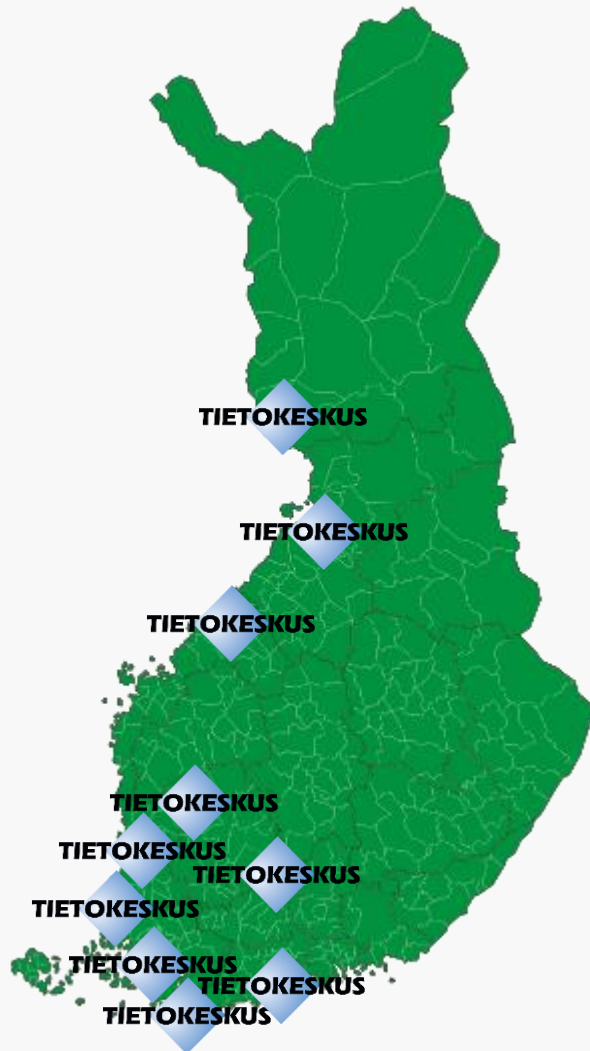


# Tietokeskuksen Tietoturvakartoituspaketit ja niiden selkäranka F-Secure RADAR

Samuli Lindström  
6.4.2017



# TIETOKESKUS



## Tietokeskus on

Suomen läheisin ja nopein,  
teknisesti osaava IT-palvelutalo,  
jonka lähes 200 alan ammattilaista  
ovat palvelleet asiakkaita  
ylivoimaisella huolenpidolla  
jo kolme vuosikymmentä.

Tietotunne	Projektointi	Toiminnanohjaus	Päiväpalvelut	Käintä koulutusilmiä	Linkkaamen luallinta
Konesali	Asiantuntijapalvelut	Laittehuolto	Laittehallinta	Helpdesk	Logistiikka
Tietoliikenne ja verkot	Valvonta	Laitteet ja ohjelmistot	Datan palautus	Lähtäki	Nimetty yhteistyökliö

# Agenda

- Kartoituksen tarkoitus: Mitä kartoitetaan ja miten?
- Kartoituksen tasot
- F-secure Radar

# Kartoituksen tarkoitus

- Näkymä tietoturvan tilaan – suosituksia jatkoon
- Kartoitus ei ole kaiken kattava ja parantava viisasten kivi
- Kartoituskohteet:
  - Verkkoliikenne
  - Verkon haavoittuvuudet (hyökkäyspinta-alan selvitys)
  - Ohjeistus
  - Käytäntö / valvotuneisuus (testihyökkäys)

# Kartoituksen tasot – Taso 1

- Verkkoliikenne
  - Toteutetaan fyysisellä laitteella asiakkaan verkossa – kerätään dataa liikenne mirroraamalla vähintään kaksi viikkoa
  - Raportointi raakadataa analysoimalla
  - Saamme tiedon mitä verkossa liikkuu protokolla- ja ohjelmatasolla. Kartoituksen tuloksena tiedämme onko verkossa paljon asiatonta liikennettä kuten torrentteja tai muuta vastaavaa

# Kartoituksen tasot – Taso 2

- Verkon haavoittuvuudet / hyökkäyspinta-ala
  - Suljetut verkot skannataan fyysisellä laitteella "normaali" verkot pilvipalveluna. Kertaskannaukseen hyvä varata aikaa raportteineen kuukausi.
  - Tuotoksena raportti valmiiksi pureskeltuna raakadatatista (jota esim. meidän ympäristöstä tuhansia sivuja).

# Kartoituksen tasot – Taso 3

- Tietoturva audit - Ohjeistus vs. Käytäntö
  - Auditoidaan asiakkaan tietoturvaa heidän ohjeistuksen, tasojen 1 ja 2 sekä käytännön kannalta haastattelemalla ja vertaamalla tietoturva standardeihin (esim. ISO 27001) huomioiden kevyesti myös fyysistä tietoturvaa
  - Tarvittaessa voidaan myös avustaa sovittaessa asiakasta oman ohjeistuksen luomisessa

# Kartoituksen tasot – Taso 4

- Tietoturvan testaus käytännössä
  - Sovitaan yhdessä etukäteen mitä tietoa koitetaan kalastella ja pyritään kyseinen tieto saamaan loppukäyttäjien kautta käyttämällä kevyitä hyökkäyskeinoja esim. sähköpostitse, puhelimitse, menemällä paikalle häiritsemättä kuitenkaan asiakkaan liiketoimintaa.
  - Tärkeää sopia yhdessä kirjallisesti etukäteen raamit joiden sisällä toimitaan.



# Miten eteen päin?

- Kontaktoi yhteyshenkilösi tahi Samppa

Samuli Lindström

 @lindstromit

#tietoiskuseminaari

samuli.lindstrom@tietokeskus.com