Tekoälyn hyödyntäminen turvallisuus-valvonnassa

Mahdollisuudet ja lainsäädäntö

Turvallisuusjohdon koulutusohjelma TJK 18

Lopputyöraportti

Markku Uurainen

Senaatti-Kiinteistöt

Helsingissä 12.3.2024

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Tämän lopputyön tarkoituksena on tutustua erilaisiin mahdollisuuksiin hyödyntää tekoälyä, koneoppimista, keinoälyä, analytiikkaa ja muita tekoälyn kattotermin alla olevia teknologioita käytännön turvallisuusvalvonnan kontekstissa. Näihin kuuluvat perinteisesti kameravalvonta, kulunvalvonta, rikosilmoitin- ja ääniohjausjärjestelmät, sekä joissain konteksteissa myös lukitusta ja kulunvalvontaa yhdistelevät järjestelmät. Tarkoituksena on analysoida myös lainsäädännön kannalta tarvittavia toimenpiteitä, kun näillä kyvykkyyksillä olevia järjestelmiä otetaan käyttöön. Tarkempana kontekstina turvallisuusvalvontana tässä tarkoitetaan etävalvontaa, hälytyskeskuksesta suoritettavaa valvontaa tai paikallisvalvomosta suoritettavaa valvontaa, jossa hyödynnetään jotakin teknologiaa. Lainsäädännön osalta on huomioitu lähinnä tällä hetkellä voimassaoleva lainsäädäntö, koska kirjoitushetkellä tuloillaan oleva EU:n Ai-Act ei vielä ole hyväksytty. Ai-Actin vaatimuksia kuitenkin sivuttiin vuoropuhelussa eri ohjelmisto- ja laitevalmistajien kanssa.

Lähestyin työtä varten Suomessa toimivia valmistajien edustajia, jotka tuottavat jotakin tekoälyä, analytiikkaa yms. hyödyntävää järjestelmää ja joka on jo käytössä Suomessa. Jokaiselle valmistajalle esitettiin soveltuvasti samansuuntaiset kysymykset, joilla pyrittiin selvittämään järjestelmän käyttökohteet, mahdolliset referenssitoteutukset Suomessa, sekä järjestelmän lainmukaisuus nyt ja tulevaisuudessa. Järjestelmien ominaisuuksia ei ole tarkoitus vertailla keskenään, vaan kartoittaa erinäisiä käyttökohteita ja mahdollisuuksia järjestelmien kyvykkyyksien perusteella. Työtä varten haastattelin myös Tietosuojavaltuutetun toimiston edustajaa, jolta sain tarkennuksia siihen, mitä lainsäädäntöä tulee huomioida ja pitää silmällä tässä kontekstissa.

Sisältö

1 Mitä on tekoäly turvallisuusvalvonnan kontekstissa

Tekoälyä voidaan käyttää kattoterminä useille eri automatisoiduille järjestelmille, jotka käyttötarkoituksensa ja kontekstinsa mukaan nojautuvat enemmän tai vähemmän automaattiseen tai avustettuun päätöksentekoon. Euroopan komission mukaan tekoäly on ”koneen kyky käyttää perinteisesti ihmisen älyyn liitettyjä taitoja, kuten päättelyä, oppimista, suunnittelemista tai luomista”. Tekoälyjärjestelmät kykenevät muokkaamaan itseään ja analysoimaan aiempia päätöksiä tuottaen siten iteroivalla metodilla tarkempia tuloksia. Komission mukaan tekoälyä käytetään mm. markkinoinnissa, digitaalisissa avustajissa, konekäännöksissä, älykodeissa, autoissa, kyberturvassa ja monessa muussa käyttökohteessa. (1)

Helsingin yliopiston tekoälykurssit tarjoavat erityisesti kahta avaintermiä tekoälyn määrittämiseen; Autonomisuus ja Adaptiivisuus. Tekoälyä hyödyntävät järjestelmät kykenevät siis suorittamaan tehtäviä monimutkaisissa ympäristöissä ilman käyttäjän ohjausta ja pystyvät parantamaan suorituskykyään oppimalla aiemmasta kokemuksesta. (2)

Toisaalta lähiaikoina ovat yleistyneet myös termit generatiivinen tekoäly sekä laajat kielimallit. Näillä tarkoitetaan usein yhdysvaltalaisen OpenAI -yrityksen popularisoimaa ChatGPT -kielimallia, vaikka kattoterminä ne käsittävät myös muita tekoälyjärjestelmiä. (3) Tekoälyn määrittelyssä käytettävät termit ja käyttötarkoitus vaihtelevatkin suuresti ja lukijan tulisi aina määrittää konteksti mahdollisimman tarkasti ennen, kuin kategorisoi järjestelmän jollakin tekoälyyn viittaavalla tarkemmalla termillä.

Tekoälyn oppimisessa ja opettamisessa on avainasemassa nimenomaan iteroiva lähestymistapa; asioita toistetaan ja dataa haravoidaan tarkkuuden parantamiseksi. Tarpeeksi monen toiston jälkeen tekoäly pystyy tunnistamaan tietyn asian tarvittavalla varmuudella ja käyttämään asiaa päätöksenteossa.

Toisaalta yhtä tärkeää on myös opettaa asiat toisin päin, eli esimerkiksi kuvantunnistamisessa ihminen ja mannekiini ovat samannäköisiä, mutta eivät ole sama asia.

Tekoälyn kattotermistön alle lukeutuu myös Selittävä tekoäly. Useimmat käytössä olevat tekoälyjärjestelmät eivät tarjoa päätöksenteon ketjua tarkasteltavassa muodossa loppukäyttäjälle, vaan tarjoavat monimutkaisuutensa vuoksi vain päättelyketjun lopputuloksen. Tällaisia järjestelmiä on laajasti käytössä mm. pankkialalla, jossa lainapäätökset perustuvat täysin automaattiseen päätöksentekoon. Näistä konepäätöksistä ei ole tarjolla järjestelmän käyttäjälle taustaparametrejä tai päätöksen perusteita kuin yleisellä tasolla. Selittävä tekoäly pyrkii vastaamaan kysymykseen, ”Mihin tehty päätös perustuu” ja tarjoamaan päätöksentekoketjulle ns. Audit Trailin. Oskari Nenonen käsittelee Pro gradu -tutkielmassaan (2021) selittävää tekoälyä ja mainitsee mm. Lainsäädäntövaatimusten noudattamisen yhtenä asiana, joihin nämä järjestelmät kykenevät ns. suljettua järjestelmää paremmin. Myös järjestelmän toiminnan varmistaminen ja parantaminen sekä järjestelmältä oppiminen helpottuvat, kun päätökset ovat näkyvissä (4).

Turvallisuusvalvonnassa tekoälyä voidaan hyödyntää hahmon- tai objektin tunnistamiseen, puheen, kasvojen, tai muiden fyysisten ominaisuuksien linkittämiseen tiettyyn identiteettiin, henkilön kulkureittien- ja käytöksen analysoimiseen ja moniin muihin tarpeisiin. Yleisimmät jo käytössä olevat metodit liittyvät kuvantunnistukseen; kameravalvontajärjestelmä voi esimerkiksi tunnistaa kuvasta tietyt objektit ja nostaa ihmisoperaattorille hälytyksen sääntöpohjaisesti riippuen objektien liikkeestä ja kulkusuunnasta. Toisaalta järjestelmä voi myös ohjata operaattorin keskittymistä pois sellaisista tapahtumista, jotka sääntöpohjaisesti on määritelty epäkiinnostaviksi tai turhiksi. Näin toimien suurissa järjestelmissä operaattorin eli käyttäjän huomio keskittyy oikeisiin asioihin. Erilaiset konenäkö-sovellutukset käyttävät myös vahvasti tekoälyä mm. ajoneuvojen tunnistamisessa tai rekisterikilpien tarkastelussa. Markkinoilla on myös järjestelmiä, jotka kokoavat sääntöpohjaisesti dataa useista eri lähteistä. Järjestelmät voivat analysoida kulunvalvonta-, rikosilmoitin- ja kameravalvontadataa samasta tapahtumasta tai hälytyksestä ja antaa toimenpidesuosituksia datasta tehtyjen havaintojen perusteella. Näissä sovellutuksissa esimerkiksi rikosilmoitinlaitteiston hälytys voidaan luokitella alemmalle prioriteetille, jos kyseisen hälytyksen yhteydessä on samalla käytetty kulunvalvontajärjestelmän tuottavaa dataa prioriteetin määrittämisessä.

Toisaalta hälytyksen prioriteettia voi taas nostaa epätavallinen kellonaika tai kulkureitti.

2 Teknistä turvallisuusvalvontaa käsittelevä lainsäädäntö

Turvallisuusvalvonta ja siihen liittyvä teknologia sisältävät lähes poikkeuksetta henkilötietojen käsittelyä. Täten tekoälyn soveltamiseen liittyvää lainsäädäntöä yrityksissä tulisikin tarkastella ensisijaisesti tietosuojan ja henkilötietojen käsittelyn näkökulmasta. Teknisessä turvallisuusvalvonnassa valvonta kohdistuu lähes aina kaikkiin käytettävän valvontajärjestelmän alaisiin henkilöihin ottamatta kantaa siihen, onko henkilö yrityksen työntekijä, ohikulkija, alihankkija ym. Varsinkin kameravalvonnassa muodostuu useimmiten laajoja henkilötietorekistereitä. Toisaalta näissä järjestelmissä rekisteröidyn yksilöiminen voi olla haastavaa.

