Xebia Security

Security & CI/CD

PVIB - 7 april 2021

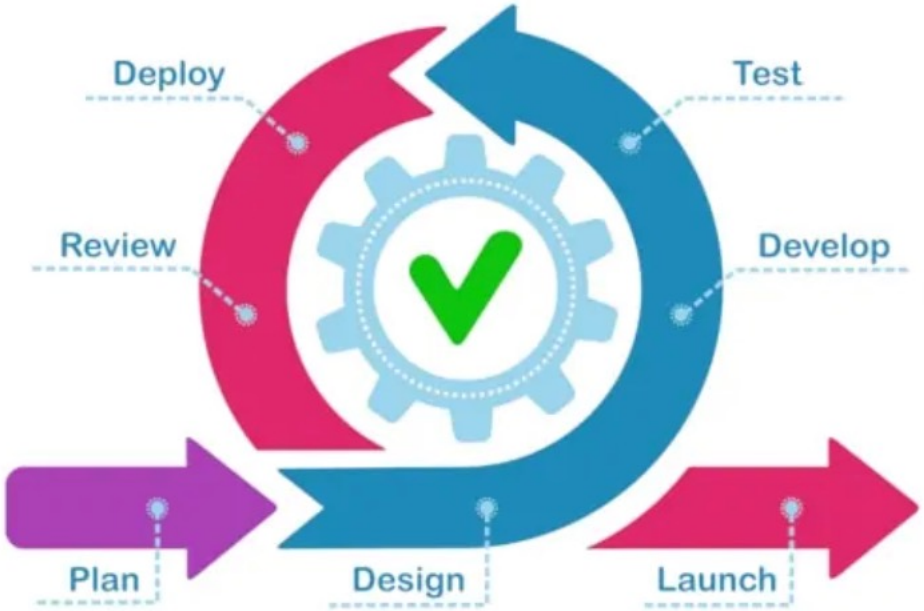
Xebia

- XEBIA SECURITY
- SECURITY TRANSFORMATIES
- AGILE SECURITY
- PEOPLE & PROCESS

Xebia Security

Terug in de tijd…

- In 2001: Agile Manifesto voor software ontwikkeling
- Agile is een reeks principes voor het ontwikkelen van betere software.
- Kenmerken: werkende software, vermogen om snel aan te passen, kort cyclisch, development teams en business werken samen
- Toepassingen: Scrum, Kanban, XP, Lean software developement



Xebia Security

Agile Manifesto

Mensen en hun onderlinge interactie boven processen en tools

Werkende software boven allesomvattende documentatie

Samenwerking met de klant boven contractonderhandelingen

Inspelen op verandering boven het volgen van een plan

Xebia Security

Terug in de tijd…

- In 2009: Eerste DevOpsDays in België
- Cultuur verandering: DevOps is de samen-werking tussen **mensen**, **proces** en **technologie** om **continuous delivery** van **waarde** aan **klanten** te leveren.
- Principes:

