

Agile Security Testing

Lessons learned

David Vaartjes



OWASP AppSecEU 15
Amsterdam, The Netherlands

Agenda

1. Introduction
2. The software security dream
3. How it's done
4. From Waterfall to Agile security



About me

- Co-founder Securify (Software Security / Build Security In)
- 2 yrs software security @ Rabobank (internet banking teams)
- 8 yrs software security @ finance, insurance, gov, retail, ...



david.vaartjes@securify.nl / @securifybv

The software security dream

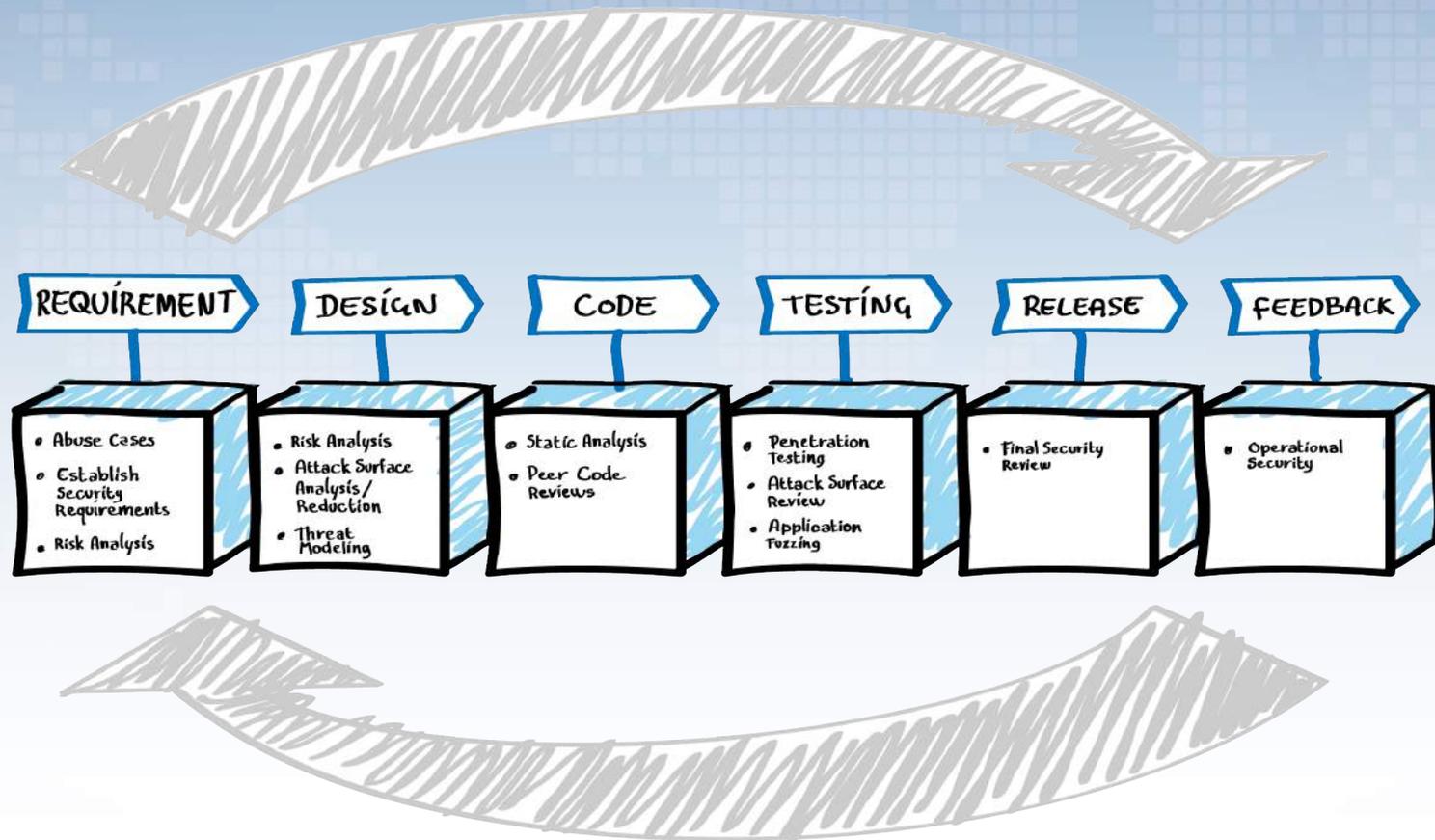


david.vaartjes@securify.nl / @securifybv