Ensisijaisena lainsäädäntönä tietosuoja-asioissa toimii EU:n tietosuoja-asetus (5), josta löytyy useita velvoittavia artikloja henkilötietojen käsittelyyn liittyen. Tätä lakia täydentää suomessa säädetty Tietosuojalaki (6). Laki yksityisyyden suojasta työelämässä (7) taas ottaa kantaa tilanteisiin, jossa turvallisuusvalvontatyökalu kohdistuu yrityksen työntekijöihin.

Tekoälyn kontekstissa turvallisuusvalvontaan sovellettavat lait ja asetukset eivät juuri muutu, mutta tekoälyn käyttö saattaa laajentaa järjestelmän jo olemassa olevia kyvykkyyksiä tai rekisteröidystä kerättäviä tietoja. Tekoälyn toimesta rekisteröityyn saattaa kohdistua myös automaattista päätöksentekoa ja/tai profilointia, joka tulee ottaa huomioon vaikutustenarvioinnissa. Vaikka vaikutustenarviointi ei ole pakollinen prosessi/työkalu jokaisen järjestelmän käyttöönotossa, niin vaikutustenarvioinnilla saa kuitenkin hyvät suuntaviivat sille, onko järjestelmän käyttöönotto ylipäätään mahdollista ja minkälaisia tietosuojatoimenpiteitä tulisi toteuttaa ennen käyttöönottoa sekä järjestelmän käytön aikana. Vaikutustenarvioinnin pakollisuus lainsäädännön nojalla määräytyy EU:n tietosuoja-asetuksessa yksilöidystä käsittelytilanteista, tietosuojaviranomaisen käsittelytoimenpiteiden luettelosta tai kansallisesta lainsää-

dännöstä. Turvallisuusvalvonnan kontekstissa valvonta perustuu usein rekisteröityjen järjestelmälliseen valvontaan eli esimerkiksi kameravalvontaan yleisölle avoimissa tiloissa, jolloin vaikutustenarviointi tulee tehdä joka tapauksessa. Vaikutustenarviointia kannattaakin käyttää suositeltavana työkaluna aina järjestelmiä käyttöönotettaessa.

Vaikutustenarviointia ei tule sotkea riskienarviointiin, joka taasen on pakollista kaikissa käyttöönottotilanteissa lainsäädännön noudattamiseksi. Riskienarvioinnissa tunnistetaan jo suunnitteluvaiheessa ne toimenpiteet, jotka on tehtävä henkilötietojen asianmukaisen käsittelyn turvaamiseksi. Riskienarvioinnin pakollisuus tulee EU:n Tietosuoja-asetuksesta. Riskienarvioinnista ja vaikutustenarvioinnista löytyy ohjeita ja työkaluja Tietosuojavaltuutetun ylläpitämältä https://tietosuoja.fi -sivustolta (8). Arvioitaessa järjestelmien riskejä kannattaa huomioida, että järjestelmän valmistajalla ei periaatteessa ole velvollisuuksia järjestelmän kyvykkyyksien rajoittamiseen liittyen, vaan velvollisuus koskee lähinnä käyttäjää ja ostajaa. Hankittava tuote tulee siis tuntea ja konfiguroida oikein, jotta se täyttää lainsäädännön vaatimukset. Järjestelmän kyvykkyyksiä arvioidessa pitää huomioida myös Rikoslaki (9), koska järjestelmä saattaa oletuskonfiguraatiolla mahdollistaa sellaisen tiedon keräämisen, jonka tallentamista on mahdoton oikeuttaa. Tällainen tieto voi olla esim. äänitallenteet julkisilta paikoilta (salakuuntelu). Vaikutustenarviointia ja riskienarviointia kannattaa siis soveltaa laajasti ja tekoälyä hyödyntävien turvallisuusjärjestelmien hankkiminen vaatii vahvaa ammattitaitoa myös hankintaorganisaatiolta.

Tietosuojavaltuutettu määrittelee henkilötietojen käsittelyn seuraavasti: ”käsittely tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.” (10). Täten esimerkiksi kameravalvonta ilman tallentamista ei välttämättä ole henkilötietojen käsittelyä. Tekoälyä käyttävät järjestelmät kuitenkin useimmiten joutuvat tallentamaan käsiteltävän datan ainakin väliaikaisesti ja turvallisuusvalvontaan soveltuvan tekoälyjärjestelmän hankkija päätyykin useimmiten oman järjestelmänsä rekisterinpitäjäksi ja silloin organisaatioon sovelletaan aiemmin mainittujen lakien velvollisuuksia tältä näkökannalta. Järjestelmän tyypilliset loppukäyttäjät, esimerkiksi vartiointiliikkeen työntekijät, ovat useimmiten henkilötietojen käsittelijän asemassa. Henkilötietojen käsittely edellyttää aina laista löytyvää

käsittelyperustetta (11). Käsittelyperustetta tarkastellessa tulee myös huomioida erityiset henkilötietoryhmät, joiden käsittely vaatii erityisiä perusteluja (12).

Jos järjestelmä toteuttaa automaattista päätöksentekoa tai profilointia, niin silloin myös näille toimenpiteille pitää löytyä lainsäädännöllinen peruste. Profiloinnin ja automaattisen päätöksenteon raja turvallisuusvalvonnan kontekstissa voi olla häilyvä; useimmiten järjestelmät voivat esimerkiksi nostaa hälytyksiä tietynlaisen havaitun käytöksen perusteella, mutta jos hälytyksen käsittely vaatii myös luonnollisen henkilön tosiasiallisen osallistumisen päätöksentekoon, niin kyseessä ei välttämättä ole automaattisen päätöksenteon määritelmän täyttävä toiminne. Tässäkin tapauksessa käytettävä järjestelmä tulee tuntea riittävän tarkasti.

Tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat (13). Osoitusvelvollisuus on keskeinen periaate tietosuoja-asetuksessa. Tietosuoja-asetuksessa on osoitusvelvollisuutta koskevia vaatimuksia, joiden velvoittavuus on arvioitava tapauskohtaisesti. Rekisterinpitäjän on huomioitava osoitusvelvollisuus jo henkilötietojen käsittelyn suunnitteluvaiheessa (14). Tietosuojavaltuutetun ylläpitämä Tietosuoja.fi -sivusto kertoo listauksen tarvittavista toimenpiteistä ja dokumentaatiosta osoitusvelvollisuuden toteuttamiseksi. Useimmiten suuri osa näistä velvollisuuksista voidaan täyttää vaikutus- ja riskienarvioinnin jälkeen tehtävällä julkisella tietosuojaselosteella, jossa on eriteltynä jokainen kohta. Tietosuojaselostetta kutsuttiin aiemmin nimellä Rekisteriseloste, joka oli pakollinen asiakirja kumotun Henkilötietolain (15) perusteella. Nykyisin tietosuojaseloste ei ole EU:n tietosuoja-asetuksen mukainen pakollinen asiakirja, mutta rekisteröityä tulee kuitenkin informoida hänen henkilötietojensa käsittelystä. Aiemmin mainitut vaatimukset on siis helppo täyttää käyttämällä tietosuojaselostetta, joka on pyydettäessä saatavilla.

Lainsäädäntö antaa rekisteröidylle myös oikeuksia ja näiden toteutuminen turvallisuusvalvontajärjestelmissä ei välttämättä ole itsestäänselvyys (16). Esimerkiksi kameravalvontajärjestelmässä unohdetuksi tuleminen ei välttämättä ole edes teknisesti mahdollista ja tällöin järjestelmään liittyvä dokumentointi täytyy olla sillä tasolla, että tämä asia pystytään perustelemaan. Jos rekisteröity käyttää esimerkiksi oikeuttaan ”Saada jäljennös häntä koskevista

henkilötiedoista” (17), niin kameravalvontajärjestelmien osalta pitää pystyä myös tarvittaessa tarkastelemaan tällaisen pyynnön toteutusmahdollisuutta ja tarvittaessa käyttää kieltäytymisperustetta; tällainen peruste voi olla esimerkiksi se, että samalla kameratallenteella näkyy muita henkilöitä, jolloin tietojen luovutus vaarantaisi heidän henkilötietonsa. Rekisterinpitäjän tulee jälleen tuntea myös rekisteröidyn oikeuksia koskeva lainsäädäntö tarkasti.

Tietosuojaan liittyy myös tietoturva. Rekisterinpitäjän velvollisuutena on toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet tietojen suojaamiseksi. Näissä tulisi olla kuvattuna myös mahdollisten tietoturvaloukkausten käsittelyprosessi. Turvallisuusvalvonnan kontekstissa tällainen loukkaus voi tapahtua esimerkiksi silloin, jos järjestelmän tietoja pääsee katselemaan joku ulkopuolinen tai koko järjestelmä on esimerkiksi saavutettavissa internetistä ja hakkeroitavissa. Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille (18).

