DevSecOps - by any other name?

Seb Rose
Twitter: @sebrose
Blog: https://cucumber.io/blog/
E-mail: seb.rose@smartbear.com

SMARTBEAR

Agenda

Dev, Sec, Ops

DevOps

DevSecOps

What’s in a name?

seb.rose@smartbear.com

Agenda

Dev, Sec, Ops

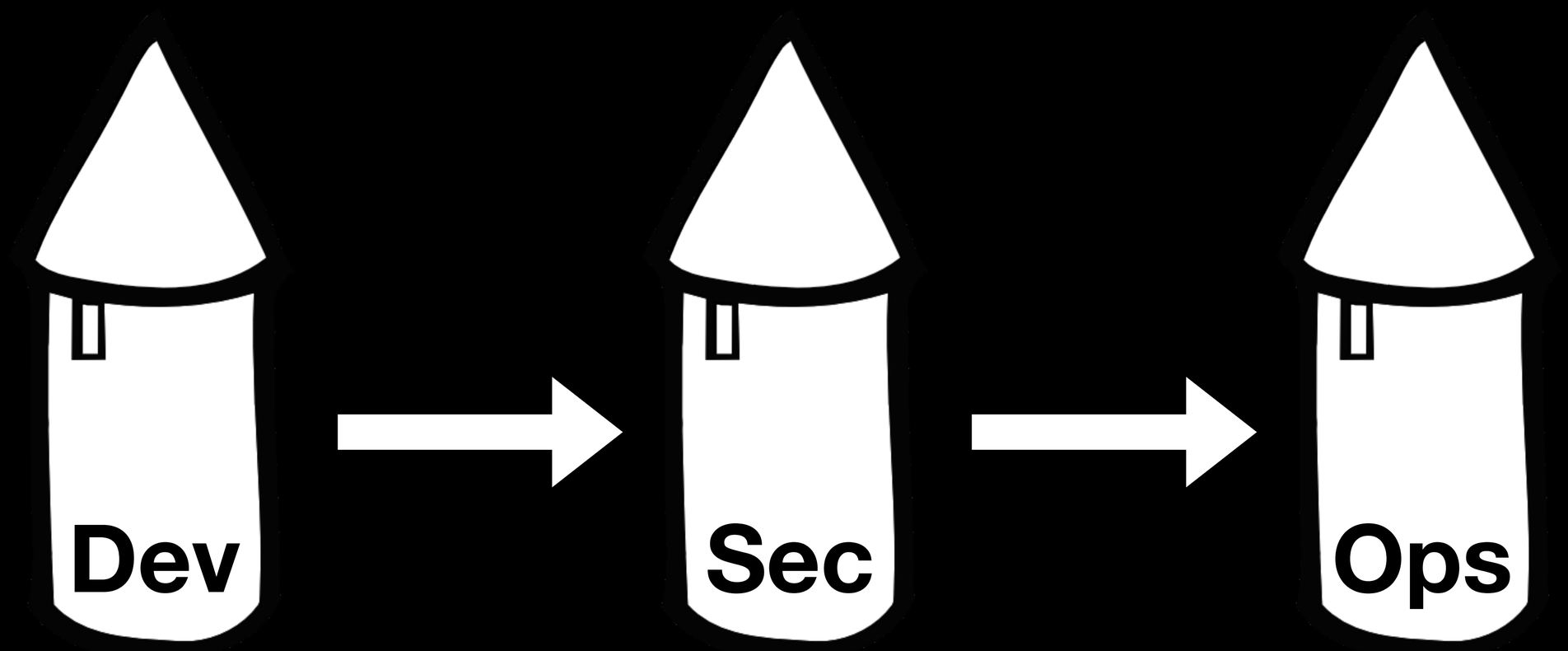
DevOps

DevSecOps

What’s in a name?

