Agile Application Security

centrum informatiebeveiliging
en privacybescherming

Introduction - David Vaartjes

Now:

- Securify B.V. — Proactive Application Security

  Code reviews | Security Testing | Agile Security | Design Security

Before:

- 2 jaar software security @ Rabobank (IB teams web & mobile)
- 8 jaar software security @ finance, insurance, gov, retail, ..

5 important rules in Agile Security.

1. Fit security into your dev process, not the other way around.
2. If security isn't on the team's board, it wont get done.
3. Involve a software security specialist. (just like UX, performance, etc.)
4. Only test/verify when needed. Know your risks/mitigations up front.
5. Agile Security != Automated security testing.

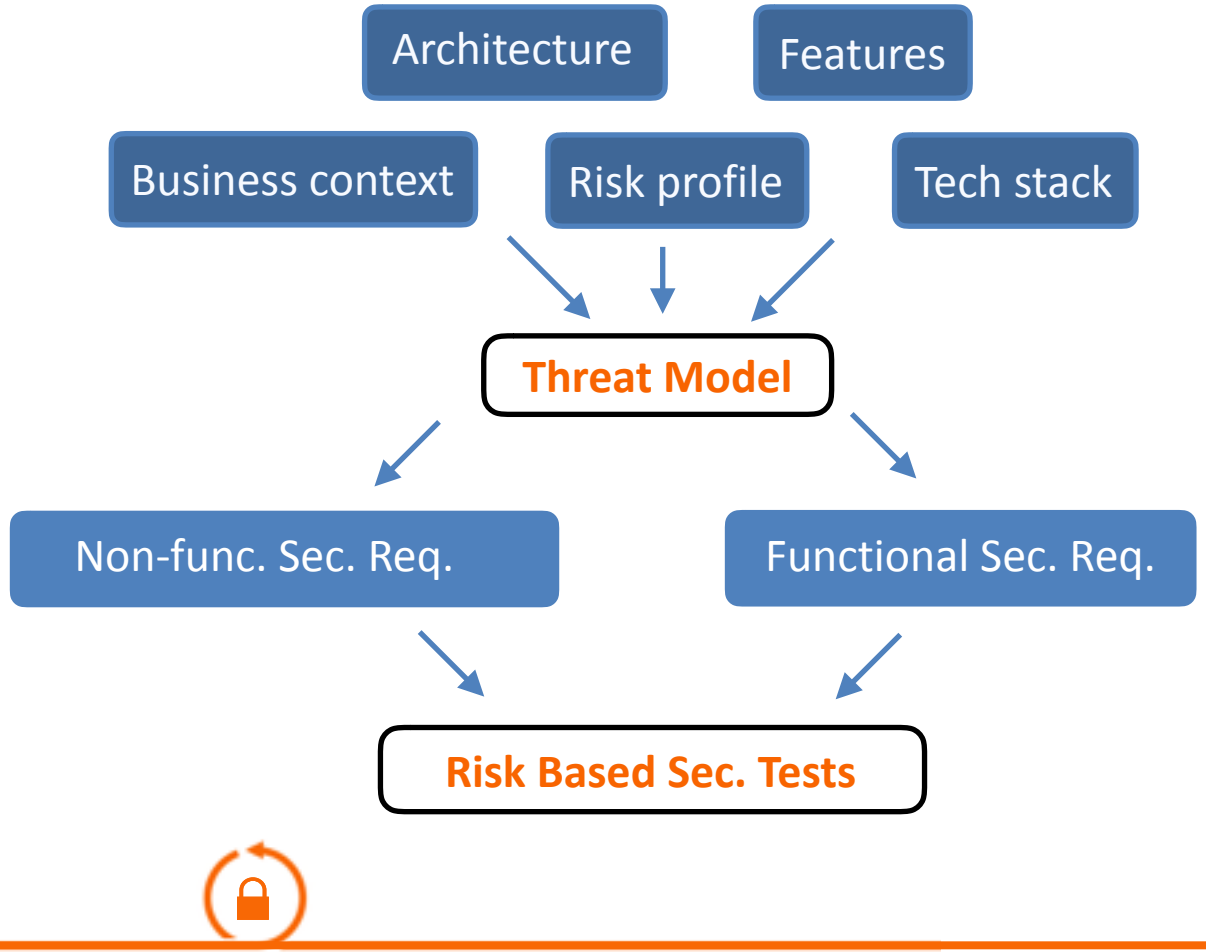
Lets make it 6.

- WF,
- Agile,
- DevOps,
- DecDevOps,
- SuperSecFastDevOps,
- AwesomeSuperDevSecOpsDepMainPartey…

Lets make it 6.

