

Securing DevOps: Where to start and what to measure



Stefania Chaplin @devstefops

Solutions Architect @ Gitlab

Credit to Image Creators



@devstefops



@devstefops



@devstefops



stefania-chaplin

Agenda

- #whoami
- What?
- Who?
- How?
- Why?
- Summary
- Q&A in slack



@devstefops



@devstefops



@devstefops



stefania-chaplin

#whoami 🦄



Python, Java
Rest APIs



DevSecOps
AppSec, CloudSec



GitLab

The DevOps
Platform



@devstefops



@devstefops



@devstefops



stefania-chaplin

What?



@devstefops



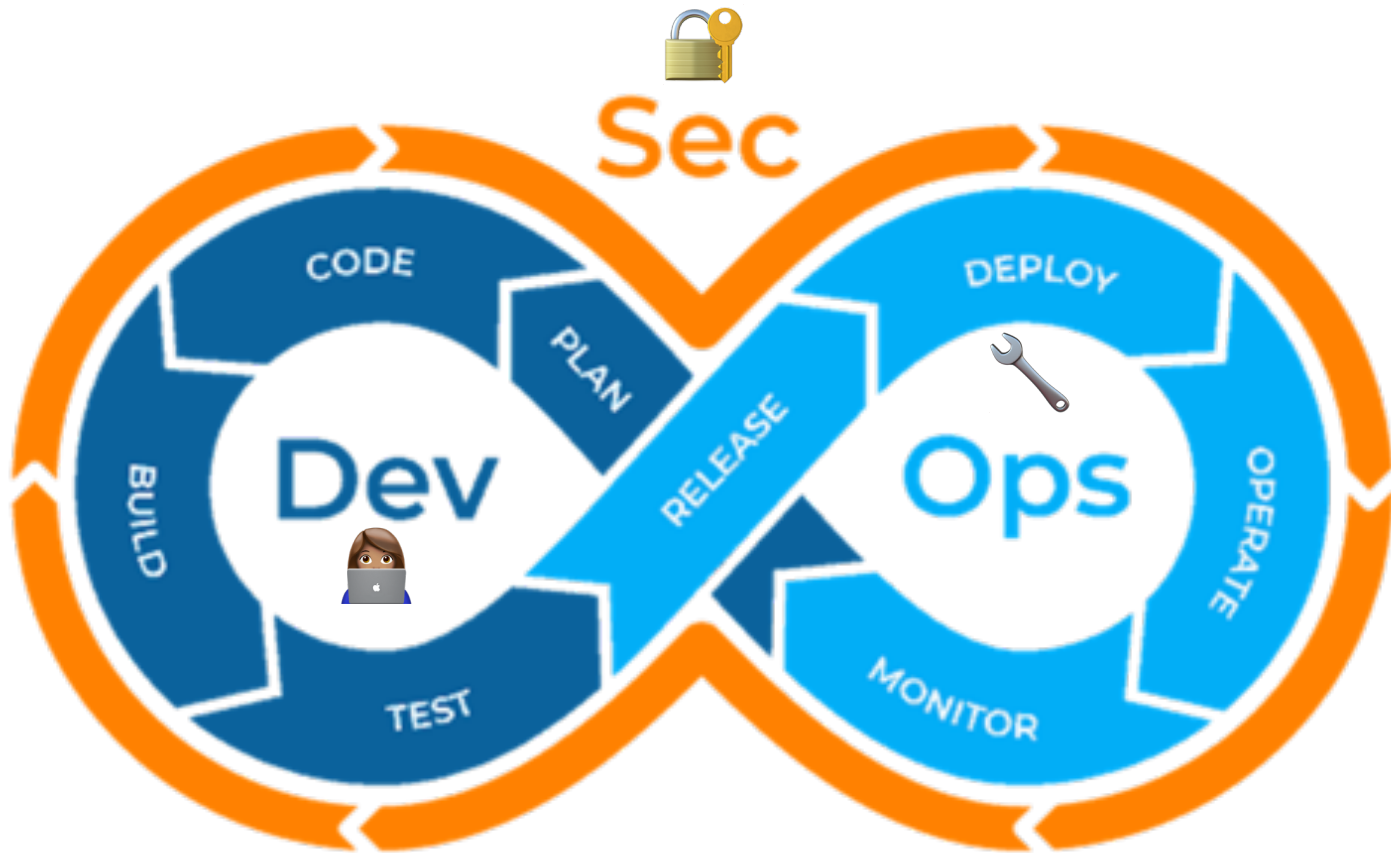
@devstefops



@devstefops



stefania-chaplin



@devstefops



@devstefops

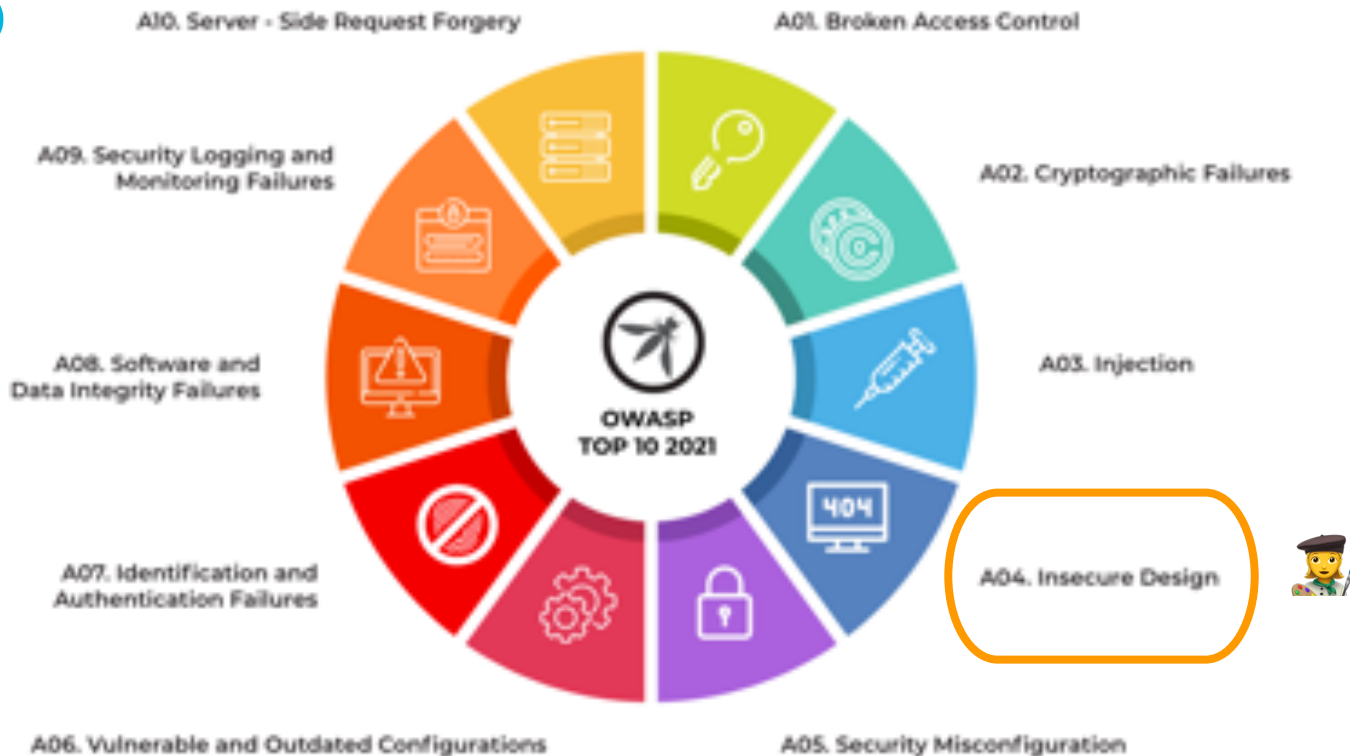


@devstefops



stefania-chaplin

Web



@devstefops



@devstefops






@devstefops



stefania-chaplin

Common Pain Points

- Security is the bad guy 
- Vulnerabilities (known + unknown) make it to production 
- Delays, fails, or.... 'worse' 



@devstefops



@devstefops



@devstefops



stefania-chaplin

Who?



