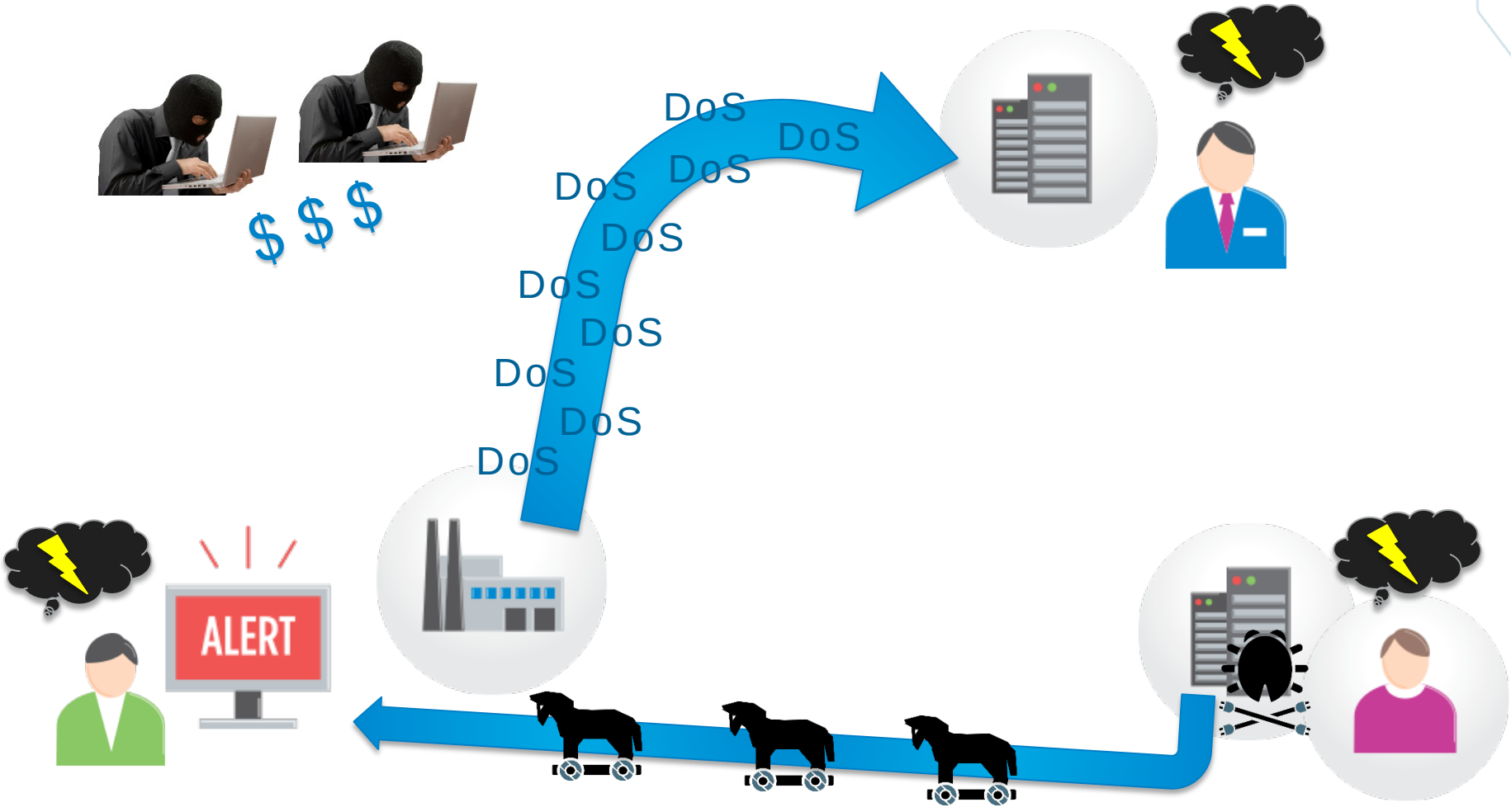
KOLME KEINOA OHJELMISTOTURVALLISUUTEEN

Anne Oikarinen
Senior Security Consultant

nixu

TARINOITA TIETOMURROISTA



~~ESINEIDEN~~
REIKÄISTEN WEB-PALVELIMIEN INTERNET

nixu

ONKO KÄYTTÄJÄN ANTAMA SYÖTE TURVALLISTA?

- **ZyXEL-kotireititin: Komentojen injektointi lokienkatselun kautta**
  1. Lokeja saa katsella tunnistautumatta 
  2. Syötettä ei tarkisteta 
  3. Käyttäjän antama syöte suoritetaan 

