Generatiivisen tekoälyn hyödyntäminen ulkoistetun turvallisuuspäällikön työssä syksyllä 2025

Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Tero Ruokonen

Takana Oy

Tampere 29.3.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Tämän työn aiheena on generatiivisen tekoälyn käyttökelpoisuus ulkoistetun turvallisuusasiantuntijan työssä tilanteissa, joissa asiantuntija tukee tai sijaistaa asiakasorganisaation turvallisuuspäällikköä. Tarkastelu kohdistui matkustusturvallisuuteen, tilannekuvan muodostamiseen sekä poikkeama ja kriisitilanteiden tukemiseen syksyllä 2025 toteutuneissa toimeksiannoissa. Tavoitteena oli selvittää, miten tekoälyä voidaan hyödyntää niin, että se tukee analyysiä ja päätöksentekoa vaarantamatta tiedon luotettavuutta tai turvallisia toimintatapoja.

Työ toteutettiin laadullisena, teoriaohjaavaa lähestymistapaa noudattavana kehittämistutkimuksena. Aineisto kerättiin kolmessa vaiheessa asiantuntijakyselyllä, yksilöllisillä teemahaastatteluilla ja ryhmätyöpajalla, jossa aiempia havaintoja validoitiin ja tarkennettiin. Analyysi tehtiin teoriaohjaavana sisällönanalyysina, ja viitekehys rakentui turvallisuusjohtamisen, matkustusturvallisuuden, riskienhallinnan, tilannekuvan muodostamisen sekä tekoälyn asiantuntijakäytön tarkastelulle.

Tulosten mukaan generatiivinen tekoäly on käyttökelpoinen vain tietyin ehdoin. Suurin hyöty kohdistui tiedon jäsentämiseen, hajanaisen aineiston kokoamiseen, alustavan tilannekuvan muodostamiseen, vaihtoehtojen vertailuun ja analyysin valmisteluun. Tekoäly ei korvannut asiantuntijan harkintaa, kontekstiosaamista, vastuunkantoa eikä päätöksentekoa. Käyttökelpoisuus riippui organisaation turvallisuusjohtamisen rakenteiden selkeydestä, lähtöaineiston laadusta ja siitä, kuinka systemaattisesti tekoälyn tuottamaa sisältöä validoitiin.

Keskeiset rajoitteet liittyivät kontekstin ymmärtämiseen, ajantasaisuuteen, lähteiden laatuun ja näennäisesti uskottavan mutta virheellisen sisällön riskiin. Johtopäätöksenä generatiivinen tekoäly toimii tarkoituksenmukaisesti vain hallitusti, rajatusti ja asiantuntijan johtamassa työprosessissa. Tekoäly ei ole vaihtoehto turvallisuusasiantuntijalle vaan hänen työtään tehostava väline.

Avainsanat: generatiivinen tekoäly, turvallisuusjohtaminen, ulkoistettu turvallisuusasiantuntija, matkustusturvallisuus, tilannekuva, päätöksenteon tuki, validointi

Abstract

This thesis examines the usability of generative artificial intelligence in the work of an outsourced security specialist in situations where the specialist supports or substitutes the client organization's security manager. The analysis focused on travel security, the formation of situational awareness, and support for incident and crisis situations in assignments carried out in autumn 2025. The objective was to determine how AI can be used to support analysis and decision-making without compromising information reliability or safe operating practices.

The study was conducted as a qualitative development-oriented research project applying a theory-guided approach. Data were collected in three stages using an expert survey, individual themed interviews, and a workshop in which earlier findings were validated and refined. The analysis employed theory-guided content analysis, and the theoretical framework drew on security management, travel risk management, risk management, situational awareness, and professional use of AI.

The results indicate that generative AI is usable only under specific conditions. The greatest benefits concerned structuring information, consolidating scattered material, building a preliminary situational picture, comparing alternatives, and preparing analysis. AI did not replace the specialist's judgement, contextual expertise, accountability, or decision-making. Usability depended primarily on the clarity of the client's security-management structures, the quality of the available source material, and the systematic validation of AI-generated content.

Key limitations related to contextual understanding, timeliness of information, source reliability, and the risk of producing content that appears credible yet is incorrect or poorly suited to the situation. The main conclusion is that generative AI is appropriate only when used in a controlled and bounded manner within a specialist-led work process. AI is not a substitute for the security professional but a tool that enhances professional work.

Keywords: Generative AI, Security Management, Outsourced Security Expert, Travel Security, Situational Awareness, Decision Support, Validation

Sisältö

1 Johdanto 1
1.1 Tausta ja ongelmanasettelu 2
1.2 Työn tavoite 3
1.3 Rajaukset 3
1.4 Menetelmä ja aineisto 4
1.5 Keskeiset käsitteet ja määrittely 4
2 Teoreettinen viitekehys 6
2.1 Turvallisuusjohtaminen asiantuntijatyön perustana 6
2.2 Matkustusturvallisuus ja riskienhallinta 8
2.3 Standardit 10
2.4 Tiedon hajanaisuus ja tilannekuvan muodostamisen haasteet 12
2.5 Tekoälyn rooli asiantuntijatyössä 14
2.6 Teoreettisen viitekehyksen yhteenveto 17
3 Tutkimusasetelma, menetelmät ja aineisto 19
3.1 Tutkimusasetelma 19
3.2 Menetelmät ja tutkimusote 20
3.3 Aineisto 21
3.4 Tiedonkeruun kolme vaihetta 21
3.4.1 Asiantuntijakysely 22
3.4.2 Puolistrukturoidut teemahaastattelut 22
3.4.3 Ryhmätyöpaja (validointi) 22
3.5 Analyysimenetelmä 23
3.6 Tutkimuksen luotettavuus ja eettisyys 24
4 Tutkimustulokset 26
4.1 Asiantuntijakyselyn keskeiset havainnot 26
4.2 Yksilöhaastattelujen keskeiset havainnot 28
4.3 Ryhmätyöpajan validointihavainnot 30
4.4 Yhteenveto tutkimustuloksista 32
5 Johtopäätökset ja pohdinta 34
5.1 Johtopäätökset suhteessa tutkimuskysymykseen 34
5.2 Tekoälyn käyttökelpoisuuden ehdot ulkoistetun turvallisuusasiantuntijan työssä 35
5.3 Tutkimuksen rajoitukset 38
5.4 Yhteenveto: mitä tulokset merkitsevät ulkoistetun turvallisuusasiantuntijan työssä 40
5.5 Jatkotutkimus- ja kehittämisehdotukset 41
6 Lähdeviitteet ja kirjallisuusluettelo 44

1 Johdanto

Turvallisuusympäristö on muuttunut viime vuosina tavalla, joka korostaa turvallisuusjohtamisen systemaattisuutta ja ennakoivaa riskienhallintaa myös organisaatioissa, joissa turvallisuus ei ole ydinliiketoimintaa. Geopoliittinen jännitteisyys, kyberuhat, tietosuojavaatimusten kiristyminen ja maineriskien nopea eskaloituminen ovat laajentaneet turvallisuuden kokonaisuutta fyysisestä suojautumisesta kohti toimintakyvyn ja luottamuspääoman turvaamista. Tämän kehityksen vaikutus näkyy erityisen konkreettisesti ulkomaan työmatkoissa ja ulkomailla pitkäaikaisesti toteutettavissa työtehtävissä (ulkomailla asuvat - expatriate), joissa turvallisuusriskit voivat olla monitasoisia ja muuttua nopeasti. Kriisialueilla matkustamiseen liittyvät geopoliittiset jännitteet, sisäiset konfliktit, terrorismin uhka ja poliittinen epävakaus haastavat perinteiset käytännöt ja edellyttävät ennakoivaa riskienhallintaa, sekä suunniteltuja erityisjärjestelyjä. Samalla työnantajan vastuu korostuu eettisenä velvoitteena huolehtia henkilöstön hyvinvoinnista ja turvallisuudesta myös haastavissa toimintaympäristöissä, sillä turvallisuuden laiminlyönti voi johtaa henkilöstöriskien lisäksi taloudellisiin, maineellisiin ja oikeudellisiin seurauksiin. (Takana, 2025a; Takana, 2025b; Takana, 2026a; Takana, 2025 c)

Samaan aikaan teknologinen kehitys, erityisesti generatiivisen tekoälyn nopea murros, on muuttanut asiantuntijatyön luonnetta. Viimeisen kahden vuoden aikana generatiiviset kielimallit (GenAI) ovat kehittyneet poikkeuksellisen nopeasti, mikä on johtanut tilanteeseen, jossa käytettävät työkalut ja menetelmät voivat muuttua jo kuukausien sisällä. Tämä kehitysvauhti näkyy myös turvallisuustyössä: tekoäly tarjoaa mahdollisuuksia tiedon jäsentämiseen, tilannekuvan tuottamiseen ja ohjeistuksen valmisteluun, mutta samalla se pakottaa arvioimaan uudelleen luotettavuuden, validoinnin ja vastuunjaon periaatteita. Edellä mainitut muutokset toimintaympäristössä ja työnantajan vastuu toiminnan eettisestä pitävyydestä voivat edellyttää turvallisuuden asi-

antuntijapalveluiden tilapäiselle tai jatkuvaluonteiselle ulkoistamiselle. Tämän työn lähtökohta ei ole kuvata tekoälyä yleisellä tasolla, vaan tarkastella sen käytettävyyttä ulkoistetussa turvallisuusasiantuntijatyössä, jossa matkustusturvallisuus, tilannekuvan muodostaminen ja poikkeamienhallinta ovat keskiössä. (Takana, 2025a; Takana, 2025b)

Tämän työn ytimessä on seuraava tutkimuskysymys: miten generatiivista tekoälyä voidaan hyödyntää ulkoistetun turvallisuusasiantuntijan työssä siten, että se tukee analyysiä ja päätöksentekoa, mutta ei vaaranna tiedon luotettavuutta tai turvallisia toimintatapoja?

1.1 Tausta ja ongelmanasettelu

Ulkopuolinen turvallisuusasiantuntija kutsutaan organisaation tueksi tyypillisesti tilanteissa, joissa organisaation oma turvallisuustoiminto ei ole käytettävissä tai kapasiteetti ei riitä. Tällöin ulkoistettu turvallisuusasiantuntija joutuu nopeasti omaksumaan organisaation sisäisen ohjeistuksen, johtosuhteet ja raportointikäytännöt ja toimimaan samalla käytännön työn tasolla matkustusturvallisuuden ja poikkeamatilanteiden tukena. Tämä korostaa rakenteen ja dokumentaation merkitystä: jos politiikat, ohjeet ja toimintamallit eivät ole selkeästi löydettävissä ja sovellettavissa, ulkoistetun asiantuntijan työ muuttuu helposti reaktiiviseksi, ja aikaa kuluu olennaisen tiedon etsimiseen ja tulkintaan.

Ulkoistetun turvallisuusasiantuntijan työ on myös tiedonhallintaa. Tilannekuva muodostuu samanaikaisesti kansainvälisistä uutislähteistä, viranomaisviestinnästä, turvallisuusorganisaatioiden analyyseista, paikallisista havainnoista sekä organisaation omista ohjeista ja prosesseista. Tietoa on usein paljon, mutta se on hajallaan ja vaihtelevan laatuista. Tiedon yhdistäminen koherentiksi, toimintaa ohjaavaksi kokonaisuudeksi vaatii huomattavaa työpanosta juuri silloin, kun tilanteet muuttuvat nopeasti. Tästä syntyy työn varsinainen ongelma: voiko generatiivinen tekoäly tehostaa ulkoistetun turvallisuusasiantuntijan kykyä jäsentää suuria tietomassoja ja muodostaa tilannekuvaa niin, että analyysin laatu ja päätöksenteon luotettavuus eivät heikkene.

Poikkeama- ja kriisitilanteiden osalta keskeistä on myös tiedon nopea luokittelu ja eskalointi. Turvallisuustyössä on tunnistettava, onko kyseessä poikkeama vai kriisi, joka edellyttää laajemman kriisijohtamisen rakenteen akti-

voimista. Generatiivinen tekoäly voi tukea tiedon jäsentämistä ja vaihtoehtojen vertailua, mutta se ei voi tehdä päätöstä siitä, miten tai mikä organisaation johtomalli aktivoidaan ja kuka kantaa päätösvastuun. Tästä syystä tekoälyn rooli on tässä kontekstissa nähtävä analyysin vahvistajana, ei päätöksentekijänä.

1.2 Työn tavoite

Tämän lopputyön tavoitteena on tarkastella generatiivisen tekoälyn käyttökelpoisuutta ulkoistetun turvallisuusasiantuntijan työssä ja kuvata, millä edellytyksillä tekoäly voi parantaa työn laatua, tehokkuutta ja päätöksenteon tukea. Tarkoituksena on tuottaa toimintamalli, jonka avulla tekoäly voidaan liittää osaksi ulkoistetun toimijan turvallisuusjohtamista hallitusti ja luotettavasti, käytännön tasolla. Samalla työ arvioi tekoälyn tuottamaa lisäarvoa ja rajoitteita konkreettisessa toimeksiantokontekstissa sekä tunnistaa jatkokehitystarpeita, koska teknologian nopea kehitys tekee pitkäjänteisestä arvioinnista haastavaa.

Työn tavoitteena ei ole tuottaa valmista työkalupakettia, vaan rakentaa selkeä rakenne ja perusteltu kokonaiskuva, jonka pohjalta organisaatio voi kehittää omia ohjeistuksiaan ja käytäntöjään tekoälyn hyödyntämiseksi, ulkoistetun turvallisuusasiantuntijan toteuttamissa toimeksiannoissa.

1.3 Rajaukset

Työ on rajattu koskemaan ulkoistetun turvallisuusasiantuntijan käytännön tehtäviä matkustusturvallisuuden, tilannekuvan muodostamisen sekä poikkeamienhallinnan ja kriisijohtamisen tukemisen kontekstissa. Tarkastelun kohteena on se, miten tekoäly soveltuu turvallisuusasiantuntijan arjen työvaiheisiin, joissa tieto on hajallaan, aikapaine on merkittävä ja organisaation ohjeistukseen on kyettävä nojaamaan nopeasti. Ajallisesti havainnot ovat kerätty syksyllä 2025 tapahtuneista todellisista toimeksiannosta, joissa turvallisuusasiantuntija on kutsuttu asiakasorganisaation tueksi joko sijaistamaan turvallisuuspäällikköä tai johtamaan yllättäen alkaneen poikkeustilanteen toimenpiteitä.

Työ ei käsittele tekoälyn teknisiä toteutuksia tai mallien kehittämistä, fyysisiä turvallisuusjärjestelmiä eikä tietoturva-arkkitehtuurin suunnittelua. Työ ei

käsittelemään tekoälyn eettisiä kysymyksiä laajalla yhteiskunnallisella tasolla, vaan tarkastelu on rajattu käytännön asiantuntijatyön käyttökelpoisuuteen ja luotettavuuden varmistamiseen ulkoistetun turvallisuusasiantuntijan toimeksiantoympäristössä.

1.4 Menetelmä ja aineisto

Tutkimus toteutettiin laadullisena, teoriaohjaavaa lähestymistapaa noudattavana kehittämistutkimuksena. Aineisto kerättiin kolmessa vaiheessa: asiantuntijakyselyllä, yksilöhaastatteluilla sekä ryhmätyöpajalla, jossa aiemmissa vaiheissa muodostettuja havaintoja validoitiin ja tarkennettiin. Aineiston analyysissa hyödynnettiin teoriaohjaavaa sisällönanalyysiä, jotta havaintoja voitiin tarkastella sekä käytännön kokemusten että teoreettisen viitekehyksen kautta.

Tutkimuksen teoreettinen viitekehys rakentuu turvallisuusjohtamisen, matkustusturvallisuuden, riskienhallinnan sekä tekoälyn asiantuntijakäytön tarkastelulle. Aineisto koostuu aiempien toimeksiantojen dokumenteista sekä turvallisuusasiantuntijoiden kokemuksista. Aineisto on anonymisoitu siten, ettei työ sisällä viittauksia toimeksiantajaorganisaatioihin tai tunnistettaviin yksityiskohtiin. Tutkimusasetelma on rajattu tiettyyn toimeksiantokokonaisuuteen ja ajanjaksoon, jotta tulkinta pysyy johdonmukaisena nopeasti muuttuvasta teknologiaympäristöstä huolimatta.