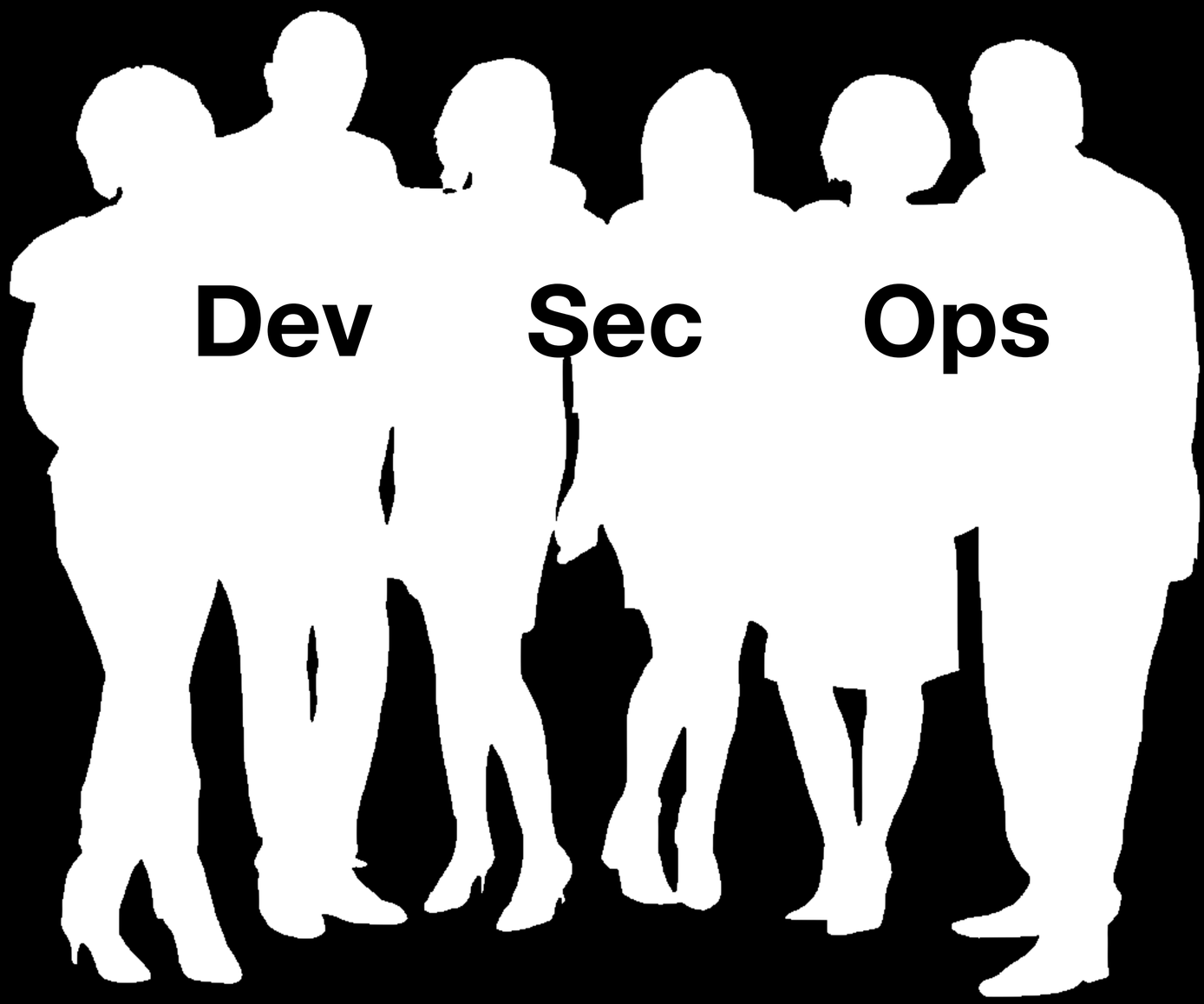
seb.rose@smartbear.com

Traditional silos



seb.rose@smartbear.com

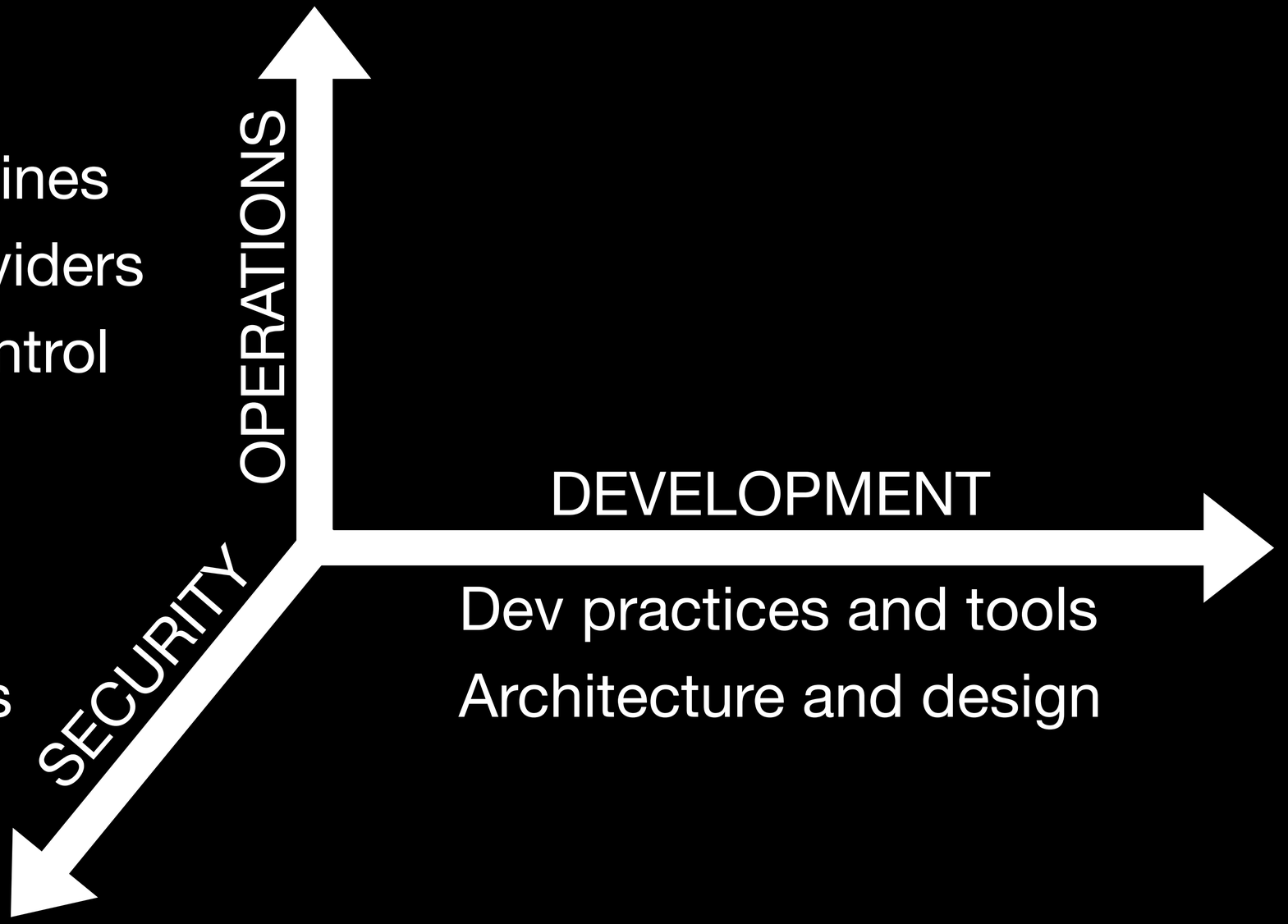
Agile dream



seb.rose@smartbear.com

Orthogonal concerns

Build pipelines
Cloud providers
Source control



OWASP scans
Code vulnerabilities

Dev practices and tools
Architecture and design

seb.rose@smartbear.com

Agenda

Dev, Sec, Ops

DevOps

DevSecOps

What’s in a name?

There is no universally agreed definition of the term.

