Tekoäly kyberuhkien tunnistamisessa

Ville Pulkkinen

2024 Laurea

Laurea-ammattikorkeakoulu

Tekoäly kyberuhkien tunnistamisessa

Ville Pulkkinen

Liiketalous

Opinnäytetyö

Joulukuu 2024

Laurea-ammattikorkeakoulu **Tiivistelmä**
Liiketalouden koulutus
Tradenomi (AMK)

Ville Pulkkinen
Tekoäly kyberuhkien tunnistamisessa
Vuosi 2024 Sivumäärä 37

Tämän opinnäytetyön tavoitteena on tehdä selkokielinen ja helposti ymmärrettävä analyysi siitä, kuinka tekoälyä hyödynnetään kyberhyökkäysten tunnistamisessa. Tavoitteena on, että lukija ymmärtää työn sisällön ilman aiempaa kokemusta tai ymmärrystä aiheesta. Työn tarkoitus on analysoida eri tapoja, miten tekoälyä voitaisiin hyödyntää kyberuhkien tunnistamisessa. Työssä käydään läpi missä ja miten tekoälyä voidaan hyödyntää. Työn loppupuolella kootaan yhteen sen tuomia hyötyjä, haasteita sekä tehdään lyhyt katsaus sen tulevaisuuteen.

Työn menetelmänä käytetään kirjallisten lähteiden analysointia. Työn tietoperustana toimii alan yritysten tuottama sisältö kuten artikkelit aiheesta. Niiden avulla pyritään takaamaan tiedon laatu, ajankohtaisuus sekä luotettavuus.

Tuloksista voidaan sanoa, että tekoäly omaa merkittävän potentiaalin uhkien tunnistuksen osalta. Se voi tuoda tunnistusprosessiin nopeutta ja tehokkuutta mihin ihmisen voi olla haastava vastata. Se tuo kuitenkin mukanaan haasteita, jotka tulee ratkaista ensin ennen kuin tekoälyä voitaisiin ottaa laajemmin käyttöön kyberuhkien tunnistamisessa. Tämän vuoksi iso osa sen tuomista hyödyistä on toistaiseksi vielä tulevaisuudessa ja nähtäväksi jää miten isoon rooliin tekoäly nousee.

Asiasanat: kyberturvallisuus, kyberuhka, tekoäly

Laurea University of Applied Sciences
Degree Programme in Business Administration
Bachelor of Business Administration (BBA)

Ville Pulkkinen

Artificial intelligence in identifying cyber threats

Year 2024 Pages 37

Abstract

The objective of this thesis is to provide a plain-language and easily understandable analysis of how artificial intelligence is utilized in identifying cyberattacks. The aim is for readers to understand the content without prior experience or knowledge of the subject. The purpose of the thesis is to analyse various ways AI can be used in detecting cyber threats. The study explores where and how AI can be utilized. Toward the end of the thesis, the benefits and challenges of AI in this context are summarized, along with a brief outlook on its future.

The method used in this thesis is the analysis of written sources. The knowledge base is built on content produced by companies in the field, such as articles on the subject. This approach aims to ensure the quality, timeliness, and reliability of the information.

The findings indicate that AI holds significant potential in threat detection. It can enhance the speed and efficiency of detection processes, surpassing what humans can typically achieve. However, AI also introduces challenges that must be addressed before it can be widely adopted in cyber threat detection. As a result, many of its benefits remain in the future, leaving the ultimate role of AI in this field to be determined.

Keywords: artificial intelligence, cybersecurity, cyber threat

Sisällys

1 Johdanto

Tekoäly on muuttanut maailmaa ja samalla myös kyberturvallisuutta. Se tuo uusia mahdollisuuksia niin kyberhyökkäyksien torjuntaan kuin hyökkäysten toteuttamiseen. Hyökkäykset ovat ja tulevat olemaan entistä tehokkaampia, automatisoidumpia sekä kohdennetumpia (Huoltovarmuuskeskus 2022). Hyökkäykset kehittyvät jatkuvasti ja tämän vuoksi on tärkeää ymmärtää tekoälyn tuomat mahdollisuudet näiden kehittyneempien hyökkäyksien torjumiseksi. Perinteiset kyberturvaohjelmistot eivät tule yksinään riittämään. Tekoäly on tullut jäädäkseen.

Opinnäytetyön aiheena on tekoäly kyberhyökkäyksien tunnistamisessa. Työn tarkoituksena on analysoida eri tapoja, miten tekoälyä on hyödynnetty kyberhyökkäysten ja uhkien havaitsemisessa. Työn aihe on valikoitunut tekoälysovellusten edistyneisyyden perusteella. Uhkien havaitsemisessa tekoäly sovellukset ovat työn teko hetkellä yksi edistyneimpiä osa-alueita. (Marchal, Nawrotek & WithSecure 2024, 15.)

Työn tavoitteena on tehdä selkokielinen ja helposti ymmärrettävä analyysi siitä, kuinka tekoälyä hyödynnetään kyberhyökkäysten havaitsemisessa. Tavoitteena on, että lukija ymmärtää työn sisällön ilman aiempaa kokemusta tai ymmärrystä aiheesta. Opinnäytetyön menetelmä on kirjallisten lähteiden analysointi. Työn laadun kannalta lähteiden tulee olla luotettavia/laadukkaita sekä ajankohtaisia. Kyberturvallisuus muuttuu jatkuvasti, joten luotettavat lähteet sekä niiden ajankohtaisuus nousevat tärkeään rooliin. Pyrin työssä valitsemaan ja käyttämään lähteitä alan yrityksien sivuilta, jotta tieto on laadukasta sekä luotettavaa. Jos lähde on liian vanha en voi käyttää sitä työssä. Kyberturvallisuus ja digimaailma muutenkin kehittyy niin nopeasti, että muutaman vuoden vanha artikkeli ei välttämättä pidä enää täysin paikkaansa.

Työ jaetaan muutamaan eri kokonaisuuteen. Alkuun käydään läpi tekoälyä yleisellä tasolla. Siitä siirrytään kyberturvallisuuden ja yleisimpien hyökkäyksien pariin, jotta saamme paremman ymmärryksen kyberturvallisuuden perusteista sekä tämän hetken tyypillisimmistä uhista, joilta puolustaudumme. Kun aihe on pohjustettu, siirrymme työn pääosa-alueeseen eli kyberhyökkäysten tunnistamiseen tekoälyn avulla. Pääosa-alueen olen jakanut useampaan pienempään osuuteen työn selkeyden kannalta. Lopuksi käydään läpi vielä johtopäätökset ja omaa pohdintaa aiheeseen liittyen.

2 Tekoäly

Vaikka tekoäly on tullut vasta viime vuosien aikana ison yleisön tietoisuuteen ja käyttöön, se on konseptina ollut jo pitkään käytössä. Se on saanut alkunsa jo 1950-luvulla Alan Turingin julkaisemasta artikkelista, jossa hän ehdotti, että testataan, voidaanko tietokone lukea älykkääksi. Turingin testissä on kaksi huonetta. Toisessa on ihminen ja toisessa kone. Molemmilta kysytään kysymyksiä, joihin ihmisen pystyy vastaamaan, liittyen esimerkiksi tunteisiin ja kokemuksiin. Testi ei kuitenkaan kerro onko koneella kykyä ihmisen älykkyyteen ja ymmärrykseen, lähinnä kykyä vastata kysymykseen kuten ihminen. Testiä ja sen läpäisemistä on kuitenkin pidetty askeleena kohti tekoälyä. (Whitfield 2023.) Tekoälyn kehitys lähti kovaan nousuun, kunnes tietokoneiden kapasiteetti tiedon säilyttämiseen sekä prosessointiin tuli vastaan. (ISO 2024.) Tämän seurauksena mielenkiinto ja rahoitus heikkenivät johtaen tekoälyn kehityksen seisahtamiseen. Vasta 1980-luvun puolivälissä kiinnostus tekoälyyn heräsi uudelleen tehokkaampien tietokoneiden saapuessa. Tätä seurasi kuitenkin uudet vaikeudet, jotka jatkuivat pitkälle 1990-luvulle saakka. Uudet innovaatiot prosessointi tehoon sekä edistyneet syväoppimistekniikat lopulta auttoivat tekoälyn kehitystä kohti sen nykyistä tasoa. (Builtin 2024.)

Tekoälyllä tarkoitetaan tietokonejärjestelmiä, jotka kykenevät tekemään tehtäviä mitkä ovat yleensä yhdistetty ihmisen älykkyyteen ja taitoihin. Tällaisia tehtäviä ovat esimerkiksi asioiden ja esineiden tunnistaminen sekä luontevan tekstin tuottaminen. Tekoälyn opettamisen tavoitteena onkin se, että se ajattelisi kuin ihminen. (Builtin 2024.) Kaikessa yksinkertaisuudessaan tekoäly analysoi dataa, muodostaa siitä malleja ja tekee niiden pohjalta ennustuksia ja päätöksiä (ISO 2024).

Sen avulla pystytäänkin automatisoimaan ja tehostamaan useita eri työtehtäviä, useilla eri aloilla. Tekoälykään ei pysty kaikkeen, mutta se kehittyy jatkuvasti ja pystyy ratkaisemaan yhä haastavampia tehtäviä.

Tekoäly on saanut valtavan suosion viimeisten vuosien aikana muun muassa erilaisten chatbottien avulla, jotka voivat auttaa esimerkiksi tuottamaan tekstiä sekä koodaamaan. Tällainen chatbotti on esimerkiksi ChatGPT. Tekoälyn tulevaisuus tuo mukanaan paljon uusia mahdollisuuksia monella alalla. Se voi auttaa esimerkiksi töiden automatisoinnissa sekä ongelmanratkaisussa (Builtin 2024).

