Turvallisen sovelluskehityksen käsikirja

Antti Vähä-Sipilä, F-Secure

antti.vaha-sipila@f-secure.com, Twitter @anttivs

Väestörekisterikeskus

Tavoitteet

Käsikirjan tavoitteena on tukea nykyaikaista, DevOps-henkistä ketterää ohjelmistotuotantoa rikkomatta sitä

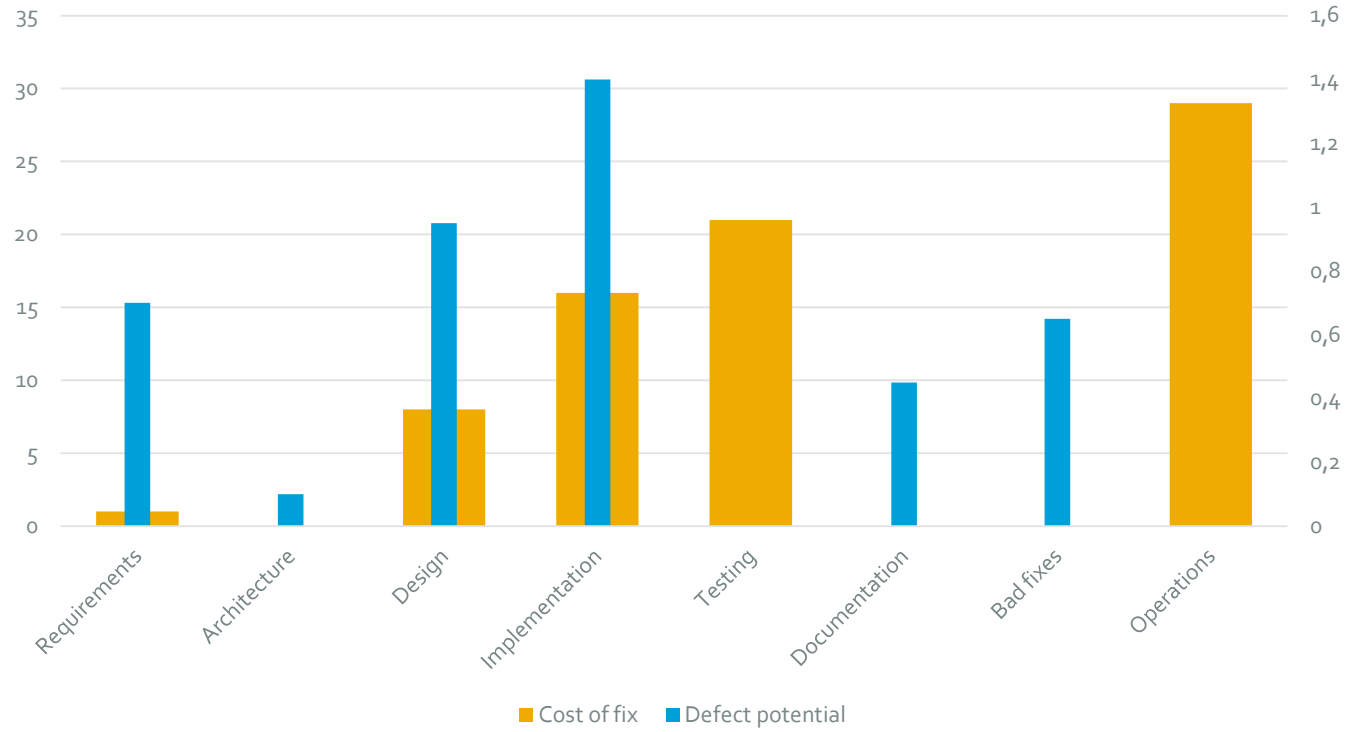
Väestörekisterikeskus

Tavoitteet

- Tehokas sekä käytetyn ajan että reagointinopeuden suhteen
- Mahdollisimman vähän pakottavaa lisätyötä
- Ei saa rikkoa ketteryyden tai leanin periaatteita
- On oltava riskipohjainen ja oikeasuhtainen
- On mahdollistettava seuranta ja auditointi