Laki yksityisyyden suojasta työelämässä luku 5 §16 ja §17 sisältää yksityiskohtaisia säädöksiä kameravalvonnan toteuttamisesta työpaikalla (19). Nämä säädökset kohdistuvat nimenomaan yrityksen omiin työntekijöihin tai alihankkijoihin. Laki sisältää myös yleisiä säädöksiä henkilötietojen käsittelyyn, mutta näissä on suurin piirtein samansuuntaisia vaatimuksia kuin EU:n tietosuoja-asetuksessa (mm. Tarpeellisuusvaatimus). Lähtökohtaisesti työnantaja saa toteuttaa työpaikalla kameravalvontaa tietyin rajoituksin, mutta kameravalvontaa ei kuitenkaan saa käyttää tietyn työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla. Kuten monissa laeissa, niin tähänkin on poikkeuksia; yksittäistä työpistettä saa kuvata esimerkiksi työntekijä turvallisuuden takaamiseksi, merkittävään omaisuuteen kohdistuvien rikosten estämiseksi, tai työntekijän etujen ja oikeuksien varmistamiseksi, jos kameravalvonta perustuu työntekijän pyyntöön. Kameravalvonnan käyttöönotto työpaikalla edellyttää myös ennakkoselvityksiä; ennen kameravalvonnan käyttöönottamista pitää selvittää työntekijöiden yksityisyyteen vähemmän puuttuvien

muiden keinojen käyttömahdollisuudet. Tallenteiden käyttömahdollisuus pitää rajata ennalta suunniteltuihin tapauksiin ja kameravalvonnasta sekä sen toteuttamisesta pitää ilmoittaa näkyvällä tavalla niissä tiloissa, joihin kamerat on sijoitettu. Lisäksi työntekijöille pitää tiedottaa asiasta 21 §:ssä tarkoitetun yhteistoiminta- tai kuulemismenettelyn jälkeen kameravalvonnan alkamisesta, toteuttamisesta ja siitä, miten ja missä tilanteissa mahdollisia tallenteita käytetään sekä 16 §:n 2 momentin tarkoittamissa tilanteissa kameroiden sijainnista.

Euroopan komissio on julkaissut hyvän ohjeen henkilötietojen käsittelystä videolaitteilla, joka käy läpi henkilötietolain oleellisimmat kohdat suhteessa videovalvontaan (21).

Laki yksityisyyden suojasta työelämässä Luku 7 §21 mainitsee, että työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat yhteistoimintalaissa tarkoitetun vuoropuhelun sekä yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnassa ja hyvinvointialueella annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin (20). Käytännössä siis pelkän yksikertaisen, lokeja keräävän kulunvalvontajärjestelmänkin asennus vaatii yhteistoimintamenettelyä yrityksessä. Tällaisista asioista on usein kuitenkin sovittu kattosopimuksella, jolloin samaa menettelyä ei tarvitse toistaa jokaisen erillisen järjestelmälaajennuksen tai käyttöönoton yhteydessä. Yrityksen tulee kuitenkin olla tarkkana siitä, että järjestelmien käyttötarkoitus ja menetelmät on dokumentoitu ja tiedotus hoidettu asiallisesti.

Yhteenvetona lainsäädäntö näyttelee isoa osaa minkä tahansa turvallisuusvalvonnassa käytettävän järjestelmän käyttöönotossa. Tekoäly- tai keinoälyominaisuudet saattavat useinkin rikastaa järjestelmän käyttökohteita, mutta eivät varsinaisesti muuta järjestelmän käyttötarkoitusta. Järjestelmien osalta tulee tunnistaa se, mitä dataa järjestelmät keräävät ja löytyykö ko. datalle lainmukaista käsittelyperustetta. Joissakin tapauksissa tiettyjä lainkohtia voidaan kuitenkin vältellä esimerkiksi anonymisoimalla; jos kameravalvonnalla toteutetaan vain koneoppimispohjaista henkilölaskentaa livekuvaa tallenta-

matta, niin tällöin dataa voidaan käsitellä huomattavasti keveimmin lainsäädäntöperustein; järjestelmä ei tallenna henkilötietoja ja lopputuloksena on vain numeerinen laskenta. Samoin esimerkiksi kulunvalvontajärjestelmän tuottamaa dataa voidaan käsitellä poikkeamien tunnistamiseksi siten, että välissä data anonymisoidaan; tällöin datassa ei periaatteessa ole henkilötietoja analysoivan järjestelmän puolella. Useimmissa käyttötapauksissa seurattaisiin kuitenkin esimerkiksi kulkutunnistetta, joka on sidottavissa tunnistettavaan henkilöön toisen järjestelmän puolella ja tällöin tietosuoja-asetuksen säädökset saattavat astua voimaan myös poikkeamia tunnistavan järjestelmän osalta. Toisaalta kulunvalvontadataa voidaan käyttää täysin anonymisoituna esimerkiksi käyttöasteen mittaukseen. Näissäkin tapauksissa ko. järjestelmälle tehtävä riskien- ja vaikutustenarviointi todennäköisesti kertoo tarvittavat menettelyt järjestelmän käyttöönottamiseksi.

3 Tuotteita ja niiden kyvykkyyksiä

Suomessa on käytössä useita eri tekoälyä tai koneoppimista käyttäviä turvallisuusvalvontatuotteita. Valtaosa näistä painottuu kamera-analytiikkaan tai kuva-analyysiin, mutta osa tuotteista analysoi myös kulunvalvontadataa poikkeamien löytämiseksi tai yhdistelee jopa dataa eri sensoreista tai lähteistä. Järjestelmät poikkeavat toisistaan suuresti ja tässä työssä keskitytään niihin järjestelmien tarjoamiin ominaisuuksiin, joita on käytettävissä tässä ja nyt. Monella valmistajalla oli kehitysputkessa myös tulevaisuudessa mielenkiintoisia ominaisuuksia, mutta ne on rajattu tämän työn ulkopuolelle. Alla käsitellyt järjestelmät esitellään yleisellä tasolla järjestelmän yleisimpien kyvykkyyksien kartoittamiseksi, mutta kaikkia järjestelmän tarjoamia ominaisuuksia ei välttämättä ole listattu. Järjestelmien kartoittamista on lähestytty turvallisuusvalvomo- ja hälytyskeskusnäkökulmasta sekä tuotteiden käytettävyydestä nimenomaan tämänkaltaisissa ympäristöissä. Järjestelmien osalta on kartoitettu myös kysymystä datan omistajuudesta; analytiikka-osio saattaa tapahtua pilvessä, jolloin datan omistajuus tietosuojan näkökulmasta on tärkeä kysymys. Kaikkien järjestelmien osalta ei ollut mahdollista saada valmistajien kommentteja ja osa järjestelmistä rajautui myös ulkopuolelle, koska niistä ei ollut saatavissa tarpeeksi tietoa tätä työtä varten. Kuvankaappaukset järjestelmistä on otettu joko Senaatti-Kiinteistöjen käytössä olevista asennuksista tai järjestelmien markkinointimateriaaleista.

Lähtökohtaisesti järjestelmistä oli hankala löytää julkisesti mainittavaa referenssikohdeasennusta, koska turvallisuusalalla kohdekohtaiset järjestelmät ovat usein salassa pidettävää tietoa. Tähänkin ”sääntöön” löytyi kuitenkin muutama poikkeus.

3.1 Milestone

Milestone systems on globaalin Canon Groupin alainen, alun perin tanskalainen tallennin- ja tallenninohjelmistovalmistaja. Milestonen ohjelmistoratkaisu on laajalti käytössä niin suomessa kuin maailmallakin. Analytiikan

osalta Milestone toimii integraatio-alustana muille tuotteille; Milestonessa itsessään ei siis ole varsinaisia analytiikka- tai AI-ominaisuuksia. Järjestelmään voidaan integroida mm. Axis, Bosch, Hikvision, Hanwha tai muunmerkkisten valmistajien kameroita analytiikka-ominaisuuksineen. Kaikenkaikkiaan Milestonella on satoja teknologiapartnereita (23) ja integraatiot ulottuvat myös ovipuhelimiin ja muihin tuotteisiin. Lisäksi Milestone tukee perinteisenä tallenninratkaisuna toimiessaan myös harvinaisempia kameravalmistajien kameroita. Analytiikan integrointi Milestoneen ei vaadi väliin esimerkiksi relelähtöä tai vastaavaa fyysistä integrointia, vaan aiemmin mainituista partnerikameroista saadaan analytiikkahälytykset suoraan Milestonen ohjelmistoon tietoverkon ylitse kohteen sisällä. Milestonen ohjelmistolla voi myös ohjata esimerkiksi PTZ-kameran valmisasennon hälytyksen aiheuttaneen objektin suuntaan. Lisäksi Milestone on osa CVE-ohjelmaa (Common Vulnerabilities and Exposures) (22).

Valmistajan mukaan järjestelmä on yhteensopiva nykyisen ja mahdollisesti tulevan lainsäädännön kanssa (EU:n AI-Act), koska lain nykytulkinnan mukaan järjestelmän käyttäjä vastaa järjestelmän ominaisuuksien lainmukaisesta käytöstä ja käyttöönotosta.

Järjestelmässä voidaan kytkeä päälle tapahtumien lokitus, jota analysoimalla voi saada osviittaa analytiikan/AI:n tekemästä luokittelusta esimerkiksi objektintunnistuksessa. Analyysikyvykkyys on kuitenkin kolmannen osapuolen kameroissa itsessään, ei Milestonen ohjelmistossa. Järjestelmä ei opiskele käyttäjän toimia tuotekehitysmielessä tai analytiikan opetustarkoituksissa.

Milestonen osalta rekisterinpitäjä omistaa datan yksiselitteisesti, jos järjestelmä on asennettu paikalliseen tallentimeen. Analytiikan käyttöönotto ei vaikuta tähän seikkaan. Pilviratkaisuissa datan omistajuus voi vaihdella sopimuksellisesti.

