Working on DevSecOps Culture

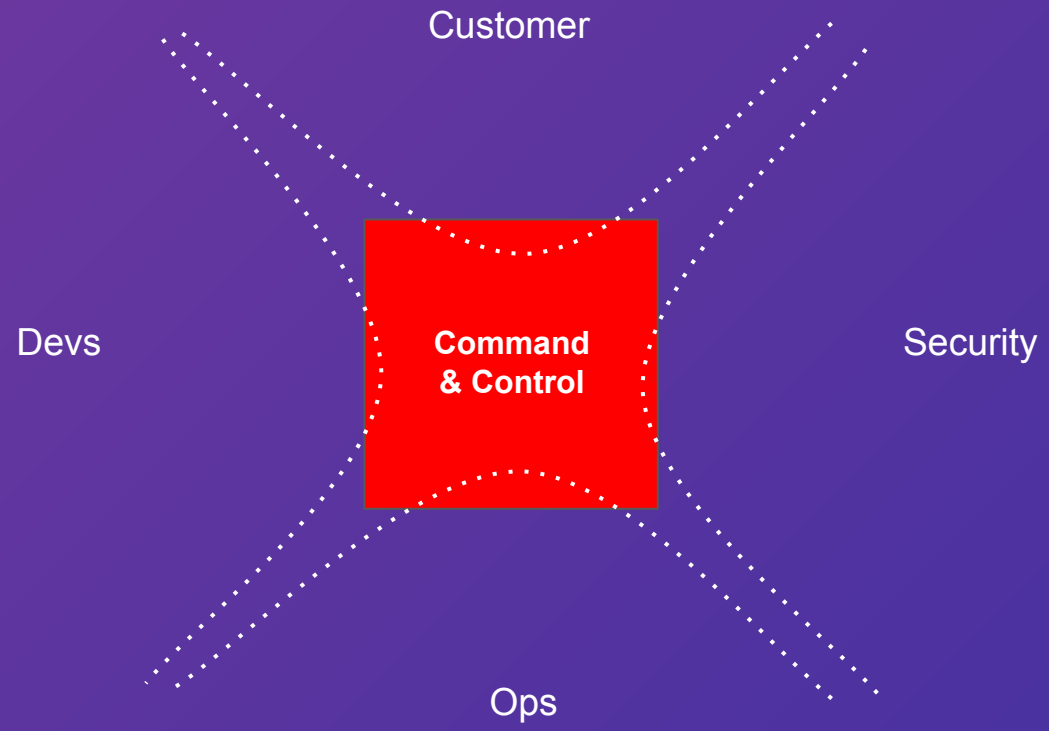
A team centric view

Patrick Debois | patrick.debois@snyk.io

Tools & Culture

Patrick Debois – #thinktogether
Dev(sec)Ops: everything you do to overcome the friction created by silos ... All the rest is plain engineering

Dev(Sec)Ops Friction Points



Know your pains

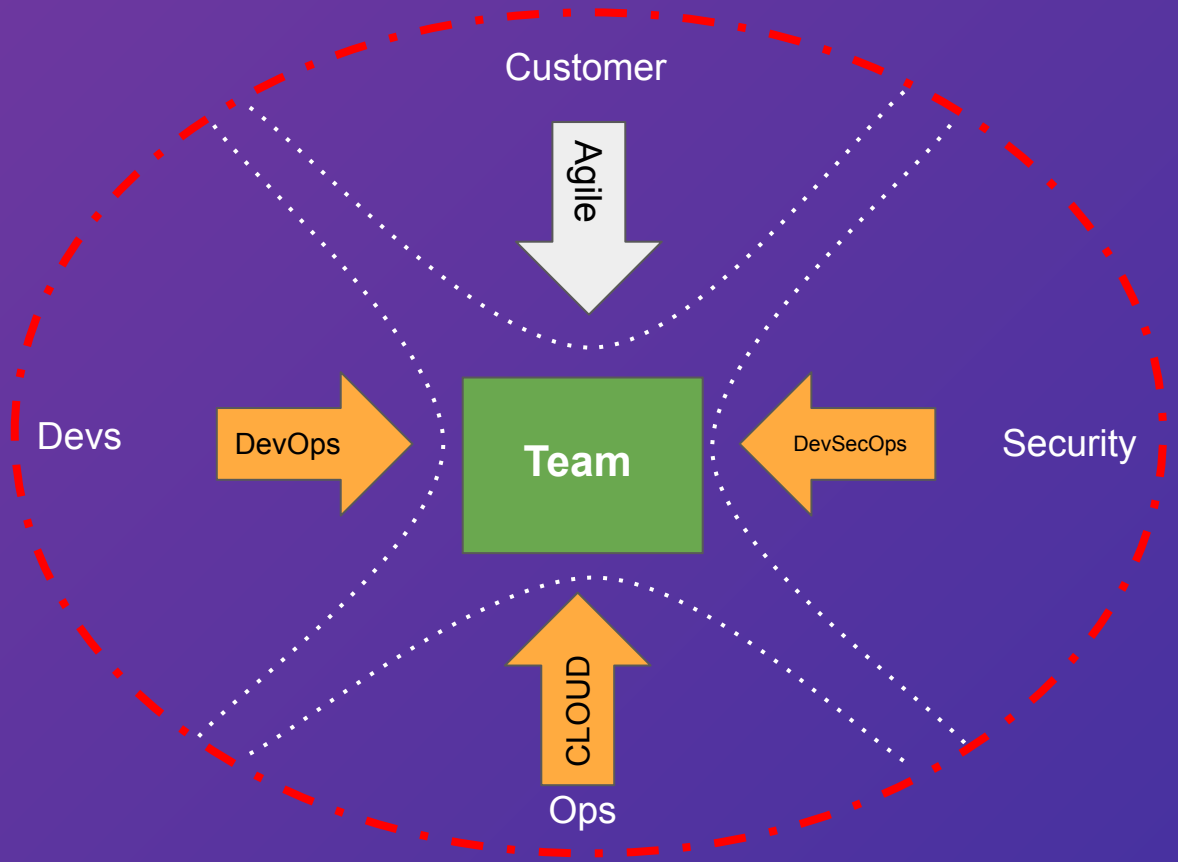
Understand the **bottlenecks** introduced by **Silos** you need to overcome.

