DevOps and DevSecOps: Fundamentals

BCS DevSecOps Specialist Group

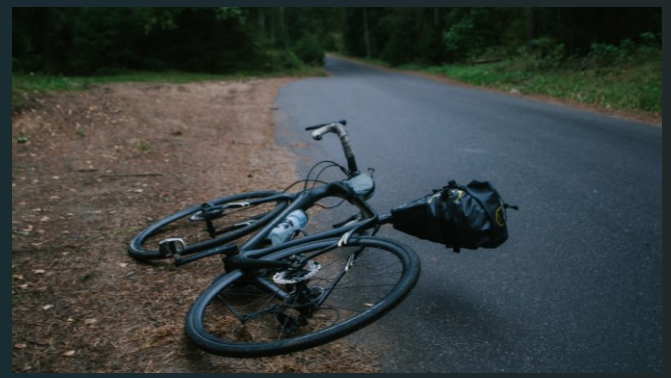
29th November 2023

Speaking today

Nick Barham

DevSecOps Advisor

VERACODE



DevOps: A primer

Before DevOps

Segregation of IT functions

Application Development	Enterprise Architecture	Quality Assurance
Technical operations	UAT	Quality Assurance
IT Management	Project Management	Information Security

Emphasis on project structure

Less than desirable consequences

- ‘Idea to production’ takes a long time
- Ticket-based collaboration
- Only some parts stood up with automation
- “Big bang” releases
- Limited experimentation
- Poor uptime and long time-to-recovery
- Confusion/panic when things go wrong

Is there a better way?

Foundations for DevOps

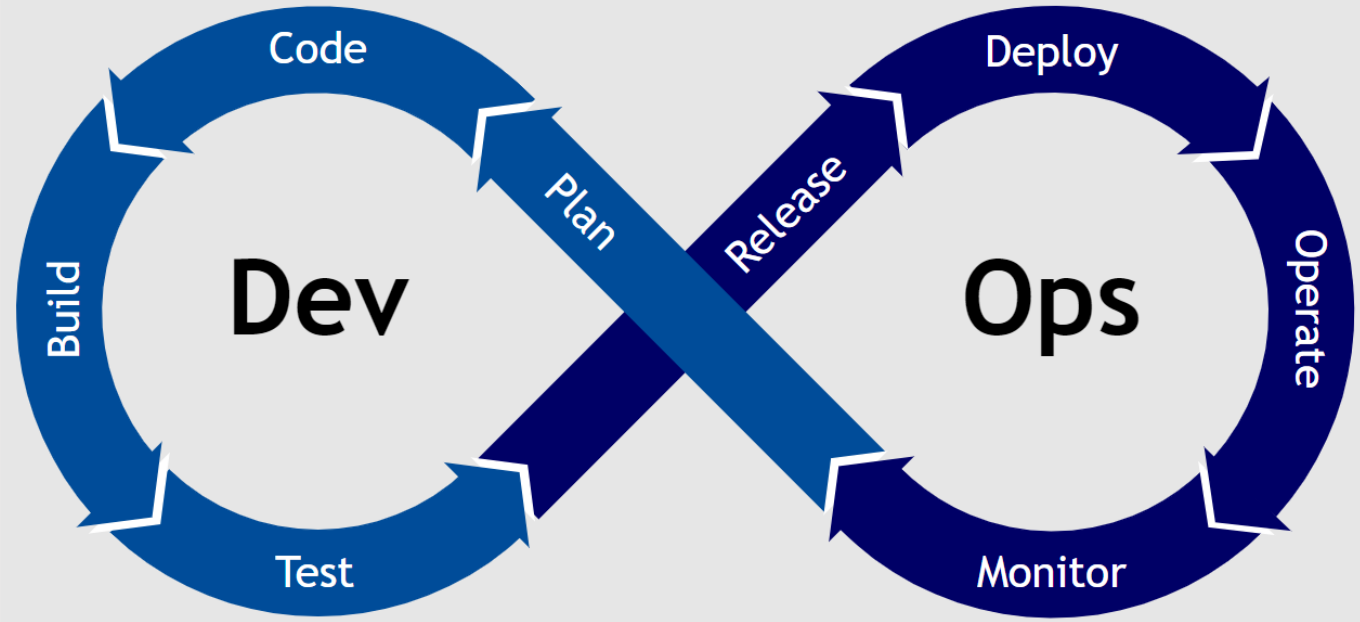
Agile

- Earlier delivery
- Continuous delivery
- Collaboration
- Open Communication
- Trust and independence
- Efficiency & simplicity
- Embrace change
- Satisfy customers