Vaikka tekoäly tuo paljon uusia mahdollisuuksia, se tuo mukanaan myös potentiaalisia haittoja. Yksi tekoälyn käytön lisääntymisen tuoma pelko on työpaikkojen menetys. Ihmiset pelkäävät tekoälyn vievän heidän työpaikkansa, koska se pystyy tekemään työtehtäviä huomattavasti tehokkaammin kuin tavallinen työntekijä. Tekoäly kykenee jo nyt niin moneen eri tehtävään, että tämä huoli on aito ja otettava huomioon. Tämän lisäksi disinformaation levittäminen tekoälyä hyödyntäen on herättänyt huolta (Builtin 2024). Informaatiovaikuttaminen tulee

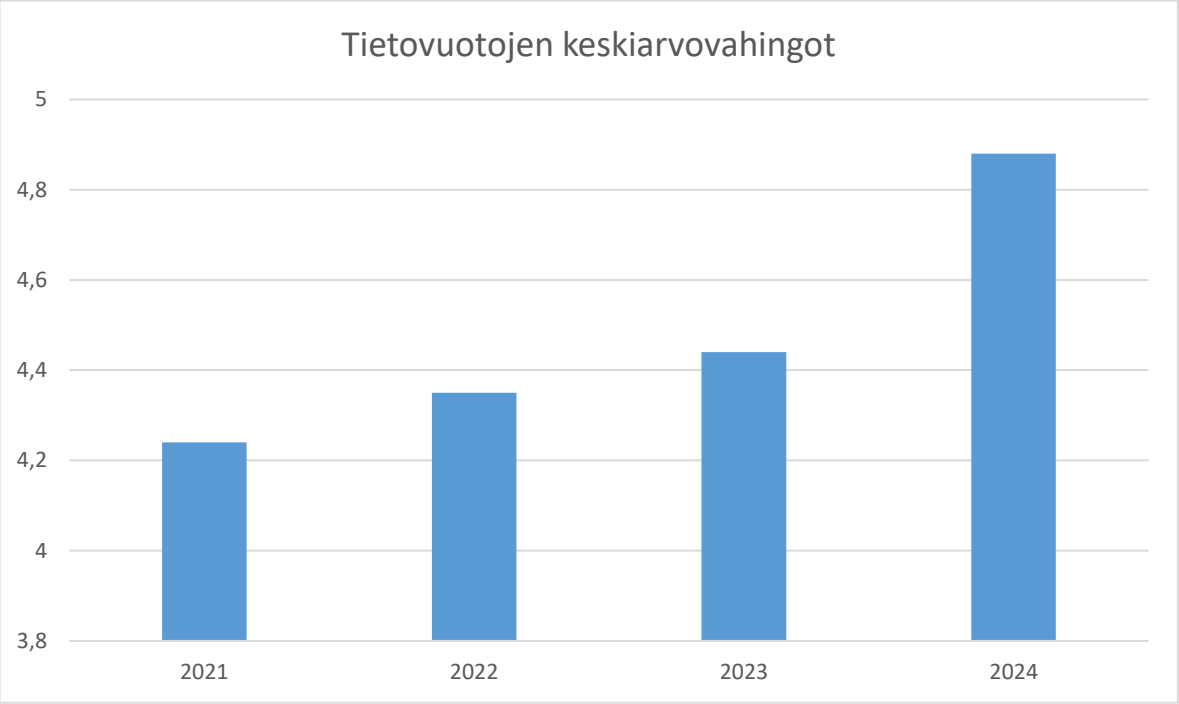
lisääntymään entisestään tekoälyn avulla sekä disinformaation tunnistaminen vaikeutuu entisestään sen myötä. Näiden asioiden vuoksi on erittäin tärkeää, että tekoälyä kehitetään ja käytetään vastuullisesti (ISO 2024).

3 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan teknologioita, toimintatapoja ja säädöksiä, joilla pyritään estämään kyberhyökkäyksiä tapahtumasta. Ja jos sellainen pääsee tapahtumaan, kyberturvallisuuden toinen tarkoitus on pyrkiä minimoimaan hyökkäyksen vaikutukset organisaatioon. Kyberturva suojaa mm. laitteita, sovelluksia sekä dataa. (Kosinski & Lindemulder 2024.) Kyberturvallisuus on ollut aina tärkeää, mutta sen tärkeys korostuu entisestään laitteiden määrän sekä hyökkääjien kekseliäisyyden takia (Cisco 2024a). Hyökkäykset ovat jatkuvasti kehittyneempiä, mikä tekee niiltä puolustautumiselta haastavampaa.

Tehokkaan kyberturvan rakentamiseen vaaditaan, että kaikki osa-alueet ovat kunnossa. Teknologian ja prosessien on palveltava toisiaan, jotta saadaan aikaan tehokas ja laadukas puolustus kyberhyökkäyksiltä (Cisco 2024a). Unohtamatta henkilökunnan kouluttamisen tärkeyttä. Teknologia menettää osittain merkityksensä, jos yrityksen henkilökuntaa ei ole koulutettu.

Kyberturvallisuuden tärkeyttä ei voi korostaa tarpeeksi. Kyberhyökkäys voi johtaa identiteettivarkauksiin, arkaluontoisen tiedon menetykseen ja moneen muuhun yrityksille ja yksilöille tärkeän asian vaarantumiseen. Yhden arvion mukaan kyberrikollisuus voi johtaa jopa 10.5 triljoonan dollarin vahinkoihin vuodessa. (Kosinski & Lindemulder 2024.) Seuraava Kuvio 1 korostaa entisestään kyberturvallisuuden tärkeyttä tietovuotojen tuomien keskiarvovahinkojen muodossa. Kuviossa 1 tiedot on esitetty miljoonissa dollareissa.



Kuvio 1: Tietovuotojen keskiarvovahingot (tiedot: IBM 2021; 2022; 2024)

Tämän opinnäytetyön kannalta on myös hyvä ymmärtää tietoturvan ja kyberturvan ero. Nämä kaksi termiä sekoittuvat keskenään helposti ja niitä saatetaan käyttää myös synonyymeinä toisilleen. Kyberturvallisuus keskittyy järjestelmien ja laitteiden turvallisuuteen, kun taas tietoturva kattaa laajemman kokonaisuuden. Tietoturvaan kuuluu esimerkiksi tiedon fyysinen suojaaminen digimaailman ulkopuolella, jota ei lueta kyberturvallisuuden osa-alueeksi. Kyberturvallisuus on siis käytännössä osa tietoturvallisuutta. Tietoturvaan voidaan liittää vain useampia asioita kuin kyberturvaan, kattaen tiedon turvaamisen laajemmin. (F-Secure 2024.)

Kyberhyökkäyksiä tehdään joka päivä ja niiden määrä on vain kasvanut viime vuosien aikana (Cisco 2024b). Kyberhyökkäys on yksinkertaisuudessaan yritys päästä käsiksi erilaisiin tietokonejärjestelmiin ja varastaa, tuhota tai muokata siellä olevia tietoja. Tavoitteita voi olla monia. Kyberhyökkäyksien tekemisen motiiveja voi olla myös useita. Hyökkäyksellä voi olla poliittisia tavoitteita ja silloin kohteena voi olla esimerkiksi erilaiset valtiolliset kohteet. Muita motiiveja ovat rikollisuus ja jopa henkilökohtaiset syyt. (Microsoft 2024a.)

Yleisimpiä uhkia ja hyökkäysmuotoja ovat muun muassa erilaiset kiristysohjelmat. Niiden avulla hyökkääjä voi lukita laitteita tai tiedostoja ja vaatia lunnaita niiden avaamista vastaan. Muita yleisiä hyökkäyksiä ovat haittaohjelmat, palvelunestohyökkäykset sekä vakoiluohjelmat. Sekä monelle tuttu smishing eli tekstiviestihuijaukset. Viestissä voidaan esimerkiksi pyytää yrityksien nimissä tekemään jotain kiireellisesti ja sitä kautta saadaan kohde painamaan haitallista linkkiä. (F-Secure 2024.)

Hyökkäyksiä on siis monia ja myös tavallisten ihmisten on hyvä hahmottaa hieman yleisimpiä kyberuhkia, jotta niiltä voidaan suojautua paremmin. Esimerkiksi tekstiviestihuijaukset tunnistetaan helpommin, jos ihminen on niistä tietoinen.

Kyberhyökkäyksiltä puolustautuminen vaikeutuu edistyneempien hyökkäyksien saapuessa. Hyökkäyksiä toteutetaan tekoälyn voimin, joka tuo tehokkuutta ja tarkkuutta hyökkäyksiin. Useilta uhilta voidaan kuitenkin välttyä oikeilla toimilla. Virussuoja tai antivirusohjelmat toimivat hyvin muun muassa troijalaisten sekä muiden haittaohjelmien havaitsemisessa. Näiden ohjelmien ohella ne on hyvä pitää ajan tasalla. Hakkerit pystyvät löytämään ja osaavat hyödyntää vanhoja versioita ohjelmista, mitkä saattavat sisältää tietoturva aukkoja. Päivityksillä takaat mahdollisimman turvallisen käytön. On myös hyvä hyödyntää kaksivaiheista tunnistautumista sekä käyttää vahvoja salasanoja. (F-Secure 2024.)

Etenkin yrityksissä tietoturvan kannalta on erittäin tärkeää kouluttaa henkilökuntaa jatkuvasti. Hyökkäykset voivat alkaa esimerkiksi siitä, että työntekijä avaa hämärän linkin, mikä on tullut hänen sähköpostiinsa. Koulutettu henkilökunta vahvistaa tietoturvaa ja ymmärtää seuraukset ja toimenpiteet, jos tietomurto pääsee sattumaan. (Microsoft 2024a.)