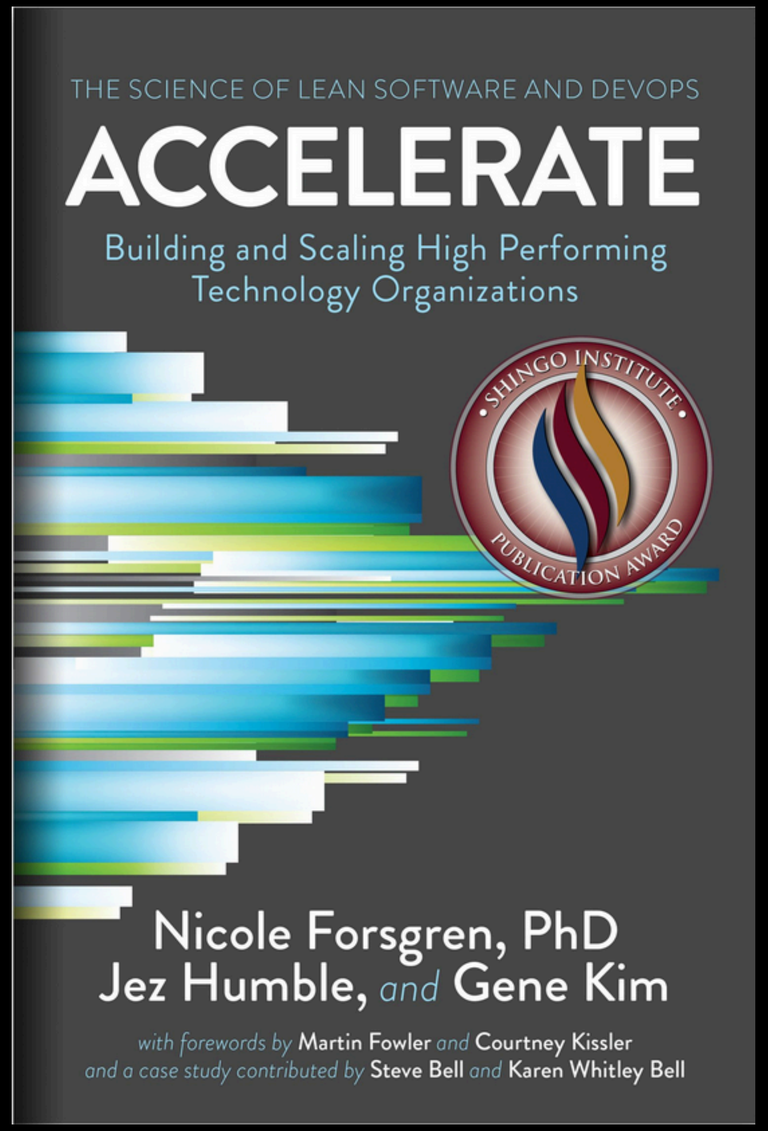
Characterized by key principles: shared ownership, workflow automation, and rapid feedback. At its most successful, DevOps is a combination of specific practices, culture change, and tools.

“A set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality” - Bass, Weber, Zhu

Ideal outcomes

DORA metrics

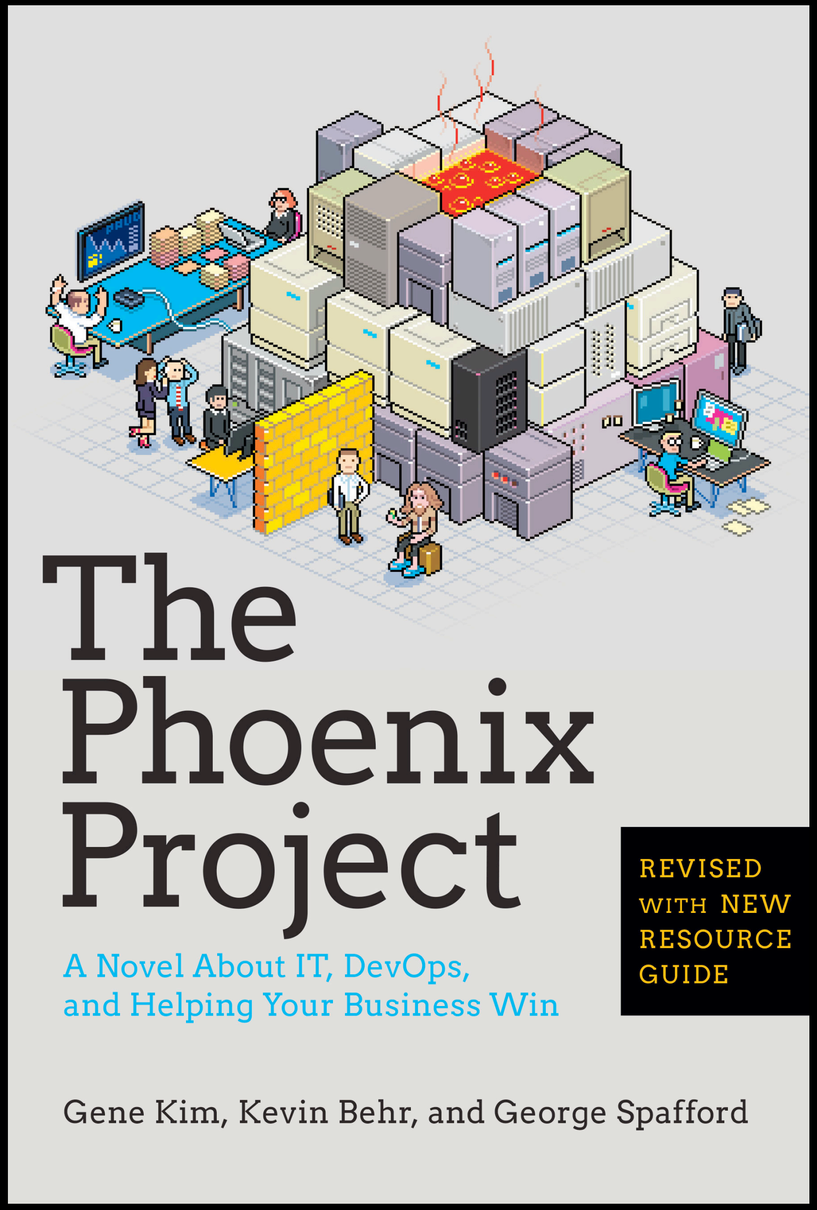
- Lead/cycle time (shorter)
- Deployment frequency (higher)
- Mean time to restore (shorter)
- Change fail percentage (lower)



seb.rose@smartbear.com

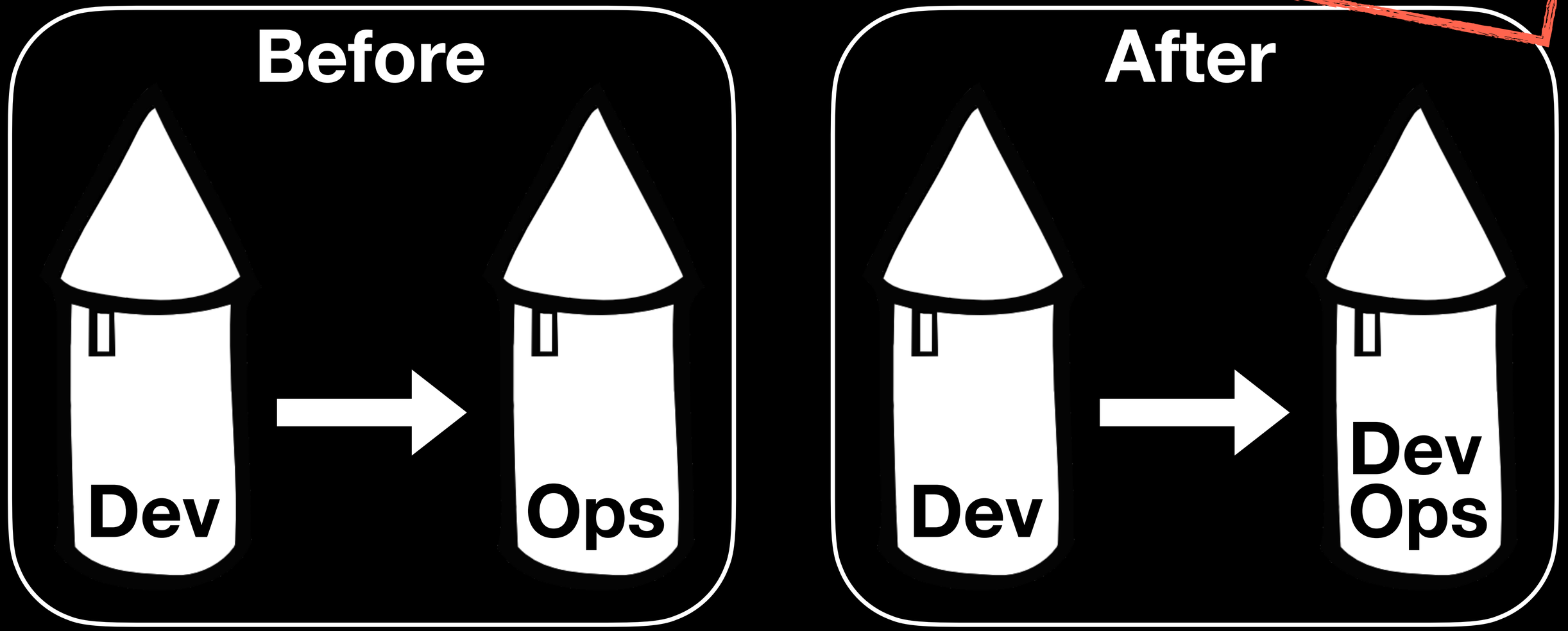
Idealised transformation

With the help of a prospective board member and his mysterious philosophy of The Three Ways, Bill starts to see that IT work has more in common with manufacturing plant work than he ever imagined. With the clock ticking, Bill must organize work flow streamline interdepartmental communications, and effectively serve the other business functions at Parts Unlimited.