  → Customer-centric action

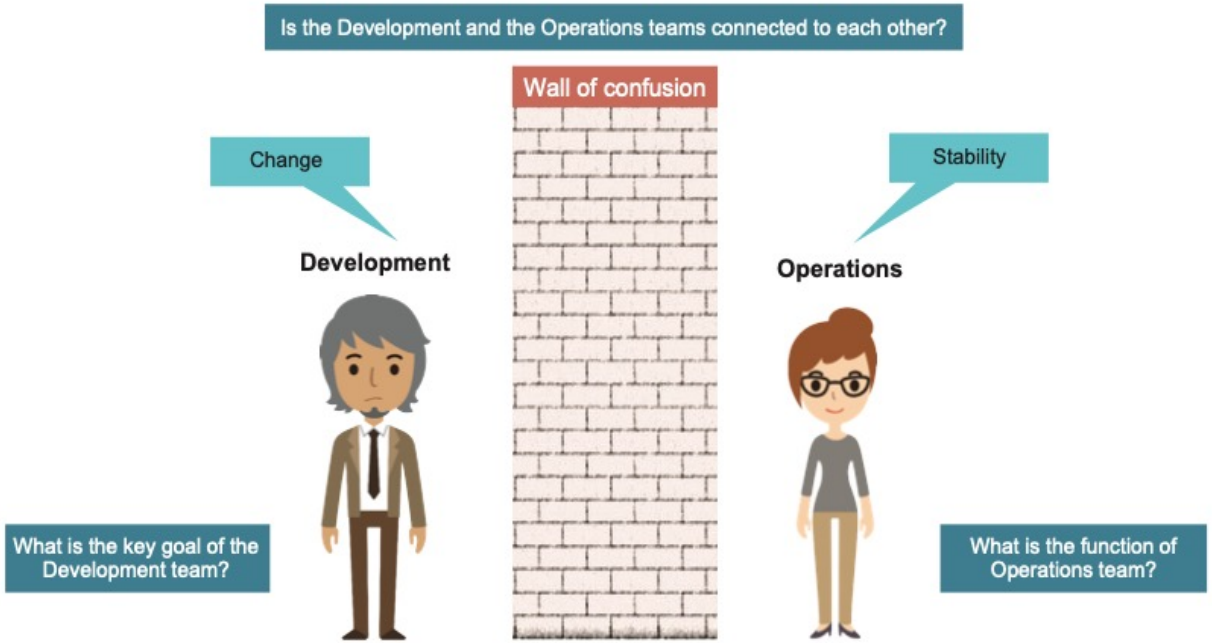
  → Create with the end in mind

  → End-to-end responsibility

  → Cross-functional autonomous team

  → Continuous improvement

  → Automate everything you can



Xebia Security

Business case voor DevOps

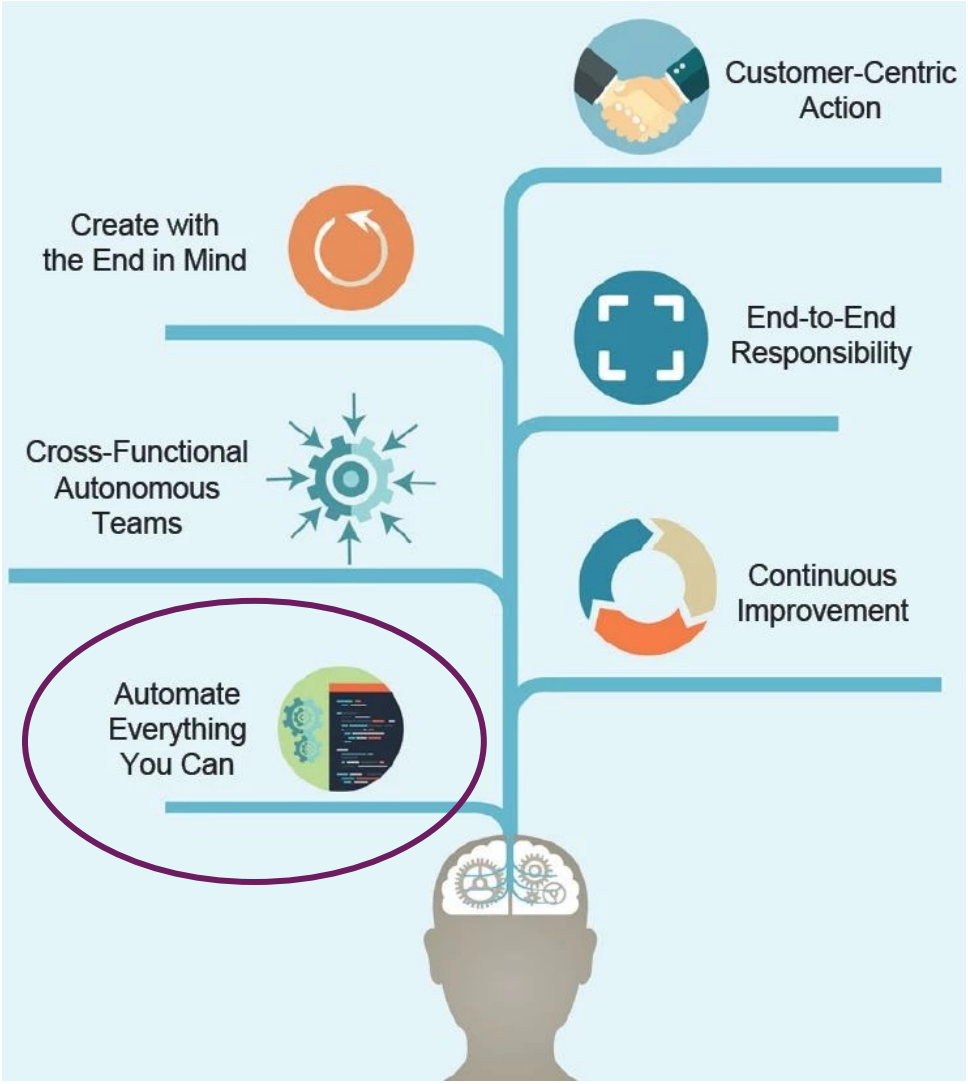
Key indicators for high-performing IT according to the State of DevOps report 2016 confirm the benefits:

1. Improved speed to market
2. Continuous Integration and delivery
3. Higher quality, fewer failures, and higher stability
4. Innovation and creativity
5. Increased employee engagement and job satisfaction
6. Breaking down silos and eliminating waste; It is all about collaboration!
7. Customer-centric action