Väestörekisterikeskus

Tehokkuus 1/2



Vikapotentiaali (vikoja komponenttia kohden): Capers Jones, *A Comparison of Commercial and Defense Software*, Crosstalk Nov/Dec 2016, vol. 29, no. 6. Korjausten hinta (vaatimukset = 1; avaruusalusten järjestelmämuutoksista; monet muut lähteet antavat korkeampia arvioita ohjelmistoille): NASA, *Error cost escalation through the project life cycle*. 2010.

Väestörekisterikeskus

Tehokkuus 2/2

- Tärkein tarkastelukohta on teknisten vaatimusten sisäänottovaiheessa
- Edellisen kuvan mukaan näin hoidettaisiin 40 % ongelmista 0,4-kertaisella kustannuksella testausaikaiseen havaintoon nähden
- Ei kuitenkaan poista tietoturvatestauksen tarvetta, mutta pidemmällä aikavälillä muuttaisi sen luonnetta testauksesta varmistamiseen

Väestörekisterikeskus

Lisätyö ja ketteryys

- Ylimääräinen ”prosessityö” on perinteisesti vahva allergeeni
- Lisätyö, joka aiheuttaa työjonon (esim. hyväksyntäportti) aiheuttaa ongelmia jatkuvalle tuotantoonviennille
- Kehitystiimin ulkopuolinen lisätyö on pyritty pitämään mahdollisimman mekanistisena

Väestörekisterikeskus

Riskipohjaisuus ja oikeasuhtaisuus

- Kehitystiimiin tuleva turvallisuustyö pyritään tekemään näkyväksi, jotta siihen varataan aikaa (eikä vain oleteta sitä tehtäväksi)
- Kun tarvittava turvallisuustyö on erikseen näkyvissä tehtävälistalla, investointi siihen tehdään suhteessa kaikkeen muuhun arvontuottoon
- Turvallisuustyö liitetään vain siihen tehtävälistan työhön, joka sitä tarvitsee
- Tukeutuu merkittävässä määrin *uhkamallinnukseen*, joka on riskiarviointimenetelmä

Väestörekisterikeskus

Seurattavuus ja auditoitavuus

- Erillisten raporttien ja riskilistojen sijaan riskit, työ, löydökset ja niiden tilanne kirjataan tiketointijärjestelmään
- Sama järjestelmä, jota tuotehallinta ja kehittäjät käyttävät
- Kattava jälkikäteinen auditoitavuus riskipäätöksille ja ensi käden todiste riskiarviointien suorittamisesta
- Mahdollistaa reaaliaikaisen seurannan yli kaikkien projektien

Väestörekisterikeskus

Yleisnäkymä

Tietoturva- ja tietosuoja-aktiviteetit eivät rajoitu vain koodaukseen tai testaukseen

Väestörekisterikeskus

Konseptista koodiksi

Portfoliovaihe (~palvelumuotoilu):

- Lakien vaatimukset
- Formaalin tietosuojavaikutusten arvioinnin suoritus (DPIA)
- *(Tulevaisuudessa* palvelumuotoilu voisi tehdä myös omankaltaista uhkamallinnustaan)

Tehtävälistan hallintavaihe:

- Uhkamallinnus- ja muiden tietoturvatarpeiden mekaaninen löytäminen
- Tekninen tietosuoja-vaikutusten arviointi (PIA)

Toteutus:

- Uhkamallinnuksen suorittaminen
- Design-katselmointi
- Koodikatselmointi
- Automaattisten testien kehittäminen

Tutkiva testaus:

- Tietoturvatarkastus tutkivan testauksen menetelmin
- Sis. myös haavoittuvuus-palkkio-ohjelman

Väestörekisterikeskus

Konseptista koodiksi

Portfoliovaihe (~palvelumuotoilu):