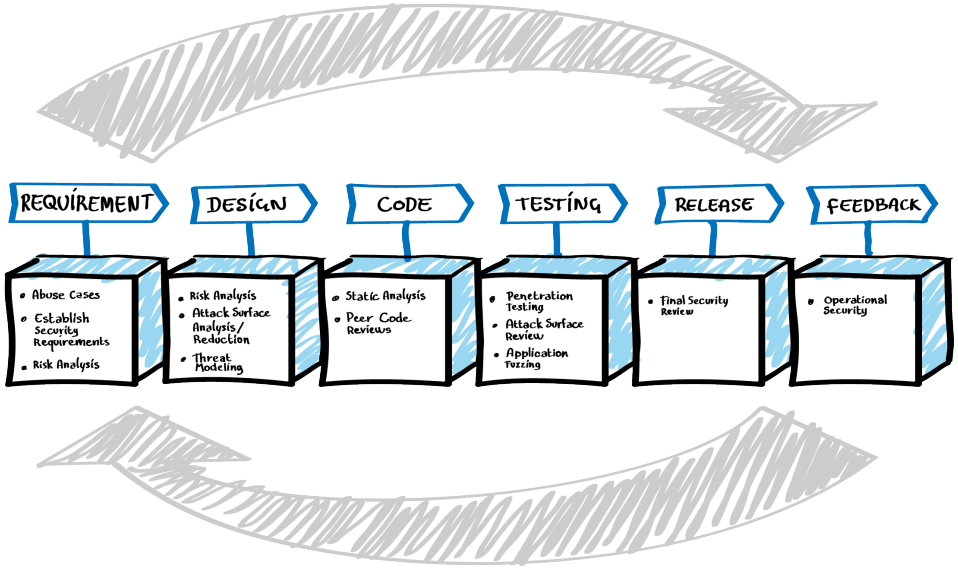
We still need to do this!

Where SSD can help you!

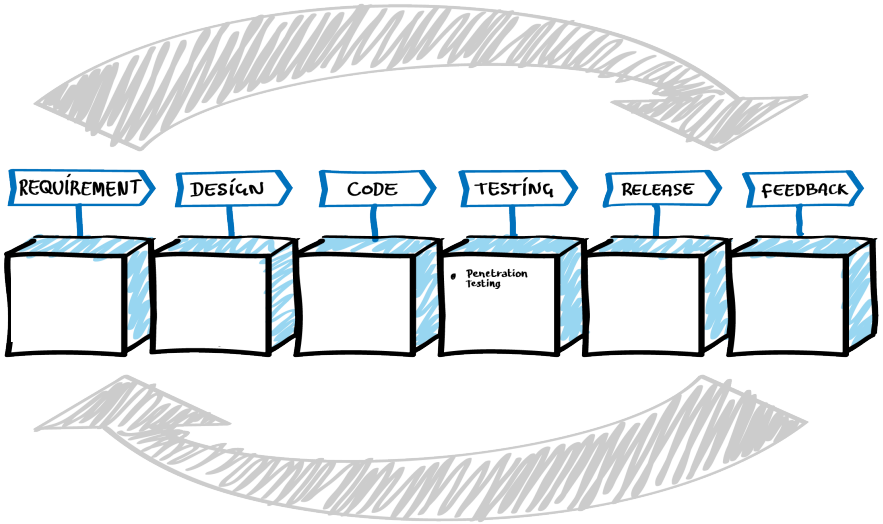


The software security dream

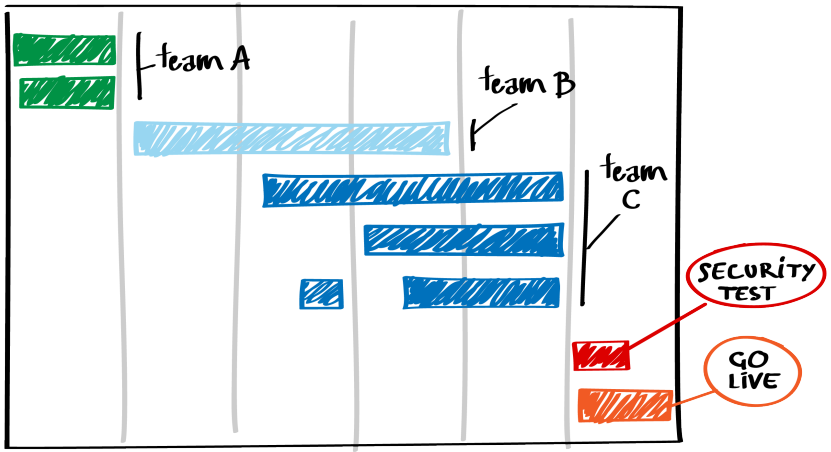
Software security dream



What we still do this a lot

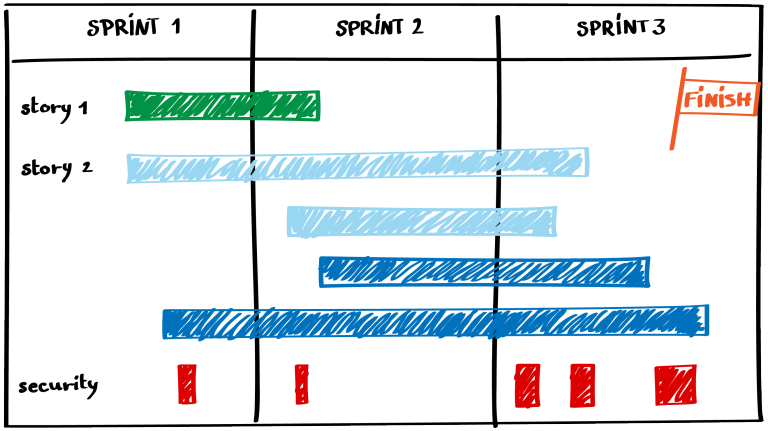


Old fashion security



Security focuses too much on testing and remains out of the dev. process.