Xebia Security

Automation

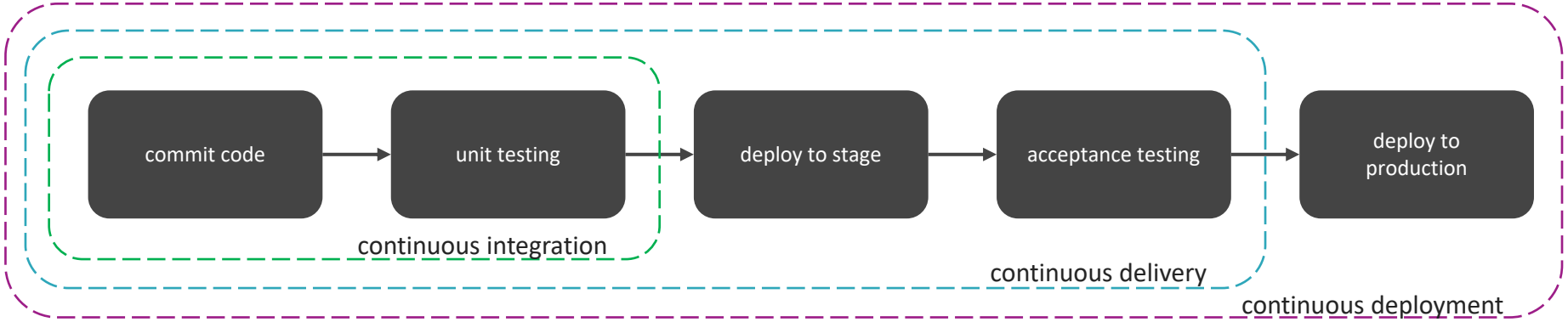
- Automatisering van **routine jobs**
- Automatisering delivery proces
- Platform standaardisatie: data center automatisering
- Everything as Code, Cloud, Containerization



Xebia Security

CI/CD

- Automatiseren van het build en release proces:
  - → Release frequency gaat omhoog
  - → Reduceert menselijk falen
  - → Verhoogt reproduceerbaarheid
- CI: Continuous Integration
- CD: Continuous Delivery of Continuous Deployment
- Fail fast, Early feedback



Xebia Security

FULLY AUTOMATED SOFTWARE DELIVERY PROCESS

Agile Organization

Deliver fast
Deliver often
Do the right things

Automated Build

Continuous Integration

Improve quality
Increase predictability

Automated Test

Improve reliability
Repeatable
Reduce cost
Increase speed

Automated Deployment

Release insight
Reduce release time
Reduce errors
Less downtime
Cost reduction

Automated Provisioning

Reduce costs
Increase speed
Reduce risk

✓ Architecture

Xebia Security

DevSecOps

- Het integreren van security practices in DevOps processen
- Shift left
- DevOps team is end-to-end verantwoordelijk voor een product, dus ook security

Xebia Security

Twee uitdagingen

#1 Beveiligen van de CI/CD pipeline

#2 Integreren van security in de CI/CD pipeline

Xebia Security

Uitdaging #1: Beveiligen van de CI/CD pipeline

Xebia Security

Waar moeten we rekening mee houden?

	Found	Signature Name	Matches	File	★
	8:21:19 AM	Log file	–	/alogger/tests/examples/sge.log	2
	8:19:51 AM	SSH Password	[redacted]	/test/Makefile	-1
	8:15:20 AM	Log file	–	/debug.log	0

Xebia Security

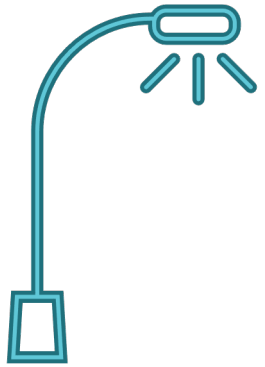
Oplossingen

- Bewustzijn belang van CI/CD pipeline binnen jouw organisatie
  Wat kan er misgaan? Hoe erg is dat en waarom?
- Inrichten controls, zoals
  - → Hardening
  - → Secret Management
  - → Access Controls
  - → Monitoring
- Zoek samenwerking op met development teams

