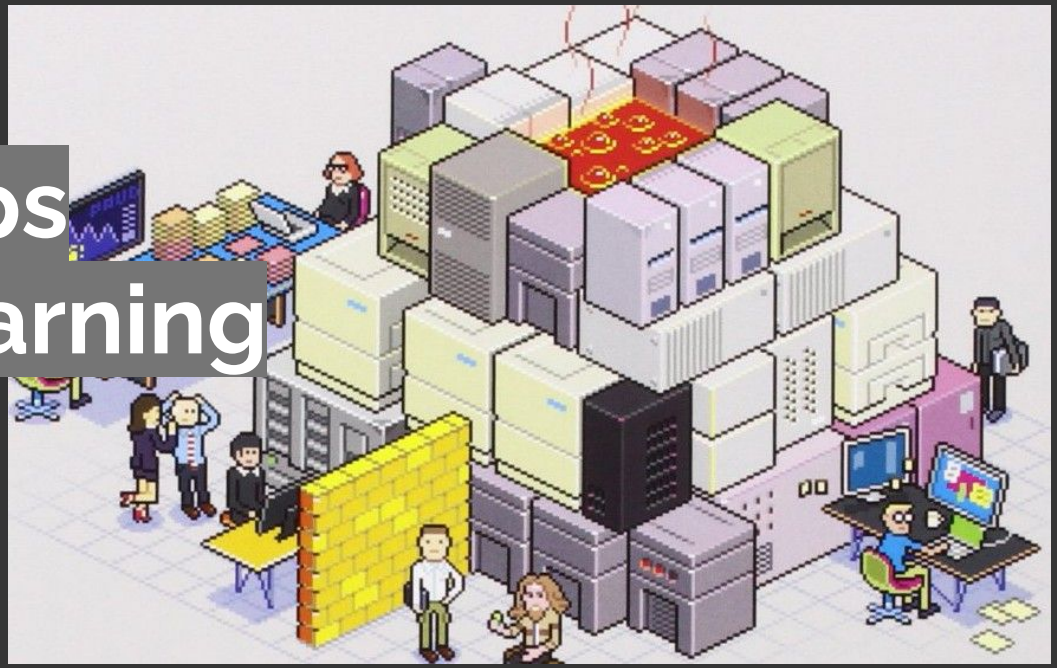
Next slide contains gratuitous DevOps infinity loop symbolism

What is DevOps?
What is DevSecOps?



