Oliver Vahokoski

TEKOÄLYN POTENTIAALI ORGANISAATIOIDEN TIETOTURVAN HALLINNASSA

Johtamisen ja talouden tiedekunta
Yrityksen johtaminen, kandidaatin tutkielma
Ohjaaja: Kari Lohivesi
Toukokuu 2024

TIIVISTELMÄ

Oliver Vahokoski: Tekoälyn potentiaali organisaatioiden tietoturvan hallinnassa
Kandidaatin tutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma, yrityksen johtaminen
Toukokuu 2024

Tämän tutkimuksen tavoitteena oli selvittää, millainen potentiaali laajoilla kielimalleilla on organisaatioiden tietoturvan hallinnassa. Tarkoituksena oli kartoittaa kielimallien käyttömahdollisuuksia sekä käyttöönoton haasteita tietoturvan hallinnassa. Laajat kielimallit, jotka ovat eräs tekoälyn sovellusmuoto, kykenevät käsittelemään ja generoimaan erilaisia tekstejä. Tietoturvan hallinnalla pyritään suojaamaan organisaation tiedot varmistamalla tietojen saatavuus, eheys ja luottamuksellisuus. Sekä kielimallit että tietoturvan hallinta ovat tutkimusalueina merkittävässä murrosvaiheessa teknologian kehittymisen vuoksi. Tämän tutkimuksen toteuttaminen koettiin perustelluksi, koska kielimallien osuutta tietoturvan hallinnassa on tutkimuskirjallisuudessa käsitelty varsin niukasti.

Tutkimusaihetta käsittelevä kirjallisuus koostui pääosin vertaisarvioiduista akateemisista artikkeleista. Kirjallisuuskatsaus toteutettiin narratiivisena ja se käsiteltiin kolmessa osassa. Ensin kartoitettiin tietoturvan hallintaa yleisellä tasolla, minkä jälkeen perehdyttiin laajojen kielimallien ominaisuuksiin ja haasteisiin. Kirjallisuuskatsauksen päätteeksi tarkasteltiin vielä kielimallien hyödyntämistä tietoturvan hallinnassa. Kirjallisuuskatsauksen avulla laadittiin tutkielmalle teoreettinen viitekehys. Tutkimusaiheen luonteen vuoksi tutkimusmenetelmäksi valikoitui laadullinen tutkimus. Empiirinen aineisto perustui kahteen teemahaastatteluun, joissa asiantuntijoilta kysyttiin näkemyksiä kielimallien potentiaalista tietoturvan hallinnasta. Haastattelut litteroitiin ja dokumentoitiin tutkielman empiirisessä osassa, jonka jälkeen aineistoa analysoitiin suhteessa kirjallisuuskatsauksessa esiin nousseisiin aihealueen pääkohtiin.

Tutkimuksen tulokset mukailivat pääsääntöisesti kirjallisuuskatsauksessa tehtyjä havaintoja. Kielimallien todettiin olevan tekstinkäsittelyä tehostavia työkaluja, jotka kykenevät tuottamaan varsin yksityiskohtaista tekstiä, analysoimaan suuria datamääriä sekä avustamaan ideoinnissa. Näitä kykyjä voidaan hyödyntää muun muassa tietoturvapolitiikkojen luomisessa, raporttien kirjoittamisessa, räätälöityjen koulutusmateriaalien laatimisessa, osittaisessa prosessien automatisoinnissa sekä tietoturvallisen ohjelmistokoodin tuottamisessa. Toisaalta tutkimuksessa ilmeni myös kielimallien hyödyntämiseen liittyviä haasteita. Sensitiivisen datan käsittely tekoälyn kanssa herättää epäluottamusta, ja kielimallien käyttöönottoon on iso digitalisaatiokynnys.

Tämän tutkimuksen perusteella kielimalleilla on potentiaalia avustaa organisaatioita työn tehostamisen työkaluna. Tutkimus tarjoaa näkökulmia kielimallien käyttömahdollisuuksista organisaatioiden tietoturvan hallintaan sekä käsittelee sen käyttöönottoon liittyviä haasteita ja rajoituksia.

Avainsanat: tietoturva, tietoturvan hallinta, tekoäly, kielimallit

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Tutkimuksen tausta

Viime vuosikymmenten teknologiset saavutukset ovat muovanneet tuntemaamme maailmaa valtavasti. Etenkin tietokoneiden ja internetin yleistyminen on vaikuttanut kaikkiin organisaatioihin ja yksilöihin, tarjoamalla uusia mahdollisuuksia eri toimintoihin kuten maksuliikenteeseen tai asiakirjojen säilyttämiseen. Tiedonhallinta on muuttunut helpommaksi, esimerkiksi mahdollistamalla tiedon samanaikaisen käsittelyn useassa paikassa. Tämä kehitys on avannut uusia ovia myös tietoturvauhkille, mikä tekee yritysten tietoturvan hallinnasta yhä tärkeämmän osan liiketoimintaa. Teknologian nopean kehityksen myötä yritysten tiedonhallinta ja tietoturva eivät ole pelkästään helpottuneet, vaan myös muuttuneet yhä haasteellisemmaksi (Singh ym., 2014). Tämä johtuu muun muassa siitä, että teknologian kehittyessä eri järjestelmät ja prosessit muuttuvat yhä monimutkaisemmiksi kehityksen avaten uusia hyökkäysväyliä ja antaen hyökkääjille työkalut yhä innovatiivisempiin metodeihin (Berman, ym., 2019, 1). Tietoturva on yrityksille entistä tärkeämpää, sillä ne toimivat kansainvälisillä markkinoilla ja ovat syvästi riippuvaisia tietotekniikasta. Tämä riippuvuus korostuu, kun yritysten toiminta on siirtynyt lähes kokonaan verkkoon ja digitaaliseen muotoon. (Antunes ym., 2021).

OpenAI:n julkaistua yleisölle laajan kielimallin, ChatGPT:n, loppuvuodesta 2022, keskustelu laajojen kielimallien potentiaalista on kiihtynyt, ja monet ovat alkaneet hyödyntää tätä teknologiaa päivittäisessä työskentelyssä. Tekoäly on yleistynyt nopeasti ja nykyään sitä käytetäänkin lähes jokaisella toimialalla (Okey ym., 2023). Laajojen kielimallien yleistyminen tuo tietoturva-alalle samanaikaisesti niin haasteita kuin mahdollisuuksia (Iqbal ym., 2023). Vaikka ne mahdollistavat tehokkaampien kyberhyökkäysten toteuttamisen, kuten uskottavampien huijausviestien luomisen ja haittaohjelmien kirjoittamisen, tarjoavat ne myös keinoja kyberpuolustuksen vahvistamiseen (Okey ym., 2023; Gupta ym., 2023).

Vaikka ChatGPT:n ja muiden laajojen kielimallien vaikutusta tietoturvaan on jo jonkin verran tutkittu, tutkimukset ovat keskittyneet sekä kielimallien itsensä muodostamiin uhkiin että niiden kautta luotaviin uusiin tietoturvauhkiin, kuten kehittyneisiin

tietojenkalasteluviesteihin (Okey ym., 2023). Joissain tutkimuksissa, kuten McKee & Noever (2022) ja Al-Hawawreh, Aljuhani, & Jararweh (2023), on tarkasteltu laajojen kielimallien kykyä kirjoittaa tietoturvallisempaa ohjelmistokoodia, mutta laaja-alaisesti kielimallien potentiaalista tietoturvan hallinnassa ei ole vielä merkittävästi tutkittu. Tämä osoittaa, että tutkimuskentässä on selkeä aukko kielimallien puolustuksellisessa potentiaalissa, tarjoten mahdollisuuksia aiheen syvemmälle tutkimiselle.

1.2 Tutkimuksen tavoite ja tutkimustehtävä

Tämän työn *tutkimustehtävänä on selvittää laajojen kielimallien potentiaalia organisaatioiden tietoturvan hallinnassa.*

Tutkimustehtävään pyritään vastaamaan tutkimalla aihetta käsittelevää aiempaa kirjallisuutta, sekä haastattelemalla asiantuntijoita ja peilaamalla heidän näkemyksiään kirjallisuudessa esitettyyn tietoon. Tutkimus painottaa haastatteluista saatavaa aineistoa, sillä aiheen aikaisempaa kirjallisuutta on saatavilla niukasti. Tutkimuksen tavoitteena ei ole tarjota ohjeita tietoturvan hallinnan parantamiseksi, vaan nostaa esille huomioita kielimallien tuomasta potentiaalista sekä kartoittaa niiden käyttöönottoon liittyviä haasteita.

Tutkimuksessa keskitytään erityisesti laajojen kielimallien käyttöön tietoturvan hallinnassa, eikä käsitellä muita tekoälyn sovellusalueita. Lisäksi tutkimus keskittyy organisaatioiden näkökulmaan, jättäen yksilöiden tietoturvan tarkastelun vähemmälle huomiolle. Tämä rajaus auttaa syventämään ymmärrystä nimenomaan organisaatiotason tietoturvahaasteista ja -ratkaisuista.

1.3 Keskeiset käsitteet

Koneoppiminen on prosessi, jossa järjestelmät oppivat datasta tai kokemuksista laskennallisten tekniikoiden avulla. Se hyödyntää tilastollisia menetelmiä mallinteiden löytämiseksi olemassa olevasta datasta, joita käytetään ennusteiden tekemisessä. Toisin kuin perinteisessä tietokoneohjelmoinnissa, jossa ohjelmoija määrittelee logiikan tarkasti, koneoppimismallit oppivat ja paranevat ajan myötä, ja niitä voidaan optimoida uudella datalla ilman, että niitä kirjoitetaan uudelleen. (Suomen Standardisoimisliitto, 2023b).

Tietoturvastandardi on virallinen ohjeistus tai normisto, joka määrittelee vaatimukset ja parhaat käytännöt tietoturvan hallintaan ja suojaamiseen organisaatiossa (National Institute of Standards and Technology, 2020).

ISO/IEC 27001 on tunnetuin ja globaalisti käytetyin tietoturvastandardi, joka kuvaa vaatimukset tietoturvallisuuden hallintajärjestelmälle. Se luo puitteet tietoturvan sekä sen riskien hallintaan. (Ilmonen ym., 2022).

OpenAI on yhdysvaltalainen tutkimusorganisaatio, joka keskittyy tekoälytutkimukseen. Tutkimuksen keskiössä on etenkin generatiivinen tekoäly. OpenAI on julkaissut useita eri tekoälysovelluksia, kuten ChatGPT:n ja DALL-E:n. (Alto, 2023).

ChatGPT on OpenAI:n loppuvuodesta 2022 julkaisema keskustelubotti, joka perustuu GPT-kielimalleihin. ChatGPT kykenee ymmärtämään ja tuottamaan tekstiä saamiensa syötteiden perusteella, ja se hyödyntää edistyneitä koneoppimistekniikoita suoriutuakseen erilaisista luonnollisen kielen käsittelytehtävistä, kuten kysymyksiin vastaamisesta, selitysten antamisesta ja vuoropuheluun osallistumisesta. (Alto, 2023).

GDPR, eli EU:n yleinen tietosuoja-asetus, asettaa tiukat säännöt henkilötietojen käsittelylle ja korostaa yksilöiden oikeuksia hallita omia tietojaan. GDPR velvoittaa organisaatioita noudattamaan tiettyjä periaatteita, kuten tietojen minimointia, läpinäkyvyyttä ja tietoturvaa. (European Parliament and Council of the European Union, 2016).

Kirjallisuudessa tekoälyyn viittaus on varsin epätasaista, ja vakiintunutta termistöä ei ole vielä muodostunut. Siksi, kun tässä tutkimuksessa puhutaan tekoälystä, tekstigeneratiivisesta tekoälystä tai laajoista kielimalleista, viitataan kaikilla pohjimmiltaan samaan konseptiin: laajoihin kielimalleihin.

Tekoälyn lisäksi myös tietoturvakentällä termistö ei ole täysin vakiintunutta. Usein kirjallisuudessa esimerkiksi tietoturva ja kyberturva ovat keskenään synonyymejä. Tässä tutkimuksessa käytetään termiä tietoturva, ja sillä viitataan samalla myös kyberympäristön ulkopuolelle sijoittuviin elementteihin, kuten fyysiseen maailmaan.

1.4 Tutkimuksen rakenne

Tämä tutkimus koostuu viidestä pääluvusta, jotka ovat järjestyksessään johdantoluku, teoreettinen tausta, metodologia, empiirinen osuus ja johtopäätökset. Johdantoluvussa esitellään ensin tutkimuksen taustaa sekä määritellään tutkimustehtävä. Lisäksi esitellään aihealueen rajaus sekä keskeisimmät käsitteet.

Toisessa luvussa tutustutaan aiheen kirjallisuuteen. Ensimmäiseksi perehdytään tietoturvaan ja sen hallintaan yleisesti, jonka jälkeen tutustutaan tekstigeneratiiviseen tekoälyyn ja laajoihin kielimalleihin. Seuraavaksi tarkastellaan, kuinka laajat kielimallit ja tietoturvan hallinta esiintyy keskenään aikaisemmassa kirjallisuudessa. Lopuksi luodaan tutkimuksen teoreettinen viitekehys aikaisemman kirjallisuuden pohjalta.

Kolmannessa luvussa esitellään tutkimuksessa käytetty tutkimusmenetelmä sekä aineiston keruun ja analysoinnin vaiheet. Neljännessä luvussa esitellään kerätty aineisto. Viimeisessä luvussa verrataan kerättyä aineistoa aiheesta löytyvään kirjallisuuteen. Pohdinnan jälkeen annetaan vielä yhteenveto koko tutkimuksesta ja vastataan tutkimustehtävään. Lopuksi annetaan suosituksia jatkotutkimusmenetelmistä.

2 TUTKIMUKSEN TEOREETTINEN TAUSTA

2.1 Organisaation tietoturvan hallinta

2.1.1 Tietoturvan perusteet

Organisaatioilla on hallussaan tietoa, jonka suojaaminen on ensiarvoisen tärkeää; tämä tieto käsittää muun muassa liikesalaisuudet, tuotesuunnitteluun liittyvät tiedot sekä henkilö- ja asiakastiedot (Chopra ym., 2019; Suomen Standardisoimisliitto, 2020). Mikäli tällainen arkaluonteinen tieto vuotaa ulkopuolisille tahoille, voi seurauksena olla organisaatiolle merkittävää vahinkoa (Nancylia ym., 2014). Tietoturvapoikkeamat voivat vaikuttaa huomattavasti yritysten markkina-arvoon, maineeseen ja kilpailukykyyn (Goel & Shawky, 2009; Shaikh & Siponen, 2023). Rikkomusten seurauksena yritykselle voi myös koitua sakoista, hyvityksistä ja muista ylimääräisistä kustannuksista aiheutuvia lisämaksuja (Shaikh & Siponen, 2023). Näin ollen tietoturvan laiminlyönti ja siinä säästäminen voivat pitkällä tähtäimellä maksaa yritykselle enemmän kuin mitä alun perin säästötoimenpiteillä saavutettiin.

Tietoturvan tavoitteena on varmistaa tiedon saatavuus (availability), eheys (integrity) ja luottamuksellisuus (confidentiality) (VAHTI, 2009; Sarker ym., 2021). ”Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.” (Turvallisuuskomitea, 2018, 15). Näitä kolmea tietoturvan elementtiä yhdessä kutsutaan CIA-kolmioksi (CIA-triad). Tietoturvan integroiminen osaksi organisaation päivittäistä toimintaa edellyttää tehokasta tietoturvan hallintaa, jonka tavoitteena on liittää yhteen turvallisuuden periaatteet ja organisaation liiketoiminnalliset tarpeet (Singh ym., 2014). On välttämätöntä, että tietoturvan hallinta toimii saumattomasti osana organisaation muita prosesseja ja että sen merkitys on tunnustettu aina ylimmän johdon tasolle asti (Singh ym., 2014; von Solms & von Solms, 2004).