4 Tekoäly kyberturvallisuudessa

Tekoälystä on tullut viime vuosien aikana pysyvä osa kyberturvallisuutta. Tekoäly pystyy analysoimaan tapahtumia ja kyberuhkia ja sitä kautta avustamaan ammattilaisia työssään. Kyberhyökkäyksen täyttäessä tietyt kriteerit, tekoälyn avulla voidaan automatisoida vastaus siihen. (Microsoft 2024b.)

Tekoäly kykenee tukemaan kyberturvallisuus ammattilaisia analysoimalla valtavia määriä dataa useista eri lähteistä ja muodostaa niistä erilaisia malleja minkä pohjalta se tekee ratkaisuja. Data voi olla esimerkiksi mistä ja milloin ihmiset kirjautuvat sisään järjestelmiin sekä mitä laitteita ja pilvisovelluksia työntekijät käyttävät. Tämän datan ja mallien pohjalta tekoäly tunnistaa poikkeavuuksia tietoliikenteessä ja voi havaita kyberhyökkäyksen. (Microsoft 2024b).

Tekoälyn tuominen kyberturvaan ei välttämättä vie työpaikkoja vaan tukee ammattilaisia töissään. Työntekijät pysyvät edelleen tärkeässä roolissa, tekoäly vain tukee heidän toimintaansa. Tekoälyllä voi olla useita eri käyttötarkoituksia. Se voi olla apuna esimerkiksi pääsyn hallinnassa. Se tunnistaa käyttäytymismallien avulla poikkeavaa toimintaa ja voi esimerkiksi pakottaa salasanan vaihtoja, jos ennalta asetetut ehdot täyttyvät ja tekoäly kokee sen silloin

tarpeelliseksi. Tekoälystä voi olla apua myös uhkien tunnistamisessa ja verkon turvaamisessa. (Microsoft 2024b.)

Tekoälyn käyttöön näissä osa-alueissa pureudutaan syvällisemmin myöhemmin työssä. Tekoälystä voi olla siis paljonkin hyötyä kyberturvan eri osa-alueilla. Sen lisäksi, että se tukee teknisellä tasolla, siitä voi olla apua myös analysoinnissa ja raportoinnissa sekä työntekijöiden osaamisen kehittämisessä.

Erilaisten tekoälyä hyödyntävien työkalujen avulla voidaan luoda helposti ymmärrettäviä dokumentteja ja raportteja. Tällaisten dokumenttien etuna on se, että niitä voidaan jakaa yritysten sisällä henkilöille, joilla ei välttämättä ole osaamista kyberturvallisuudesta ja raportin sisältö saadaan silti ymmärrettyä. Vastaavasti se voi auttaa uusia työntekijöitä hahmottamaan esimerkiksi kyberhyökkäyksen sattuessa tehtävät toimenpiteet helpommin ja parantaa heidän osaamistaan. (Microsoft 2024b.)

Vaikka tekoäly tuo paljon erilaisia mahdollisuuksia ja hyötyjä, liittyy sen käyttöön myös riskejä ja haasteita. Yksi haaste/riski tekoälyn kanssa on sen kouluttaminen. Jos koulutukseen käytetty data ei ole riittävällä tasolla ja teknologia sisältää virheitä, voi lopputulos olla huono. Heikko tekoälyn koulutus voi johtaa siihen, että se antaa väärää tietoa ja tuottaa sen faktana, vaikka se olisi täysin virheellinen tulos. (National Cyber Security Centre 2024.) Ja hyvin tiedetty riski mikä, on mainittu jo useaan kertaan, on se, että vastapuolella on myös käytössä tekoäly, ei vain puolustajalla.

Tekoälyn käyttö kyberturvallisuudessa tulee kasvamaan vain tulevaisuudessa. Siitä tulee tehokkaampi työkalu sekä sen avulla kyberturvallisuus ammattilaiset voivat automatisoida toistuvia työtehtäviään. Tekoälyn käytön lisääntyminen ei kuitenkaan tarkoita sitä, että kyberturvallisuus ammattilaisten tarve pieninisi. On hyvä muistaa, että tekoäly on käytössä myös hyökkääjällä. Hakkerit tulevat mahdollisesti murtamaan salasanoja tehokkaammin sekä kehittämään edistyneempiä kalastelukampanjoita sekä vaikeasti tunnistettavia haittaohjelmia. Tekoälyn saapuminen kyberturvaan tuo mukanaan niin hyötyjä kuin haittoja/riskejä. Onkin elintärkeää, että on hyvä ymmärrys siitä, mitä hyökkääjä voi tekoälyä käyttämällä saada aikaan. (Microsoft 2024b.)

5 Kyberuhkien tunnistaminen

Uhkien ja niiden ennaltaehkäisy on yksinkertaisuudessaan haitallisen toiminnan havaitsemista, joka voisi vaarantaa koko verkon. Tunnistamisen jälkeen uhka pyritään neutralisoimaan tai vähintään lieventämään sen vaikutuksia. Myös parhaiden tietoturva ohjelmien on kuitenkin varauduttava siihen, että esimerkiksi haittaohjelma on päässyt tunnistuksen ohi ja aiheuttaa uhan. (Rapid7 2024.) Kyberuhkien tunnistamisessa ehkä tärkein elementti on nopeus.

Tietoturva ohjelmien pitää pystyä tunnistamaan potentiaaliset uhat nopeasti, jotta hyökkääjän aika minimoidaan.

Organisaatiot kohtaavat kahden tyyppisiä uhkia. Niin sanottuja ”tunnettuja” sekä ”tuntemattomia” uhkia. Tunnetut uhat pitäisi olla helpompi torjua, koska niiden toiminta on tiedossa sekä kuinka niiltä pitää suojautua. Tuntemattomat uhat ovat puolestaan haastavampia, koska hyökkääjä voi käyttää jotain organisaatiolle ennen näkemätöntä tapaa tai teknologiaa. Niin tunnettuja kuin tuntemattomia uhkia pyritään tunnistamaan organisaatioissa, koska tunnetutkin uhat saattavat päästä huomaamatta livahtamaan tietoturva ohjelmien läpi. (Rapid7 2024.)

Kun uhka havaitaan, siihen pyritään vastaamaan ja sen vaikutuksia lievittämään. Uhkien havaitsemisella on paljon hyötyjä organisaation kyberturvallisuudelle. Tunnistamisen avulla pystytään estämään laajamittaiset murrot, kun uhka havaitaan nopeasti. Laajemman murron estäminen on tärkeää, koska silloin vältytään isoilta niin taloudellisilta kuin maine vahingoilta. (Microsoft 2024c.)

Ennen kuin sukellamme syvemmälle tekoälyn hyödyntämiseen uhkien tunnistamisessa, on hyvä tunnistaa peruskonseptit, miten tekoäly auttaa tunnistamaan kyberuhkia. Tekoäly hyödyntää koneoppimisalgoritmeja uhkien tunnistamisessa. Algoritmien avulla se pystyy tunnistamaan uusia ja haastavia uhkia nopeasti ja tehokkaasti. Nämä algoritmit tunnistavat malleja ja kykenevät ennustamaan mahdollisia uhkia analysoimalla suuria määriä dataa. Tämä data voi sisältää tietoa esimerkiksi vanhoista tapauksista ja uhista. Näiden koneoppimisalgoritmien käytön tavoitteena on nopeuttaa kyberuhkien tunnistamista sekä tarkkuutta. Tarkkuudella voidaan tarkoittaa esimerkiksi sitä, että tekoäly ei antaisi ”vääriä positiivisia”, vaan osaisi tunnistaa oikeat uhat ja jättää vaarattoman liikenteen huomioimatta. (Paloalto Networks 2024a.)

Koneoppimisalgoritmeihin liittyy vahvasti datan hallinta ja prosessointi. Kyberuhkien tunnistamista varten data kerätään, siivotaan ja analysoidaan. Datan analysoimisella ja sen yhdistämisellä tekoäly algoritmeihin pystytään havaitsemaan poikkeuksellista toimintaa ja liikennettä. Sen avulla pyritään tunnistamaan mahdollinen tietomurto tai kyberhyökkäys. Data voi olla peräisin esimerkiksi järjestelmän tapahtumalokeista tai käyttäjien toimintaa keräävistä tietueista. (Paloalto Networks 2024a.)

6 Haittaohjelmat

Tekoäly järjestelmien pitää pystyä toimimaan jo olemassa olevien järjestelmien kanssa ongelmitta. On erittäin tärkeää, että nämä järjestelmät kykenevät kommunikoimaan ja siirtämään dataa laitteelta toiselle. Kaikkien tietoturva järjestelmien pitää olla ajan tasalla sekä niitä pitää päivittää jatkuvasti. (Paloalto Networks 2024a.) Vanhat versiot ja päivitysten

laiminlyöminen voi pahimmillaan johtaa siihen, että uudet uhat jäävät havaitsematta ja vakava tietomurto pääsee tapahtumaan.

Kyberuhkien havainnoinnissa tekoälyä pääasiassa käytetään haittaohjelmien tunnistamiseen. Tekoälyn tehtävänä havainnoinnissa haittaohjelmien leviämisen estämiseksi on tunnistaa haitallinen koodi turvallisesta koodista. Koodia voi olla piilotettu aidon oloisiin asiakirjoihin, erilaisiin tiedostoihin ja URL-osoitteisiin. Tämän tyyppisten uhkien tunnistamiseen käytetään tiedostoanalysoijia. Tiedostoanalysoijia on kahden tyyppisiä, staattisia ja dynaamisia. Yksinkertaisuudessaan näiden ero on se, että staattiset analysoijat tuottavat nopeita vastauksia, kun puolestaan dynaamiset analysoijat tekevät hitaamman ja tarkemman lähdekoodin tarkistuksen. (Marchal, Nawrotek & WithSecure 2024, 16.)