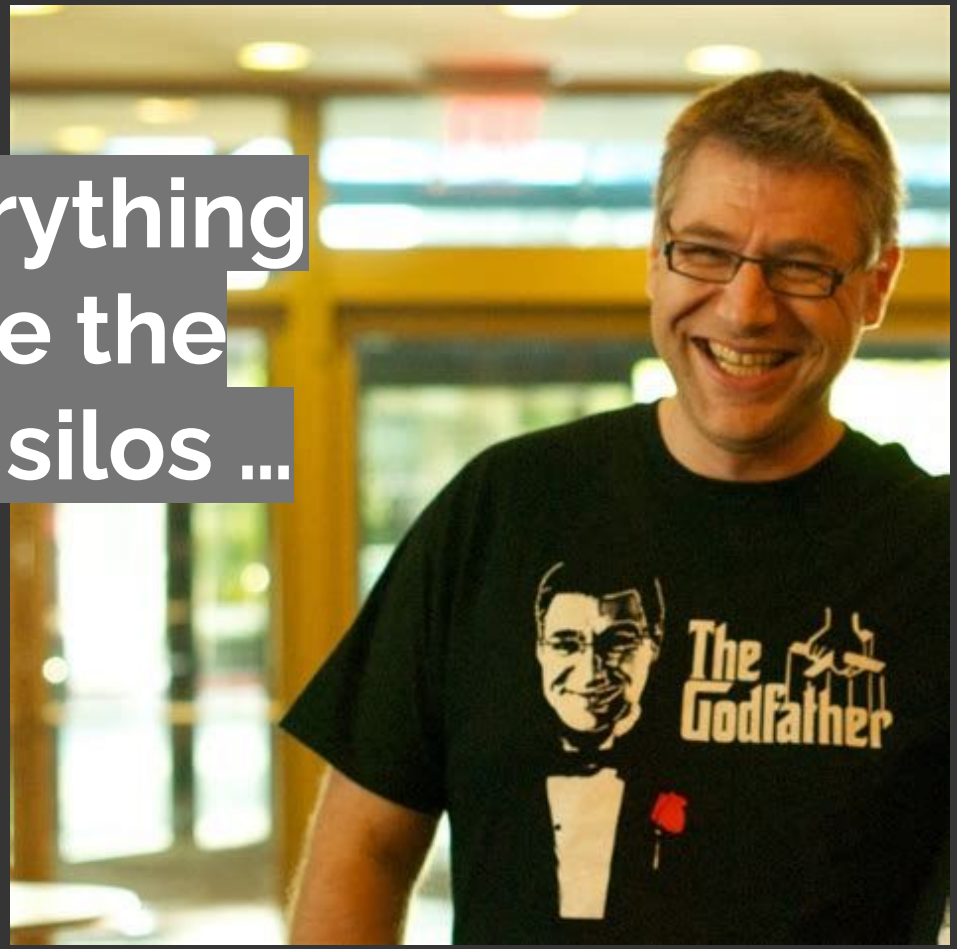
The Keys to DevOps

Flow
Feedback Loops
Continuous Learning



“Dev(Sec)Ops: everything you do to overcome the friction created by silos … All the rest is plain engineering”

- Patrick Debois



Deployment Frequency
Change Lead Time
Change Failure Rate
Mean Time to Recovery