- Lakien vaatimukset
- Formaalin tietosuojavaikutusten arvioinnin suoritus (DPIA)
- *(Tulevaisuudessa* palvelumuotoilu voisi tehdä myös omankaltaista uhkamallinnustaan)

Tehtävälistan hallintavaihe:

- Uhkamallinnus- ja muiden tietoturvatarpeiden mekaaninen löytäminen
- Tekninen tietosuoja-vaikutusten arviointi (PIA)

Toteutus:

- Uhkamallinnuksen suorittaminen
- Design-katselmointi
- Koodikatselmointi
- Automaattisten testien kehittäminen

Tutkiva testaus:

- Tietoturvatarkastus tutkivan testauksen menetelmin
- Sis. myös haavoittuvuus-palkkio-ohjelman

Palaute (juurisyyanalyysi)

Väestörekisterikeskus

Työkalut ja vaatimustasot

Tietoturva- ja tietosuojavaatimusten tasot ja ohjeistus on määritelty niin, että niiden pakottavuus on selkeää

Väestörekisterikeskus

Vaatimukset

- *Pakolliset* vaatimukset lainsäädännöstä
  - Sovellusaluekohtaisia, portfoliovaiheessa
- *Tuotantoonvientivaatimukset* käsikirjan liitteessä 1
  - Voidaan laittaa tehtävälistalle suunnitteluvaiheessa, jolloin tulevat huomioon otetuiksi (ehkä vain kerran per hanke)
- *Yleiset suunnitteluperiaatteet* käsikirjan liitteessä 2
  - Tiedostettavia asioita, joista tulee ”kantaa huolta” oman roolin perusteella

Väestörekisterikeskus

Työkalut ja ohjeet

- *Triage-tarkastuslista* käsikirjan liitteessä 3 ohjaa tuoteomistajaa
- *Tekninen liite tietoturvakäsikirjaan* kattaa erityisesti web-sovellusten teknisiä nyansseja
- Joillekin alueille on olemassa *ulkoisia ohjeita*, joita noudatetaan, jos tarve niille on tunnistettu – esimerkiksi uhkamallinnuksessa
  - Esimerkiksi Center for Internet Securityn (CIS) kovennusohjeet; Euroopan tietosuojaneuvoston ohjeet; VAHTI-ohjeet; OWASPin dokumentit (mm. ASVS)