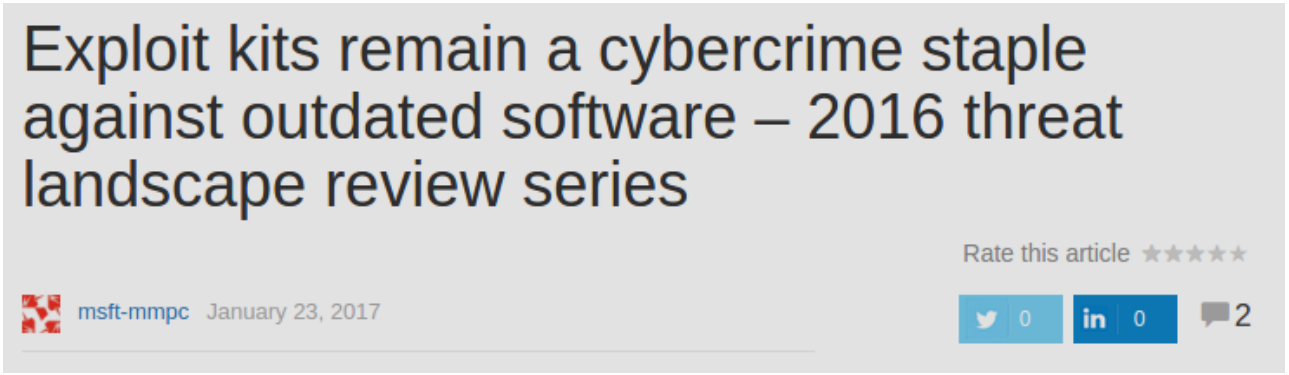
```
1 POST /cgi-bin/adv_remotelog.asp HTTP/1.1
2 Host: 192.168.1.1
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 85
5
6 RemotelogEnable=1&syslogServerAddr=1.1.1.1%3bping+-c+3+192.168.1.35%3b&serverPort=514
```

The injection is in the *syslogServerAddr* parameter that can be exploited by entering a valid IP address, followed by ";<*COMMAND*>;"

https://blogs.securiteam.com/index.php/archives/2910

nixu

JOKO SINULLAKIN ON EXPLOIT KIT?



https://blogs.technet.microsoft.com/mmpc/2017/01/23/exploit-kits-remain-a-cybercrime-staple-against-outdated-software-2016-threat-landscape-review-series/

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/04/ttn201604151223.html

Suomalaissivustoille ilmestyi Isistä panetteleva viesti – Viestintävirasto selvittää verkkohyökkäystä

Verkkohyökkäyksen kohteeksi on joutunut yksittäisiä suomalaisia sivustoja. Viestintäviraston käsityksen mukaan kyse on suhteellisen harmittomasta hyökkäyksestä.

Verkkojulkaisut 5.2.2017 klo 14:49

Hacked By MuhmadEmad

29.1.2017
Urheiluseurat
0 | 13
Kuopio, taitoluistelu

HaCkeD By MuhmadEmad

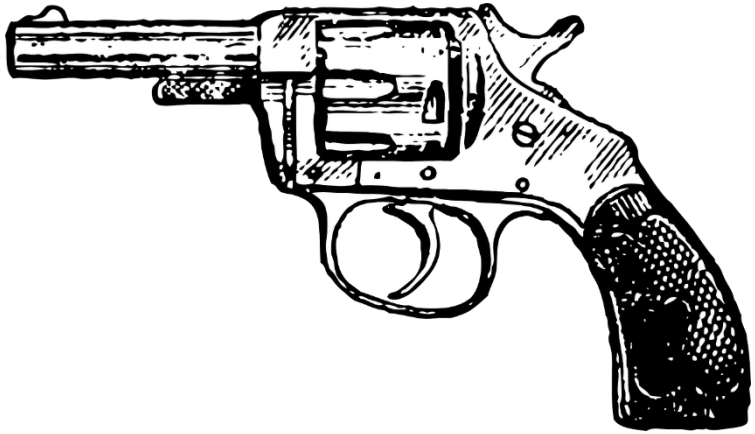
Long Live to peshmarga

KurDish HaCk3rS WaS Here

kurdlinux007@gmail.com
FUCK ISIS !

25 2

http://yle.fi/uutiset/3-9443283



tivi | CIO | MIKRO

Tilaa Tivi-lehti | Tilaa uutiskirje | Ilmoita Tivissä

ETUSIVU | KAIKKI UUTISET | BLOGIT | KUMPPANIBLOGIT | VIIKON SOFTA & VINKIT

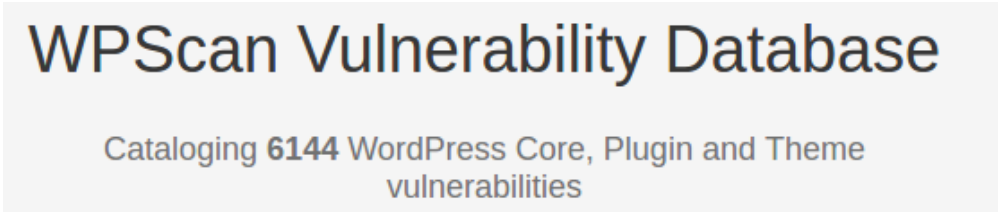
TIETOTURVA | Teemu Laitila 3.2. klo 15:32

WordPress jätti kertomatta kriittisen aukon paikkaamisesta – syy kuitenkin melko hyvä

http://www.tivi.fi/Kaikki_uutiset/wordpress-jatti-kertomatta-kriittisen-aukon-paikkaamisesta-syy-kuitenkin-melko-hyva-6621374

nixu

HAAVOITTUVUUKSIEN HYÖDYNTÄMINEN ON HELPPOA



Popular Videos - Vulnerability & Exploit - YouTube
https://www.youtube.com/playlist?list... ▾ Käännä tämä sivu
Vulnerability - Topic; 200 **videos**; 2,284 views; Updated today ... How To **Exploit** Joomla SQL Injection **Vulnerability Exploit** Results in Full Administrative Access.