Tekoälymallien yksi merkittävistä eduista on sen kyky sopeutua koko ajan muuttuvaan ja kehittyvään ympäristöön. Haittaohjelmat kehittyvät jatkuvasti ja sen takia onkin erityisen tärkeää, että tekoäly kykenee tunnistamaan uusia hyökkäystekniikoita. Tekoälymallit ovat loistavia tiedon ekstrapoloinnissa. Tässä tapauksessa tällä tarkoitetaan sitä, että tekoäly kykenee tunnistamaan esimerkiksi haitallisia tiedostoja, joissa on käytetty joitain ennalta tunnettujen haittaohjelmien kaltaisia tekniikoita ja toimintatapoja. Eli tekoäly tunnistaa vanhan tiedon pohjalta tiedoston haitalliseksi, vaikka se ei täyttäisi kaikkia edeltävien haittaohjelmien tunnusmerkkejä. Tätä kautta tekoälymallit pystyvät havaitsemaan uusia hyökkäystekniikoita. (Marchal, Nawrotek & WithSecure 2024, 16.)

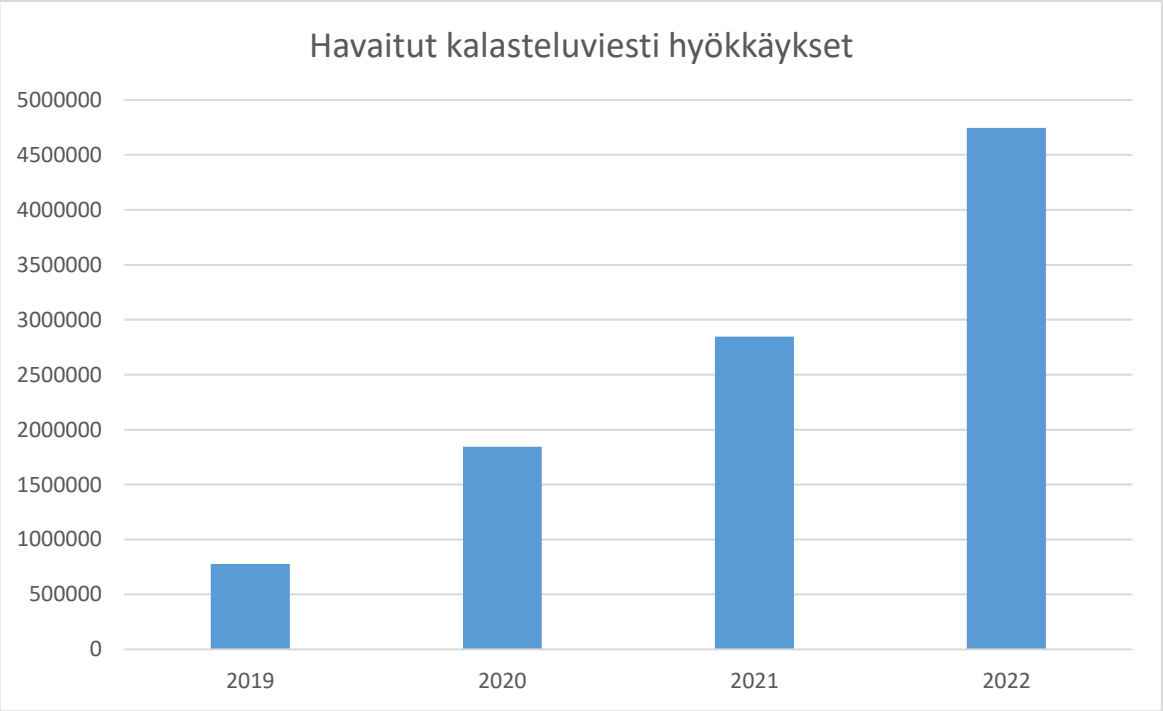
Haittaohjelmien tunnistamisessa tekoäly algoritmit voivat analysoida tiedostojen käyttäytymistä sekä tunnistaa sitä kautta malleja, jotka voivat auttaa jatkossa uhkien tunnistamista. Nämä algoritmit voivat auttaa myös havaitsemaan epätavallista käytöstä järjestelmissä. Esimerkkinä tallainen käytös voi olla sitä, että tiedosto pyrkii käyttämään sille epätyypillisiä resursseja. Niin kuin aikaisemmissa kappaleissa mainitaan, että tekoäly on hyvä tiedon ekstrapoloinnissa ja sitä kautta uusien uhkien tunnistamisessa, on myös epätavallisen käytöksen havaitseminen hyvä tapa tunnistaa uudenlaisia uhkia ja hyökkäyksiä. Tekoäly algoritmit tukevat myös tietoturva ammattilaisten töitä automaattisesti luokittelemalla tiedostoja ja asiakirjoja turvallisiksi tai haitallisiksi. Tämä helpottaa ja nopeuttaa samalla koko uhkien tunnistamisprosessia. (Sibanda 2023.)

Tekoälyn pääasiallinen käyttö uhkien havaitsemisessa on haittaohjelmien tunnistaminen. Se on kuitenkin myös tehokas tunnistamaan erilaisia kalasteluviestejä sekä roskapostia. Tietojenkalasteluviestien havaitseminen on kehittynyt viime vuosina syväoppimisen ja luontevan kielen kehityksen ansiosta. (Marchal, Nawrotek & WithSecure 2024, 16.)

Kalasteluviesteillä tarkoitetaan hyökkäyksiä millä pyritään varastamaan arkaluontoisia tietoja uhrilta. Kalasteluviestejä voi tulla esimerkiksi sähköpostiisi. Nämä viestit saattavat näyttää siltä, että ovat tulleet luotettavista osoitteista, vaikka todellisuus voi olla toinen. Viestin

tavoitteena voi olla se, että vastaanottaja saadaan lataamaan viestin liite tai klikkaamaan linkkiä ja sitä kautta lataamaan jokin haittaohjelman laitteelleen johtaen tietojen menetykseen. (Sennovate 2024.) Yleisesti tietojenkalasteluviestillä pyritään myös ohjaamaan kohde väärennetylle verkkosivulle ja saada hänet syöttämään tietonsa sivulle, milloin ne päätyvät hyökkääjän käsiin. Vaarallisen hyökkäyksestä tekee sen, että väärennetyt sivut ovat hyvinkin aidon oloisia. (F-Secure 2022.) Tämän takia onkin hyödyllistä, että tekoäly kykenee tunnistamaan paremmin tämän tyylisiä kalasteluviestejä.

Alla olevalla Kuviolla 2 haluan vielä korostaa kalasteluviestin merkittävyyttä ja niiden luomaa uhkaa. Siitä voi huomata, että kalasteluviestin kasvu on ollut merkittävää viime vuosien aikana. On myös hyvä huomioida, että Kuviossa 2 olevat luvut ovat vain havaitut hyökkäykset. Havaittujen/raportoitujen hyökkäysten määrä on todennäköisesti melkoisesti alakanttiin, sillä jopa 39 % työntekijöistä myöntää, etteivät he raportoisi työpaikalla tapahtuneesta turvallisuusriskistä. Peräti 3.4 miljardia kalasteluviestiä lähetetään päivittäin ja kaikista kyberhyökkäyksistä arviolta 91 % alkaa tietojenkalastelusähköpostilla. (Smith 2024.)



Kuvio 2: Havaitut kalasteluviesti hyökkäykset (tiedot: StationX 2024)

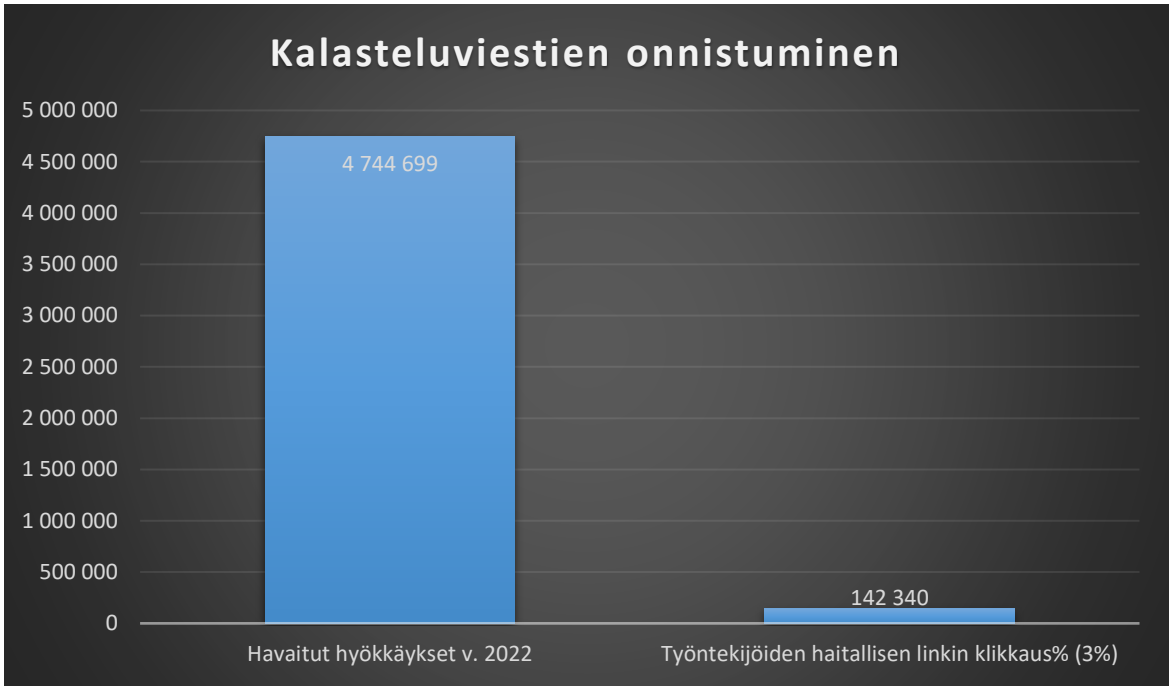
Tekoäly voi nopeuttaa sähköpostiviestien analysointia. Tekoälyn haasteena on kuitenkin se, että se pystyy erottamaan aidon viestin, spämmin ja kalasteluviestin toisistaan. Se analysoi viestin sisällön, otsikon sekä lähettäjän. Haittaohjelma tunnistuksen tapaan tekoäly voi tunnistaa kalasteluviestejä tunnistamalla niistä poikkeuksellisia piirteitä ja malleja. Tällaisia poikkeuksellisia piirteitä voisi olla esimerkiksi se, että viestin sisällössä vedotaan

kiireellisyyteen täyttää jotain tietoja tai painaa joitain viestin sisältämää linkkiä jne. Kiireellisyyteen viittaaminen on tietojenkalasteluviestin yksi pääpiirteistä. (Sennovate 2024.)