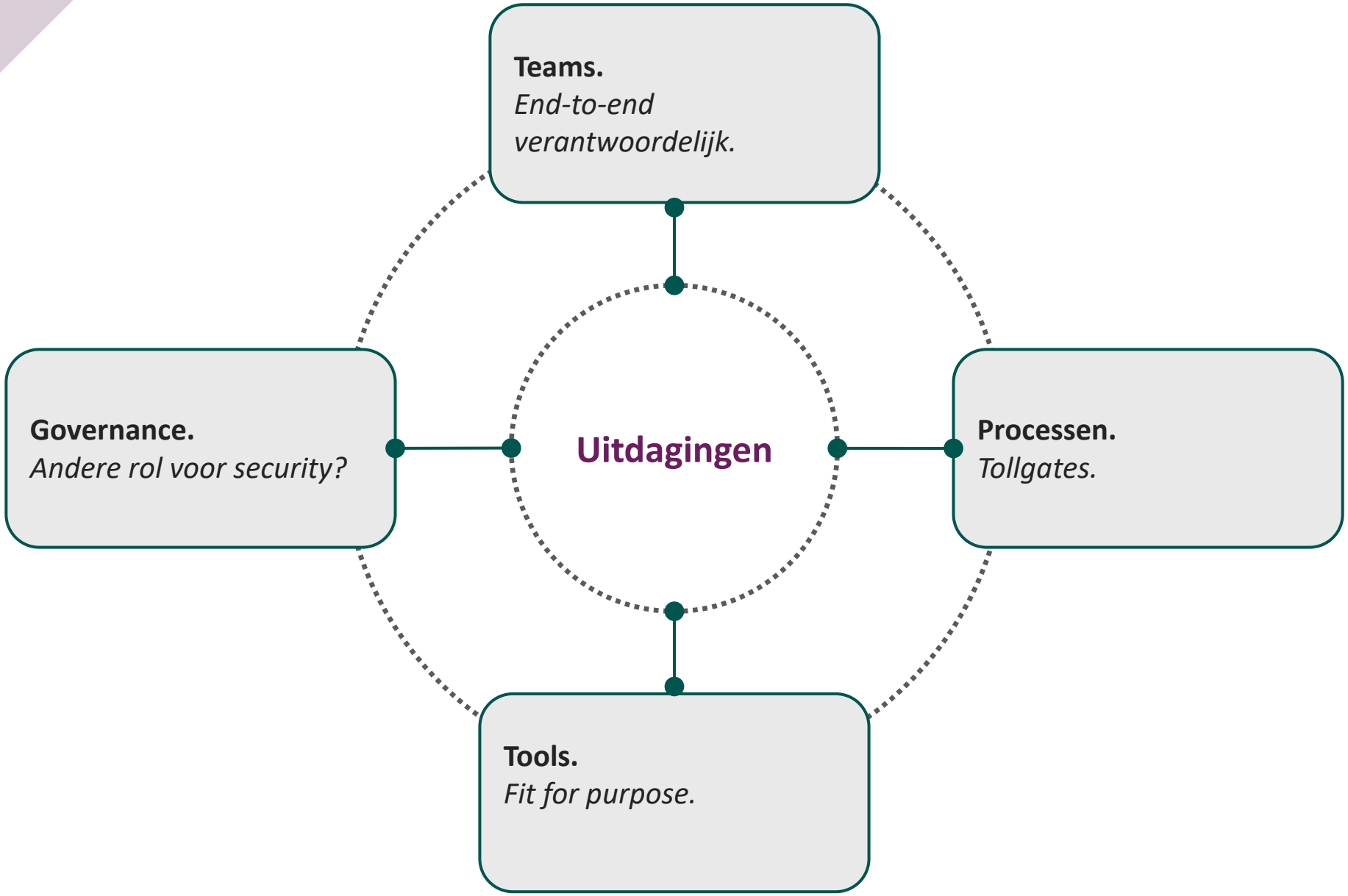
Xebia Security

Uitdaging #2: Integreren van security in de CI/CD pipeline

…eigenlijk is dit een kans…



Xebia Security



Xebia Security

Teams. *End-to-end verantwoordelijk*

- Verantwoordelijk voor een product gedurende de hele levensduur, inclusief kwaliteit, performance en security
- Help teams om die verantwoordelijkheid in te vullen
- Schep de juiste voorwaarden

Xebia Security

Processen. *Tollgates*

- Minimaliseer tollgates
- Shift left: test early, test often
- Automatiseer simpele processen
- Paralleliseer “langzame” processen

Xebia Security

Tools. *Fit for purpose*

development

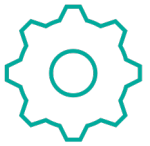
- ✓ Threat modelling
- ✓ **IDE security plug-ins**
- ✓ Secure coding
- ✓ Peer review

build (CI)

- ✓ **SAST**
- ✓ **Unit tests**
- ✓ **Dependency checks**
- ✓ **Container verificatie**

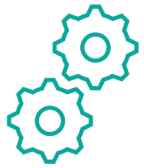
acceptance (CD)

