

5 oppia: Kyberturvallisuus tekoälyn aikakaudella

AI Finland ja Kyberala ry kokosivat yhteen kyberalan asiantuntijoita keskustelemaan tekoälyn tuomista mahdollisuuksista ja riskeistä kyberturvallisuuden näkökulmasta. Kokosimme **viisi keskeistä oppia** keskustelusta.

1. Hallintamallit ovat kriittisiä tekoälyn turvalliselle hyödyntämiselle

- Tekoälyn nopea kehitys ja organisaatioiden kilpailupaineet johtavat usein siihen, että turvallisuutta ja ohjeistusta lykätään myöhemmäksi.
- Hallintamallin avulla voidaan turvata vastuullinen käyttö ja varmistaa, että ihmiset ymmärtävät sekä teknologian rajoitteet että vastuut.

Oppi:

Tekoälyn hallitsematon käyttö voi altistaa organisaatiot sekä eettisille että teknisille riskeille. Tekoälyn hallintamalli tukee vastuullista käyttöä tuomalla valvontarakenteet, vastuut ja viitekehyksen.

2. Agenttipohjainen tekoäly tuo mahdollisuuksia, mutta on tietoturvan ja kyberturvallisuuden näkökulmasta nouseva riski ja valvontahaaste

- Käyttöoikeuksien hallinta ja valvonta monimutkaistuvat, kun tekoäly kykenee itse luomaan uusia toimintapolkuja.
- Tekoälylle tulee toteuttaa tiukat ja selkeät rajoitteet, joita kyetään valvomaan. Valvontaan voidaan käyttää toista tekoälyä.
- Tekoälyn tekemät toimet pitää kyetä valvomaan vastaavasti kuin ihmiskäyttäjän tekeminen.

Oppi:

Agenttipohjainen tekoäly kasvattaa valvonnan ja käyttöoikeuksien hallinnan vaatimuksia, ja vaatii uudenlaisia identiteetin- ja pääsynhallinnan innovaatioita.

5 oppia: Kyberturvallisuus tekoälyn aikakaudella

AI Finland ja Kyberala ry kokosivat yhteen kyberalan asiantuntijoita keskustelemaan tekoälyn tuomista mahdollisuuksista ja riskeistä kyberturvallisuuden näkökulmasta. Kokosimme **viisi keskeistä oppia** keskustelusta.

3. Ihmiset ja kulttuuri ovat suurimmat riskitekijät, ei teknologia

- Riskit liittyvät kiireeseen, riittämättömään ohjeistukseen ja siihen, että tekoälyä otetaan käyttöön ilman ymmärrystä sen vaikutuksista.
- Erityisesti **demokratisoitunut teknologia** mahdollistaa laajamittaisen käytön, mutta myös virheet ja väärinkäytön. **Muutosjohtaminen ja koulutus** ovat kriittisiä tekoälyn vastuullisessa käyttöönotossa.

Oppi:

Tekoälyn käyttöönotossa suurimmat riskit liittyvät usein ihmisiin – osaamisen kehittäminen ja kulttuuri ovat tehokkain suoja teknisiä riskejä vastaan.

4. Tekoäly oikein toteutettuna voi toimia tehokkaana työkaluna kyberuhkien torjunnassa

- Esimerkiksi palautemekanismit ja valvotut agentit voivat auttaa tunnistamaan ja neutraloimaan uhkia nopeasti. Tekoäly voi analysoida suuria datamääriä, löytää poikkeamia ja automatisoida tietoturvalvontaa.
- Kyberuhkien torjunnassa tekoälyratkaisujen on oltava rajattuja, kontekstisidonnaisia ja kontrolloituja; ”kaiken kattavat” mallit aiheuttavat enemmän haittaa kuin hyötyä.

Oppi:

Tekoäly voi parantaa kyberturvaa, mutta vain jos sen toiminta on rajattu, valvottu ja sille asetetaan selkeät palautekanavat ja vastuupisteet.

5. Laatu ja tarkoituksenmukaisuus ovat tärkeämpiä kuin nopeus ja tehokkuus

- **Tekoälykehitystä ohjaa liiallinen tehostamisen logiikka**, jossa laatu ja eettisyys jäävät taka-alalle. Tekoälystä tulisi hakea **kasvua ja laatua**, ei pelkästään tehokkuutta.
- Vastuullinen käyttöönotto ja pitkäjänteinen hyödyntäminen voivat tuottaa kilpailuetua niille, jotka eivät sorru pelkkään nopeuden illuusioon.

Oppi:

Kestävän tekoälyn käytön lähtökohta on laatu, ei tehokkuus. Todellinen kilpailuetu syntyy vastuullisuudesta ja hallitusta kehityksestä, ei nopeasta implementoinnista.