Technical
stack, environment, tools

Management
prioritisation, budget , authority, hiring , incentives

Personal
education, knowledge, motivation

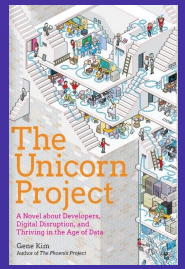
Pressure / Shifts



Forces At Work

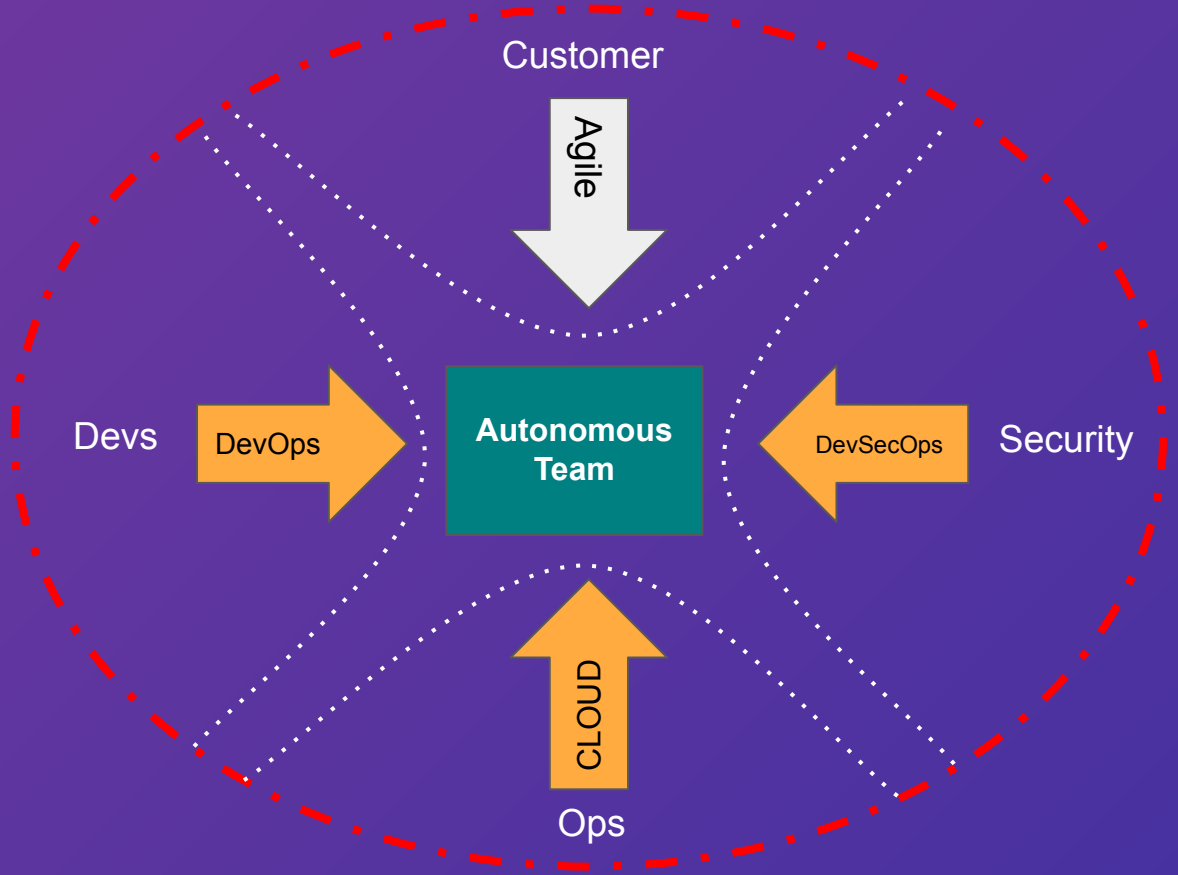
Different forces at work will cause movement.

*Shift Down - **Agile***
*Shift Right - **DevOps***
*Shift Left - **DevSecOps***
*Shift Up - **Cloud***



https://itrevolution.com/devops-books/

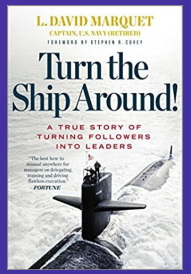
Power to the Team



Focus on team

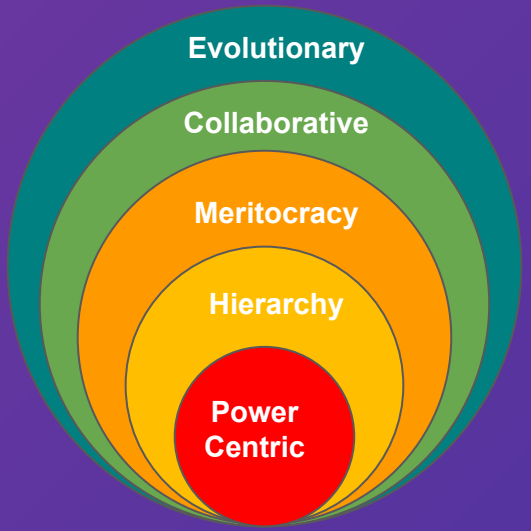
Empower the people doing the work to make the right decisions. **Delegation of authority** does not happen magically overnight.