- ✓ **In-depth SAST**
- ✓ **DAST**
- ✓ **Integration tests**
- ✓ **IaC verificatie**



production

- ✓ In-depth DAST
- ✓ Pentesten

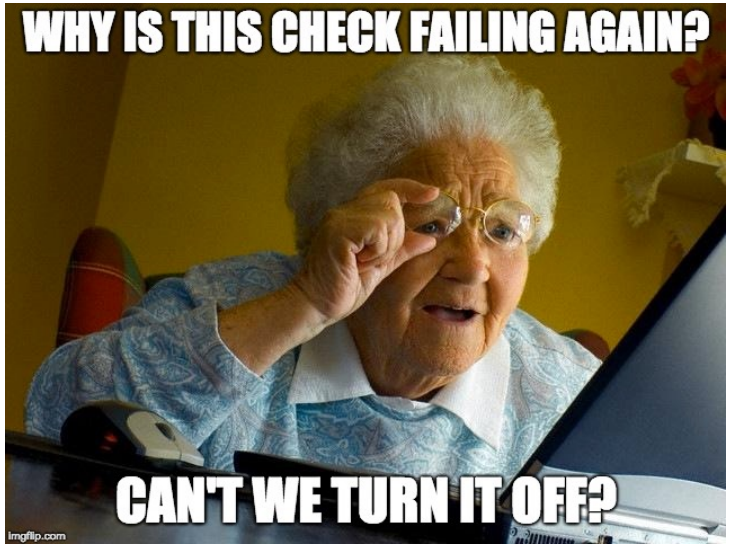


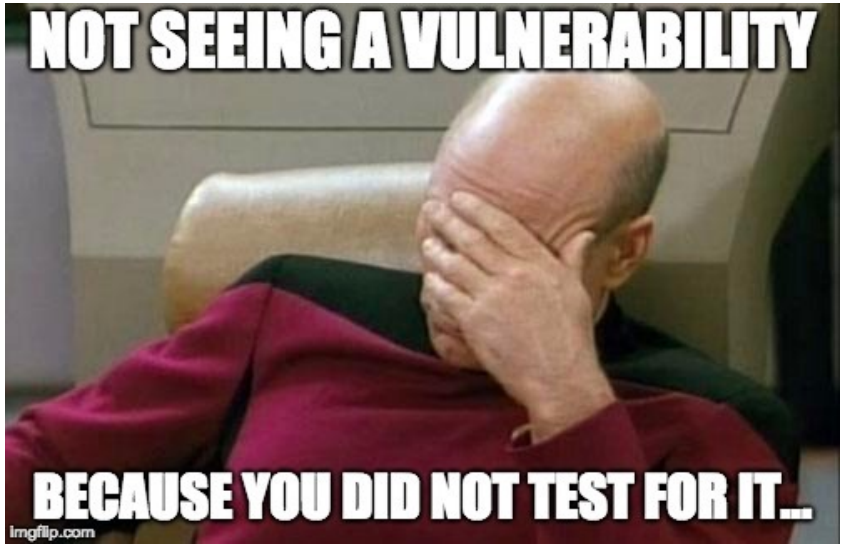
operations

- ✓ Monitoring
- ✓ Threat Intel
- ✓ Pentesten
- ✓ Postmortems

Xebia Security

Complexiteit





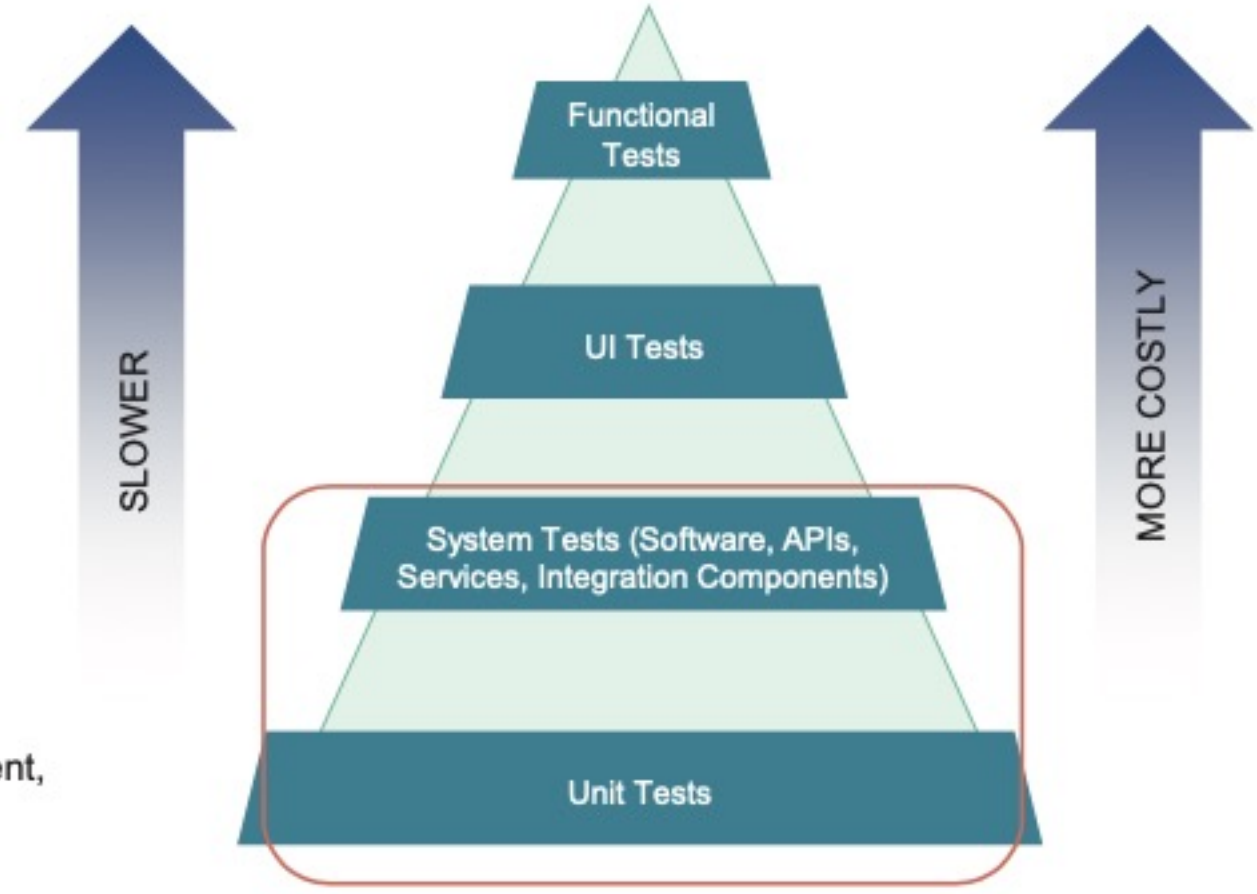
Xebia Security

End-to-End or Functional Tests:
Very slow, inconsequent feedback, costly, late feedback

User Interface (UI) Tests:
Slow, tested after deployment, more tedious, late feedback

System Tests:
Fast, tested after deployment, immediate feedback

Unit Tests:
Quick, tested even before deployment, immediate feedback, “the detail”