Flow

Source Code Management (SCM)

- Where can other devs find my code?
- Who last worked on this code?
- Who might be able to help me write the next bit?
- Removes Friction

Continuous Integration (CI)

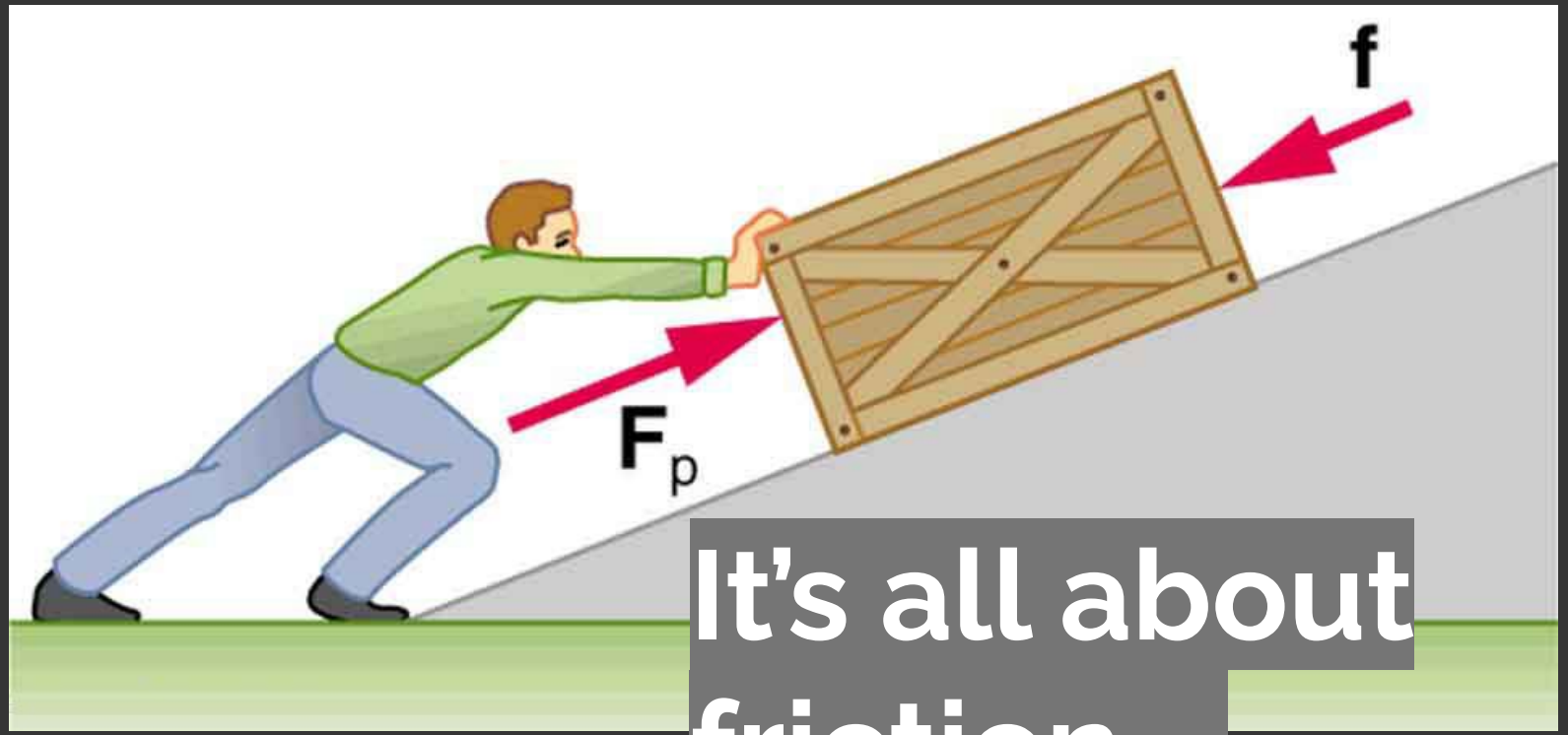
- Did those changes work OK?
- Who broke the build?
- Removes friction