Organisaatioihin kohdistuu lukuisia ulkoisia tietoturvauhkia. Näitä ovat muun muassa tietojen kalastelut, haittaohjelmat, vakoiluohjelmat sekä tietomurrot (Wang ym., 2015). Ulkoisten uhkien lisäksi organisaatioiden tulee puolustautua sisäisiltä toimijoilta (insider

threat), jotka voivat esimerkiksi olla työntekijöitä, jotka väärinkäyttävät oikeuksiaan (Berman, ym., 2019, 1).

Vaikka organisaatiolla ei olisikaan resursseja investoida IT-infrastruktuuriin, se voi silti vähentää riskejä kehittämällä prosessejaan, politiikkaansa ja henkilöstönsä käyttäytymistä (Antunes ym., 2021). Turvallisuuspolitiikkojen luominen on organisaation tietoturvan turvaamisen ensisijainen askel. Nämä politiikat määrittävät tietoturvan perustan ja ohjaavat, miten eri prosesseihin tulisi suhtautua. (Antunes ym., 2021, 221). On myös olennaista, että organisaatiot varmistavat työntekijöidensä pätevyyden tietoturva-asioissa. Työntekijöiden osaamista voidaan kehittää jatkuvalla koulutuksella ja lisäämällä yleistä tietoturvatietoisuutta (Kamil ym., 2023).

Vaikka tieto voi olla arkaluontoista, on sen olemassaololle jokin tarkoitus. Tiedon säilyttämisen päätöksenteossa tulee punnita keskenään hyötyä ja turvallisuutta (Line ym., 2011; Tjoa, 2011, 27). Yhtenä haasteena voidaan pitää tiedon saatavuuden nopeutta, sillä kaikissa tilanteissa ei ole aikaa kirjautua eri järjestelmiin, vaan tiedon tulisi olla heti saatavilla. Vaikka organisaatio suojautuisi tehokkaimmin mahdollisin keinoin, se ei voi koskaan olla täysin immuuni ulkoisille hyökkäyksille (Shaikh & Siponen, 2023).

Tietojen keskeinen merkitys organisaation eri toimintojen kannalta korostaa niiden luottamuksellisuuden suojaamisen tärkeyttä. Tämä edellyttää organisaation sisäisten menettelytapojen ja sääntöjen huolellista suunnittelua ja toteuttamista, jotta voidaan määritellä, kuka on oikeutettu käyttämään tietoja ja millä edellytyksillä. Tiedon eheys ja saatavuus ovat myös kriittisiä tekijöitä, jotka keskittyvät varmistamaan, että valtuutetut henkilöt pääsevät käsiksi luotettaviin ja tarkkoihin tietoihin. Täten tietoturvan hallinnan standardit ja viitekehykset muodostuvat keskeisiksi välineiksi organisaation turvallisuusstrategioiden ja riskienhallinnan kehittämisessä. (Antunes ym., 2021, 220–221).

2.1.2 Tietoturvan hallintajärjestelmät (ISMS)

> *”Tietoturvallisuuden hallintajärjestelmä (ISMS) koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista ja toiminnoista, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan.*

> *Tietoturvallisuuden hallintajärjestelmä on järjestelmällinen lähestymistapa organisaation tietoturvallisuuden laatimiseen, toteuttamiseen, käyttöön, seurantaan, katselmointiin, ylläpitoon ja parantamiseen liiketoimintatavoitteiden saavuttamista varten."* (Suomen Standardisoimisliitto, 2020).

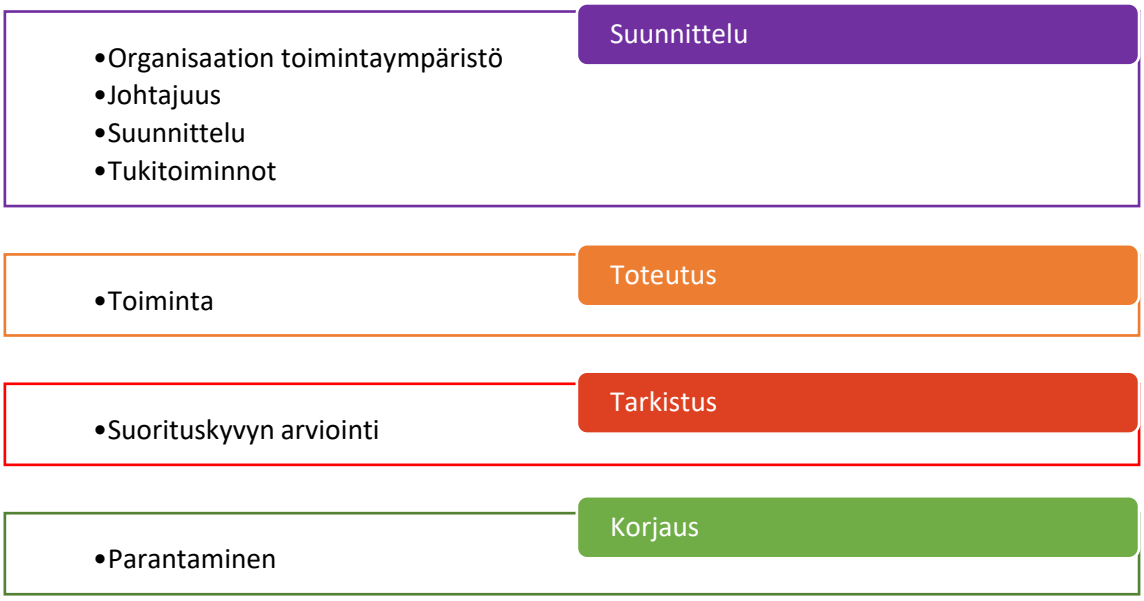
Tietoturvan hallintajärjestelmän avulla organisaatio kykenee suojelemaan tietojen saatavuutta, eheyttä ja luotettavuutta (Fonseca-Herrera ym., 2021; Suomen Standardisoimisliitto, 2023a) Noudattamalla näitä hallintajärjestelmiä organisaatiot saavat vankan perustan tietojensa suojaamiseen ja voivat soveltaa systemaattista lähestymistapaa tiedon suojaamiseksi (Suomen Standardisoimisliitto, 2020; Nancylia ym., 2014). Hallintajärjestelmiin ei ole olemassa valmiita ratkaisuja, vaan ne on räätälöitävä kohdeorganisaation mukaan. Organisaatiot päätyvät usein käyttämään tietoturvan hallintajärjestelmiä, jotta niiden tietoturvan hallinta olisi järjestelmällistä ja jättäisi mahdollisimman vähän aukkoja.

Tietoturvallisuuden hallintajärjestelmiä käsitteleviä standardeja on useita, kuten ISO 27000 -perhe (Suomen Standardisoimisliitto, 2020), NIST SP 800-53 (National Institute of Standards and Technology, 2020), COBIT (ISACA, 2019) ja PCI DSS (PCI Security Standards Council, 2022). Näistä standardeista ISO 27000 -perhe on kaikista tunnetuin, ja kansainvälisyyden sekä yleistettävyytensä puolesta soveltuu parhaiten tämän tutkimuksen keskeiseksi standardiksi (Antunes ym., 2021). ISO 27001 -standardi on suunniteltu tarjoamaan kattava viitekehys organisaatioille, riippumatta niiden koosta tai tyypistä, datan ja informaation turvallisen hallinnan varmistamiseksi niin elektronisissa, fyysisissä, kuin verbaalisissa muodoissa. Sen monipuolisuus mahdollistaa standardin soveltamisen laajasti tietoturvan hallintajärjestelmän implementointiin erityyppisissä liiketoimintaympäristöissä ja skenaarioissa, mikä korostaa sen asemaa alan parhaana käytäntönä. (Antunes ym., 2021, 221).

Kamil ym. (2023) toteavat, että ISO 27001 -standardin noudattaminen mahdollistaa korkean laadun tietoturvajohtamisessa/hallinnassa. Kyseinen standardi painottaa CIA-kolmion varmistamista organisaatioissa ja tarjoaa siihen ohjenuoria. ISO 27001:n mukaisen hallintajärjestelmän käyttäminen ja sertifioituminen lisää sidosryhmien luottamusta organisaatioon. ISO 27001 -standardin tavoitteena on opastaa organisaatioita

tietoturvariskien tunnistamisessa ja auttaa kontrollien käyttöönottamisessa, joiden avulla vähennetään tunnistettujen riskien todennäköisyyttä. (Antunes ym., 2021, 222).

”Organisaatiot yleensä ottavat käyttöön ISO/IEC 27001 -standardin, jotta ne voivat perustaa järjestelmällisen ja luotettavan lähestymistavan tietoturvaongelmien käsittelyyn ja tiettyjen tavoitteiden saavuttamiseen” [1] (Kamil ym., 2023, 716). Samalla organisaatiot pyrkivät varmistamaan, että niiden toimintatavat tietoturvan osalta ovat jatkuvan tarkastelun ja ylläpidon alla. Jatkuvan tarkastelun varmistamiseksi ISO 27001 -standardi noudattaa PDCA-sykliä (Plan-Do-Check-Act) (Heisel ym., 2014). Suunnitteluvaiheessa (Plan) suunnitellaan tavoitteet ja prosessit sekä perustetaan tietoturvan hallintajärjestelmä. Toteutusvaiheessa (Do) kyseinen järjestelmä otetaan käyttöön ja sitä aletaan soveltaa käytännössä. Tarkistusvaiheessa (Check) järjestelmän toimivuutta ja tehokkuutta valvotaan sekä korjausvaiheessa (Act) järjestelmää ylläpidetään sekä kehitetään havaintojen pohjata. (Heisel ym., 2014; Nancylia ym., 2014). Tietoturvan hallinta on siis jatkuvaa ylläpitämistä, jonka kanssa ei olla ikinä ”valmiita”. ISO 27001 -standardille keskeinen jatkuvan kehittämisen malli osana sen prosessia on esitetty alla olevassa kuviossa.



Kuvio 1: PDCA-syklin ja ISO 27001 -standardin välinen suhde (Mukaillen Nancylia ym., 2014).

[1] Vapaa suomennos lauseesta: “*Organizations commonly adopt ISO/IEC 27001 as a means to establish a systematic and reliable approach to addressing information security concerns and achieving specific objectives.*”

Tietoturvan hallintajärjestelmät tarjoavat hyviä ohjenuoria ja parhaita käytäntöjä tietoturvan hallintaan, joiden avulla organisaatiot kykenevät osoittamaan heidän sitoutumisensa tietoturvaan. Niiden ongelmana on kuitenkin ohjeiden geneerinen laatu, ja onnistuakseen ohjeistusta tulisi räätälöidä kunkin organisaation toimintaympäristön mukaan. (Siponen & Willison, 2009). Ne eivät tarjoa valmista sapluunaa organisaatiolle, vaan ainoastaan täydentää organisaation tietoturvan hallintaa (Kamil ym., 2023). Standardien soveltaminen organisaation tarpeisiin ja rakenteisiin edellyttää siis sekä alan, että organisaation asiantuntemusta.

2.1.3 Tietoturvan hallintatoimenpiteet

ISO 27001:2023 luettelee erilaisia tietoturvallisuuden hallintakeinoja, jotka tarjoavat konkreettisia toimenpiteitä tietoturvan hallinnan ylläpitämiseksi. Ne voidaan jakaa neljään osa-alueeseen, jotka ovat organisaatioon liittyvät hallintakeinot, henkilöstöön liittyvät hallintakeinot, fyysiset hallintakeinot sekä teknologiset hallintakeinot. (Suomen Standardisoimisliitto, 2023a).

Organisaatioon liittyvät hallintakeinot sisältävät muun muassa politiikkoja, toimintaperiaatteita, vastuualueita, tietoturvahäiriöihin reagointia, sekä pääsynhallintakeinoja (Suomen Standardisoimisliitto, 2023a). Esimerkiksi yksinkertainen tapa hallita pääsyä tietoon on pakottaa käyttäjiä kirjautumaan tietoa sisältävään järjestelmään (Line ym., 2011). Tällöin ulkopuolisten pääsy tiedon äärelle hankaloituu ja sisäisten uhkien tapauksessa on helpompi tunnistaa tapahtuman aiheuttaja. Mikäli tietoa ei voida keskittää tiettyyn järjestelmään, vaan se on saatavilla esimerkiksi ilmoitustaululla, on hankalaa tietää, kenellä kaikilla on pääsy näkyvillä olevaan tietoon.

Henkilöstöön liittyvät hallintakeinot sisältävät muun muassa turvallisuusselvityksiä, koulutuksia, vaitiolositoumuksia sekä etätyöskentelyn ohjeistuksia (Suomen Standardisoimisliitto, 2023a). Usein sanotaan, että ihminen on tietoturvan heikoin lenkki, ja siksi onkin erityisen tärkeää panostaa henkilöstön osaamiseen tietoturva-asioissa kouluttamisella sekä tietoturvatietoisuuden lisäämisellä (Kamil ym., 2023).

Fyysiset hallintakeinot sisältävät muun muassa kulunvalvonnan toteuttamista, laitteiden ylläpitoa, tilojen fyysistä suojausta sekä sähkökatkoilta suojautumista (Suomen Standardisoimisliitto, 2023a). Esimerkiksi lukolliset ovet ovat yksi tapa suojata tiloja sekä

varmistaa henkilöiden pääsyoikeus. Oikosuluilta, laitteiden rikkoutumiselta sekä asiakirjojen tuhoutumiselta suojautuminen on myös oleellinen osa fyysisiä hallintakeinoja. (Suomen Standardisoimisliitto, 2023a).

Teknologiset hallintakeinot sisältävät muun muassa haittaohjelmilta suojautumista, tietojen varmuuskopiointia, turvallisen ohjelmoinnin periaatteita sekä verkkopalveluiden turvaamista (Suomen Standardisoimisliitto, 2023a). Perinteisesti kyberturvakäsitteeseen liittyvät keinot ovat useimmiten juuri teknologisia hallintakeinoja, sillä ne sisältävät esimerkiksi virustorjuntaohjelmistot sekä salatut yhteydet.

ISO 27001 -standardin luettelemat hallintakeinot eivät kuitenkaan kata kaikkia mahdollisia keinoja. Näiden, sekä muiden standardien hallintakeinokirjastojen lisäksi organisaatiot voivat hyödyntää muitakin keinoja. ISO 27001 -standardi tarjoaa kuitenkin varsin kattavan listan keinoja, joka osaltaan varmistaa sen, ettei sitä käyttävät organisaatiot jätä huomioimatta mitään tärkeää kategoriaa (Suomen Standardisoimisliitto, 2023a).

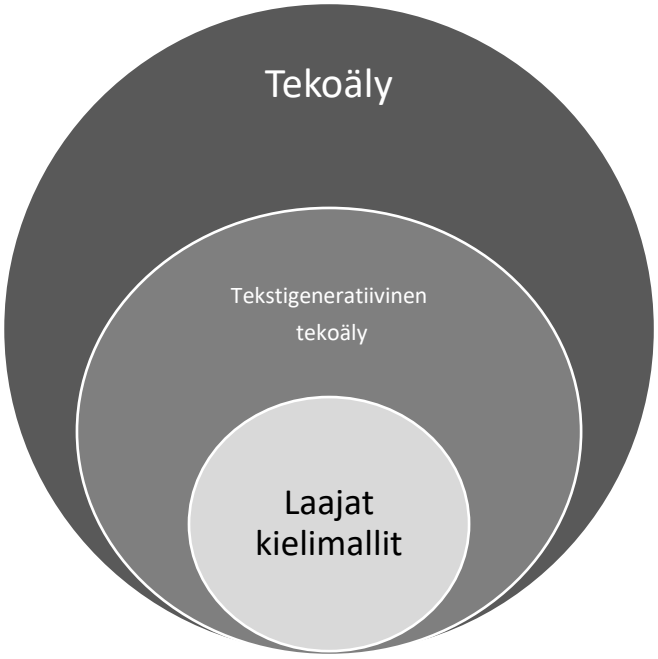
2.2 Tekstigeneratiivinen tekoäly ja laajat kielimallit

2.2.1 Yleiskatsaus tekstigeneratiiviseen tekoälyyn

Generatiivisella tekoälyllä viitataan koneoppimismallien (machine learning) hyödyntämiseen uuden sisällön luomiseksi. Uusi sisältö voi olla niin tekstiä, kuvia, videoita, ääntä kuin ohjelmakoodia, joka perustuvat koulutusmateriaalina käytettyihin laajoihin tietoaineistoihin. (Budhwar ym., 2023, 609). Tekstigeneratiiviseen tekoälyyn perustuvat keskustelubotit (eng. chatbot), kuten ChatGPT ja Gemini (ent. Bard), ovat viime vuosina saavuttaneet yhä kasvavaa suosiota. Niiden helppokäyttöisyyttä tukee niiden kyky käydä keskustelevaa vuoropuhelua sekä kyky ammentaa tietoa olemassa olevista tietokannoista (Chen ym., 2023; Budhwar ym., 2023).