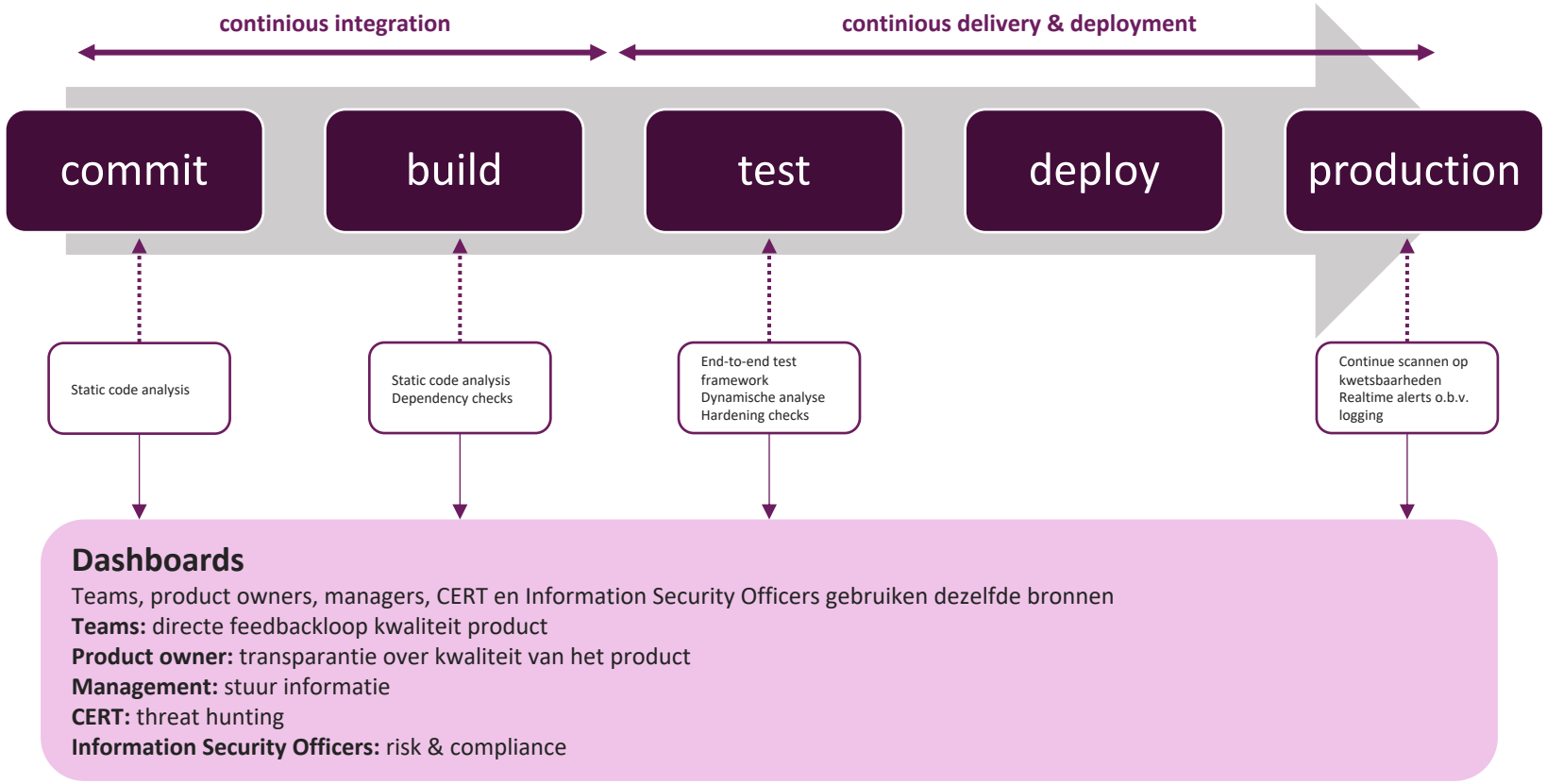
Xebia Security

Begin simpel en experimenteer

- ★ Analyseer: waar zitten de meeste problemen
- ★ Definieer patronen samen met de teams
- ★ Introduceer tools stap voor stap
- ★ Start met OSS
- ★ Start handmatig. Ga pas automatiseren als de output duidelijk is
- ★ Dubbelingen? Ga aan de slag met een vulnerability manager
- ★ Zet threat models en pentests in om:
  1. te vinden wat de scan tools niet zien
  2. de pipeline te optimaliseren: verdere automatisering en custom checks