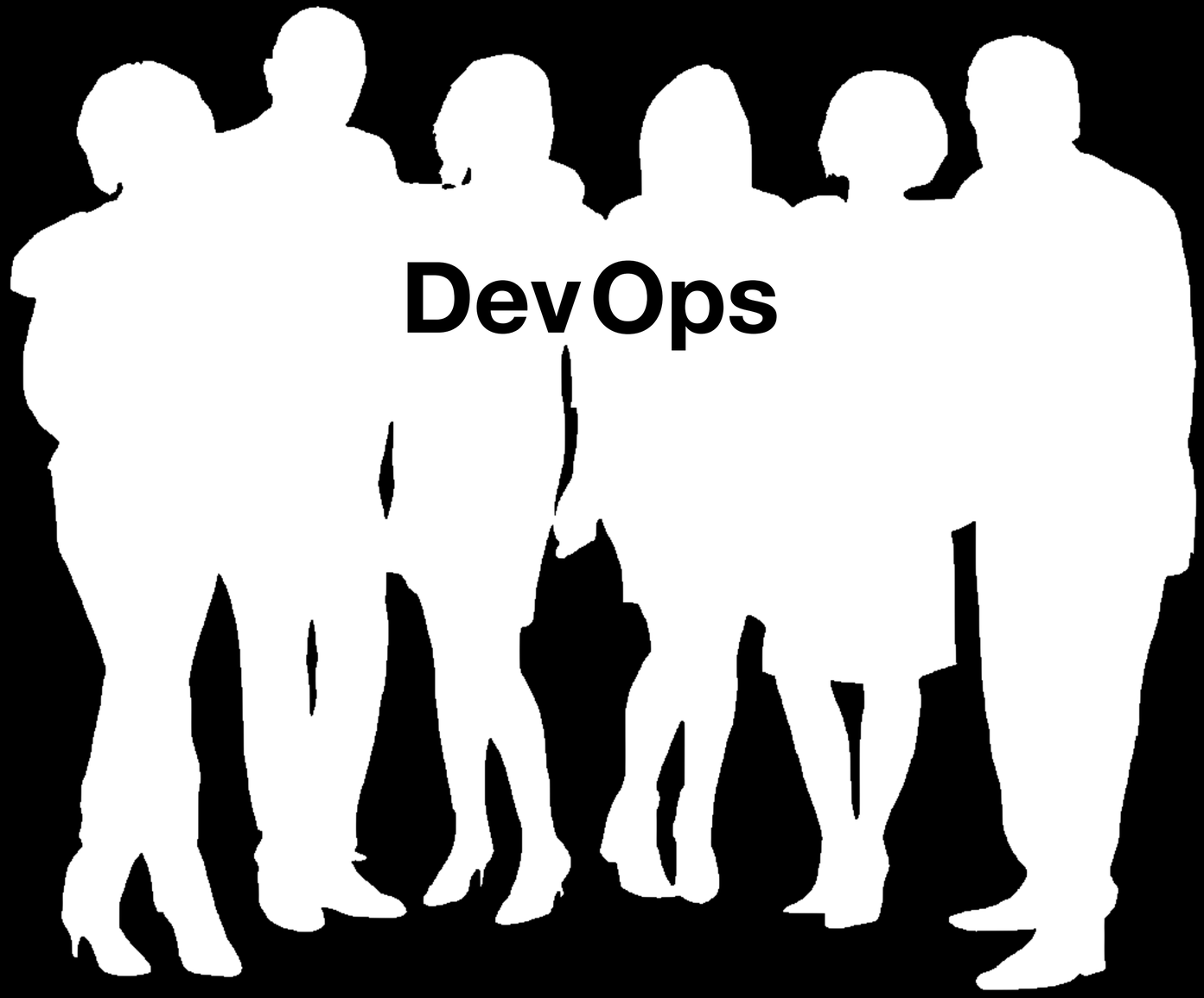
Typical transformation

Excessively cynical

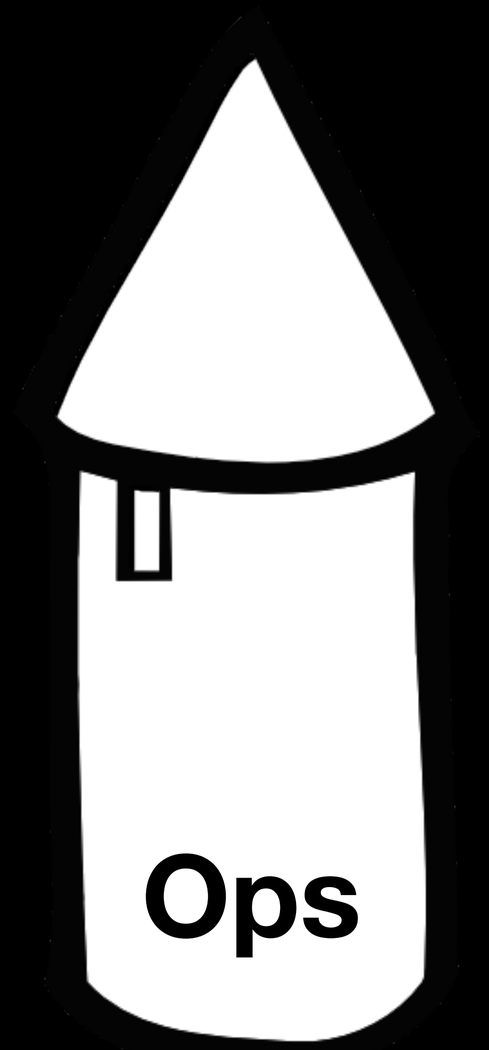


seb.rose@smartbear.com

Living the dream



Ops as platform team



Platform tools

platform team

Agenda

Dev, Sec, Ops

DevOps

DevSecOps

What’s in a name?

seb.rose@smartbear.com

Who owns security?

The [dev] team is trusted to do its own security research and implementation

There's a security team, but it doesn't involve face to face with us, the dev team. So we just run the dev process without counting on them

I regularly put security suggestions in the box of suggestions, only to be ignored

I am the only one who actually cares about security in my organization

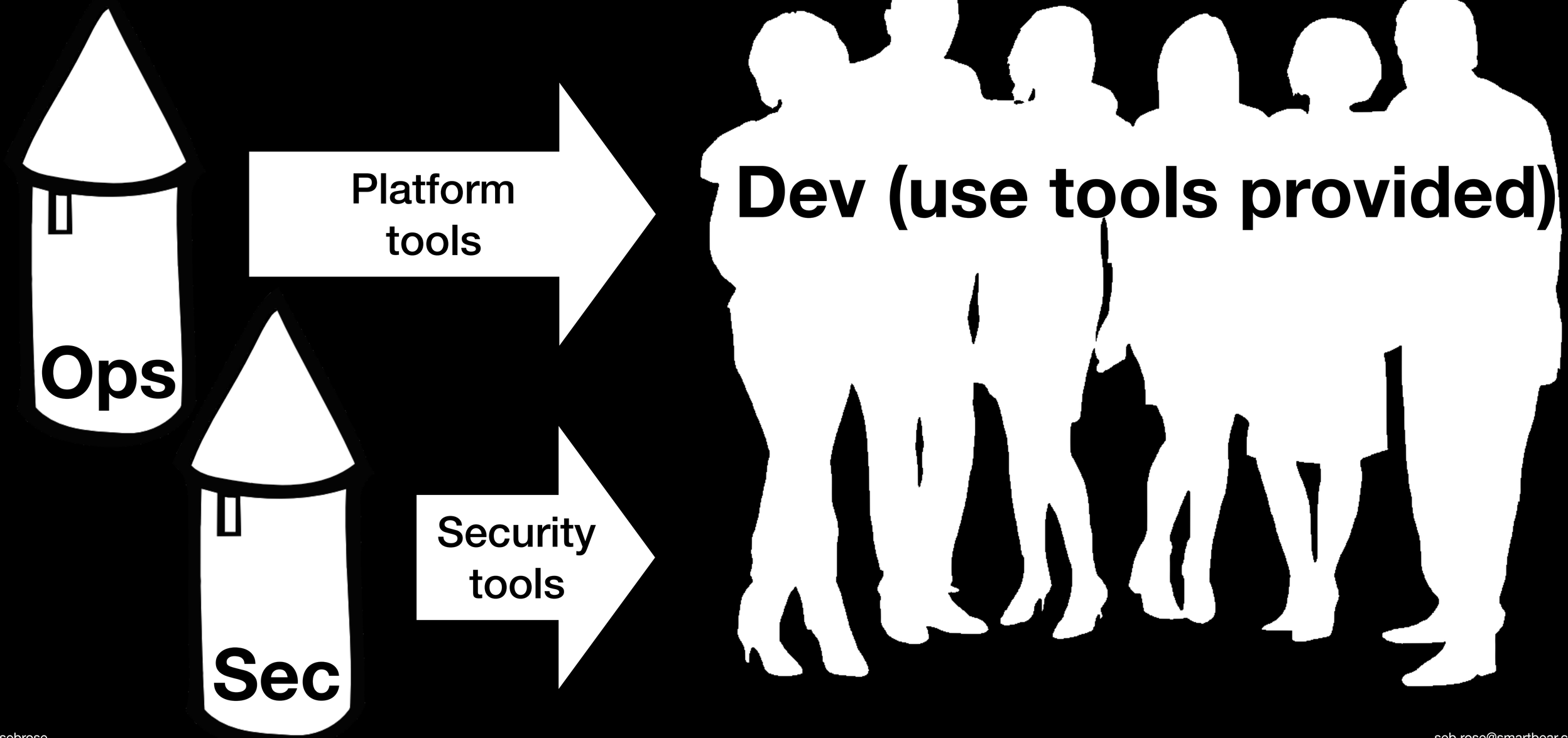
https://devops.com/whos-responsible-for-security-apparently-it-depends/