Seuranta ja auditoitavuus

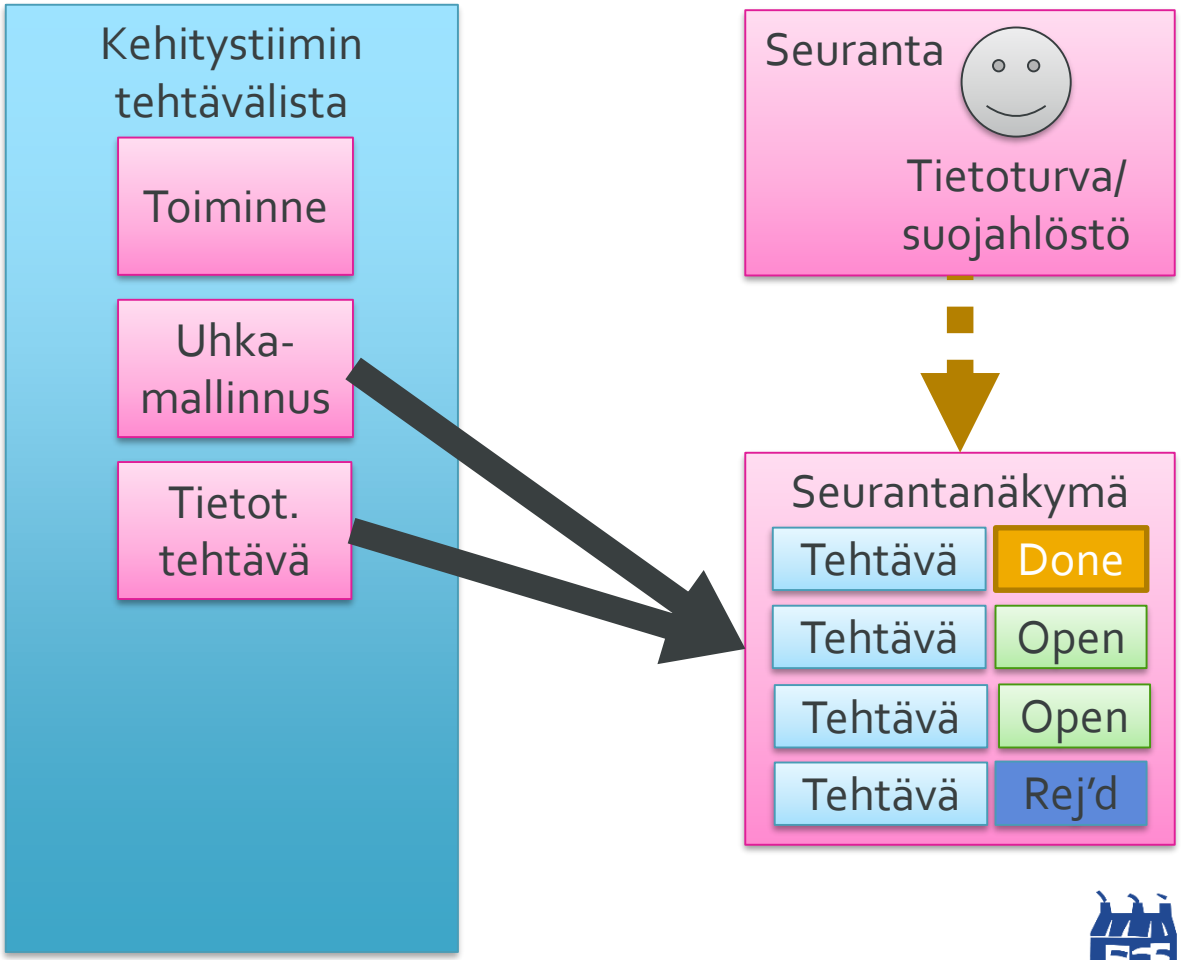
Seuranta perustuu tiketöintiin

Väestörekisterikeskus

Seuranta

- Tiketöinnissä (esim. JIRA) käytetään linkkejä ja leimoja
- Leimat standardoidaan organisaation laajuisesti, esim. ”uhkamallinnus”
- Jokainen hanke tuottaa uusia leimattuja tikettejä tietyllä taajuudella
  - Jos näitä ei synny, tietoturva/suojafunktio voi olla yhteydessä
- Erityisen tärkeää seurata esimerkiksi tietosuojavastaavan roolissa

Väestörekisterikeskus



Väestörekisterikeskus

Auditoitavuus

- Toiminnallisuus linkittyy tiketöinnissä tietoturvatyöhönsä
- Tietoturvatyö (esim. uhkamallinnus) linkittyy löydöksiinsä
- Auditoija voi todeta työn tehdyksi ja löydösten tilan
- Riskien hyväksyntä on dokumentoitu tikettien kommentteihin

Väestörekisterikeskus

Tuki

Merkittävin tuen tarve on uhkamallinnukseen ja tietoturvatarkastukseen

Väestörekisterikeskus

Tiedostettu tuen tarve

- Uhkamallinnus (kehittäjille Microsoft STRIDEn pohjalta, palvelukehitykselle hyökkääjätarinoita hyödyntämällä) on usein uusi asia
- Tavoitteena on työn ohessa oppiminen