Exploit 0day : WordPress Remote File Upload Vulnerability - YouTube

https://www.youtube.com/watch?v=MkBwCB0eApw ▾
22.8.2014 - Lataaja: Hamzah Uygun
9:22. 17 **videos** Play all Watch Dogs 2 Original Game Soundtrack by Hudson MohawkeBoss Gaming ...

Windows 10 Exploit! - Multihandler Remote Execution Vulnerability ...

https://www.youtube.com/watch?v=S0gMMGSkFmI ▾
22.2.2015 - Lataaja: Metasploitation
Windows 10 **Exploit**! - Multihandler Remote Execution **Vulnerability** ... This **video** is purely for educational ...

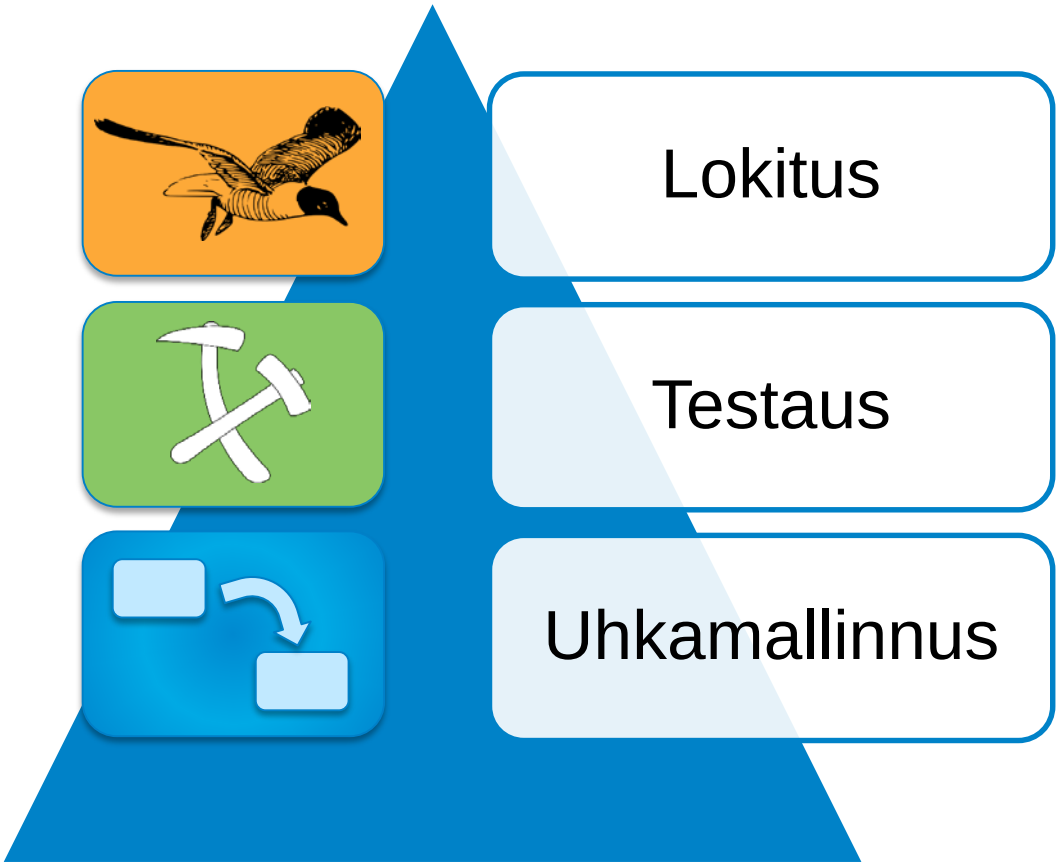
nixu

Kuinka nämä olisi voitu estää?