Tekoäly kykenee tunnistamaan myös kirjoitusvirheitä lähettäjän nimessä ja sitä kautta havaitsemaan mahdollisesti epämääräisiä viestejä. Tekoäly ottaa myös huomioon edelliset viestit lähettäjän ja vastaanottajan välillä, jos niitä on, mahdolliset tiedot mitä lähettäjä pyytää ja aiheen sekä otsikon liittymisen toisiinsa. (Sennovate 2024.) Jos lähettäjän ja vastaanottajan välillä ei ole aikaisempaa keskusteluhistoriaa, se voi olla merkki kalasteluviestistä. Tämä ei kuitenkaan ole lähellekään aina totta ja tämä tieto ei yksinään riitä tunnistamaan kalasteluviestiä aidosta yhteydenotosta. Viestin sisällön analysointi on toinen tapa ja mielestäni myös tehokkaampi tapa.

Aikaisemminkin mainittu kiireellisyyteen viittaaminen ja esimerkiksi pankkitunnusten tai muiden arkaluontoisten tietojen pyytäminen sähköpostin välityksellä pitäisi olla selkeä merkki tietojenkalastelusta. Myös otsikon ja viestin sisällön merkittävät erot voivat olla yksi merkki tästä. Mutta kuten aikaisempi keskusteluhistoria, tämäkään tapa ei yksinään riitä tunnistamiseen, lähinnä tukemaan tunnistusprosessia. Lähettäjän osoitteessa olevat kirjoitusvirheet voivat olla puolestaan tärkeämpi osa tunnistusta. Esimerkiksi, jos viesti tulee pankin nimissä, lähettäjän osoitteessa ei voi olla virheitä. Tämä olisi selkeä merkki kalasteluviestistä, minkä tekoäly havaitsisi nopeasti.

Seuraavassa Kuviossa 3 näytetään kuinka hyvällä prosentilla kalasteluviestit onnistuvat. Yritysten työntekijöistä 3 % klikkaa viestissä ollutta haitallista linkkiä (Smith 2024). 3 % voi jonkun korvaan kuulostaa mitättömältä määrältä, mutta kun sen suhteuttaa vuoden 2022 havaittuihin hyökkäyksiin, luku olisi n. 142 000 klikkausta. Tämän vuoden (2024) luku vuoden loppuun mennessä on varmasti huomattavasti suurempi. Tekoälyn apu voi olla tarpeen, jotta mahdollisimman moni kalasteluviesti saataisiin tunnistettua. Peräti 36 % kaikista tietomurroissa on käytetty tietojenkalastelua osana hyökkäystä (Smith 2024).



Kuvio 3: Kalasteluviestien onnistuminen (tiedot: StationX 2024)

7 Verkon kyberturva

Tekoäly algoritmit kykenevät tunnistamaan haittaohjelmia ja uhkia myös verkoissa. Kuten muissakin tunnistustehtävissä, tekoäly pyrkii löytämään poikkeavuuksia verkon liikenteestä. Se voi tunnistaa liikenteestä merkkejä hakkeroinnista, tietovuodosta ja haittaohjelmista. Yleisimpiä paikkoja missä tekoälyä käytetään verkon turvaamisessa ovat IDS- sekä IPS järjestelmät. (Paloalto Networks 2024a.)

Tekoälyn ehkä parhaimmat tai ainakin tämän hetken kehittyneimmät sovellukset ja omimaisuudet ovat massiivisten verkosta tulevan liikenteen analysointi sekä IDS ja IPS järjestelmät. Kuten aikaisemmassa kappaleessa mainitaan, kaikissa edellä mainituissa järjestelmissä tekoäly pyrkii havaitsemaan poikkeavaa ja epäilyttävää toimintaa, jotka saattavat olla merkki kyberhyökkäyksestä. (Marchal, Nawrotek & WithSecure 2024, 18.)

7.1 IDS & IPS

IDS sekä IPS järjestelmät (intrusion detection & intrusion prevention) kuuluvat tärkeimpien sovellusalueiden joukkoon, kun puhutaan verkon turvallisuudesta (Marchal, Nawrotek & WithSecure 2024, 18). IDS eli suomeksi tunkeutumisen havaitsemisjärjestelmä valvoo ja seuraa esimerkiksi yrityksen verkossa tapahtuvaa liikennettä ja tapahtumia. Se pyrkii

havaitsemaan epäilyttävää ja normaalista poikkeavaa liikennettä ja toimintaa. Tätä kautta IDS kykenee tunnistamaan mahdollisia tietomurtoja ja hyökkäyksiä. Se analysoi verkkopaketteja ja pystyy löytämään niistä merkkejä hyökkäyksistä. Ja tekee tietenkin siitä hälytyksen tällaista löytäessään. (EC-Council 2023.)

IPS eli tunkeutumisen ehkäisyjärjestelmä on vastaava järjestelmä, mutta tunnistamisen lisäksi se pystyy myös vastaamaan ja minimoimaan hyökkäyksien vaikutuksia. Yksinkertaisuudessaan näiden kahden erona on se, että toinen (IDS) havaitsee uhkia, kun taas toinen (IPS) pystyy havaitsemaan sekä vastaamaan uhkiin. (EC-Council 2023.)

Tekoälyä pystytään hyödyntämään hyvin sekä IDS että IPS käytössä. Näiden kahden lisäksi verkon turvallisuuden toinen suosittu osa-alue missä tekoälyä hyödynnetään, on tuntemattoman liikenteen analysointi sekä tämän liikenteen lähteen tunnistaminen (Marchal, Nawrotek & WithSecure 2024, 18). IDS ja IPS järjestelmät mallintavat tavallista verkkoliikennettä ja vertaavat sitä hyökkäyksiin liitettyihin poikkeaviin käyttäytymismalleihin (EC-Council 2023).

Tämä on tehokasta niin kauan kun uhka/hyökkäys aiheuttaa selvää poikkeavuutta muusta verkossa tapahtuvasta liikenteestä Esimerkiksi porttiskannaukset saattavat aiheuttaa merkkejä luvattomasta toiminnasta (Marchal, Nawrotek & WithSecure 2024, 18.) Porttiskannauksilla halutaan usein tarkistaa palvelimen avoimia portteja ja niissä pyöriviä palveluita sekä niiden versioita ja yrittää löytää haavoittuvaisuuksia sitä kautta. Tämä saattaa olla merkki siitä, että joku on aloittanut kyberhyökkäyksen.

Palvelunestohyökkäykset ovat toinen esimerkki, milloin hyökkäys aiheuttaa selvät jäljet (Marchal, Nawrotek & WithSecure 2024, 18). Palvelunestohyökkäyksien tavoite on estää jonkin palvelun käyttö ja se tehdään käytännössä ylikuormittamalla palvelin verkkoliikenteellä. Käyn työssä myöhemmin läpi tarkemmin palvelunestohyökkäyksiä ja kuinka tekoälyä voisi hyödyntää niiden havaitsemisessa.

Nämä kaksi kuitenkin aiheuttavat usein selkeitä merkkejä hyökkäyksestä ja tämän tyylisiä hyökkäyksiä vastaan IDS ja IPS järjestelmät ovat tehokkaita. Tehokkuus kärsii kuitenkin, kun vastaan tulee hienovaraisempia hyökkäyksiä, jotka voivat muistuttaa täysin tavallista viestinvaihtoa. Jotta tällaisetkin hyökkäykset saataisiin tunnistettua, tulee järjestelmiä säätää herkemmiksi. Kääntöpuolena tälle on se, että se on järjestelmät ovat herkempiä kaikkia mahdollisia hyökkäyksiä kohtaan, milloin vääriä positiivisia tulee huomattavasti enemmän. (Marchal, Nawrotek & WithSecure 2024, 18.)

Kaikkien näiden sovelluksien yksi haaste on viestintäprotokollien määrä. Verkkoliikenne on todella monimuotoista. Käyttäytymisen ja ympäristöjen mallintaminen, minkä pohjalta nämä järjestelmät tekevät päätöksiä, voi olla hankalaa. Myös verkkoliikenteen salauksen taso voi aiheuttaa haasteita. Salaus nimittäin evää pääsyn tärkeisiin pakettitietoihin. Monimutkaiset

ympäristöt, joita on haastava ennustaa, eivät välttämättä ole optimaalisia ympäristöjä tekoälysovelluksille. Ennustettavat ja yksinkertaisemmat laitteet ja ympäristöt ovat puolestaan parhaita paikkoja tekoälylle. Tällaisia laitteita ovat esimerkiksi IoT-laitteet. (Marchal, Nawrotek & WithSecure 2024, 19.)