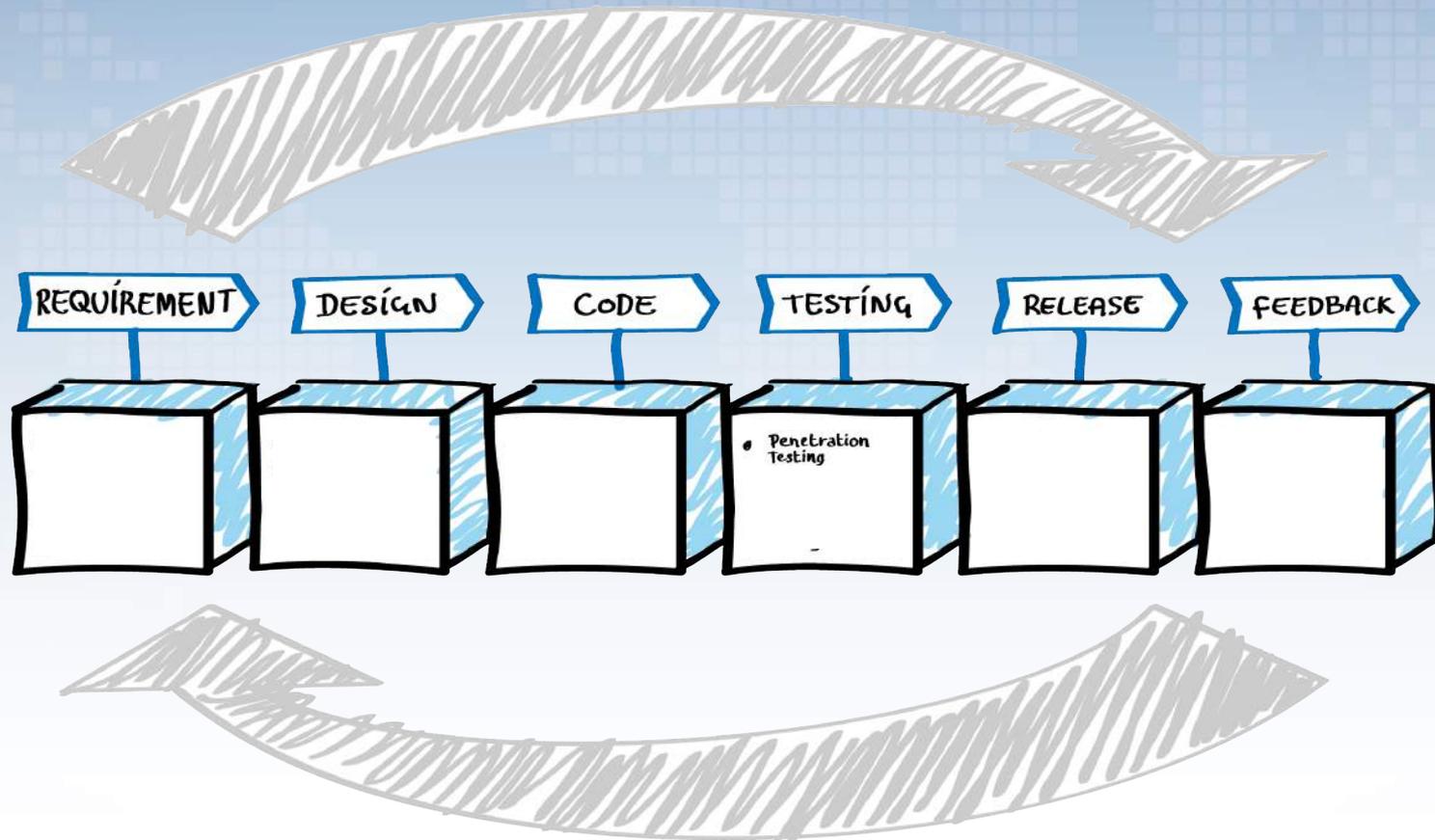


OWASP AppSecEU 15
Amsterdam, The Netherlands

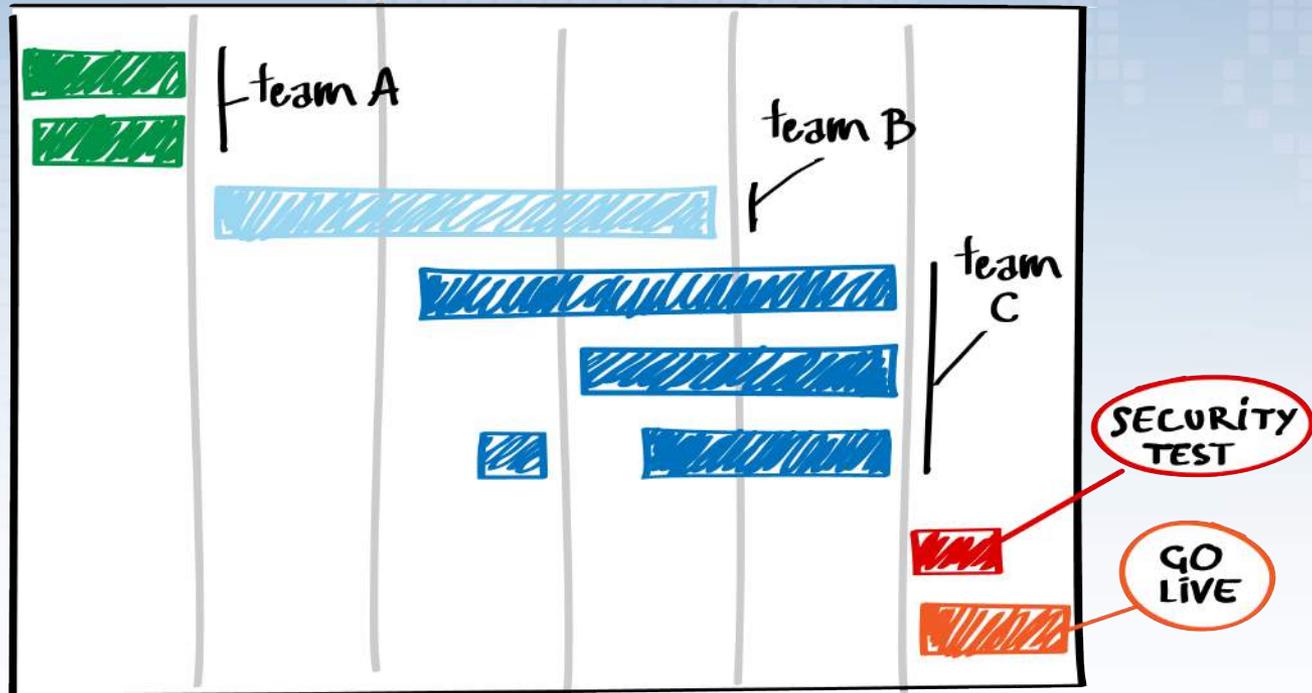
We know this



But still do a lot of this



But still do a lot of this



Meet the security end boss

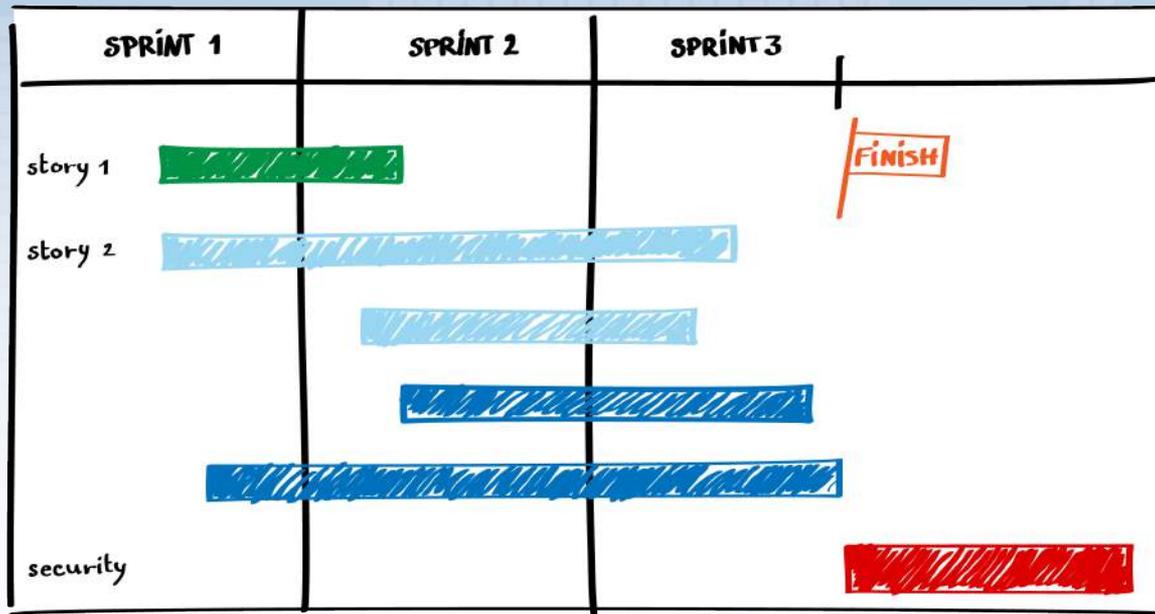


david.vaartjes@securify.nl / [@securifybv](https://twitter.com/securifybv)



OWASP AppSecEU 15
Amsterdam, The Netherlands

Security sticks to waterfall



Security can't catch up..



david.vaartjes@securify.nl / [@securifybv](https://twitter.com/securifybv)



OWASP AppSecEU 15
Amsterdam, The Netherlands

We need change

