Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Lauttatonttu

Loppuraportti

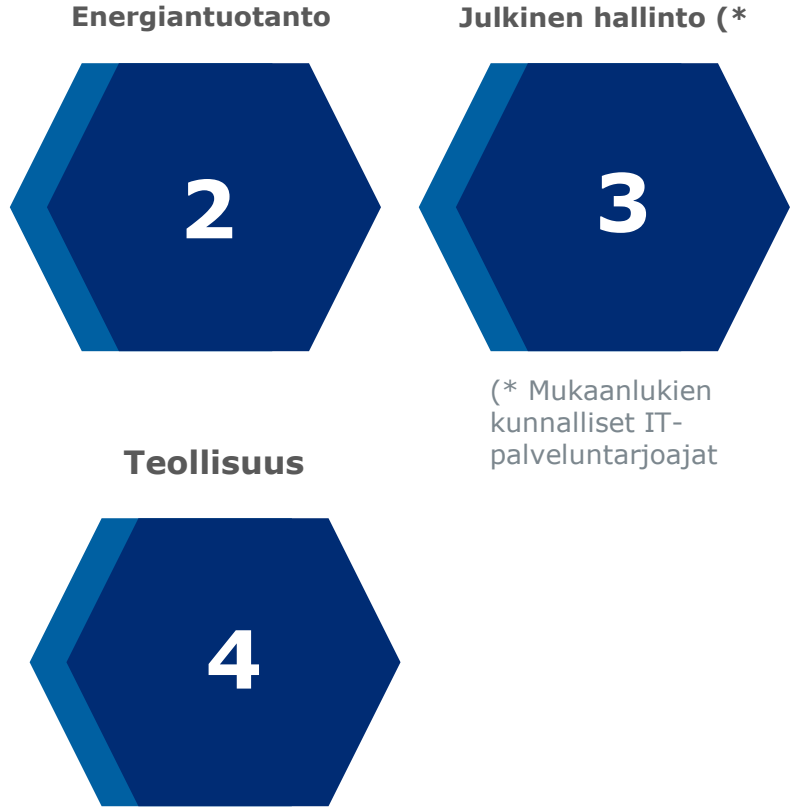
Tiivistelmä

- Lauttatontussa kokeiltiin sisäverkon valvonnan jalkauttamista loppukäyttäjille kevytsensoreiden muodossa.
  - Kokeiltiin vakioituja kyvykkyyksiä (Instrumentteja).
  - Arvioitiin kyselyn pohjalta hyötyjä organisaatioille.
  - Hankittiin kokemuksia laajemman jalkauttamisen varalle.
- Tavoitteena arvioida perusasioiden valvonnan laajamittaista toteutettavuutta sekä tarvittavia kyvykkyyksiä.
- Tulokset olivat rohkaisevia:
  - Sensorikokeiluun osallistui 9 organisaatiota.
  - Osallistujat antoivat kokeilun helppoudesta ja hyödyllisyydestä loistavaa palautetta.
  - Kokeilun perusteella kyselyyn vastanneista organisaatioista 3/5 tarkisti tai korjasi tietoverkkojensa konfiguraatioita.

Lauttatontun osallistujien rekrytointi

- Lauttatonttu- rekrytointi tapahtui osana Kalastajatonttu- kampanjointia.
  - Sopivaksi arvioidut organisaatiot.
  - Tarkka luku joille Lauttatonttu alustavasti esiteltiin ei tiedossa.
- Yksityiskohtainen esittelytapaaminen 14 organisaatiolle.
  - 12 ilmoittautui mukaan.
  - 9 Eteni kokeilun loppuun.