1.5 Keskeiset käsitteet ja määrittely

Tässä luvussa kerrotaan tämän opinnäytetyön keskeiset käsitteet, jotka ovat ulkoistettu turvallisuusasiantuntija, matkustusriskienhallinta, poikkeama ja kriisi, tilannekuva, generatiivinen tekoäly ja validointi.

> Ulkoistetulla turvallisuusasiantuntijalla tarkoitetaan asiantuntijaa, joka tukee tai tilapäisesti sijaistaa asiakasorganisaation turvallisuuspäällikköä toimeksiannon aikana, osana organisaation turvallisuustoimintojen tuottamista tai hankintaa ja niihin liittyviä rooleja, vastuita ja valvontaa (ISO 18788:2015; ISO 31030:2021).

> Matkustusriskienhallinnalla tarkoitetaan työmatkustamiseen liittyvien riskien ennakointia, ohjeistamista, seurantaa ja tarvittavien tuki-

toimien koordinointia organisaation velvoitteiden ja käytäntöjen mukaisesti, ohjelmamaisena matkustusriskienhallintana (ISO 31030:2021).

Poikkeamalla tarkoitetaan tapahtumaa tai tilannetta, joka poikkeaa normaalista ja edellyttää hallittuja toimenpiteitä sekä tilanteen johtamista roolien, vastuiden ja yhteistoiminnan kautta, kun taas kriisillä tarkoitetaan laajempaa, nopeasti eskaloituvaa tai merkittäviä vaikutuksia aiheuttavaa tilannetta, joka edellyttää organisaation jatkuvuuden ja johtamiskyvyn järjestelmällistä aktivointia ja toimeenpanoa (ISO 22320:2018; ISO 22301:2019).

Tilannekuvalla tarkoitetaan useista lähteistä koottua ja jatkuvasti päivittyvää kokonaisnäkemystä, jonka tarkoituksena on tukea päätöksentekoa ja ohjeistamista; tilannekuva voi muodostua sekä organisaation ylläpitämänä että matkustajan omien havaintojen kautta (Puolustusvoimat, 2025).

Generatiivisella tekoälyllä tarkoitetaan järjestelmiä, jotka tuottavat uutta sisältöä (esim. tekstiä) käyttäjän antamien syötteiden perusteella, ja joiden käyttö tässä työssä rajautuu asiantuntijatyön tukemiseen (NIST, 2024).

Validoinnilla tarkoitetaan tässä työssä menettelyä, jossa tekoälyn tuottama sisältö tarkistetaan lähteiden, ajantasaisuuden ja kontekstin sopivuuden osalta ennen käyttöä päätöksenteon tukena, koska generatiiviseen tekoälyyn liittyy riskejä kuten uskottavalta vaikuttavan mutta virheellisen sisällön tuottaminen ja liiallinen luottaminen tuotoksiin, mikä korostaa ihmisen valvontaa ja arviointia (NIST, 2024).

2 Teoreettinen viitekehys

Tässä luvussa muodostetaan teoreettinen viitekehys, jonka varaan työn empiirinen tarkastelu rakentuu. Viitekehyksen tehtävänä on kuvata ne käsitteet, rakenteet ja periaatteet, jotka määrittävät ulkoistetun turvallisuusasiantuntijan työn luonnetta matkustusturvallisuuden, tilannekuvan muodostamisen sekä poikkeama- ja kriisitilanteiden hallinnan kontekstissa. Viitekehyksessä kuvataan ensin turvallisuusjohtaminen asiantuntijatyön perustana ja se, miksi ulkoistetun asiantuntijan rooli korostaa rakenteiden ja vastuiden selkeyttä. Tämän jälkeen tarkastellaan matkustusturvallisuutta riskienhallinnan näkökulmasta ja kuvataan, miten tilannekuva muodostuu tiedonkeruun, jalostamisen ja analyysin kautta. Kolmannessa osassa käydään läpi keskeiset standardit, jotka toimivat yhteisenä kielenä ja vertailupohjana organisaatioiden käytännöille. Lopuksi tarkastellaan tiedon hajanaisuutta ja tekoälyn roolia asiantuntijatyössä, jotta empiiriset havainnot voidaan myöhemmin tulkita johdonmukaisesti suhteessa tähän kehikkoon.

2.1 Turvallisuusjohtaminen asiantuntijatyön perustana

Turvallisuusjohtaminen voidaan jäsentää riskiperusteiseksi johtamiseksi, jossa organisaatio tunnistaa, arvioi ja käsittelee toimintaansa kohdistuvia uhkia sekä varmistaa toimintakyvyn myös häiriö- ja kriisitilanteissa. Tämän työn näkökulmasta olennaista on, että turvallisuusjohtaminen ei ole erillinen turvallisuustoiminto, vaan osa organisaation johtamisjärjestelmää: tavoitteet, roolit, päätöksenteko ja dokumentointi muodostavat kokonaisuuden, jonka on toimittava myös paineen alla ja epävarmuudessa. Riskiperusteisen ajattelun perustaksi voidaan käyttää riskienhallinnan standardia, ISO 31000:2018 Risk management - Guidelines, joka antaa periaatteet ja ohjeet riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan sekä viestintään koko organisaatiossa Standardin keskeinen viesti on, että riskienhallinta tulee integroida organisaation hallintoon, strategiaan, suunnitteluun ja raportointiin sekä toimintakulttuuriin, jolloin se palvelee päätöksentekoa eikä jää irralliseksi arviointiharjoitukseksi (ISO 31000:2018).

Turvallisuusjohtamisen kyvykkyys ei kuitenkaan rajaudu riskien tunnistamiseen, vaan se näkyy erityisesti siinä, kuinka organisaatio varautuu häiriöihin ja palautuu niistä. Tätä näkökulmaa tukee liiketoiminnan jatkuvuuden hallintajärjestelmän standardi, ISO 22301:2015 Security and resilience — Business continuity management systems — Requirements, joka määrittää vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmälle (Business Continuity Management System, BCMS) ja antaa viitekehyksen dokumentoidun järjestelmän suunnitteluun, käyttöönottoon, seurantaan, ylläpitoon ja jatkuvaan parantamiseen siten, että organisaatio pystyy suojaamaan toimintaansa, vähentämään häiriöiden todennäköisyyttä ja varmistamaan toipumisen häiriötilanteista. Ulkoistetun turvallisuusasiantuntijan työn kannalta tämä korostuu tilanteissa, joissa matkustukseen, ulkomaantoimintaan tai poikkeamiin liittyvät tapahtumat voivat uhata kriittisiä toimintoja, ja päätöksentekoa on tuettava myös silloin, kun organisaation oma turvallisuusorganisaatio ei ole täysimääräisesti käytettävissä (ISO 22301:2019). (Takana 2026a)

Poikkeama- ja kriisitilanteissa turvallisuusjohtamisen onnistuminen riippuu lisäksi siitä, kuinka selkeästi organisaatio kykenee johtamaan tilannetta, jakamaan vastuut ja hallitsemaan tietoa. Häiriötilanteiden hallintaan osoitettu standardi, ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management, antaa ohjeistuksen poikkeamien hallintaan (Incident Management) ja korostaa periaatteita sekä rakenteita, jotka liittyvät rooleihin ja vastuisiin, tehtäviin, resurssien hallintaan sekä yhteiseen ohjaukseen ja yhteistyöhön tilanteissa, joissa yksi tai useampi organisaatio toimii yhdessä tapahtuman hallitsemiseksi (ISO 22320:2018). Tämä on relevanttia tilanteen hoitamiseksi hankitun asiantuntija resurssin osalta, koska kyseinen asiantuntija toimii käytännössä osana organisaation tilannejohtamisen ketjua ja tarvitsee selkeän päätöksenteko- ja raportointimallin, jotta tehtävät ja vastuut eivät jää epäselviksi, ja estä työn tehokasta toteuttamista. (Takana 2026a)

Koska tämän työn konteksti painottuu ulkomaan matkustamiseen ja ulkomailla toteutettaviin työtehtäviin, turvallisuusjohtamisen viitekehystä on tarkoituksenmukaista täydentää matkustusriskienhallinnan standardilla. ISO 31030:2021 Travel risk management — Guidance for organizations, antaa organisaatioille ohjeet matkustamiseen liittyvien riskien hallintaan ja tarjoaa rakenteisen lähestymistavan politiikan ja ohjelman kehittämiseen, uhkien ja

vaarojen tunnistamiseen, riskien arviointiin sekä ehkäisy- ja lieventämisstrategioihin. Standardi rajaa tarkastelunsa organisaation puolesta tehtävään matkustamiseen ja soveltuu toimialasta ja koosta riippumatta, mikä tekee siitä käyttökelpoisen vertailupohjan myös ulkoistetulle turvallisuusasiantuntijalle (ISO 31030:2021). (Takana 2025a)

Ulkoistamisen näkökulmasta turvallisuusjohtamisen perustaa on lisäksi hyödyllistä peilata yksityisen turvallisuusalan turvallisuusoperaatioiden johtamisjärjestelmän standardista, ISO 18788:2015 Management system for private security operations — Requirements with guidance for use, joka tarjoaa viitekehyksen turvallisuusoperaatioiden hallinnalle ja korostaa toiminnan ammattimaisuutta, riskiperusteista johtamista sekä vastuullisuutta, mukaan lukien lain noudattaminen ja ihmisoikeuksien kunnioittaminen (ISO 18788:2015). Tämä on relevanttia ulkoistetun turvallisuusasiantuntijan työn kannalta, koska ulkoistaminen on käytännössä turvallisuuspalvelun tuottamista tai hankkimista, jolloin onnistuminen edellyttää: roolien, vastuiden, dokumentoinnin ja valvonnan selkeyttä samalla tavalla kuin muussakin riskiperusteisessa johtamisessa (ISO 18788:2015). (Takana 2025b)

2.2 Matkustusturvallisuus ja riskienhallinta

Matkustusturvallisuus on turvallisuusjohtamisen osa-alue, jossa työnantajan velvollisuus huolehtia henkilöstön turvallisuudesta konkretisoituu erityisesti ulkomaan työmatkoissa sekä ulkomailla pitkäkestoisesti toteutettavissa työtehtävissä. Kriisialueille suuntautuva matkustaminen ja toimintaympäristöt, joissa turvallisuustilanne on epävakaa, nostavat esiin riskien moniulotteisuuden: geopoliittiset jännitteet, sisäiset konfliktit, terrorismin uhka ja poliittinen epävakaus voivat muuttaa turvallisuustilannetta nopeasti, eikä perinteinen “varovaisuus” riitä hallitsemaan tilannetta, saati täyttämään työnantajan huolehtimisvelvollisuutta. Lisäksi infrastruktuurin haavoittuvuudet, kuten epäluotettavat viestintäyhteydet, sähkökatkokset ja kulkuyhteyksien äkilliset katkokset, edellyttävät vaihtoehtoisten toimintamallien ja erityisjärjestelyjen suunnittelua ennen matkaa sekä matkan aikana. (Takana 2025b)

Matkustusturvallisuuden johtaminen voidaan ankkuroida matkustusriskienhallinnan viitekehykseen, jota ISO 31030 standardi kuvaa organisaatioille suunnattuna ohjeistuksena. Standardi määrittää, että matkustamiseen liittyviä riskejä tulee tarkastella sekä organisaation että matkustajien näkökulmasta, ja

se antaa rakenteisen lähestymistavan matkustusriskien hallinnan kehittämiseen, käyttöönottoon, arviointiin ja säännölliseen tarkasteluun. Tämän näkökulman kannalta keskeistä on, että matkustusturvallisuus ei ole yksittäisten matkojen ympärille rakennettu ohje, vaan ohjelmamainen kokonaisuus, jossa politiikka, riskien arviointi sekä ehkäisy- ja lieventämistoimet muodostavat toisiaan tukevan rakenteen. ISO 31030 standardi myös rajaa soveltamisalansa organisaation puolesta tehtävään matkustamiseen, mikä tekee siitä luontevan viitepisteen työmatkustamisen ja ulkomaantoiminnan tarkasteluun. (ISO 31030:2021)

Riskienhallinnan yleinen logiikka voidaan puolestaan kuvata ISO 31000 -standardin kautta, jossa riskienhallinta nähdään periaatteiden ja ohjeiden kokonaisuutena riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan sekä viestintään koko organisaatiossa. Matkustusturvallisuuden näkökulmasta tämä tarkoittaa, että matkakohtainen riskiarvio ei ole irrallinen turvallisuustarkistus, vaan osa organisaation päätöksentekoa. Riskinottohalukkuus, hyväksymiskäytännöt, roolit ja vastuut sekä dokumentointi muodostavat yhdessä sen, mitä matkustaja voi tehdä, sekä millä edellytyksillä matka hyväksytään ja miten organisaatio toimii, jos tilanne muuttuu. (ISO 31000:2018) Mikäli matkustamisen riskit realisoituvat, turvallisuusjohtamisen rakenne näkyy erityisesti eskaloinnissa ja johtamisessa, jolloin organisaation on kyettävä siirtymään nopeasti tilannekuvan ylläpidosta kohti päätöksentekoa ja toimenpiteiden koordinointia. Tällöin Incident Management -toiminnan periaatteet, roolit ja vastuut sekä yhteistyö ja yhteinen ohjaus nousevat keskeisiksi, ja näitä ISO 22320 käsittelee Incident Managementin ohjeistuksena. Samalla matkustamiseen liittyvien häiriöiden vaikutukset organisaation toimintakykyyn korostaa jatkuvuudenhallinnan merkitystä. ISO 22301 standardi määrittää vaatimukset dokumentoidulle jatkuvuudenhallintajärjestelmälle, jonka tarkoitus on suojata toimintaa, vähentää häiriöiden todennäköisyyttä ja varmistaa toipuminen häiriötilanteista.

Matkustusturvallisuus on kuitenkin muutakin kuin riskiprosessi. Se on myös työnantajan vastuullisuuden ja toimintakulttuurin mittari, koska matkustamiseen liittyvä riskienhallinta edellyttää organisaatiolta politiikkaa, roolien ja vastuiden määrittelyä, viestintää sekä ohjelman seurantaa ja säännöllistä arviointia, ja riskienhallinnan periaatteet tulee integroida osaksi organisaation johtamista ja toimintakulttuuria (ISO 31030:2021; ISO 31000:2018). Kriisialueiden matkustusturvallisuus edellyttää kokonaisvaltaista lähestymistapaa,

jossa riskit tunnistetaan ennakoivasti, turvallisuussuunnittelu tehdään systemaattisesti ja tilannetta seurataan jatkuvasti, jotta reagointi muuttuviin olosuhteisiin on mahdollista. Samassa yhteydessä korostuu myös yritysvastuun näkökulma, jossa vastuullinen organisaatio huolehtii henkilöstönsä turvallisuudesta myös haastavissa toimintaympäristöissä, mikä vaikuttaa työntekijöiden sitoutumiseen ja sidosryhmien luottamukseen. (Takana 2025b) Jos varautuminen ja toimintamallit jäävät puutteellisiksi, organisaation kyky toimia johdonmukaisesti heikkenee. Monissa organisaatioissa kriisitilanteisiin varautuminen on puutteellista ja vain noin kolmasosalla suomalaisia organisaatioita on ajantasainen ja kattava toimintamalli kriisitilanteiden varalle. Tämä havainto on olennainen myös matkustusturvallisuuden kannalta: ulkomaanmatkoissa ja ulkomaantoiminnassa poikkeamat voivat eskaloitua nopeasti, jolloin valmiiksi määritellyt toimintamallit, vastuut ja harjoittelu ovat käytännössä se mekanismi, joka muuttaa riskienhallinnan paperilta toiminnaksi. (Takana 2025c)

2.3 Standardit

Kansainväliset standardit muodostavat turvallisuusjohtamiseen ja matkustusriskienhallintaan yhteisen viitekehyksen, jonka avulla organisaatio voi kuvata tavoitteensa, roolinsa, prosessinsa ja vaatimustenmukaisuuden yhdenmukaisella tavalla. Standardien arvo tässä työssä ei ole todistaa yksittäisen organisaation toimintaa oikeaksi tai vääräksi, vaan tarjota rakenne, jonka avulla ulkoistetun turvallisuusasiantuntijan työ voidaan kytkeä organisaation johtamiseen niin, että päätöksenteko perustuu dokumentoituun ja toistettavaan toimintatapaan. Standardien mukainen toiminta määrittelee ulkoistetun turvallisuusasiantuntijan työskentelyn perusmallin, jota hän peilaa kulloisenkin organisaation omaan turvallisuusjohtamisen malliin ja käytänteisiin. Strukturoitu osaaminen korostuu erityisesti tilanteissa, joissa turvallisuusjohtamisen käytännöt ovat hajallaan tai painottuvat liikaa yksittäisten henkilöiden hiljaiseen tietoon, jolloin ulkoistettu turvallisuusasiantuntija voi esittää toimintamalleja, jotka kestävät jälkikäteistarkastelun. (Takana 2025a)