Agile security (little, early, often)



But should be an integrated part of the ongoing dev and testing of code.

Security needs to change

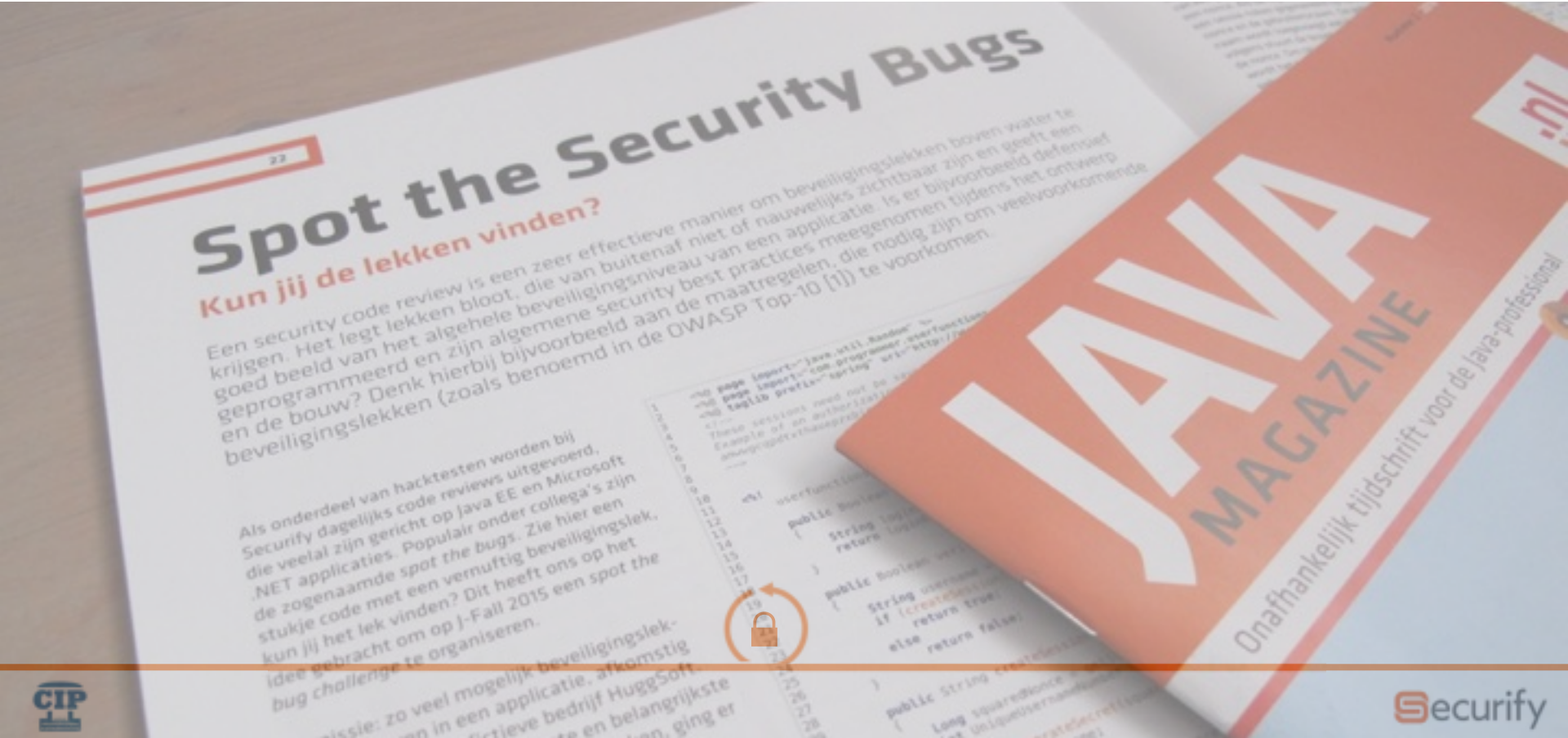
Security must change to fit the current development process!

Security, leave your comfort zone!

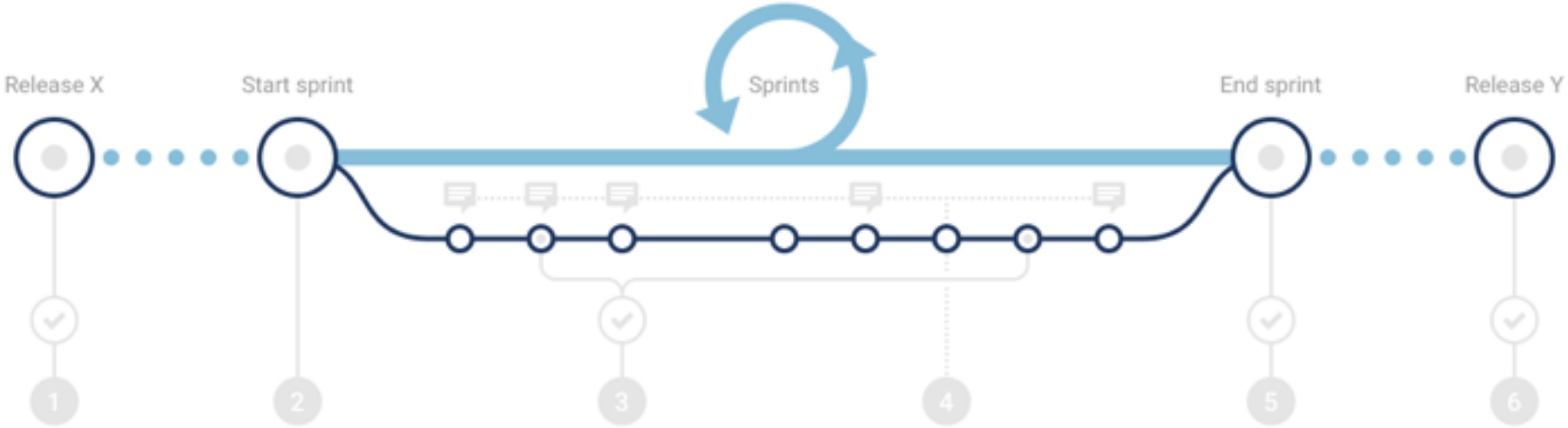
Don’t throw reports, but interface with the team and their tools!