Tai ainakin pienentää vahinkoja

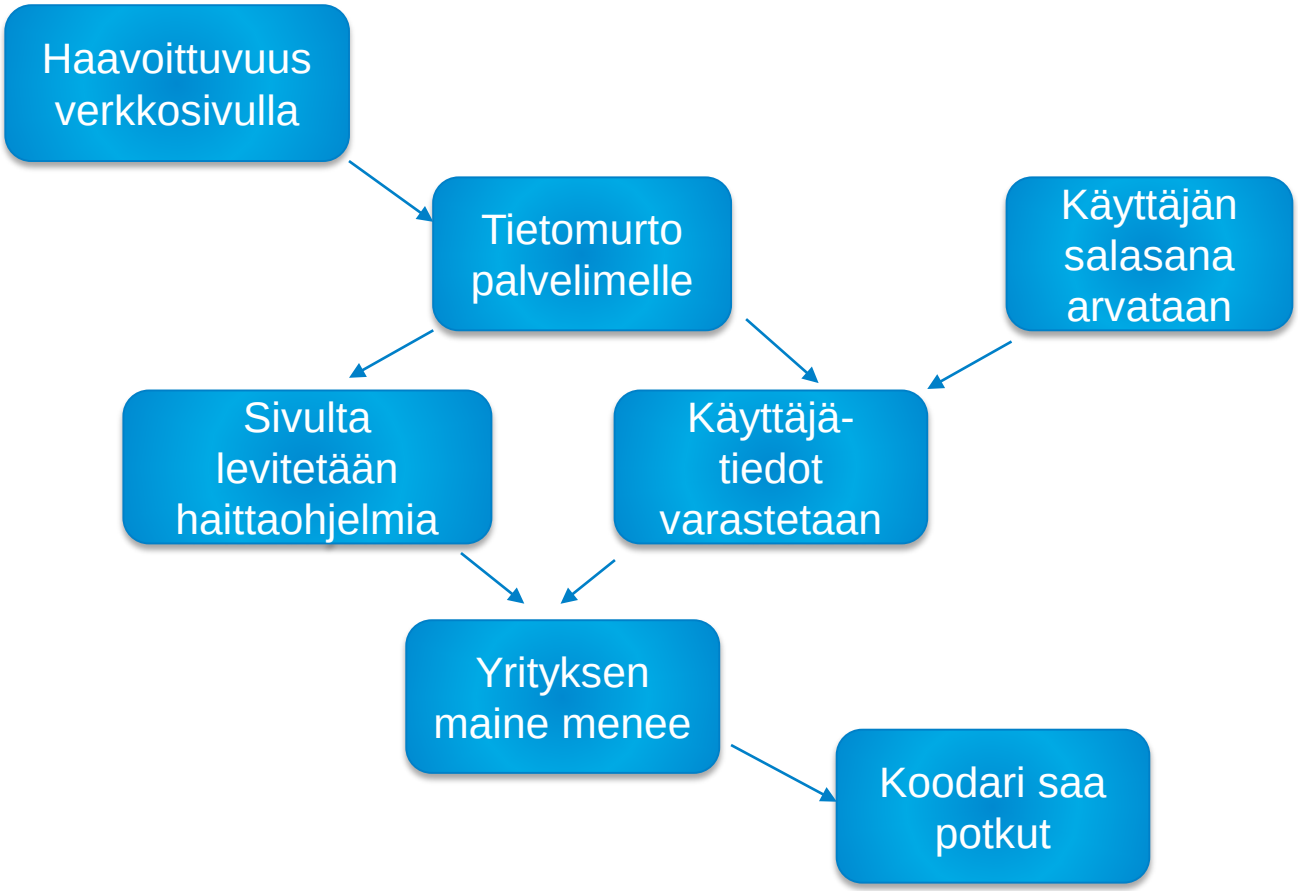
29.3.2017

KOLME KEINOA TURVALLISEMPIIN OHJELMISTOIHIN



nixu

UHKAMALLINNUS – MIKÄ VOI MENNÄ PIELEEN?