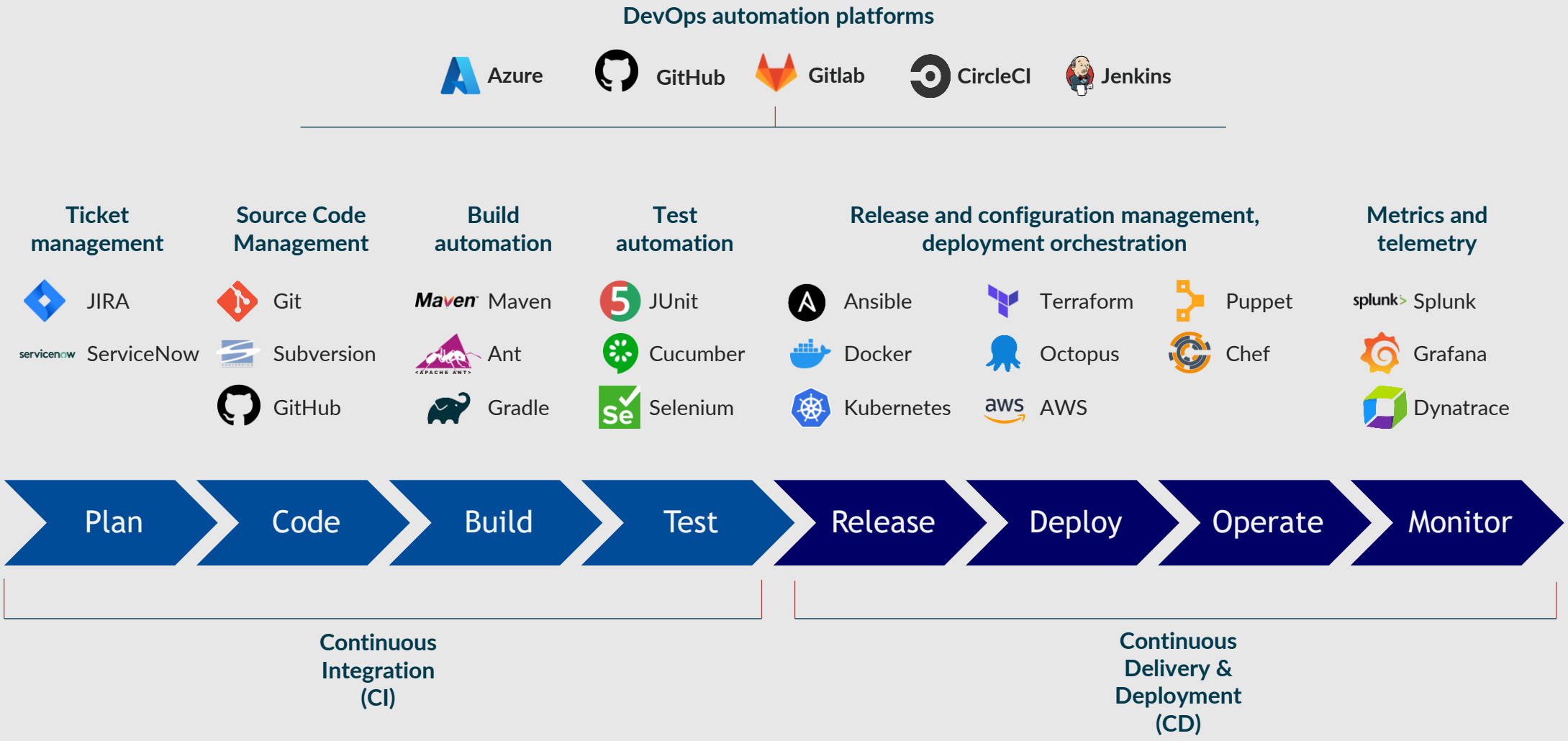
Lean

- Focus on value
- Attack bottlenecks
- Eliminate waste
- Continuous learning
- Prevent overburdening
- Small batch delivery
- Automate everything
- Reduce friction