Management becomes supportive vs control.



https://davidmarquet.com/books/

Company Collaboration Culture



Autonomy - Meaning

Empower - Customer Centric

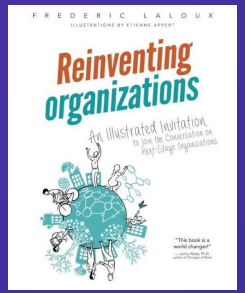
Measure - Scientific & KPIs

Automation - Order & Stability

Command & Control

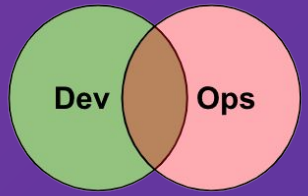
Your CEO will set the tone

Organization have different cultures. Depending on your context you will focus more on automation, metrics, empowerment or command and control. You need to **work on ALL layers to embed it** in the organization.



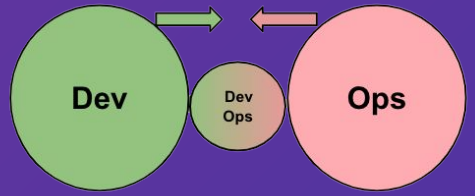
https://www.reinventingorganizations.com/

Dev(Sec)Ops Team Patterns

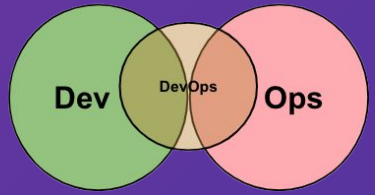


Dev and Ops
Collaboration

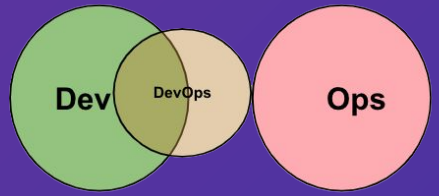
Fully Shared Ops
Responsibilities



Devops
with Expiry date



DevOps
Evangelist Team



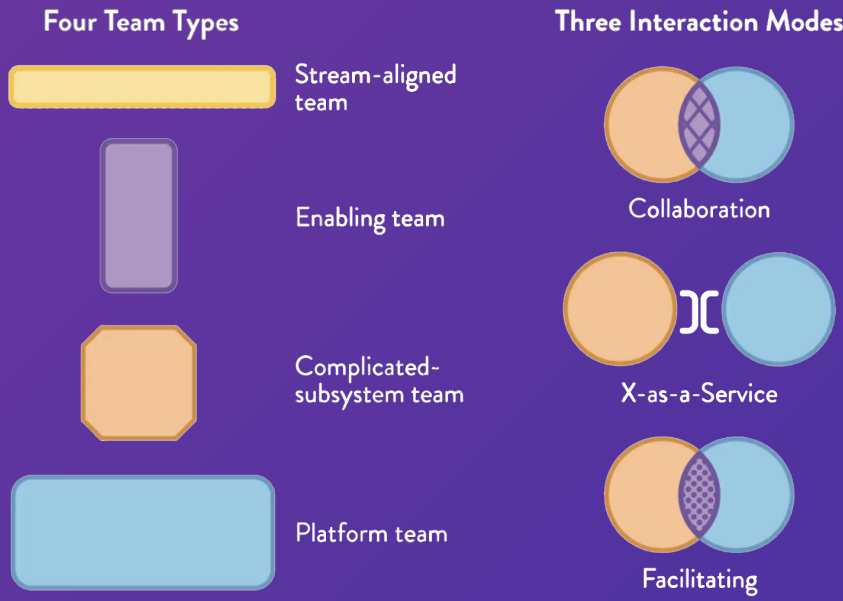
Container-Driven
Collaboration

How will security interact?

Different topologies exist , some are more efficient than others but it depends on your organization's culture.

