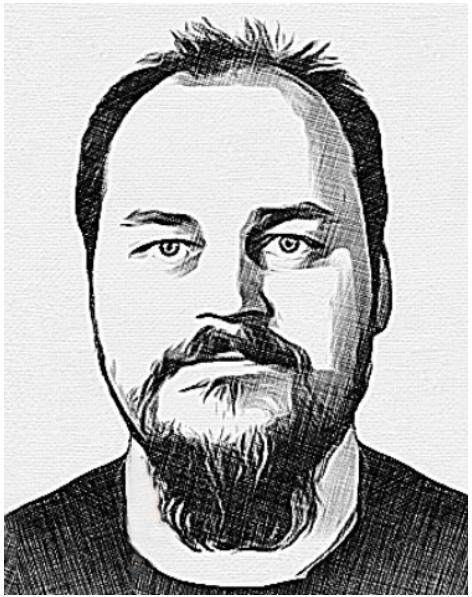
Testaajan muuttuva rooli

Jani Salmikivi

OP

Kuka minä olen?



Jani Salmikivi, OP Palvelut Oy

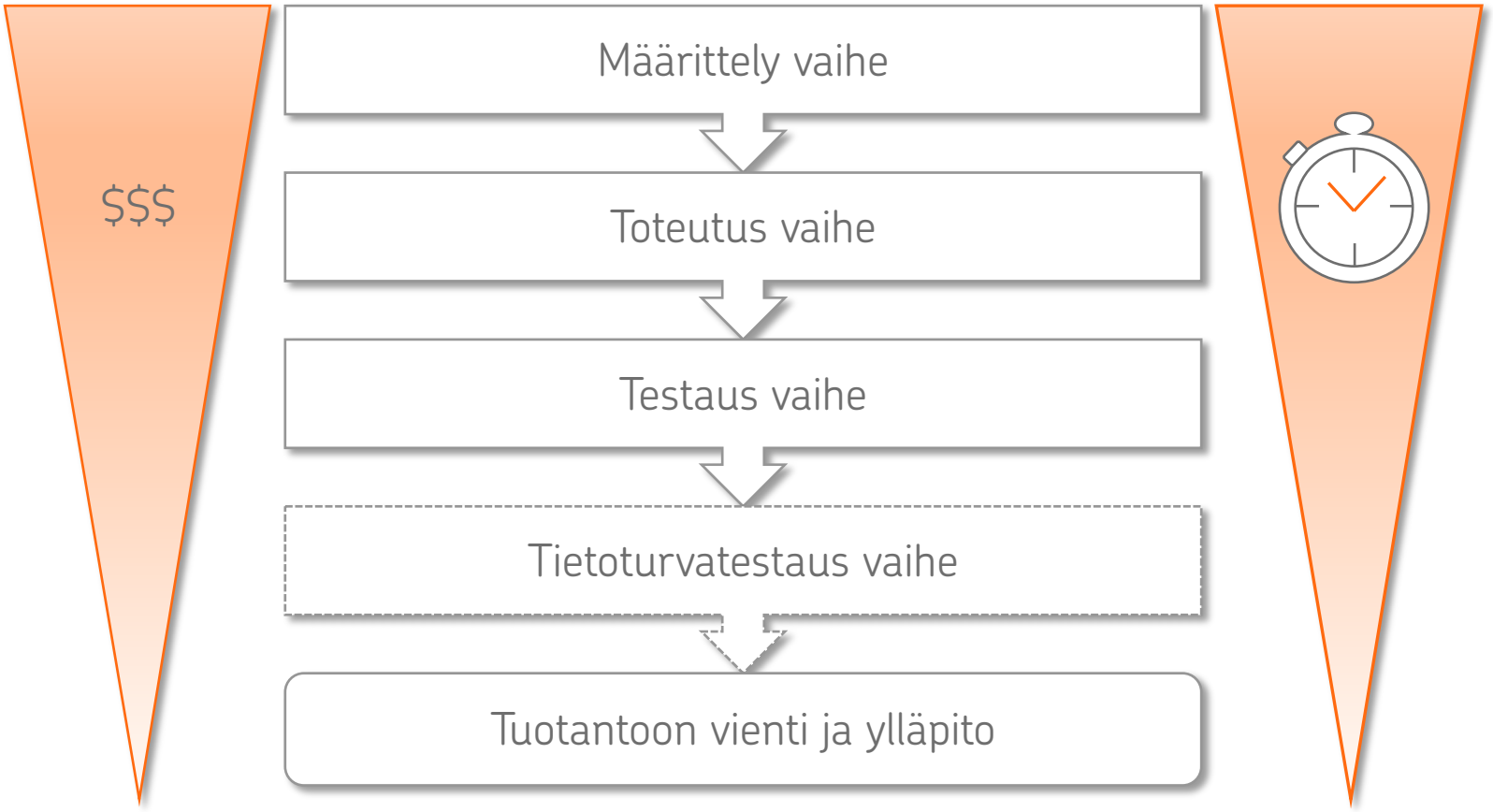
Head of security testing & audit