Tekoäly on ollut osana verkon kyberturvallisuutta pitkään. Tekoälysovelluksien kehitystä on kuitenkin haitannut tai ainakin hidastanut tietoverkkojen jatkuva kehitys. Sen myötä tietoverkot ovat monimutkaisia ja tekoälyn soveltaminen sinne on haastavaa. (Marchal, Nawrotek & WithSecure 2024, 19.) On täysin ymmärrettävää, että verkot kehittyvät ja samalla siellä käytettävien tekniikoiden kehittäminen siinä yhteydessä on työlästä.

7.2 Network Detection and Response

NDR eli Network Detection and Response on kyberturvallisuuden teknologia, jonka avulla organisaatiot voivat havaita, tutkia ja vastata kyberuhkiin verkossaan. Siinä hyödynnetään usein tekoälyä ja koneoppimista (IBM 2024). Etuna sillä on se, että perinteiset teknologiat eivät välttämättä ole enää niin tehokkaita jatkuvasti kehittyviä hyökkäyksiä vastaan (Vectra AI 2024a). Tekoälyn hyödyntämisen tärkeys tulee korostumaan lähitulevaisuudessa entistä enemmän. NDR valvoo jatkuvasti verkossa tapahtuvaa liikennettä. Analysoimalla tapahtumia se voi tunnistaa potentiaalisia uhkia ja hälyttää niistä (IBM 2024). Kuten useasti aikaisemmin mainittu, epätavalliset käyttäytymismallit voivat olla merkki uhasta.

Hyvin yksinkertaisesti NDR työkalut toimivat keräämällä dataa. Ja data on peräisin siis verkkoliikenteestä. Datan keräämisen jälkeen pyritään samaan aikaan omanlainen pohja verkossa tapahtuvalle liikenteelle. Haetaan normaalia tilaa, mihin voidaan verrata poikkeamia. Poikkeamien pohjalta tunnistetaan uhkia. Poikkeamia voivat olla esimerkiksi useat kirjautumisyritykset sekä hyvin erikoiset ajankohdat, kun jotain palvelua yritetään käyttää. Esimerkiksi jotain palvelua yritetään käyttää keskellä yötä. Tämän pitäisi olla merkki hyvin todennäköisestä luvattomasta käytöstä. Nimensä mukaisesti (Detection and Response), kun uhka havaitaan NDR tekee siitä hälytyksen sekä tilanteen vaatiessa/salliessa, riippuen siitä, annetaanko kyseisessä organisaatiossa tekoälyn tehdä vastatoimia vai pitääkö ihmisen tehdä se, vastaa siihen. Vastauksena voi olla, vaikka IP-osoitteen blokkaaminen. (IBM 2024.)

Mutta mitä konkreettista hyötyä NDR ratkaisusta on yrityksille ja organisaatioille ja mitä tekoäly tuo siihen? Jatkuvalla valvonnalla uhat ja mahdolliset hyökkäykset saadaan aikaisemmin kiinni. NDR valvoo niin verkkoon saapuvaa kuin ulos menevää liikennettä, mutta myös verkon sisällä tapahtuvaa liikennettä. Tämän avulla se voi tunnistaa jo verkkoon päässeitä uhkia. (IBM 2024.) Tuntemattomien uhkien havaitseminen, automaattiset toimet uhkien vaikutuksen minimoimiseen ja kyky integroitua muihin työkaluihin tai järjestelmiin ovat vain muutamia NDR teknologian tuomista eduista. Uusien uhkien tunnistaminen sekä mahdollisuus automatisoida vastatoimia ovat erittäin tärkeitä etenkin sen takia, että vastapuolellakin on käytössään

tekoäly. Uusia hyökkäyksiä tulee lisää koko ajan. NDR työkalujen integroiminen on myös edullista, sillä sen yhdistäminen tietokantaan voi tehostaa sen tarkkuutta tunnistustehtävissä. (IBM 2024.)

Monesti mainittu asia, resurssien vapauttaminen on yksi merkittävä hyöty minkä tekoälyn käyttö tuo mukanaan. Alan ammattilaisten ja samalla yritysten on hyvä ymmärtää, että kaikki esimerkiksi NDR:n tekemät hälytykset eivät ole samanarvoisia. Toiset hälytykset voivat odottaa hetken, kun toiset vaativat välitöntä reagointia. Tekoälyllä on potentiaalia auttaa tässä priorisaatiossa. Sen kyvyllä analysoida dataa, tekoäly voisi paremmin erotella hälytyksiä toisistaan. Tällöin välitöntä vastausta vaativat hälytykset hoidetaan ensimmäisenä sekä pienemän uhan aiheuttavat hälytykset siirtyvät jonossa taaksepäin. Tällä tarkkuudella voidaan vähentää työntekijöiden taakkaa tai ainakin ohjata se kyberturvallisuuden näkövinkkelistä paremmin. (Grady 2023.)

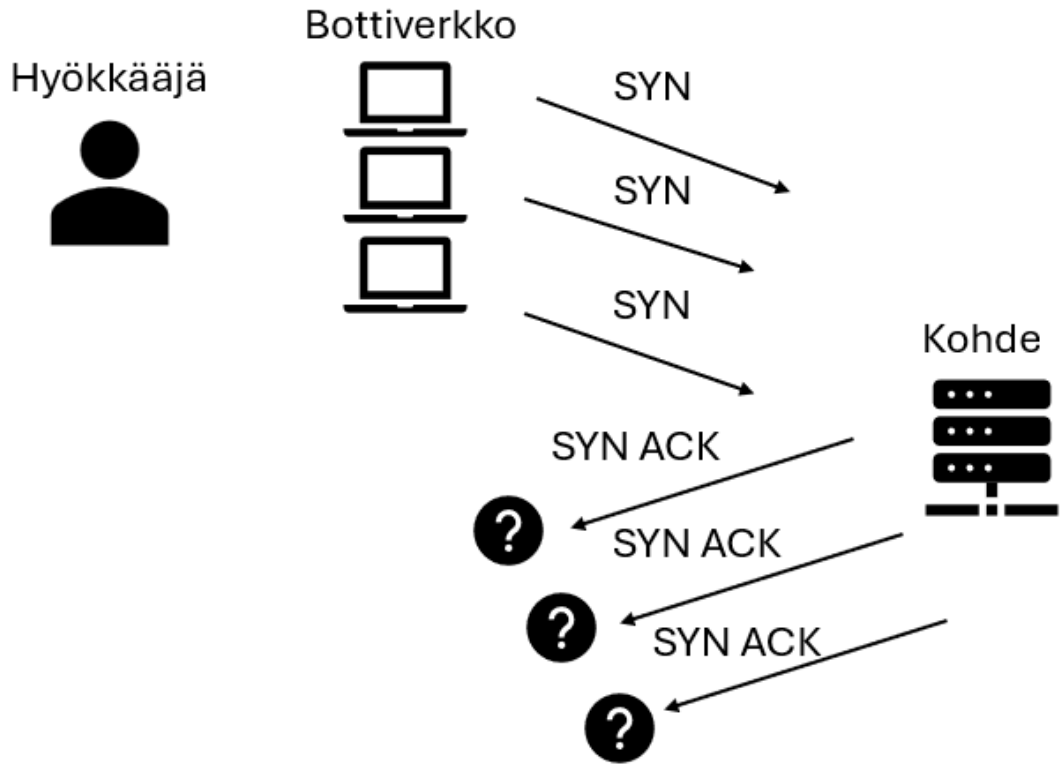
Yksi tekoälyn ehkä odottamaton apu on sen kyky tukea työntekijöitä havainnoimaan uhkien tyyppejä, vaikutusaluetta jne. Etenkin tuoreita alantyöntekijöitä se voisi auttaa eteenpäin ja samalla nopeuttaa heidän toimintaansa, kun edellä mainitut asiat ovat selvillä nopeasti eikä niitä tarvitse lähteä etsimään. (Grady 2023.) Toinen vastaava apu on kommunikaatio. Tekoälyn luonnollinen kieli on kehittyneempää ja kyberturvatiimit voisivat käyttää tekoälyä rakentaakseen helposti ymmärrettäviä raportteja johtoportaalle. Tämä tukisi työntekijöiden ja johtajien välistä kommunikaatiota ilman suurempaa ymmärrystä kyberturvallisuudesta. Tämäkin osa-alue tulee varmasti kehittymään, mutta nämä tekoälyn luomat tekstit tai vastaavat pitäisi silti lukea läpi, kunnes pystyttäisiin toteamaan, että se tuottaa virheetöntä ja ymmärrettävää tekstiä joka kerta. Siihen asti tekoäly voisi tukea raporttien luomista. (Grady 2023.)

Tulevaisuudessa tekoäly voi olla vahvemmin mukana operoimassa vastauksia/vastatoimia havaittuihin hyökkäyksiin. Se voisi tehdä näitä jopa täysin ilman, että ihminen tulee johonkin väliin tukemaan tekoälyn toimintaa. Tämän tyyliset toimet olisivat kuitenkin hieman yksinkertaisempia kuten pääsynhallinta. (Grady 2023.) NDR työkalut kehittyvät tasaiseen tahtiin, mutta monella organisaatiolla on vielä epäilyjä niiden toiminnasta ja ehkä tässä kontekstissa, tekoälyn toiminnasta. Suurimmat riskit yritysten silmissä ovat niiden tuottamat väärät positiiviset ja niihin reagoiminen. Se voisi pahimmillaan häiritä yrityksen toimintaa. (Grady 2023.)