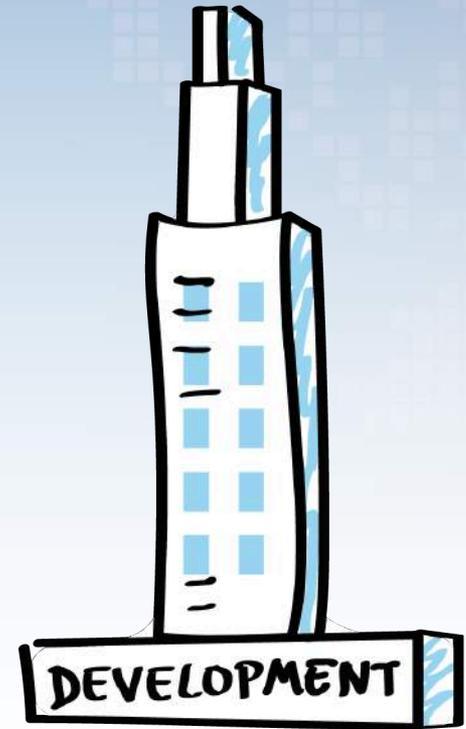
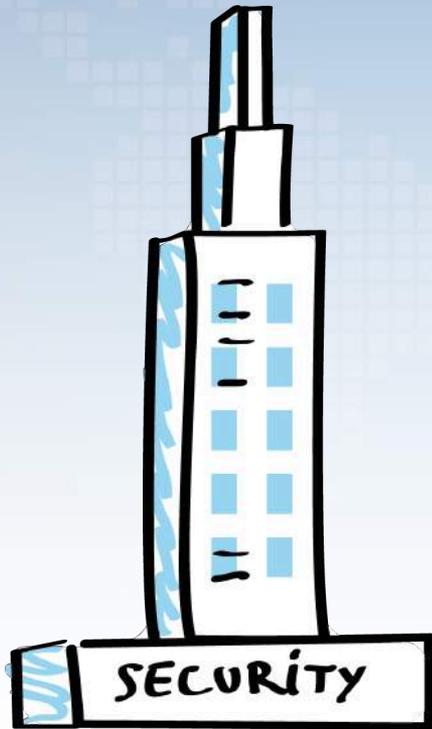


david.vaartjes@securify.nl / @securifybv



OWASP AppSecEU 15
Amsterdam, The Netherlands

Lets fix this together - pilot



Join meetings

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
stand-up (15 mn)	stand-up (15mn)	stand-up (15mn)	stand-up (15 mn)	stand-up (15mn)
grooming (2u)				

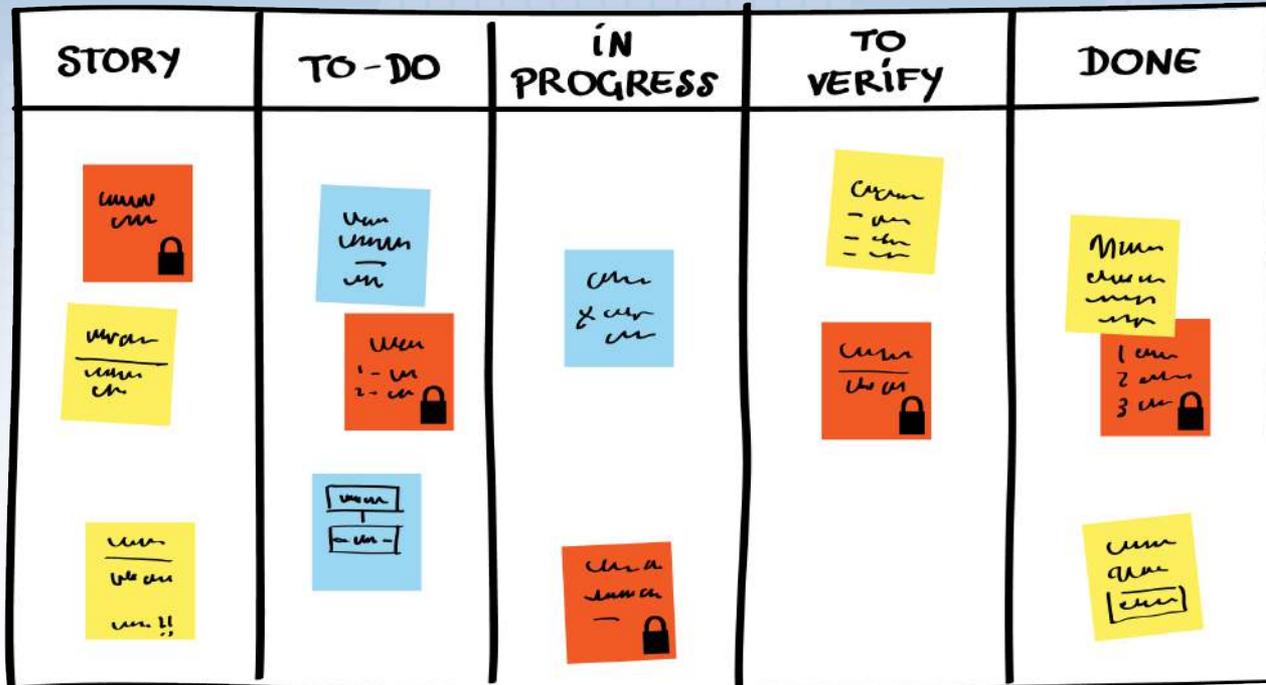
MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
stand-up (15mn)	stand-up (15mn)	stand up (15 mn)	stand-up (15 mn)	demo (1u)
grooming (2u)				retro (1u)