Riskienhallinnan näkökulmasta ISO 31000 standardi toimii perustana, joka määrittää riskienhallinnan periaatteet ja ohjeistuksen sekä korostaa riskienhallinnan integrointia organisaation johtamiseen, strategiaan, suunnitteluun ja toimintakulttuuriin. Tässä toimintakulttuurissa turvallisuusjohtaminen ja

matkustusturvallisuus eivät näyttäydy irrallisina käytäntöinä, vaan johdonmukaisena tapana tunnistaa riskejä, arvioida niitä ja määrittää toimenpiteet, joiden avulla organisaatio hallitsee epävarmuutta. (ISO 31030:2021)

Jatkuvuudenhallinnan ja häiriötilanteisiin varautumisen osalta ISO 22301 standardi tuo viitekehyksen dokumentoidulle jatkuvuudenhallintajärjestelmälle, jonka tarkoitus on suojata toimintaa, vähentää häiriöiden todennäköisyyttä ja varmistaa toipuminen häiriötilanteista. Tämä on tärkeätä matkustamiseen ja ulkomaantoimintaan liittyvissä tilanteissa, joissa organisaation toimintakyky voi heikentyä nopeasti sekä henkilöstöön kohdistuvien riskien että infrastruktuurihäiriöiden vuoksi. Kun jatkuvuudenhallinnan periaatteet on jäsennetty ja dokumentoitu, myös ulkoistetun asiantuntijan kyky tukea toimintaa paranee merkittävästi, koska päätöksenteon reunaehdot, vastuut ja toimintamallit ovat olemassa eikä niitä tarvitse selvittää tai rakentaa tilanteen keskellä. (ISO 22301:2019)

Poikkeama- ja kriisitilanteiden johtamisen osalta ISO 22320 standardi tarjoaa Incident Management -toimintaan ohjeistuksen, joka määrittelee mm. roolit ja vastuut, tehtävien ja resurssien hallinnan sekä toiminnan ohjauksen ja yhteistyön tilanteissa, joissa yksi tai useampi organisaatio toimii yhdessä tapahtuman hallitsemiseksi. Viitekehys tukee erityisesti sellaista tilannetta, jossa ulkoistettu turvallisuusasiantuntija tulee osaksi organisaation tilannejohtamisen ketjua ja jossa työn tehokkuus riippuu siitä, kuinka nopeasti tehtävät, vastuut ja raportointimalli saadaan selväksi ja toimivaksi. (ISO 22320:2018)

Matkustusriskienhallinnan osalta ISO 31030 standardi on keskeinen, koska se käsittelee organisaation matkustamiseen liittyvien riskien hallintaa ja antaa rakenteellisen lähestymistavan ohjaavan politiikan ja ohjelman kehittämiseen, uhkien ja vaarojen tunnistamiseen, riskien arviointiin sekä niiden ehkäisy- ja lieventämisstrategioihin. (ISO 31030:2021) Standardi on tässä työssä luonteva viitepiste siksi, että matkustusturvallisuus kriisialueilla edellyttää käytännössä ohjelmamaista kokonaisuutta, jossa ennakoiva riskien tunnistaminen, turvallisuussuunnittelu ja jatkuva seuranta nivoutuvat yhteen, eikä turvallisuutta voida rakentaa pelkän yleisen varovaisuuden varaan. (Takana 2025b)

Ulkoistetun turvallisuusasiantuntijatyön ja niistä johdettujen turvallisuuspalveluiden johtamisen näkökulmasta ISO 18788 standardi tarjoaa viitekehyksen turvallisuusoperaatioiden hallinnalle (Security Operations Management System, SOMS) ja korostamalla riskiperusteista johtamista ja vastuullisuutta. Turvallisuuspalveluiden ulkoistaminen, mukaan lukien turvallisuudenasiantuntijapalvelut, tarkoittaa käytännössä turvallisuuspalvelun tuottamista tai hankkimista, jolloin roolien, vastuiden, dokumentoinnin ja valvonnan selkeys muodostaa edellytyksen sille, että palvelu tuottaa arvoa eikä jää irralliseksi suoritteeksi. (ISO 18788:2015)

Yhteenvetona standardit muodostavat tässä työssä rakenteen, jonka avulla turvallisuusjohtamista, matkustusturvallisuutta ja poikkeamienhallintaa voidaan tarkastella yhtenä kokonaisuutena: ISO 31000 jäsentää riskienhallinnan peruslogiikan, ISO 22301 jatkuvuudenhallinnan, ISO 22320 tilannejohtamisen periaatteet, ISO 31030 matkustusriskienhallinnan ohjelmamaisen rakenteen ja ISO 18788 ulkoistetun turvallisuusoperaation johtamisjärjestelmän näkökulman.

2.4 Tiedon hajanaisuus ja tilannekuvan muodostamisen haasteet

Ulkomaan työmatkoissa ja ulkomailla toteutettavissa työtehtävissä turvallisuustilanne rakentuu harvoin yhdestä selkeästä lähteestä, vaan se muodostuu useiden samanaikaisten riskitekijöiden ja jatkuvasti päivittyvän tiedon varaan. Kriisitilanteissa riskit voivat muuttua nopeasti, ja samalla korostuvat infrastruktuurin häiriöt, viestintäkatkokset sekä muut tilanteet, jotka vaikeuttavat sekä tiedon saatavuutta että matkustajan tavoittamista. Tällöin tilannekuva pirstaloituu helposti, jolloin osa tiedosta on ajantasaista, osa viiveellistä, osa tulkinnanvaraista ja osa voi olla tilanteen kannalta epäolennaista tai väärää. (Takana 2025b)

Matkustusturvallisuuden kriisitilanteessa tilannekuvan muodostamisen keskeinen haaste on se, että päätöksenteon kannalta olennainen tieto syntyy eri aikaan, eri muodossa ja eri käsittelyasteilla. Puolustusvoimien data- ja tekoälystrategian (kuvan 1) logiikkaa soveltaen matkustusturvallisuuden tieto etenee tyypillisesti ensihavainnoista ja raakadatasta, kuten viranomaisilmoituksista, uutisvirrasta, turvallisuuspalveluiden hälytyksistä, matkustajien yhteydenotoista ja paikallisista havaintotiedoista, kohti jäsennellympää tilannekuvaa, raportteja, ohjeita ja myöhemmin laadittavia arvioita ja suunnitelmia.

Haaste syntyy siitä, että osa tiedosta on saatavilla sekunneissa tai minuuteissa, kun taas analysoitu ja päätöksentekoon soveltuva tieto muodostuu viiveellä, vaikka kriisi vaatii samanaikaisesti nopeita ratkaisuja. Tämän vuoksi organisaation on kyettävä kokoamaan hajallaan oleva tieto yhteen, prosessoimaan rakenteellista ja rakenteetonta dataa käyttökelpoiseksi tilannekuvaksi, sekä varmistamaan samalla tiedon laatu, saatavuus ja luotettavuus, jotta matkustusturvallisuutta koskevat päätökset eivät perustu pelkkään yksittäiseen havaintoon vaan useista lähteistä koottuun ja jatkuvasti päivittyvään tilannekuvaan. (Puolustusvoimat, 2025, s. 2–3)

Tilannekuvan muodostaminen on matkustusturvallisuudessa käytännöllinen johtamisen väline, ei pelkkä raportointituote. Kun kriisi alkaa, ensimmäinen prioriteetti on matkustavan henkilöstön sijainnin selvittäminen ja turvallisuuden varmistaminen. Tämän jälkeen kriisin vakavuus arvioidaan ja päätös tarvittavista toimenpiteistä tehdään nopeasti, mutta harkitusti, perustuen ennalta määriteltyihin protokolliin ja ajantasaiseen tilannekuvaan. Tilannekuvan laatu vaikuttaa suoraan siihen, kuinka nopeasti organisaatio kykenee siirtymään havainnoinnista koordinoituun toimintaan ja miten johdonmukaisesti päätökset voidaan perustella. (Takana 2026c) Tilannekuvan hajanaisuus heikentää tätä siirtymää. Jos tieto on eri kanavissa, eri ihmisillä ja eri muodoissa, päätöksenteko altistuu sekä ali- että ylireagoinnille ja toimenpiteiden epäjohdonmukaisuudelle. (Takana 2026b)

Tiedon hajanaisuutta voidaan pienentää vain, jos tilannekuvan ylläpito on rakennettu prosessiksi, joka kattaa matkustuksen kaikki vaiheet ja määrittää, mitä tietoa kerätään, miten sitä tulkitaan ja miten se jaetaan. (Takana 2025d) Kriisitilanteiden koordinoidun toimintamallin kautta tilannekuvan muodostaminen mahdollistaa nopean reagoinnin tilanteeseen, sekä tilanteen jälkiseurannan. (Takana 2026b)

Käytännön tasolla tiedon hajanaisuus näkyy erityisesti viestinnässä ja yhteydenpidossa. Jos kriisitilanteessa tiedonkulku ei toimi kaikissa suunnissa, matkustajan tilannekuva ja organisaation tilannekuva eriytyvät, ja koordinaatio heikkenee. Tehokas varautuminen edellyttää systemaattista lähestymistapaa matkustusturvallisuuteen, ja nostaa esiin jatkuvan tilannetietoisuuden ja ajantasaisen tiedon merkityksen kohdemaan olosuhteista. Käytännön haasteita voi tuottaa reaaliaikaisen tilannekuvan ja ympärivuorokautisen tuen (24/7)

tuottaminen tilanteissa, joissa työnantajan huolehtimisvelvollisuuden täyttäminen ja matkustajan tukeminen edellyttävät sitä. (Takana 2025e)

Tilannekuvan muodostamisen haaste ei siten ole pelkkä tiedon määrä, vaan se, miten tiedosta tehdään päätöksentekoa tukevaa ja miten se sidotaan organisaation rakenteisiin ja vastuisiin. Riskienhallinnan standardi korostaa riskienhallinnan kokonaisuudessa myös viestintää ja seurantaa, mikä tukee näkemystä siitä, että tilannekuvan ylläpito ei voi olla kertaluonteinen tai virka-aikaan sidottu suorite vaan jatkuva kyvykkyys. (ISO 31000:2018) Myös matkustusriskienhallinnan standardi painottaa ohjelmamaisuutta, jossa matkustusriskienhallintaa kehitetään, arvioidaan ja tarkastellaan, jotta tieto ei jää satunnaiseksi, vaan se muuttuu rakenteeksi. (ISO 31030:2021) Kun tähän yhdistetään kriisin jälkeinen seuranta ja oppiminen, muodostuu jatkuvan parantamisen sykli. Tapahtumat dokumentoidaan, toimenpiteitä arvioidaan ja toimintamalleja päivitetään, jotta seuraavassa tilanteessa tilannekuva rakentuu nopeammin ja luotettavammin. (Takana 2026b)

2.5 Tekoälyn rooli asiantuntijatyössä

Tekoälyn roolia asiantuntijatyössä voidaan tarkastella ennen kaikkea työn tukemisen, ei työn korvaamisen näkökulmasta. Generatiivinen tekoäly kykenee käsittelemään suuria tekstimääriä, tiivistämään tietoa, tuottamaan vaihtoehtoisia jäsennyksiä ja tukemaan alustavaa analyysia tavalla, joka voi nopeuttaa asiantuntijatyön alkuvaiheita merkittävästi. OECD:n mukaan generatiivinen tekoäly voi parantaa työn tuottavuutta automatisoimalla yksittäisiä tehtäviä ja vahvistamalla työntekijän suoriutumista erityisesti kirjoittamiseen, tiivistämiseen, vertailuun ja ideointiin liittyvissä tehtävissä (OECD, 2025). Tästä näkökulmasta tekoäly ei näyttäydy irrallisena teknisenä työkaluna, vaan osana asiantuntijatyön muuttuvaa työnjakoa, jossa osa työvaiheista siirtyy koneavusteisiksi ja asiantuntijan oma työ painottuu yhä enemmän arviointiin, tulkintaan ja päätelmien perusteluun.

Asiantuntijatyössä tekoälyn käyttökelpoisuus liittyy erityisesti tilanteisiin, joissa tietoa on paljon, se on hajallaan ja sen käsittelyyn kohdistuu aikapainetta. Tällaisissa tilanteissa tekoäly voi toimia niin sanottuna kognitiivisena tukena, jolloin se auttaa kokoamaan yhteen hajanaista aineistoa, tunnistamaan toistuvia teemoja, vertailemaan vaihtoehtoisia toimintatapoja ja laatimaan alustavia luonnoksia ohjeista, raporteista tai tilannearvioista. OECD on ku-

vannut, että generatiivisen tekoälyn suurin hyöty syntyy usein juuri työntekijän ja tekoälyn yhteistoiminnasta, jossa tekoäly vahvistaa ihmisen osaamista (OECD, 2025).

Tekoälyn hyöty asiantuntijatyössä ei kuitenkaan synny automaattisesti, vaan se riippuu tehtävän luonteesta ja työn kontekstista. Generatiivisen tekoälyn hyöty asiantuntijatyössä painottuu tehtäviin, joissa korostuvat kirjoittaminen, tiivistäminen, vertailu, ideointi ja hajanaisen aineiston kokoaminen, kun taas sen rajoitteet korostuvat tehtävissä, jotka edellyttävät asiayhteyden ymmärtämistä, harkintaa ja tuotosten kriittistä arviointia (OECD, 2025; NIST, 2024). Tämän vuoksi tekoälyn käyttö muuttaa asiantuntijatyötä ennen kaikkea siten, että asiantuntijan rooli siirtyy tiedon tuottajasta yhä selvemmin tiedon arvioijaksi, ohjaajaksi ja validoijaksi. Käytännössä tämä tarkoittaa, että asiantuntijan on osattava määritellä kysymys oikein, tunnistaa tehtävään soveltuva käyttötilanne, arvioida tuotetun vastauksen käyttökelpoisuus sekä erottaa toisistaan todennettavissa oleva tieto, tulkinta ja pelkkä kielellisesti uskottava sisältö.

Turvallisuusasiantuntijan työssä henkilön tekoälyosaamiseen liittyvät generatiivisen tekoälyn keskeiset rajoitteet ja riskit, jossa väärä tulkinta voi vaikuttaa suoraan ihmisten henkeen ja terveyteen. *"…tekoäly kertoi minulle, että [kohdemaan] vaaleissa ei ole levottomuuksia… se ei vastannut käsillä olevaa tilannetta"* (AS-2, 1.3.2026, yksilöhaastattelu). NIST kuvaa generatiivisen tekoälyn riskiksi niin sanotun hallusinaation, jossa järjestelmä tuottaa virheellistä tai täysin väärää sisältöä itsevarman ja uskottavan oloisesti. Samassa yhteydessä NIST korostaa myös yli luottamisen, automaatiovinouman, tietosuojariskien ja tiedon eheyttä koskevien riskien merkitystä generatiivisen tekoälyn käytössä (NIST, 2024). Asiantuntijatyössä nämä rajoitteet ovat olennaisia, koska työn lopputuloksen on kestettävä paitsi käytännön soveltaminen myös jälkikäteinen arviointi. Tekoäly voi siis tuottaa nopeasti vakuuttavan ehdotuksen, mutta se ei takaa, että ehdotus olisi asiayhteyteen sopiva, ajantasainen tai organisaation riskinsietokyvyn mukainen. Tästä syystä tekoälyä ei voida pitää itsenäisenä asiantuntijana, vaan sen tuottama sisältö on ymmärrettävä alustavaksi ja tarkastettavaksi aineistoksi.

