# Sotealan kyberpoikkeamien tunnistus ja hallinta -projekti

# Projektin tausta ja tarve

Terveydenhuollossa poikkeamat koskettavat laajaa ihmisjoukkoa. Tämän vuoksi terveydenhuollon kyberturvallisuuden tilannekuvaan, havainnointiin ja reagointikykyyn on tarpeen kiinnittää huomiota ja kehittää sitä edelleen.

Vuoden 2023 kansallisen riskiarvion mukaan tieto- ja viestintäverkkojen ja palveluidenhäiriöt on tunnistettu turvallisuuteen kohdistuvaksi uhkaksi.

Projekti kehittää hyvinvointialueiden valmiussuunnitelmia kyberturvallisuuden varautumisen osalta. Sen avulla kehitetään hyvinvointialueiden huoltovarmuutta.

istekki

# Projektin tavoittelemat hyödyt

Istekki tarjoaa palveluita 16 hyvinvointialueelle sekä HUS:lle. Projektiin osallistuu 4 hyvinvointialuetta, joista kolmessa on yliopistollinen sairaala. Istekki Oy haluaa kehittää kansallista sote-sektorin kyberturvallisuutta ja tuottaa projektin avulla tietoa kansallisen kyberturvallisuusvarautumisen kehittämiseen. Huoltovarmuuskeskuksen verkoston avulla projektin tuloksista saadaan julkisia hyviä käytäntöjä ja anonymisoitua tietoa yleisesti saataville

Projekti synnyttää välittömiä hyötyjä osallistujilleen, kun parannetaan kyberhäiriövastetta. Projektin tuloksena syntyy kansallisesti Sotealalle:

- Ymmärrystä tietoturva- ja tietosuojatilannekuvan muodostamiseksi ja häiriöhallintaprosessista
- Esimerkit käyttötapauksien muodostamiseen ja toimintamallit valvontaan
- Ohjeet tietoturvavalvomoon havannointi ja reagointikyvyn parantamiseksi

Mikäli projektin aikana havaitaan puutteita asiakas- ja potilastietojärjestelmien valvonnassa, tiedot toimitetaan sovellustoimittajille puutteiden korjaamista varten. Lisäksi projektin tuloksissa osallistuvat organisaatiot saavat lisäätietoa, jonka avulla he voivat kehittää varautumista ja jatkuvuudenhallintaa.

**Käyttötapausten tunnistaminen**

- Selvitetään mitkä käyttötapaukset ovat kriittisimmät tietoturvatilannekuvan muodostamiseksi

**Käyttötapausten valinta ja dokumentointi**

- Tietoturvavalvomon häiriönhallintaprosessista valitaan ja suunnitellaan 6-8 käyttötapausta


**Ohjeiden luonti ja käyttötapausten määrittely asiakas- ja potilastietojärjestelmään**

- Ohjeet tietoturvavalvomoon havainnointi ja reagointikyvyn parantamiseksi ja käyttötapauksista toteutetaan vähintään 3.

**Tarkastaminen**

- Lopputulosten validointi harjoittelun avulla

# Projektin toteutus

istekki

# Esimerkki käyttötapauksesta

- Haittaohjelmatartunta muistitikulla
- Tekninen tietoturvavalvonta (SOC (SIEM + SOAR + AV)) havaitsee poikkeaman ja käynnistää automaattisesti välittömät vastatoimet (eristäminen) sekä aloittaa tietoturvatutkinnan
- Päätelaitteen tiedoista saadaan tietää kuka on konetta käyttänyt ja kulunvalvonnan tiedoilla varmistetaan, kuka on koneella ollut poikkeaman aikana


# Osallistujat

Projektiin perustetaan ohjausryhmä ja projektiryhmä sekä istekin sisäinen projektiryhmä.

- Hyvinvointialueiden edustajia
- Istekki Oy:n Digiturvapalveluiden tietoturva- ja SOC-asiantuntijat
- Kumppaniverkostosta tarvittava lisäosaaminen
- Traficom Kyberturvallisuuskeskus

# Aikataulu

- Projektisuunnitelman mukainen aikataulu 1.9.2023 – 15.3.2025
- Projektin valmistelutyöt aloitetaan heti ja aikataulua tarkennetaan projektissa
  - Aloitetaan 1.11.2023
- Projektilla on kansallisesti suuri merkitys ja sitä tullaan hyödyntämään viestinnässä projektin aikana
- Jatkossakin tullaan tunnistamaan yhteisiä kehityskohteita ja suunnitellaan niihin rahoitus

| Tehtävä | Kuvaus | Työmäärä ja tekijä(t) | Aikataulu |
|---|---|---|---|
| **Hallinnointi** | Projektin organisointi ja hallinta | 25 htp<br>Projekti- ja ohjausryhmä | 1.9.2023 – 15.3.2025 |
| **Käyttötapausten tunnistaminen** | Selvitetään mitkä käyttötapaukset ovat kriittisimmät tietoturvatilannekuvan muodostamiseksi | 40 htp<br>Projektiryhmä | 1.11.2023 – 22.12.2023 |
| **Käyttötapausten valinta ja dokumentointi** | Tietoturvavalvomon häiriönhallintaprosessista valitaan ja suunnitellaan 6-8 käyttötapausta | 20 htp<br>Projektiryhmä | 3.1.2024 – 29.2.2024 |
| **Ohjeiden luonti ja käyttötapausten määrittely asiakas- ja potilastietojärjestelmään** | Ohjeet tietoturvavalvomoon havainnointi ja reagointikyvyn parantamiseksi ja käyttötapauksista toteutetaan vähintään 3. | 95 htp<br>Projektiryhmä | 1.3.2024 – 19.12.2024 |
| **Tarkastaminen** | Lopputulosten validointi harjoittelun avulla | 5 htp<br>projektiryhmä | 16.1.2025 – 26.1.2025 |
| **Ohjeiden anonymisointi ja julkaisu** | Ohjeiden sekä oppien anonymisointi ja julkaiseminen | 15 htp<br>Projektiryhmä | 29.1.2025 – 15.3.2025 |

istekki

# Kiitos!