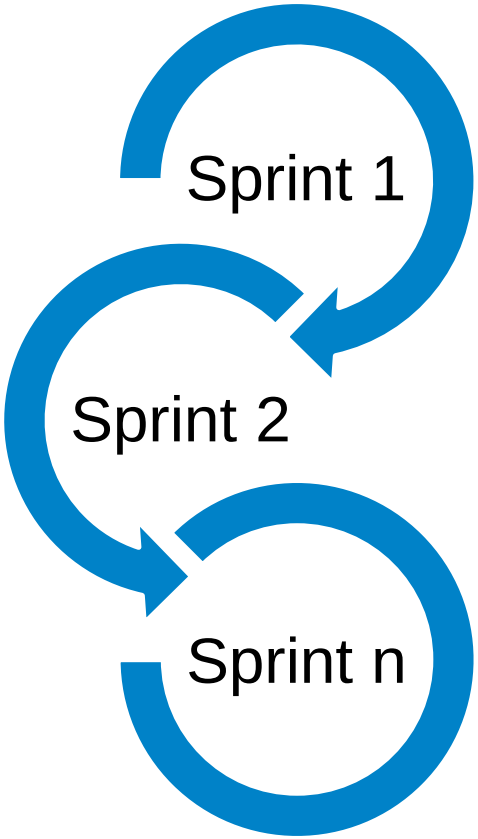
UHKAMALLIN PERUSTEELLA SUOJATOIMENPITEET

Testaajat

Devaajat

Product Owner

Tietoturva-asiantuntija



- **Uhkamallinnus**
- **Hyökkäyspinnat**

- **Tarkista uhkamalli**
- **Jäännösriskit**

Bugit

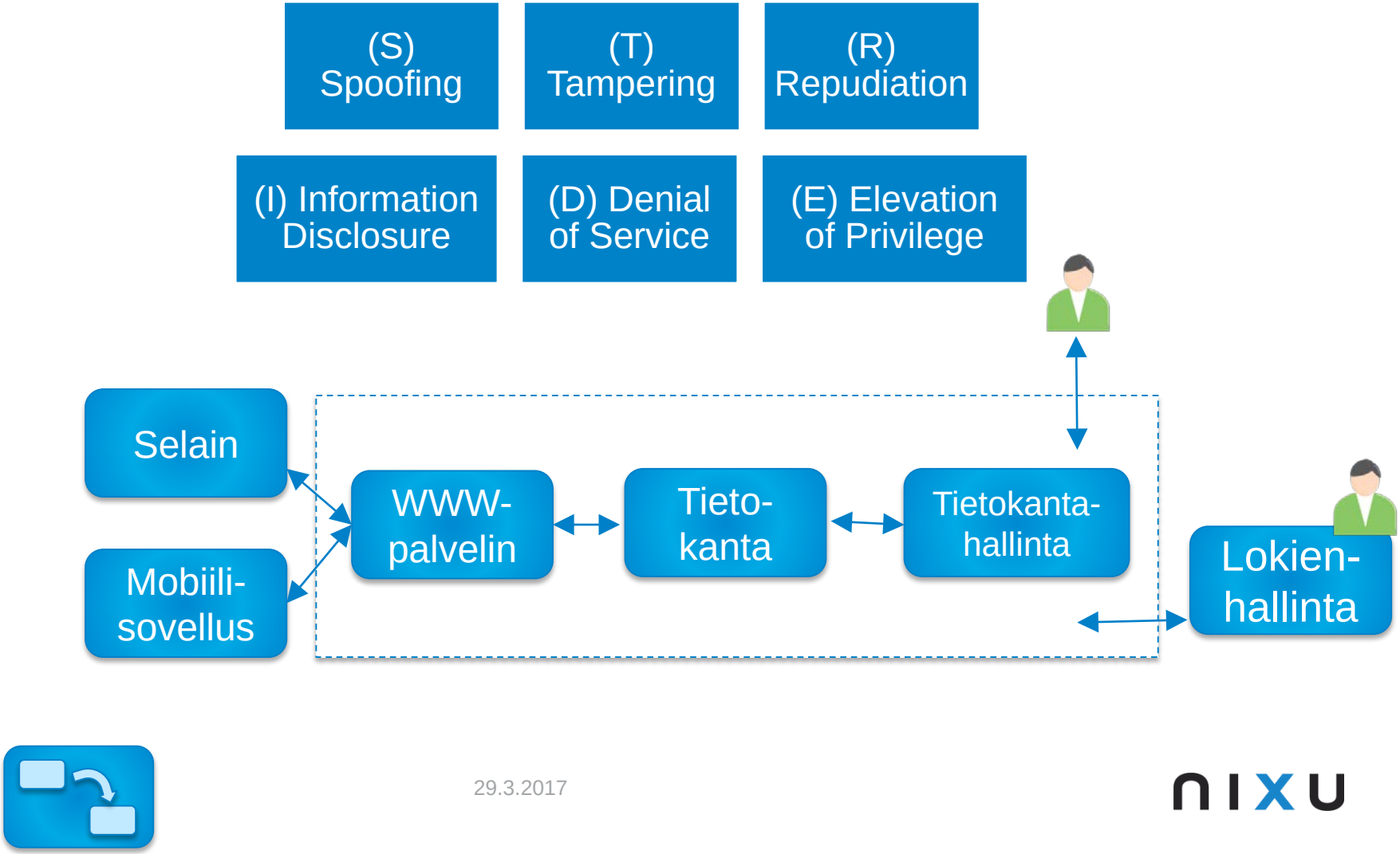
Testi-tapaukset

Backlog

Dokumen-taatio

nixu

STRIDE-MALLI ARKKITEHTUURIN JA TIETOVUON TARKASTELUN TUEKSI



”People are not, as is often claimed, the weakest link or beyond help. The weakest link is almost always a vulnerability in Internet-facing code.”

Adam Shostack

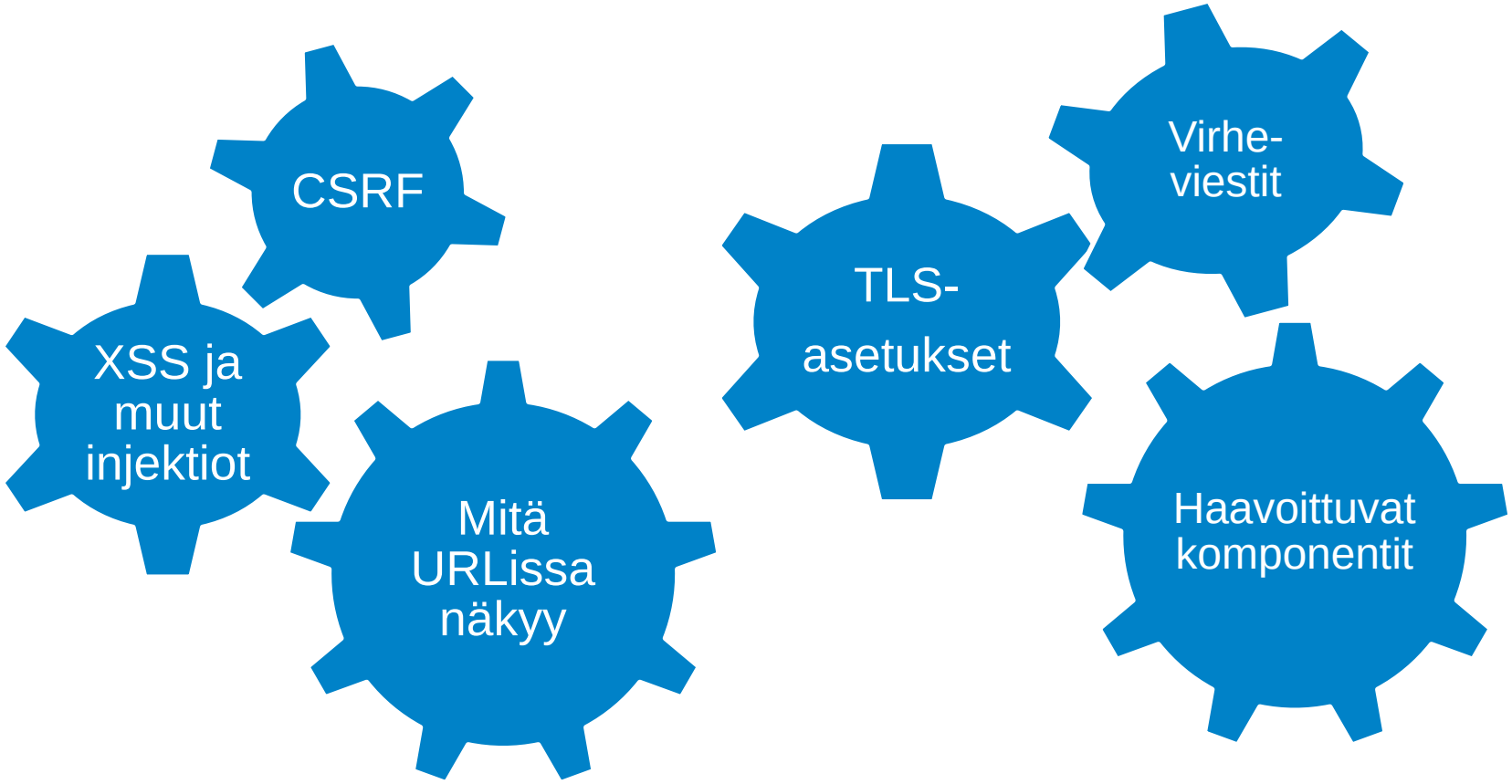
Threat Modeling – Designing for Security