Ihmisen valvonnan merkitys korostuu erityisesti silloin, kun tekoälyn tuottamaa tietoa käytetään suositusten, arvioiden tai päätöksentekoa tukevien johtopäätösten pohjana. Euroopan unionin tekoälysääntelyssä ihmisen valvonta

määritellään keskeiseksi periaatteeksi, jossa käyttäjän tulee olla mahdollisuus ymmärtää tekoälyjärjestelmien käytön kyvykkyyksiä ja rajoitteita sekä tunnistaa poikkeamat ja välttää liiallista luottamusta tuotoksiin, että voi jättää tuotos käyttämättä tai ohittaa sen kokonaan (EU AI Act, 2024, art. 14). Tämä periaate on asiantuntijatyössä erityisen relevantti, koska monissa tehtävissä tekoäly ei anna lopullista vastausta vaan ehdottaa tulkintaa, jonka hyväksyminen tai hylkääminen jää käyttäjälle (turvallisuusasiantuntija). Mitä suurempi vaikutus vastauksella on turvallisuuteen, jatkuvuuteen tai organisaation vastuisiin, sitä vahvempi vaatimus kohdistuu turvallisuusasiantuntijan tekemään arvioon, lähteiden tarkistamiseen ja johtopäätösten perusteluun.

Tekoälyn rooli asiantuntijatyössä voidaan siten jäsentää kolmelle tasolle. Ensimmäisellä tasolla tekoäly toimii tiedon käsittelyn välineenä ja auttaa kokoamaan, tiivistämään ja muotoilemaan aineistoa. Toisella tasolla se toimii analyysin tukena tuottamalla vaihtoehtoja, alustavia luokitteluja ja ehdotuksia jatkokäsittelyä varten. Kolmannella tasolla sen käyttö vaikuttaa työn organisointiin laajemmin, koska se siirtää asiantuntijan työpanosta pois mekaanisesta tiedon läpikäynnistä kohti valvontaa, harkintaa ja päätöksenteon tukemista. Näin tarkasteltuna tekoälyn varsinainen arvo ei ole siinä, että se poistaisi asiantuntijan tarpeen, vaan siinä, että se voi vapauttaa asiantuntijan aikaa sellaisiin tehtäviin, joissa kontekstiosaaminen, vastuunotto ja kyky sovittaa tieto organisaation toimintaympäristöön ovat ratkaisevia.

Tämän työn näkökulmasta tekoälyn rooli asiantuntijatyössä on perusteltua ymmärtää ehdolliseksi, sillä sen käyttökelpoisuus ja tuottama lisäarvo eivät synny automaattisesti vaan riippuvat tehtävätyypistä, työn kontekstista sekä käyttäjän kyvystä rajata tehtävä, muotoilla kehotteet ja arvioida tuotosten soveltuvuutta (OECD, 2025). Se on käyttökelpoinen silloin, kun työprosessi, lähdeaineisto, vastuut ja validointimenettelyt ovat riittävän selkeitä ja kun organisaatiolla ja asiantuntijalla on riittävä osaaminen ohjata käyttöä tarkoituksenmukaisesti, sillä nämä tekijät vaikuttavat suoraan siihen, mitä tekoäly tuottaa ja miten luotettavuus voidaan varmistaa (OECD, 2025). Se on ongelmallinen silloin, kun organisaation toimintamallit ovat epäselviä, lähtötieto on puutteellista tai tekoälyn tuottamaa sisältöä aletaan käsitellä sellaisenaan luotettavana analyysina, koska generatiiviseen tekoälyyn liittyy riski tuottaa itsevarmasti esitettyä mutta virheellistä sisältöä sekä taipumus liialliseen luottamiseen tuotoksiin, mikä korostaa asiantuntijan tekemän validoinnin ja val-

vonnan välttämättömyyttä (NIST, 2024). Siksi tekoäly ei ole asiantuntijatyössä autonominen toimija, vaan väline, jonka vaikuttavuus määräytyy sen mukaan, kuinka hyvin se sidotaan osaksi asiantuntijan johtamaa ja valvomaa työprosessia, ja jonka hyöty realisoituu vain, jos organisaatio kykenee yhdistämään sen käyttöön osaamisen, ohjeistuksen, valvonnan ja vastuun (NIST, 2024).

2.6 Teoreettisen viitekehyksen yhteenveto

Tämän työn teoreettinen viitekehys rakentuu riskiperusteisen turvallisuusjohtamisen näkökulmasta ja kokoaa ne periaatteet, joiden avulla ulkoistetun turvallisuusasiantuntijan työ voidaan kytkeä organisaation johtamiseen, päätöksentekoon ja dokumentointiin. Viitekehys korostaa, että turvallisuusjohtaminen edellyttää systemaattista riskienhallintaa ja sen integrointia osaksi organisaation toimintaa sekä päätöksenteon reunaehtoja myös epävarmuuden ja aikapaineen tilanteissa (ISO 31000:2018).

Tässä luvussa muodostettu viitekehys kokoaa matkustusturvallisuuden ohjelmalliseksi kokonaisuudeksi, jossa politiikka, riskien arviointi, ehkäisy- ja lieventämistoimet sekä jatkuva seuranta muodostavat toisiaan tukevan rakenteen eikä turvallisuus jää yksittäisten matkojen ympärille rakennetuiksi tarkistuslistoiksi (ISO 31030:2021). Samalla viitekehys jäsentää tiedon hajanaisuuden ja tilannekuvan muodostamisen keskeiseksi käytännön haasteeksi, jossa ratkaisevaa ei ole tiedon määrä vaan kyky yhdistää eri lähteistä tuleva tieto ajantasaiseksi ja päätöksentekoa tukevaksi kokonaisuudeksi, erityisesti poikkeama- ja kriisitilanteissa.

Tämän työn teoreettinen viitekehys liittää ulkoistamisen tarkasteluun näkökulman, jossa turvallisuuspalvelun tuottamisen tai hankinnan onnistuminen edellyttää roolien, vastuiden, hyväksymiskäytäntöjen ja valvonnan selkeyttä sekä vastuullista toimintatapaa (ISO 18788:2015). Viitekehys tukee erityisesti tilanteita, joissa ulkoistettu asiantuntija toimii turvallisuuspäällikön sijaisena tai resurssitukena, jolloin työn vaikuttavuus riippuu siitä, kuinka nopeasti asiantuntija pystyy kiinnittymään organisaation johtamis- ja raportointirakenteisiin ja toimimaan niiden mukaisesti.

Tässä työssä teoreettinen viitekehys määrittää generatiivisen tekoälyn roolin asiantuntijatyössä ehdolliseksi ja asiantuntijan työtä vahvistavaksi. Se kokoaa tutkimus- ja ohjeistuslähtöisen näkemyksen siitä, että generatiivinen tekoäly

on vahvimmillaan tehtävissä, joissa painottuvat tiedon jäsentäminen, kielellinen muotoilu ja alustava analyysi, mutta sen rajoitteet, kuten asiantuntijan tekoälyosaaminen, korostuvat tehtävissä, joissa tarvitaan syvää kontekstin ymmärtämistä, tilannesidonnaista harkintaa ja päätösvastuuta (OECD, 2025; NIST, 2024). Viitekehys korostaa samalla, että luotettava käyttö edellyttää systemaattista validointia ja ihmisen valvontaa, koska generatiiviseen tekoälyyn liittyy riski tuottaa uskottavan oloista mutta virheellistä sisältöä ja lisätä liiallista luottamusta tuotoksiin (NIST, 2024).

3 Tutkimusasetelma, menetelmät ja aineisto

Tässä luvussa kuvataan tutkimuksen toteutus, tutkimusasetelma, menetelmälliset valinnat, aineiston muodostuminen sekä analyysin eteneminen. Luvun tarkoituksena on tehdä näkyväksi, miten työn empiirinen osa on rakennettu ja millä perusteilla tutkimuksen tuloksia voidaan arvioida. Tutkimuksen menetelmällinen läpinäkyvyys on tärkeää, koska tutkimusosaaminen ei ole vain akateemisen tutkimuksen väline, vaan myös työelämässä tarvittava taito, johon kuuluvat tiedon analysointi, tiedonhallinta, erilaisten aineistojen käyttö sekä tiedon tarkoituksenmukaisuuden, oikeellisuuden ja laadun arviointi (Vilkka, 2021).

Tässä työssä tutkimuksen kohteena ei ole tekoäly teknologisena järjestelmänä sinänsä, vaan generatiivisen tekoälyn käyttökelpoisuus ulkoistetun turvallisuusasiantuntijan työssä. Tämän vuoksi tutkimus kohdistuu käytännön työprosesseihin, asiantuntijatyön kokemuksiin ja niihin ehtoihin, joiden varassa tekoäly voi tukea turvallisuusasiantuntijan työtä luotettavasti. Menetelmällisesti tämä tarkoittaa, että huomio kohdistuu tiedon tuottamiseen, jäsentämiseen, arviointiin ja tulkintaan sellaisessa muodossa, joka palvelee työelämän kehittämistä. Vilkan mukaan tutkimuksellinen osaaminen liittyykin olennaisesti kykyyn tehdä tutkimuksia, selvityksiä ja kartoituksia osana työelämää ja sen käytäntöjä (Vilkka, 2021).

3.1 Tutkimusasetelma

Tutkimus toteutettiin laadullisena, työelämälähtöisenä kehittämistutkimuksena. Tavoitteena ei ollut mitata generatiivisen tekoälyn vaikutuksia määrällisesti eikä vertailla eri tekoälyratkaisujen teknistä suorituskykyä, vaan tarkastella sen käyttökelpoisuutta ulkoistetun turvallisuusasiantuntijan työssä. Tutkimuksen kohteena oli ilmiö, joka liittyi ulkoistetun turvallisuusasiantuntijatyön käytäntöihin, tiedon käsittelyyn, vastuisiin ja päätöksenteon tukemiseen.

Tutkimusasetelma rakentui käytännön kehittämistarpeen ympärille. Työn lähtökohtana oli tarve ymmärtää, missä työvaiheissa generatiivinen tekoäly voi tukea ulkoistetun turvallisuusasiantuntijan työtä, millaisia rajoitteita käyttöön liittyy ja millä edellytyksillä sen hyödyntäminen on tarkoituksenmukaista. Vilkan mukaan tutkimuksellinen kehittäminen liittyy työelämässä tiedon tuottamiseen, arviointiin ja hyödyntämiseen käytännön toiminnan kehittämiseksi (Vilkka, 2021).

Tässä työssä tarkastelu rajattiin ulkoistetun turvallisuusasiantuntijan työhön tilanteessa, jossa hänen tehtäväkseen tulee organisaation turvallisuuspäällikön sijaistaminen tai alkaneen poikkeama-/ kriisitilanteen koordinointi. Havainnointijaksolla työtehtävät käsittelivät erityisesti organisaatioiden tukemista matkustusturvallisuuden, tilannekuvan muodostamisen sekä poikkeama- ja kriisitilanteiden tukemisessa. Ajallisen ja toimeksiantotyyppien mukaisen rajauksen avulla tutkimuskohde pysyy hallittavana ja samalla riittävän konkreettisena, jotta tutkimuksessa voidaan tarkastella työn todellisia vaiheita, vastuita ja rajoitteita, ja työ voidaan suhteuttaa johdonmukaisesti lopputyön teoreettiseen viitekehykseen.

3.2 Menetelmät ja tutkimusote

Tutkimus perustui laadulliseen tutkimusotteeseen, koska tavoitteena oli tarkastella generatiivisen tekoälyn käyttökelpoisuutta käytännön kokemusten, tulkintojen ja työprosessien näkökulmasta. Laadullinen lähestymistapa soveltuu tilanteisiin, joissa tutkimuksen kohteena ovat merkitykset, toimintatavat ja kontekstisidonnaiset kokemukset eikä määrällinen vertailu (Vilkka, 2021).

Tutkimuksessa hyödynnettiin kolmea toisiaan täydentävää menetelmää: asiantuntijakyselyä, yksilöllisiä teemahaastatteluja ja ryhmätyöpajaa. Näiden yhdistämisen tarkoituksena oli muodostaa tutkittavasta ilmiöstä mahdollisimman monipuolinen kuva. Ojasalon, Moilasen ja Ritalahden mukaan kehittämistyössä tiedonkeruun menetelmiä voidaan yhdistää, kun tavoitteena on tuottaa käytännön kehittämistä tukevaa tietoa ja tarkastella ilmiötä useasta näkökulmasta (Ojasalo, Moilanen ja Ritalahti, 2015).

Tutkimusote oli teoriaohjaava. Aineiston tulkintaa ohjasivat työn teoreettisessa viitekehyksessä esiin nousseet näkökulmat, kuten turvallisuusjohtaminen, tiedon hajanaisuus, tilannekuvan muodostaminen, validointi ja tekoälyn

käytön ehdollisuus. Näin empiiriset havainnot voitiin kytkeä laajempaan turvallisuusasiantuntijatyön kokonaisuuteen

3.3 Aineisto

Tutkimuksen aineisto muodostui kolmesta osasta: asiantuntijakyselyn vastauksista, yksilöllisistä teemahaastatteluista sekä ryhmätyöpajassa tuotetusta aineistosta. Kokonaisuus rakennettiin siten, että aineisto tukee tutkimuskysymystä mahdollisimman käytännönläheisesti ja mahdollistaa generatiivisen tekoälyn käyttökelpoisuuden tarkastelun useasta näkökulmasta. Laadullisessa tutkimuksessa aineiston tehtävänä on tuottaa tutkittavasta ilmiöstä syvällistä ja kontekstiin sidottua ymmärrystä (Vilkka, 2021).

Aineiston valinnassa keskeinen periaate oli tarkoituksenmukaisuus. Tutkimukseen osallistuneet henkilöt valittiin sen perusteella, että heillä oli pitkä kokemus turvallisuusasiantuntijatyöstä, turvallisuusjohtamisen käytännöistä ja heillä tiedettiin olevan kokemusta generatiivisen tekoälyn hyödyntämisestä asiantuntijatyössä. Tavoitteena ei ollut muodostaa tilastollisesti edustavaa otosta, vaan koota tutkimuskysymyksen kannalta olennaista ja sisällöllisesti rikasta aineistoa (Ojasalo, Moilanen ja Ritalahti, 2015). Täten tarkoituksena oli pyrkiä keräämään erille parhaat tutkimuskysymykseen liittyvät parhaat käytänteet tekoälyn hyödyntämiseksi tosi elämässä.

Aineisto käsiteltiin anonymisoidusti. Yksittäiset henkilöt tunnistettiin tutkimuksessa tunnuksilla AS-1 ja AS-2, eikä organisaatioita, toimeksiantoja tai muita tunnistettavia tietoja esitetä valmiissa työssä tunnistettavassa muodossa.

3.4 Tiedonkeruun kolme vaihetta

Tiedonkeruu eteni kolmessa toisiaan täydentävässä vaiheessa, jotta ilmiöstä saatiin sekä yleiskuva että syvyyttä, ja löydösten käytäntöön vietävyys voitiin varmistaa. Vaiheistus noudattaa työelämälähtöisen kehittämistutkimuksen periaatetta, jossa edetään tarkoituksenmukaisin askelin, dokumentoidaan menettelyt ja kytketään osallistujat mukaan tulosten arviointiin (Ojasalo, Moilanen & Ritalahti, 2015; Vilkka, 2021).

Kaikissa vaiheissa aineiston eettinen käsittely varmistettiin anonymisoinnilla, osallistujien informoinnilla ja vapaaehtoisuudella. Aineiston keruu, talletus ja

siirrot analyysiin dokumentoitiin jäljitettävästi, ja tunnisteelliset yksityiskohdat poistettiin tai karkeistettiin, jotta yksittäisiä henkilöitä tai organisaatioita ei voida tunnistaa (TENK, 2019; TENK, 2023).

3.4.1 Asiantuntijakysely

Ensimmäisessä vaiheessa toteutettu kysely kartoitti, missä työvaiheissa generatiivista tekoälyä käytetään tai voidaan käyttää, millaisia hyötyjä ja rajoitteita turvallisuusasiantuntijat tunnistavat ja miten tuotosten validointi oli järjestetty. Kysymykset muotoiltiin pääosin strukturoiduiksi vertailtavuuden takaamiseksi, ja niitä täydennettiin valikoiduilla avoimilla kentillä, jotta kontekstisidonnaiset perustelut saatiin talteen. Kyselyn rooli oli tuottaa systemaattinen lähtöaineisto seuraavien vaiheiden suunnitteluun, jota kehittämistyön kirjallisuus suosittelee, kun tavoitteena on yhdistää tilannekuva ja kohdennettu jatkotiedonkeruu (Ojasalo, Moilanen & Ritalahti, 2015; Vilkka, 2021).