Testing (QA)

- Are the tests visible?
- Do we have assurance that things are working?
- Can we audit from declarative tests?
- Removes friction

Configuration as Code

- A full declarative description of your infrastructure
- You can get started quickly as all the code is there
- Removes friction



It's all about friction ...

Image: Download for free at http://cnx.org/contents/031da8d3-b525-429c-80cf-6c8ed997733a@11.1.

Automation is Power

- To automate one must be declarative
- Make code visible
- Make tests visible
- Make compliance visible

Intro to Dev(Sec)Ops

Just Add Security

Repelling Friction

Takeaways

Add...

SAST / DAST

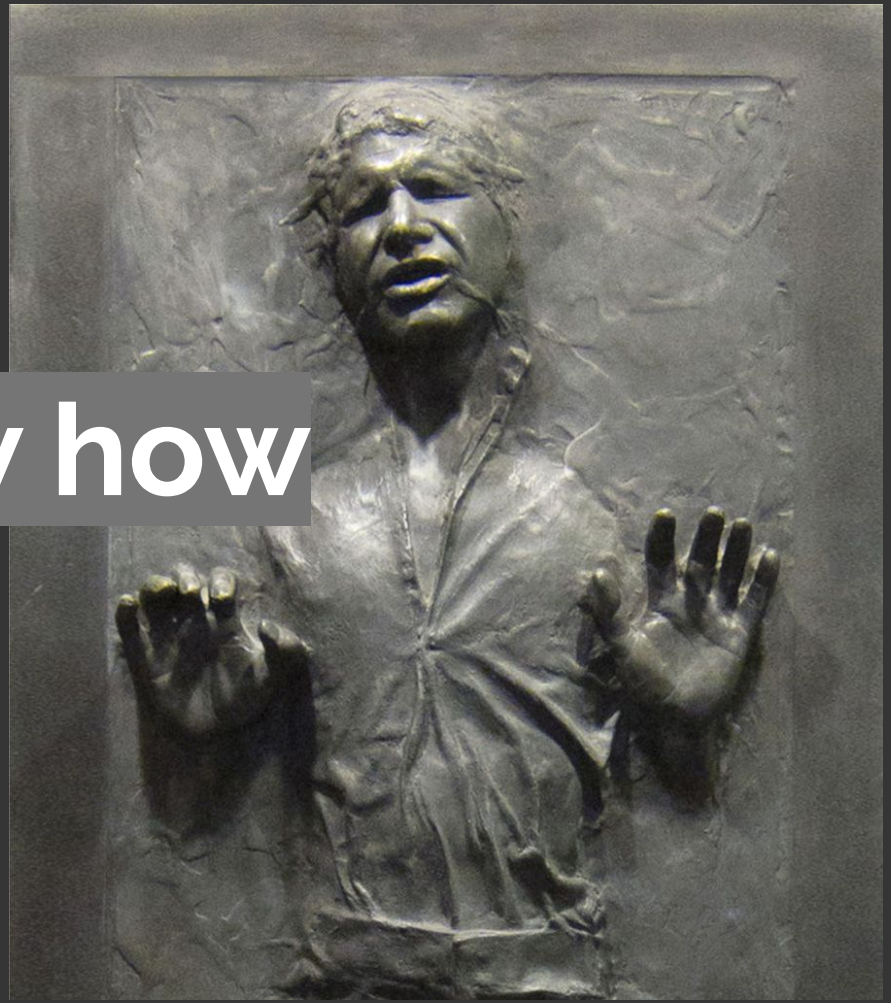
Image Scanning

OWASP tests

Expert Security Coding

Bear with me...

I think we know how this will end...