NIXU


I FIND YOUR LACK OF
SECURITY TESTING
DISTURBING
memegenerator.net

nixu

MONTA OWASP TOP 10 –ONGELMAA LÖYTYY AUTOMAATIOLLA



nixu

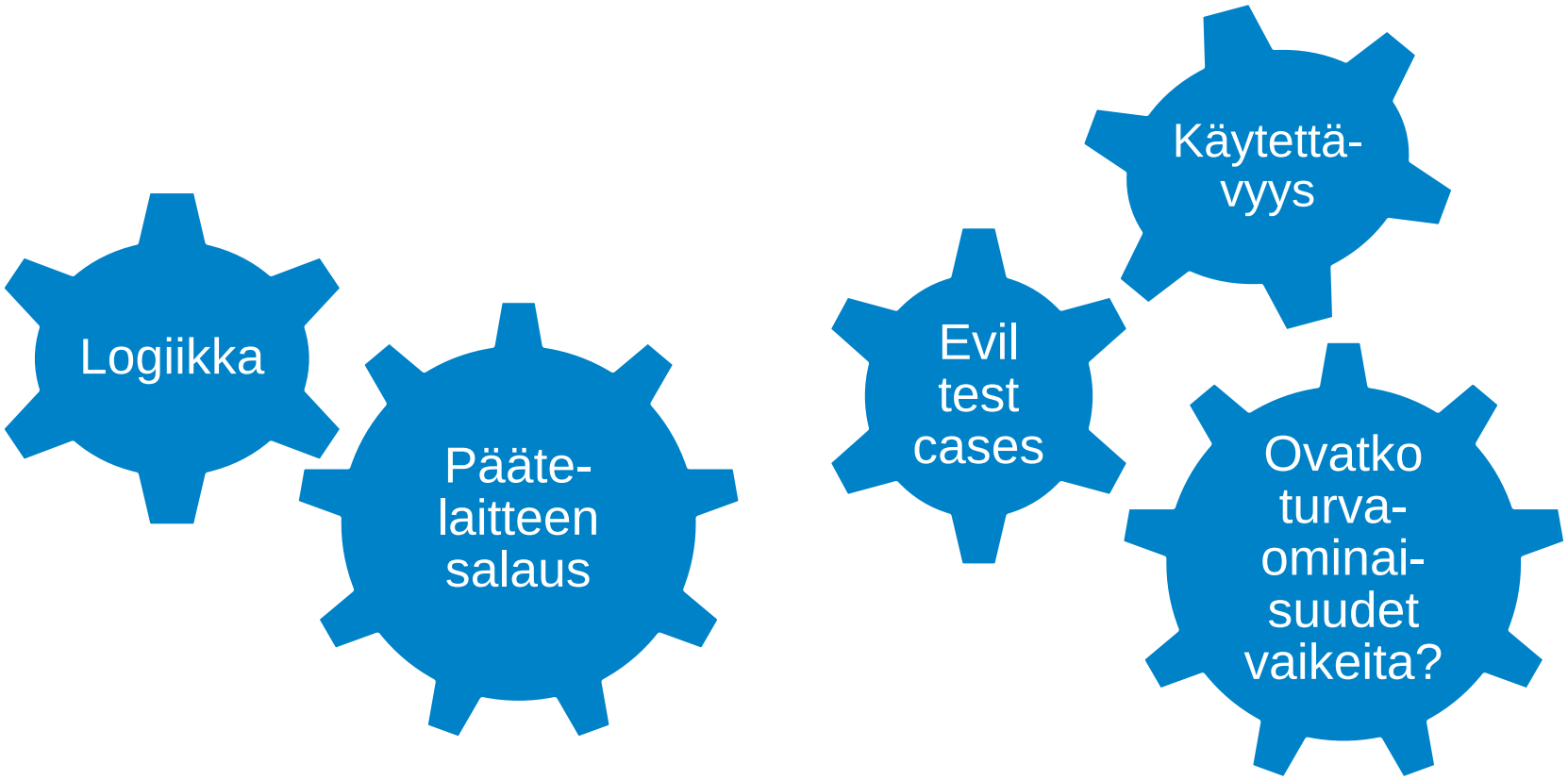
AUTOMATISOI MAHDOLLISIMMAN PALJON

Siten manuaalisessa tietoturvatestauksessa ehtii enemmän ja löytyy mielenkiintoisempia löydöksiä.