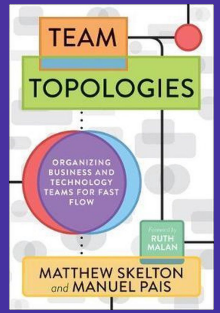
https://web.devopstopologies.com/

Team Interaction Modes



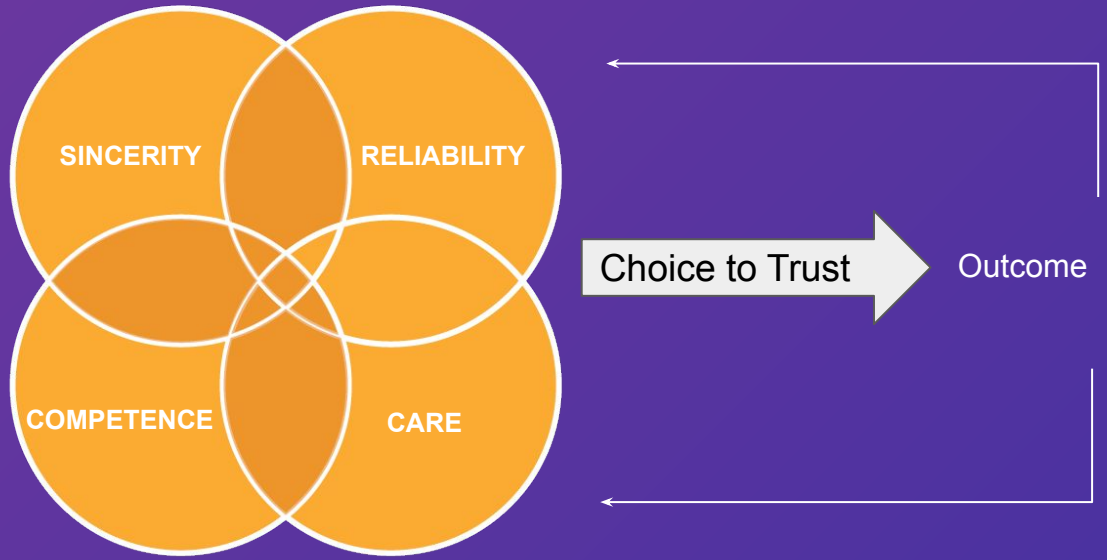
How will your security team collaborate?