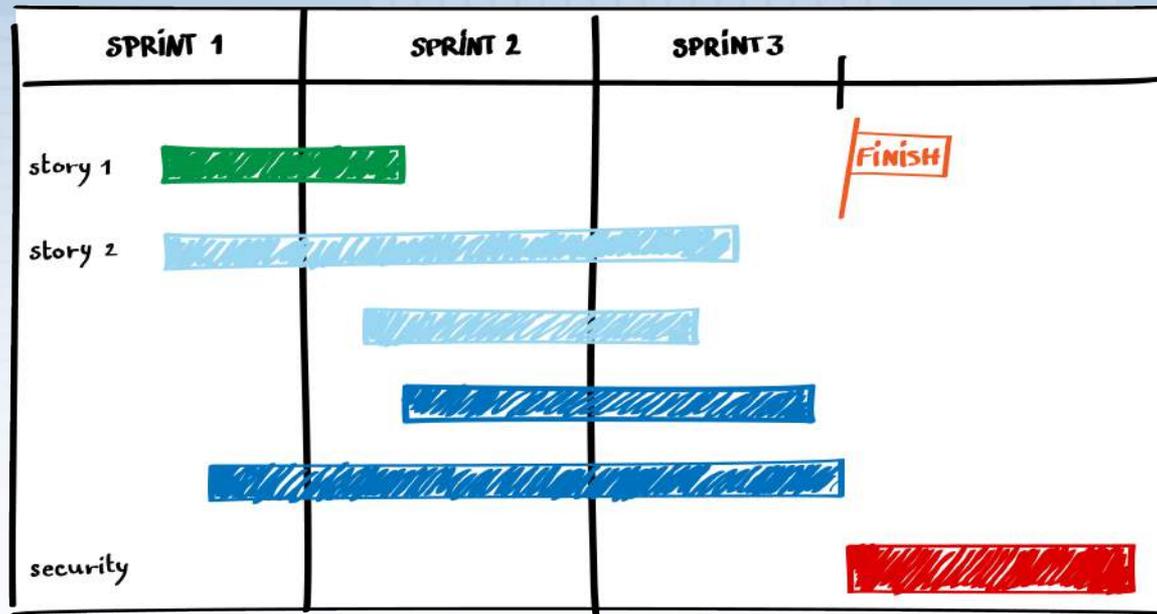
Grooming



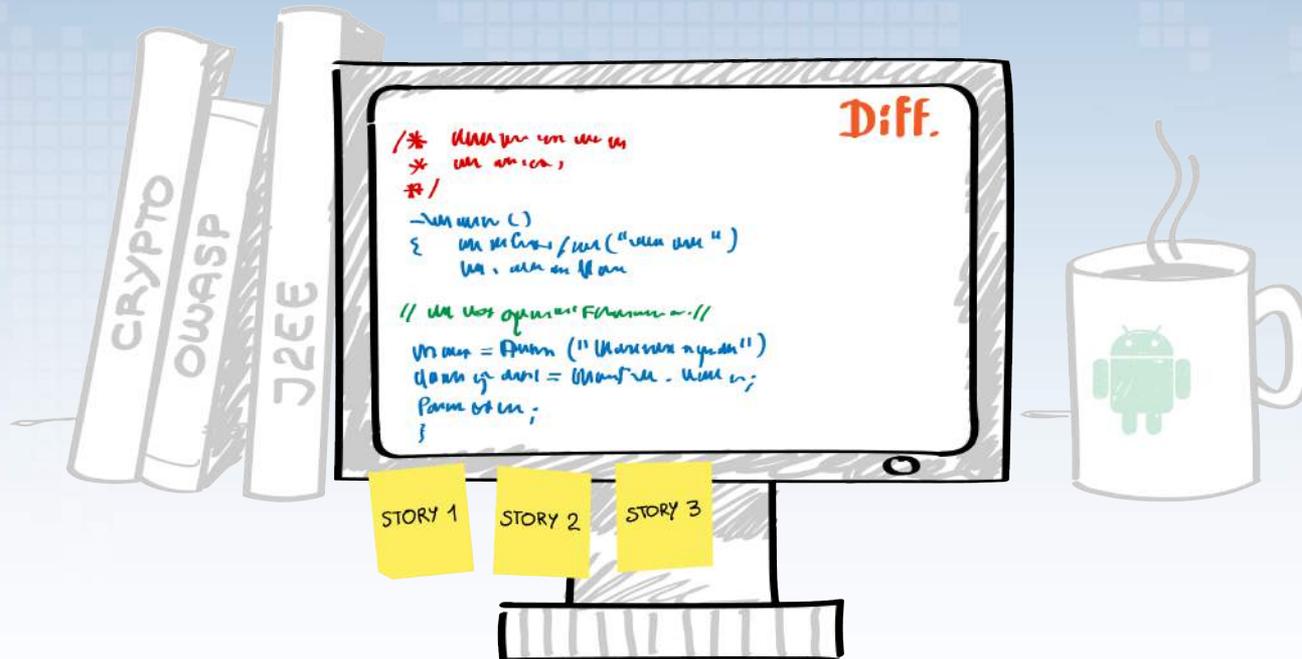
Tag user stories / risk based



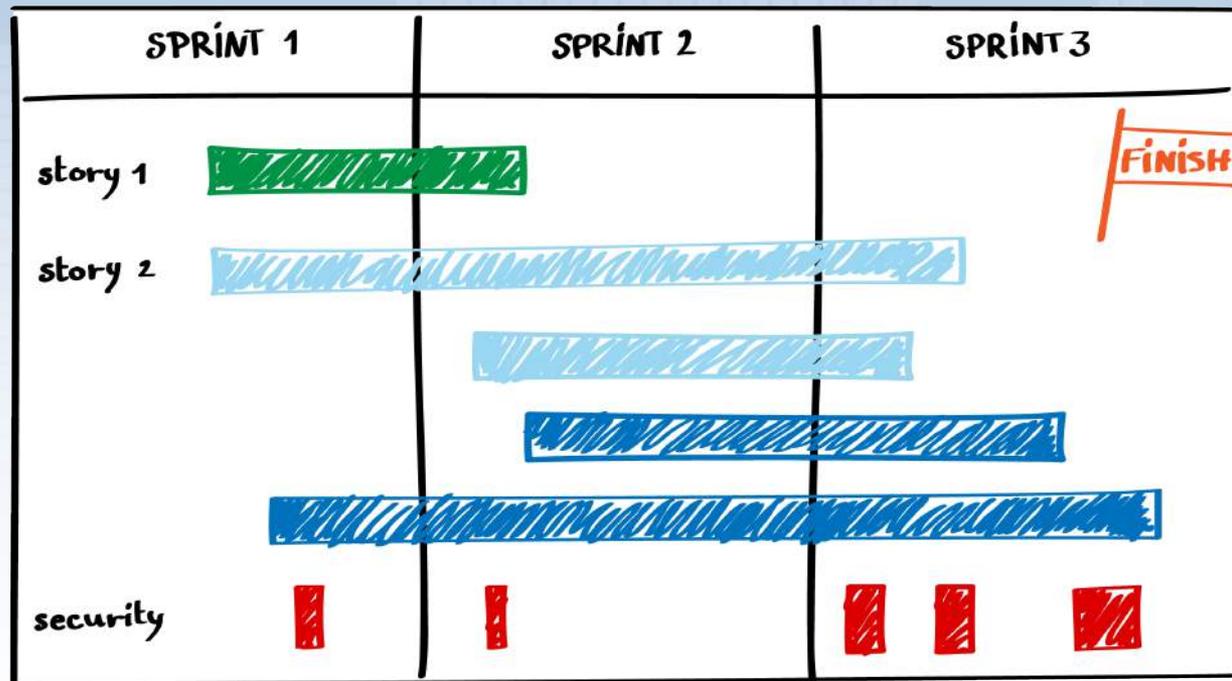
More efficient test/review



Next: early code reviews



Slicing up this end boss



Retro

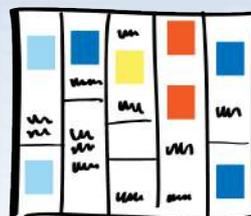


GOOD



80-90%

BAD



Better planning

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
 onsite testing	stand-up (15mn) —	stand-up (15mn) —	stand-up (15mn) —	stand-up (15mn) —
				

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
 onsite testing	stand-up (15mn) —	stand up (15mn) —	stand-up (15mn) —	demo (1u) —
				retro (1u) —



This works



Next: be visible on the board

The screenshot displays a Jira board with four columns: **To Do** (52 items), **In Progress** (13 items), **Verify** (1 item), and **Done** (39 items). A card titled **OPINIT-2326** is currently in the **Verify** column. The card's content includes:

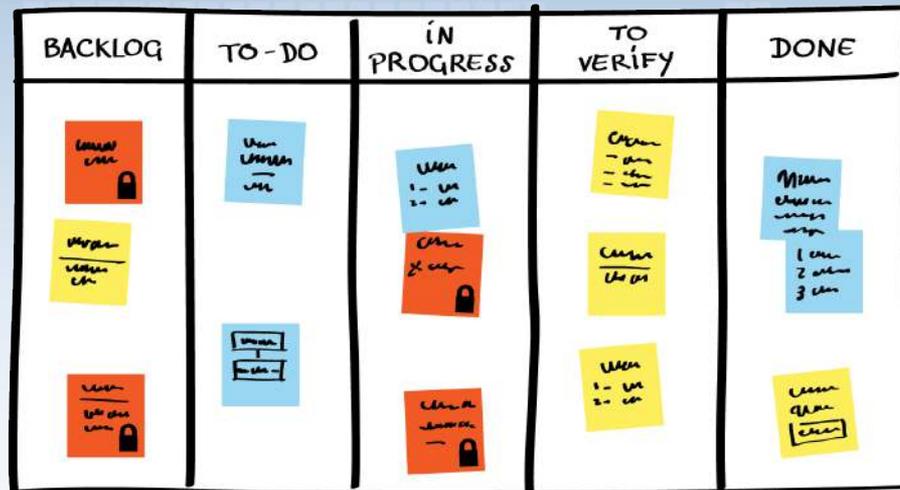
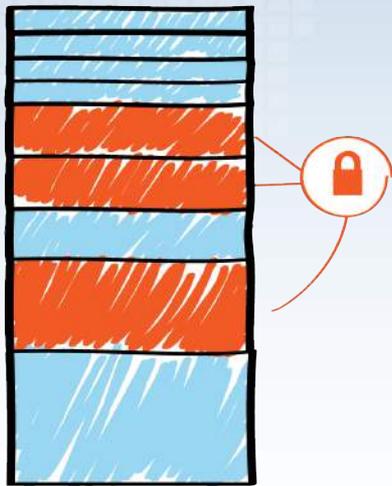
- As a [user] user I would like to have the last edited/viewed payment to scroll into view when I re
- Store payment in session
- OPIN... 2344: Adding payment ID to response
- OPIN... 2402: Securitytest** (highlighted)
- OPIN... 2743: CLONE - Browser testing
- OPIN... 2755: [Bug] Scroll payment into

The right sidebar provides details for the selected card, **OPINIT-2402 / Securitytest**. It shows an **Unestimated** estimate, no linked issues, and a description: "Based on the story discription, no potential securityrisks are identified. No sectest required." There is also a **Comments** section with a **Comment** button.