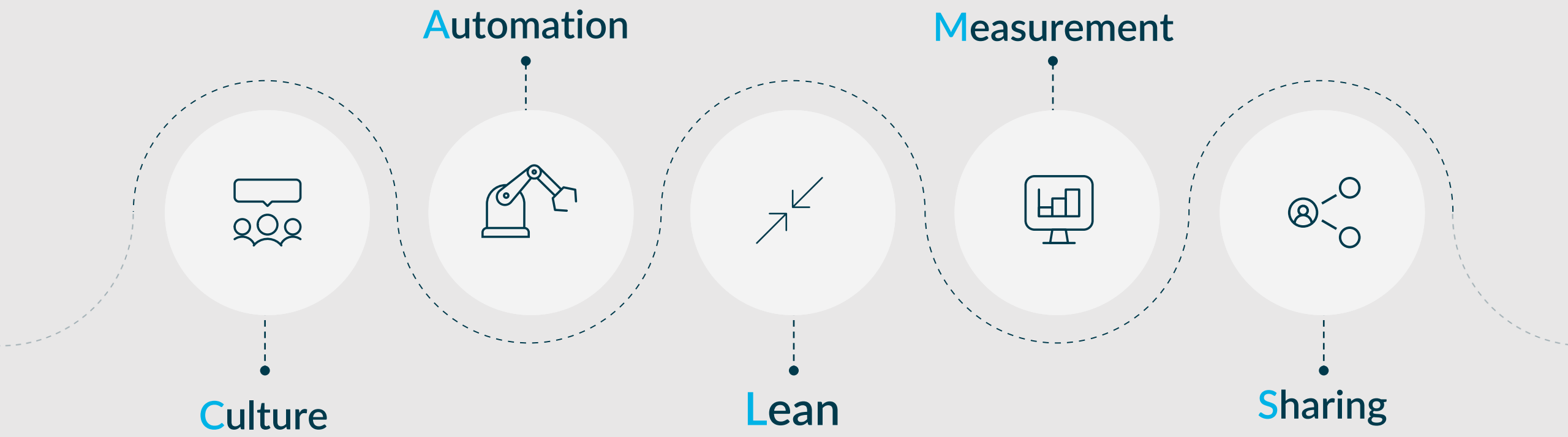
Faster, cyclical iteration and improvement



Automation is a key part of DevOps…



… but only part



What DevOps is and isn't

- Consistent & standardised automation
- Lean practices, small batch delivery
- Open collaboration & sharing
- Continuous improvement mindset
- Focus on the customer/user
- Optimizing constraints

- A single tool or technology
- Something you can 'buy in'
- Necessarily easy or quick to implement
- Relevant for *every* company or team
- One model, one way of working
- Only for developers

Lots of definitions. Same core ideas.

‘DevOps is a combination of software developers (dev) and operations (ops). It is defined as a software engineering methodology which aims to integrate the work of software development and software operations teams by facilitating a culture of collaboration and shared responsibility.’

https://about.gitlab.com/topics/devops/

‘DevOps is a set of practices, tools, and a cultural philosophy that automate and integrate the processes between software development and IT teams. It emphasizes team empowerment, cross-team communication and collaboration, and technology automation.’

https://www.atlassian.com/devops

‘DevOps enables formerly siloed roles—development, IT operations, quality engineering, and security—to coordinate and collaborate to produce better, more reliable products. By adopting a DevOps culture along with DevOps practices and tools, teams gain the ability to better respond to customer needs, increase confidence in the applications they build, and achieve business goals faster.’