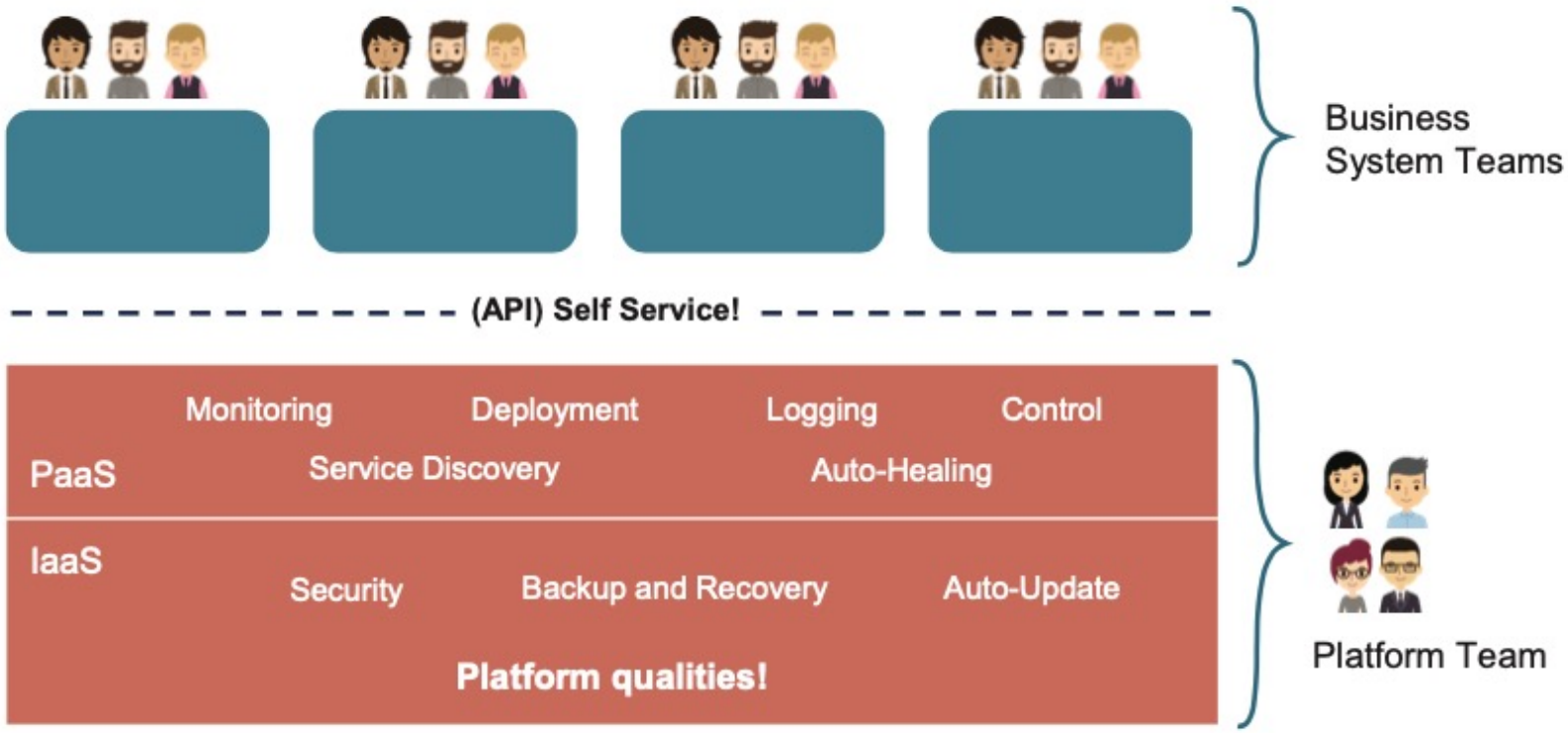
Xebia Security

CI/CD en dashboards



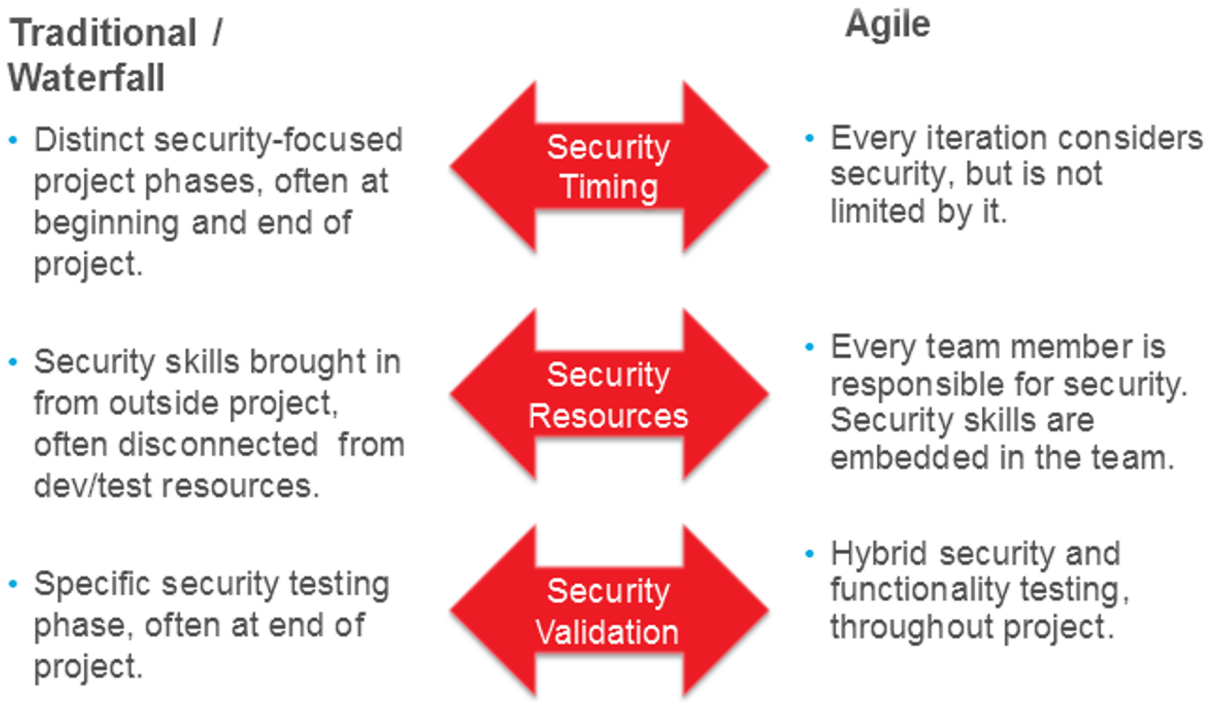
Xebia Security

Security as a Service



Xebia Security

Governance. *Een nieuwe rol voor security*



Xebia Security

Security Manifest

Leaning in over Always Saying “No”

Data & Security Science over Fear, Uncertainty and Doubt

Open Contribution & Collaboration over Security-Only Requirements

Consumable Security Services with APIs over Mandated Security Controls

Business Driven Security Scores over Rubber Stamp Security

Team Based Exploit Testing over Relying on Scans & Theoretical Vulnerabilities

Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

Compliance Operations over Clipboards & Checklists

Bron: https://www.devsecops.org/

Xebia Security

Contact

Anne-Sophie Teunissen
Security Transformation Consultant

Xebia Security BV
Laapersveld 27
1213VB Hilversum
e: ateunissen@xebia.com