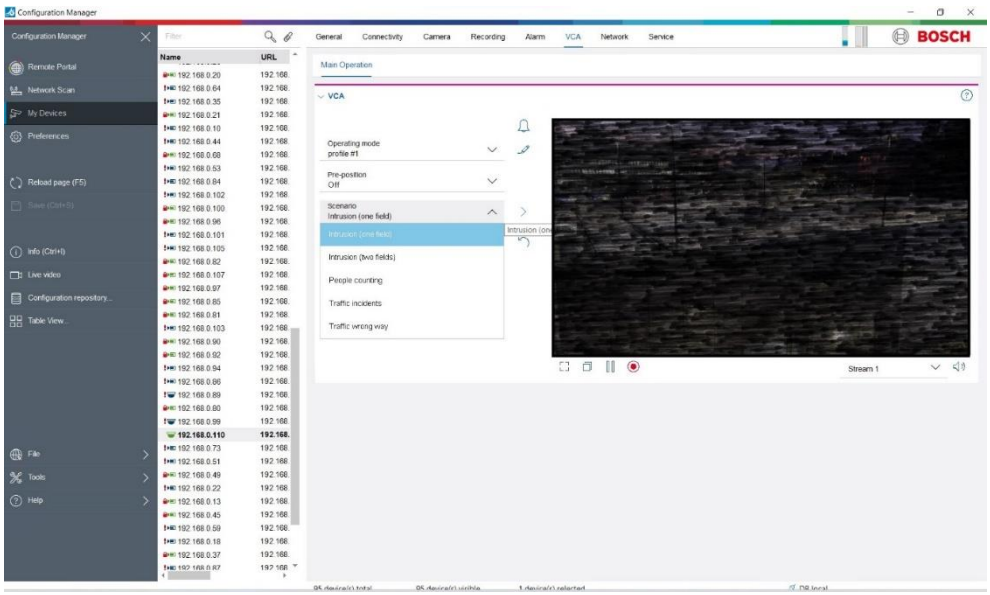
Kuva 1 Milestonen hallintaohjelmiston käyttöliittymä.

3.2 Bosch Security Systems

Bosch Security on osa kansainvälistä Robert Boschin säätiön alaista konglomeraattia. Boschin on perustanut saksalainen Robert Bosch, jonka nimeä nykyisin yrityksen 94% -prosenttisesti omistava säätiö kantaa. Bosch Securityn innovaatiot juontavat juurensa ajoneuvojen tekniikkaan, jossa Boschin tuotteet näyttelevät edelläkävijän roolia. Bosch Security Systems valmistaa kameroita, IP-kaiuttimia, äänihälytysjärjestelmiä, rikosilmoitinjärjestelmiä ja muita turvallisuustuotteita. Tässä keskitytään Boschin tarjoamiin kameraanalytiikkatuotteisiin. Bosch valmistaa tuotteensa itse omilla tehtaillaan paikallisille markkinoille; esimerkiksi Euroopan tuotteet tulevat Portugalin tehtaalta, eivät kaukoidästä. Myös Boschin ohjelmistokehitys on In-House -tuotantoa.

Boschilla on jonkinlaista analytiikkaa vakiona hyvin monessa eri kameramallissa. Analytiikka on viime vuosina pystynyt tunnistamaan ja luokittelemaan esimerkiksi ihmisiä, ajoneuvoja tai objekteja. Lisäksi näiden perusteella voidaan luoda sääntöpohjaisia hälytyksiä, joilla voidaan esimerkiksi havaita ajoradalla kävelevät ihmiset tai junaradan raiteille paikalleen jäävät ajoneuvot. Boschin kamerat tunnistavat myös objektien ominaisuudet; esimerkiksi autoa seuratessa analytiikka ymmärtää, että autolla on massa ja auto ei voi pysähtyä tai vaihtaa suuntaa välittömästi. Tämä mahdollistaa myös saman objektin

”seuraamisen”, vaikka objekti menee piiloon toisen objektin taakse ja tulee takaisin näkyviin muutaman sekunnin päästä. Lähiaikoina järjestelmää on kehitetty tunnistamaan mm. erilaisia aseita tai droneja. Käytössä olevat ominaisuudet riippuvat hankitusta kameralisenssistä sekä kameran ominaisuuksista. Boschin kameroilla voidaan lähettää hälytyksiä muille järjestelmille esim. http-sanomilla käyttämällä Boschin ATSL (Alarm Task Script Language)-skriptimoottoria tai hälytykset voidaan integroida erilliseen fyysiseen releläh-töön. Näin voidaan ohjata myös suoraan samassa lähiverkossa sijaitsevia IP-kaiuttimia esimerkiksi automaattisanoman muodossa, kun analytiikka havaitsee henkilön kiipeämässä vaikkapa virtuaalisen tai fyysisen aidan ylitse.

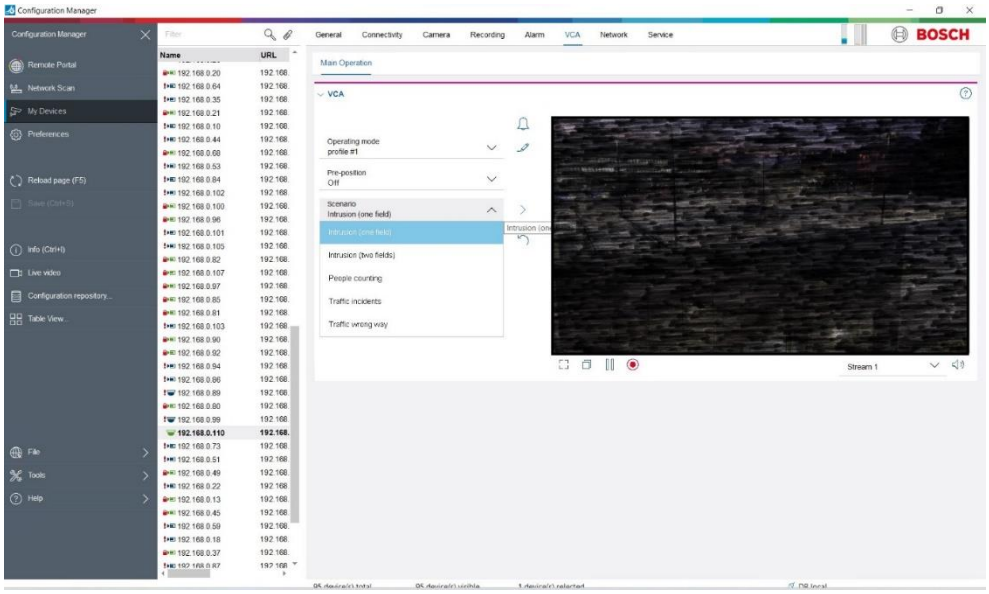


Kuva 2 Boschin kamera-analytiikkaa, jossa objektit luokitellaan ja kulkusuunnat/reitit piirretään analyysitarkoituksessa. (24)

Boschin kameroita on käytössä Suomessa laajasti mm. virastotaloissa.

Järjestelmän/analytiikan tekemiä päätöksiä ei varsinaisesti pääse auditoimaan, mutta kehittäjillä on käytössään debug-työkaluja, joilla mahdollisesti yksittäistä tapahtumaa voidaan pyrkiä selittämään. Järjestelmän käyttötapaukset on käyttäjän määriteltävissä ja siten lainsäädäntö-yhteensopivuus nyt ja tulevaisuudessa riippuu järjestelmän konfiguroinnista ja asennustavasta.

Analyysit tapahtuvat aina suoraan kamerassa ja näissä ei ole minkäänlaista pilvikytkentää tai etälaskentaa. Datan omistajuus säilyy sillä osapuolella, joka analyysejä ja kameratallenteita hallinnoi (rekisterinpitäjä).



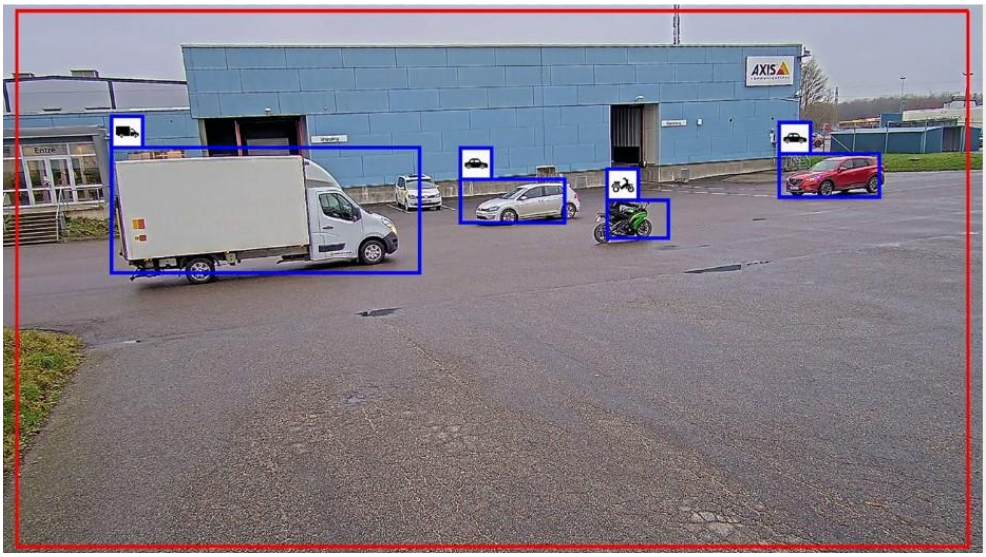
Kuva 3 Boschin kamera-analyysin konfigurointivaihtoehtoja Bosch Configuration Managerissa. Saatavilla olevat ominaisuudet riippuvat kamerasta ja lisenssistä.

3.3 Axis Communications

Axis Communications on osa globaalia Canon Groupia. Axis profiloituu kuitenkin ruotsalaisena, itsenäisenä yhtiötä. Yhtiön tuotteisiin kuuluu kameroita, IP-kaiuttimia, kulunvalvontalaitteistoa, rikosilmoittimia ynnä muita alan tuotteta (25). Axis kuuluu myös CVE-Ohjelmaan (22). Axiksen erikoisuutena on In-house suunnitellut ”ARTPEC” SOC:it (System on chip), eli käytännössä Axis suunnittelee itse käyttämänsä järjestelmäpiirit ja valmistuttaa ne täysin itse hallinnoimallaan ketjulla alihankkijoita (26). Tämä antaa Axikselle mahdollisuuden räätälöidä tuotteita entistä tarkemmin ja tietoturva-näkökulmasta antaa valmistajalle mahdollisuuden vaikuttaa tuotteidensa tietoturvaan myös rautatasolla. Kyberturvallisuus onkin yksi Axiksen listaamista kulmakivistä heidän liiketoiminnassaan.