Focus on code instead of pentesting.

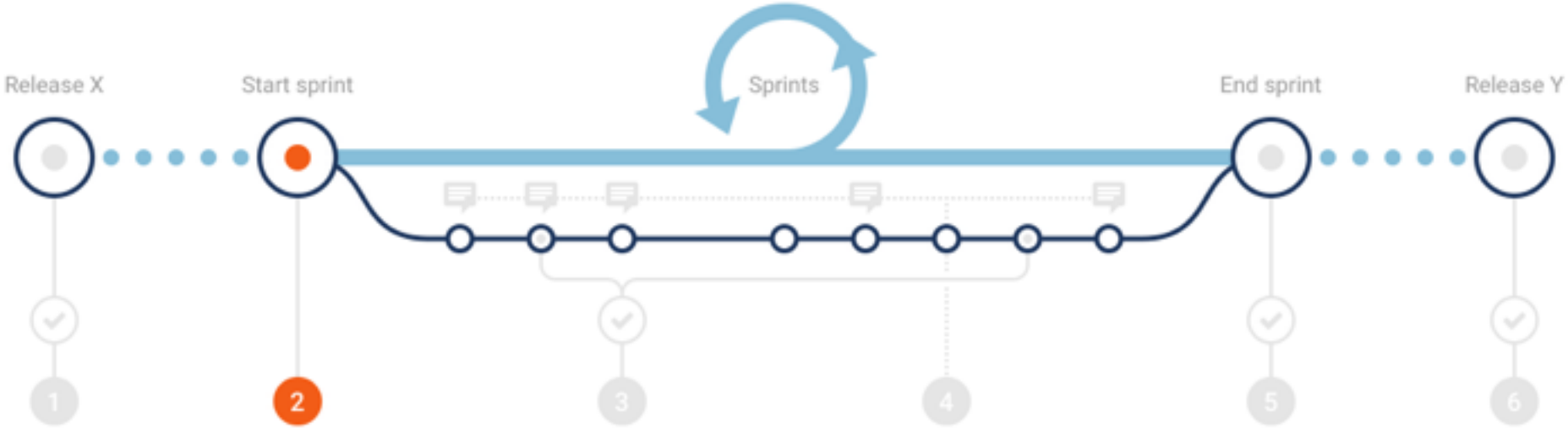
At least 10 high-risk security flaws/bugs in this code!



Ok nice, but what to do when?

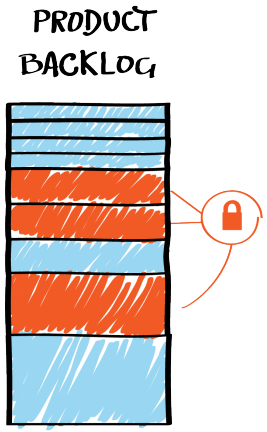


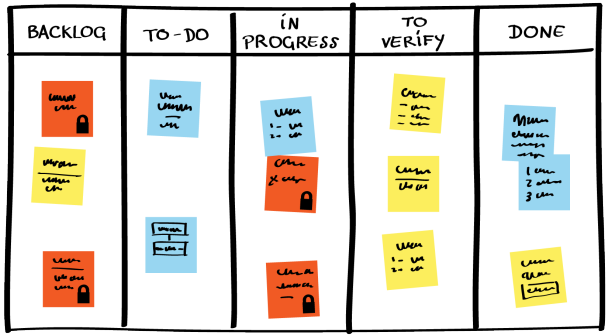
Security Grooming / Requirements



Security Grooming / Requirements

Where SSD
can help you!



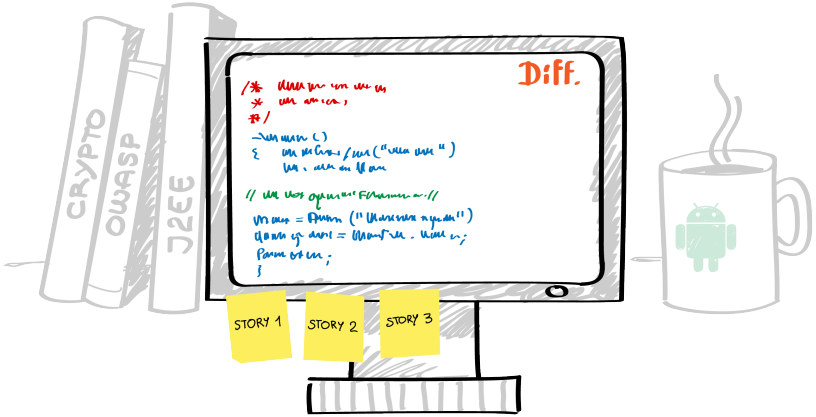


Involve a security specialist when filling and prioritising your backlog.