Laajat kielimallit (LLM) ovat eräs tekstigeneratiivisen tekoälyn muoto. Ne kykenevät vastaamaan jatkokysymyksiin sekä mukautumaan käyttäjän äänensävyn mukaan. Laajat kielimallit eroavat huomattavasti perinteisistä koneoppimiseen perustuvista tekoälyalgoritmeista, joita käytetään esimerkiksi Googlen hakukoneessa ja jotka

perustuvat tietoaineistosta ennustamiseen. (Budhwar ym., 2023). Laajat kielimallit on koulutettu suurella määrällä tekstidataa. Esimerkiksi OpenAI:n GPT4 malli on koulutettu yli 45 teratavulla netistä louhittua dataa. Laajat kielimallit päättelevät sanojen välisiä yhteyksiä ja täten koittavat ennustaa lauseessa esiintyviä seuraavia sanoja. (Budhwar ym., 2023). Ne eivät siis ole älykkäitä, vaan ne koittavat ennustaa toivottua lopputulosta valtavan koulutusmateriaalinsa perusteella. Tämä voi kuitenkin johtaa virheelliseen tietoon, kun mallit 'hallusinoivat' tuottaen epätarkkoja vastauksia (Budhwar ym., 2023).



Kuvio 2: Laajat kielimallit suhteessa tekoälyyn, (Budhwar ym., 2023)

Tekoälyllä on moninkertainen kyky luoda ja analysoida tietoa verrattuna ihmisiin (Budhwar ym., 2023, 608). Laajoja kielimalleja on jo hyödynnetty monilla alueilla, kuten terveydenhuollossa, koulutuksessa, asiakaspalvelussa, sisällöntuotannossa, kielikäännöksissä, viihteessä, neuvonantajina ja ohjelmoinnin avustajina (Hariri, 2023). Niiden laajan koulutusmateriaalin ansiosta ne kykenevät käymään kattavia keskusteluja useista eri aiheista. Toisin kuin muut tekoälymallit, laajat kielimallit ymmärtävät konteksteja, mikä mahdollistaa niiden suoriutumisen tehtävistä, joille ne eivät ole saaneet tarkkoja ohjeita. Tämän myötä tekoälyä hyödyntävän tarvitsee nähdä yhä vähemmän vaivaa tuloksia saadakseen. (Zaboli ym., 2023). Vaikka laajat kielimallit ovat tehokkaita työkaluja, niiden integroiminen yrityksen prosesseihin vaatii huomattavaa vaivaa,

lisäresursseja ja koulutusta (Budhwar ym., 2023). Teubner ym. (2023) mukaan näiden mallien tehokkuus työskentelyn apuvälineenä riippuu käyttäjien osaamistasosta.

Koska kielimallit ovat taitavia luomaan tekstiä, ne mahdollistavat käyttäjilleen enemmän aikaa keskittyä sisällön suunnitteluun vähentämällä kirjoittamiseen käytettävää aikaa (Teubner ym., 2023). Teubner ym. (2023) ennustavat, että laajat kielimallit voivat mullistaa tekstinkäsittelyn tavalla, joka vastaa Excelin vaikutusta numeroiden käsittelyyn. Heidän mukaansa kielimallit nopeuttavat monia tekstinkäsittelyyn liittyviä työvaiheita, kuten oikolukua ja kielioppivirheiden tarkastamista, ja ne pystyvät tarjoamaan parannusehdotuksia tai vaihtoehtoisia kirjoitustapoja. Niiden tuottaman tekstin laatu on myös vertailukelpoista ihmisten kirjoittaman tekstin kanssa.

2.2.2 Laajojen kielimallien rajoitukset

Laajat kielimallit tuovat mukanaan useita tietoturvariskejä (Hariri, 2023). Sharma ja Garg (2022, 233) korostavat, että yksi suurimmista haasteista tekoälyn käytössä yrityksissä on sensitiivisen datan hallinta. Monet yritykset säilyttävät tietokannoissaan arkaluonteista tietoa, joka on tarkoitettu vain yrityksen sisäiseen käyttöön ja jota ne haluavat suojata. Tietoturvariskinä on, että jos tekoäly pääsee käsittelemään tällaista dataa, se voi vuotaa esimerkiksi tietomurron myötä ulkopuolisille tahoille. Euroopan unionin tietosuoja-asetus GDPR rajoittaa yksityisen datan käsittelyä ja tämä koskee myös tekoälylle annettavaa tietoa (European Parliament and Council of the European Union, 2016). Yrityksillä voi olla myös omia yrityssalaisuuksia, joita ne eivät halua ulkopuolisille tahoille, kuten tekoälyohjelmille, käsiteltäväksi (Chopra ym., 2019).

On riski, että tekoälyä hyödyntävä henkilö syöttää vahingossa sille luottamuksellista tietoa, joka voi vuotaa, mikäli yhteys tekoälypalveluun ei ole suojattu (Sebastian, 2023). Lisäksi jotkin kielimallien tarjoajat saattavat päästä käsiksi käyttäjien syöttämiin tietoihin, jolloin nämä tiedot voivat vuotaa ainakin palveluntarjoajalle (Kshetri, 2023). Esimerkiksi keväällä 2023 Samsungin työntekijät jakoivat ChatGPT:lle sensitiivistä lähdekoodia, joka myöhemmin vuoti muiden käyttäjien saataville (Petkauskas, 2023; Kshetri, 2023). Tällaiset tietovuodot herättävät keskustelua kielimallien luotettavuudesta ja siitä, mitä tietoja niille uskaltaa syöttää. Kucharavy ym. (2023) ja Kshetri (2023, 12) suosittelevat, että laajoille kielimalleille syötetään vain julkista tietoa, jotta vältetään

tiedon leviämisen haittavaikutuksia. Vaikka tietoja ei käytettäisi koulutusmateriaalina, on mahdollista, että palveluntarjoajan, kuten OpenAI:n, kohdalle sattuva tietomurto voi johtaa vuotoon (Kshetri, 2023).

Luottamuksellisen tiedon suojaamiseksi tekoälyltä on käytettävissä useita menetelmiä. Yksi keino on datan anonymisointi, jossa yksilöitävät ja tunnistettavat osuudet on peitetty tai pseudonimoitu, mikä toimii tehokkaana riskienhallintakeinona (Sebastian, 2023). Lisäksi käyttämällä ylimääräistä keksittyä dataa voidaan vaikeuttaa aidon tiedon tunnistamista (Sebastian, 2023). Tietosuoja-asetus GDPR määrittelee selkeät ohjeistukset henkilötietojen käsittelylle ja mikäli yritykset toimivat GDPR:n asettamien vaatimusten mukaan, nämä toimet samalla suojaavat luottamuksellista tietoa tekoälyltä. On myös välttämätöntä, että data salataan sekä sen säilytyksen että siirron aikana. (Sebastian, 2023).

Kucharavy ym. (2023) mukaan laajoilla kielimalleilla on lukuisia heikkouksia: Tekoäly ei kykene ajatteluun eikä kriittiseen pohdintaan, vaan se tuottaa tekstiä todennäköisyyksien perusteella, minkä vuoksi se ei aina pohjaa tietoa faktoihin. Kielimallit unohtavat keskustelut nopeasti, niillä on rajoitettu muisti, ja ne vastaavat ainoastaan sen perusteella, mitä niille on koulutusdatassa opetettu, oppien samalla myös koulutusaineiston vinoumat. Hariri (2023) lisää, että vinoumien ohella laajoja kielimalleja rajoittavat myös niiden kyvyttömyys ymmärtää spesifejä aihealueita, vaatimus laajasta koulutusmateriaalista sekä vastausten laadun epävarmuus.

Vaikka laajat kielimallit kykenevät generoimaan myös ohjelmointikoodia, ne eivät automaattisesti takaa koodin turvallisuutta. Sen sijaan ne toimivat tehokkaina työkaluina ohjelmoijille, jotka voivat hyväksyä tai hylätä tekoälyn ehdottamat koodinpätkät (Sandoval ym., 2022). Toisaalta Gupta ym. (2023) osoittivat, että laajat kielimallit kykenevät luomaan varsin tietoturvallista koodipohjaa, sekä testaamaan jo olemassa olevan koodin turvallisuutta. Sandovalin ja muiden (2022) tutkimuksen mukaan ohjelmoijat, jotka käyttivät tekoälyä apunaan, eivät tuottaneet turvattomampaa koodia; päinvastoin, heidän työskentelynsä tehokkuus parani.

Laajojen kielimallien yleistymiseen liittyy myös uhkakuvia. Nämä tekoälymallit kykenevät käsittelemään suuria määriä dataa, mikä mahdollistaa yksityiskohtaisen tiedon

tuottamisen esimerkiksi yrityksistä yhdistelemällä eri julkisista lähteistä saatua koulutusmateriaalia. Kielimallit voivat esimerkiksi arvioida, millaisia tietojärjestelmiä tietyt yritykset käyttävät. Lisäksi niiden kyky tuottaa laadukasta tekstiä voi helpottaa tietojenkalasteluviestien laatimista, tehden niistä entistä vakuuttavampia. Samoin kielimallien ohjelmistokoodin generointikyky saattaa edistää haittaohjelmien kehittämistä ja leviämistä (Derner & Batistič, 2023; Kshetri, 2023).

2.3 Laajojen kielimallien käyttö tietoturvan hallinnassa

2.3.1 Tietoturvan automatisointi

Montesino ja Fenz (2011) toteavat, että tietoturvakentän monimutkaistuessa on välttämätöntä automatisoida tietoturvan hallintaa sen tehokkuuden ylläpitämiseksi. Erilaisia automatisointitekniikoita on ollut jo pitkään käytössä, mutta tekoäly tulee tehostamaan sitä entistä enemmän. Koska tietoturva ei ole pelkästään tekninen kysymys, vaan siihen sisältyy myös ihmiset ja prosessit, ei sitä ole mahdollista automatisoida kokonaan (Montesino & Fenz, 2011). Vaikka tietoturvan täydellinen automatisointi ei ole mahdollista, tiettyjä osa-alueita voidaan automatisoida osittain.

Tietoturvan osittainen automatisoiminen esimerkiksi tekoälyn avulla pienentää kustannuksia ja siihen liittyvää työkuormaa (Montesino & Fenz 2011). Gill ym. (2021) huomauttavat, että tietoturvan automatisointi vähentää inhimillisten virheiden määrää, pienentää työkuormaa ja auttaa noudattamaan erilaisia tietoturvaan ja yksityisyyteen liittyviä standardeja, lakeja ja määräyksiä. Toisaalta Gill ym. (2021) osoittivat tutkimuksessaan, että noin puolet NIST SP 800-53 -tietoturvastandardin tietoturvavaatimuksista voidaan jo automatisoida muilla työkaluilla kuin tekoälyllä. Lisäksi tietoturvan automatisoiminen tuo omia haasteitaan. Näitä ovat Gill ym. (2021) mukaan muun muassa erilaisten järjestelmien ja ratkaisujen integroiminen, automatisointiin liittyvän henkilöstön asiantuntemuksen varmistaminen sekä automatisointiin liittyvä epävarmuus tietoturvauhkien poistumisesta. Jotta tekoälyä voitaisiin hyödyntää osana automatisointia mahdollisimman tehokkaasti, on tärkeää, että henkilöstö ymmärtää tekoälyn ominaisuuksia ja rajoitteita (Hussain ym., 2022).

Joidenkin tutkimusten mukaan nimenomaan laajoja kielimalleja voidaan hyödyntää tietoturvan automatisoinnissa. Ne kykenevät esimerkiksi käymään läpi tapahtumalokeja ja analysoimaan tietoturvapoikkeamia varsin nopeasti (Gupta ym., 2023, 80234). On kuitenkin syytä huomioida, että laajat kielimallit eivät voi täysin automatisoida toimintoja, vaan ne voivat toimia tehokkuutta lisäävinä työkaluina asiantuntioille. Feuerriegel ym. (2022, 612) mukaan tekoälyohjelmia ei voida automatisoida täysin johtamisen ja hallinnoinnin osalta, mutta ne voivat lisätä tuottavuutta ja auttaa ihmisiä, kuten johtoa, päätöksenteossa. Tietoturvan hallinnassa tekoäly voi esimerkiksi auttaa uusien uhkien tunnistamisessa ja tarjota päätöksentekoon tarvittavaa tietoa, jolloin ihmiset voivat hyödyntää sekä tekoälyn tarjoamaa tietoa että omaa asiantuntemustaan päätöksissään.

”Kielimallit kykenevät auttamaan organisaatioita tekemään informoidumpia päätöksiä tietoturvastrategioistaan ja -sijoituksistaan tarjoamalla näkemyksiä turvallisuuteen liittyvästä datasta.” (Gupta ym., 2023, 80235)

2.3.2 Tietoturvan analyysi ja raportointi

Laajat kielimallit pystyvät luomaan raportteja tietoturvaan liittyvistä aiheista, jolloin esimerkiksi eri sidosryhmille lähetettävien raporttien laatimiseen käytettyä aikaa voidaan lyhentää tekoälyn avulla (Gupta ym., 2023, 80235). Nämä kielimallit kykenevät analysoimaan tietoturvaa koskevaa tietoa ja tunnistamaan sen pohjalta organisaatioon kohdistuvia uhkia. Tekoälyn tuottamien analyysien pohjalta laaditut raportit auttavat organisaatioita tunnistamaan toimintaansa liittyviä riskejä ja käynnistämään niiden hallintaan tarvittavat toimenpiteet.

Tekstigeneratiivinen tekoäly on osoittanut suurta potentiaalia kyvyssään analysoida laajoja tietomääriä, tunnistaa uhkakuvioita sekä tuottaa räätälöityjä ohjeita ja menettelytapoja (Iqbal ym., 2023). Esimerkiksi laajat kielimallit voivat analysoida suuria määriä kyberhyökkäysten dataa, mikä auttaa tietoturva-asiantuntijoita parantamaan toimintamallejaan ja tunnistamaan uusia uhkia (Gupta ym., 2023). Tietoturvapoikkeaman sattuessa nämä kielimallit voivat myös avustaa selvityksessä, esimerkiksi läpikäymällä lokitiedostoja ja järjestelmän tulostetietoja, nopeuttaen näin reagointia (Gupta ym., 2023).

Von Krogh ym., (2023, 368) korostavat, että on tärkeää valita tehtävään sopiva tekoäly. Esimerkiksi ChatGPT:llä on mahdollisuus luoda omia GPT-malleja (OpenAI, 2023), joihin voidaan syöttää erityistä koulutusmateriaalia. Näin tekoälyohjelma suoriutuu paremmin juuri tähän materiaaliin liittyvistä tehtävistä. Mikäli laajat kielimallit koulutettaisiin toimialakohtaisesti, ne suoriutuisivat huomattavasti paremmin tehtävistään verrattuna yleisiin malleihin, kuten ChatGPT ja Google Gemini (Paria ym., 2023).

2.3.3 Laajat kielimallit kontrollien tukena

Tekstigeneratiivisia tekoälyjä, kuten ChatGPT:tä, voidaan hyödyntää tietoturvan teknisissä aspekteissa. Niiden kyky tuottaa ja muokata koodipohjaa sekä analysoida laajoja datamääriä tehostaa esimerkiksi suojautumista haittaohjelmilta (McKee & Noever, 2022; Al-Hawawreh ym., 2023; Sarker ym., 2021). Pääsy tietokantaan mahdollistaa myös potentiaalisten haavoittuvuuksien löytämisen ja korjaamisen, mikä on osoittautunut muita työkaluja tehokkaammaksi (Iqbal ym., 2023). Ne tarjoavat myös suurta potentiaalia tietoturvahäiriöihin reagoimiseen ja uhkien tunnistamiseen (Ferrag ym., 2023). Esimerkiksi Jamal ja Hayden (2023) ovat osoittaneet, että kielimallit tunnistavat tietojenkalasteluviestejä tehokkaasti.