Interaction will happen through automation, abstraction **AND collaboration**



https://teamtopologies.com/

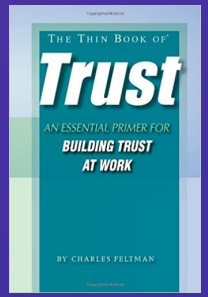
Building & Gaining Trust



Trust is a Choice

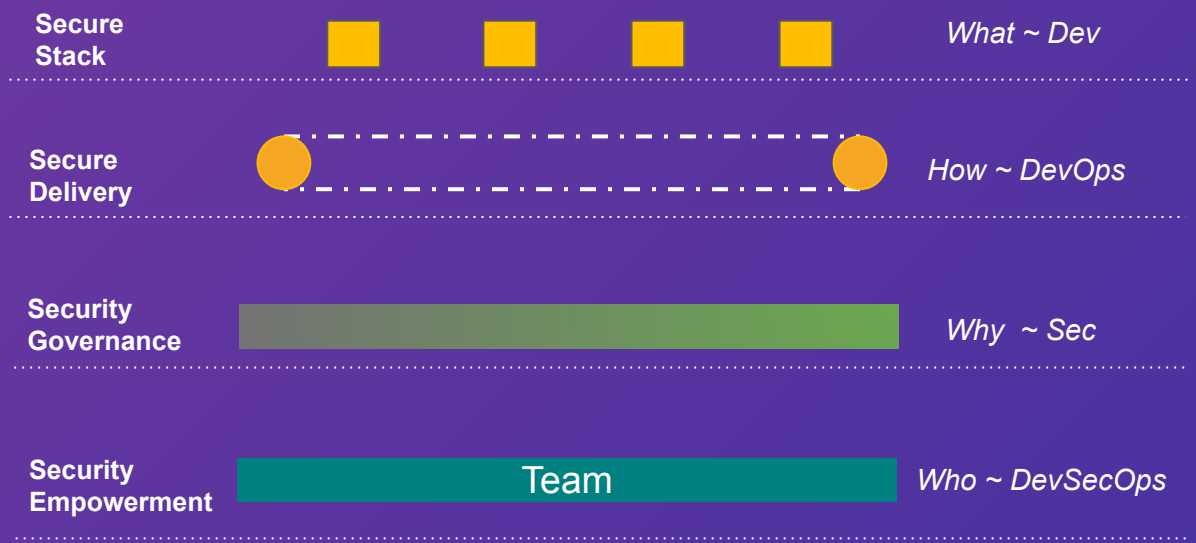
Trust is **Bi-Directional**

Asking for Trust vs being **Trustworthy**



https://www.thinbook.com

4 DevSecOps Areas

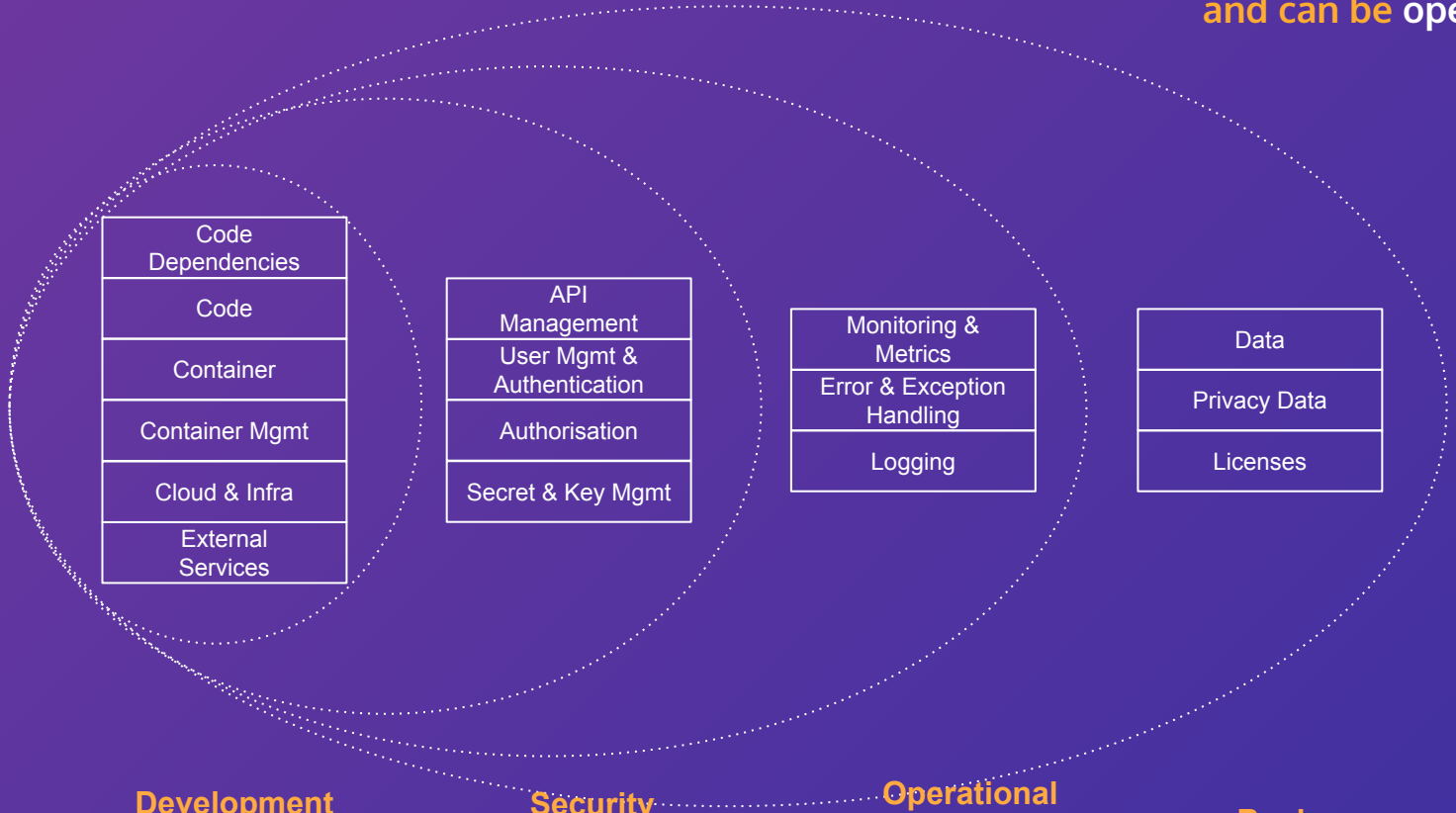


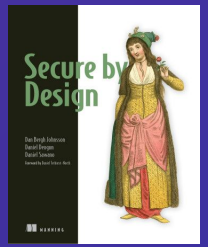
Areas influence each other

Is **what** we are delivering secure?
Is **how** we are delivering it secure?
Do we understand **why** we are securing it?
Do we trust **who** is delivering it ?

Secure Stack

As a developer we want to make sure that the application is secure and can be operated securely.