Early - Story/commit reviews

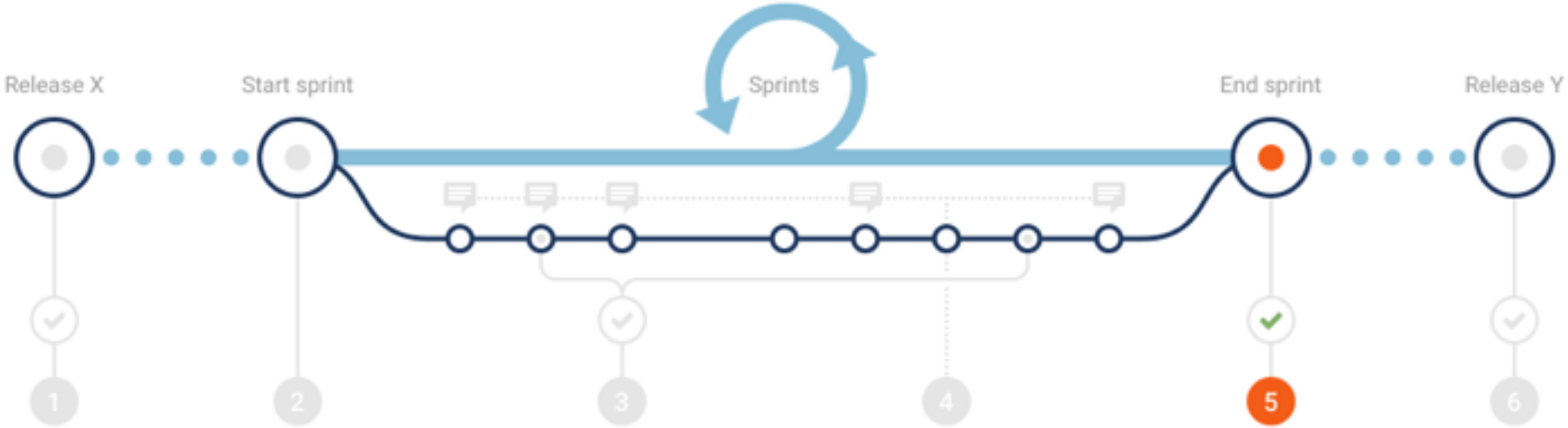
```
    PublicKey puk = TorCrypto.asn1GetPrivateKeyPublic(privkey);
    return generateHSDescriptor((RSAPublicKey) puk, pk);
}


public static String generateHSDescriptor(RSAPublicKey pk, RSAPrivateKey prk) throws IOExcep
    String serviceb32 = publicKeyToOnion(pk);

    StringBuilder desc = new StringBuilder();
    desc.append("rendezvous-service-descriptor "+new Base32().encodeAsString(getDescId(servi
    desc.append("version 2\n");
    desc.append("permanent-key\n-----BEGIN RSA PUBLIC KEY-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String(TorCrypto.publicKeyToASN1(pk))
    desc.append("\n-----END RSA PUBLIC KEY-----\n");
    desc.append("secret-id-part "+new Base32().encodeAsString(getSecretId(serviceb32, (byte
    DateFormat df = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss");
    desc.append("publication-time "+df.format(new Date())+"\n");
    desc.append("protocol-versions 2,3\n");
    desc.append("introduction-points\n" +
```

```
    String serviceb32 = publicKeyToOnion(pk);

    StringBuilder desc = new StringBuilder();
    desc.append("rendezvous-service-descriptor "+new Base32().encodeAs
    desc.append("version 2\n");
    desc.append("permanent-key\n-----BEGIN RSA PUBLIC KEY-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String(TorCrypt
    desc.append("\n-----END RSA PUBLIC KEY-----\n");
    desc.append("secret-id-part "+new Base32().encodeAsString(getSecre
    desc.append("introduction-points\n" +
            "-----BEGIN MESSAGE-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String("nothing
    desc.append("\n-----END MESSAGE-----\n" +
            "signature\n");

    byte sig[];
    try {
        Signature instance = Signature.getInstance("SHA1withRSA");
        instance.initSign(prk);
```