Yksi tekstigeneratiivisen tekoälyn vahvuuksista on sen kyky toimia ideointityökaluna, jolloin se kykenee tuottamaan uusia tietoturvapolitiikkaan liittyviä ideoita, tarjoamaan syvällisempiä selostuksia ja raportteja tietoturvan eri aiheista sekä luomaan näiden perusteella valmiita viitekehikkoja. Monet kyberturvallisuusasiantuntijat ovat ilmoittaneet käyttävänsä tekoälyä apuna muotoilemaan riskienhallintakehyksiä, tarjoamaan näkemyksiä ja keskustelua tietoturvan eri aiheista sekä hahmottelemaan erilaisia tietoturvaan liittyviä raportteja. (Al-Hawawreh ym., 2023, 3424).

Toinen tekstigeneratiivisen tekoälyn merkittävistä vahvuuksista on sen kyky opettaa monimutkaisia aiheita erilaisille yleisöille. Se pystyy tuottamaan yksilöllistä opetusmateriaalia, mikä mahdollistaa tietoturvaan liittyvien koulutusten räätälöinnin kunkin henkilön osaamistason ja työtehtävien mukaan (Kasneci ym., 2023; Al-Hawawreh ym., 2023, 3425; Iqbal ym., 2023). Laajat kielimallit ovat erityisen taitavia muuntamaan

teknisen datan ymmärrettävään muotoon, mikä auttaa myös ei-asiantuntijoita ymmärtämään aiheita paremmin (Gupta ym., 2023).

Tekoäly voi tuottaa varsin yksilöllisiä ohjeistuksia ja avustaa tietoturvapolitiikan laatimisessa. Se kykenee lisäksi tunnistamaan riskejä ja uhkia, sekä laatimaan toimintasuunnitelmia tunnistettujen riskien korjaamiseksi. (Iqbal ym., 2023). Laajat kielimallit kykenevät myös luomaan valmiita toimintaohjeita erilaisia skenaarioita varten. Esimerkiksi palvelunestohyökkäyksen (DDoS) sekä SQL-injektion varalle voi olla valmiita ohjeita, joiden toimeenpanon tekoäly kykenee automaattisesti aloittamaan poikkeaman havaittuaan (Gupta ym., 2023). Valmiiden toimintaohjeiden lisäksi laajat kielimallit kykenevät luomaan toimintamalleja ja ehdotuksia siitä, kuinka organisaatio ylläpitää toiminnan eettisyyden ja noudattaa rajoituksia ja säädöksiä. Esimerkiksi GDPR:n noudattaminen on keskeistä kaikille Euroopan Unionin alueella toimiville organisaatioille, ja kielimallit voivat tukea tämän asetuksen noudattamista (Gupta ym., 2023).

2.3.4 Laajojen kielimallien käytön haasteet

Laajojen kielimallien käyttöön liittyy monia tietoturvallisuuteen liittyviä kysymyksiä, kuten yksityisyys ja tietojen näkyvyys. Esimerkiksi ChatGPT kerää ja tallentaa suuren määrän käyttäjien henkilökohtaista tietoa, mukaan lukien viestien sisällöt ja laitetiedot. Tämä voi rikkoa yksityisyyden suojaa ja altistaa tiedot ulkopuolisille tahoille tai hyökkääjille. Lisäksi laajat kielimallit voivat tuottaa harhaanjohtavaa tietoa, sillä niiden koulutusaineisto on peräisin monenlaisista lähteistä. Tämä voi johtaa virheellisiin tuloksiin, mikä on erityisen ongelmallista kriittistä tietoa etsittäessä. Luottamuksen ylläpitäminen ja henkilökohtaisten tietojen suojaaminen, kun kielimallit jakavat tietoja kolmansien osapuolien kanssa, on myös suuri haaste. (Al-Hawawreh ym., 2023, 3432). Pääsynvalvontamenetelmien käyttöönotto myös tekoälylle ja sen toiminnan valvonta ovat välttämättömiä suojattujen tietojen ja tietokantojen käsittelyn estämiseksi. On mahdollista, että muuten luotettava tekoäly vahingossa vuotaisi luottamuksellista tietoa, minkä vuoksi sen jatkuva valvonta on tarpeellista. (Zaboli ym., 2023).

Von Krogh, Roberson ja Gruber (2023, 368) totesivat tutkimuksessaan tekoälyn toistavansa koulutusmateriaalinsa vinoumia. Tekoälyä hyödyntäessä tulee olla tarkkana

siitä, että käsiteltävä asia on sille koulutettu. Esimerkiksi ISO 27001 -standardi on päivitetty vuonna 2023, mutta monet tekoälyohjelmat ovat saaneet koulutuksensa vanhemman, vuoden 2017 version mukaan (Suomen Standardisoimisliitto, 2023a). Tämä voi johtaa siihen, että tekoälyn tiedot eivät ole ajantasaisia, mikä puolestaan altistaa päätöksenteon virheille. Lisäksi mikäli tekoäly osallistuu rekrytointiprosessiin, se saattaa suosia niitä kandidaatteja, joiden näkemykset vastaavat sen koulutusmateriaalissa toistuvia näkemyksiä, mikä tulisi ottaa huomioon taustatarkistuksia ja muita rekrytointitoimenpiteitä suoritettaessa. Vinoumien vaikutuksia voi kuitenkin lieventää yhdistämällä tekoälyn ja ihmisen asiantuntijuutta (Feuerriegel ym., 2022, 612). Laajojen kielimallien tiedon paikkansapitävyyden todentaminen voi olla haastavaa, koska ne saavat koulutusmateriaalinsa monista lähteistä, kuten Wikipediasta, joka voi sisältää virheellistä tietoa. Tästä syystä kielimallien tarjoamaan tietoon tulee suhtautua kriittisesti. Kielimallit voivat esimerkiksi virheellisesti väittää, että pitkien salasanojen uudelleenkäyttö olisi järkevää (Chen ym., 2023). On kuitenkin huomattava, että uusimmat mallit suoriutuvat tiedon oikeellisuudessa paremmin kuin vanhemmat mallit ja ne voivat tulevaisuudessa olla erittäin tarkkoja (Paria ym., 2023).

2.4 Kirjallisuuden yhteenveto ja teoreettinen viitekehys

Kirjallisuuskatsauksen perusteella organisaatioiden on tärkeää suojata kriittistä tietoaan, kuten tuotesuunnitteluun liittyviä tietoja, talouslukuja tai henkilötietoja (Chopra ym., 2019). Mikäli tietoa ei onnistuta suojaamaan, voi se aiheuttaa mainehaittaa, kilpailuedun menettämisen tai markkina-arvon laskun (Goel & Shawky, 2009; Shaikh & Siponen, 2023). Tiedon suojaaminen onnistuu varmistamalla tiedon luotettavuus, eheys ja saatavuus (VAHTI, 2009; Sarker ym., 2021). Tehokas tietoturvan hallinta yhdistää nämä elementit organisaatioiden tavoitteisiin sekä on osa organisaation prosesseja kaikilla tasoilla (Singh ym., 2014; von Solms & von Solms, 2004).

Tietoturvan systemaattinen hallinta on mahdollista tietoturvan hallintajärjestelmän (ISMS) avulla. ISMS koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja resursseista, joita organisaatio käyttää suojatakseen tietojaan systemaattisesti ja saavuttaakseen liiketoimintatavoitteensa (Suomen Standardisoimisliitto, 2020; Fonseca-Herrera ym., 2021). Kansainvälisesti tunnetuin ISMS-standardi on ISO 27000 -perhe,

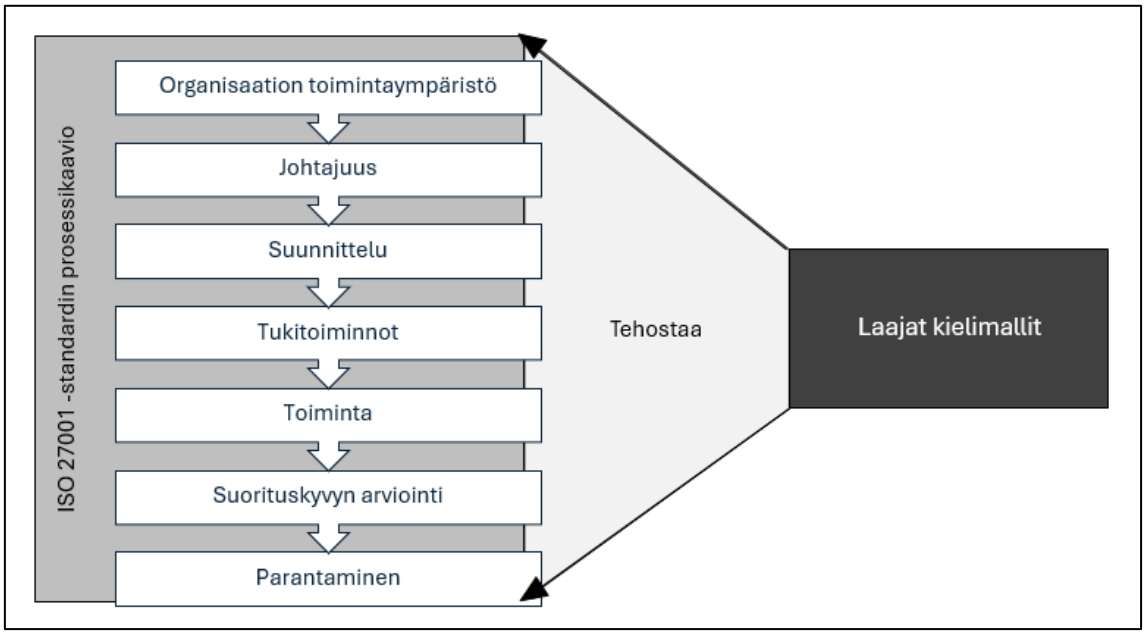
joka soveltuu erilaisille organisaatioille ja tukee jatkuvan parantamisen kulttuuria (Antunes ym., 2021; Nancylia ym., 2014; Heisel ym., 2014). Kirjallisuuden mukaan standardit, kuten ISO 27001, tarjoavat hyvän pohjan organisaatioiden tietoturvan hallintaan.

Laajat kielimallit, jotka ovat tekoälyn eräs sovellusmuoto, ovat tutkimuskirjallisuudessa suhteellisen uusi ilmiö, ja niiden kehitys on ollut nopeaa. Ne ovat saaneet suuren määrän koulutusmateriaalia ja pyrkivät sen perusteella päättelemään sanojen välistä yhteyttä ja ennustamaan tekstin toivottua lopputulosta (Budhwar ym., 2023). Laajat kielimallit ovat täten tehokkaita luomaan tekstiä sekä analysoimaan tietoa (Teubner ym., 2023; Budhwar ym., 2023). Kielimallit kykenevät tehostamaan työskentelyä ja niitä onkin käytetty jo useilla eri aloilla työskentelyn tueksi (Zaboli ym., 2023; Hariri, 2023).

Tutkimuskirjallisuudessa on käsitelty varsin vähän laajojen kielimallien ja tietoturvan hallinnan välistä yhteyttä. Yleisesti tekoälyn käyttöönottoa esimerkiksi automaation välineenä (Montesino & Fenz, 2011; Gill ym., 2021) sekä turvallisemman ohjelmistokoodin kirjoittamisessa (McKee & Noever, 2022; Al-Hawawreh ym., 2023; Sarker ym., 2021) on keskusteltu jo aikaisemmin, mutta kokonaisvaltaiseen tietoturvan hallintaan liittyvää kirjallisuutta on varsin niukasti. Aikaisemmissa tutkimuksissa on kuitenkin käsitelty kielimallien potentiaalia yksittäisien tietoturvan hallinnan kontrollien tukena sekä tietoturvan suunnittelussa. Laajat kielimallit esimerkiksi voivat analysoida tietoturvapoikkeamia ja täten tukea päätöksenteossa (Gupta ym., 2023; Feuerriegel ym., 2022). Ne voivat myös tuottaa raportteja, tunnistaa uhkia ja luoda toimintasuunnitelmia (Iqbal ym., 2023). Kielimallien kyky luoda tekstiä on osoittanut potentiaalia räätälöidä koulutusmateriaalia (Kasneci ym., 2023; Al-Hawawreh ym., 2023; Iqbal ym., 2023) sekä toimia ideointityökaluna esimerkiksi tietoturvapolitiikkojen hahmottelemisessa (Al-Hawawreh ym., 2023; Iqbal ym., 2023).

Kirjallisuuden mukaan laajojen kielimallien hyödyntäminen osana tietoturvan hallintaa tuo mukanaan merkittäviä haasteita. Näiden mallien käyttöön liittyy tietoturvariskejä, kuten sensitiivisen datan hallinnan ongelmia ja mahdollisia tietovuotoja (Hariri, 2023; Sharma & Garg, 2022; Petkauskas, 2023; Kshetri, 2023). Laajat kielimallit eivät kykene itsenäiseen ajatteluun tai kriittiseen pohdintaan, vaan ne tuottavat tekstiä tilastollisten todennäköisyyksien perusteella, mikä voi johtaa virheellisiin tietoihin (Kucharavy ym.,

2023; Chen ym., 2023). Tämän seurauksena niiden tuottama sisältö ei aina perustu faktoihin ja saattaa sisältää merkittäviä virheitä, mikä voi johtaa vääriin johtopäätöksiin.



Kuvio 3: Tutkimuksen teoreettinen viitekehys.

Teoriaosuuden perusteella laadittiin yllä oleva tutkimuksen teoreettinen viitekehys. Se toimii empiirisen tutkimuksen pohjana sekä teoriaosuuden yhteenvetona. Kirjallisuudessa todetaan, että laadukas tietoturvan hallinta vaatii yleensä tietoturvan hallintajärjestelmän käyttöönottoa. Näiden järjestelmien luomisen avuksi on olemassa erilaisia tietoturvastandardeja, jotka tarjoavat järjestelmällisen lähestymistavan tietoturvan hallintaan. (Kamil ym., 2023). Tunnetuin tietoturvastandardi on ISO 27001, jonka prosessikaavio on esitettynä yllä olevassa kuviossa (Nancylia ym., 2014; Suomen Standardisoimisliitto, 2023a). Samalla kuvio havainnollistaa, miten laajat kielimallit voivat tehostaa laadukkaan tietoturvan hallinnan eri vaiheita. Laajat kielimallit voivat esimerkiksi nopeuttaa suunnitteluun sekä suorituskyvyn arviointiin sisältyviä tehtäviä. Näin ollen laajat kielimallit voivat toimia työkaluna tietoturvan hallinnan tehostamisessa, mahdollistaen entistä tehokkaammat ja kokonaisvaltaisemmat ratkaisut tietoturvan hallinnan suunnitteluun ja ylläpitoon.

3 TUTKIMUSMENETELMÄT

3.1 Tutkimusmenetelmät

Tutkimuksen metodologia perustuu kvalitatiiviseen, eli laadulliseen tutkimusotteeseen, jonka tavoitteena on kartoittaa laajojen kielimallien potentiaalia yritysten tietoturvan hallinnassa. Hirsjärvi ym. (2009, 138) mukaan tutkimuksen tarkoitus on kartoittava, kun halutaan selvittää vähän tunnettuja ilmiöitä ja etsiä uusia näkökulmia. Koska tutkimuksen aihe on varsin nuori ja siten ilmiönä vielä suhteellisen tuntematon, kartoittavan laadullisen tutkimuksen valinta on perusteltua.