Five Ideals

Locality and Simplicity

Need security? Lose locality

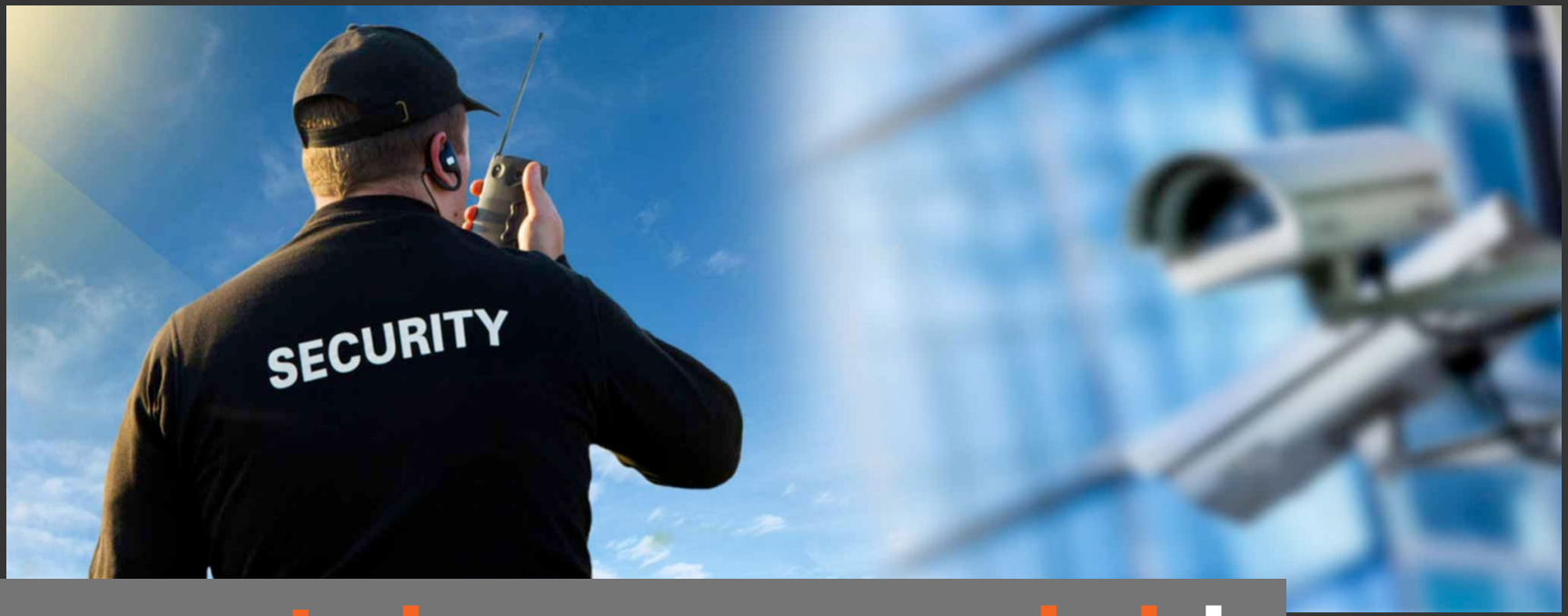
Focus, Flow and Joy

Way too easy to lose this

Psychological Safety

What if security say ‘no’?

How can you innovate when instead you have to plan?



The gatekeeper model is not compatible with flow

Let’s look at what we want to add...

Security

- Vulnerability Scanning
- Compliance Testing
- Threat Modelling
- Secure Coding

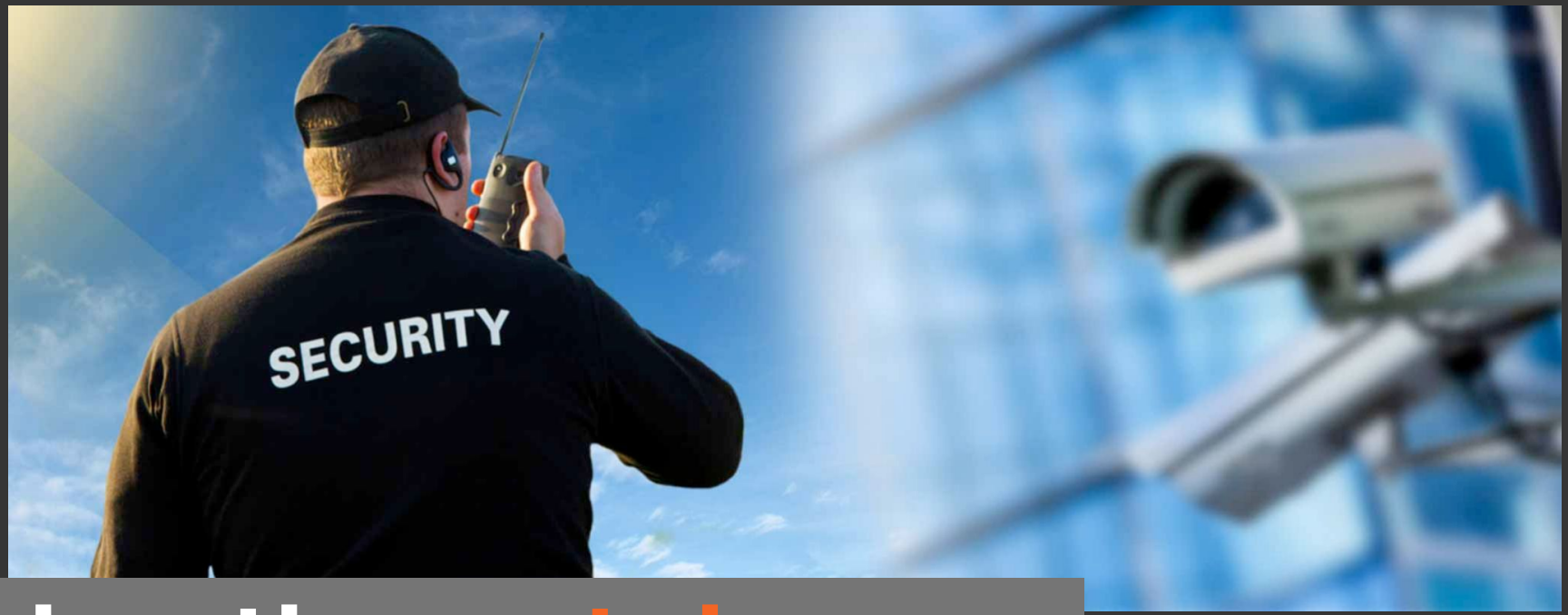
How can we add all this security and still deliver code?