Desire paths

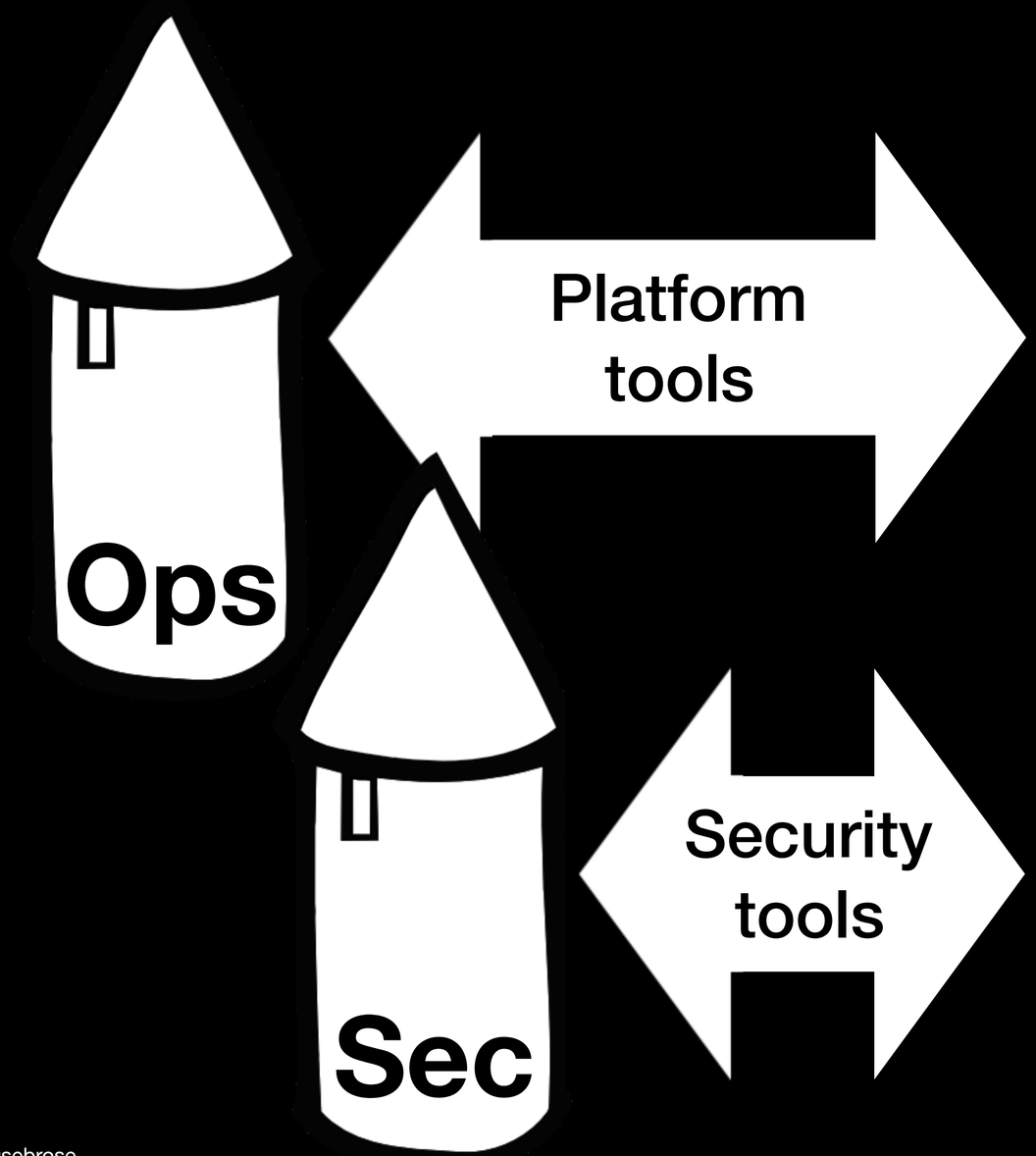
http://www.databoxdigital.com/2014/02/02/desire-paths/

seb.rose@smartbear.com

Building on DevOps



Dev enablement



Platform tools

Security tools

seb.rose@smartbear.com

Agenda

Dev, Sec, Ops

DevOps

DevSecOps

What’s in a name?