Aineistonkeruumenetelmänä käytetään puolistrukturoituja teemahaastatteluja, jotka mahdollistavat tutkimusaiheen keskeisten teemojen syvällisen tutkimisen. Puolistrukturoitu haastattelu tarjoaa joustavuutta haastattelutilanteessa, mahdollistaen kysymysten tarkentamisen ja syventämisen vastausten pohjalta, mikä edesauttaa monipuolisen aineiston keräämistä sekä haastateltavien äänen kuulumista (Hirsjärvi & Hurme, 2020, 109–112; Tuomi & Sarajärvi, 2018, 62, 65). Lisäksi se tarjoaa haastateltaville mahdollisuuden vastata myös ennalta määriteltyjen kysymysten ulkopuolelta. Haastatteluiden teemat rakentuvat kirjallisuuskatsauksen ja tutkimuksen tavoitteiden pohjalta, keskittyen erityisesti tietoturvan hallintaan ja tekoälyn potentiaaliin. (Hirsjärvi & Hurme, 2020, 48; Tuomi & Sarajärvi, 2018).

Laajojen kielimallien potentiaalista organisaatioiden tietoturvan hallinnassa tiedetään vielä varsin vähän, jolloin kvalitatiivisen teemahaastattelun toteuttaminen on perusteltua (Hirsjärvi & Hurme, 2020, 35). Haastatteluiden avulla asiantuntijoiden käsityksiä ja näkemyksiä voi verrata tutkimuksen viitekehykseen.

3.2 Aineiston keruu

Aineisto kerättiin teemahaastatteluin sellaisten henkilöiden kanssa, jotka ovat olleet tekemisissä tutkittavan ilmiön kanssa. Ensimmäinen haastateltavista (H1) on informaatioteknologia-startupin toimitusjohtaja, jonka yritys toimii keskustelubottien kehitystyössä. Toinen haastateltavista (H2) on toiminut pitkään tietoturva-alalla, viimeisimpänä erään suuren tietoturvayhtiön toimitusjohtajana.

Taulukko 1: Haastattelut

Haastateltava	Ajankohta	Kesto	Litteraatin pituus	Paikka
H1	26.2.2024	67 min.	31 sivua	Teams
H2	7.3.2024	42 min.	20 sivua	Puhelin

Haastattelut toteutettiin yksilöhaastatteluina taulukon 1 mukaisesti Teams-puhelua sekä puhelinhaastattelua hyödyntäen. Haastattelut nauhoitettiin ja litteroitiin haastateltavien luvalla. Haastatteluja varten luotiin teemahaastattelurunko, joka löytyy tämän asiakirjan lopusta liitteet-osiosta (Liite 1). Haastattelurunko koostuu johdannon ja lopetuksen lisäksi kolmesta osa-alueesta, jotka ovat tietoturvan nykytila ja haasteet, tekoälyn käyttö tietoturvassa sekä tietoturvan tulevaisuus tekoälyn myötä. Haastattelurunkoa käytettiin molemmissa haastatteluissa niiden pohjana, mutta kummassakin haastattelussa esitettiin teemahaastattelulle tyypillisiä lisäkysymyksiä tarkentamaan esille nousseita asioita (Hirsjärvi & Hurme, 2020).

3.3 Aineiston käsittely ja analysointi

Haastatteluaineiston pohjalta tehty litterointi käsiteltiin teoriaohjaavan sisällönanalyysin avulla. Sisällönanalyysissa keskitytään aineiston sisältöön sanallisesti kuvaamalla ja erilaisten merkitysten etsimisellä (Tuomi & Sarajärvi, 2018). Teoriaohjaavassa analyysissa tutkija yhdistelee keskenään aineistoa sekä valmiita malleja (Tuomi & Sarajärvi, 2018). Tutkimuksen teoreettinen viitekehys ohjasi haastattelurungon muodostamista sekä aineiston analyysia. Aineistoa käytiin läpi useaan otteeseen havainnoiden tutkimuksen kannalta oleellisia teemoja. Analyysin myötä aineisto päätettiin esittää järjestelmällisesti kerronnallisessa muodossa, käyttäen tukena runsaasti haastateltavien lainauksia, teoriaosuuden runkoa mukaillen. Näin aineisto onnistuttiin jäsentämään tutkimuksen kannalta tarkoituksenmukaiseen ja selkeään muotoon.

3.4 Tutkimuksen luotettavuuden arviointi

Tuomi ja Sarajärvi (2018) korostavat, että laadullisen tutkimuksen luotettavuuden arvioiminen on monimutkaisempi prosessi verrattuna määrälliseen tutkimukseen. Tutkimuksen luotettavuutta tarkasteltaessa tulee huomioida, että kvalitatiivisen

tutkimuksen aineistosta tehtäviä havaintoja ei voida suoraan yleistää rajallisen otoskoon vuoksi. Kuitenkin syventyessä tarkemmin voidaan saada selville se, mikä ilmiössä on merkittävää ja yleisellä tasolla toistuvaa. (Hirsjärvi ym., 2009, 182; Tuomi & Sarajärvi, 2018).

Analyysin luotettavuutta rajoittivat haastateltavien vähäinen määrä sekä heidän erikoistumisalueidensa painotukset. Molemmat haastateltavat olivat saaneet kokemuksensa pääasiassa yritysten toimitusjohtajan tehtävistä, mikä korostaa vastauksissa yritysjohdon näkökulmaa. Tutkimuksen luotettavuutta voitaisiin parantaa laajentamalla haastateltavien joukkoa sisällyttämällä mukaan esimerkiksi tietoturvajohtajia tai teknisiä tietoturva-asiantuntijoita, jolloin ilmiöön saataisiin myös operatiivisen tason näkemyksiä.

Tutkimuksen teorialla on vaikutusta tutkimuksen laatuun (Tuomi & Sarajärvi, 2018). Täten kirjallisuuskatsauksessa ja teoreettisen viitekehyksen muodostamisessa on kiinnitetty erityistä huomiota lähteiden laatuun ja moninaisuuteen. Lähteiksi on valikoitunut pääosin vertaisarvioituja akateemisia tekstejä, joihin on viitattu kirjallisuuskatsauksessa tarkasti. On kuitenkin huomioitava, että tutkittava ilmiö on varsin nuori, joka osaltaan saattaa vaikuttaa kirjallisuuden laatuun.

”Laadullisen tutkimuksen luotettavuutta kohentaa tutkijan tarkka selostus tutkimuksen toteuttamisesta” (Hirsjärvi ym., 2009, 232). Täten tutkimuksen luotettavuutta on pyritty kohentamaan avaamalla mahdollisimman selvästi ja näkyvästi tutkimuksen toteuttamisen vaiheita sekä rakentamalla tutkimuskokonaisuudesta yhtenäinen ja loogisesti jäsentyvä (Tuomi & Sarajärvi, 2018).

4 TUTKIMUKSEN EMPIIRINEN OSUUS

4.1 Tietoturvan merkitys organisaatioille

Haastateltavat ovat yhtä mieltä siitä, että tietoturvan merkitys on kasvanut viime aikoina. Molemmat nostavat esimerkiksi, kuinka motivaatio tietoturvan parantamiseen tulee yleensä viimeistään yrityksen asiakkailta, jotka vaativat siihen tiettyä tasoa. Yhä enenevissä määrin tietyt vaatimukset ja säädökset, kuten GDPR, ovat nostaneet yritysten tietoturvatietoisuutta.

> *Tietoturvallahan on tietenkin kasvava merkitys johtuen siitä, että enenevissä määrin toimittajapalvelut siirtyy digitaaliseksi. Ja vaikka ne ei olisi digitaalisia palveluita, niin taustajärjestelmät ovat kuitenkin digitaalisia ja ne manuaaliset vaiheet sieltä häviää, niin sitten se tietoturvan merkitys korostuu. – H2*

Molemmat haastateltavat korostavat, että tietoturvatyöhön liittyy olennaisesti myös tiedon saatavuuden varmistaminen. Sen lisäksi, että tieto tulisi pitää suojattuna, on oleellista, että tieto on helposti käytettävissä, eikä tietoturvatoimenpiteistä koostu ylimääräistä haittaa.

> *– – [Tietoturvan merkityksestä puhuttaessa] nimenomaan puhutaan siitä tietoturvan CIA-kolminaisuudesta, eli jatkuvuudesta eli saatavuudesta, eheydestä ja luottamuksellisuudesta, ja ehkä jopa niin että se jatkuvuus ja eheys korostuu mun mielestä tänä päivänä jopa enemmän kuin se luottamuksellisuus ja on sitten yleisesti tietoturvaan liitettävä asia eli tavallaan yritysten kannalta, kai se luottamuksellisuus ja tietosuojajutut sun muut on kurjia, mutta sitten jatkuvuus kuitenkin sitten kaikissa digitaalisissa palveluissa on sitten kaikista kriittisintä. – H2*

> *Ei riitä, että se [suojattava tieto] on hyvin säilötty. Se pitää olla myös tarvittaessa jaettavissa ja saatavissa. – H1*

Haastatteluissa käy ilmi, kuinka helppokäyttöisyyteen olisi tärkeää panostaa enenevissä määrin. Pahimmillaan huonosti tehdyt tietoturvaohjeistukset voivat jopa vaarantaa tietoturvaa entisestään:

> *– – järjestelmä kuin järjestelmä, jos se on vaikeakäyttöinen, hankala ja mutkikas, niin sitä ei ylipäätään käytetä vaan siihen keksitään jotain kiertoteitä, jotka voi olla hyvinkin vaarallisia. – H1*

Toisaalta toinen haastateltava korostaa, kuinka tietoturvaan panostaminen on varsin monimutkaista sen moninaisuuden vuoksi. Laadukas tietoturvan hallinta on vaativaa, ja haastateltava toteaa, että mikäli organisaation toiminta ei ole yleisellä tasolla laadukasta ja prosessit selkeitä, on tietoturvan hallitseminenkin silloin hankalaa. Molemmat haastateltavat ovat yhtä mieltä siitä, että joka yrityksessä ei edes ole henkilöä, jonka vastuulla yrityksen tietoturvakäytännöt olisivat.

> *– – tietoturva on niin monessa mukana. Monta asiaa voi tehdä, kun löytyy se selkeä omistaja ja vastuu ja voima, mutta tietoturva on niin kaiken kattavaa ja kokonaisvaltaista niin teknisestä hallinnolliseen ja läpi kaikkien prosessien ja liiketoimintayksiköiden ja muiden, niin siihen on hirveän vaikeaa löytää sellaista yksittäistä päättäjää, joka siunaa sen budjetin esimerkiksi ja mitä sillä pitäisi tehdä, kuinka paljon asioita tehdään sun muuta. – H2*

4.2 Tekoäly tietoturvan työkaluna

Kummassakin haastattelussa painotettiin useampaan otteeseen tekoälyn roolia nimenomaan työskentelyä nopeuttavana työkaluna. Molemmat haastateltavat olivat sitä mieltä, että tekoäly ei tässä kohtaa kykene luomaan mitään uutta ja mullistavaa, vaan ainoastaan nopeuttaa sitä työtä, joita ihminen muutenkin tekisi. Toinen haastateltavista totesi, että tekoälyn avulla voisi tuottaa myös sellaisia ratkaisuja, joita ei muuten työajalla ehtisi tekemään. Täten tekoäly toimii pelkästään nopeuttavan työkalun lisäksi myös mahdollistajana.

> *Sillä [tekoälyllä] voi teettää asioita nopeuttaakseen omaa työtä. – H1*

> *Ylipäätään nämä kielimalliset tekoälyt, niin nehän pysyvät nopeuttamaan sitä datan tuottamista – – ja se [tekoäly] ei poista ihmisten työtä, vaan se ainoastaan nopeuttaa tiettyjä työvaiheita ja parhaimmillaan käytettynä tuo sitä lisäarvoa siihen tekemiseen. – H2*

> *– – se on työkalu, joka nopeuttaa asioita, mitä voitaisiin ihmisten voiminkin tehdä. Nyt on enemmänkin kyse siitä, että pitää olla ne edellytykset sille, että ihmiset pystyvät sitä tekemään ja tekoäly voi tuoda siihen jotain lisää – – Se enemmänkin avaa skaalautuvia mahdollisuuksia, jota ihmisten voimin ei ennen pystytty tekemään, mutta se edelleen vaatii sen, että joku ihminen on toimeenpaneva voima sille asialle. – H2*

> *– – jos on ylipäätään aika päivittää jotain tietoturvasuunnitelmaa tai riskianalyysiä tai jotain muuta, niin voisi tutkia, että löytyykö tekoälystä jotain apuvoimia, että saa jonkun osa-alueen tehtyä nyt sitten helpommin ja kevyemmin. – H1*

Haastateltavat myös totesivat, että tiettyjä työskentelyvaiheita nopeuttaessa tekoäly mahdollistaa ammattilaisten keskittymisen muihin työtehtäviensä oleellisiin asioihin, ja täten mahdollisesti moninkertaistamaan työtehonsa. Toinen haastateltavista viittasi, että etenkin kirjoittamaan tottumattomat tekniset ammattilaiset voisivat keskittyä työnsä kannalta olennaiseen, mikäli tekoäly pystyisi heidän puolestaan kirjoittamaan työläät raportit.

> *Eli varsinkin ammatikseen tietoturvatyötä tekevien olisi järkevää ottaa käyttöön, esimerkiksi just tällaisten politiikkojen, riskianalyysien, liiketoiminnan jatkuvuussuunnitelmien tekemisessä, niin siellä varmastikin heille räätälöidyiksi työkaluiksi tehdyt tekoälymallit varmasti nopeuttaisivat sitä konsultatiivista työtä ja tietysti raporttien kirjoittamista. Jos tehdään tietoturvatarkastuksia, niin raporttien kirjoittaminen yleensä on se pitkällisin ja kiusallisin vaihe niille konsulteille, varsinkin teknillisille konsulteille. Jos konsultti sitten vaan voisi syöttää ne tekniset tulokset johonkin tekoälymalliin, joka sitten kirjoittaisi siitä kivan ja hyvällä kieliopilla varustetun raportin ja*

> *monella kielelläkin saman tien, niin siinä olisi huikeaa säästöpotentiaalia. – H2*

> *– – [verraten tietoturva-ammattilaisiin] esimerkiksi jos mä olisin juristi, enkä aikoisi käyttää tekoälyä, niin sitten mä olisin hyvin huolissani, koska esimerkiksi tekoäly pystyy todella nopeasti jostain lakiteksteistä löytämään asioita tai tekemään jotain sopimuksia tai sopimuspohjia tai tulkitsemaan niitä sekunneissa, kun ihmiseltä siihen menee tunteja. Juristin työ ei välttämättä häviä mihinkään, mutta sä osaat sitten tehdä niitä asioita nopeammin tekoälyä hyödyntäen. – H1*

Tekoälyn hyödyntäminen työkaluna saattaa keventää työkuormaa, jolloin työn tehokkuus lisääntyy. Parhaimmillaan tekoälyn oikeaoppinen hyödyntäminen voi siis lisätä yrityksen kilpailuetua. Toinen haastateltavista muistuttaa, että vaikka yritys ei menettäisi markkina-asemaansa jättämällä käyttöönottamatta tekoälyä ja siihen liittyvää tekniikkaa, tietoturvauhat voivat kuitenkin lisääntyä.

> *– – pitää olla hereillä, tietoturvan tämmöisessä koulutuskäytössä, että jos sä oot ennen itse käsin naputtanut jonkun manuaalin Wordiin niin tuskin sä nyt mitään oleellista häviät, jos sä jatkatkin sitä, etkä käytä tekoälyä siinä. Mutta sitten taas vastaavasti se, että jos taas tää niin sanottu vastapuoli, 'pahikset', alkaa käyttämään tekoälyä jotenkin aivan uudella tavalla, mitä ei edes vielä tiedetä tai tajuta, että miten se onnistuu, niin kuin tekemällä just näitä esimerkiksi deepfake-videopuheluita, toimitusjohtajahuijaus onkin silloin vähän erilainen – – Niin sanotaan, että pitää olla varautunut, että miten tekoälyä voidaan käyttää hyödyksi. Vahingoittavissa tarkoituksissa ja sen torjumiseen. – H1*

4.3 Tekoälyn käyttömahdollisuudet tietoturvan hallinnassa

Tekstigeneratiivista tekoälyn käyttöä tietoturvan tukena ei kumpikaan haastateltavista ollut vielä havainnut. Toinen haastateltavista huomautti, että muita tekoälysovelluksia on tietoturvassa käytetty pidempäänkin, mutta laajat kielimallit ovat niin uusi ilmiö, ettei niillä ole vakiintunutta käyttöä edes tietoturvaan erikoistuneissa yrityksissä.