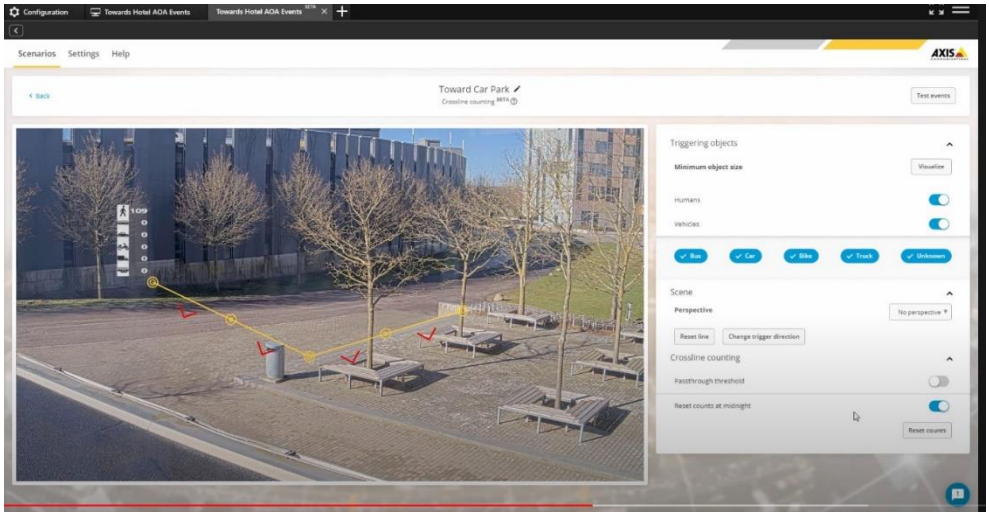
Axiksen kameroissa on laajalti analytiikka-ominaisuuksia mallisarjasta riippuen; näihin kuuluvat mm. objektien ja ajoneuvojen luokittelu, kulkusuuntien analysointi, kasvontunnistus, ihmisten laskenta ja muut sovellutukset (26).

Ominaisuuksiin kuuluu myös live privacy masking, eli esimerkiksi alueevalvontaa toteutettaessa voidaan liikkuvat hahmot sumentaa kokonaan tai kasvojen kohdalta, mutta muu kuva säilyy valvontakäyttöön normaalina. Tällöin esimerkiksi julkisten alueiden kuvaaminen voi olla hyväksyttävämpää. Axiksen kamera-analytiikkaa voidaan yhdistellä muihin tuotteisiin, esimerkiksi aluevalvonnassa käytettäviin tutkiin. Joissain kameramalleissa on myös tutkakeilain valmiina, jolloin kamera tuottaa dataa useasta eri sensorista. Axiksen tuotteet kommunikoivat keskenään IP-verkossa, eli laiteiden väliin ei välttämättä tarvitse tehdä releasennuksia tai erillistä palvelinta. Axiksen kamera-analytiikan tuottamat hälytykset saa vietyä esimerkiksi Axiksen omaan VMS-ohjelmistoon (Axis Camera Station) tai Milestoneen. Myös esimerkiksi PTZ-kameraa voidaan ohjata tutkasignaalin tai havainnon suuntaan ja sen jälkeen tunnistaa objekti analytiikalla.



Kuva 4 Axiksen objektiluokittelua (27)

Axiksen kamerat tuottavat analyysit aina laitteessa itsessään, eli laskentaa ei tehdä pilvessä eikä data poistu järjestelmästä. Analyysin tekemiä päätöksiä ei varsinaisesti voi auditoida, mutta laitteiden järjestelmälokia voi tulkita valmistajan toimesta. Datan omistus säilyy aina laitteen omistajalla ja laite ei opiskele käyttäjän toimia analytiikan- tai tuotekehityksen nimissä.

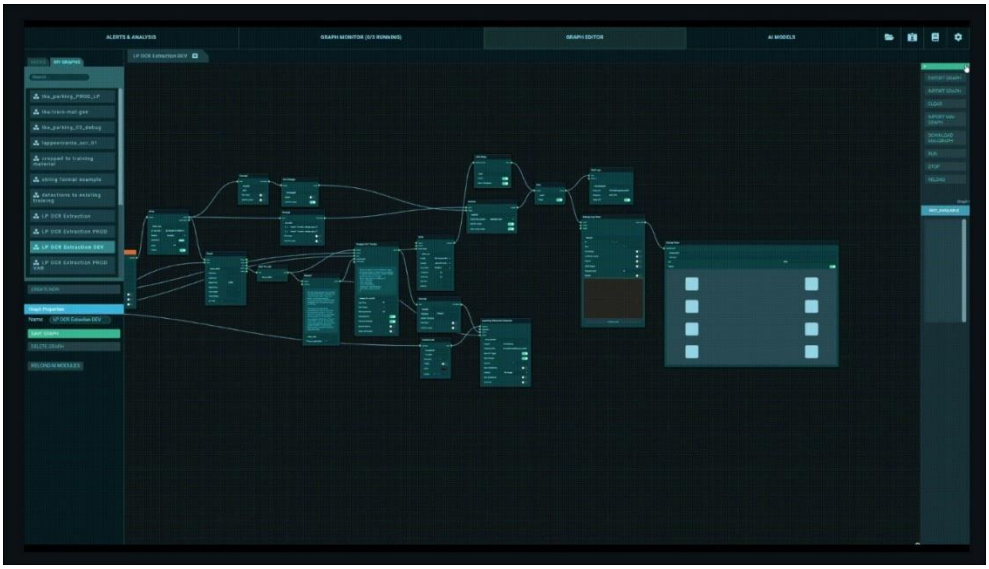


Kuva 5 Axiksen konfigurointinäkymä kamera-analytiikalle (27)

3.4 MarshallAI

MarshallAI on Suomalainen kamera-analytiikkaan erikoistunut yhtiö, jonka päätuotteena on itsekonfiguroitava ”No-code” tyyppinen analytiikka-alusta. MarshallAI:n ohjelmisto voidaan opettaa sääntöpohjaisesti havaitsemaan kuvasta lähes mitä tahansa. MarshallAI voi tunnistaa myös ääntä esimerkiksi kamerasta tai dataa muista sensoreista. MarshallAI tarjoaa ohjelmistoa joko työkaluna asiakkaan itsetehtävään konfigurointiin, tai valmiiksi konfiguroituna tiettyyn tarkoitukseen/käyttötapaukseen. Alusta on rakennettu siten, että edistynyt tekninen pääkäyttäjä voi itse konfiguroida ja opettaa analytiikkaohjelmistoa. Itse laskenta voi tapahtua joko paikallisella erillislaitteella, on-prem palvelimella näytönohjaimella, tai pilvessä/konesalissa tapahtuvilla resursseilla. MarshallAI on Yhdysvaltalaisen näytönohjainvalmistaja Nvidian teknologiapartneri (28). MarshallAI:n teknologia on valmistajariippumatonta kuvaa tuottavan elementin osalta, eli kunhan kamerakuva täyttää tietyt tekniset vaatimukset, niin kameran valmistajalla ei periaatteessa ole väliä. Myös analogiset kamerat ovat rajatusti tuettuja. MarshallAI kuitenkin valikoi liiketoiminta-alueitaan jonkin verran; esimerkiksi itärajan ylitse järjestelmää ei myydä ja tietyt kiinalaiset kameramerkit eivät periaatteessa ole tuettuja järjestelmässä, vaikka teknisesti tuki olisikin toteuttavissa. Järjestelmän ominaisuudet riippuvat myös hieman ostajan asemasta; esimerkiksi kasvontunnistusta ei Suomessa aktivoida viranomaiskäyttäjien ulkopuolella.

Julkisena referenssikohteena järjestelmällä on mm. Suomen tulli (29).

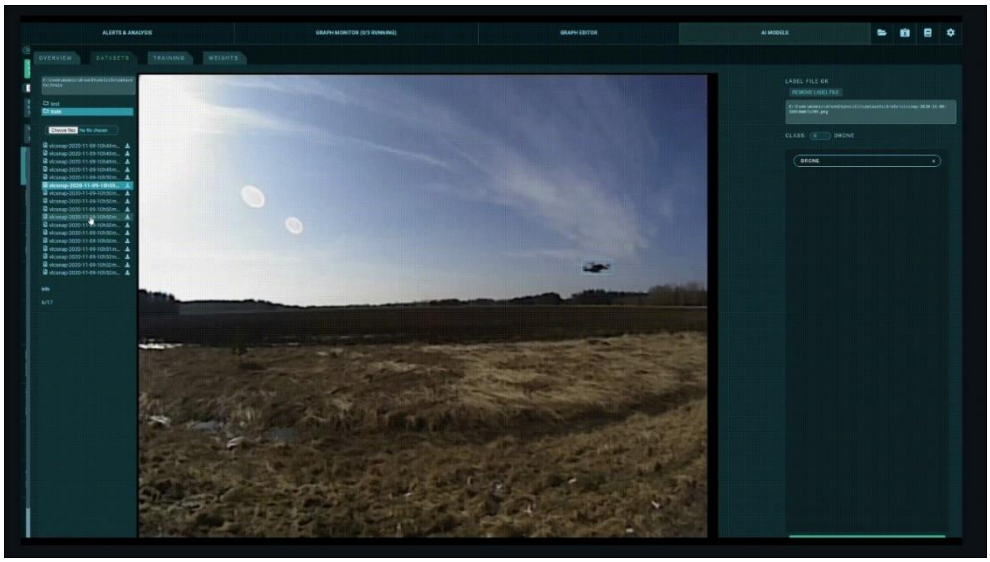


Kuva 6 MarshallAI:n ”No Code” -käyttöliittymä analyysitapahtumien konfigurointiin.