https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-devops/

DevSecOps emerges

By the mid-2010s

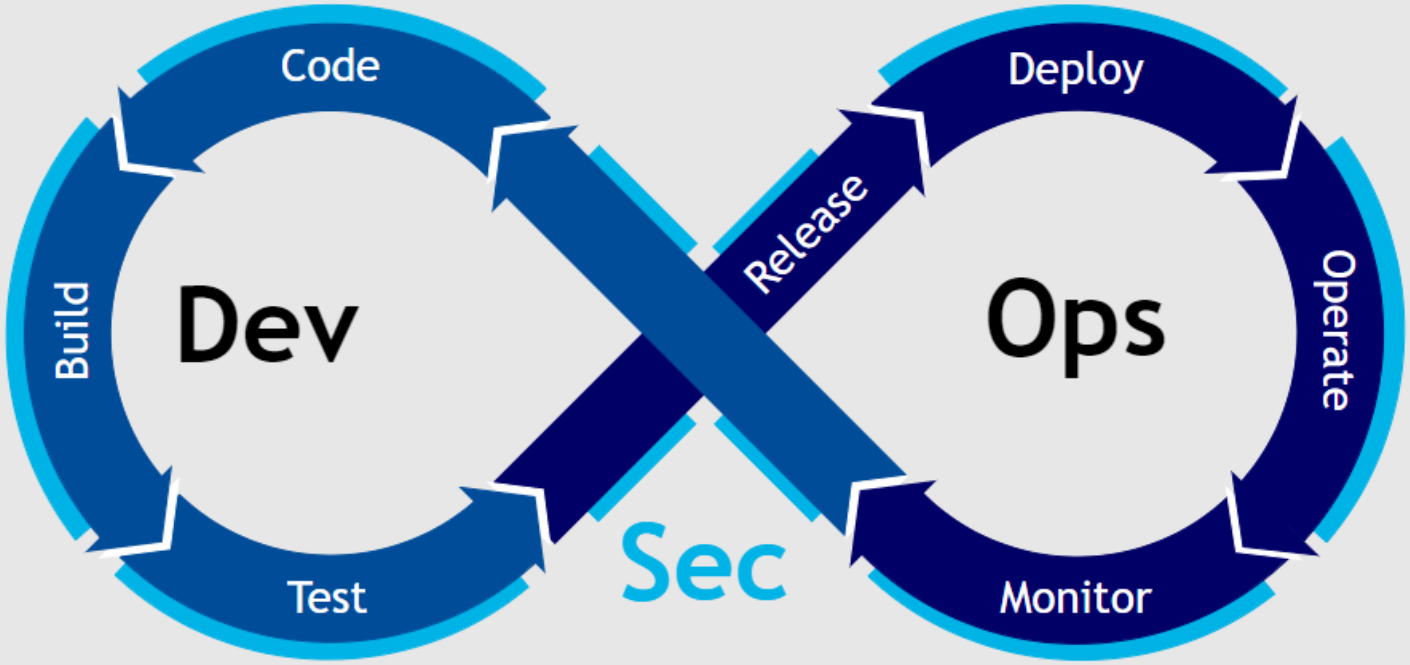
- Huge amount of work to stand up, configure and optimise DevOps pipelines
- Developers working more efficiently and delivering new features quicker
- Culture starting to shift toward more open collaboration and communication
- Release velocity increases, product consumers see faster product iteration
- Businesses see improvements to profits and customer retention

Security not invited to the party

- Secondary consideration or a bottleneck
- Little/no automation of scanning
- Proliferation of new apps and features exacerbates risk
- Risk profile of application estate grows
- Security incidents gain international press, regulatory attention and record fines
- Garners board-level attention – protect our reputation (and profits!)

Revisiting the SDLC (and pipelines!)

Embed security at every stage



A shift in mindset?

A quality product is a secure product

Have appropriate controls

But no unnecessary bottlenecks!

All stakeholders need to collaborate to improve the flow of work

Lots of definitions. Same core ideas (part 2)

‘DevSecOps stands for development, security, and operations. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.’

https://www.redhat.com/en/topics/devops/what-is-devsecops

‘DevSecOps is the practice of integrating security into a continuous integration, continuous delivery, and continuous deployment pipeline. By incorporating DevOps values into software security, security verification becomes an active, integrated part of the development process.’

https://www.atlassian.com/devops/devops-tools/devsecops-tools

‘DevSecOps weaves security practices into every stage of software development right through deployment with the use of tools and methods to protect and monitor live applications. New attack surfaces such as containers and orchestrators must be monitored and protected alongside the application itself.’

https://about.gitlab.com/topics/devsecops/

Benefits of securing DevOps

Apps consistently secure by design

Pervasive security mindset

Valuable security and business insights

Relevant data for quickly reacting to incidents

Greatly reduced cost spent on fixes

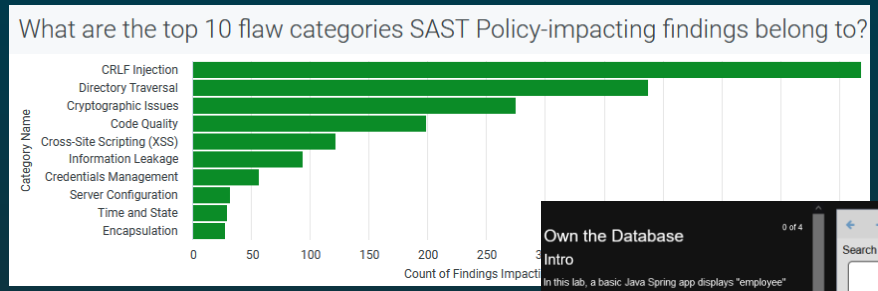
More developer time spent on new features