3.4.2 Puolistrukturoidut teemahaastattelut

Toisessa vaiheessa haastattelut syvensivät kyselyssä esiin nousseita teemoja. Haastattelurunko kohdistettiin työnkulkuihin, vastuunjakoon ja hyväksymiskriteereihin, kuten: mihin tehtäviin tekoälyä käytetään, missä kohdin tarvitaan asiantuntijan nimenomainen tarkistus ja millä perusteilla tuotokset hyväksytään tai hylätään. Puolistrukturointi mahdollisti sekä yhtenäisen etenemisen että kontekstiin kiinnittyvien tapausesimerkkien käsittelyn. Ratkaisun joka on suositeltava, kun tarkoituksena on vastata kehittämistä varten esitettäviin kysymyksiin “miksi” ja “miten” (Vilkka, 2021).

3.4.3 Ryhmätyöpaja (validointi)

Kolmannessa vaiheessa osallistujat arvioivat yhdessä löydösten sovellettavuutta päätöksenteon ja ohjeistuksen näkökulmista. Työpajassa tunnistettiin, mitkä havainnot voidaan siirtää sellaisenaan toimintaan, mitkä edellyttävät rajauksia sekä millaiset roolit, vastuut ja hyväksymiskäytännöt tulee kirjata, jotta tekoälyn käyttö säilyy asiantuntijan valvonnassa. Kehittämisorientaation tavoitteena oli, että tulokset validoidaan ja muotoillaan toimeenpantavaan muotoon ulkoistetun turvallisuusasiantuntijan toimeksiannoissa (Ojasalo, Moilanen & Ritalahti, 2015).

3.5 Analyysimenetelmä

Aineiston analyysissä hyödynnettiin teoriaohjaavaa sisällönanalyysiä. Menetelmä soveltui tähän tutkimukseen, koska tavoitteena ei ollut ainoastaan kuvata yksittäisiä vastauksia, vaan muodostaa useasta aineistovaiheesta jäsennelty kokonaiskuva generatiivisen tekoälyn käyttökelpoisuudesta ulkoistetun turvallisuusasiantuntijan työssä. Teoriaohjaavassa analyysissä aineisto toimii tulkinnan perustana, mutta sen jäsentämistä ohjaavat tutkimuksen teoreettisessa viitekehyksessä kuvatut näkökulmat, kuten turvallisuusjohtamisen rakenne, tiedon hajanaisuus, tilannekuvan muodostaminen, validointi, vastuunjako ja tekoälyn käytön ehdollisuus (Vilkka, 2021).

Analyysi eteni aineistonkeruun rakennetta seuraten. Ensin tarkasteltiin asiantuntijakyselyn vastauksia ja tunnistettiin niistä toistuvat teemat sekä kohdat, joissa näkemykset erosivat toisistaan. Tämän jälkeen analyysia syvennettiin yksilöllisillä teemahaastatteluilla, joissa tarkennettiin kyselyssä esiin nousseita havaintoja, varmistettiin tulkintoja ja haettiin esimerkkejä käytännön työtilanteista. AS-1:n haastattelussa painottuivat esimerkiksi johtosuhteiden muodollisen ja käytännöllisen selkeyden välinen ristiriita, tiedon hajanaisuuden syyt sekä tekoälyn hyöty raakatiedon jäsentämisessä, kun taas AS-2:n haastattelussa syvennettiin erityisesti roolin epäselvyyttä toimeksiannon alussa, kontekstin puutteen vaikutuksia sekä validoinnin tarvetta.

Kyselyn ja haastattelujen perusteella muodostetut havainnot koottiin teemoiksi, joita käsiteltiin ryhmätyöpajassa. Työpajan tarkoituksena oli vahvistaa tai kyseenalaistaa keskeiset havainnot, arvioida alustavia johtopäätöksiä ja tarkentaa niiden käytännöllistä merkitystä. Sisällönanalyysin käytännön toteutuksessa aineistosta poimittiin tutkimuskysymyksen kannalta merkityksselliset ilmaisut ja havainnot, minkä jälkeen niitä ryhmiteltiin temaattisesti. Teemoiksi muodostuivat esimerkiksi turvallisuusjohtamisen rakenteen selkeys, roolien ja johtosuhteiden epäselvyys, tiedon hajanaisuus, tekoälyn hyöty tiedon jäsentämisessä, kontekstin ymmärtämisen rajat, validoinnin välttämättömyys sekä raja analyysin tukemisen ja varsinaisen päätöksenteon välillä.

Tämän jälkeen teemoja verrattiin eri aineistovaiheiden välillä ja tarkasteltiin, mitä kysely nosti esiin, mitä haastattelut tarkensivat ja mitä työpaja lopulta vahvisti tai täsmensi. Näin analyysi eteni alustavien havaintojen tunnistamisesta niiden tarkentamiseen ja lopulta yhteisesti validoituihin johtopäätöksiin

(Ojasalo, Moilanen ja Ritalahti, 2015). Analyysin lopputuloksena muodostettiin teemoiteltu tulkinta siitä, missä työvaiheissa generatiivinen tekoäly tuottaa lisäarvoa ulkoistetun turvallisuusasiantuntijan työssä, millaisia rajoitteita sen käyttöön liittyy ja millä edellytyksillä sen käyttö voidaan liittää osaksi asiantuntijan työprosessia hallitusti ja luotettavasti.

3.6 Tutkimuksen luotettavuus ja eettisyys

Tutkimuksen luotettavuutta tarkasteltiin laadullisen tutkimuksen lähtökohdista. Keskeistä oli, että tutkimusprosessi, aineiston muodostuminen ja analyysin eteneminen kuvataan läpinäkyvästi, jotta lukija voi arvioida, miten johtopäätöksiin on päädytty. Tässä tutkimuksessa luotettavuutta vahvisti erityisesti aineistonkeruun vaiheittainen ja toisiaan täydentävä rakenne (Vilkka, 2021).

Luotettavuutta vahvisti myös se, että havaintoja ei rakennettu yhden aineistolähteen varaan, vaan niitä tarkasteltiin useasta näkökulmasta ja useassa vaiheessa. Kehittämistutkimukselle on ominaista, että osallistujat kytketään mukaan arvioimaan muodostettuja havaintoja ja niiden käytännöllistä sovellettavuutta, mikä tukee tulkinnan kestävyyttä (Ojasalo, Moilanen ja Ritalahti, 2015). Samalla on kuitenkin tunnistettava, että tutkimuksen tulokset ovat kontekstisidonnaisia, eikä niiden tarkoituksena ole tuottaa tilastollisesti yleistettäviä väitteitä, vaan kuvata generatiivisen tekoälyn käyttökelpoisuutta tässä ajallisesti, tehtävällisesti ja tilanteellisesti rajatussa kontekstissa.

Tutkimuksen eettisyydessä keskeistä oli osallistujien ja organisaatioiden anonymiteetin suojaaminen, aineiston asianmukainen käsittely sekä aiheen sensitiivisyyden huomioiminen. Tässä työssä yksittäiset henkilöt anonymisoitiin tunnuksilla AS-#, eikä organisaatioita, toimeksiantoja tai muita tunnistettavia tietoja esitetä tunnistettavassa muodossa. Tutkimuksessa noudatettiin tutkimuseettisen neuvottelukunnan hyvän tieteellisen käytännön periaatteita, kuten rehellisyyttä, huolellisuutta, avoimuutta ja asianmukaista dokumentointia (TENK, 2023). Lisäksi huomioitiin ihmiseen kohdistuvan tutkimuksen eettiset periaatteet, kuten osallistumisen vapaaehtoisuus, riittävä informointi ja tutkittavien oikeuksien kunnioittaminen (TENK, 2019).

Eettisestä näkökulmasta oli tärkeää tunnistaa myös tutkijan oma asema suhteessa tutkimusaiheeseen ja asiakasorganisaatioihin. Koska tutkimus liittyy

käytännön työelämän kehittämiseen ja turvallisuusasiantuntijatyöhön, tutkijan omat kokemukset ja ennakkokäsitykset voivat vaikuttaa tulkintaan. Tätä riskiä pyrittiin pienentämään aineiston triangulaatiolla, vaiheittaisella analyysilla ja havaintojen yhteisellä validoinnilla. Tutkimuksen eettistä kestävyyttä vahvistaa lisäksi se, että generatiivista tekoälyä ei käsitellä automaattisesti hyödyllisenä ratkaisuna, vaan sen mahdollisuuksia ja rajoitteita arvioidaan kriittisesti asiantuntijavastuuta korostaen.

4 Tutkimustulokset

Tässä luvussa esitetään tutkimuksen keskeiset tulokset kolmessa vaiheessa kootun aineiston pohjalta. Tulokset rakentuvat asiantuntijakyselystä, yksilöhaastatteluista sekä ryhmätyöpajassa tehdystä havaintojen validoinnista. Luvun tarkoituksena on kuvata, millaisena generatiivisen tekoälyn käyttökelpoisuus näyttäytyi ulkoistetun turvallisuusasiantuntijan työssä syksyllä 2025 ja millaisia hyötyjä, rajoitteita sekä käyttöehtoja aineistosta tunnistettiin. Tavoitteena ei ole kuvata yksittäisiä vastauksia irrallisina havaintoina, vaan muodostaa jäsennelty kokonaiskuva siitä, miten generatiivinen tekoäly soveltuu ulkoistetun turvallisuusasiantuntijan työprosessiin.

Tulokset esitetään aineistonkeruun rakennetta seuraten. Ensin tarkastellaan asiantuntijakyselyn keskeisiä havaintoja, joiden avulla muodostettiin yleiskuva siitä, missä työvaiheissa generatiivista tekoälyä pidettiin hyödyllisenä ja mitä rajoitteita sen käyttöön liitettiin. Tämän jälkeen käsitellään yksilöhaastattelujen tuottamaa syventävää aineistoa, jonka avulla tarkennettiin kyselyssä esiin nousseita havaintoja ja ymmärrettiin paremmin niiden taustalla olevia eroja ja perusteluja. Lopuksi tarkastellaan ryhmätyöpajan validointihavaintoja, joiden avulla aiemmissa vaiheissa muodostettuja tulkintoja arvioitiin ja täsmennettiin käytännön työn näkökulmasta. Tuloksia tarkastellaan erityisesti tiedon jäsentämisen, tilannekuvan muodostamisen, analyysin valmistelun, päätöksenteon tuen sekä validoinnin näkökulmista, koska nämä teemat nousivat aineistossa toistuvasti esiin.

4.1 Asiantuntijakyselyn keskeiset havainnot

Asiantuntijakyselyn perusteella generatiivinen tekoäly näyttäytyi ennen kaikkea tiedon jäsentämisen, tilannekuvan kokoamisen ja analyysivaiheen tukena. Vastauksissa korostui erityisesti se, että tekoäly nopeutti hajallaan olevan tiedon kokoamista yhteen, helpotti yleiskuvan muodostamista ja auttoi käsittelemään useista lähteistä tulevaa aineistoa tiiviimpään muotoon. Kyselyaineistossa tätä kuvattiin muun muassa siten, että tekoäly auttoi kokoamaan

eri lähteistä tuotettua tietoa yhdeksi tilanneraportiksi, nopeutti yleiskuvan luomista ja mahdollisti laajemman datamassan hyödyntämisen samassa ajassa. Kyselyyn vastanneilla asiantuntijoilla oli ennestään kokemusta generatiivisen tekoälyn hyödyntämisestä, mutta osaamista ei mitattu erillisellä testillä, minkä vuoksi tekoälyn käytön hyöty ja tuotosten laatu kytkeytyivät myös vastaajien kykyyn rajata tehtävä ja ohjata työkalun käyttöä.

Kyselyssä nousi samalla esiin, että tekoälyn tuottama hyöty oli selvästi tehtävä- ja roolisidonnaista. Toiselle vastaajalle tekoälyn merkitys painottui turvallisuusjohtamisen viitekehyksen ja standardien vertailevaan tarkasteluun, kun taas toiselle se näyttäytyi erityisesti uutisvirran, taustatiedon ja kokonaistilannekuvan kokoamisen välineenä. Tämä viittaa siihen, että tekoälyn käyttökelpoisuus ei muodostu yhdestä yleisestä käyttötavasta, vaan siitä, millaiseen toimeksiantoon, lähtötietoon ja asiantuntijarooliin sen käyttö sijoittuu. Kyselyssä nähtiin myös, että tekoäly voi tukea ohjeistusten ja suunnitelmien luonnostelua, mutta käytännön hyöty vaihteli sen mukaan, oliko organisaatiolla jo olemassa valmista materiaalia, kuten turvallisuuspolitiikkaa tai toimialaa ohjaavaa standardia, jota turvallisuusasiantuntija saattoi hyödyntää ilman tekoälyä.

Kyselyn perusteella tekoälyn käyttökelpoisuus oli kuitenkin selvästi ehdollista. Vastauksissa korostui, että tekoäly toimii hyvin vain silloin, kun turvallisuusasiantuntijalla on riittävä rakenne, kysymysasetelma ja konteksti valmiina. Tätä kuvattiin esimerkiksi ajatuksella, että "tekoäly on hyvä renki mutta huono isäntä", ja että sen käyttö edellyttää kontekstin ymmärtävää turvallisuusasiantuntijaa. Samoin korostui näkemys, että oikeilla kysymyksillä ja rajoitetulla lähdeaineistolla tekoäly pystyy rajaamaan epäolennaista tietoa pois, mutta ilman asiantuntijan ohjausta vastaukset voivat jäädä yleisluontoisiksi tai harhaanjohtaviksi. Kyselyaineisto tukee siten havaintoa, että tekoäly ei korvaa asiantuntijaa, vaan sen arvo syntyy asiantuntijan ja työkalun välisessä vuorovaikutuksessa.

Kyselyn merkittävimmät rajoitteet liittyivät kontekstin ymmärtämiseen, tiedon ajantasaisuuteen ja tuotosten luotettavuuteen. Vastauksissa kuvattiin tilanteita, joissa tekoäly käytti vanhentunutta tietoa, antoi liian yleisiä tulkintoja tai rakensi analyysia lähteisiin, joiden ajantasaisuus ei vastannut käsillä olevaa tilannetta. Näiden havaintojen seurauksena vastaajat korostivat omaa lähdekriittisyyttään, lähteiden rajaamista ja tekoälyn tuotosten tarkistamista

ennen niiden hyödyntämistä. Tämä vahvistaa näkemystä siitä, että tekoälyn käyttö turvallisuusasiantuntijatyössä edellyttää systemaattista validointia, eikä tekoälyn tuottamaa sisältöä voida käyttää sellaisenaan.

Kyselyaineiston perusteella tekoälyä ei myöskään nähty varsinaisena päätöksentekijänä eikä turvallisuusasiantuntijan vuorovaikutusroolin korvaajana. Vaikka tekoälyn koettiin joissain tilanteissa tukevan poikkeaman ja kriisin alustavaa erottelua tai nopeuttavan esimerkiksi matkustusvaihtoehtojen ja alueellisten rajoitteiden selvittämistä, lopullinen arvio, päätös ja vastuu säilyivät ihmisellä. Erityisen selvästi tämä näkyi vastauksissa, joissa korostettiin, että kriisitilanteessa turvallisuusasiantuntijan rooli painottuu henkilöstön rauhoittamiseen, luottamuksen rakentamiseen ja päätösten perustelemiseen tavalla, johon tekoäly ei kykene. Tämän perusteella kyselyn keskeinen johtopäätös oli, että tekoälyn hyöty kohdistuu analyysin valmisteluun ja tiedon jäsentämiseen, mutta asiantuntijavastuu, kontekstiosaaminen ja päätöksenteko pysyvät ihmisen tehtävinä.

4.2 Yksilöhaastattelujen keskeiset havainnot

Yksilöhaastattelut syvensivät asiantuntijakyselyssä esiin nousseita havaintoja ja osoittivat, että generatiivisen tekoälyn käyttökelpoisuus rakentuu vahvasti työn rakenteiden, asiantuntijan osaamisen ja toimeksiannon luonteen varaan. Haastatteluissa vahvistui erityisesti havainto siitä, että tekoälyn hyöty ei synny pelkästään työkalun ominaisuuksista, vaan siitä, kuinka hyvin turvallisuusasiantuntija pystyy ohjaamaan sen käyttöä. Molempien asiantuntijoiden näkemyksissä korostui, että tekoäly tuottaa lisäarvoa erityisesti silloin, kun sillä on käytettävissään riittävä rakenne, rajattu aineisto ja selkeä tehtävä. Ilman tätä vastausten koettiin jäävän helposti yleisluontoisiksi, epätarkoiksi tai käytännön tilanteeseen huonosti soveltuviksi.