Tekoäly on monella kyberturvallisuuden osa-alueella kohtuun tuore, joten epäilykset sen toimivuudesta ovat ymmärrettäviä ja tekoäly tullaankin varmasti ottamaan käyttöön monessa yrityksessä osissa. Esimerkiksi alkuun ihmiset vahvistavat tekoälyn tekemät ratkaisut ennen kuin ne ajetaan läpi. Tekoälyn kehittyessä sille voitaisiin antaa enemmän vapauksia tehdä ratkaisuja. Kun se otetaan hiljalleen mukaan toimintaan ja sen toimivuus voidaan varmistaa, se voi johtaa siihen, että se otetaan käyttöön laajemmin. (Grady 2023.)

7.3 Palvelunestohyökkäykset

Palvelunestohyökkäyksessä eli DoS (Denial of Service) tai DDoS (Distributed Denial of Service) saatetaan tehdä esimerkiksi niin, että hyökkääjä lähettää valtavia määriä TCP SYN (Synchronize) paketteja kohteeseen, johon kohde vastaa SYN ACK (Synchronize-Acknowledge), mutta hyökkääjä jättää viimeisen ACK (Acknowledge) paketin lähettämättä, milloin yhteydenottopyyntö jää keskeneräiseksi. Lopulta pyyntöjä on niin paljon, että palvelin ei enää kykene vastaanottamaan uusia pyyntöjä. (Kyberturvallisuuskeskus 2022.) Alla Kuvassa 1 vielä karkeasti kuinka tämä tapahtuu.



Kuva 1: Palvelunestohyökkäys (tiedot: Cloudflare 2024a)

Useasti hyökkäykset ovat hajautettuja eli yhteydenottopyyntöjä tehdään samanaikaisesti usealla eri laitteella. Yleensä hyökkääjällä on tällöin käytössään bottiverkko (botnet), jossa on useita kaapattuja verkkolaitteita. Laitteiden omistajilla ei ole mitään tietoa, että heidän laitteitaan hyödynnetään hyökkäykseen. (Kyberturvallisuuskeskus 2022.) Palvelunestohyökkäysten määrä on noussut viime vuosina huomattavasti. 2023 niiden määrä nousi n. 90 %. Hyökkäykset eivät myöskään aina ole samanlaisia, mikä tekee niiltä puolustautumiselta hankalampaa. (CEO Monthly 2024.)

Tekoäly voi tukea DDoS hyökkäyksiltä suojautumista. Perinteiset järjestelmät eroavat tekoälypohjaisista ratkaisuista siten, että ne käyttävät olemassa olevaa tietoa eli vanhoja hyökkäyksiä vertailukohteinaan. Vanhempien hyökkäysten piirteiden perusteella tekemät ratkaisut ovat hyvä ja tehokas tapa puolustautua palvelunestohyökkäyksiltä, kunnes hyökkääjä muuttaa jotain tekniikkaa/taktiikkaa ja hyökkäys ei enää omaa samoja piirteitä muiden hyökkäysten kanssa. Tämä vaikeuttaa tunnistusta ja samalla tietoturva-ammattilaisten työskentelyä, sillä heidän aikaikkunansa vastatoimille pienenee, kun hyökkäys on edennyt pidemmälle heikomman uhkien tunnistuksen takia. (CEO Monthly 2024.)

Tekoälyllä on muutamia eri käyttötarkoituksia ja hyötyjä, kun puhutaan DDoS hyökkäyksiltä puolustautumiselta. Jälleen esiin nousee tekoälyn kyky analysoida suuria määriä tapahtumia ja dataa sekunneissa. Tässä tarkoituksessa se pyrkii jopa miljoonista yhteyksistä analysoimaan, että onko verkkoliikenne aitoa vai onko se botin/koneen luomaa liikennettä. Tätä kautta se kykenee blokkaamaan mahdollisesti haitallisen liikenteen tai liikenteen, jonka tarkoitusperä on haitallinen. Samanaikaisesti mahdollistaen oikeiden käyttäjien pääsyn haluttuun palveluun. (CEO Monthly 2024.)

Toinen etu minkä se tarjoaa perinteisiin järjestelmiin verrattuna, on se, että tekoäly oppii. Kouluttamalla tekoälyä erilaisilla hyökkäys skenaarioilla se voi tunnistaa paremmin erilaisten hyökkäyksien piirteitä. Parhaimmillaan tekoäly voi saada ymmärrystä myös siitä miltä kyberhyökkäykset voisivat näyttää tulevaisuudessa. (CEO Monthly 2024.) Tekoäly tuo myös DDoS hyökkäysten torjuntaan ja havaitsemiseen lisää tehoa. Kuten monessa muussakin osa-alueessa, tekoäly tuo tehoa ja tarkkuutta, mutta ennen kaikkea, se vapauttaa resursseja. DDoS hyökkäykset ovat valitettavan yleisiä ja hyvin hajautettuna ne aiheuttavat isoja ongelmia kohteelle.

7.4 Extended Detection and Response

Tekoälyä voidaan hyödyntää myös XDR teknologiassa. XDR (extended detection and response) suojaa yrityksen IT-infrastruktuuria. XDR kerää tietoa eri suojaustasoilta kuten päätepisteistä, verkoista, sovelluksista jne. Tämän avulla kyberuhat voidaan havaita nopeasti ja niihin voidaan reagoida tilanteen vaatimalla tavalla. XDR on edistyneempi versio EDR (endpoint detection and response) teknologiasta. EDR keskittyy päätepisteiden turvallisuuteen, kun XDR keskittyy useampaan suojaustasoon. XDR:n käyttöön ottaminen parantaa muun muassa uhkien tunnistuskykyä. (Kaspersky 2024.)

Niin kuin monessa muussakin kyberuhkien havaitsemisessa, tekoäly tuo myös XDR:n havaitsemiseen lisää tehokkuutta ja tarkkuutta. Tekoälyn avulla pyritään vähentämään vääriä positiivisia eli vähentämään turhanpäiväisiä hälytyksiä. Väärät positiiviset työllistävät kyberturvallisuus ammattilaisia turhaan, kun se aika voitaisiin käyttää johonkin täysin muuhun. Kuten aikaisemminkin on mainittu tekoälyn kyky analysoida suuria määriä dataa laadukkaasti, on

erinomainen. Laadukkaasti tarkoittaen vähemmän vääriä positiivisia. Ihmisen tekemä sama työ manuaalisesti ei mitenkään pysty vastaamaan tekoälyn nopeuteen. Ja toinen merkittävä etu on uhkien havainnoinnin automatisointi. (Freed, A. M. 2024.) Tekoälyn avulla alan ammattilaisten toistuvia työtehtäviä voidaan automatisoida ja resurssit voidaan käyttää tehokkaammin.

Tekoäly kykenee myös muodostamaan hyvinkin yksityiskohtaisen näkökulman siitä, kuinka hyökkääjä toteuttaa itse hyökkäyksen. Tämän avulla hyökkäykset voidaan havaita aikaisessa vaiheessa, ennen kuin isompaa vahinkoa on päässyt tapahtumaan. Hyvin tarkasti kohdennetut hyökkäykset, jotka hyödyntävät jotain uutta tekniikkaa/taktiikkaa voivat olla erittäin haastavia havaittavia. Ne saattavat päästä jopa tietoturvasovellusten läpi ilman hälytystä. (Freed, A. M. 2024.)

Kyberhyökkäyksen sattuessa, yhdenkin sen osan löytäminen saattaa mahdollistaa koko hyökkäyksen alkuperäisen syyn löytämisen. Ja tässä tuleekin iso ero jälleen tekoälyn ja ihmisen välillä. Tekoäly pystyy automaattisesti käymään läpi miljoonia tapahtumia sekunneissa verrattuna ihmisiin, jotka etsivät ja vahvistavat hälytyksiä manuaalisesti. Tämä prosessi saattaa kestä tunteja, pahimmillaan jopa päiviä. Kuten työn aikana olen jo monesti todennut, nopeus on tärkeää. Tällaisessa tilanteessa on tärkeää pystyä vastaamaan uhkaan mahdollisimman nopeasti, jotta siitä ei tule yritykselle merkittävää ongelmaa. (Freed, A. M. 2024.) On hyvä kuitenkin muistaa, että myös ihmisiä tarvitaan. Tulevaisuuden kannalta parhaimpia vaihtoehtoja taitaa olla kombinaatio alan ammattilaisia sekä tekoälypohjaisia sovelluksia. Yksinään molemmissa olisi parantamisen varaa.

Zero day hyökkäykset/haavoittuvuudet ovat yksi isoimmista haasteista organisaatioille. Zero-day haavoittuvuudet ovat haavoittuvuuksia, jotka eivät ole kenenkään tiedossa. Zero-day hyökkäys on tilanne, jossa hakkeri hyödyntää tällaista haavoittuvuutta hyökkäyksessään. Zero-day haavoittuvuudet ovat sovelluksessa tai järjestelmässä usein jo julkaisuvaiheesta lähtien. Tämän tyyppiset haavoittuvuudet ovat siis haastavia, koska mitään päivitystä ei ole valmiina. Tästä alkaakin kilpajuoksu hyökkääjän ja puolustajan välillä, kumpi ehtii ensin luomaan hyökkäyksen tai poistamaan ongelman. (IBM 2023.) Vaarallisia zero-day haavoittuvuuksista tekee juuri se, että ne voivat aiheuttaa isoja vahinkoja ennen kuin se saadaan korjattua (Vectra AI 2024b). Tekoäly voi kuitenkin tukea näiden haavoittuvuuksien löytämistä sekä hyökkäysten havaitsemista.

Kuten monella muullakin osa-alueella, myös zero-day hyökkäysten tunnistamiseen hyödynnetään tekoälyn kyvykkyyttä tunnistaa epäilyttävää toimintaa (IBM 2023). Jatkuva valvonta on elinehto sille, että näitä hyökkäyksiä voidaan tunnistaa. Aikaisemmissa kappaleissa läpi käydyt IPS ja IDS järjestelmät voivat tunnistaa myös uhkia, mutta rajoittaa myös sen liikettä

verkon sisällä, ettei se pääse liikkumaan vapaasti järjestelmästä toiseen. (Vectra AI 2024b.) Myös XDR järjestelmä kykenee näiden hyökkäysten tunnistukseen (IBM 2023).