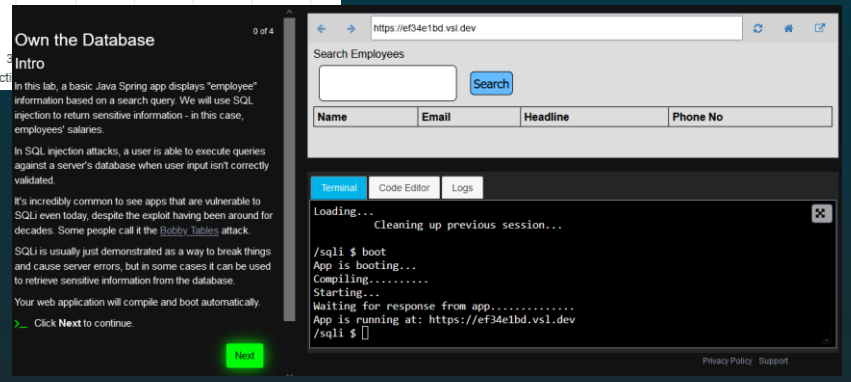
Gives assurance to stakeholders

Overall improved risk and security posture

Apply a DevOps mindset to more than tech

Continual DevSecOps feedback loop



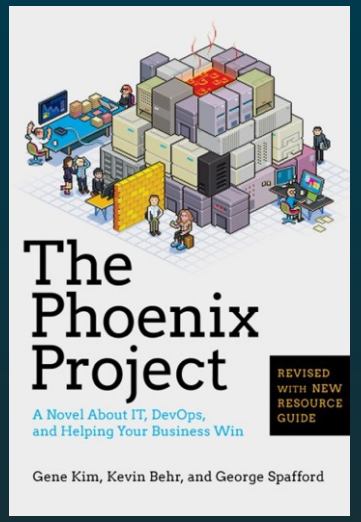


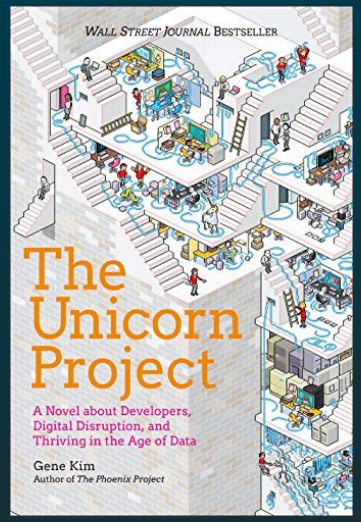
Continuous education & risk reduction

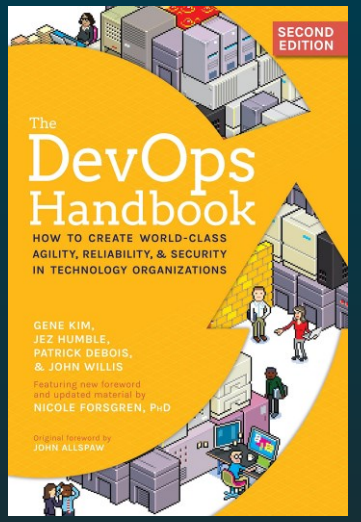
To summarise

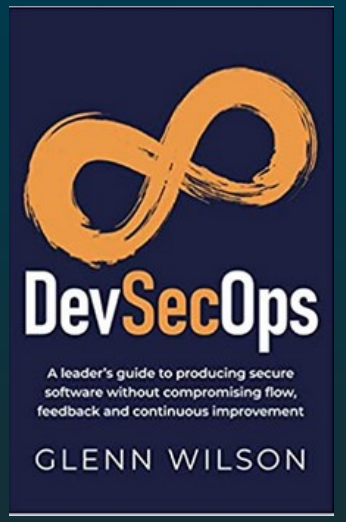
- DevOps & DevSecOps – lots of definitions, same core ideas
- Collective movements which continue to evolve
- It’s not just about the technology
- Security is a key characteristic of a quality product
- Lots of benefits from securing your software

Some further reading...









VERACODE

Thank you

Nick Barham

nbarham@veracode.com

https://uk.linkedin.com/in/nicholasbarham