- OP uraa takana lähes 10v
- Tietoturvan alueella ~ 15v

Historiaa myös näillä alueilla:

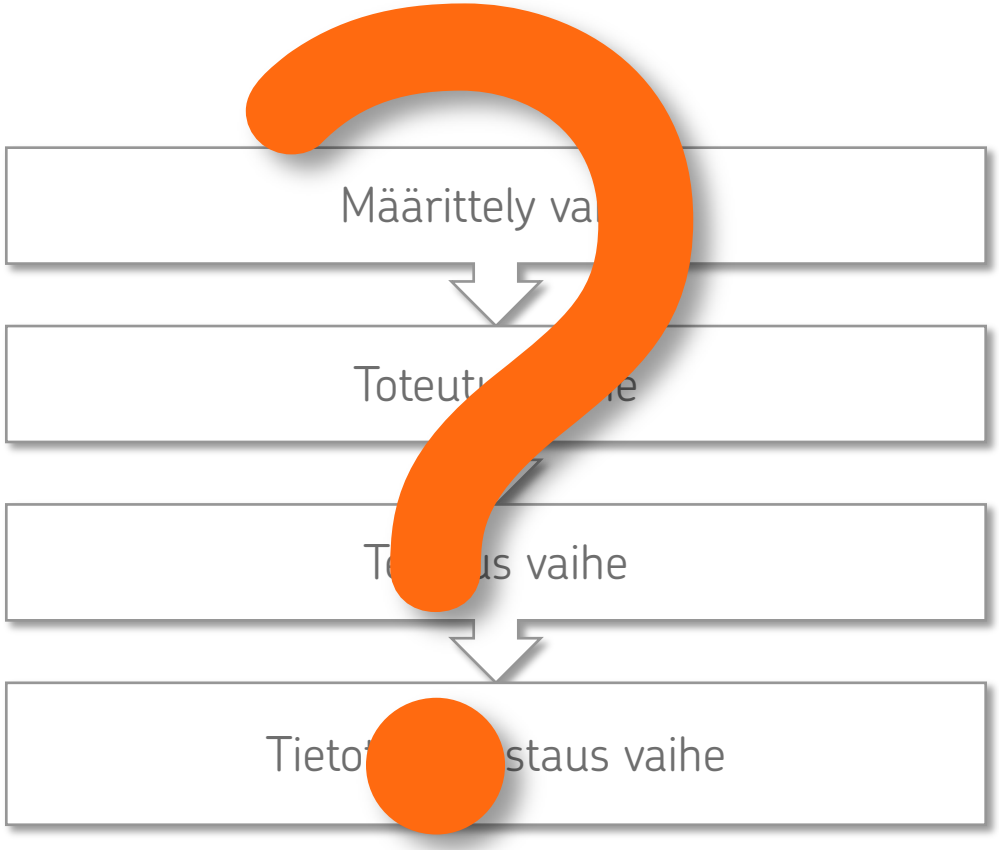
- Manuaalitestaus
- Testausautomaatio
- Testaushallinnointi
- HW suunnittelu ja testaus