seb.rose@smartbear.com

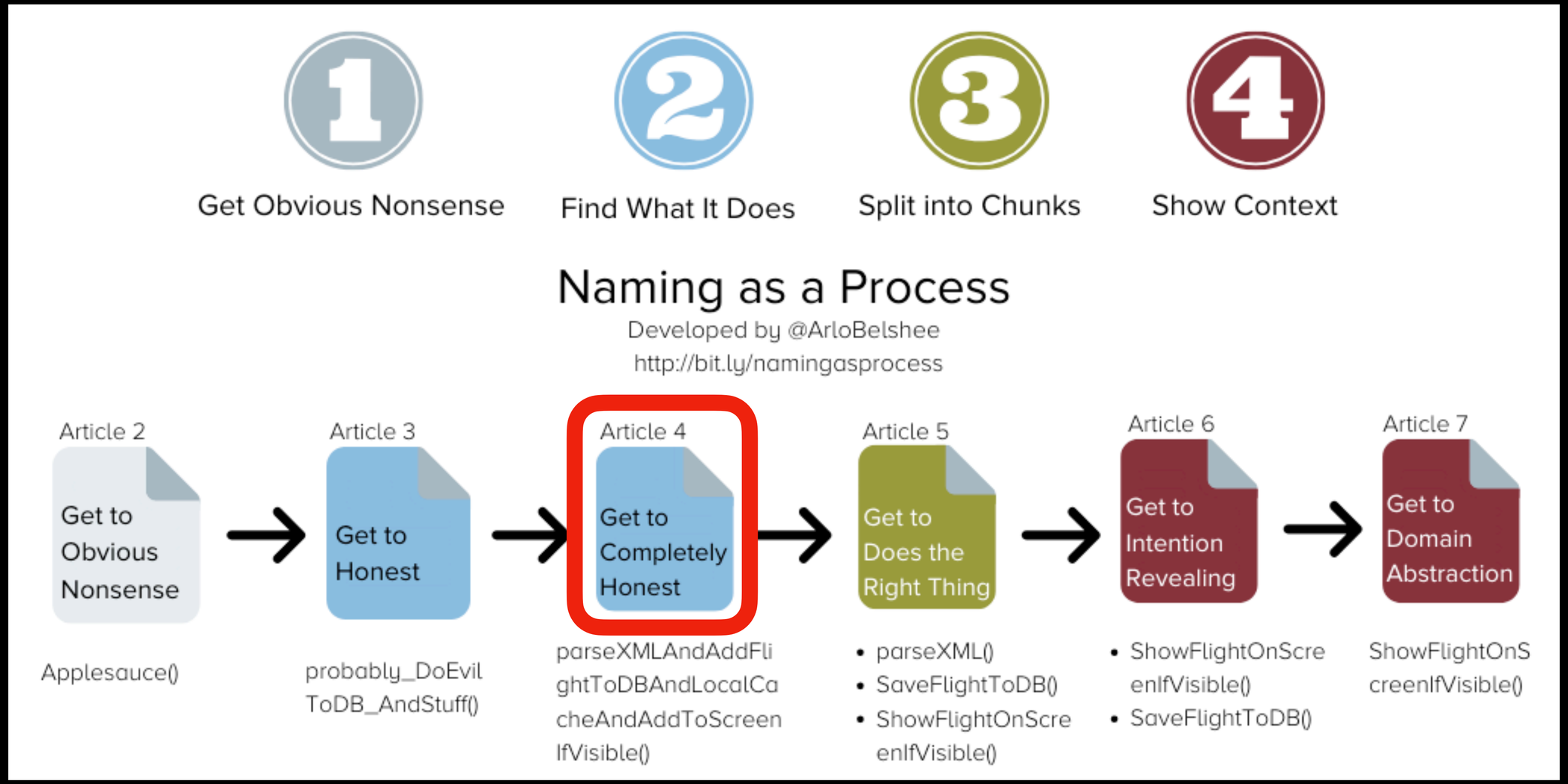
What’s in a name?

O, be some other name!
What’s in a name? That which we call a rose
By any other name would smell as sweet