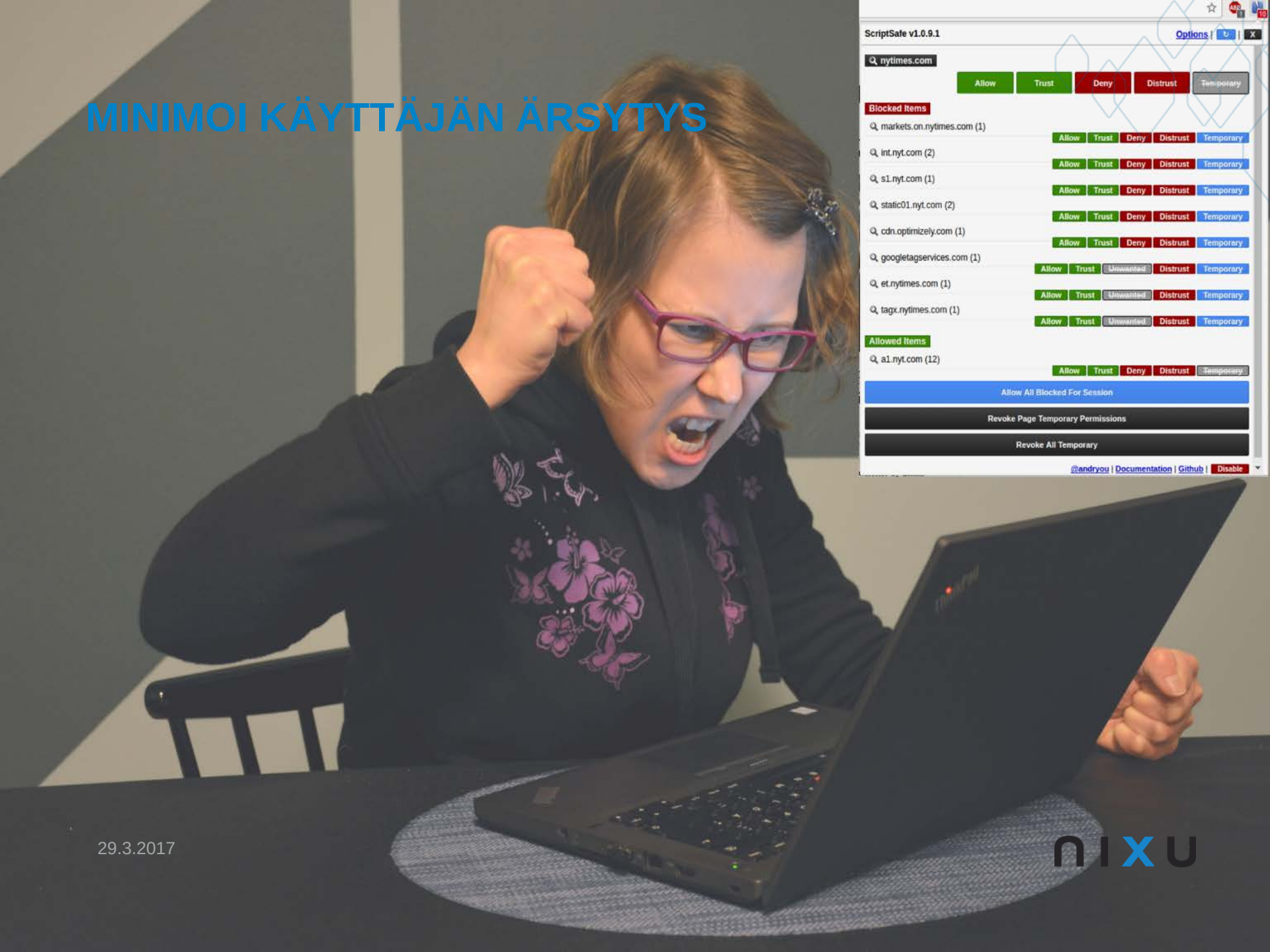
29.3.2017

nixu

TESTAA MONIPUOLISESTI JA ERI NÄKÖKULMISTA



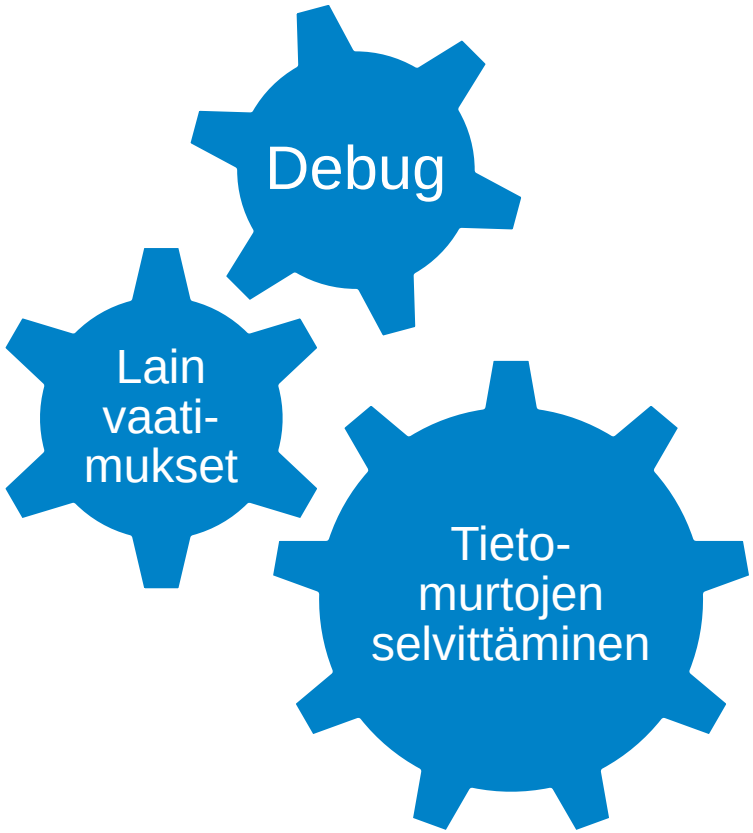
MINIMOI KÄYTTÄJÄN ÄRSYTYS

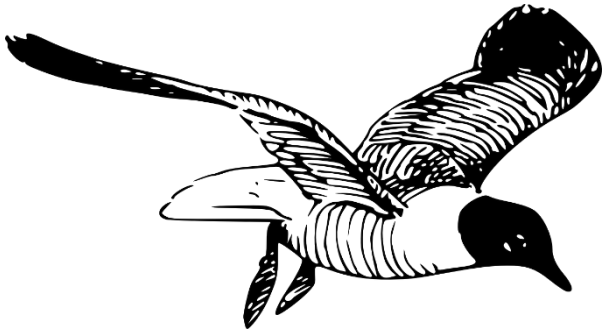


29.3.2017

nixu

MIKSI PITÄÄ LOKITTAA?





nixu

KULTAKUTRIN LOKIENHALLINTA

Lokia ei ole tai se on hyödytöntä