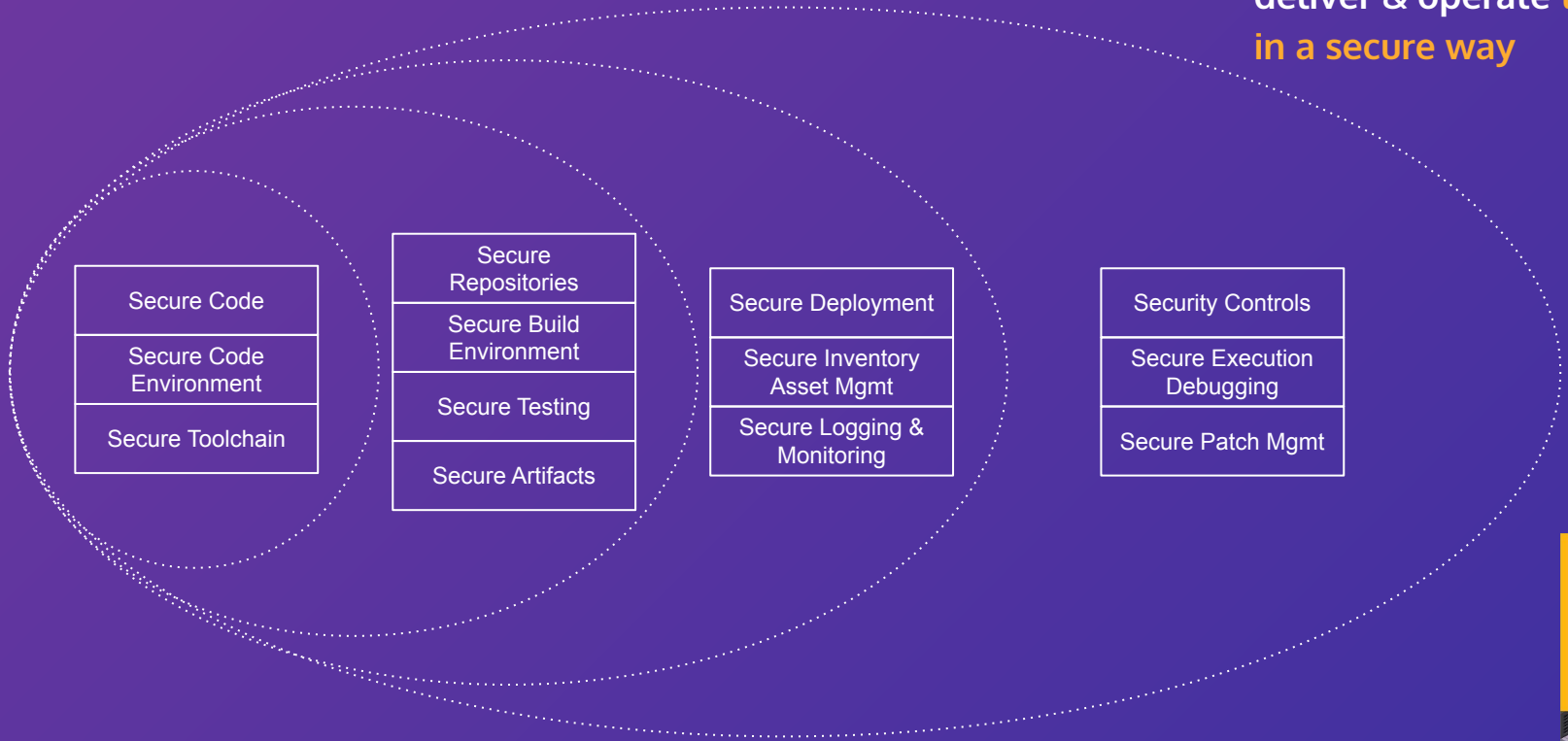


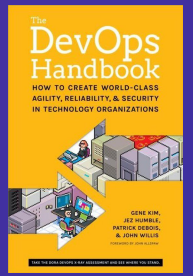


https://www.manning.com/books/secure-by-design

Secure Delivery

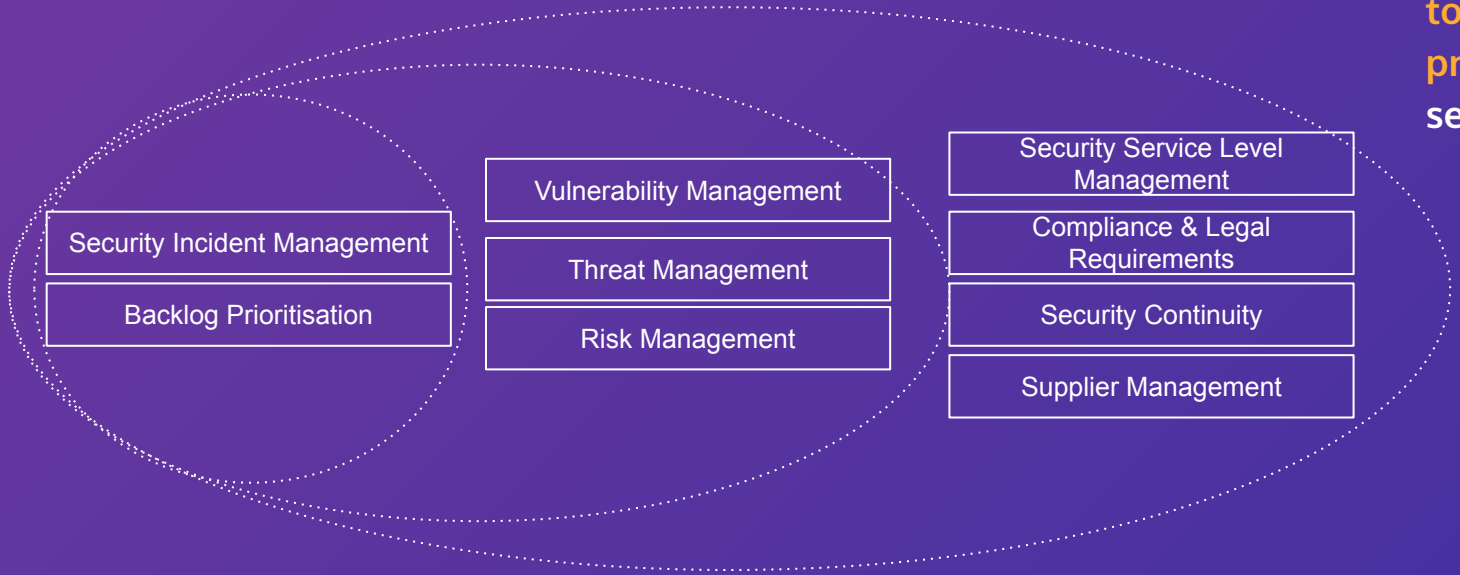
As a developer we want to make sure we can **build, deliver & operate** the service in a secure way



