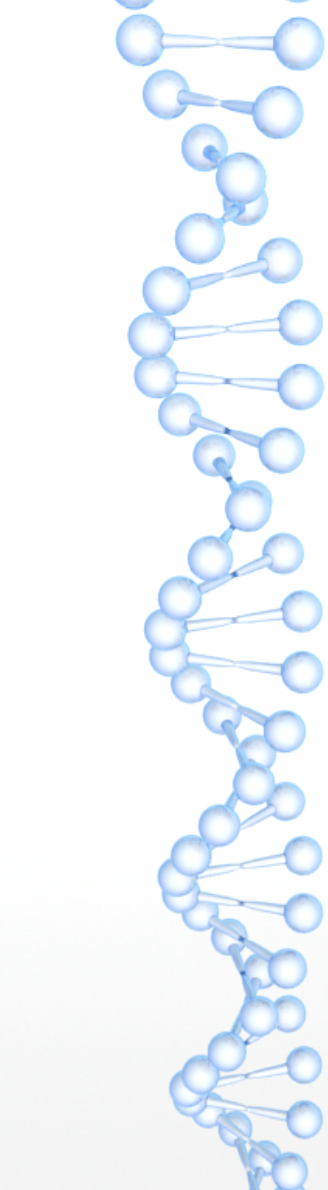
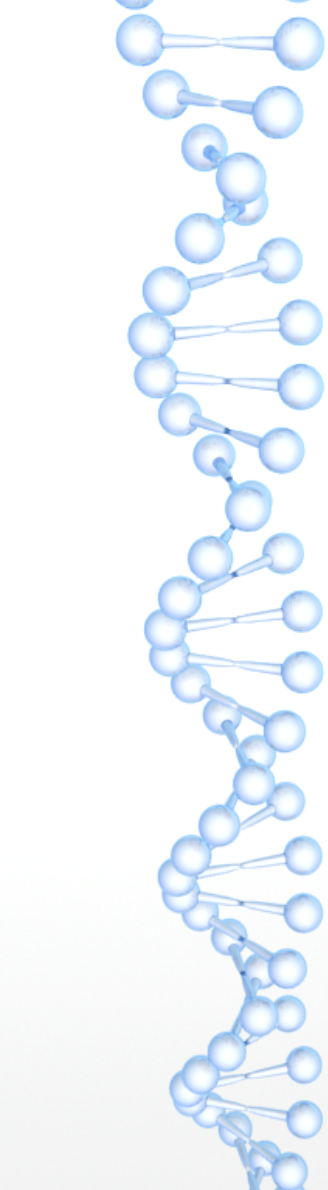


Sensorointi

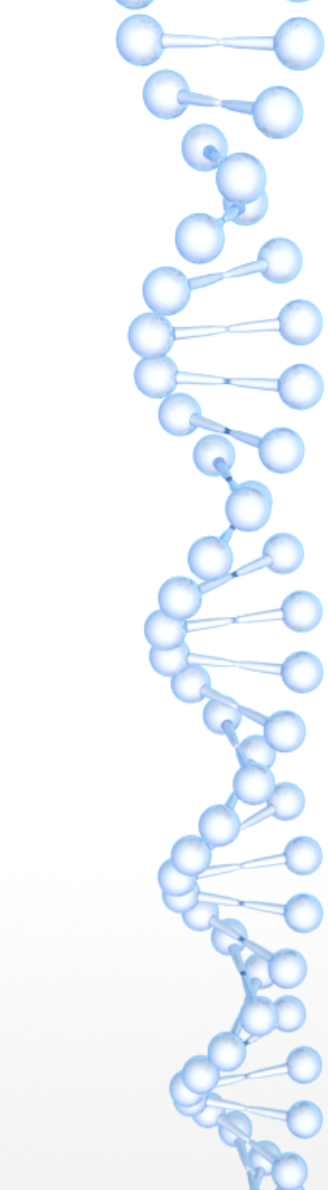
Tuomas Tenkanen

ITKST55



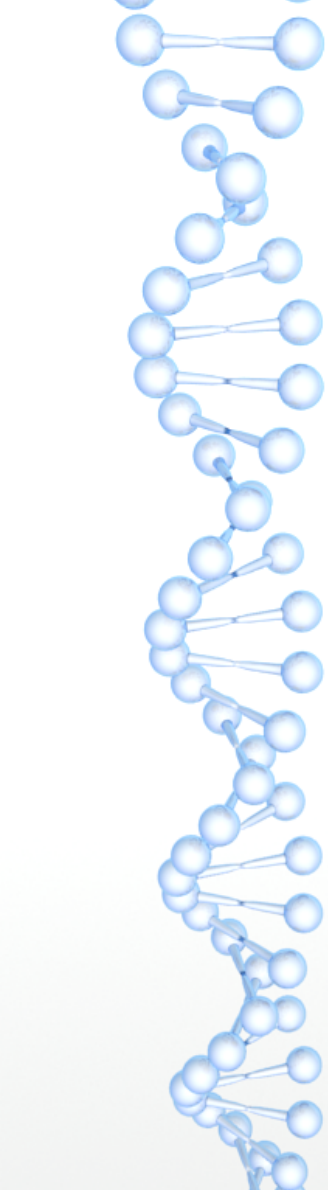
Sensorointi

- Liikenteen lähteet (peilaus, TAPit)
- Sensorit, sensorin instrumentit
    - Suricata, Snort (sääntöpohjainen havainnointi)
    - Zeek (Bro) (protokolla-analyysi)
- Lokikeräimet
- Lokivarasto
- Indeksointi
- Hakutoiminnot
- Näkymät
- Säännöstöt, hälytykset