Järjestelmässä datan omistajuus riippuu siitä, millä sopimuksella järjestelmää on otettu käyttöön; esimerkiksi pelkästään asiakkaan konfiguroimissa on-prem ratkaisuissa omistajuus säilyy asiakkaalla. Toisaalta pilvilaskenta- tai palvelumallissa tapahtuvassa sovellutuksessa tilanne on monimutkaisempi ja ostajan täytyy olla tarkkana, että rekisteripitäjän velvollisuudet tulevat täytettyä. Kameroiden / sensoreiden tuottaman datan omistaa joka tapauksessa asiakas. Valmistaja näkee järjestelmän yhteensopivana EU:n tulevan tekoälyasetuksen / AI-Actin kanssa, jos asetus menee tämänhetkisessä muodossaan lävitse. Järjestelmän / analyyseihin käytettävän neuroverkon päätökset on selitettävissä erillisellä työkalulla, eli tällöin myös vaatimus selitettävyydestä täyttyy asetusta silmälläpitäen. Järjestelmää opetettaessa voidaan myös opettaa pois tiettyjä malleja, jolloin järjestelmän selitettävyys paranee entisestään. Loppukäyttäjälle kaikki analyysidata on myös luettavissa, jolloin halutessaan analyyseihin voidaan pureutua syvemminkin. Järjestelmä ei analysoi käyttäjän toimia millään tavalla automaattisesti, mutta järjestelmä voi opetustarkoituksessa nostaa tiettyjä tapahtumia ihmisen varmistettavaksi. Myöskään järjestelmän lokit eivät mene MarshallAI:n käyttöön ilman asiakkaan lupaa.

Järjestelmän analyysikyvykkyydet ovat verrattaen edistyneitä ja ulottuvat mm. liikkuvasta kuvasta Dronejen poimimiseen. Opetustapahtuma voidaan tehdä myös itsetehdyllä 3D -animaatiolla tai objektilla. Lisäksi järjestelmä

voi arvioida kuvasta objektien etäisyydet ja sijoittaa nämä suoraan kartastoon koordinaateille. Yhtenä sovellutuksena oli myös radioaaltojen tunnistus, eli esimerkiksi tietynlainen laite voidaan tunnistaa suoraan jo ennen kuva-havaintoa ja havaintoa voidaan rikastaa ääni- ja kuva-analyysillä. Periaatteellisesti minkä tahansa sensorin data vodaan integroida järjestelmään.

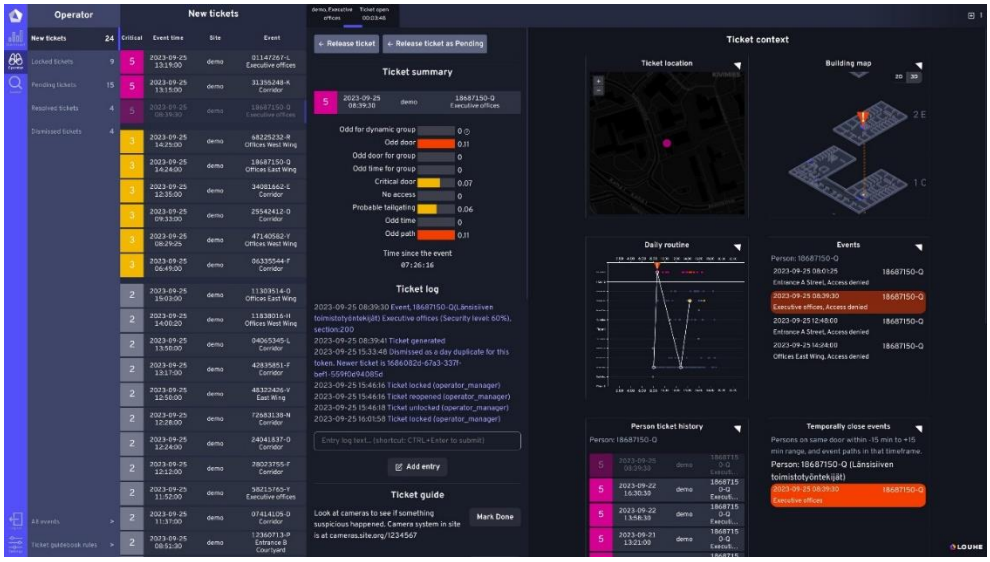


Kuva 7 MarshallAI:n käyttöliittymä ja Drone-tunnistus käytännössä.

3.5 Louhe

Louhe (ex Louhos Solutions) on suomalainen ohjelmistotalo, joka kehittää koneoppimiseen ja neuroverkkoihin perustuvaa menetelmää poikkeamien tunnistamiseen. Louheen tuotteen idea on se, että mistä tahansa suuresta datamäärästä voidaan tunnistaan ensin ”tavanomaisuus” ja sen jälkeen tunnistaa tavanomaisuudesta tapahtuvat poikkeamat. Lähestymistapa soveltuisi monelle eri toimialalle, mutta Louhe on päättänyt keskittyä nimenomaan turvallisuusalaan toistaiseksi. Louheen ydinidea perustuu siihen, että järjestelmälle ei välttämättä tarvitse ihmisvoimin kertoa sitä, mitä datasta etsitään; poikkeamat nostetaan esiin tilastollisesti ja analyyttisin menetelmin. Analyyseissä käytetään professori Kary Främlingin tutkimusdataan perustuvaa menetelmää ja INKA -neuroverkkoa (30). Nykyisellään menetelmä pyörii Louheen omilla palvelimilla.

Louheella on käytössä kaksi eri tuotetta, Detection & Response sekä Insights. Näistä ensimmäinen keskittyy neuroverkolla ja tekoälyllä tehtäviin reaaliaikaisiin analyyseihin tietystä lähteestä ja jälkimmäistä voidaan käyttää koneoppivalla menetelmällä analysoimaan tiettyä tietoaineistoa, tyypillisesti esim. X-ajalta otettua kulunvalvontajärjestelmän dataa. Kulunvalvontajärjestelmät ovatkin ihanteellisia kohteita Louheen menetelmän soveltamiseen suuren aikaleimatun datamääränsä vuoksi ja datasta voidaan tehdä havaintoja, joita ihmisoperaattori ei voisi välttämättä koskaan havaita. Tällainen havainto voi olla vaikkapa henkilön poikkeava kulkukäytös; jos henkilö normaalisti kulkee työpäivinään aina etuovelta kahvilaan ja siitä työpisteelleen, mutta yhtäkkiä onkin käynyt vaikkapa kellarin turvavyöhykkeellä sijaitsevassa turvalaitetilassa tai yrittänyt mennä toimitusjohtajan huoneeseen keskellä yötä (hyväksytyllä tai hylätyllä kululla), niin järjestelmä voi nostaa tästä esiin poikkeaman jopa reaaliajassa. Tällöin kiinteistön omistaja voi selvittää, onko henkilöllä mahdollisesti työtehtävän edellyttämiä kulkuoikeuksia laajemmat oikeudet tai onko henkilö käynyt ko. tilassa esimerkiksi rikollisessa tarkoituksessa. Insights -työkalulla yksittäisestä datasetistä voidaan tehdä vastaavia analyysejä ja voidaan kaivaa esimerkiksi kiinteistön vilkkaimmat ovet tai nostaa esiin prosentuaalisesti merkittäviä tapahtumia. Jos esimerkiksi tietyllä kulkutunnisteella (token) on vaikkapa 20% kaikista kulkutapahtumista hylättyjä, niin se voi tarkoittaa, että tunnisteen käyttäjä on yrittänyt päästä vääriin paikkoihin tai vaihtoehtoisesti henkilöllä ei ole työtehtävän edellyttämät kulkuoikeudet kunnossa. Louheen Detect & Response -sovellusta voidaan ajaa joko pilvessä tai On-Prem -ratkaisuna ja Insights on kerta-analyysityyppinen palvelu, jossa dataa ei säilötä pilveen ja laskenta tapahtuu datasetistä internetselaimessa koneoppivin menetelmin toteutettuna.

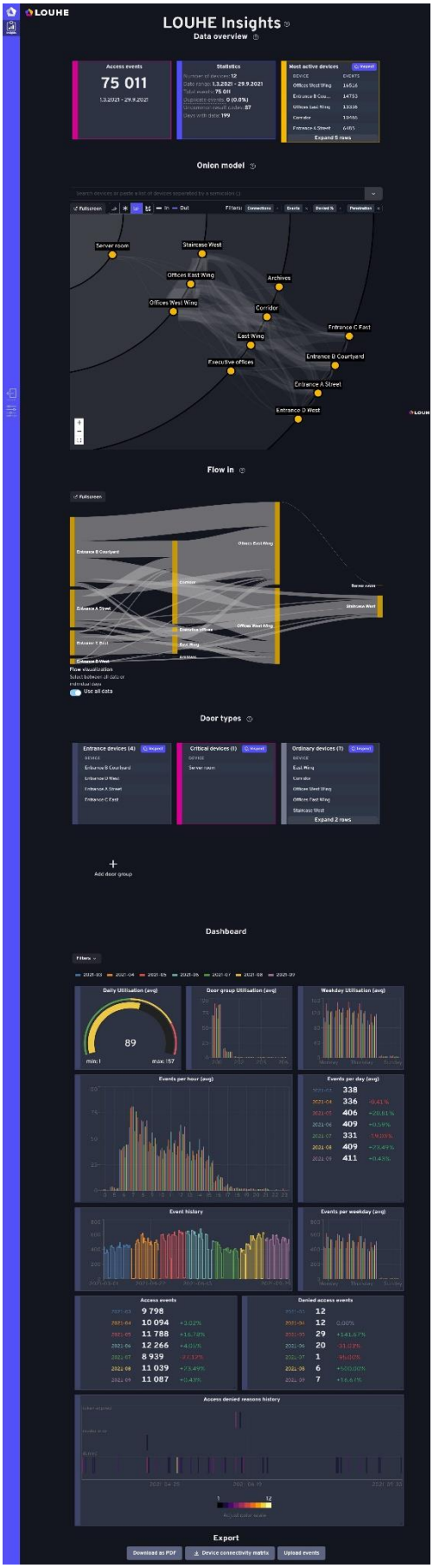


Kuva 8 Louhe Detection & Response -sovellus, jossa järjestelmä on luokitellut tietyt poikkeamat numeerisesti tärkeysjärjestykseen. Käyttäjä voi poimia tapahtumia jonosta ja käsitellä ne tikettityyppisesti.