William Shakespeare, Romeo and Juliet

The name is not the thing

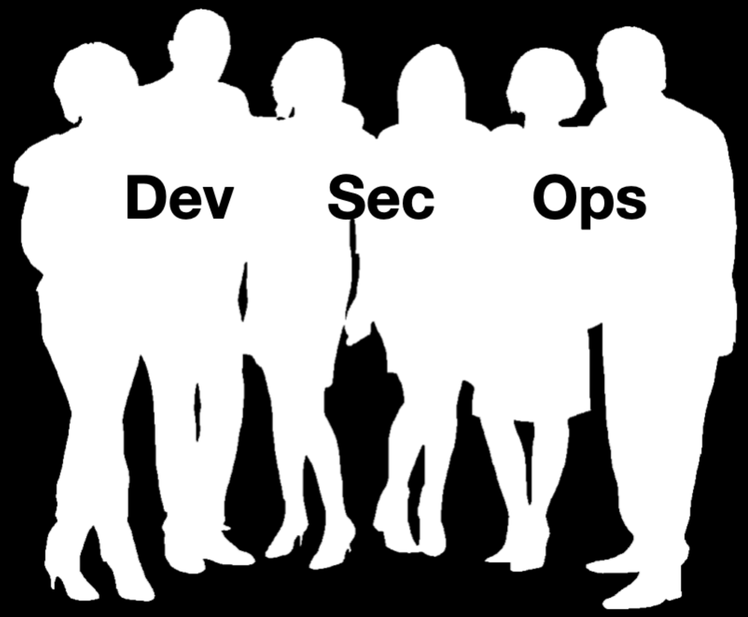
Names are important

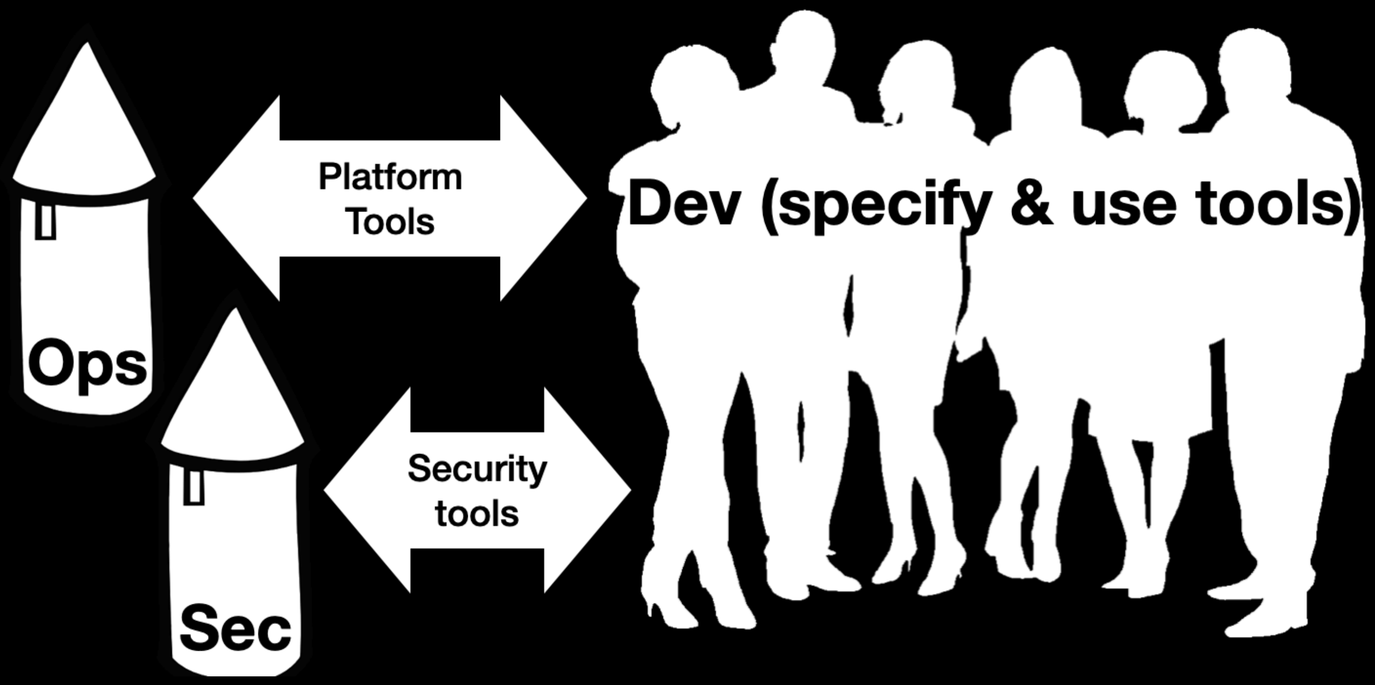


https://www.digdeeproots.com/articles/on/naming-process/

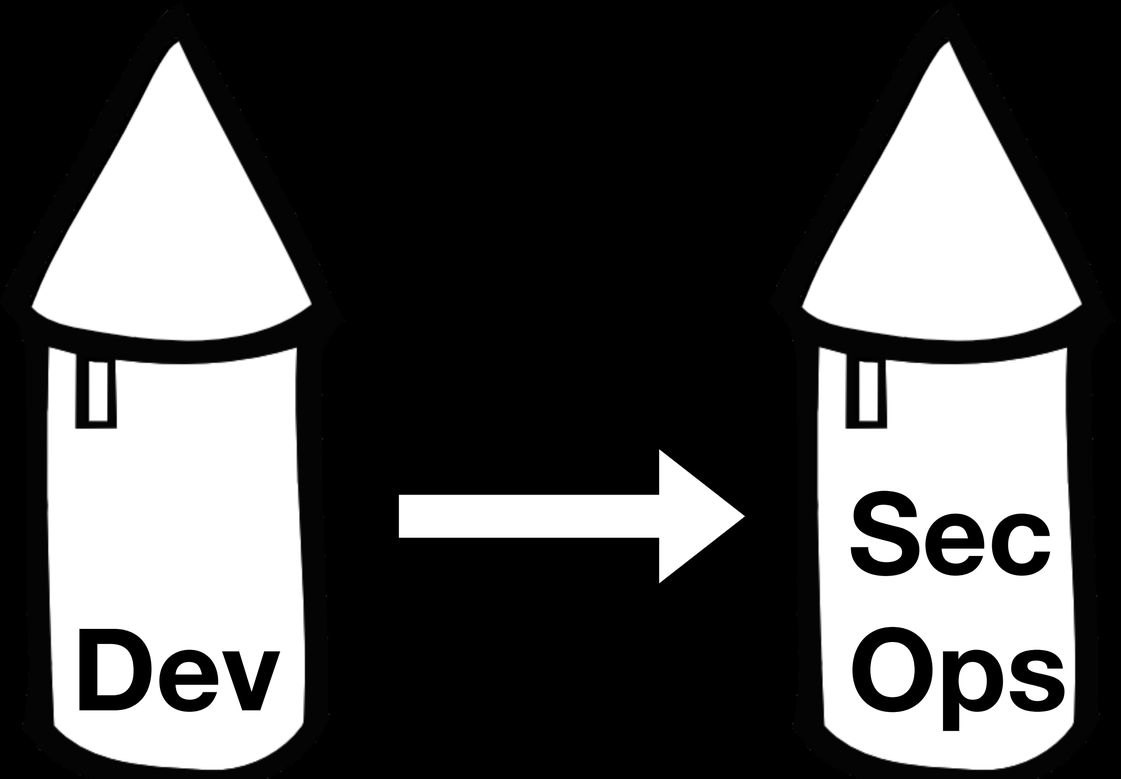
seb.rose@smartbear.com

Honest


Dev
Sec
Ops


Ops
Sec
Platform
Tools
Security
tools
Dev (specify & use tools)

Dishonest



Takeaways

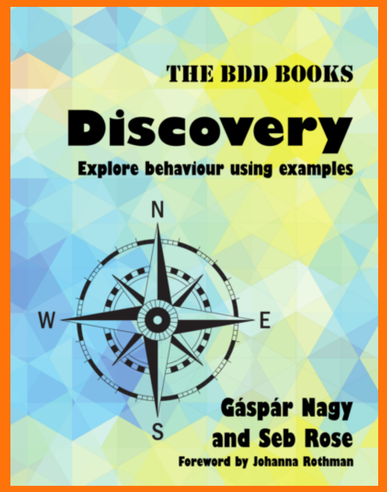
The name is not the thing

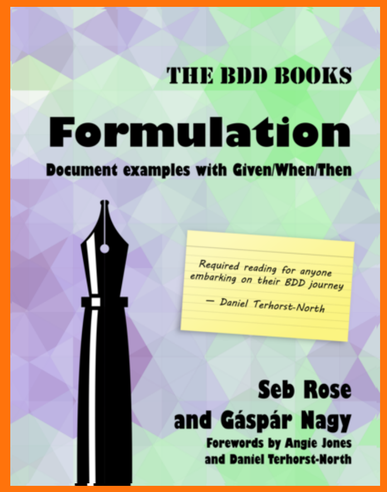
Investment is required to deliver benefits (time and money)

Process changes aren't side effects

Platform teams facilitate delivery AND enable consistency

seb.rose@smartbear.com





http://bddbooks.com

Seb Rose

Twitter: @sebrose

Blog: https://cucumber.io/blog/

E-mail: seb.rose@smartbear.com

SMARTBEAR