Haastattelut toivat samalla näkyväksi sen, että ulkoistetun turvallisuusasiantuntijan työn lähtötilanne vaikuttaa ratkaisevasti myös tekoälyn käyttökelpoisuuteen. AS-1 kuvasi tilannetta, jossa organisaation muodolliset johtosuhteet ja käytännön toiminta eivät täysin vastanneet toisiaan. Tällöin tekoäly oli hyödyllinen etenkin raakatiedon jäsentämisessä ja viitekehysten vertailemisessa, mutta se ei ratkaissut rakenteellista epäselvyyttä. AS-2 puolestaan korosti toimeksiannon alkuvaiheessa omaan rooliin ja vastuualueisiin liittynyttä epäselvyyttä, mikä hidasti työn käynnistymistä. Haastattelujen perusteella keskeinen havainto on, että tekoäly voi tukea turvallisuusasiantuntijan työtä,

mutta se ei kykene korvaamaan puutteellista turvallisuusjohtamisen rakennetta eikä selkeyttämään toimeksiannon johtosuhteita asiantuntijan puolesta.

Haastatteluissa tarkentuivat myös erot siinä, miten tiedon hajanaisuus koettiin. AS-1:n näkökulmasta hajanaisuus näyttäytyi merkittävänä käytännön haasteena, joka liittyi erityisesti siihen, ettei organisaatiolla ollut riittävän selkeää turvallisuusjohtamisen viitekehystä tai toimintamallia, johon turvallisuusasiantuntija olisi voinut nojata. AS-2 taas koki tiedon hajanaisuuden vähäisempänä ongelmana, mikä viittaa siihen, että hajanaisuuden kokemus ei riipu yksin tiedon määrästä, vaan myös turvallisuusasiantuntijan omasta kontekstiosaamisesta, toimeksiannon luonteesta ja siitä, kuinka nopeasti olennaiset tietolähteet saadaan tunnistettu tai rajattua. Haastattelut vahvistivat siten käsitystä, että tiedon hajanaisuus on turvallisuusasiantuntijatyössä sekä rakenteellinen että tilannesidonnainen ilmiö.

Molemmat haastattelut tukivat vahvasti havaintoa siitä, että tekoälyn suurin käytännöllinen hyöty liittyy tiedon jäsentämiseen, vaihtoehtojen kokoamiseen ja analyysin valmisteluun. AS-1 korosti tekoälyn arvoa erityisesti raakatiedon jäsentämisessä silloin, kun asiantuntijalla oli jo valmiina rakenne aiemmista toimeksiannoista ja ymmärrys siitä, mitä tietoa tarvitaan ja miten sitä tulee käsitellä. AS-2 toi esiin tilanteita, joissa tekoäly nopeutti käytännön päätöksentekoa tukevan tiedon kokoamista, esimerkiksi matkustusvaihtoehtojen, lentorajoitteiden tai muiden operatiivisten vaihtoehtojen tarkastelussa. Näissäkin tilanteissa lopullinen johtopäätös on, että päätös ja vastuu säilyivät aina asiantuntijalla. Haastattelujen perusteella tekoäly näyttäytyi siis ennen kaikkea työn valmistelijana ja analyysin tukena, ei itsenäisenä ratkaisijana.

Haastattelut syvensivät myös kyselyssä esiin nousseita rajoitteita. Erityisesti kontekstin ymmärtämisen puute, ajantasaisen tiedon varmistaminen ja lähteiden luotettavuus nousivat selvästi esiin. Haastatteluissa kuvattiin, että tekoäly saattoi käyttää vanhentunutta tai tilanteeseen huonosti sopivaa tietoa, mikäli asiantuntija ei itse ohjannut lähdeaineistoa riittävän tarkasti. Tämän vuoksi molempien asiantuntijoiden näkemyksissä korostui validoinnin välttämättömyys. Haastattelujen perusteella luotettavuus ei synny pelkästään siitä, että tekoäly tuottaa vakuuttavan vastauksen, vaan siitä, että turvallisuusasiantuntija kykenee arvioimaan lähteet, tarkistamaan sisällön ja suhteuttamaan sen käsillä olevaan tilanteeseen.

Yksilöhaastattelujen keskeinen johtopäätös oli, että generatiivisen tekoälyn käyttökelpoisuus ulkoistetun turvallisuusasiantuntijan työssä on vahvasti osaamis-, rakenne- ja kontekstisidonnaista, vaatien pääsyn asiakasorganisaation turvallisuutta ohjaaviin dokumentteihin. Tekoäly tuottaa eniten lisäarvoa silloin, kun asiantuntijalla on selkeä ymmärrys toimeksiannosta, käytettävissä olevista lähteistä, organisaation toimintamalleista ja siitä, mihin kysymykseen vastausta ollaan hakemassa. Haastattelut vahvistivat näin kyselyaineiston johtopäätöstä, että tekoäly ei korvaa turvallisuusasiantuntijaa, vaan sen hyöty syntyy vain asiantuntijan ohjauksessa, asiantuntijan vastuulla ja osana selkeästi jäsennettyä työprosessia.

Taulukko 1 Yhteenveto tekoälyn käytettävyydestä haastattelujen perusteella

Teema	**AS-1**	**AS-2**	**Merkitys tekoälyn käyttökelpoisuudelle**
Toimeksiannon lähtötilanne ja rakenteet	Johtosuhteet ja käytäntö eivät kohdanneet.	Rooli ja vastuut olivat alussa epäselvät.	Tekoälyn käytettävyys heikko, mikäli dokumentoitua turvallisuusjohtamisen mallia ei ole.
Tiedon hajanaisuus	Hajanaisuus oli merkittävä haaste.	Hajanaisuus koettiin tilanteesta riippuen vähäiseksi.	Hyöty riippui tehtävästä ja kontekstista, ei tiedon määrästä.
Vahvuusalueet	Raakatiedon jäsentäminen ja viitekehysten vertailu.	Operatiivisten vaihtoehtojen koonti ja päätöksenteon tuki.	Lisäarvo kohdistui valmisteluun ja analyysin strukturointiin.
Konteksti ja ajantasaisuus	Ilman ohjausta vastaukset jäivät yleisiksi.	Ajantasaisuus petti ja vaati lähdeohjauksen.	Ajantasaisuus ja kontekstin rajaus olivat kriittisiä.
Validointi ja vastuu	Tuotokset tarkistettiin ja sovitettiin organisaatioon ja tilanteeseen.	Tuotokset varmistettiin ja korjattiin lähteiden hallinnalla.	Validointi määritti luotettavuuden ja hyödyn.
Johtopäätös tekoälyn roolista	Tekoäly oli valmistelutyökalu.	Tekoäly oli työkalu, jota piti ohjata tarkasti.	Tekoäly jäi avustavaksi, asiantuntija säilytti vastuun.

4.3 Ryhmätyöpajan validointihavainnot

Ryhmätyöpaja vahvisti kyselyn ja yksilöhaastattelujen perusteella muodostunutta kokonaiskuvaa generatiivisen tekoälyn käyttökelpoisuudesta ulkoistetun turvallisuusasiantuntijan työssä. Työpajan keskusteluissa korostui, että tekoälyllä on selvä käytännöllinen arvo erityisesti silloin, kun sitä käytetään tiedon kokoamiseen, jäsentämiseen ja alustavan analyysin valmisteluun. Samalla osallistujat olivat varsin yksimielisiä siitä, että tekoälyn hyöty ei realisoidu automaattisesti, vaan se edellyttää asiantuntijalta selkeää ohjausta, riittävää kontekstin tuntemusta ja kykyä arvioida tuotetun tiedon luotettavuutta.

Työpajassa vahvistui erityisesti havainto siitä, että organisaation omat rakenteet ja dokumentaatio määrittävät suoraan tekoälyn käytettävyyttä. Mitä selkeämmin turvallisuusjohtamisen vastuut, toimintamallit, suunnitelmat ja hyväksymiskäytännöt ovat määritelty, sitä helpompi turvallisuusasiantuntijan on käyttää tekoälyä työnsä tukena. Vastaavasti tilanteissa, joissa organisaation rakenteet ovat epäselviä tai dokumentaatio hajanaista, tekoäly ei poista epäselvyyttä vaan voi jopa vahvistaa sitä tuottamalla näennäisesti johdonmukaisia mutta käytännön toimintaan huonosti kiinnittyviä vastauksia. Työpaja vahvisti siten käsitystä siitä, että tekoäly toimii parhaiten osana jo olemassa olevaa ja toimivaa turvallisuusjohtamisen rakennetta.

Validointikeskustelussa korostui myös se, että tekoälyn realistinen rooli sijoittuu selvästi analyysin tukemiseen eikä varsinaiseen päätöksentekoon. Työpajassa nähtiin, että tekoäly voi helpottaa vaihtoehtojen kokoamista, nopeuttaa alustavaa tilannekuvan muodostamista ja tukea ohjeiden tai raporttien luonnostelua, mutta se ei kykene kantamaan asiantuntijalle kuuluvaa vastuuta. Päätöksenteko, tilanteen vakavuuden arviointi, organisaation riskinsietokyvyn huomiointi ja henkilöstöön kohdistuvien vaikutusten punninta jäivät selvästi turvallisuusasiantuntijan tehtäviksi. Tämän vuoksi työpaja vahvisti aiemmissa vaiheissa syntynyttä näkemystä siitä, että tekoälyä ei tule tarkastella itsenäisenä toimijana vaan asiantuntijan työprosessia tukevana välineenä.

Työpajassa tarkentuivat myös tekoälyn käyttöön liittyvät hyväksymiskriteerit. Osallistujien keskusteluissa nousi esiin, että tekoälyn tuottaman sisällön käyttökelpoisuus riippuu ennen kaikkea siitä, onko lähdeaineisto rajattu, onko kysymys asetettu riittävän tarkasti ja onko tuotosta verrattu organisaation omaan tilanteeseen sekä ajantasaiseen tietoon. Tämä tarkoittaa käytännössä, että tekoälyn käyttö vaatii systemaattista validointia eikä sen tuottamaa sisältöä voida siirtää suoraan turvallisuusasiantuntijan työn lopputulokseksi. Työpaja vahvisti näin sen, että tekoälyn käytön keskeinen ehto on asiantuntijan tekemä arviointi, tarkistus, hyväksyntä ja vastuunkanto.

Työpajassa piirtyi käsitys siitä, miten tekoälyä olisi tarkoituksenmukaista hyödyntää silloin, kun organisaation rakenteet ja dokumentaatio ovat kunnossa. Toimivina käyttötapoina pidettiin sellaista valmistelutyötä, jossa tekoälylle annetaan rajattu tehtävä ja selkeä lähtöaineisto, ja lopputulos tarkistetaan ennen käyttöä (validointi). Tällaisia olivat esimerkiksi tilannekuvan

luonnostelu useista lähteistä koottavaksi yhteenvedoksi, vaihtoehtoisten toimintalinjojen vertailun pohja sekä matkustajan ohjeistuksen ensimmäinen luonnos, jota asiantuntija muokkaa organisaation käytäntöihin soveltuvaksi. Lisäksi tekoälyä pidettiin hyödyllisenä organisaation ohjeiden ja standardien läpikäynnin tukena siten, että se auttaa nostamaan esiin keskeiset kohdat ja mahdolliset ristiriidat, jotka voivat vaikuttaa ulkoistetun turvallisuusasiantuntijan työhön tai asiakasorganisaation odotuksiin halutusta palvelusta. Työpajan perusteella tekoälyn hyöty turvallisuustyössä realisoituisi parhaiten, kun organisaatiolla olisi valmiiksi sovitut kehotepohjat, hyväksymiskriteerit ja tarkistusvaihe, jolloin tekoälyn rooli pysyy valmistelun tukena eikä se siirry päätöksenteon korvaajaksi. Tätä väitettä korostaa tilannekuvan muodostamisen vaikeus, kun organisaation on ajautunut poikkeustilanteeseen ja oikeat päätökset pitäisi pystyä tekemään nopeasti.

Ryhmätyöpajan keskeinen johtopäätös oli, että generatiivinen tekoäly on käyttökelpoinen ulkoistetun turvallisuusasiantuntijan työssä silloin, kun sen käyttö sidotaan selkeään prosessiin, rajattuun aineistoon ja kontekstin tuntevan asiantuntijan vastuulla tapahtuvaan validointiin. Työpajan tulokset eivät muuttaneet aiemmin muodostunutta kokonaiskuvaa, vaan vahvistivat sitä ja konkretisoivat sen entistä tarkemmin käytännön työn kannalta. Tekoälyn lisäarvo nähtiin erityisesti tehokkuuden, tiedon jäsentämisen ja analyysin valmistelun näkökulmasta, kun taas sen rajat liittyivät kontekstin ymmärtämiseen, luotettavuuteen ja vastuulliseen päätöksentekoon.

4.4 Yhteenveto tutkimustuloksista

Tutkimustulokset osoittavat, että generatiivinen tekoäly on käyttökelpoinen ulkoistetun turvallisuusasiantuntijan työssä, mutta sen käyttökelpoisuus on selvästi ehdollista. Sekä asiantuntijakysely, yksilöhaastattelut että ryhmätyöpajan validointikeskustelu tuottivat samansuuntaisen tuloksen: tekoäly tuottaa eniten lisäarvoa tiedon jäsentämisessä, tilannekuvan kokoamisessa, vaihtoehtojen kokoamisessa ja analyysin valmistelussa. Sen sijaan tekoäly ei näyttäydy työssä itsenäisenä päätöksentekijänä eikä turvallisuusasiantuntijan korvaajana, vaan välineenä, jonka hyöty realisoituu vain asiantuntijan ohjauksessa ja vastuulla.

Tuloksissa korostui erityisesti se, että tekoälyn hyöty riippuu vahvasti työn rakenteista ja käytettävissä olevasta kontekstista. Kun turvallisuusjohtamisen vastuut, toimintamallit, dokumentaatio ja lähtöaineisto ovat selkeitä, tekoäly

tukee turvallisuusasiantuntijan työtä tehokkaasti. Vastaavasti epäselvässä toimintaympäristössä tai puutteellisen lähtöaineiston varassa sen käyttökelpoisuus heikkenee ja voi vaarantaa henkilöstön tai organisaation jatkuvuuden. Tämän perusteella voidaan todeta, että tekoäly ei kykene paikkaamaan puutteellista turvallisuusjohtamisen rakennetta, vaan toimii parhaiten silloin, kun se liitetään osaksi jo valmiiksi jäsennettyä ja toimivaa prosessia.

Tutkimustulokset osoittavat myös, että generatiivisen tekoälyn keskeisimmät rajoitteet liittyvät kontekstin ymmärtämiseen, tiedon ajantasaisuuteen, lähteiden luotettavuuteen ja siihen, että se voi tuottaa näennäisesti uskottavaa mutta käytännössä virheellistä tai tilanteeseen huonosti soveltuvaa sisältöä. Tästä syystä kaikissa aineistovaiheissa korostui validoinnin välttämättömyys. Tekoälyn tuottamaa sisältöä ei voida käyttää sellaisenaan, vaan turvallisuusasiantuntijan on arvioitava, tarkistettava ja hyväksyttävä se suhteessa organisaation tilanteeseen, ajantasaiseen tietoon ja päätöksenteon vaatimuksiin.

Kokonaisuutena tutkimus vahvistaa käsitystä siitä, että generatiivisen tekoälyn käyttökelpoisuus ulkoistetun turvallisuusasiantuntijan työssä on ennen kaikkea osaamis-, rakenne- ja prosessisidonnaista. Tekoälyn lisäarvo liittyy tehokkuuteen, tiedon käsittelyyn ja analyysin tukemiseen, mutta sen rajat tulevat vastaan siellä, missä tarvitaan harkintaa, vastuunkantoa, organisaation toimintaympäristön ymmärtämistä ja ihmisten johtamista. Näin tutkimustulokset osoittavat, että tekoäly voi vahvistaa turvallisuusasiantuntijan työtä, mutta vain silloin, kun sen käyttö on hallittua, rajattua ja sidottu asiantuntijan johtamaan työprosessiin.