Intro to Dev(Sec)Ops

Just Add Security

Repelling Friction

Takeaways



Bring the gatekeeper into the team

I mean really into the team

Incentivise security people in terms of flow, not metrics

Align the incentives with the devs

Don’t aim too high

Look closely at the Developer Experience

Put the appropriate testing in the hands of the devs

DevSecGitOps

- GitOps principles make security visible
- Compliance in code

Change SAST/DAST

Static/Dynamic Application Testing

Put SAST into CI

This is the easier bit

Put DAST into CI

This is harder

SAST

Test as you go

DAST

Needs a finished system

SAST

Dev-centric

DAST

Hacker-centric

Devs need a hacker mentality

Security need a dev mentality

Devs need a hacker mentality
Security need a dev mentality

Work on DAST tools together

Consultative approach from security

Document

What will be scanned?

When?

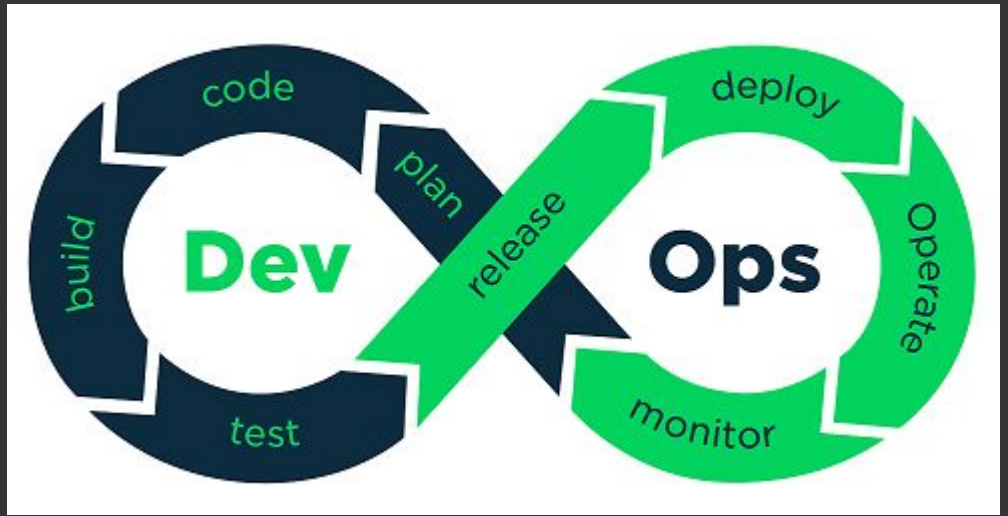
How?

Decide together!

Give the tools to dev

Give the code to sec

Above all - iterate and learn



Intro to Dev(Sec)Ops

Just Add Security

Repelling Friction

Takeaways

Takeaways

Gartner

12 Things to Get Right for Successful DevSecOps

FOUNDATIONAL Refreshed 9 April 2021, Published 19 December 2019 - ID G00450792 - 29 min read

By Neil MacDonald, Dale Gardner

Integrating security into DevOps to deliver DevSecOps demands changed mindsets, processes and technologies. Security and risk management leaders must adhere to the collaborative, agile nature of DevOps for security testing to be seamless in development, making the “Sec” in DevSecOps transparent.

Overview

Gatekeepers


Flow


Collaboration

Adaptavist

Platinum Solution Partner ENTERPRISE

slack OFFICIAL PARTNER

Platinum Top Vendor

Thank You!

Matt Saunders
matts@yoyo.org
twitter.com/cm6051
linkedin.com/in/msaunders