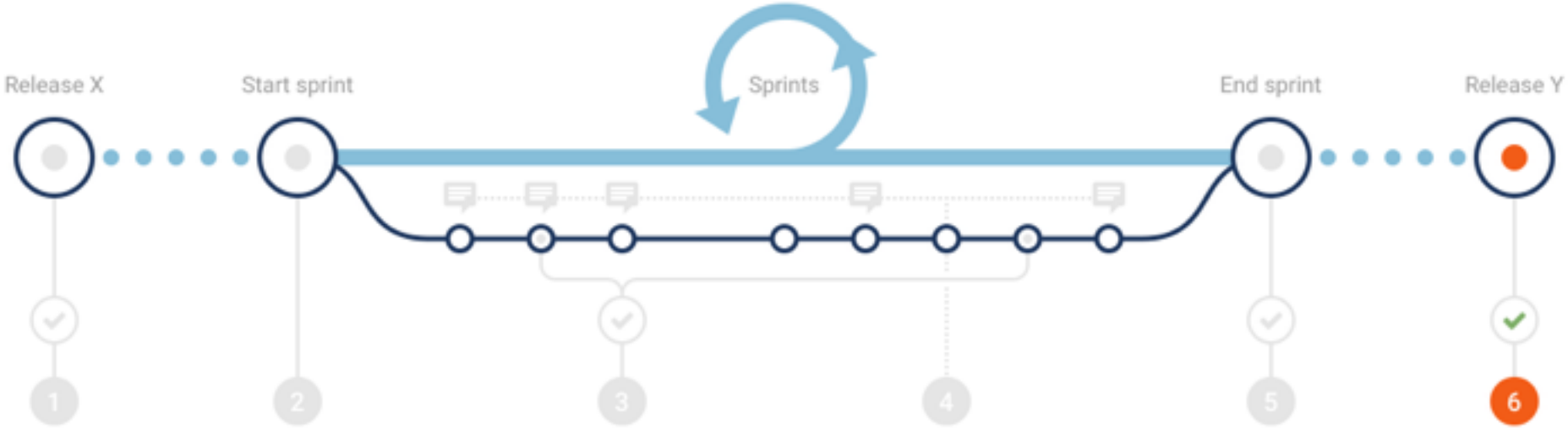


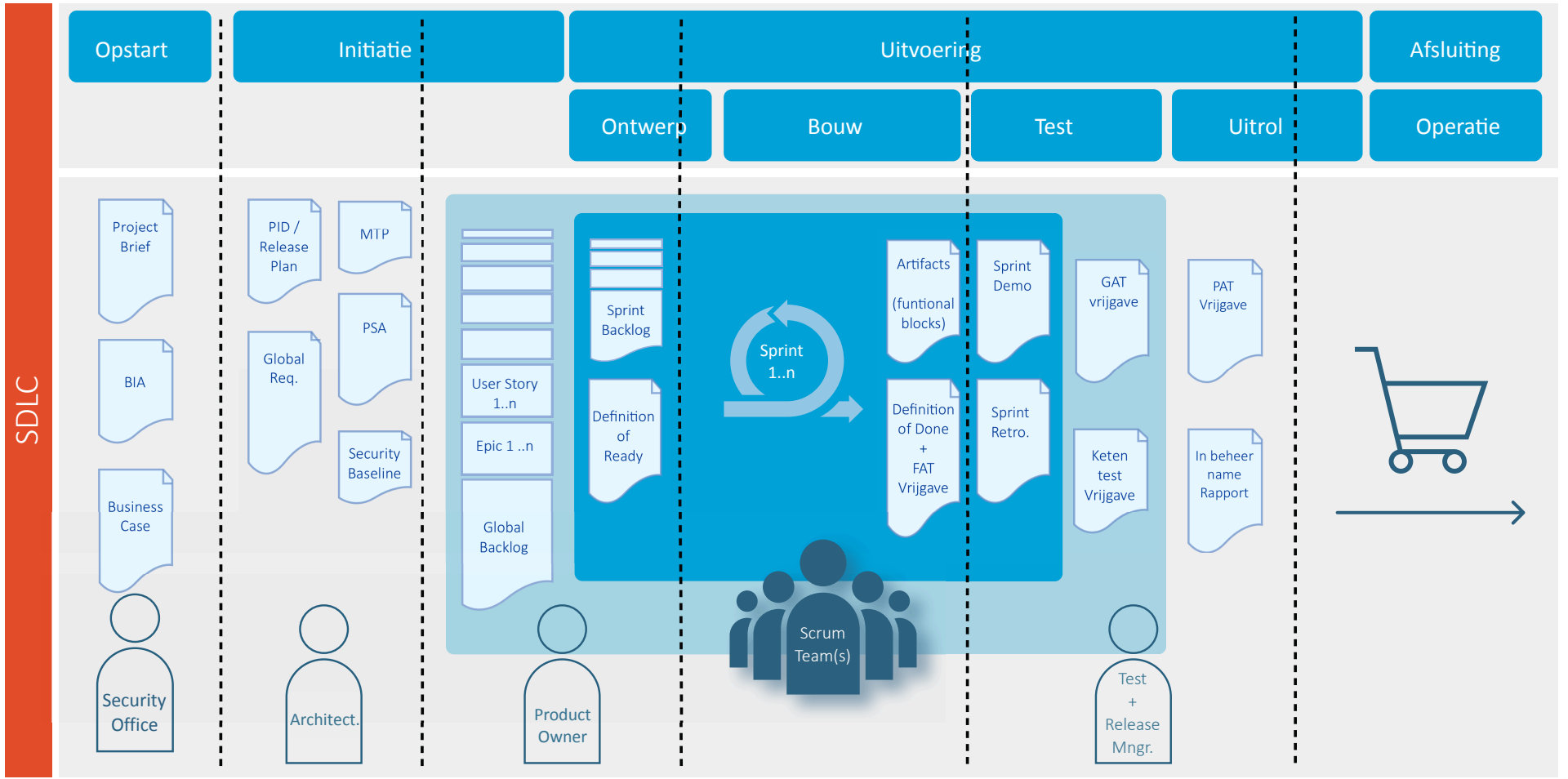
Support the team - be available - create awareness!