OP

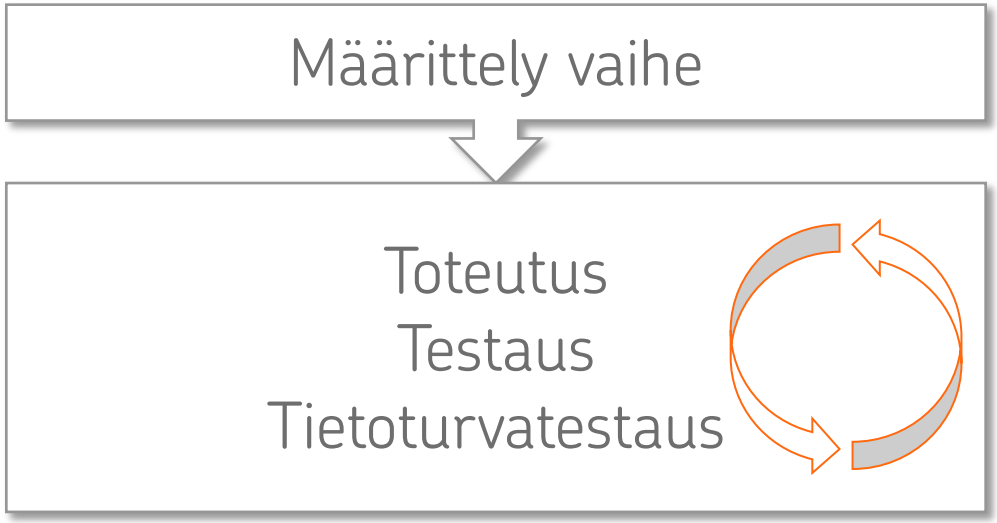


Tietoturvatestaus

Huomenna



Toteutus, testaus sekä tietoturvatestaus sulautuvat



Miten tämä saadaan aikaan?

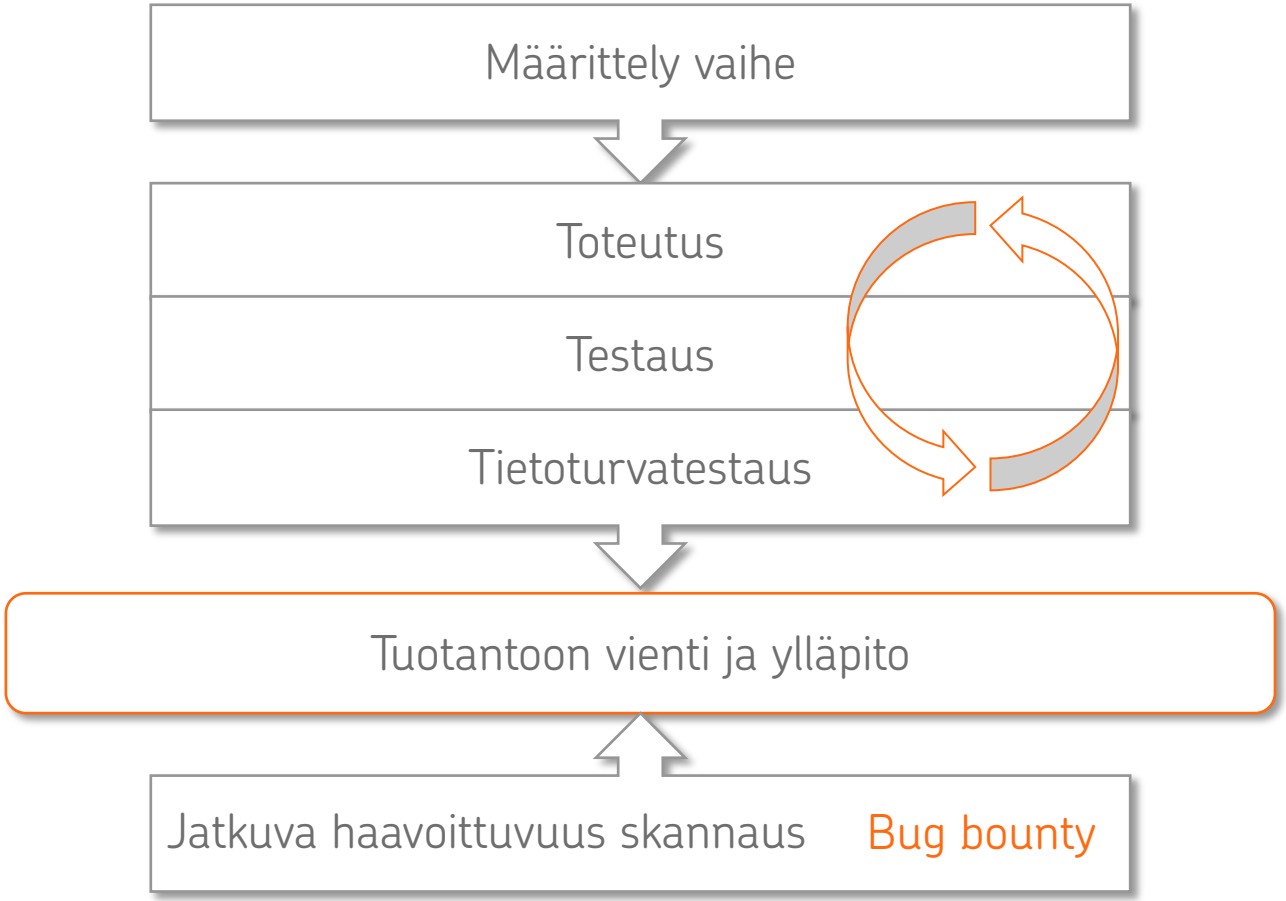
- Automaation lisääminen
  - Toiminnalisen testauksen automaatio
    - *Selenium, Appium…*
  - Kuormitustestausautomaatio
    - *jMeter, Loadrunner (Micro Focus)…*
  - Tietoturvatestausautomaatio
    - Tietoturvan staattinen koodianalyysi (SAST)
      - *Synopsys, IBM AppScan*
    - Tietoturvan dynaaminen analyysi (DAST)
      - *Burp Enterprise…*