Lokien käsittelystä

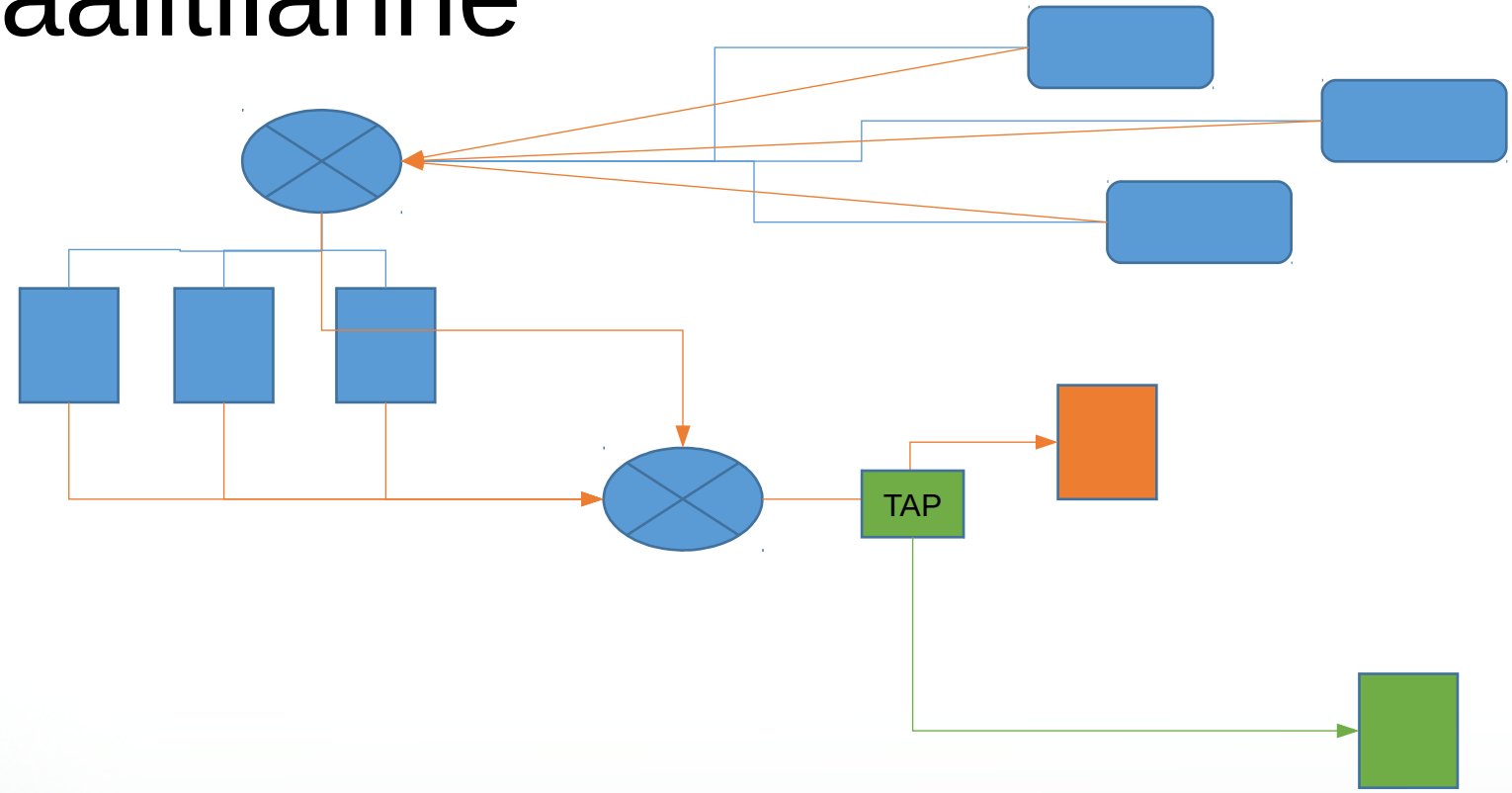
- Lokeja useista lähteistä
  - sensorit, aktiivilaitteet, palomuurit, palvelimet, päätelaitteet
- Rikastaminen
  - yhdistetään eri lähteiden samaa tapahtumaa (-sarjaa) koskevia lokeja
    - joku IP tehnyt jotain epäilyttävää
    - millä koneella (MAC-osoite) ko. IP ollut käytössä
    - kuka käyttäjä ollut kirjautuneena ko. koneelle
- Käsittelyoikeudet: henkilörekisterit, viestinnän tunnistetiedot



Lokien välittäminen varastoon

- **Paikalliset** lokit auttavat **paikallisessa** selvittämisessä
- Keskitetty lokivarasto antaa näkymän koko järjestelmään
  - mahdollisuus tarkastella asioita oudon tapahtuman ympäristöstä sekä ajallisesti että sijainnillisesti
- Lokeja ei pidä välittää käyttöverkossa. Miksi?

Ideaalitilanne



käyttö
hallinta
valvonta

Sensorin sijoittelu

- Mitä halutaan nähdä? Segmentit, palvelut
- Mistä edellinen nähdään?

- Optimal-Sensor-Placement-in-Network-Topology-From-the-Defence-Point-of-View.pdf