@devstefops



@devstefops



@devstefops



stefania-chaplin



What is Culture?



Pathological <i>Power-oriented</i>	Bureaucratic <i>Rule-oriented</i>	Generative <i>Performance-oriented</i>
Low cooperation	Modest cooperation	High cooperation
Messengers shot	Messengers neglected	Messengers trained
Responsibilities shirked	Narrow responsibilities	Risks are shared
Bridging discouraged	Bridging tolerated	Bridging encouraged
Failure leads to scapegoating	Failure leads to justice	Failure leads to inquiry
Novelty crushed	Novelty leads to problems	Novelty implemented

Warstrum 2004



@devstefops



@devstefops



@devstefops



stefania-chaplin



@devstefops



@devstefops



@devstefops



stefania-chaplin

How?



@devstefops



@devstefops



@devstefops



stefania-chaplin

Make Security Fun & Easy 😊



@devstefops



@devstefops

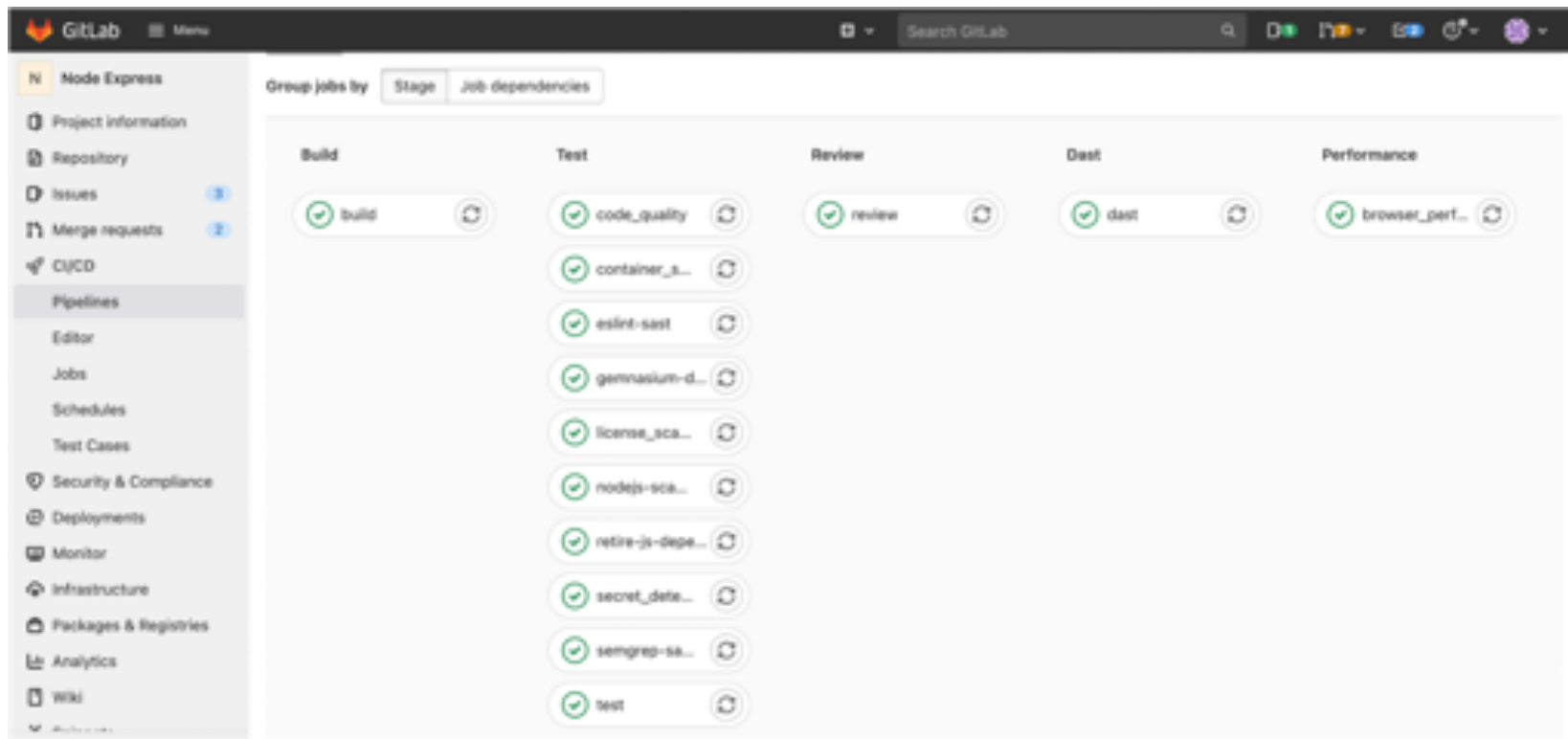


@devstefops



stefania-chaplin

Shift Security Left



@devstefops



@devstefops

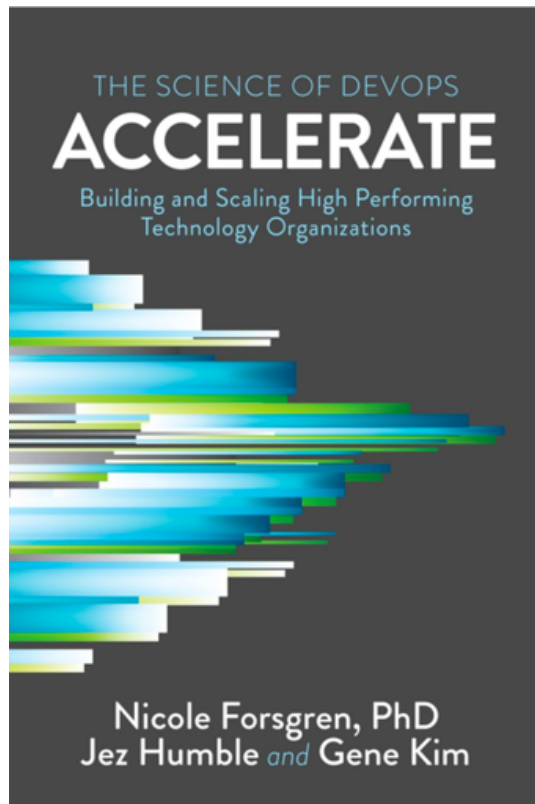


@devstefops



stefania-chaplin

DORA Metrics



1

LEAD TIME

Lead time is the time it takes to go from a customer making a request to the request being satisfied. Shorter lead times enable faster feedback.



DEPLOYMENT FREQUENCY

Deployment frequency is a proxy metric for batch size; the more frequently you deploy the smaller the size of the batch. Small batch sizes reduce cycle times, reduce risk and overhead, improve efficiency, increase motivation and urgency, and reduce costs and schedule growth.

2

3

MEAN TIME TO RESTORE

