Sirtfi-itsearviointi (v1)

HUOM!

Tämä on **Sirtfi v1** ohjeistus. Tämän rinnalle on tullut uudempi Sirtfi v2, jonka käyttö on suositeltavaa. Sen ohjeistus löytyy tä ältä

REFEDS Sirtfi (Security Incident Response Trust Framework for Federated Identity) -kehikolla on ennaltaehkäisevä sekä reaktiivinen vaikutus luottamusverkostossa tapahtuviin tietoturvapoikkeamiin. Ennaltaehkäisevästi toimijat tekevät kehikon mukaisen itsearvioinnin. Reagointi tietoturvapoikkeamiin edellyttää usein ripeää viestintää luottamusverkoston toimijoiden välillä, jonka edistämiseksi toimijat julkaisevat yhteystiedot luottamusverkoston metadatassa.

Palveluorganisaatiot sitoutuvat Haka-luottamusverkostoon liittyessään voimassa olevaan CoCo käytännesääntöön, jossa edellytetään Sirtfi käyttöönottoa.

Lisätietoa: SIRTFI – REFEDS

Sirtfi-itsearviointiprosessi

Organisaatio voi osoittaa toimivansa Sirtfi-kehikon vaatimusten mukaisesti suorittamalla itsearvioinnin. Itsearvioinnin suorittaminen on tarpeellista vain eduGAIN-luottamusverkostoon kuuluvilla organisaatioilla, mutta suositeltavaa kaikille Haka-luottamusverkostoon kuuluvilla organisaatioilla. Itsearviointi tehdään organisaatiokohtaisesti.

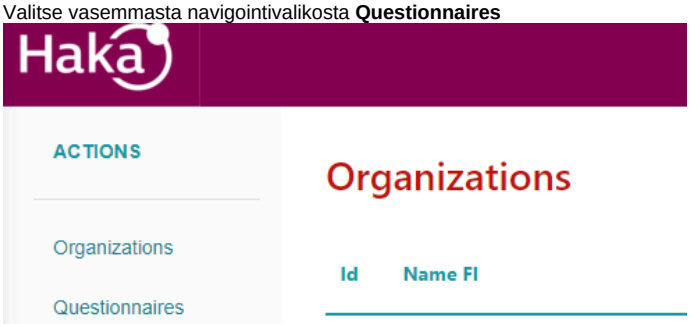
Organisaation edustaja (tietoturvan edustaja tai hallinnollinen yhteyshenkilö) täyttää Sirtfi-lomakkeen, jossa on 18 väittämää. Jos itsearvioinnin kaikkiin väittämiin valitaan vastaukseksi True, organisaatio täyttää Sirtfi-vaatimuksenmukaisuuden (18/18). Tällöin organisaation tunnistuslähteisiin tai palveluihin voidaan tehdä merkintä Haka-resurssirekisterissä Sirtfi-vaatimuksenmukaisuuden osoittamiseksi. Mikäli haluatte päivittää hallinnollisen yhteyshenkilön tai tietoturvan edustajan tietoja, olkaa yhteydessä haka@csc.fi.

Itsearviointia ei tarvitse suorittaa säännöllisesti, vaan Sirtfi-prosessi lähtee oletuksesta, että itsearviointi on ajantasainen. Organisaation vastuulla on huolehtia itsearvioninin ajantasaisuudesta ja päivittää sitä tarvittaessa. Mikäli itsearvioinnin tulos päivityksen jälkeen ei täytä Sirtfi-vaatimuksenmukaisuutta (18/18), on organisaation vastuulla huolehtia, että organisaation tunnistuslähteet / palvelut päivitetään vastaamaan itsearvioinnin tulosta Haka-resurssirekisterissä.

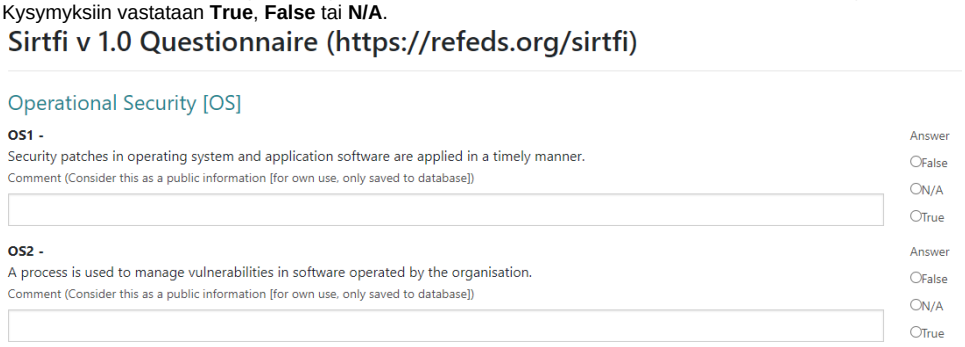
Itsearvioinnin suorittaminen

Mikäli organisaatiosi on jo suorittanut itsearvioinnin, voit siirtyä kohtaan Sirtfi-tiedon päivittäminen resurssirekisterissä IdP:lle / SP:lle

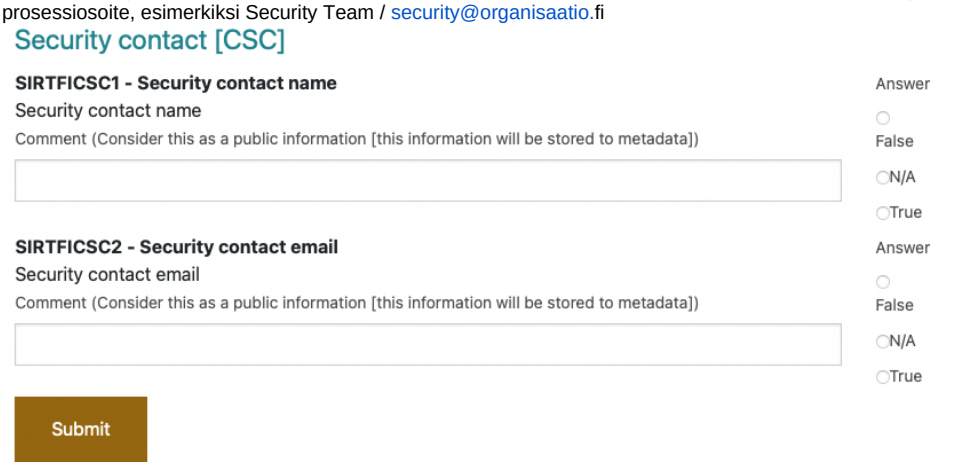
- Kirjaudu osoitteeseen https://rr.funet.fi/haf
- Valitse vasemmasta navigointivalikosta **Questionnaires**



- Itsearviointilomake aukeaa (kuva alla). Lomakkeella on 18 väittämää itsearviointia suorittavan organisaation tietoturvakäytäntöihin liittyen. Kysymyksiin vastataan **True**, **False** tai **N/A**.



- Lomakkeen lopussa kysytään yhteystietoja tietoturva-asioihin liittyen. Täytä osoitteeseen nimi ja sähköpostiosoite. Osoite pitäisi olla ns. prosessiosoite, esimerkiksi Security Team / security@organisaatio.fi

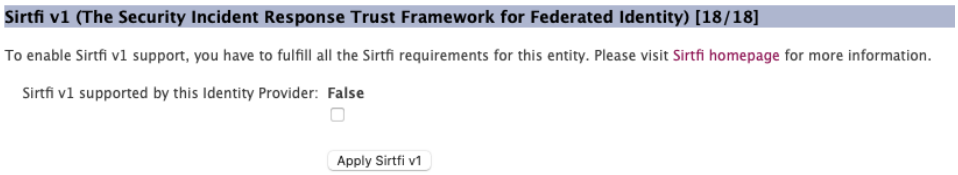


- Paina lopuksi Submit.
- Organisaation osalta Sirtfi-kysely on suoritettu ja voidaan siirtyä seuraavaan kohtaan.

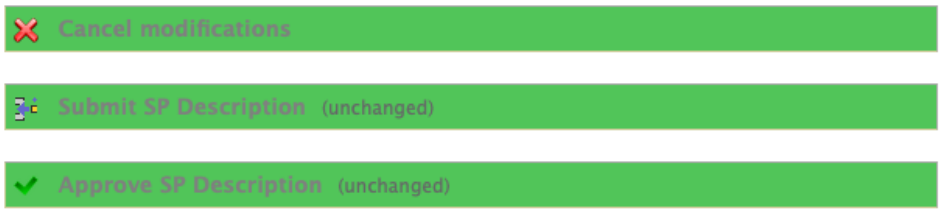
Sirtfi-tiedon päivittäminen resurssirekisterissä IdP:lle / SP:lle

Kun Sirfi-kysely on täytetty, tunnistuslähteen tai palvelun ylläpitäjä voi Haka-resurssirekisterissä päivittää tiedon Sirtfi-kehikon mukaisten tietoturvakäytäntöjen noudattamisesta haluamissaan tunnistuslähteissä tai palveluissa.

- Kirjaudu Haka-resurssirekisteriin
- Avaa Manage IdPs tai Manage SPs ja avaa haluamasi IdP / SP
- Päivitä merkintä Sirtfi tuesta. Mikäli organisaatiosi ei ole vielä suorittanut itsearviointia, valinta on harmaana.



- Tallenna muutokset painamalla **Apply Sirtfi v1**
- Tallenna muutospyyntö painamalla **Submit IdP / SP Description**



- Haka-operaattori hyväksyy muutoksen ja se **julkaistaan eduGain-metadataan seuraavan metadatapäivityksen yhteydessä**.
- Tarkista vielä muokatun IdP:n eduGain-säännöt, mikäli haluat suodattaa eduGain-metadasta vain palvelut, jotka ovat Sirtfi-vaatimuksenmukaisia. (ks. Ohje)