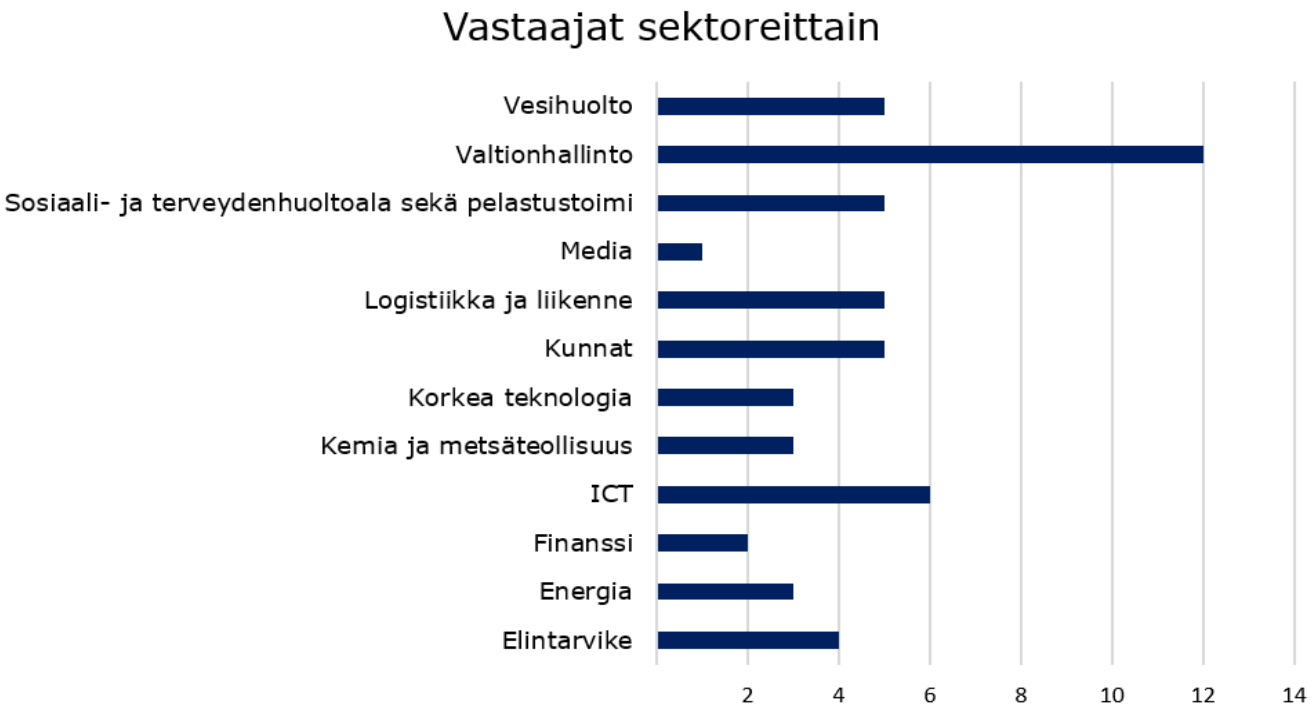
Liite: Laajat tulokset



N=54

Kyselyyn vastasi yhteensä 54 eri organisaation edustajaa. Kyselyn tulokset ovat suuntaa antavia.

Vastaajista 90 % oli käytössään tekoälyratkaisuja

- Yksikään vastaajista ei ole ottanut tekoälyratkaisuja käyttöön, ja sen jälkeen luopunut niistä.
- Tekoälyä hyödyntävistä vastaajista 29 % käyttää tekoälyratkaisuja ydinliiketoiminnalle kriittisissä käyttötapauksissa, 92 % ei-kriittisissä.
- Vastaajista 91 % suunnittelee ottavansa käyttöön uusia tekoälyratkaisuja. 47 % suunnittelee ottavansa käyttöön tekoälyratkaisuja ydinliiketoiminnalle kriittisissä käyttötapauksissa.
- Vastausten perusteella tekoälyratkaisut tulevat yhdistymään tulevaisuudessa yhä vahvemmin yhteiskunnalle kriittisiin toimintoihin.

Tekoälyä hyödyntävistä vastaajista 98 % käytti avustajia

- Valtaosa vastaajista hyödyntää tekoälyavustajia, kuten chatbotteja.

- Vastaajista 19 %hyödyntää autonomisia järjestelmiä, kuten tekoälyagentteja, jotka voivat tehdä itsenäisiä päätöksiä.

Vastaajista 35 % ei ole varmuutta, onko tekoäly otettu käyttöön turvallisesti

- Vastaajista 80 % on käyttöpolitiikka ja 48 % tekoälystrategia (tai tekoäly on osa jotain laajempaa strategiaa).
- Vastaajaorganisaatioista 17 % ei ole käyttöpolitiikkaa, hallintamalleja tai strategiaa.
- Vastaajista 65 % kokee, että tekoäly on otettu organisaatiossa käyttöön turvallisesti
- Monessa organisaatiossa tekoälyn käyttöä ohjataan käytännön tasolla, mutta kokonaisvaltainen strateginen johtaminen puuttuu. Riskit kasvavat erityisesti silloin, kun tekoälyä hyödynnetään kriittisissä toiminnoissa ilman selkeää hallintamallia.

Vastaajista 41 % on uhkamallintanut tekoälyjärjestelmänsä

- Vastaajista 41 % on käytössä tekoälyjärjestelmiä suojaavia teknisiä ratkaisuja.
- Vastaajista 28 % kokee, että organisaatiossa on riittävästi osaamista tekoälyn kyberturvallisuudesta.
- Vastaajaorganisaatioissa 25 % on rekrytoitu tai koulutettu erityisesti tekoälyn kyberturvallisuuden osaajia.
- Vastaukset viittaavat siihen, että tekoälyä otetaan käyttöön nopeammin kuin siihen liittyviä turvallisuusosaamista ehditään kehittää.

Vastaajista 51 % on ottanut tai suunnittelee ottavansa käyttöön uusia tekoälyratkaisuja kyberturvallisuuden parantamiseksi

- Tekoälyratkaisuja hyödynnetään muun muassa haavoittuvuuksien hallinnan automatisoinnissa sekä uhkien havainnoinnissa.

Vastaajista 28 % on havainnut organisaatioon kohdistettuja tekoälyllä toteutettuja hyökkäyksiä.

- Havaitut tapaukset liittyivät pääosin tekoälyavusteiseen kalasteluun, mikä on tällä hetkellä näkyvin ja helpoimmin tunnistettava tekoälyn hyödyntämistapa hyökkäyksissä.

- Vastaajista 72 % ei ole havainnut tekoälyllä tehtyjä hyökkäyksiä. Avoimissa vastauksissa korostettiin, että on vaikeaa todentaa tekoälyn käyttöä hyökkäyksissä.