Hyödyt

- Tuotantoon viennit nopeutuvat
  - Mahdollistaa atomiset toimitukset
- Osaaminen kasvaa asiantuntijoilla
- Tiimien ‘resilienssi’ kasvaa, kaikki osaavat vähän kaikkea
- Vastuu kasvaa
  - Kaikille löytyy mielekästä tekemistä isosta vastuualueesta

Haitat

- False positive havaintojen määrä kasvaa
  - Vaatii aikaa käsitellä ne oikein
  - Hidastavat lähes aina alkuvaiheessa tuotantoon vientejä
- Vastuu kasvaa
  - Kaikki eivät ole mielissään isosta vastuualueesta
- “Kaikki osaavat vähän kaikkea” johtaa siihen että erikosalueiden syväosaajat puuttuvat
- Osaamisen tarve kasvaa
  - Aloittelevan asiantuntijan kynnys päästä ‘sisään’ kasvaa
  - Osaajapula (koko Suomi etsii hyviä tekijöitä!)



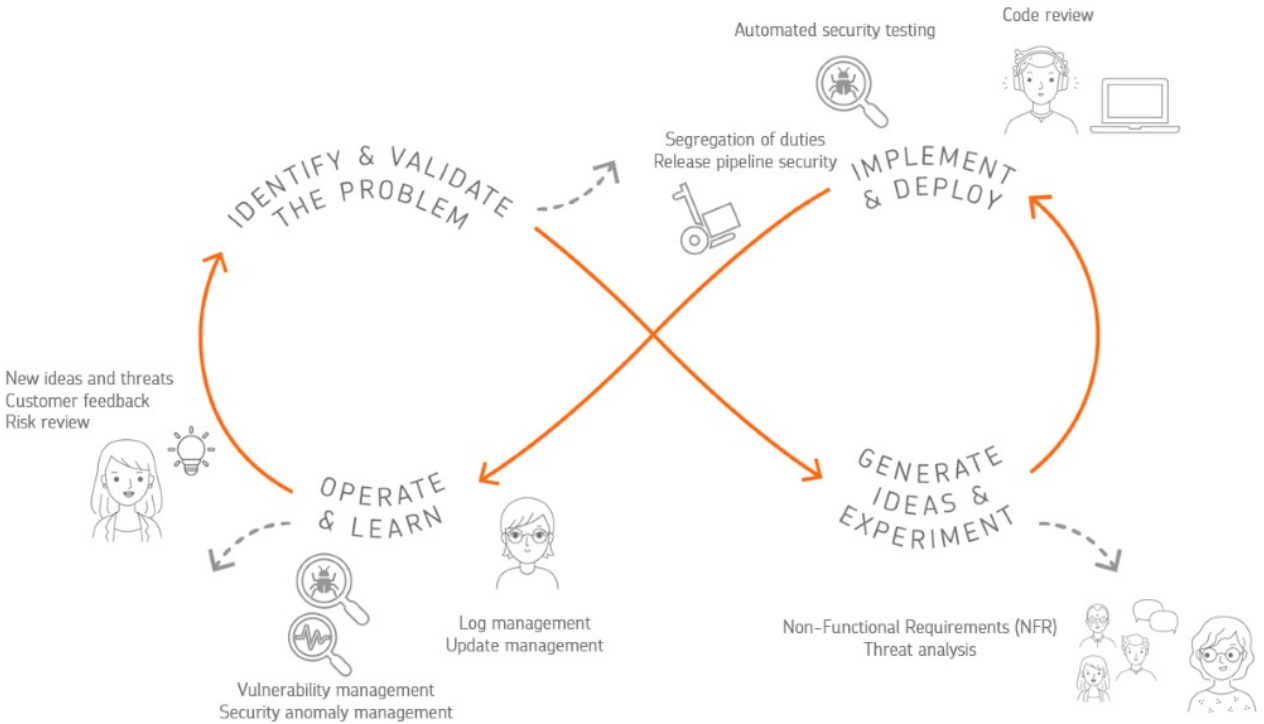
Määrittely vaihe

Toteutus vaihe

Testaus vaihe

Tietoturvatestaus vaihe

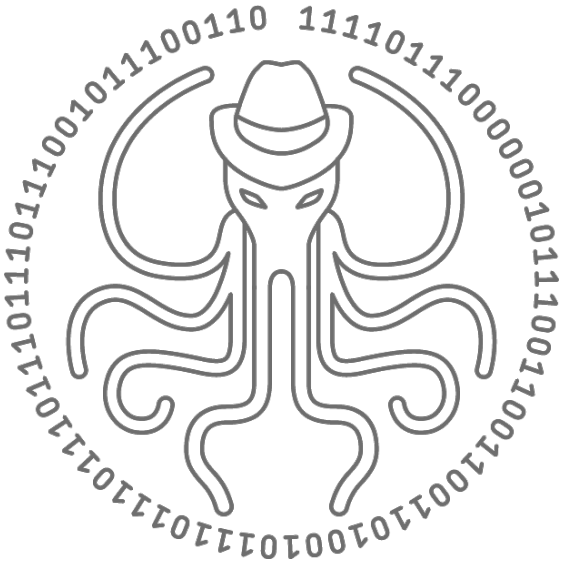
Tuotantoon vienti ja ylläpito



Bug bounty-ohjelma

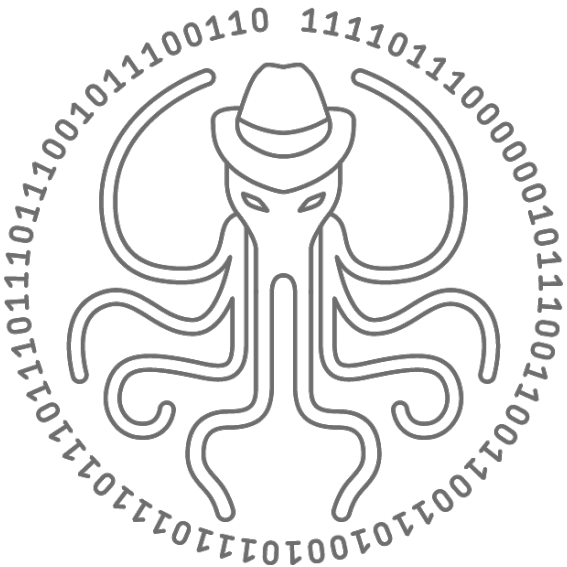
Bug bounty lyhyesti

- Bug bounty on ohjelma jonka avulla joukkoistetaan haavoittuvuuksien etsintä valituista kohteista
- Hakkereille (haavoittuvuuksien etsijöille) maksetaan vain oikeaksi todetuista haavoittuvuuksista
- Bug bounty –ohjelmilla on säännöstö (policy) jota hakkerit noudattavat
- Hakkerit toimivat yleensä tuotannon järjestelmissä, eivätkä testiympäristöissä



Bug bounty OPlla

- OP aloitti oman Bug bounty -ohjelman joulukuussa 2019
- Ohjelmassamme on hakkereita ympäri Eurooppaa mm Suomi, Ruotsi, Saksa ovat edustettuina
- Ohjelmamme aktiivisin hakkeri on saanut palkkioita lähes 10 000$
- Korkein yksittäinen maksamamme palkkio on 4000$



Miten tiimit hyötyvät Bug bountystä?

- Tiimit saavat ajantasaisen ja realistisen kuvan tuotannon tietoturvan tilasta
- Kehittävät tiimit oppivat torjumaan uusimpia hyökkäystapoja
- Tiimit saavat käyttöönsä pohjoismaiden parhaimpien tietoturvatutkijoiden ammattitaidon