Next: add findings / create stories

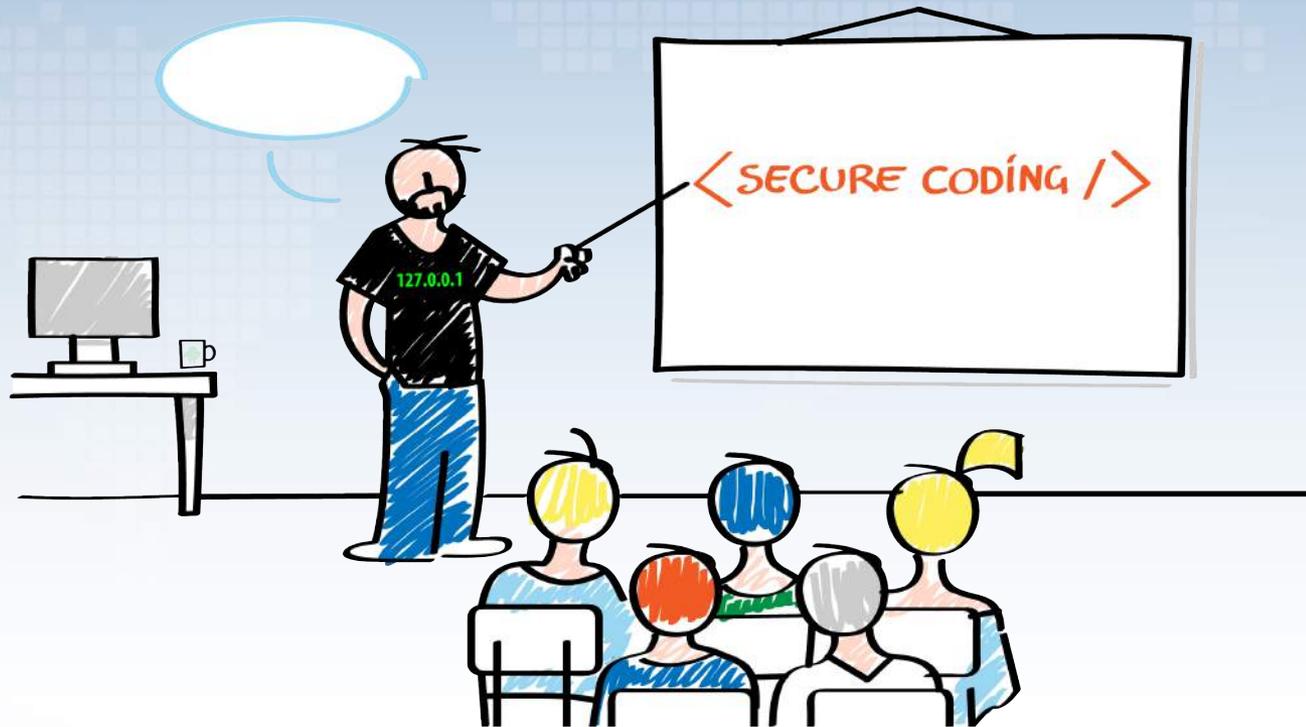
PRODUCT
BACKLOG



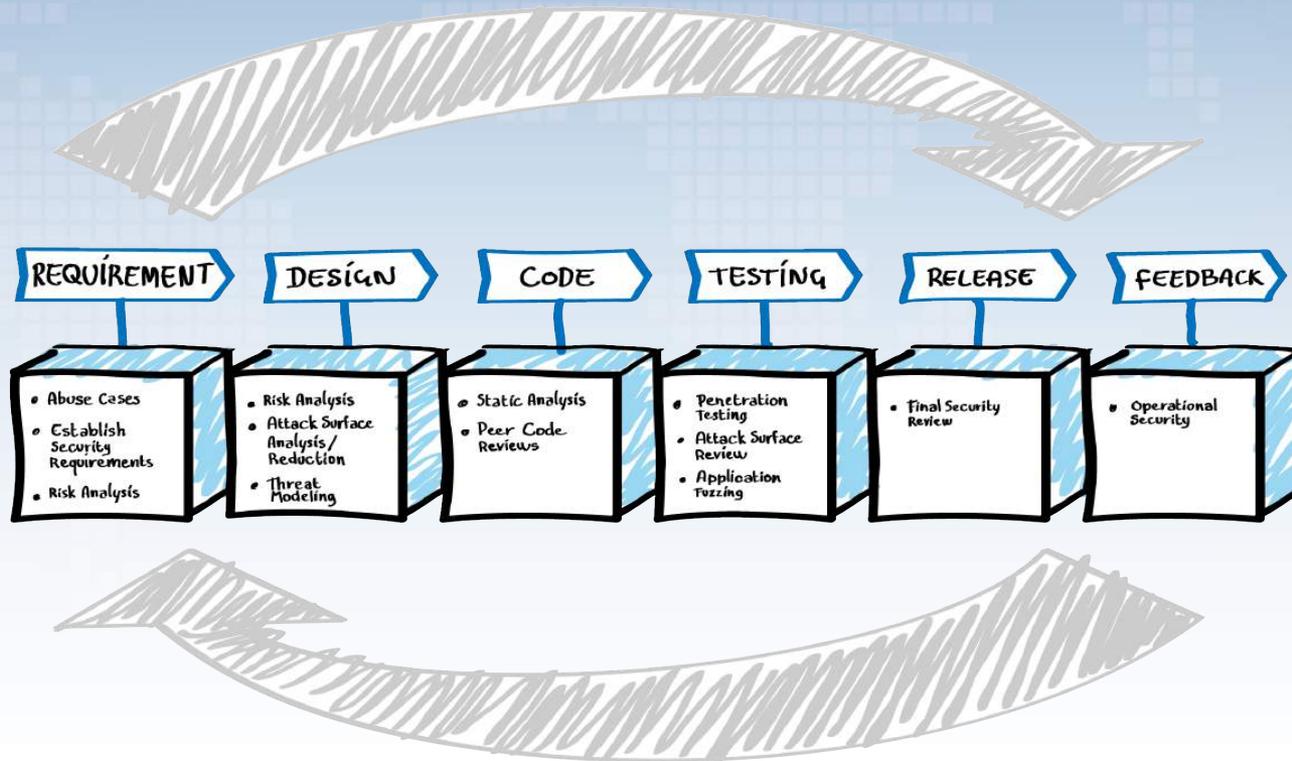
Have (simple) security sign-off



Share knowledge



Hey, this all starts to look like..



Agile, a blessing for software security?