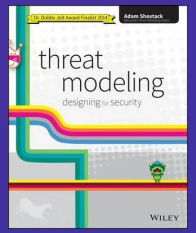


https://itrevolution.com/devops-books/

Secure Governance

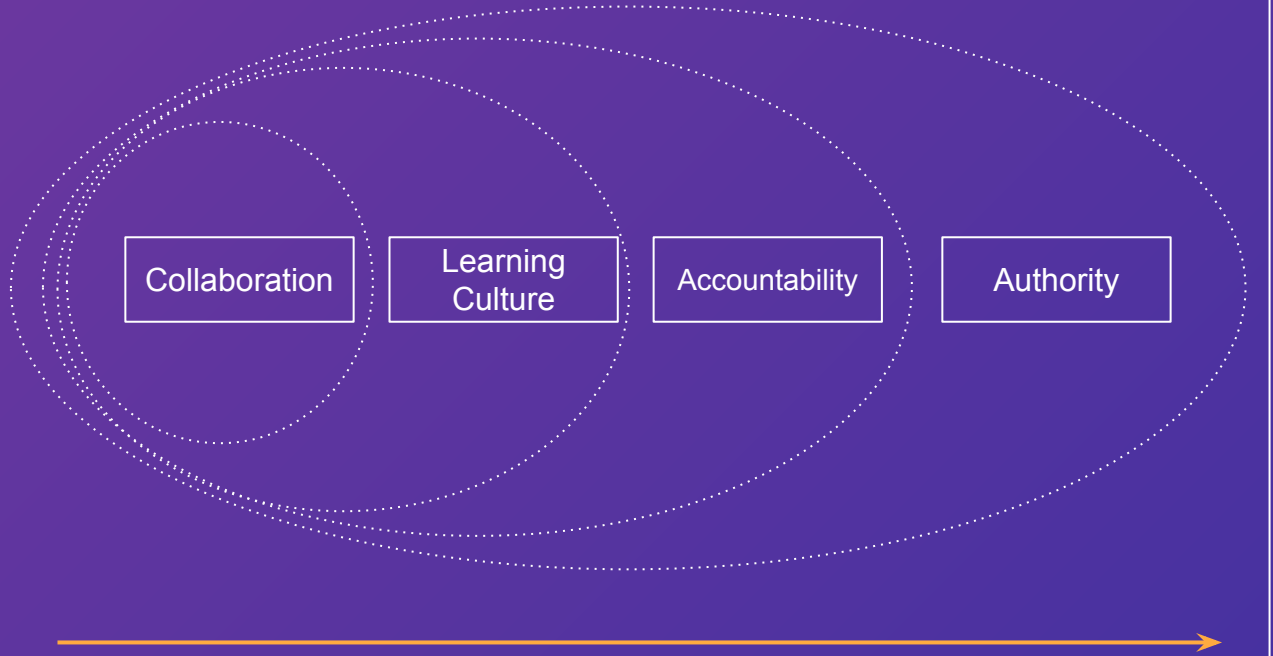


As a developer we want to participate in the processes for managing security better