- Tiimit saavat asiantuntijatiimin tuen korjauksille
- Oman osaamisen ‘benchmarkkaus’ nykyaikaisin menetelmin
- Ohjelmien kautta saadut raportit ovat todella laadukkaita
- Saatu testaus on aikarajatonta

OP

Miten testaajan osaamisen tulee kehittyä?

Testaajien osaamisen muuttuminen

- Automaatio osaamisen tarve kasvaa
  - Automaation kehittäminen
  - Automaation oikeanlainen/järkevä kuluttaminen
  - Vaikka automaatio osaamisen tarve kasvaa, ei tutkivan testaamisen tarve poistu!
- Tuotekehitysprojektien laaja-alainen osaaminen
- Tietoturva ongelmien ratkaiseminen ja tunnistaminen
  - Tietoturvatestaamisen kyvykkyydet

"Tietoturvasta tulee osa laatua"

Miten lähden kasvattamaan omaa osaamistani?

- Verkko-opinnot
  - Portswigger Web security Academy (ilmainen): https://portswigger.net/web-security
  - Hack this site (ilmainen): https://www.hackthissite.org/missions/basic/
- Tutki Bug bounty ohjelmille kirjattuja havaintoja
  - "Apinoi" niitä, ja testaa samoja menetelmiä omissa (sallituissa) kohteissa
    - https://hackerone.com/hacktivity
- Ota osaa Bug bounty ohjelmiin
  - https://www.hackr.fi || https://www.yeswehack.com/ || https://hackerone.com
- Tutustu OWASP-säätiön tarjoamiin materiaaleihin, koulutuksiin sekä tapaamisiin
  - https://owasp.org/

Miten lähden kasvattamaan omaa osaamistani?

- Ota osaa ilmaisiin tietoturvatapahtumiin ympäri Suomea
  - Helsinki || Seinäjoki-Vaasa || Jyväskylä || Turku || Oulu || Tampere jne...
  - https://citysec.fi/
- Osallistu tietoturva aiheisiin seminaareihin
  - https://disobey.fi

OP

Lisätietoa

- Hyvä hakkeri paljastaa tietoturvasi aukot
  - https://www.op-media.fi/digitalisaatio/hyva-hakkeri-paljastaa-tietoturvasi-aukot/
- Podcast, Miten Bug bounty –ohjelma soveltuu tietoturvahaavoittuvuuksien ratkomiseen?
  - https://op-careers.fi/content/optech35/

OP