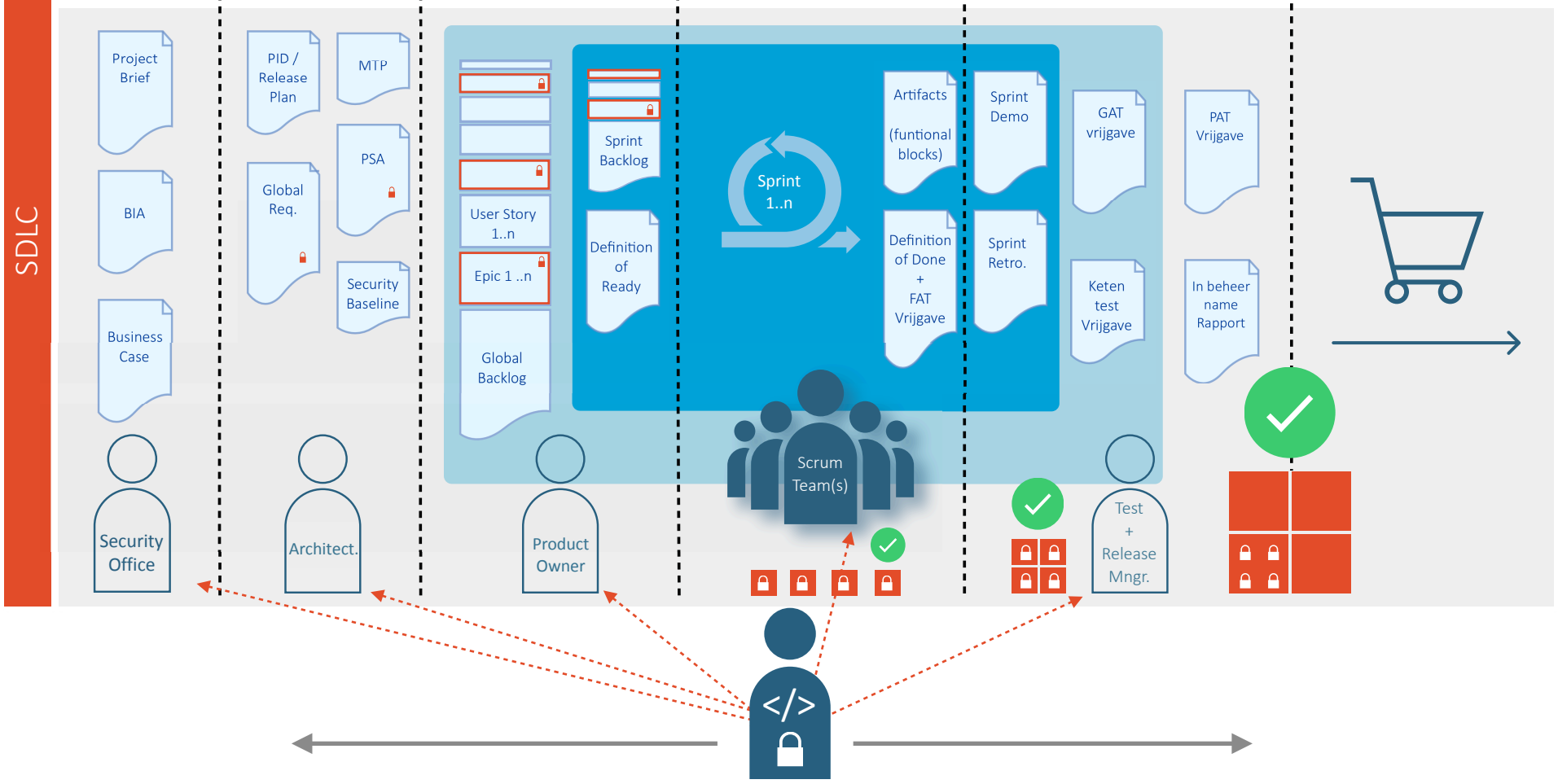
Sprint security sign-off (keep it simple!)



