

Osaamiskartoituskysely (Microsoft Forms):

Sote-alan ammattilaisten kyberturvallisuusosaaminen

Kyselyn käyttöohjeet

Kohderyhmä ja toteutus:

1. Kohderyhmä:

- Kysely on suunnattu sote-alan ammattilaisille, kuten hoitajille, lääkäreille, sosiaalityöntekijöille, fysioterapeuteille ja hallinnon henkilöstölle.
- Kysely soveltuu erityisesti henkilöstölle, joka käsittelee arkaluonteisia tietoja työssään ja/tai käyttää digitaalista teknologiaa osana työtehtäviään.
- Vastaajilta ei edellytetä erityistä teknistä osaamista – kysymykset on muotoiltu selkeästi ja ymmärrettävästi.

2. Toteutustapa:

- **Perustiedot:** alkuun voidaan lisätä perustiedot (esim. vastaajan vastuualue, ikä, sukupuoli tms. mikäli se on tarpeen).
- **Sähköisesti:** Suositellaan toteutettavaksi verkkokyselynä (Microsoft forms), jonka voi täyttää helposti tietokoneella tai mobiililaitteella.
- **Paperilomake:** Vaihtoehtoisesti kysely voidaan tulostaa ja jakaa paperiversiona esimerkiksi tiimipalavereissa.
- **Termistö:** Mikäli organisaatio käyttää esim. termiä digitaalinen kyberturvallisuus (kyberturvallisuus termin sijasta) kannattaa termistön osalta tehdä räätälöintiä, jotta kysely on organisaation linjan mukainen.
- Vastaaminen vie aikaa noin 10–15 minuuttia.

3. Tietosuoja:

- Kyselyn vastaukset käsitellään luottamuksellisesti, ja niitä käytetään vain osaamisen kartoittamiseen ja kehittämistoimien suunnitteluun.
- Kyselyyn vastataan anonymisti.

Tulosten analysointi ja raportointi

1. Tiimien ja osastojen analyysi:

- Tulosten avulla voidaan kartoittaa, miten tiimien ja osastojen osaaminen jakautuu.
- Lisäksi voidaan tunnistaa osa-alueet, joissa on eniten yhteisiä kehittämis- ja koulutustarpeita.

2. Organisaatiotason arviointi:

- Tulosten avulla organisaatio saa kokonaiskuvan henkilöstön kyberturvallisuusosaamisesta.
- Tulosten avulla organisaatio pystyy tunnistamaan vahvuudet sekä keskeiset riskialueet, joissa lisäkoulutus tai tekniset toimet voivat olla tarpeen.

3. Tulosten esittäminen:

- Microsoft Forms luo raportin tuloksista, joka sisältää selkeitä kaavioita. Raportti voidaan viedä Exceliin jatkotyöstettäväksi. Myös yksittäisen vastaajan tulokset on mahdollista nähdä (mutta vastaajaa ei voida tunnistaa).
- Formsin raporttia voidaan käyttää strategisen päätöksenteon tukena esimerkiksi koulutussuunnitelmien tai resurssien kohdentamisen osalta.

Kyselyn tulosten hyödyntäminen

1. Koulutusten suunnittelu:

- Kyselyn tulosten pohjalta voidaan suunnitella kohdennettuja koulutuksia (liittyen esimerkiksi kyberuhkien tunnistamiseen).

2. Tietoturvakäytäntöjen kehittäminen:

- Hyödynnä tuloksia organisaation tietoturvapoliitiikan päivittämisessä ja henkilöstön ohjeistuksessa (esimerkiksi lisäohjeet potilastiedon tietoturvalliseen käsittelyyn tai uhkatilanteiden raportointiin).

3. Toimintatapojen arviointi:

- Selvitä, miten hyvin nykyiset käytännöt tukevat turvallista toimintaa ja missä tarvitaan muutoksia (esimerkiksi onko henkilöstölle selvää, miten etätöissä toimitaan tietoturvallisesti).

4. Riskienhallinta:

- Käytä tuloksia osana organisaation riskienhallintaa tunnistamalla henkilöstöön liittyvät kyberturvariskit.

- Kohdenna resurssit tehokkaasti niiden riskien ehkäisemiseen, jotka voivat vaikuttaa kriittisesti organisaation toimintaan.

5. Seuranta ja jatkuva parantaminen:

- Toista kysely säännöllisesti (suositus: vuosittain) seurataksesi henkilöstön osaamisen kehitystä ja kyberturvallisuustoimien vaikuttavuutta.
- Vertaa eri ajankohtien tuloksia ja tarkastele kehitystrendejä.