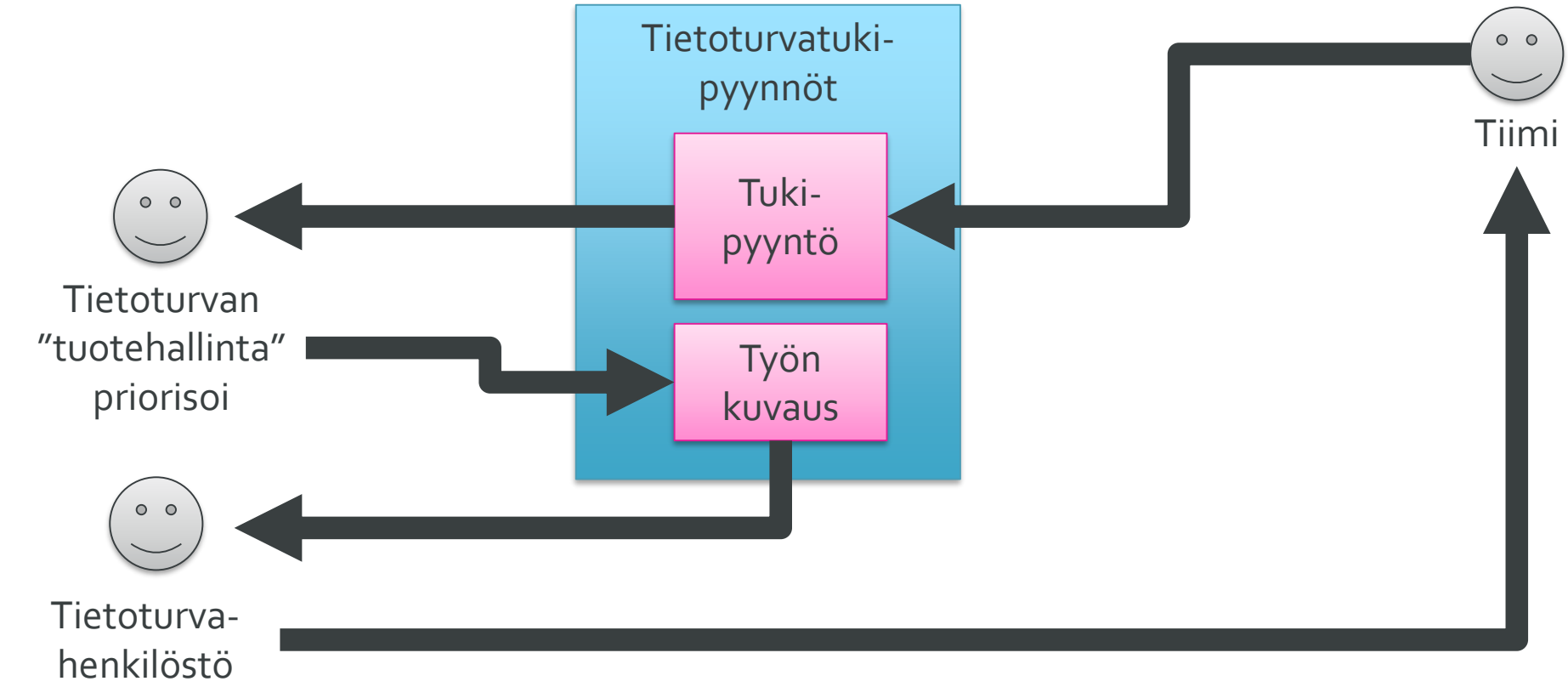
Väestörekisterikeskus

Tukimalli

- Tukimallina toimii ”tuen työjono”
- Kehitystiimeillä on valta ja vastuu pyytää apua avaamalla tiketti
- Tukiresurssien omistaja priorisoi hankkeiden tukipyynnöt
- Tukiresurssi toimittaa avun tiketin perusteella

- Tietoturvatehtävä on edelleen **kehitystiimin** työlistalla, ainoastaan tukitarve on tiimin ulkoisella tehtävälistalla

Väestörekisterikeskus



Väestörekisterikeskus

Kiitos!

Lisätietoja VRK:n toteutuksesta: pekka.ristimaki@vrk.fi
Yleisesti mallista: antti.vaha-sipila@f-secure.com

Väestörekisterikeskus