david.vaartjes@securify.nl / @securifybv



OWASP AppSecEU 15
Amsterdam, The Netherlands

Takeaways

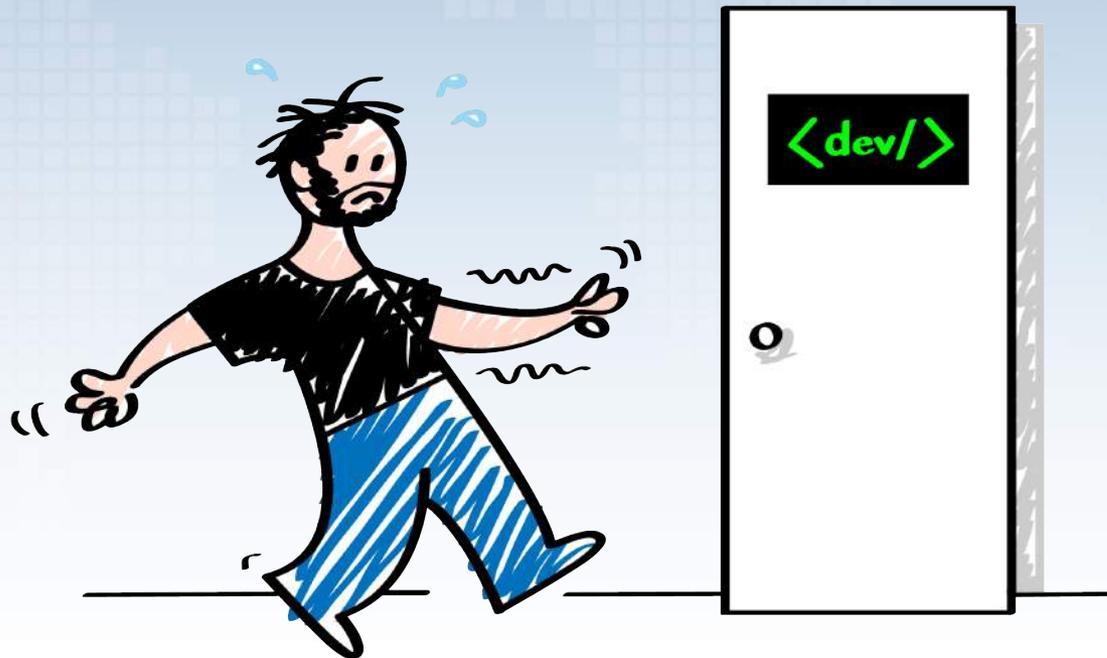


david.vaartjes@securify.nl / [@securifybv](https://twitter.com/securifybv)



OWASP AppSecEU 15
Amsterdam, The Netherlands

Security, leave your comfort zone!