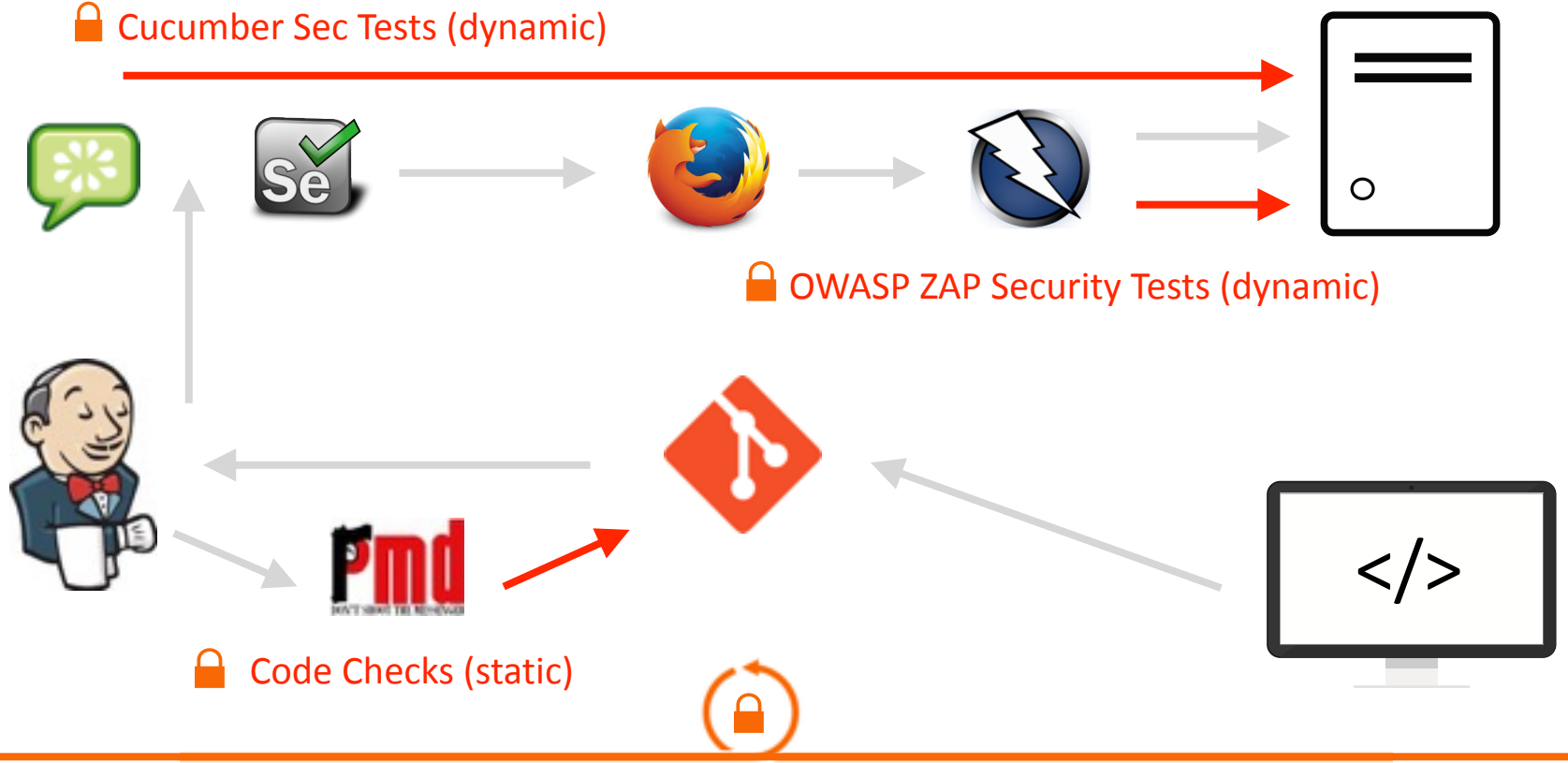
Sprint security sign-off (keep it simple!)



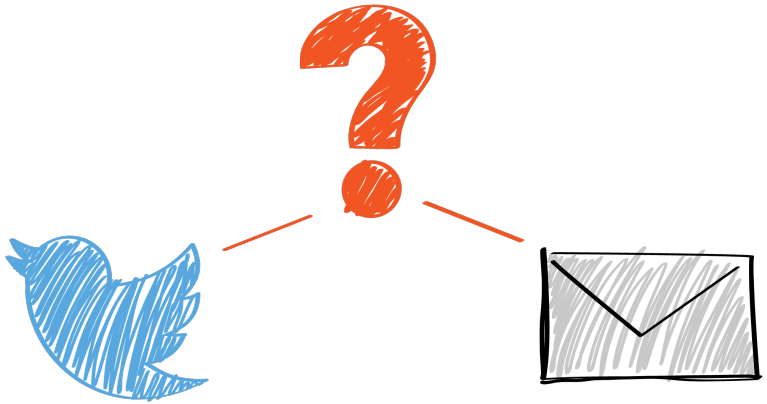

SDLC
Opstart
Initiatie
Uitvoering
Afsluiting
Ontwerp
Bouw
Test
Uitrol
Operatie
Project Brief
BIA
Business Case
Security Office
PID / Release Plan
Global Req.
MTP
PSA
Security Baseline
Architect.
User Story 1..n
Epic 1 ..n
Global Backlog
Product Owner
Sprint Backlog
Definition of Ready
Sprint 1..n
Artifacts (funtional blocks)
Definition of Done + FAT Vrijgave
Sprint Demo
Sprint Retro.
Scrum Team(s)
GAT vrijgave
Keten test Vrijgave
Test + Release Mngr.
PAT Vrijgave
In beheer name Rapport


SDLC
Project Brief
BIA
Business Case
PID / Release Plan
Global Req.
MTP
PSA
Security Baseline
User Story 1..n
Epic 1 ..n
Global Backlog
Sprint Backlog
Definition of Ready
Sprint 1..n
Artifacts (funtional blocks)
Definition of Done + FAT Vrijgave
Sprint Demo
Sprint Retro.
GAT vrijgave
Keten test Vrijgave
PAT Vrijgave
In beheer name Rapport
Security Office
Architect.
Product Owner
Scrum Team(s)
Test + Release Mngr.
</>

Security automation can support you (~20%)



Bedankt!



@securifybv

david.vaartjes@securify.nl