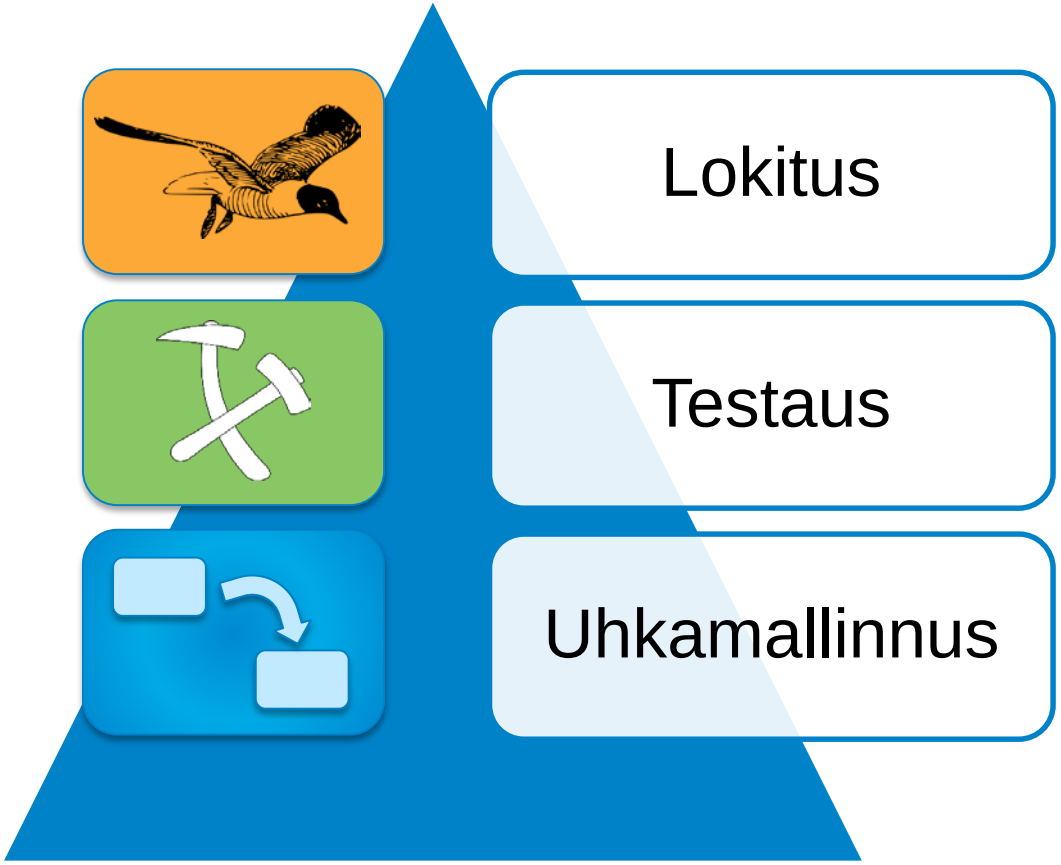
- Kiistämättömyys
- Sanitointi
- Vianselvitys tai tietomurron tutkinta onnistuu
- Synkronoituja

- Gigakaupalla
- Salasanoja, API-avaimia, henkilötietoja
- Irrelevantteja tietoja

nixu

KOLME KEINOA TURVALLISEMPIIN OHJELMISTOIHIN

TUML



nixu

nixu
cybersecurity.

www.nixu.fi

/nixuoy

@nixutigerteam

/company/nixu-oy