Code reviews over (pen)testing!

```
ipcirc.send(introcell, TorCircuit.RELAY_COMMAND_INTRODUCE1, false, (short) 0);
log.debug("waiting for introduce acknowledgement");
ipcirc.waitForState(TorCircuit.STATES INTRODUCED, false);

log.debug("Now waiting for rendezvous connect");
rendz.waitForState(TorCircuit.STATES.RENDEZVOUS_COMPLETE, false);

ipcirc.destroy(); // no longer needed
log.debug("Hidden Service circuit built");

public static String publicKeyToOnion(RSAPublicKey pk) throws IOException {
    byte []service = TorCrypto.getSHA1().digest(TorCrypto.publicKeyToASNI(pk));
    String service32 = new Base32().encodeAsString(Arrays.copyOfRange(service,0,10)).toLowerCase();
    return service32;
}

public static String generateHSDescriptor(byte[] privkey) throws IOException {
    RSAPrivateKey pk = TorCrypto.asn1GetPrivateKey(privkey);
    PublicKey puk = TorCrypto.asn1GetPrivateKeyPublic(privkey);
    return generateHSDescriptor((RSAPublicKey) puk, pk);
}

public static String generateHSDescriptor(RSAPublicKey pk, RSAPrivateKey prk) throws IOException {
    String service32 = publicKeyToOnion(pk);

    StringBuilder desc = new StringBuilder();
    desc.append("rendezvous-service-descriptor "+new Base32().encodeAsString(getDescId(service32));
    desc.append("version 2\n");
    desc.append("permanent-key\n-----BEGIN RSA PUBLIC KEY-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String(TorCrypto.publicKeyToASNI(pk)));
    desc.append("\n-----END RSA PUBLIC KEY-----\n");
    desc.append("secret-id-part "+new Base32().encodeAsString(getSecretId(service32, (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"+
    "-----BEGIN MESSAGE-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String("nothing to see :-~)).getBytes();
    desc.append("\n-----END MESSAGE-----\n"+
    "signature\n");

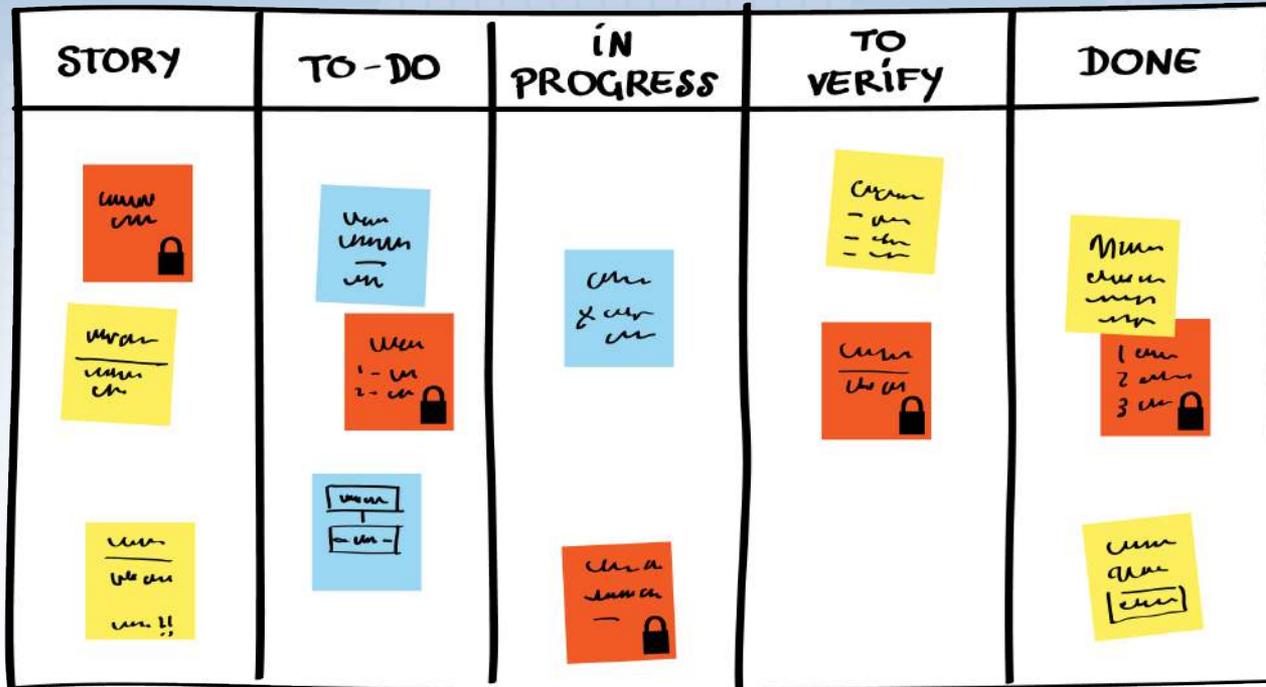
    byte sig[];
    try {
        Signature instance = Signature.getInstance("SHA1withRSA");
        instance.initSign(pk);
        instance.update(desc.toString().getBytes());
        sig = instance.sign();
    } catch (InvalidKeyException | NoSuchAlgorithmException | SignatureException e) {
        e.printStackTrace();
    }

    desc.append("-----BEGIN SIGNATURE-----\n");
    desc.append(MiscUtil.stringMaxWidth(Base64.toBase64String(sig), 64));
    desc.append("\n-----END SIGNATURE-----\n");
    return desc.toString();
}

7 differences Deleted Changed Inserted
```



Only test when needed!



Stay Agile, keep improving!

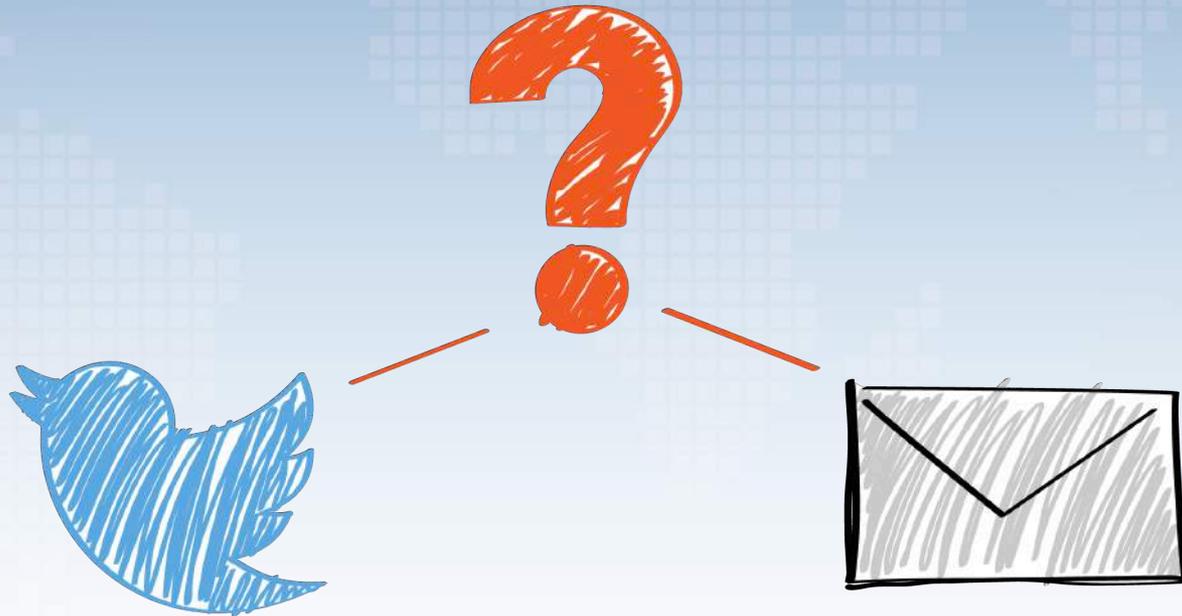
WORK IN PROGRESS

01	02	03	04	05
✓ [unclear]		✓ [unclear]	✓ [unclear]	[unclear]
[unclear]	[unclear]	✓ [unclear]		✓ [unclear]
✓ [unclear]	✓ [unclear]	[unclear]	✓ [unclear]	✓ [unclear]
	✓ [unclear]	[unclear]	[unclear]	

Automation ;-)



Thanks!



@securifybv

david.vaartjes@securify.nl