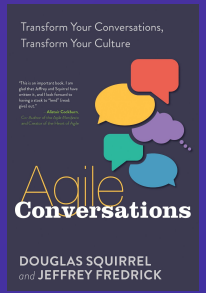


https://threatmodelingbook.com/

Secure Empowerment

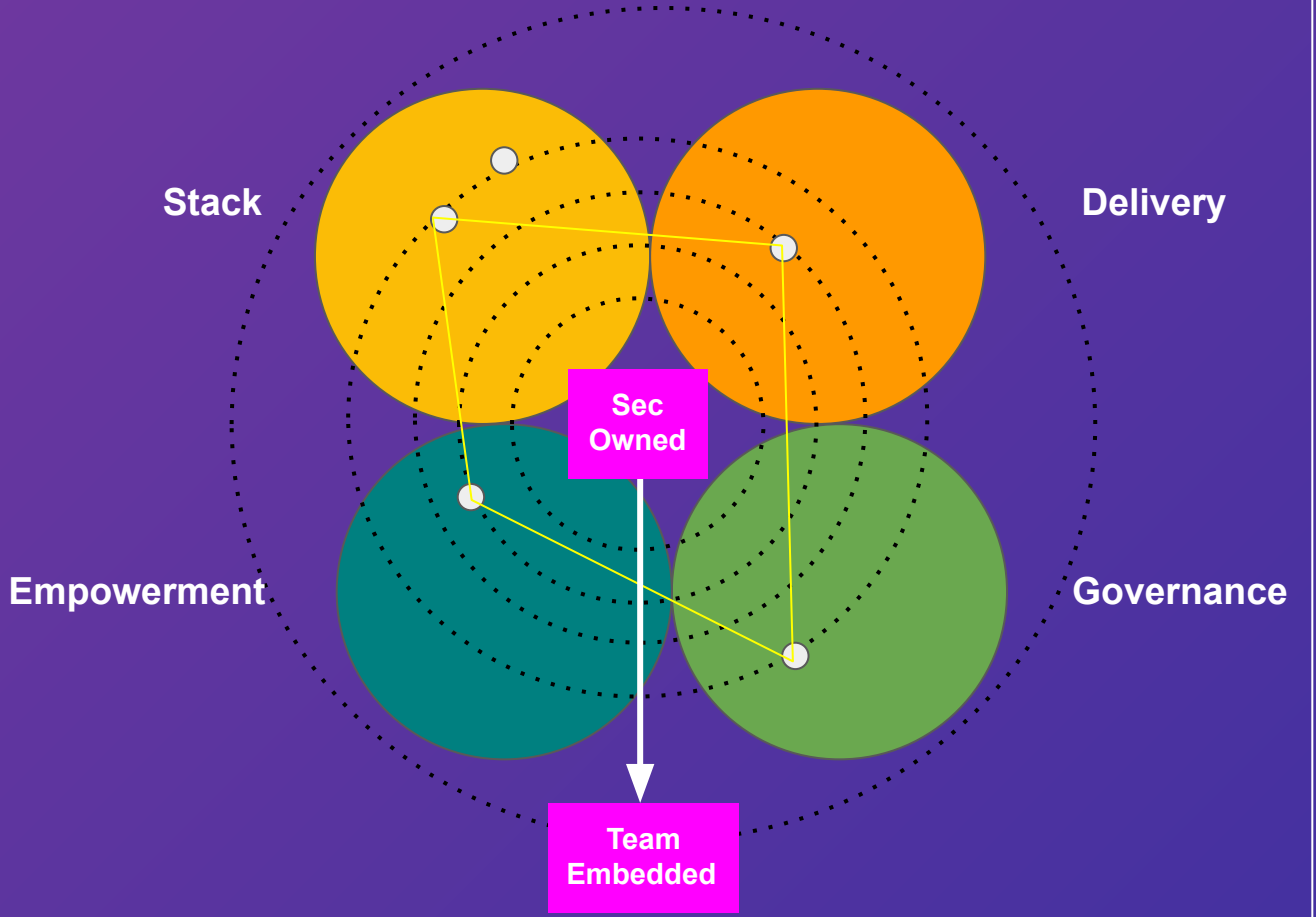


As a developer we want to take ownership of the security of our application



https://itrevolution.com/agile-conversations/

DevSecOps Inspiration

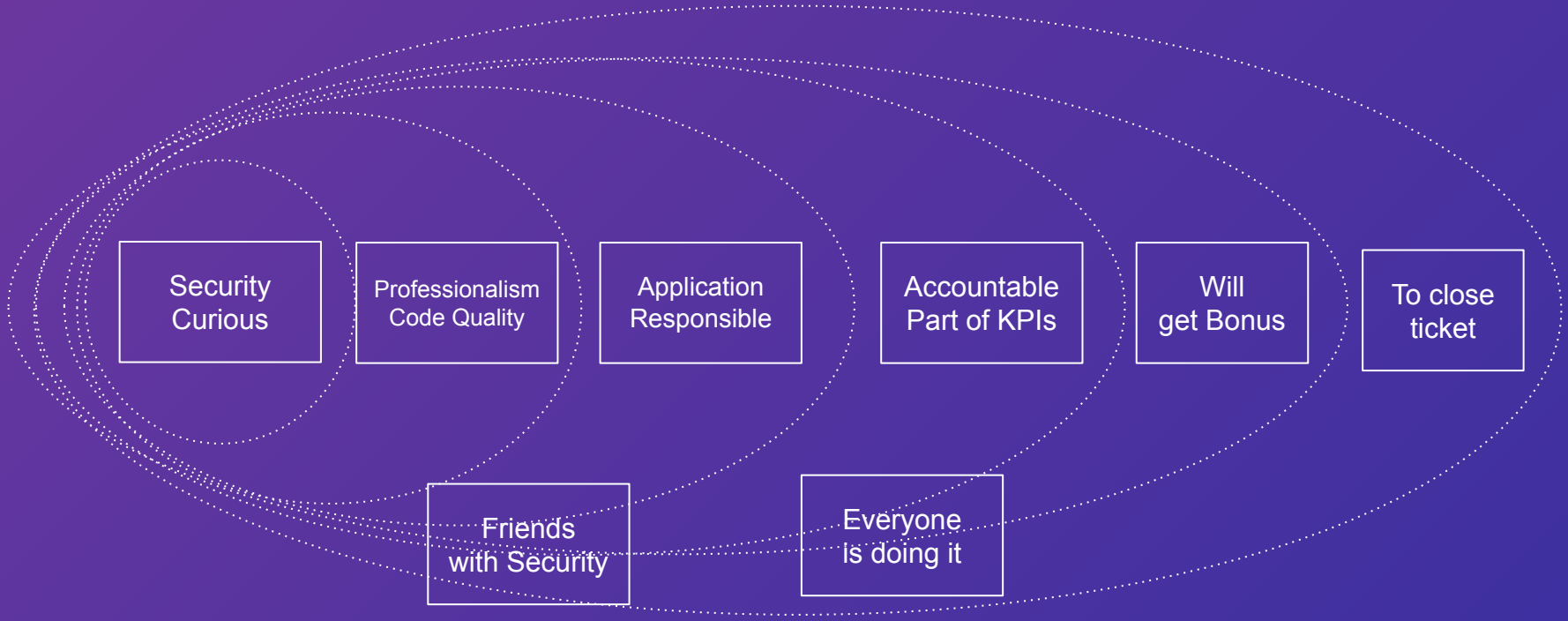


Level up each of the aspects gradually - they all influence the progress of the ownership handover

Developer Security Motivation

Inspiration is not enough

"It's good for business is rarely a personal motivation"

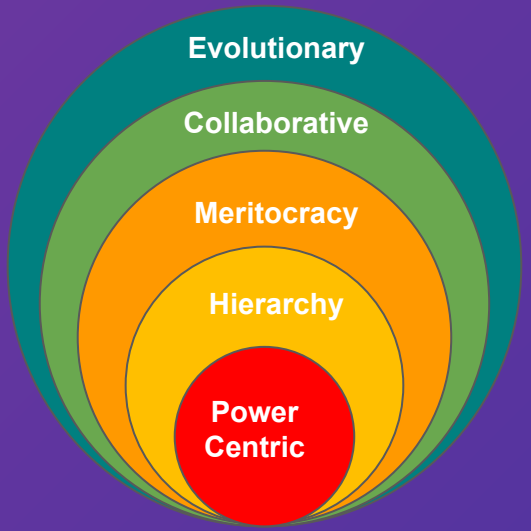


I want to (broad interest)

They want different things

I have to (narrow interest)

Paradoxes



Autonomy - Meaning

Empower - Customer Centric

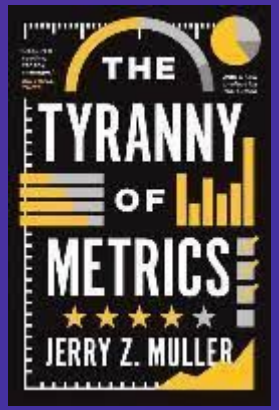
Measure - Scientific & KPIs

Automation - Order & Stability

Command & Control

You are never done

Each of these improvements will be countered by a paradox. You will need to keep investing.



https://www.amazon.com/Tyranny-Metrics-Jerry-Z-Muller/dp/0691174954

Tools & Culture

Patrick Debois – #thinktogether
Dev(sec)Ops: everything you do to overcome the friction created by silos ... All the rest is plain engineering

Love to hear your feedback!

patrick.debois@snyk.io
@patrickdebois

#ThinkingTogether