Louheella julkisia referenssikohteita on mm. Kansaeläkelaitos (31), Yleisradio (32) ja UPM.

Louheen menetelmän kulmakivinä on läpinäkyvyys ja selitettävyys; Louhe markkinoikin itseään nimenomaan selittävän tekoälyn sovelluksena. Tältä pohjalta Louhe näkeekin mm. tulevan EU:n tekoälyasetuksen hyvänä asiana ja uskoo, että heidän tuotteensa täyttää kaikki asetuksen vaatimukset jo nykyisellään. Järjestelmä näyttää tunnistetuista poikkeamista aina syyt ja tarvittaessa päätöksiä voidaan analysoida myös kooditasolla.

Järjestelmässä datan omistajuus on aina käyttäjällä, mutta sovellutuksesta riippuen data saattaa olla säilössä myös pilvessä ainakin väliaikaisesti. Ihannetyyppisessä käyttötapauksessa sovelluksella analysoitaisiinkin esimerkiksi tiettyjä kulkutunnisteita ja tunnisteiden omistaja-data löytyisi vain toisesta järjestelmästä (kulunvalvontajärjestelmä). Tällöin Louhe ei käsittele henkilötietoja. Pilvisovelluksissa Louhe käyttää anonymisoitua datasyötettä graafeina ja matemaattisena datana menetelmän opettamiseen ja hiomiseen. On-prem asennuksissa vastaava datankeräys voidaan estää tarvittaessa. Menetelmän jatkuva opettaminen on kuitenkin tärkeää, että järjestelmä voi tunnistaa poikkeamia nyt ja tulevaisuudessa; malli on hieman sama, kuin tietoturvayhtiöillä pilvipohjaisessa virustorjunnassa.

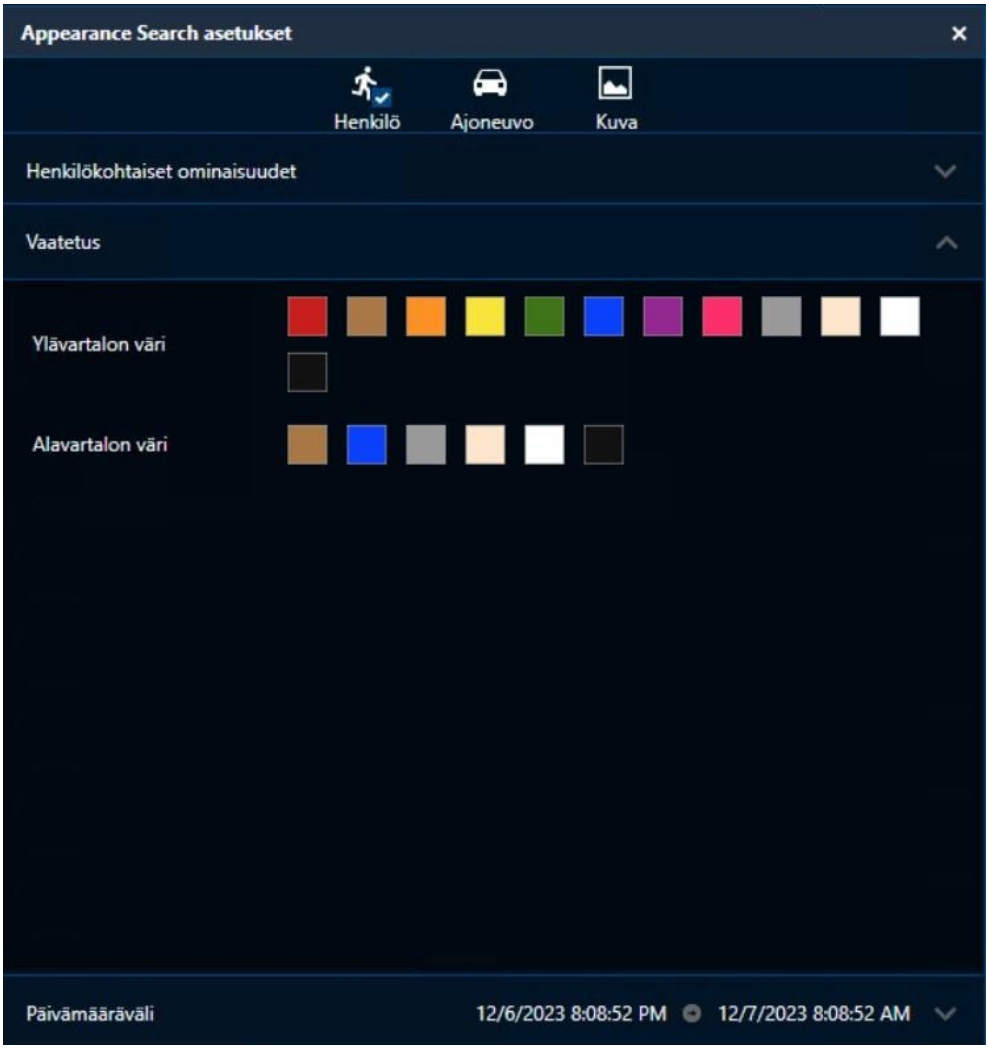


Kuva 9 Louhe Insights -sovellus, joka on olemassaolevan datasetin perusteella analysoinut kulkutapahtumien määrän ja luonut ovipäätteistä ns. sipulimallin. Järjestelmä on myös luonut graafeja valmiiksi kiinnostavista statistiikoista ja nostanut esiin kiinteistön käyttöstatistiikka datan perusteella.

3.6 Muut Sovellukset ja tuotteet

Aiemmin lueteltujen sovellusten lisäksi Suomessa on käytössä muitakin tekoälyä hyödyntäviä sovelluksia; muun muassa suomalainen Mirasys ja yhdysvaltalaisen Motorola -konsernin Avigilon. Avigilon valmistaa myös kameroita, joissa on sisäänrakennettua analytiikkaa. Avigilonin kamerat kykenevät kasvojen- ja hahmojentunnistukseen, liikesuuntien tunnistukseen, ihmislaskentaan ja moniin muihin sovellutuksiin. Suomessa on käytössä myös paljon kiinalaisia Hikvision- ja Dahua -merkkisiä kameroita ja tallentimia, joiden analytiikka-ominaisuudet ovat varsin kehittyneitä. Hikvision mainostaa kykenevänsä mm. kasvojentunnistukseen, autojen merkin, mallin ja rekisterikilventunnistukseen ja ihmislaskentaan. Tietyt toimijat myös myyvät näitä kiinalaisia kameroita uudelleenbrändättyinä oman yrityksensä logoilla. Suomessa kiinalaisten valvontatuotteiden käyttö on kuitenkin vähenemässä erinäisistä maailmanpoliittisista syistä johtuen.

Tämän otsikon 1.2.6 alla luetelluista tuotteista ei saanut valmistajan kommentteja, joten järjestelmiä käsiteltiin vain päällisin puolin julkisista lähteistä saatavilla olevilla tiedoilla. Allaoleva kuvankaappaus Avigilonista on Senaatti-kiinteistöillä käytössä olevasta järjestelmästä.



Kuva 10 Avigilonin ”Appearance Search” -näkymän konfiguraatiosivu, jossa voidaan etsiä esimerkiksi tietynvärisillä vaatteilla varustettua henkilöä tallenteista. Näkymässä voidaan etsiä myös suoraan kuvan perusteella vastaavuuksia tallenteesta aiemmilta ajankohdilla.

4 Yhteenveto ja pohdinta

Minkä tahansa turvallisuusvalvonnassa käytettävän järjestelmän käyttöönotto on Suomessa nykyään monivaiheinen prosessi. Järjestelmähankintaa tehdessä ostajan pitää etukäteen kartoittaa se, mitä järjestelmällä halutaan saavuttaa ja se, onko hankittava järjestelmä ylipäätään voimassaolevien lakien ja asetusten mukainen. Järjestelmän ostaja- tai käyttäjätaho päätyy usein järjestelmän osalta myös rekisterinpitäjäksi, jolloin etukäteen tehty selvitystyö ja dokumentointi voi vähentää tai mitigoida mahdollisesta tietosuojarikkomustilanteesta aiheutuvia seuraamuksia. Vastuuta ei voi vierittää esimerkiksi myyvälle taholle ja organisaation nimetyn tietosuojavastaavan tulee olla tehtäviensä tasalla, kun järjestelmien hankintaa ja käyttöönottoa tehdään. Toisinaan tietosuojavaltuutettu antaa huomautuksia tai jopa sakkoja, jos järjestelmän käyttöönoton aikaiset tietosuojatoimenpiteet on laiminlyöty, kuten tapahtui mm. Poliisin ClearView AI -tapauksessa (33). Yksityisistä yrityksistä poiketen tietyt viranomaiset voivat käyttää myös ominaisuuksia, jotka saattaisivat olla mahdottomia perustella viranomaiskentän ulkopuolella. Näihin kuuluu mm. kasvojentunnistus (34).