Reliability is traditionally measured as time between failures, but in a modern software organization failure is inevitable. Thus, reliability is measured by how long it takes to restore service when a failure occurs.



CHANGE FAIL PERCENTAGE

This metric looks at the percentage of changes made to production that fail; the same as percent complete and accurate in Lean product delivery.

4



@devstefops



@devstefops



@devstefops



stefania-chaplin

Elite Performers



208

TIMES MORE
frequent code
deployments



106

TIMES FASTER
lead time from
commit to deploy



2,604

TIMES FASTER
time to recover
from incidents



7

TIMES LOWER
change failure rate



Throughput



Stability

Source: State of DevOps 2019

'Elite performers spend 50% less time remediating security issues than low performers'



@devstefops



@devstefops






@devstefops



stefania-chaplin

Why?

- If we secure our DevOps pipeline we can improve operational efficiencies, deliver better software faster with reduced security and compliance risk 
- We can innovate and iterate, listening to our customer and outperforming our competitors! 
- This will drive true business value 



@devstefops



@devstefops



@devstefops



stefania-chaplin

Summary

- Take a #securityfirst approach 
- Break down silos, we are all on the same team! 
- Make it fun, automate & measure results
#empowerdevelopers 



@devstefops



@devstefops



@devstefops



stefania-chaplin

Thank you!

stefania@devstefops.com



GitLab

The DevOps
Platform

schaplin@gitlab.com



@devstefops



@devstefops



@devstefops



stefania-chaplin