> *Tavallaan tekoälyä on erinäköisissä tietoturvateknologioissa jossain määrin jo hyödynnetty, kuten dataoppimista, mutta sitten näitä LLM:iä niin, jos niitä on hyödynnetty, se on tapahtunut vasta 2023 [jälkeen]. – H2*

> *Aika paljon nykyään tekoälysovellutukset tietoturvassa liittyy nimenomaan datan käsittelyyn ja datan pyörittämiseen. – H2*

Toisaalta toinen haastateltavista ei ole törmännyt ollenkaan edellä mainittuihin datan käsittelyyn liittyviin tekoälysovelluksiin. Tekstigeneratiivinen tekoäly saattaisi tarjota helpon ratkaisun suuren tietomäärän kanssa kamppailevalle työntekijälle.

> *– – voiko niille [tekoälysovelluksille] sitten syöttää jotain massiivista datamäärää, omaa dataa, ja sitten sanoa, että etsi tästä joku olennainen juttu – – Mulla on 20 eri PDF-dokumenttia meidän jostain tietojärjestelmistä ja jokaisessa on vaikka 20–30 sivua, niin siinä on aika monta sivua tekstiä ihmisen kahlata läpi. – H1*

4.3.1 Tietoturvapolitiikat

Kysyttäessä tekstigeneratiivisen tekoälyn potentiaalisista käyttömahdollisuuksista tietoturvan hallinnassa, molemmat haastateltavat nostivat esiin tietoturvapolitiikkojen laatimisen. Eräs haastateltavista totesi, kuinka tekoäly voisi avustaa juuri niiden politiikkojen laatimisessa. Toinen puolestaan korosti, että erityisesti pienet yritykset voivat hyötyä tekstigeneratiivisen tekoälyn luomista tietoturvapolitiikoista ja vihjasi, että isoimmilla yrityksillä on yleensä omat tietoturvavastaavat, joiden työtehtäviin niiden laatiminen kuuluu. Molemmat painottivat, että nimenomaan räätälöidyt ratkaisut ovat tärkeitä, mutta suuntaa antavat geneerisemmät ohjeistukset ovat kuitenkin tyhjää parempia.

> *– – toinen tärkeä osa [tietoturvassa] on se, että pitää tehdä jonkin sortin suunnitelma ja politiikka – – ja sitten se [tekoäly] voisi tehdä semmoisia tietoturvapolitiikkoja, manuaaleja ynnä muita. – H1*

Ja pienemmille yrityksille varmaan juuri tällainen politiikkojen ja prosessimallien luonti – – sen pitäisi syntyä nimenomaan keskustellen sen tekoälyn kanssa ja toisaalta se pitäisi itse myös luoda sen näköiseksi mitä se yritys sitten kaipaa ja tarvitsee. – H2

– – jos ajatellaan että tietoturvapolitiikka on vaan geneerinen paperi ja kaikilla on samanlainen politiikka, niin sitten ei ole täysin ymmärretty, että mistä on kyse, koska sen politiikanhan tulisi nimenomaan kuvastaa sen yrityksen omia käytänteitä ja omaan liiketoimintaan sopivia käytänteitä ja pitäisi ne sitten määritellä. – H2

4.3.2 Koulutus

Haastatteluissa tuli ilmi, kuinka yrityksissä varsin keskeisenä keinona tietoturvan parantamiseen pidettiin henkilöstön kouluttamista. Haastateltavat nostivat esiin, kuinka tekoäly voisi nopeuttaa koulutusmateriaalien laatimisessa, sekä kuinka se voisi räätälöidä materiaalin tietyille osastoille ja työtehtäville. Yksityiskohtainen räätälöinti ei yleisesti ottaen ole aikaisemmin ollut niin merkityksellistä, että siihen olisi kannattanut käyttää aikaa, mutta tekoälyn kanssa se onnistuisi nopeasti. Räätälöinti voisi tuoda lisäarvoa koulutukselle.

– – vaikka sulla on hyvä suunnitelma, mutta sä et ole sitä kouluttanut henkilöstölle niin se on melkein yhtä tyhjän kanssa. – H1

Koulutusohjelmia, perehdytysohjelmia tai jotain muita tällaisia vastaavia, niin se [tekoäly] voisi jotain runkoja tai miksi ei tekstejäkin tehdä. – H1

Sanotaan jos on vaikka vähänkin isompi firma ja siellä on erinäköisiä käytäntöjä, politiikkoja ja muita, niin jos siellä on vaikkapa 100 eri osastoa, niin tuskin niille tehdään mitään omaa manuaalia, mikä sopii just tähän hommaan. Mutta jos tekoälyn avulla pystyy tekemään jonkun paremman manuaalin tai ohjeen tai jonkun, mikä on räätälöity juuri tähän, niin ehkä sitä kautta voi tavallinenkin työntekijä saada siitä jotain irti, joka on juuri minulle ja minun osastolleni tehty. – H1

4.3.3 Tekstien ja mallien kirjoittaminen

Haastateltavat tuovat esille, kuinka tekoäly voisi luoda valmiita malleja ja toimintaohjeita yrityksen käyttöön. Eräs haastateltavista listaa erilaisia tekstipohjia, joiden luomisessa tekoäly voi auttaa, mainiten esimerkiksi tiivistelmien kirjoittamisen tai kriisiviestintään osallistumisen. Samalla hän ehdottaa, kuinka tekoälyn kanssa voisi esimerkiksi ideoida erilaisia skenaarioita, joiden pohjalta se sitten loisi yritykselle valmiita, räätälöityjä toimintaohjeita.

> *Sillä [tekoälyllä] voi teettää – – skenaarioita, eli voisi pyytää sitä luomaan semmoisia 'caseja' ja ajatuksia, niin se on yksi [esimerkki miten tekoälyä voi hyödyntää]. Toinen voisi olla sitten jonkin sortin koulutusmateriaaleja tai toimintaohjeita tai sitten juuri sellaisia tarkastuslistoja, mitä sitä voisi pyytää tekemään. – H1*

Haastateltava mainitsee esimerkkinä, että tekoäly voisi luoda tarkastuslistan siitä, kuinka yrityksen tulisi toimia työntekijän lopettaessa heillä. Listaamalla muun muassa käyttäjätunnusten poistamisen yritys pienentäisi tietoturvariskejä. Myös toinen haastateltava on samaa mieltä tekoälyn hyödyntämisestä mallien ja pohjien luomisessa, sekä mainitsee tekoälyn hyödyntämisen tietynlaisessa 'red-team'-roolissa:

> *– – äkkiseltään tulee mieleen tällainen niin kuin mallien ja pohjien tuottaminen. Ja sitten toinen voisi olla tällainen tietoturvan koulutusmateriaalit ja sellaisten ohjelmien tekeminen tai sitten tällaisten yritysten sisäisten kampanjoiden tekeminen, eli jos halutaan luoda sellaista tietoturvakulttuuria, niin hyödynnetään tekoälyä tekemään sitten huijausviestejä, joita sitten talon sisällä lähetellään ja katsotaan että langetaanko siihen. Ehkä tavallaan niin kuin sellaisten asioiden nopeuttaminen, mitä muuten ihmistyönä tehtäisiin. – H2*

4.3.4 Tekoäly neuvonantajana

Tekstin luomisen lisäksi haastateltavat nostavat esille, kuinka tekoälyn kanssa voi myös keskustella. Keskusteltaessa käyttäjät voisivat saada jotain lisätietoa tai näkemyksiä, mitä

itse ei olisi välttämättä keksinyt. Samalla tekoälyn kanssa keskustelu voisi vapauttaa tietoturva-ammattilaisten työaikaa, mikäli he aikaisemmin ovat panostaneet muiden työntekijöiden tietoturva-asioissa neuvomiseen.

> *– – suunnittelijatahoille esimerkiksi, ketkä suunnittelee tietoturvaa tai jotain riskejä tai muuta tällaista riskienhallintaa, niin niille [tekoäly voisi avittaa] just, että ne saa tällaisia eri näkökulmia asioihin, mitä ei olisi tullut mieleenkään. – H1*

> *– – [tekstigeneratiivisen tekoälyn yksi käyttömahdollisuus voisi olla] sellainen sisäinen tietoturvaneuvonantaja, joka voisi olla sellainen chatbotti, jolta voisi kysyä niin kuin tietoturvakonsultilta, elikkä se ois tällainen yrityksen sisäinen vastauspankki siihen. Jos jokin asia arveluttaa tai ei tiedä miten pitäisi tietoturvallisesti toimia jossain asiassa niin se pystyisi sitten antamaan vastauksia. Koska aika paljonhan talon sisäisten tietoturvaihmisten aikaa menee nimenomaan sellaisessa neuvonannossa, että jossain asiassa halutaan ottaa tietoturva huomioon, mutta ei tiedetä miten se tehdään, niin sitten ne kysyy ja tietoturvaihminen on siellä mukana neuvomassa ja kertomassa ja kouluttamassa. – H2*

Haastateltavat ovat tuoneet esiin esimerkkejä, kuinka geneeriset kielimallit voivat tuoda lisäarvoa tietoturvan hallintaan. Molemmat ovat kuitenkin sitä mieltä, että räätälöidyt tekoälyt olisivat kuitenkin tehtävissään tehokkaampia kuin geneeriset. Räätälöinti kuitenkin usein voi aiheuttaa lisäkustannuksia yrityksille.

> *Jos ajattelee tällaisia pakasta otettavia kielimalleja, niin ei ne hirveästi tuo itsessään siihen peruskäyttäjätasolle hirveästi lisäarvoa. Mutta tosiaan jos tehdään räätälöityjä tietoturvatekoälysovellutuksia, niin nehän pystyvät tuomaan [sitä lisäarvoa]. – H2*

4.4 Tekoälyn käyttöönottamisen haasteet

4.4.1 Kustannukset

Molemmat haastateltavista totesivat, että tietoturva on yritysten kannalta riskienhallintaa, joka ei tuota kassavirtaan lisää tuloja, eikä siihen täten haluta investoida. Yritykset pyrkivät usein ratkaisuihin, jotka eivät kustanna niille yhtään mitään.

> *Ei se [tietoturva] yritysten kassaan tuo yhtään mitään, että nää tietoturvatoimet, panostukset siihen tai ne asiat mitä siellä pitäis tehdä, niin niissä aina tasapainotellaan sen kanssa, kuinka paljon tähän voidaan rahaa käyttää ja mitä se uhka nyt oikeasti on ja onko se uhka todennäköinen vai eikö ole. Eli tavallaan vaikka se tarve olisi aivan polttava ja päivän selvä, niin siihen ei ole silti aivan selvää et siihen käytetään rahaa sitten tarvittava määrä. – H2*

> *Kannattaako meidän sijoittaa 20 000 € tietoturvaan, jos meidän suojattavan omaisuuden arvo on 21 000 €? – H1*

> *– – mekin jouduimme miettimään, kun oltiin pieni startup, kuinka paljon siihen [tietoturvaan] panostetaan. Kaikki mikä oli ilmaista ja jollain politiikalla säädeltävissä niin tehtiin, mutta jos olisi heti pitänyt ostaa… kalliita virustorjuntajärjestelmiä tai muita tuollaisia estojuttuja niin ei tehty. Mikä nyt on kustannustehokasta oikeastaan. – H1*

> *Mitä enemmän kustannuksia tulee, niin se on se kaikkein kriittisin asia. – H2*

Toinen haastateltavista nosti esiin, että vaikka tekstigeneratiiviset tekoälyt ovat kustannuksiltaan yleensä varsin edullisia, se ei ole riittävän houkutteleva aspekti, jotta yritykset alkaisivat käyttämään niitä tietoturvansa parantamiseen.

> *– – täytyy muistaa, että aika monessa tällaisessa firmassa sille tietoturvalle ei ole lähtökohtaisesti tehty mitään. Ei aikaisemmin ole ollut sellaista tietoturvakonsulttia, jolta on kyselty ja maksettu sille tuntihintaa. Jolloin tavallaan maksoi se mitä tahansa se palvelun käyttö, niin se on kalliimpaa kuin se nykytila mikä siinä firmassa on ollut. – H2*

Samalla todettiin, kuinka tekoälyn hyödyntämisen esteenä ei ole välttämättä kustannukset, vaan se on pikemminkin tekninen kysymys. Molemmat haastateltavat totesivat, että yrityksen toimiala vaikuttaa sen kykyyn siirtyä käyttämään tällaisia palveluita. Samalla annettiin esimerkkejä historiasta, kuinka siirtyminen sähköposteihin ja internetiin oli toisilla toimialoilla nopeampaa kuin toisilla.

> *Hinta ei varmaankaan ole tällä hetkellä este. Vaan enemmänkin se kynnys lähteä siihen. – H2*

> *– – digitalisaatiokynnys on valtavan korkea. Että tavallaan, jos se yritys itsessään, pieni yritys varsinkin, jos se ei toimi teknologia-alalla, niin kyllä ne johtavat henkilöt siellä on aikalailla tietokoneiden kanssa ummikkoja. – H2*

4.4.2 Luotettavuus

> *Ihan heti en luottaisi sataprosenttisesti mihinkään tekoälyyn enkä edes yksittäisen ihmisenkään älyyn. Jos sitä osaa käyttää osana inspiraation lähteenä, niin siinä se on varmaan hyvä. Se, että olisi joku aukoton automatisoija, missä ei olisi mitään ihmistä mukana [prosessissa], niin mielellään odottelisin hetken aikaa ja varmistuisin siitä, että se ihan satavarmasti toimii. – – mutta missä vaiheessa uskaltaa luottaa siihen tarpeeksi? – H1*

Keskusteltaessa tekoälyjen turvallisuudesta ja luotettavuudesta haastateltavien välille syntyy eroja. Ensimmäinen ei uskaltaisi käyttää tekoälyjä kuin hyvin geneerisesti, ellei se pyörisi täysin oman yrityksen sisällä eikä luovuttaisi tietoa esimerkiksi valmistajalleen koulutuskäyttöön. Toinen haastateltavista on puolestaan avoimempi, ja toteaa, kuinka palveluihin syötettävä tieto ei ole niin kriittistä haavoittuvuuksien määrän ja tiedon syöttämisen ja sen siirtymiseen käytetyn ajan osalta.

> *LLM:iä voidaan pyörittää omissa [tieto]kannoissa ja muuta. Dataa joka tapauksessa syötetään nykyäänkin tietoturvayritysten omiin järjestelmiin ja toki sieltä sitä vähän varmaan poistetaankin mutta enenevissä määrin*

[tietoturvayhtiöiden] asiakkaatkin haluavat sellaista vertailukelpoisuutta ja historiallista dataa. – H2

– – niitä haavoittuvuuksia on ihan riittävästi niissä yritysten järjestelmissä joka tapauksessa, se että jostain [tekoälyn opetusmateriaalista] löytyy joku tietoturvaraporttidata kolmen vuoden takaa jostain, niin se on aika pieni murhe. Jos sitä ei korjattu sen raportin luovuttamisen jälkeen, niin silloin [tietoturvayhtiön] asiakas saa syyttää itse itseään. – H2

Jos se on ChatGPT:n malli ja haluaisit käydä sen kanssa keskustelua sun firman tietoturvakäytänteistä, niin pitääkö olla huolissaan tiedon luottamuksellisuudesta tai mihin se sitten ylipäätään päätyy, niin tämä on varmaan se sellainen eettis-moraalinen kulma mitä yrityksissä mietitään, ja varsinkin monet tietoturvaihmiset varmasti miettii aika paljon, että voiko niiden tekoälyjen kanssa edes käydä keskusteluja, missä annetaan niille luottamuksellista tietoa. – – varmaan itse edustan enemmän tällaista kaupallistoiminnallista näkemystä, missä jälleen kerran monessa asiassa pitää ottaa riskejä ja jos on pakka kasassa niin varmaan tarvitsee ottaa hallittuja riskejä. Mutta sitten taas monet kovanluokan tietoturvaihmiset ovat sitten hyvin mustavalkoisia siinä, että ei voi laittaa, koska ei ole todistettu, että se tieto sieltä vuotaisi tai se päätyisi vääriin käsiin tai muuta. – H2

Vastauksista voidaan päätellä, kuinka aihe on varsin mielipiteitä jakava. Jotkut priorisoivat tietoturvan korkeammalle, ja toiset taas keskittyvät tehokkuuteen. Toinen haastateltavista nostaa esille, kuinka yritys ja toimiala vaikuttavat mielipiteeseen – hän nostaa esimerkiksi, kuinka autokorjaamoissa ei todennäköisesti murehdita tietoturvasta yhtä paljon, kuin ohjelmistotaloissa.

Molemmat haastateltavista olivat yhtä mieltä siitä, että tekoäly tulee olemaan tietoturvan hallinnassa aputyökalu, joka ei korvaa tietoturva-ammattilaisia. Toisaalta se myös madaltaa kynnystä etenkin pienemmille yrityksille laajentaa tietoturvatyötään. Ainakin toistaiseksi tekstigeneratiivinen tekoäly ei haastateltavien mukaan kykene toimimaan automaattisesti ilman ihmisten ohjeistusta.

Kuten sanottu, se on työkalu, joka nopeuttaa asioita, mitä voitaisiin ihmisten voiminkin tehdä. – H2

5 JOHTOPÄÄTÖKSET JA YHTEENVETO

5.1 Johtopäätökset

Kirjallisuuden mukaan digitalisaation myötä tietoturvan hallinta on muodostunut yrityksille entistä merkittävämmäksi (Antunes ym., 2021). Tämä havainto sai vahvistusta haastatteluista, joissa saatiin konkreettisia esimerkkejä tietoturvan tärkeyden kasvusta viime vuosina. Tutkimuksen perusteella on ilmennyt, että tietojen suojaamisen lisäksi niiden saatavuuden ja helpon käytettävyyden turvaaminen on ehdottoman tärkeää.

Haastattelut vahvistivat aiemmissa tutkimuksissa tehtyjä havaintoja, joiden mukaan tekoälyä voidaan hyödyntää erilaisten skenaarioiden luomisessa ja niihin liittyvien toimintaohjeiden laatimisessa. Tähän samaan johtopäätökseen ovat aiemmin päätyneet myös Gupta ym. (2023) sekä Iqbal ym. (2023). Haastatteluissa tuli myös ilmi, kuinka tekstigeneratiivinen tekoäly voisi tarjota monipuolisia näkökulmia tietoturvaan liittyvissä kysymyksissä. Samaa mieltä ovat Gupta ym. (2023), jotka ovat todenneet, että kielimallit kykenevät tukemaan organisaatioita päätöksenteossa tarjoamalla kattavia näkemyksiä. Lisäksi haastattelujen perusteella kävi selväksi, että laajoja kielimalleja voitaisiin käyttää eräänlaisina keskustelukumppaneina, joiden avulla voidaan esittää tietoturvaan liittyviä kysymyksiä ja ideoida uusia skenaarioita. Aiemmissa tutkimuksissa Al-Hawawreh, Aljuhani ja Jararweh (2023, 3424) ovat päätyneet samaan tulokseen, korostaen kielimallien tehokkuutta ideointityökaluina.

Aikaisemmissa tutkimuksissa Montezino ja Fenz (2011), Gill ym. (2021) sekä Hussain ym. (2022) ovat osoittaneet uskovansa, että tekoäly mahdollistaa tietoturvan osittaisen automatisoinnin. Haastattelut kuitenkin osoittivat, että automatisaatioon ei ole vielä riittävästi luottamusta. Lisäksi korostettiin, että tekoäly toimii ihmisen käyttämänä työkaluna eikä kykene toimimaan itsenäisesti, mikä rajoittaa sen täydellistä automatisoitavuutta. Siitä huolimatta, että tekoäly ei tällä hetkellä kykene itsenäiseen toimintaan ilman ihmisen ohjausta, sen merkitys manuaalisesti suoritettujen prosessien nopeuttajana on selkeä ja kiistaton.

Aikaisemmissa tutkimuksissa on havaittu, että laajat kielimallit kykenevät laatimaan tietoturvaan liittyviä raportteja, mikä nopeuttaa niiden kirjoittamiseen käytettävää aikaa (Gupta ym., 2023; Iqbal ym., 2023). Tässä tutkimuksessa saavutettiin samankaltainen lopputulos. Laajoilla kielimalleilla on kyky muuttaa teknistäkin dataa selkokielelle, mikä mahdollistaa ammattijargonin selittämisen käyttäjille, jotka eivät ole aiheen asiantuntijoita (Gupta ym., 2023). Haastattelujen perusteella tätä kykyä voitaisiin hyödyntää esimerkiksi tietoturvaraportoinnissa, jossa tekniset asiantuntijat syöttäisivät kielimallille teknisen datan ja tarkastaisivat sen tuottaman raportin. Yksi tämän tutkimuksen johtopäätöksistä on, että kielimallit voivat nopeuttaa ihmisten työtehtävistä suoriutumista, esimerkiksi kirjoittamalla nopeasti raportteja, joiden valmistuminen käsin veisi huomattavasti enemmän aikaa (Gupta ym., 2023). Laajat kielimallit voivat siis tehostaa työskentelyä (Feuerriegel ym., 2022). Haastatteluissa tuli myös esiin, kuinka tekoälyn mahdollistama tehokkuuden lisääntyminen voisi jopa kasvattaa yritysten markkina-arvoa, kun resursseja voidaan keskittää tehokkaammin. Useaan otteeseen korostettiin, että tekoäly ei korvaa nykyisiä työntekijöitä eikä tuo täysin uusia kyvykkyyksiä, vaan se toimii tukityökaluna työskentelyssä. Oikein käytettynä se kykenee tehostamaan työskentelyä vähentämällä työtehtäviin käytettävää aikaa. Aiemmassa kirjallisuudessa Sandoval ym. (2022) päätyivät samaan lopputulokseen.

Haastatteluissa havaittiin, että tekoäly kykenee tuottamaan räätälöityjä ohjeistuksia ja malleja. Iqbal ym. (2023) ovat osoittaneet, että tekoäly on jo kyennyt luomaan räätälöityjä ohjeita ja menettelytapoja. Lisäksi sekä haastattelut että kirjallisuus (Iqbal ym., 2023) osoittavat tekoälyn kyvyn analysoida suuria tietomääriä, mikä voi vähentää ihmistyön kuormaa ja parantaa tietoturvaa, sillä suuria datamääriä ei aikaisemmin ole ehkä käsitelty kaikissa yrityksissä yhtä perusteellisesti. Aiemmassa kirjallisuudessa on havaittu, että erityisesti laajat kielimallit kykenevät tehokkaasti prosessoimaan laajoja tietomääriä, myös tietoturva-alalla (Iqbal ym., 2023; Budhwar ym., 2023; Gupta ym., 2023). Haastattelujen perusteella selvisi, että tietoturvayrityksissä käytetään jo tekoälysovelluksia datan käsittelyyn, mutta helppokäyttöisen tekoälysovelluksen kysyntä on suuri myös pienemmissä yrityksissä. Laajat kielimallit, kuten OpenAI:n GPT-mallit, joille voi syöttää omaa dataa, pystyisivät vastaamaan tähän kasvavaan tarpeeseen (OpenAI, 2023).

Haastatteluissa nousi esiin huoli siitä, että yritykselle kriittinen tieto saattaisi levitä eteenpäin, esimerkiksi tekoälyn palveluntarjoajalle. Al-Hawawreh ym. (2023) ovat tehneet saman havainnon, mainiten luottamuksen puutteen olevan merkittävä haaste tekstigeneratiivista tekoälyä käytettäessä. Uusi havainto oli kuitenkin, että jotkin yritykset saattavat tietoisesti olla valmiita ottamaan riskejä luovuttamalla tietoturvahaavoittuvuuksiin liittyvää tietoa laajoille kielimalleille. Tämä havainto on ristiriidassa aiemman kirjallisuuden, kuten Nancylia ym. (2014), kanssa, joka korostaa kaiken tiedon suojattuna pitämisen tärkeyttä. Tämä eroavaisuus havainnoissa saattaa johtua siitä, että eri tahot priorisoivat asiat eri tavoin.

Tekstigeneratiivisen tekoälyn yksi merkittävimmistä vahvuuksista on aiempien tutkimusten (Kasneci ym., 2023; Al-Hawawreh ym., 2023, 3425; Iqbal ym., 2023) mukaan kyky luoda räätälöityä opetusmateriaalia. Tämä havainto vahvistui myös tässä tutkimuksessa, kun molemmat haastateltavat korostivat tekoälyn potentiaalia opetusmateriaalin luomisessa. Haastatteluissa kävi ilmi, että yrityksissä pidetään henkilöstön kouluttamista keskeisenä keinona tietoturvan parantamiseen. Haastateltavat toivat esiin, kuinka tekoäly nopeuttaa koulutusmateriaalien laatimista ja mahdollistaa niiden räätälöinnin tietyille osastoille ja työtehtäville. Yksityiskohtaisen räätälöinnin merkitys on aikaisemmin ollut vähäistä, mutta tekoälyn avulla se onnistuu nopeasti ja voisi tuoda lisäarvoa koulutukselle.

Tutkimuksessa kävi ilmi, että laajat kielimallit voisivat auttaa etenkin pienempiä yrityksiä tietoturvapolitiikkojen luomisessa, räätälöimällä ne kunkin yrityksen tarpeiden ja toimintaympäristön mukaan. Tähän tavoitteeseen voitaisiin päästä keskustelemalla kielimallien kanssa, mikä mahdollistaisi yksilöllisesti sopivien politiikkojen kehittämisen. Toisaalta suuremmissa yrityksissä politiikkojen luonti on usein tietoturva-asiantuntijan vastuulla. Nämä asiantuntijat kykenevät hyödyntämään tekoälyä oman toimintansa tehostamiseksi, mikä on myös tuotu esiin aiemmassa kirjallisuudessa. Al-Hawawreh ym. (2023) mainitsevat, että tietoturva-asiantuntijat ovat jo käyttäneet laajoja kielimalleja tietoturvan viitekehysten ja politiikkojen luonnin apuna.

Aikaisemmissa tutkimuksissa on havaittu, että laajat kielimallit voivat toimia tehokkaina apuvälineinä myös kyberrikollisille, esimerkiksi auttamalla aidompien tietojenkalasteluviestien kirjoittamisessa (Okey ym., 2023; Gupta ym., 2023; Kshetri,

2023). Tämän tutkimuksen perusteella näitä kielimallien kykyjä voitaisiin kuitenkin hyödyntää myös tietoturvan hallinnassa tarjoamalla todentuntuisia ”red team” harjoituksia. Nämä harjoitukset voivat tehostaa tietoturvakulttuuria opettamalla työntekijöitä tunnistamaan tietojenkalasteluviestejä käytännön kokemuksen kautta. Samalla tässä tutkimuksessa tuodaan esiin, että kun kielimallit yleistyvät, myös tietoturvauhat kehittyvät ja monimutkaistuvat.

Kirjallisuuden perusteella laajoja kielimalleja voidaan hyödyntää myös tietoturvan hallinnan teknisimmissä osa-alueissa. On jo todettu, että kielimallit ovat tehokkaita analysoimaan laajoja datamääriä, luomaan koodipohjaa sekä havaitsemaan ja muokkaamaan koodissa olevia haavoittuvuuksia (McKee & Noever, 2022; Al-Hawawreh ym., 2023; Iqbal ym., 2023; Gupta ym., 2023). Lisäksi ne kykenevät tunnistamaan tietoturvahäiriöitä ja -uhkia sekä reagoimaan niihin (Jamal & Hayden, 2023). Tässä tutkimuksessa haastateltavilla ei kuitenkaan ollut laajempaa kokemusta tietoturvan teknisemmästä puolesta, minkä vuoksi tutkimuksessa ei voida tehdä päätelmiä laajojen kielimallien potentiaalista tässä kontekstissa. Lisäksi tämän tutkimuksen perusteella tekoäly, joka on koulutettu nimenomaan tietoturvaan räätälöidysti, suoriutuisi tietoturvaan liittyvistä tehtävistä geneeristä tekoälyä paremmin. Aiemmissa tutkimuksissa, kuten Paria ym. (2023), on osoitettu, että toimialakohtainen koulutus parantaa kielimallien suorituskykyä.

Yrityksillä on usein kynnys panostaa riskienhallintamenetelmiin, sillä ne eivät tuota lisää kassavirtaa. Tähän päätelmään päätyivät tämän tutkimuksen lisäksi ainakin Antunes ym. (2021). Silti tietoturvaan panostaminen olisi tärkeää, sillä laiminlyöminen voi aiheuttaa kustannuksia (Goel & Shawky, 2009; Shaikh & Siponen, 2023). Tämän tutkimuksen perusteella yritykset usein panostavat tietoturvaan siinä määrin, kun se on kustannustehokasta. Vaikka ilmaisia ja varsin edullisia tekoälysovelluksia on olemassa (OpenAI, 2023), yrityksillä voi silti olla valtava teknologinen kynnys hyödyntää niitä. Lisäksi haastatteluissa kävi ilmi, että monet yritykset eivät ole osoittaneet minkäänlaista kiinnostusta tietoturvaan, joten edullisetkin tekoälyratkaisut ovat niille kalliimpia kuin nykykäytäntö.

5.2 Yhteenveto

Tämän tutkimuksen tavoitteena oli tutkia laajojen kielimallien potentiaalia organisaatioiden tietoturvan hallinnassa. Tutkimuksessa pyrittiin kartoittamaan kielimallien käyttömahdollisuuksia sekä käyttöönoton haasteita. Tutkimustehtävään vastattiin tutustumalla aiempaan kirjallisuuteen sekä haastattelemalla asiantuntijoita. Kirjallisuuskatsauksessa käsiteltiin tietoturvan hallinnan perusperiaatteita, laajojen kielimallien roolia näiden periaatteiden tukena sekä niiden teknisiä yksityiskohtia ja rajoitteita. Haastattelut tarjosivat syvempää ymmärrystä siitä, miten asiantuntijat näkevät näiden teknologioiden hyödyt ja rajoitteet, sekä konkreettisia käyttötapauksia ja haasteita.

Kirjallisuuden perusteella on selvää, että tietoturvan hallinta on keskeinen osa organisaatioiden toimintaa, ja siihen panostaminen on elintärkeää liiketoiminnan jatkuvuuden kannalta. Laajat kielimallit voivat tukea tietoturvaa monin tavoin, kuten analysoimalla suuria tietomääriä, tuottamalla tietoturvaraportteja ja auttamalla uusien uhkien tunnistamisessa. Lisäksi kielimallit voivat analysoida suuria määriä kyberhyökkäysdataa, auttaa tunnistamaan uusia uhkia ja tarjota ratkaisuja. Samalla on tärkeää huomioida, että näiden mallien tuottama tieto ei aina perustu faktoihin, ja ne voivat tuottaa virheellisiä tai harhaanjohtavia vastauksia.

Haastattelut vahvistivat kirjallisuuden löydökset ja toivat esiin käytännön haasteita, kuten teknologisen kynnyksen ja kustannusten merkityksen erityisesti pienille ja keskisuurille yrityksille. Haastateltavat korostivat myös, että laajat kielimallit voivat merkittävästi parantaa työtehoa vapauttamalla asiantuntijat keskittymään vaativampiin tehtäviin. Haastateltavat toivat esille konkreettisia käyttötapauksia, joissa laajat kielimallit voivat tukea tietoturvapolitiikkojen luomista, koulutusta sekä skenaarioiden ja toimintaohjeiden laatimista.

Tutkimuksen tulokset osoittivat, että laajojen kielimallien käyttö tietoturvan hallinnassa voi tuoda merkittäviä etuja, kuten parantaa raportointia, nopeuttaa analyysiprosesseja ja tukea päätöksentekoa tarjoamalla kattavia näkemyksiä turvallisuustilanteista. Tekoälyä voidaan hyödyntää skenaarioiden luomisessa, koulutusmateriaalien ja toimintaohjeiden laatimisessa sekä tietoturvapolitiikkojen kehittämisessä. Samalla kuitenkin korostettiin, että laajojen kielimallien käyttöön liittyy merkittäviä haasteita, kuten teknologiset ja

kustannukselliset esteet sekä luottamukseen liittyvät kysymykset. Yritykset saattavat epäröidä tekoälyn käyttöönottoa näiden haasteiden vuoksi.

Haastateltavat korostivat, että vaikka tekoäly voi toimia tehokkaana työkaluna tietoturvan hallinnassa, se ei voi täysin korvata ihmisten asiantuntemusta, vaan toimii pikemminkin heidän työnsä tukena. Laajat kielimallit tarjoavat siis monia mahdollisuuksia tietoturvan hallintaan, mutta niiden käyttö vaatii huolellista suunnittelua sekä henkilöstön koulutusta ja osaamisen varmistamista.

5.3 Jatkotutkimusehdotukset

Tämä tutkimus oli pintapuolinen ja tarjosi yleiskatsauksen laajojen kielimallien potentiaalista organisaatioiden tietoturvan hallinnassa, mutta jatkotutkimuksissa voidaan syventyä tarkemmin yksittäisiin aiheisiin. Esimerkiksi laajojen kielimallien tarkempi rooli tietoturvan automatisoinnissa tai niiden vaikutus tietoturvapolitiikkojen kehittämiseen tarjoavat syvällisempiä tutkimuskohteita. Myös tietoturvaan liittyvien eettisten kysymysten sekä laajojen kielimallien käyttöön liittyvien teknologisten ja kustannuksellisten esteiden tutkiminen voisi tarjota arvokasta tietoa siitä, mitä vaatimuksia organisaatioiden on täytettävä hyödyntääkseen tekoälyä tehokkaammin tietoturvansa parantamisessa.

Tulevissa tutkimuksissa voitaisiin lisäksi keskittyä enemmän konkreettisiin esimerkkeihin laajojen kielimallien käytöstä tietoturvan hallinnassa, kuten yksityiskohtaisiin tapaustutkimuksiin eri organisaatioista ja toimialoilta. Tämä mahdollistaisi syvällisemmän ymmärryksen siitä, miten kielimalleja on käytännössä sovellettu ja millaisia tuloksia on saavutettu.

LÄHTEET

Alto, V. (2023). *Modern Generative AI with ChatGPT and OpenAI Models : Leverage the Capabilities of OpenAI's LLM for Productivity and Innovation with GPT3 and GPT4.* (1st ed.). Packt Publishing, Limited.

Al-Hawawreh, M., Aljuhani, A., & Jararweh, Y. (2023). Chatgpt for cybersecurity: practical applications, challenges, and future directions. *Cluster Computing*, *26*(6), 3421–3436. https://doi.org/10.1007/s10586-023-04124-5

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219–238. https://doi.org/10.3390/jcp1020012

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information (Basel)*, *10*(4), 122-. https://doi.org/10.3390/info10040122

Budhwar, P., Chowdhury, S., Wood, G., Aguinis, H., Bamber, G. J., Beltran, J. R., Boselie, P., Lee Cooke, F., Decker, S., DeNisi, A., Dey, P. K., Guest, D., Knoblich, A. J., Malik, A., Paauwe, J., Papagiannidis, S., Patel, C., Pereira, V., Ren, S., … Varma, A. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal*, *33*(3), 606–659. https://doi.org/10.1111/1748-8583.12524

Chen, Y., Arunasalam, A., & Celik, Z. B. (2023). Can Large Language Models Provide Security & Privacy Advice? Measuring the Ability of LLMs to Refute Misconceptions. *arXiv.Org*. https://doi.org/10.48550/arxiv.2310.02431

Chopra, A., & Chaudhary, M. (2019). *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines* (1st ed.). Apress L. P. https://doi.org/10.1007/978-1-4842-5413-4

Derner, E., & Batistič, K. (2023). Beyond the Safeguards: Exploring the Security Risks of ChatGPT. *arXiv.Org*. https://doi.org/10.48550/arxiv.2305.08005

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., & Lestable, T. (2023). Revolutionizing Cyber Threat Detection with Large Language Models. *arXiv.Org*. https://doi.org/10.48550/arxiv.2306.14263

Feuerriegel, S., Shrestha, Y. R., von Krogh, G., & Zhang, C. (2022). Bringing artificial intelligence to business management. *Nature Machine Intelligence*, *4*(7), 611–613. https://doi.org/10.1038/s42256-022-00512-5

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, *48*(2), 213-.

Gill, A. K., Zavarsky, P., & Swar, B. (2021). Automation of Security and Privacy Controls for Efficient Information Security Management. 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 371–375. https://doi.org/10.1109/ICSCCC51823.2021.9478126

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, *11*, 80218–80245. https://doi.org/10.1109/ACCESS.2023.3300381

Hariri, W. (2023). Unlocking the Potential of ChatGPT: A Comprehensive Exploration of its Applications, Advantages, Limitations, and Future Directions in Natural Language Processing. *arXiv.Org*. https://doi.org/10.48550/arxiv.2304.02017

Heisel, M., Joosen, W., López, J., & Martinelli, F. (2014). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. In *Engineering Secure Future Internet Services and Systems* (Vol. 8431, pp. 315–344). Springer International Publishing AG. https://doi.org/10.1007/978-3-319-07452-8_13

Hertzman, C. P., Meagher, N., & McGrail, K. M. (2013). Privacy by Design at Population Data BC: A case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. Journal of the American Medical Informatics Association : JAMIA, 20(1), 25–28. https://doi.org/10.1136/amiajnl-2012-001011

Hirsjärvi, S., & Hurme, H. (2020). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö* ([2. painos].). Gaudeamus.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Hussain, K., Vanathi, D., Jose, B. K., Kavitha, S., Rane, B. Y., Kaur, H., & Sandhya, C. (2022). Internet of Things- Cloud Security Automation Technology Based on Artificial Intelligence. 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 42–47. https://doi.org/10.1109/ICAAIC53929.2022.9792664

Ilmonen, I., Kallio, J., Koskinen, J., & Rajamäki, M. (2022). *Johda riskejä : käytännön opas yrityksen riskienhallintaan* (4. päivitetty painos.). FINVA Finanssikoulutus.

Iqbal, F., Samsom, F., Kamoun, F., & MacDermott, Á. (2023). When ChatGPT goes rogue: exploring the potential cybersecurity threats of AI-powered conversational chatbots. *Frontiers in Communications and Networks*, *4*. https://doi.org/10.3389/frcmn.2023.1220243

ISACA. (2019). COBIT 2019 framework: Introduction and methodology. https://www.isaca.org/resources/cobit

Jamal, S., & Wimmer, H. (2023). An Improved Transformer-based Model for Detecting Phishing, Spam, and Ham: A Large Language Model Approach. *arXiv.Org*. https://doi.org/10.48550/arxiv.2311.04913

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management*, *21*(3), 699–722. https://doi.org/10.1007/s10257-023-00646-y

Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., … Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, *103*, 102274-. https://doi.org/10.1016/j.lindif.2023.102274

Von Krogh, G., Roberson, Q., & Gruber, M. (2023). RECOGNIZING AND UTILIZING NOVEL RESEARCH OPPORTUNITIES WITH ARTIFICIAL INTELLIGENCE. *Academy of Management Journal*, *66*(2), 367–373. https://doi.org/10.5465/amj.2023.4002

Kshetri, N. (2023). Cybercrime and Privacy Threats of Large Language Models. *IT Professional*, *25*(3), 9–13. https://doi.org/10.1109/MITP.2023.3275489

Kucharavy, A., Schillaci, Z., Maréchal, L., Würsch, M., Dolamic, L., Sabonnadiere, R., Dimitri Percia David, Mermoud, A., & Lenders, V. (2023). Fundamentals of Generative Large Language Models and Perspectives in Cyber-Defense. *ArXiv.Org*. https://doi.org/10.48550/arxiv.2303.12132

Line, M. B., Tøndel, I. A., & Gjære, E. A. (2011). A Risk-Based Evaluation of Group Access Control Approaches in a Healthcare Setting. Availability, Reliability and Security for Business, Enterprise and Health Information Systems, 6908, 26–37. https://doi.org/10.1007/978-3-642-23300-5_3

MacTaggart, P., & Fiore, S. (2011). Health Care Reform and the Internet. Availability, Reliability and Security for Business, Enterprise and Health Information Systems, 6908, 82–88. https://doi.org/10.1007/978-3-642-23300-5_7

McKee, F., & Noever, D. (2022). Chatbots in a Botnet World. *ArXiv.Org*. https://doi.org/10.48550/arxiv.2212.11126

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annales Des Télécommunications*, *76*(3–4), 255–270. https://doi.org/10.1007/s12243-020-00783-2

Montesino, R., & Fenz, S. (2011). Information Security Automation: How Far Can We Go? 2011 Sixth International Conference on Availability, Reliability and Security, 280–285. https://doi.org/10.1109/ARES.2011.48

Nancylia, M., Mudjtabar, E. K., Sutikno, S., & Rosmansyah, Y. (2014). The measurement design of information security management system. *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 1–5. https://doi.org/10.1109/TSSA.2014.7065914

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5). U.S. Department of Commerce.

Okey, O. D., Udo, E. U., Rosa, R. L., Rodríguez, D. Z., & Kleinschmidt, J. H. (2023). Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis. *Computers & Security*, *135*, 103476-. https://doi.org/10.1016/j.cose.2023.103476

Paria, S., Dasgupta, A., & Bhunia, S. (2023). DIVAS: An LLM-based End-to-End Framework for SoC Security Analysis and Policy-based Protection. *arXiv.Org*. https://doi.org/10.48550/arxiv.2308.06932

PCI Security Standards Council (2022). *Payment Card Industry Data Security Standard. Requirements and Testing Procedures.* Version 4.0. Haettu osoitteesta: https://www.pcisecuritystandards.org/document_library/ [19.2.2024]

Petkauskas, V. (2023). Lessons learned from ChatGPT's Samsung leak. Cybernews. Haettu osoitteesta: https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/ 4.12.2023.

Sandoval, G., Hammond Pearce, Nys, T., Karri, R., Garg, S., & Dolan-Gavitt, B. (2022). Lost at C: A User Study on the Security Implications of Large Language Model Code Assistants. *arXiv.Org*. https://doi.org/10.48550/arxiv.2208.09727

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3). https://doi.org/10.1007/s42979-021-00557-0

Sebastian, G. (2023). Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. *International journal of security and privacy in pervasive computing*, *15*(1), 1–14. https://doi.org/10.4018/IJSPPC.325475

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974-. https://doi.org/10.1016/j.cose.2022.102974

Sharma, L., & Garg, P. K. (Eds.). (2022). *Artificial intelligence : technologies, applications, and challenges* (First edition.). CRC Press, Taylor & Francis Group.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." Journal of Enterprise Information Management, 27(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

von Solms, B., von Solms, R. (2004). The 10 deadly sins of information security management, Computers & Security, Volume 23, Issue 5, Pages 371-376, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2004.05.002. (https://www.sciencedirect.com/science/article/pii/S0167404804001221)

Suomen Standardisoimisliitto. (2020). Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto (SFS 27000:2020).

Suomen Standardisoimisliitto. (2023a). Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset (SFS 27001:2023).

Suomen Standardisoimisliitto. (2023b). Informaatioteknologia. Tekoäly. Tekoälyä koskevat käsitteet ja sanasto (SFS 22989:2023).

Teubner, T., Flath, C. M., Weinhardt, C., van der Aalst, W., & Hinz, O. (2023). Welcome to the Era of ChatGPT et al: The Prospects of Large Language Models. *Business & Information Systems Engineering*, *65*(2), 95–101. https://doi.org/10.1007/s12599-023-00795-x

Tjoa, A. M. (2011). Availability, Reliability and Security for Business, Enterprise and Health Information Systems: IFIP WG 8.4/8.9 International Cross Domain Conference and Workshop, ARES 2011, Vienna, Austria, August 22-26, 2011. Proceedings (Vol. 6908, pp. xiii–xiii). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-23300-5

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Tammi.

Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. Haettu osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf 4.12.2023

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2009). Effective information security: A Summary of General Instructions on Information Security Management. Finland: Ministry of Finance.

Wang, J., Xiao, N., & Rao, H. R. (2015). Research Note—An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior. *Information Systems Research*, *26*(3), 619–633. https://doi.org/10.1287/isre.2015.0581

Zaboli, A., Choi, S. L., Tai-Jin, S., & Hong, J. (2023). ChatGPT and other Large Language Models for Cybersecurity of Smart Grid Applications. Cornell University Library, arXiv.org.

LIITTEET

LIITE 1: Teemahaastattelun haastattelurunko

1. Johdanto

- Kerro lyhyesti opiskelu- ja työtaustastasi sekä kokemuksestasi tekoälyn ja tietoturvan parista.
- Onko sinulla kokemusta erityisistä projekteista tai tehtävistä alaan liittyen?

2. Tietoturvan nykytila ja haasteet

Nykytilan ymmärtäminen

- Millainen merkitys tietoturvalla on nykypäivän organisaatioissa?
- Mitä eri elementtejä pidät tietoturvan keskeisinä osa-alueina?
- Mikä on tietoturvan hallintajärjestelmien (ISMS) merkitys organisaation toiminnassa ja miten ne suhteutuvat tietoturva-alan yleisesti hyväksyttyihin parhaisiin käytäntöihin?

Haasteet

- Mitä erityisiä tietoturvauhkia ja tietoturvaan liittyviä vaatimuksia (kuten GDPR) organisaatiot kohtaavat?
- Kuvaile tyypillisiä ongelmia, joita organisaatiot kohtaavat tietoturvan hallinnassa.
- Usein mainitaan, että inhimilliset tekijät ovat tietoturvan suurin haaste. Miten niihin voidaan vaikuttaa?

Tulevaisuuden näkymät

- Millaisia trendejä olet havainnut tietoturva-alalla viime vuosina, ja kuinka ne voivat muokata organisaatioiden lähestymistapaa tietoturvaan?

3. Tekoälyn käyttö tietoturvassa

- Minkälaisia mahdollisuuksia näet tekoälyn tarjoavan tietoturvan hallinnalle ja miten se voi muuttaa perinteisiä lähestymistapoja?
- Voitko antaa esimerkkejä siitä, miten tekoälyä on jo hyödynnetty tietoturvan hallinnassa ja millaisia tuloksia se on tuottanut?
- Mitä käyttötapauksia voisit kuvitella tekstigeneratiiviselle tekoälylle tietoturvan kontekstissa?

Tekoälyn hyödyntämisen haasteet

- Mitkä ovat suurimmat esteet ja haasteet tekoälyn käyttöönotossa tietoturvan näkökulmasta, mukaan lukien tekniset, taloudelliset, turvallisuuteen ja eettisyyteen liittyvät tekijät?

- Missä aspekteissa tekoäly ei voi auttaa?

4. Tietoturvan tulevaisuus tekoälyn myötä

- Millaiset tahot hyötyvät eniten tekoälyn käytöstä tietoturvan hallinnassa (esimerkiksi johto, IT-osasto, tavalliset työntekijät)?
- Mitä toimenpiteitä organisaatioiden tulisi tehdä valmistautuakseen tekoälyn tuomiin muutoksiin tietoturvan hallinnassa?
- Millaisia ratkaisuja ja sovelluksia tekoälyn odotetaan tuovan lähivuosina?
- Millaisia muutoksia odotat tietoturva-ammattilaisten työnkuvassa tapahtuvan tulevaisuudessa?
- Voiko tekoälyä hyödyntää tietoturvan parantamisessa samalla tavalla Suomessa kuin muualla maailmassa, ottaen huomioon esimerkiksi lainsäädännölliset erot?
- Mitä odotat eniten tulevaisuudelta tekoälyn ja tietoturvan alueella?

5. Lopetus

- Onko jotain, mitä et ole vielä tuonut esille, mutta joka olisi tärkeää mainita tässä yhteydessä?