Markkina/tuotekartoitusvaiheessa järjestelmien vertailu voi olla hankalaa; monet järjestelmät markkinoivat tekoälyä usealla eri nimityksillä. Materiaaleissa ja järjestelmissä vilisee termejä kuten konenäkö, neuroverkko, koneoppiminen, algoritmit yms. ja näillä voidaan tarkoituksella saada jokin ominaisuus kuulostamaan sellaiselta, jota ei välttämättä löydy kilpailevasta järjestelmästä. Todellisuudessa kilpaileva järjestelmä voi sisältää saman ominaisuuden, jota kutsutaan vain eri termillä. Hankintavaiheessa saattaakin olla hedelmällisempää kuvata jokin tietty valvontatarve, johon tekoäly saattaisi soveltua ja lähestyä järjestelmätoimittajia skenaariopohjaisesti. Tällöin toimittaja voi tarjota kyseiseen valvontatarpeeseen soveltuvia järjestelmiä eikä ostajan tarvitse perehtyä kompleksiseen termiikkaan erikseen.

Tässä työssä tehdyn kartoituksen perusteella Suomen markkinoilta löytyy jo nyt monipuolisesti sekä kuvaa, että muuta dataa analysoivia järjestelmiä ja tuotteita. Tuotteilla on myös useita ”proof of concept” -tyyppisiä toteutuksia ja tekoälyn käytön turvallisuusvalvonnassa voidaankin sanoa olevan jo arkipäivää. Osaa tuotteista voidaan myös yhdistellä tai integroida toisiinsa ja esimerkiksi Milestone toimii tekoälykontekstissa monipuolisena integraatioalustana ns. tallenninohjelmiston kyljessä.

Paikallisvalvomokohteissa tarkkaan valvontatarpeeseen saattaa riittää yksittäinen järjestelmä tai parin järjestelmän yhdistelmä, jolloin kaikki kohteen turvallisuudesta vastaavat henkilöt voivat olla hyvin perillä järjestelmän kyvykkyyksistä ja käyttötavoista. Useimmiten näissä kohteissa turvallisuushenkilöstö on myös perehdytetty järjestelmän käyttöön laajasti ja järjestelmälle löytyy nimetty pääkäyttäjä, joka tuntee järjestelmän konfiguraatiot. Näissä tapauksissa kyseinen kohdetoteutus on useimmiten sidottu tiettyyn teknologiaan tai teknologioihin ja samaa järjestelmää ylläpidetään, huolletaan ja mahdollisesti laajennetaan sen elinkaaren loppuun saakka kyseisen kohteen sisällä.

Hälytyskeskuskontekstissa tai niin sanotuissa useiden kohteiden valvomoissa tilanne on monimutkaisempi; useimmiten tuotettu palvelu haluttaisiin konseptoida ainakin suurilta osin, että järjestelmien operaattorilla on mahdollisuus saavuttaa riittävä osaaminen järjestelmän käyttöön. Jos esimerkiksi isomman organisaation useiden toimipaikkojen keskitetty valvomo käyttäisi kaikkia tässä työssä mainittuja järjestelmiä samaan aikaan eri sijaintien valvontaan, niin valvomon operaattoreilla ei todennäköisesti olisi mahdollisuutta saavuttaa sellaista perehtyneisyyden tasoa järjestelmien käytössä, että kaikkia ominaisuuksia voitaisi käyttää tehokkaasti. Näissä käyttötapauksissa onkin tärkeää keskittyä löytämään tuote, joka palvelee valvomon tai hälytyskeskuksen tuottamaa konseptia. Esimerkiksi Securitas on jo toteuttanut Axiksen tuotteilla tapahtuvaa kuva-analyysiin perustuvaa valvontaa, jossa hälytyskeskus reagoi hälytyksiin ensisijaisesti etäkaiuttimella annettavilla komennoilla (35).

Senaatti-Kiinteistöjen tapauksessa Senaatin turvallisuuspalvelukeskus tuottaa saman katon alta sekä hälytyskeskus-, että pääkäyttöpalveluita erilaisiin turvateknisiin laitteistoihin. Samat henkilöt tuottavat molempia palveluita ja operaattoreiden osaamisvaatimukset määräytyvät valtion kiinteistöihin ajan

saatossa hankitun laitekannan pohjalta, joka on hyvinkin kirjava; täten Senaatilla turvallisuusvalvojana toimivalla henkilöllä on usein jo hyvä perusosaaminen kymmeniin eri turvateknisiin järjestelmiin. Tällaisessa konseptissa voitaisiin käyttää tässä työssä esiteltyjä tekoälypohjaisia järjestelmiä rikastamaan nykyistä valvontaa tai nostamaan esiin sellaisia poikkeamia, joita ei voisi havainnoida kohtuullisella ihmisresurssilla. Esimerkiksi hälytyskuvavalvontapalvelussa voitaisiin käyttää kamera-analytiikkaa nostamaan edistyneitä hälytyksiä aluevalvonnasta ja täten puuttua jo ennakoivasti murtoihin ennen kuin omaisuusvahinkoja syntyy. Näin myös paikallisvartijan vasteaika kohteelle saapumiseen pienenisi, kun vartijan tilaus voidaan tehdä ennakoivasti heti ensihavainnosta analytiikalla. Senaatti tuottaa turvallisuustekniikkaa myös turvallisuusviranomaisille, joilla voi olla omia sovellutuksia tekoälyn käytölle turvallisuusvalvonnassa. Senaatin turvallisuuspalvelukeskus voisi myös tuottaa palveluna sisäistä turvallisuutta nostamalla poikkeamia esimerkiksi kulunvalvontajärjestelmien datasta valtakunnallisesti. Haasteina tekoälyn käytössä palveluntuotannossa on kuitenkin eri järjestelmien keskinäiset vaatimukset; kaikkea ei voi integroida keskenään ja tiettyjen ominaisuuksien saamiseksi pitäisi kohteisiin asentaa vain tietynmerkkisiä- tai mallisia turvallisuusteknisiä laitteita. Senaatin turvallisuusteknologian tuotepäällikkö Pasi Pyykkinen listaa toimittajariippumattomuuden(36) yhdeksi Senaatin kulmakivistä turvallisuusteknisissä hankinnoissa, joten tietyt yksittäiset teknologiat eivät voi sanella valtiotasolla turvateknisten laitteiden hankintaa ja laitekantaa. Lisäksi valtion hankintoja sitoo Hankintalaki (37), joka taas pakottaa kilpailuttamaan hankinnat kustannustehokkaasti sekä tasapuolisesti ja siten ei myöskään mahdollista tietyn ominaisuuden priorisoimista kovinkaan tarkasti järjestelmähankinnoissa. Tekoälyn käyttöä turvallisuusvalvonnassa kuitenkin selvitetään jatkuvasti ja erilaisia konsepteja testataan ahkerasti. Näiden tuotteistaminen kustannustehokkaasti ja toimittajariippumattomasti osaksi jokapäiväistä Senaatin tuottamaa hälytyskeskus- ja etäkäyttöpalvelua on kuitenkin haasteellista.

5 Lähdeluettelo

1. https://www.europarl.europa.eu/news/fi/headlines/society/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan#

2. https://www.elementsofai.com/fi

3. https://libguides.kamk.fi/c.php?g=712843

4. https://erepo.uef.fi/bitstream/handle/123456789/25801/urn_nbn_fi_uef-20211122.pdf?sequence=1&isAllowed=y

5. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

6. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

7. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

8. https://tietosuoja.fi/arvioi-riskit

9. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

10. https://tietosuoja.fi/henkilotietojen-kasittely

11. https://tietosuoja.fi/kasittelyperusteet

12. https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely

13. https://tietosuoja.fi/tietosuojaperiaatteet

14. https://tietosuoja.fi/osoitusvelvollisuus

15. https://www.finlex.fi/fi/laki/alkup/1999/19990523

16. https://tietosuoja.fi/rekisteroidyn-oikeudet

17. https://tietosuoja.fi/oikeus-saada-tutustua-tietoihin

18. https://tietosuoja.fi/tietoturvaloukkaukset

19. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L5

20. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L7P21

21. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fi_0.pdf

22. https://www.cve.org/About/Overview

23. https://www.milestonesys.com/partners/technology-partners/technology-partner-finder/

24. https://www.youtube.com/user/BoschSecurity

25. https://www.axis.com/solutions

26. https://www.axis.com/products/analytics

27. https://www.youtube.com/@AxisCommunications/videos

28. https://developer.nvidia.com/blog/metropolis-spotlight-marshallai-optimizes-traffic-management-while-reducing-carbon-emissions/

29. https://marshallai.com/news/marshallai-pilots-groundbreaking-automatic-border-control/

30. https://github.com/KaryFramling/inka

31. https://louhe.fi/fi/reference/kela-ja-louhe-oy-yhteistyohon

32. https://louhe.fi/fi/reference/yleisradio-kehittaa-turvallisuuttaan-louhe-oyn-kanssa

33. https://yle.fi/a/3-12118726

34. https://yle.fi/a/3-10815487

35. https://www.axis.com/customer-story/kreate-securitas-construction-perimeter

36. Sähkömaailma numero 1-2 30.1.2024

37. https://www.finlex.fi/fi/laki/alkup/2016/20161397