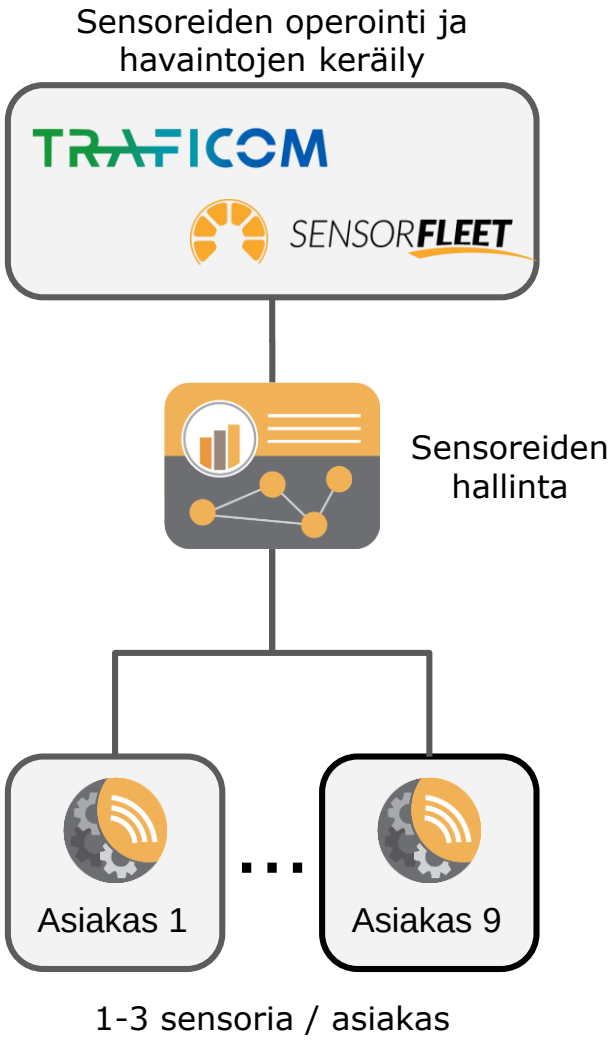
Kokeilun loppuun suorittaneet



TRAFICOM

Kokeilun toteutus ja sisältö

- Sisäverkon valvontaan tarjottiin sekä fyysisiä- että virtuaalisensoreita.
  - Asennettiin 5 rauta- ja 11 virtuaalisensoria, ml. 2 sensoria Azure- ympäristöihin.
- Kokeilussa mukana olleet kyvykkyydet (Instrumentit).
  - Avoimien palveluiden havainnointi ja valvonta.
  - Verkon assettien inventointi ja muutosten valvonta.
  - Lateraaliliikkeen havainnointi (Honeypot).
  - Sisäverkon IDS (Zeek).
  - Haavoittuvuusskannaus (Instrumentti KTK:n haavatarkistusskriptien ajamiseen).



Sensoreiden käyttöönotto ja KTK-yhteistyö

- Sensoreiden käyttöönotto / ohjeiden mukaan toimiminen koettiin helpoksi.
  - Tämä oli erityisen positiivinen löydös ottaen huomioon, että 11/16 sensoreista oli virtuaalisia.

Sensoreiden käyttöönotto

4.7/5

- Kaikki kyselyyn vastanneet ovat valmiita jakamaan sisäverkon havaintotietoja Kyberturvallisuuskeskukselle.
  - Luottamus Kyberturvallisuuskeskukseen on erinomaisella tasolla.
  - 2 vastaajaa ilmoittaa poikkeukseksi yksilöivät tiedot.

Havaintojen jakaminen KTK:lle

Note: Palautteen arvosteluasteikko 1-5. Palautekyselyyn vastasi 6/9 osallistujaa. Yhdessä tapauksessa havaintojen tarkistus on vielä kesken ja näin ollen heidän vastauksensa eivät ole mukana seuraavilla kalvoilla

Kyvykkyydet: Konfiguraatioiden valvonta

- Verkon avoimien palveluiden valvonta koetaan hyödylliseksi.
  - 2/5 kyselyyn vastaajista teki korjauksia tai tarkistuksia havaintojen pohjalta.
  - Valvonta osoittautui toimivaksi automaation hallintaverkoissa.

Avoimien palveluiden valvonta

4.8/5

- Assettien valvonta koetaan hyödylliseksi.
  - 1/5 vastaajista teki korjauksia tai tarkistuksia havaintojen pohjalta.
  - Joissain tapauksissa valvottava verkko ei ollut dynaamisuutensa (esim. toimistoverkko) takia paras mahdollinen valvontakohde.

Assettien valvonta

4.7/5

Kyvykkyydet: Hyökkäysten havainnointi

- Lateraaliliikkeen havainnointi koetaan hyödylliseksi.
  - 2/5 kyselyyn vastaajista tarkistuksia havaintojen pohjalta.
  - Havainnot aiheutuivat sisäisistä haavaskannauksista, mutta osoittivat havainnointimekanismin toimivuuden.
- IDS sisäverkossa.
  - IDS:ää (Zeek) ajettiin suppealla säännöstöllä, joka ei tuottanut havaintoja. Tästä johtuen sitä ei sisällytetty kyselyyn.
  - Menetelmän toimivuus todennettiin ja kevytsensorillakin päästiin hyvään suorituskykyyn (500mbit/s).

Tavoitteet, niiden toteutuminen ja opit

- Kyetäänkö keveitä sisäverkon sensoriratkaisuja jalkauttamaan laajassa mittakaavassa.
  - 9 loppuasiakkaan ja 16 toimitetun sensorin kokemusten pohjalta voidaan todeta, että menetelmät skaalautuvat laajallekin käyttäjäkunnalle.
  - Opit kokeilusta.
    - Tunnistettiin toimitusprosessin osia jotka voidaan ja kannattaa automatisoida.
    - Virtuaalisensorit ovat tärkeässä roolissa jos laajempaan toteutukseen mennään.
    - Asiakkaan palveluntarjoajille täytyy tarjota oma ohjeistuksensa.
- Sisäverkon IDS-valvonnan toteutettavuus.
  - Kokeilun perusteella voidaan todeta, että IDS-valvonta on mahdollista keveilläkin sensoriratkaisuilla
  - Opit kokeilusta
    - Sisäverkon IDS-valvonta vaatii huolellista säännöstön valintaa, joka ottaa valvottavan verkon luonteen huomioon

Tavoitteet, niiden toteutuminen ja opit - 2

- Laajan sisäverkon valvonnan kyvykkyyksien tunnistaminen
  - Assettien, avoimien palvelujen ja lateraaliliikkeen valvonta vaikuttavat soveltuvan suurelle osalle potentiaalisista käyttäjistä
  - Opit kokeilusta
    - Laajemman mittakaavan toteutuksessa tarjottavien kyvykkyyksien täytyy olla vakioidumpia. Kokeilussa ilmeni, että liiallinen valinnanvara hidastaa prosessia
    - Vuosikellomalli, missä kyvykkyysiä lisätään vaihettain, on selvittämisen arvoinen

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus