Tekoäly yritysturvallisuuden kehittämisen työkaluna

21.4.2026

Yritysturvallisuuden toimintaympäristö on viime vuosina muuttunut nopeasti. Digitalisaation, etätyön, pilvipalvelujen ja globaalien toimitusketjujen myötä yrityksiin kohdistuvat riskit ovat monipuolistuneet ja muuttuneet aiempaa vaikeammin havaittaviksi. Perinteiset turvallisuuskäytännöt eivät enää yksin riitä, vaan niiden rinnalle tarvitaan uusia, dataan perustuvia lähestymistapoja. Tekoäly (AI) on noussut keskeiseksi teknologiaksi, joka tarjoaa merkittäviä mahdollisuuksia yritysturvallisuuden kehittämiseen niin operatiivisella kuin strategisella tasolla.

Uhkien tunnistaminen ja ennakointi tekoälyn avulla

Yksi keskeisimmistä tekoälyn sovellusalueista yritysturvallisuudessa on uhkien ja poikkeamien tunnistaminen. Koneoppimiseen perustuvat järjestelmät kykenevät analysoimaan suuria tietomassoja ja havaitsemaan normaalista toiminnasta poikkeavia ilmiöitä, joita inhimillinen tarkastelu ei välttämättä tunnista ajoissa. Käyttäytymiseen perustuva analytiikka (User and Entity Behavior Analytics, UEBA) oppii organisaation normaalit toimintamallit ja tunnistaa poikkeamia, kuten epätavalliset kirjautumisajat, poikkeavat sijainnit tai normaalista poikkeavan tiedonsiirron.

Näiden havaintojen avulla voidaan tunnistaa esimerkiksi varastettujen käyttäjätunnusten käyttö, sisäpiiririskit tai tietomurtoyritykset jo varhaisessa vaiheessa. Kansainvälisten selvitysten mukaan tekoälyavusteinen uhkien tunnistaminen lyhentää merkittävästi havaintoaikoja ja tehostaa reagointia verrattuna perinteisiin

sääntöpohjaisiin ratkaisuihin (IBM, 2026; Fortinet, 2025).

Fyysinen turvallisuus ja ajantasainen tilannekuva

Tekoälyn hyödyntäminen ei rajoitu kyberturvallisuuteen, vaan se tukee yhä vahvemmin myös fyysistä turvallisuutta. Älykäs videoanalytiikka perustuu kuvantunnistukseen ja syväoppimiseen ja mahdollistaa poikkeavan toiminnan tunnistamisen esimerkiksi tuotanto-, varasto- ja logistiikka-alueilla. Järjestelmät voivat havaita luvattoman liikkumisen rajatuilla alueilla, poikkeavat kulkureitit tai mahdolliset tapaturmatilanteet.

Yritysturvallisuuden kannalta keskeinen hyöty on kokonaisvaltaisen tilannekuvan muodostaminen. Kun kameradata, kulunvalvontatiedot ja IoT-laitteiden tuottama informaatio yhdistetään tekoälyn avulla, turvallisuushenkilöstö saa ajantasaista ja jalostettua tietoa päätöksenteon tueksi. Valvonta perustuu poikkeamien tunnistamiseen jatkuvan tarkkailun sijaan, mikä parantaa reagointikykyä ja tehostaa resurssien käyttöä.

Turvallisuustoiminnan tehostaminen ja automaatio

Monissa organisaatioissa turvallisuustyötä kuormittaa hälytysten suuri määrä. Tekoälyä hyödynnetään yhä enemmän hälytysten suodattamiseen, ryhmittelyyn ja priorisointiin. Tekoälypohjaiset järjestelmät tunnistavat vähäriskiset ilmoitukset, yhdistävät samankaltaiset tapahtumat ja nostavat kriittisimmät tapaukset asiantuntijoiden käsiteltäviksi.

Lisäksi tekoäly voi käynnistää automaattisia toimenpiteitä, kuten käyttäjätunnusten tilapäisen lukitsemisen, epäilyttävän verkkoliikenteen rajaamisen tai lisävalvonnan aktivoimisen. Näin asiantuntijoiden työpanos kohdistuu rutiinitehtävien sijaan vaativaan analyysiin ja päätöksentekoon.

Sosiaalisen manipuloinnin torjunta

Sosiaalinen manipulointi, kuten tietojenkalastelu ja yrityksiin kohdistuvat huijausyritykset, on merkittävä yritysturvallisuusriski. Tekoälyä hyödynnetään sähköpostien ja muun viestinnän analysoinnissa, jossa se tunnistaa poikkeavaa kielenkäyttöä, epätavallisia maksupyyntöjä ja haitallisia liitteitä.

Kehittyneemmät ratkaisut kykenevät tunnistamaan myös tekoälyn tuottamaa huijaussisältöä, kuten deepfake-ääni- tai videoviestejä, jotka kohdistuvat erityisesti yritysjohdon ja taloushallinnon päätöksentekoon. Tekoäly toimii siten vastavoimana teknologialle, jota rikolliset hyödyntävät yhä kehittyneemmin.

Strateginen näkökulma ja riskienhallinta

Strategisella tasolla tekoäly tukee ennakoivaa riskienhallintaa. Se kykenee analysoimaan samanaikaisesti toimintaympäristön muutoksia, toimitusketjujen häiriöitä, taloudellisia indikaattoreita ja geopoliittisia tapahtumia. Näiden analyysien avulla johto saa paremman kokonaiskuvan organisaation haavoittuvuuksista ja voi perustaa päätöksensä aiempaa täsmällisempään tilannearvioon. Tekoäly ei korvaa johtamista, mutta se parantaa päätöksenteon tietopohjaa ja tukee strategista varautumista.

Tekoälyn käyttöön liittyvät riskit

Tekoälyyn liittyy myös uusia turvallisuusriskejä. Järjestelmät voivat olla alttiita esimerkiksi koulutusdatan manipuloinnille, mikä voi johtaa virheellisiin tai harhaanjohtaviin tuloksiin. Lisäksi tekoälyä voidaan hyödyntää itse hyökkäystoiminnassa.

Euroopan unionin kyberturvallisuusvirasto ENISA korostaa, että tekoälyn turvallinen käyttöönotto edellyttää koko elinkaaren kattavaa lähestymistapaa, jossa tietoturva, vastuunjako ja jatkuva valvonta huomioidaan jo suunnitteluvaiheessa (ENISA, 2025). Myös NIST painottaa tekoälyn kytkemistä osaksi olemassa olevia riskienhallinta- ja turvallisuusprosesseja (NIST, 2025).

Yhteenveto

Tekoäly on vakiinnuttamassa asemansa yritysturvallisuuden keskeisenä kehittämisvälineenä. Se mahdollistaa aiempaa tehokkaamman uhkien tunnistamisen, tilannekuvan muodostamisen ja riskien ennakoinnin. Samalla tekoälyn hyödyntäminen edellyttää suunnitelmallista hallintaa, osaamisen kehittämistä ja vastuullista turvallisuusjohtamista. Yritykset, jotka yhdistävät teknologian, prosessit ja ihmiset, vahvistavat sekä turvallisuuttaan että liiketoiminnan jatkuvuutta.

Beata Taijala
ins., KTL, Sertifioitu Projektiosaaja (IPMA Level D)
SEAMK

Kirjoittaja on turvallisuusjohtamisen opettaja, joka toimii asiantuntijana vAI:lla tuottavuutta -hankkeessa. Hankkeen yhtenä tavoitteena on herättää alueen toimijoissa tietoisuus ja kyvykkyys hyödyntää tekoälyteknologiaa tuottavuuden parantamiseksi.

vAI:lla tuottavuutta? -hanke on Euroopan unionin osarahoittama. Lisää tietoa hankkeesta löydät hankkeen verkkosivuilta: vAI:lla tuottavuutta?

Lähteet

ENISA. (2025). *ENISA AI Threat Landscape 2025*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/artificial-intelligence-and-next-gen-technologies

Fortinet. (2025). *Artificial intelligence in cybersecurity*. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

IBM. (2026). *AI cybersecurity solutions*. https://www.ibm.com/solutions/ai-cybersecurity

NIST. (2025). *Draft NIST guidelines rethink cybersecurity for the AI era*. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2025/12/draft-nist-guidelines-rethink-cybersecurity-ai-era