5 Johtopäätökset ja pohdinta

5.1 Johtopäätökset suhteessa tutkimuskysymykseen

Tämän lopputyön tutkimuskysymys oli, miten generatiivista tekoälyä voidaan hyödyntää ulkoistetun turvallisuusasiantuntijan työssä siten, että se tukee analyysiä ja päätöksentekoa vaarantamatta tiedon luotettavuutta tai turvallisia toimintatapoja. Tutkimustulosten perusteella voidaan todeta, että generatiivinen tekoäly on käyttökelpoinen ulkoistetun turvallisuusasiantuntijan työssä, mutta vain tietyin ehdoin. Sen hyöty kohdistuu erityisesti tiedon jäsentämiseen, hajanaisen aineiston kokoamiseen, alustavan tilannekuvan muodostamiseen, vaihtoehtojen vertailemiseen ja analyysin valmisteluun. Sen sijaan tekoäly ei kykene korvaamaan turvallisuusasiantuntijan harkintaa, kontekstiosaamista, vastuunkantoa eikä päätöksentekoa.

Keskeinen johtopäätös on, että tekoälyn käyttökelpoisuus ei määräydy ensisijaisesti teknologian ominaisuuksien perusteella, vaan sen mukaan, millaiseen työprosessiin ja toimintaympäristöön sitä sovelletaan. Jos organisaation turvallisuusjohtamisen rakenne, vastuut, toimintamallit ja dokumentaatio ovat selkeitä, tekoäly voi tukea turvallisuusasiantuntijan työtä tehokkaasti. Vastaavasti tilanteissa, joissa rakenteet ovat epäselviä, toimeksiannon rajat hahmottumattomia tai lähtöaineisto puutteellista, tekoälyn käyttökelpoisuus heikkenee olennaisesti. Tällöin se ei täydennä asiantuntijatyötä, vaan voi lisätä väärintulkintojen, näennäisesti uskottavien johtopäätösten ja epäjohdonmukaisen toiminnan riskiä, sekä luoda merkittävää hukka-aikaa aikakriittisessä ympäristössä.

Tutkimuksen perusteella generatiivinen tekoäly soveltuu parhaiten asiantuntijatyön niihin vaiheisiin, joissa tarkoituksena on käsitellä suuria tietomääriä, tunnistaa olennaisia teemoja, laatia alustavia luonnoksia tai tuottaa vertailta-

via toimintavaihtoehtoja. Tämä tekee siitä käyttökelpoisen välineen erityisesti tilanteissa, joissa ulkoistettu turvallisuusasiantuntija joutuu nopeasti muodostamaan kokonaiskuvaa hajanaisesta tiedosta tai tukemaan organisaatiota matkustusturvallisuuteen, poikkeamiin tai kriisitilanteisiin liittyvässä valmistelussa. Samalla tutkimus osoittaa, että mitä lähemmäs siirrytään varsinaista päätöksentekoa, vastuunjakoa, riskin hyväksymistä tai henkilöstöön kohdistuvien vaikutusten arviointia, sitä vähemmän tekoälyä voidaan käyttää itsenäisesti ja sitä enemmän korostuu asiantuntijan oma arviointi.

Tutkimustulokset osoittavat myös, että luotettavuus on generatiivisen tekoälyn käytön ratkaisevin reunaehto. Tekoälyn keskeiset rajoitteet liittyvät kontekstin puutteelliseen ymmärtämiseen, tiedon ajantasaisuuteen, lähteiden laatuun ja siihen, että se voi tuottaa vakuuttavan oloista mutta käytännössä virheellistä tai tilanteeseen huonosti sopivaa sisältöä. Tämän vuoksi turvallisuusasiantuntijan työssä ei ole perusteltua käyttää tekoälyn tuotoksia sellaisenaan, vaan ne on aina arvioitava, tarkistettava ja suhteutettava organisaation omaan tilanteeseen. Tutkimuskysymykseen vastaamisen kannalta tämä tarkoittaa, että tekoäly voi tukea päätöksentekoa, mutta vain välillisesti tilanteissa, joissa se tukee päätöksenteon valmistelua, ei itse päätöstä.

Johtopäätöksenä todetaan, että generatiivinen tekoäly toimii ulkoistetun turvallisuusasiantuntijan työssä tarkoituksenmukaisesti vain silloin, kun sen käyttö on hallittua, rajattua ja sidottu sekä turvallisuusasiantuntijan johtamaan työprosessiin että osaamiseen tekoälyn käytettävyydestä. Se ei ole vaihtoehto turvallisuusasiantuntijalle, vaan turvallisuusasiantuntijan työtä tehostava väline. Tutkimuskysymyksen näkökulmasta tämä merkitsee, että generatiivista tekoälyä voidaan hyödyntää ulkoistetun turvallisuusasiantuntijan työssä analyysin ja päätöksenteon tukena, mutta vain siinä tapauksessa, että organisaation toimintamallit ovat riittävän selkeitä, lähtöaineisto on hallittavissa ja turvallisuusasiantuntija vastaa tuotosten validoinnista, tulkinnasta ja lopullisesta soveltamisesta.

5.2 Tekoälyn käyttökelpoisuuden ehdot ulkoistetun turvallisuusasiantuntijan työssä

Tutkimustulosten perusteella generatiivisen tekoälyn käyttökelpoisuus ulkoistetun turvallisuusasiantuntijan työssä ei muodostu automaattisesti teknologian saatavuudesta tai yksittäisen työkalun ominaisuuksista, vaan siitä, millaisissa rakenteissa, tehtävissä ja käyttötilanteissa sitä sovelletaan. Tekoälyn

käyttökelpoisuus on siten ennen kaikkea ehdollista. Tutkimuksen perusteella voidaan tunnistaa joukko keskeisiä ehtoja, joiden täyttyessä tekoäly voi tukea turvallisuusasiantuntijan työtä tarkoituksenmukaisesti, ja joiden puuttuessa sen käyttöön liittyvät riskit kasvavat olennaisesti.

Ensimmäinen keskeinen ehto on organisaation turvallisuusjohtamisen rakenteellinen selkeys (dokumentaatio). Tekoäly tuottaa lisäarvoa vain silloin, kun turvallisuusasiantuntijalla on käytettävissään riittävän selkeä käsitys organisaation vastuista, johtosuhteista, hyväksymiskäytännöistä, toimintamalleista ja dokumentaatiosta. Jos organisaation turvallisuusjohtaminen perustuu hajanaisiin käytäntöihin, epäselviin rooleihin tai puutteellisesti dokumentoituihin toimintamalleihin, tekoäly ei kykene paikkaamaan näitä puutteita. Päinvastoin se voi vahvistaa epäselvyyttä tuottamalla sisällöllisesti uskottavia mutta käytännön toimintaan heikosti soveltuvia vastauksia. Tämän vuoksi tekoälyn hyödyntämisen edellytyksenä on, että organisaation turvallisuutta ohjaava perusrakenne on riittävän jäsennetty, jolloin ulkoistettu turvallisuusasiantuntija pystyy hyödyntämään tilanteeseen tai sen selvittämiseen luomaansa kehote kirjastoa.

Toinen keskeinen ehto liittyy turvallisuusasiantuntijan omaan osaamiseen. Tutkimus osoitti, että tekoälyn arvo syntyy vain silloin, kun asiantuntija osaa rajata tehtävän, muotoilla kehotteet tarkoituksenmukaisesti, arvioida tuotosten laatua ja suhteuttaa ne käsillä olevaan tilanteeseen. Tämä tarkoittaa, että tekoälyn käyttö ei vähennä asiantuntijuuden tarvetta, vaan pikemminkin korostaa sitä. Ulkoistetun turvallisuusasiantuntijan on hallittava sekä oma substanssialueensa että ymmärrettävä riittävästi tekoälyn käytettävyydestä, sen rajoitteista ja sen tuottamien vastausten luonteesta. Ilman tätä osaamista tekoäly voi lisätä virhetulkintojen, väärän turvallisuuden tunteen ja ajanhukan riskiä erityisesti aikakriittisissä tilanteissa.

Kolmas käyttökelpoisuuden ehto on riittävä ja hallittu lähtöaineisto. Tutkimustulosten perusteella tekoäly toimii parhaiten silloin, kun käytettävä aineisto on rajattu, tehtävään soveltuva ja ajantasainen. Turvallisuusasiantuntijatyössä tämä tarkoittaa esimerkiksi sitä, että käytössä on organisaation omia suunnitelmia, matkustusturvallisuuden ohjeita, raportointikäytäntöjä, aiempia tilannekuvia tai muuta toimeksiannon kannalta olennaista materiaalia. Jos lähtöaineisto on puutteellinen, ristiriitainen tai liian laaja ilman selkeää ra-

jausta, tekoälyn käyttökelpoisuus heikkenee. Tällöin se voi tuottaa liian yleisiä vastauksia, nojata vanhentuneeseen tietoon tai rakentaa analyysin aineistolle, joka ei tosiasiassa vastaa organisaation tilannetta.

Neljäs keskeinen ehto on tekoälyn käytön rajaaminen oikeisiin työvaiheisiin. Tutkimuksen perusteella generatiivinen tekoäly on käyttökelpoisimmillaan tiedon jäsentämisessä, tilannekuvan alustavassa kokoamisessa, vaihtoehtojen vertailemisessa, luonnosten tuottamisessa ja analyysin valmistelussa. Sen sijaan käyttökelpoisuus heikkenee selvästi niissä tehtävissä, joissa tarvitaan riskin hyväksymistä, vastuullista päätöksentekoa, organisaatiokohtaista harkintaa tai henkilöstöön kohdistuvien vaikutusten arviointia. Käytännössä tämä tarkoittaa, että tekoälyä voidaan hyödyntää valmistelun tukena, mutta ei asiantuntijan harkintaa korvaavana ratkaisuna. Käyttökelpoisuuden ehto on siis myös tehtäväkohtainen: mitä lähempänä ollaan päätöksentekoa ja vastuunkantoa, sitä varovaisemmin tekoälyä tulee käyttää.

Viides ja ehkä tärkein ehto on systemaattinen validointi. Tutkimus osoitti, että tekoälyn tuotosten luotettavuus ei voi perustua pelkkään kielelliseen uskottavuuteen tai tekniseen nopeuteen. Turvallisuusasiantuntijan on arvioitava, mistä tieto on peräisin, kuinka ajantasaista se on, miten se suhteutuu organisaation omaan tilanteeseen ja onko se päätöksenteon kannalta käyttökelpoista. Tekoälyn käyttökelpoisuus edellyttää siis aina ihmisen tekemää tarkistusta, hyväksyntää ja vastuunkantoa. Mitä vakavammasta tilanteesta, aikakriittisemmästä tehtävästä tai suuremmasta turvallisuusvaikutuksesta on kyse, sitä vahvemmaksi validoinnin vaatimus muodostuu.

Tutkimuksen perusteella voidaan lisäksi todeta, että tekoälyn käyttökelpoisuuden ehtona on myös sen liittäminen osaksi selkeästi määriteltyä työprosessia. Tekoälyn käyttö ei saa jäädä satunnaiseksi kokeiluksi tai yksittäisen asiantuntijan henkilökohtaiseksi tavaksi työskennellä, vaan sen käyttöperiaatteiden tulisi olla mahdollisimman tietoisia, toistettavia ja dokumentoituja. Tämä on erityisen tärkeää ulkoistetun turvallisuusasiantuntijan työssä, jossa toimeksiannot voivat vaihdella nopeasti ja jossa toiminnan on kestettävä myös jälkikäteinen tarkastelu. Kun tekoälyn käyttö sidotaan työprosessiin, sen hyötyjä voidaan hyödyntää hallitummin ja samalla pienentää virheiden, epäjohdonmukaisuuden ja vastuun epäselvyyden riskiä.

Yhteenvetona voidaan todeta, että generatiivisen tekoälyn käyttökelpoisuuden ehdot ulkoistetun turvallisuusasiantuntijan työssä liittyvät rakenteeseen, osaamiseen, aineistoon, tehtävän rajaukseen, validointiin ja prosessinomaiseen käyttöön. Tekoäly on käyttökelpoinen väline vain silloin, kun nämä ehdot täyttyvät riittävässä määrin. Tällöin se voi tehostaa turvallisuusasiantuntijan työtä, parantaa tiedon käsittelyä ja tukea analyysin valmistelua. Jos ehdot eivät täyty, tekoälyn käyttö voi sen sijaan lisätä epävarmuutta, kuormittaa asiantuntijaa ja heikentää työn laatua juuri niissä tilanteissa, joissa johdonmukaisuus, tiedon luotettavuus, sekä turvallisuusasiantuntijan ja asiakasorganisaation välinen luottamus ovat kaikkein tärkeimpiä arvoja.

5.3 Tutkimuksen rajoitukset

Tämän tutkimuksen keskeinen rajoitus liittyy sen rajattuun tutkimuskontekstiin. Työssä tarkasteltiin generatiivisen tekoälyn käyttökelpoisuutta nimenomaan ulkoistetun turvallisuusasiantuntijan työssä, erityisesti matkustusturvallisuuden, tilannekuvan muodostamisen sekä poikkeama- ja kriisitilanteiden tukemisen näkökulmasta. Tulokset kuvaavat siis tätä rajattua ulkoistetun turvallisuusasiantuntijan työn aluetta tilanteessa, jossa hänet on otettu tukemaan tai sijaistamaan asiakasorganisaation turvallisuuspäällikköä, eivätkä täten ole yleistettävissä kaikkeen turvallisuusalan työhön tai muihin organisaatioympäristöihin. Tutkimuksen vahvuus on käytännönläheisyydessä, mutta samalla juuri tämä rajaus asettaa rajan tulosten laajemmalle yleistettävyydelle.

Toinen rajoitus liittyy aineiston laajuuteen ja muodostumiseen. Tutkimus perustui asiantuntijakyselyyn, kahteen yksilölliseen teemahaastatteluun sekä ryhmätyöpajan validointikeskusteluun. Aineisto oli tutkimuskysymyksen kannalta tarkoituksenmukainen ja tuotti syvällistä tietoa tutkittavasta ilmiöstä, mutta se ei ollut määrällisesti laaja. Tämän vuoksi tutkimuksen tuloksia tulee lukea laadullisina, kontekstisidonnaisina havaintoina eikä tilastollisesti yleistettävinä johtopäätöksinä. Aineiston koko ei heikennä sen käyttöarvoa tämän työn tavoitteisiin nähden, mutta se rajaa sitä, kuinka laajasti havaintoja voidaan soveltaa muihin toimintaympäristöihin.

Kolmas rajoitus liittyy tutkittavan ilmiön ajalliseen sidonnaisuuteen sekä siihen, että tässä työssä ei tarkasteltu eri generatiivisten tekoälymallien tai -tuotteiden välisiä eroavaisuuksia, joilla voisi olla vaikutusta käyttökelpoisuuteen

tutkimuksen kohteena olevan kokonaisuuden kannalta. Generatiivinen tekoäly kehittyy nopeasti, ja työkalujen ominaisuudet, käyttöliittymät, luotettavuus sekä organisaatioiden käyttötavat voivat muuttua lyhyessä ajassa, jolloin myös mallikohtaiset erot esimerkiksi ajantasaisuuden, lähteiden hyödyntämisen, rajoitteiden ja virheellisen mutta uskottavan sisällön riskin suhteen voivat muuttaa havaittua hyötyä ja validointitarvetta. Tämän vuoksi tutkimus kuvaa generatiivisen tekoälyn käyttökelpoisuutta nimenomaan syksyn 2025 tilanteessa, osin aikarajatussa ja paineistetussa ympäristössä, eikä sen tuloksia tule tulkita pysyvänä tai yleispätevänä arviona generatiivisen tekoälyn käytettävyydestä eri työkaluissa. On mahdollista, että osa tässä työssä tunnistetuista rajoitteista lievenee teknologian ja käytäntöjen kehittyessä, mutta yhtä mahdollista on myös se, että uudet ominaisuudet, uudet käyttötavat ja uudet riskit muuttavat arviointia, minkä vuoksi tulokset on perusteltua nähdä ajallisesti ja toteutusympäristöltään rajattuna kuvauksena.

Rajoituksia liittyy myös tutkimusasetelmaan ja tutkijan asemaan. Koska tutkimus on työelämälähtöinen kehittämistutkimus, se sijoittuu lähelle käytännön toimintaympäristöä ja sen kehittämistarpeita. Tämä on tutkimuksen vahvuus, mutta samalla se tarkoittaa, että tutkijan omat kokemukset, tulkinnat ja ennakkokäsitykset voivat vaikuttaa siihen, mitä aineistosta pidetään merkityksellisenä. Tätä riskiä pyrittiin pienentämään vaiheittaisella aineistonkeruulla, aineistojen välisellä vertailulla ja ryhmätyöpajassa toteutetulla validoinnilla, mutta sitä ei voida poistaa kokonaan. Tämän vuoksi myös tutkimuksen johtopäätökset on ymmärrettävä tulkinnallisina, vaikka ne perustuvatkin systemaattisesti rakennettuun aineistoon.

Lisäksi tutkimuksessa tarkasteltiin generatiivisen tekoälyn käyttöä ennen kaikkea käyttökelpoisuuden näkökulmasta. Työssä ei arvioitu eri tekoälymallien teknisiä eroja, suorituskykyä, kustannusrakennetta eikä tietoturva-arkkitehtuuria. Näin ollen tutkimus ei anna vastausta siihen, mikä yksittäinen tekoälyratkaisu olisi paras tai turvallisin, vaan siihen, millä ehdoilla generatiivista tekoälyä voidaan ylipäätään käyttää tarkoituksenmukaisesti ulkoistetun turvallisuusasiantuntijan työssä. Tämä rajaus oli tutkimuskysymyksen kannalta perusteltu, mutta samalla se jättää teknologian valintaan ja järjestelmätason toteutukseen liittyvät kysymykset tämän työn ulkopuolelle.

Kokonaisuutena tutkimuksen rajoitukset eivät poista sen arvoa, mutta ne määrittävät sen, miten tuloksia tulee tulkita. Työ tuottaa rajatussa kontekstissa käytännöllistä ja tutkimuksellisesti perusteltua tietoa siitä, millaisin ehdoin generatiivinen tekoäly voi tukea ulkoistetun turvallisuusasiantuntijan työtä. Samalla se osoittaa, että ilmiö vaatii jatkossa laajempaa, vertailevampaa ja ajallisesti toistuvaa tarkastelua, jotta tekoälyn käyttökelpoisuudesta voidaan muodostaa entistä vakiintuneempi käsitys.

5.4 Yhteenveto: mitä tulokset merkitsevät ulkoistetun turvallisuusasiantuntijan työssä

Tämän tutkimuksen tulokset merkitsevät ulkoistetun turvallisuusasiantuntijan työn näkökulmasta ennen kaikkea sitä, että generatiivista tekoälyä voidaan käyttää tarkoituksenmukaisena työvälineenä, mutta ei asiantuntijatyön korvaajana. Käytännössä tämä tarkoittaa, että tekoäly voi nopeuttaa työn käynnistämistä, helpottaa hajanaisen tiedon kokoamista, tukea alustavan tilannekuvan rakentamista ja auttaa vaihtoehtojen jäsentämisessä erityisesti tilanteissa, joissa toimeksianto alkaa nopeasti ja lähtöaineisto on laaja. Samalla tutkimus osoittaa, että tekoälyn käyttö ei vähennä turvallisuusasiantuntijan vastuuta, vaan korostaa tarvetta asiantuntevalle ohjaukselle, lähdekriittisyydelle ja työn prosessimaiselle hallinnalle.

Ulkoistetun turvallisuusasiantuntijan työn näkökulmasta havainto on merkittävä siksi, että työn onnistuminen perustuu kykyyn omaksua nopeasti asiakasorganisaation toimintaympäristö, tunnistaa turvallisuutta ohjaavat rakenteet ja tuottaa päätöksentekoa tukeva kokonaiskuva myös aikapaineessa. Tutkimuksen perusteella tekoäly voi tukea tätä työtä vain silloin, kun asiantuntijalla on riittävä osaaminen tekoälyn käytöstä sekä kyky rajata tehtävä, ohjata lähtötietoja ja arvioida tuotosten luotettavuutta osana omaa asiantuntijatyötään. Asiakasorganisaation näkökulmasta edellytys on, että turvallisuusjohtamisen rakenteet ja operatiivinen turvallisuusdokumentaatio ovat ajantasaisia ja käytännössä toimivia, jolloin ulkoistettu asiantuntija pystyy kytkeytymään johtamis- ja raportointirakenteisiin ilman viivettä. Jos tätä perustaa ei ole, tekoäly ei rakenna sitä asiakasorganisaation tai asiantuntijan puolesta, vaan käyttökelpoisuus heikkenee ja työ muuttuu herkästi reaktiiviseksi. Tulokset merkitsevät siten käytännössä sitä, että tekoälyn käyttökelpoisuus on sidoksissa sekä asiantuntijan osaamiseen että asiakasorganisaation turvallisuusjohtamisen kypsyyteen.

Tulokset merkitsevät lisäksi sitä, että ulkoistetun turvallisuusasiantuntijan työnkuva voi muuttua tekoälyn myötä osittain tehokkaammaksi, mutta samalla myös vaativammaksi. Tiedon etsimiseen, kokoamiseen ja alustavaan jäsentämiseen kuluvaa aikaa voidaan joissain tilanteissa vähentää, mutta vastineeksi asiantuntijalta vaaditaan aiempaa tarkempaa kykyä arvioida tiedon alkuperää, käyttökelpoisuutta ja soveltuvuutta käsillä olevaan tilanteeseen. Käytännössä tämä tarkoittaa, että tulevaisuudessa turvallisuusasiantuntijan työssä korostuu yhä enemmän kyky käyttää tekoälyä työvälineenä hallitusti, tunnistaa sen rajat ja soveltaa sen tuotoksia osana laajempaa ammatillista harkintaa.

Tutkimuksen perusteella ulkoistetun turvallisuusasiantuntijan työssä ei ole tarkoituksenmukaista kysyä, voiko tekoäly korvata asiantuntijan, vaan millaisissa työvaiheissa se voi aidosti vahvistaa asiantuntijan toimintakykyä. Tämän työn perusteella vastaus on selkein niissä tehtävissä, jotka liittyvät tiedon jäsentämiseen, tilannekuvan alustavaan kokoamiseen, vaihtoehtojen vertailuun ja analyysin valmisteluun. Sen sijaan tehtävissä, joissa tarvitaan vastuullista päätöksentekoa, organisaatiokohtaista harkintaa, ihmisten rauhoittamista, luottamuksen rakentamista tai turvallisuustoimien oikea-aikaista suhteuttamista, turvallisuusasiantuntijan rooli säilyy ratkaisevana. Näin tulokset merkitsevät käytännössä sitä, että tekoälyn paikka ulkoistetun turvallisuusasiantuntijan työssä on avustava, ei itsenäinen.

Kokonaisuutena tutkimus osoittaa, että generatiivinen tekoäly voi muodostua merkittäväksi osaksi ulkoistetun turvallisuusasiantuntijan työkalupakkia, mutta vain silloin, kun sen käyttö ymmärretään osaksi hallittua työprosessia eikä oikopolkuna asiantuntijatyön vaatimuksista. Tulosten käytännöllinen merkitys on siinä, että organisaatioiden ja ulkoistettujen turvallisuusasiantuntijoiden on syytä tarkastella tekoälyn käyttöä yhteisten pelisääntöjen, dokumentaation, validointikäytäntöjen ja roolien selkeyden kautta. Vasta tällöin tekoäly voi tuottaa sellaista lisäarvoa, joka parantaa työn laatua ja tehokkuutta heikentämättä luotettavuutta tai turvallisia toimintatapoja.

5.5 Jatkotutkimus- ja kehittämisehdotukset

Tämän tutkimuksen perusteella generatiivisen tekoälyn käyttö ulkoistetun turvallisuusasiantuntijan työssä on lupaava mutta vielä osin jäsentymätön tutkimus- ja kehittämiskohde. Tulokset osoittivat, että tekoäly voi tukea asiantuntijatyötä erityisesti tiedon jäsentämisessä, tilannekuvan kokoamisessa ja

analyysin valmistelussa, mutta samalla myös sen käyttökelpoisuus riippuu vahvasti rakenteista, kontekstista ja asiantuntijan ohjauksesta. Tästä seuraa, että jatkotutkimuksen tulisi kohdistua aiempaa tarkemmin niihin työvaiheisiin, joissa tekoäly voi tuottaa konkreettista lisäarvoa ulkoistetun turvallisuusasiantuntijan tehtävässä.

1. Toimeksiannon alun analyysi turvallisuuspäällikön toimenkuvan ja valtuuksien määrittämiseksi

   Tämän tutkimuksen perusteella ulkoistetun turvallisuusasiantuntijan työn onnistumisen kannalta ratkaisevaa on, kuinka nopeasti ja tarkasti asiantuntija pystyy muodostamaan käsityksen asiakasorganisaation turvallisuuspäällikön toimenkuvasta, valtuuksista, johtosuhteista ja niihin liittyvistä puutteista. Jatkossa olisi perusteltua tutkia, miten generatiivista tekoälyä voidaan käyttää asiakasorganisaation turvallisuutta ohjaavien dokumenttien analysointiin heti toimeksiannon alussa siten, että niiden perusteella voidaan jäsentää turvallisuuspäällikön tehtäväkenttä, tunnistaa epäselvyydet ja paikantaa turvallisuusjohtamisen rakenteelliset puutteet. Tällainen tutkimus olisi käytännöllisesti merkittävä, koska se voisi nopeuttaa toimeksiannon käynnistymistä ja parantaa ulkoistetun turvallisuusasiantuntijan mahdollisuuksia toimia tarkoituksenmukaisesti heti tehtävän alusta lähtien.

2. Turvallisuusasiantuntijan kehotekirjasto ja sen vaikutus

   Aihe liittyy turvallisuusasiantuntijan kehotekirjaston muodostamiseen ja hyödyntämiseen. Tässä tutkimuksessa tuli esiin, että tekoälyn käyttökelpoisuus riippuu voimakkaasti siitä, kuinka hyvin asiantuntija osaa rajata tehtävän, muotoilla kysymykset ja ohjata työkalua. Tästä syystä olisi perusteltua tutkia, miten järjestelmällisesti rakennettu kehotekirjasto voisi tukea ulkoistetun turvallisuusasiantuntijan työtä erilaisissa tilanteissa, kuten tilannekuvan muodostamisessa, raporttien valmistelussa, poikkeamien jäsentämisessä tai matkustusturvallisuuden arvioinnissa. Erityisen hyödyllistä olisi arvioida, millaista ajallista ja laadullista hyötyä kehotekirjaston käyttö tuottaa verrattuna täysin tapauskohtaiseen, ilman valmista rakennetta tapahtuvaan tekoälyn käyttöön.

3. Tekoälyagentit turvallisuuspäällikön apureina

Tutkimus kartoittaisi, missä määrin vakioidut agentit pystyisivät hoitamaan toistuvia valmistelu- ja koontitehtäviä, kuten kokousmuistioiden alustusta, tilannetiedotteiden luonnoksia ja seurantalistojen ylläpitoa. Pilottina agentit integroitaisiin valittuihin työnkulkuihin ja niiden tuotoksia verrattaisiin asiantuntijan tekemiin luonnoksiin. Mittareina olisivat valmiin luonnoksen laatuarvio, ajansäästö, hylkäysprosentti validoinnissa ja käyttäjien luottamus agenttiehdotuksiin.

4. Tekoälyagentit tilannekuvan muodostamisessa ja ylläpidossa

Jatkotutkimus tarkastelisi agenttipohjaista seurantaa, jossa agentit keräisivät ja jäsentäisivät julkisia lähteitä, priorisoisivat havaintoja ja tuottaisivat päivityksiä sovituin väliajoin. Koejakso toteutettaisiin niin, että agentin päivitys arvioitaisiin rinnakkain asiantuntijan päivityksen kanssa. Mittareina olisivat havaintojen osuvuus, päivityssyklin luotettavuus, päällekkäisten havaintojen määrä ja korjaustarpeet validoinnissa sekä lähde- ja ajantasaisuusvaatimusten noudattaminen.

5. Tekoäly turvallisuusdokumentaation arvioinnissa ja standardinmukaisuuden tukena

Tutkimus selvittäisi, kuinka hyvin tekoäly tunnistaisi ohjeistusten ja standardiviittausten välisiä puutteita ja ehdottaisi korjauksia, jotka auttaisivat muokkaamaan käytäntöjä halutun turvallisuusstandardin mukaisiksi. Menettelynä olisi arviointipilotti, jossa AI-pohjainen tarkistus ajettaisiin ohjeistokokonaisuuden läpi ja ehdotukset verrattaisiin asiantuntijapaneelin arvioon. Mittareina käytettäisiin havaittuja puutteita, ehdotusten toteutuskelpoisuutta ja ajansäästöä verrattuna manuaaliseen auditointiin.

6 Lähdeviitteet ja kirjallisuusluettelo

European Union (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). EUR-Lex. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Viitattu 12.3.2026.

ISO 18788:2015 (2015) Management system for private security operations — Requirements with guidance for use. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/63380.html. Viitattu 18.3.2026.

ISO 22301:2019 (2019) Security and resilience — Business continuity management systems — Requirements. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/75106.html. Viitattu 18.3.2026.

ISO 22320:2018 (2018) Security and resilience — Emergency management — Guidelines for incident management. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/67851.html. Viitattu 18.3.2026.

ISO 31000:2018 (2018) Risk management — Guidelines. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/65694.html. Viitattu 18.3.2026.

ISO 31030:2021 (2021) Travel risk management — Guidance for organizations. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/54204.html. Viitattu 18.3.2026.

NIST (2024) Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. Viitattu 20.3.2026.

OECD (2025) The effects of generative AI on productivity, innovation and entrepreneurship. OECD Artificial Intelligence Papers, No. 39. Paris: OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/the-effects-of-generative-ai-on-productivity-innovation-and-entrepreneurship_da1d085d/b21df222-en.pdf. Viitattu 20.3.2026.

OECD (2026) Building an AI-ready public workforce. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/building-an-ai-ready-public-workforce_b89244c7-en/full-report.html. Viitattu 20.3.2026.

Ojasalo, K., Moilanen, T. and Ritalahti, J. (2015) Kehittämistyön menetelmät – uudenlaista osaamista liiketoimintaan. 3.–4. painos. Helsinki: Sanoma Pro Oy.

Puolustusvoimat (2025) Puolustusvoimien data- ja tekoälystrategia. Helsinki: Puolustusvoimat. Available at: https://puolustusvoimat.fi/documents/1948673/2273743/Puolustusvoimien_Data_ja_teko%C3%A4lystrategia_JULK.pdf/96190125-e811-e08b-dcbc-660f67a94a81?t=1764246963044https://puolustusvoimat.fi/documents/1948673/2273743/Puolustusvoimien_Data_ja_teko%C3%A4lystrategia_JULK.pdf/96190125-e811-e08b-dcbc-660f67a94a81?t=1764246963044. Viitattu 21.3.2026.

Takana (2025a) Turvallisuusjohtamisen uudistaminen – askel askeleelta opas. Takana Oy, 12 May. Available at: https://takana.fi/2025/05/12/turvallisuusjohtamisen-uudistaminen-askel-askeleelta-opas/. Viitattu 14.3.2026.

Takana (2025b) Matkustusturvallisuus kriisialueilla – erityisjärjestelyjen merkitys. Takana Oy, 28 August. Available at: https://takana.fi/2025/08/28/matkustusturvallisuus-kriisialueilla-erityisjarjestelyjen-merkitys/. Viitattu 14.3.2026.

Takana (2025c) Kriisitilanteisiin varautuminen ja toimintamallit suomalaisissa yrityksissä. Takana Oy, 13 November. Available at: https://takana.fi/2025/11/13/kriisitilanteisiin-varautuminen-ja-toimintamallit-suomalaisissa-yrityksissa/. Viitattu 14.3.2026.

Takana (2026a) Mitä turvallisuusasiantuntija tekee? Takana Oy, 14 January. Available at: https://takana.fi/2026/01/14/mita-turvallisuusasiantuntija-tekee/. Viitattu 14.3.2026.TENK (2019) Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa. Helsinki: Tutkimuseettinen neuvottelukunta. Available at: https://tenk.fi/sites/default/files/2021-01/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2020.pdf. Viitattu 14.3.2026.

TENK (2023) Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Helsinki: Tutkimuseettinen neuvottelukunta. Available at: https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf. Viitattu 14.3.2026.

Vilkka, H. (2021) Tutki ja kehitä. 5., päivitetty painos. Jyväskylä: PS-Kustannus.