Korostaakseni vielä tekoälyn jo olemassa olevaa osaamista/kyvykkyyttä ja sen potentiaalia, työnteko hetkellä Googlen Project Zeron tekoäly agentti löysi haavoittuvuuden SQLite tietokannan hallintajärjestelmästä. Onneksi se löydettiin ennen julkaisua, joten sillä ei ollut vaikutusta käyttäjiin. Tämä on työn teko hetkellä yksi ensimmäisistä julkisista entuudestaan tuntemattomista haavoittuvuuksista, jonka tekoäly on löytänyt. On kuitenkin hyvä ottaa huomioon, että hyvin kohdennetut ohjelmistontestaustyökalut ovat vähintään yhtä tehokkaita kuin tämä Big Sleep tekoäly agentti tällä hetkellä. Mutta tulevaisuudessa se voisi tuoda ison edun sekä auttaa myös haavoittuvuuksien analysoinnissa. (the Big Sleep team 2024.) Potentiaalia tekoälyn käytöstä kyberturvallisuudessa löytyy, mutta se vaatii vielä kehitystä, jotta sitä voitaisiin hyödyntää vielä enemmän.

8 Hyödyt tekoälyn käytöstä uhkien havaitsemisessa

8.1 Tarkkuus ja nopeus

Tekoäly tuo uhkien havaitsemiseen ja kyberturvallisuuteen lisää tarkkuutta. Sen kyky analysoida suuria määriä dataa eri lähteistä mahdollistaa poikkeavuuksien tunnistamisen, ja sitä kautta se kykenee havaitsemaan mahdollisia haittaohjelmia ja kyberhyökkäyksiä. Se voi auttaa siis tunnistamaan mahdollisesti täysin uusia hyökkäyksiä ja erilaisia malleja, jotka voisivat olla ihmiselle erittäin haastavia havaittavia. (Sibanda 2023.)

Tekoälyllä on myös kyvykkyyttä tunnistaa niin zero-day haavoittuvuuksia ja hyökkäyksiä sekä zero-day haittaohjelmia (Dhaliwal 2024). Zero-day haittaohjelma on haittaohjelma, jonka malli tai koodinpätkä millä tunnistus pitäisi tehdä onkin entuudestaan tuntematon. Silloin se voi päästä livahtamaan antivirus ohjelmilta ja päästä aiheuttamaan vahinkoa. (IBM 2023.) Aikaisemmissa osioissa on mainittukin, kuinka tekoäly tunnistaa näitä tuntemattomia uhkia. Tekoäly voi tunnistaa tiedostoista merkkejä, jotka ovat hieman samantyyppisiä, kuin haittaohjelmissa. Esimerkiksi, tiedosto käyttää epätavallisia resursseja tai verkossa ilmenee poikkeavaa liikennettä erikoiseen kellonaikaan. Hyökkäyksen merkkejä on useita.

Tarkkuuden lisäksi tekoäly algoritmit tuovat myös nopeutta puolustukseen. Kyberhyökkäyksen sattuessa, kuten aikaisemmin mainittu nopeus on tärkeä. Mitä vähemmän aikaa hyökkääjälle annetaan, sitä vähemmän yleensä tuhoa/vahinkoa hyökkäys saa aikaan. Parhaassa tapauksessa tietovuoto voidaan ehkäistä kokonaan nopealla vastauksella hyökkäykseen. (Sangfor Technologies 2024.) Tekoälyn nopeus verrattuna perinteisiin järjestelmiin sekä ihmiseen on valtava. Jatkuva datan läpi käyminen mahdollistaa nopeat vastatoimet hyökkäyksen sattuessa. Alan ammattilaiset ovat sanoneet sen nopeuden käydä läpi miljoonia yksittäisiä

tapauksia olevan sen suurin vahvuus ihmisiin verrattuna (Pratt 2024). Kuten työssä aikaisemmin mainitaan, tekoäly algoritmit tuottavat vähemmän virheellisiä positiivisia eli varoittavat uhasta, mikä onkin ihan tavallista liikennettä yrityksen verkossa esimerkiksi. Näiden virheellisten positiivisten hälytysten vaikutus on muun muassa se, että uhkaan on pakko reagoida ja se kuluttaa resursseja, joita olisi voitu käyttää muualla. (Sibanda 2023.)

8.2 Automatisointi & Sopeutuminen

Nopeuden ja tarkkuuden lisäksi tekoäly algoritmien yksi iso hyöty kyberammattilaisille on automatisointi. Sen avulla voidaan automatisoida vastauksia tiettyihin tilanteisiin ja vähentää sitä kautta työntekijöiden taakkaa ja yrityksen resurssit voidaan hyödyntää tehokkaammin (Sangfor Technologies 2024). Tekoäly kykenee automatisoimaan useitakin eri asioita. Hyökkäyksiin vastatoimien tekeminen on oma asiansa, mikä on varmasti eniten vielä ihmisten hallinnassa. Luotto tekoälyn tekemiin ratkaisuihin ei ole vielä sillä tasolla, että se voisi vastata omatoimisesti uhkiin. Tämä tuskin in käytäntönä hirveän monessa yrityksessä.

Tekoälyllä voidaan kuitenkin automatisoida toistuvat, pitkäveteiset tehtävät kuten lokitietojen analysointi. Samaan kastiin kuuluu muutkin yksinkertaisemmat analysointi tehtävät kuten verkkoliikenteen seuranta. Ihmiset voidaan siirtää tekemään monimutkaisempia tehtäviä, jotka eivät tekoälyltä ainakaan toistaiseksi luonnistu. Tekoäly voi auttaa ”tylsien” tehtävien kanssa, mutta tehostaa myös muuten aikaa vieviä tehtäviä. Osa näistä saattaa olla sellaisia, jotka ovat aina vähän taka-alalla, ei kriittisiä tehtäviä ja ne saattaisivat jäädä muuten tekemättä kokonaan. Harvalla yrityksellä on tilannetta, jossa työntekijöitä olisi liikaa eikä tehtävää olisi. (Watson 2024.) Sen avulla voidaan saada yksittäisen työntekijän työmäärää hieman hajautettua.

Yhtenä merkittävänä hyötynä voisin nostaa esiin sen kyvyn mukautua haastavaan ja muuttuvaan kyberympäristöön. Perinteiset metodit, perinteiset tietoturvaohjelmat eivät pysty adaptoitumaan eikä oppimaan samalla tavalla kuin tekoäly. Tekoäly oppii koko ajan lisää, mitä enemmän se käy läpi dataa. Oppimansa perusteella se mukauttaa myös omia algoritmejaan parhaaksi katsomallaan tavalla. Tekoäly oppii uutta jatkuvasti ja siitä tulee entistä tehokkaampi ajan kuluessa. (Sibanda 2023.) Tämä tekoälyn sopeutuminen on mielestäni tekoälyn ehkä merkittävin etu. Se imee tietoa jatkuvasti ja pystyy hyödyntämään sitä jatkossa, tehostaen sen nopeutta sekä tarkkuutta. Haittaohjelmat ovat erittäin yleisiä nykyään ja ne kehittyvät jatkuvasti, joten tekoäly on valtava apu etenkin uusien haittaohjelmien sekä muiden uusia tekniikoita hyödyntävien hyökkäyksien tunnistamisessa.

8.3 Analyysit & Skaalaus

Tekoäly voi tukea alan ammattilaisia uhkien havaitsemisessa sekä ottaa mahdollisesti vastuuta yksinkertaisemmista tehtävistä ja miksi ei joskus haastavimmistakin. Sen ehkä yllättävin apu

on myös se, että tekoäly voi analysoida uhkia, niiden pohjasyitä sekä auttaa ymmärtämään niitä paremmin. Se voi rakentaa raportin tai antaa selityksen riskeistä ja sitä kautta parantaa käyttäjien ymmärrystä. (Dhaliwal 2024.) Vastaavasti, jos tekoäly ei tuo mitään selitystä esimerkiksi tekemille toimilleen, jää ilmaan paljon kysymyksiä. Miksi se on tehnyt jotain, minkä tiedon pohjalta jne. Mutta tekoälyn käytön haasteita käydään läpi tarkemmin myöhemmin.

Tekoäly tai tarkemmin koneoppimisen algoritmit voivat luoda myös ennustavia analyysejä. Sen avulla voitaisiin esimerkiksi yrittää ennakoida kyberhyökkäys ja pyrkiä minimoimaan sen vaikutukset ennaltaehkäisevillä toimilla. (Paloalto Networks 2024b.) Tekoäly pystyy tekemään ennustuksia, mutta se tarvitsee ison määrän dataa. Kyberhyökkäysten ennustamisessa data voi olla peräisin esimerkiksi vanhoista hyökkäyksistä sekä käyttäytymismalleista (Paloalto Networks 2024b). Ennustamisessa hyödynnetään koneoppimista, jota koulutetaan aiheeseen sopivalla materiaalilla. Lopulta se kykenee käymään läpi isoja määriä dataa ja tapahtumia, tunnistaa niistä malleja ja sitä kautta ennustaa, jos vastaavia tilanteita sattuu tulevaisuudessa. (Cloudflare 2024b.)

Merkittävänä etuna tekoälyllä on sen skaalautuminen tarpeen mukaan. Työmäärät voivat nousta, esimerkiksi yrityksen verkkoliikenteen määrä nousee merkittävästi. Tekoäly ei tarvitse suoriutuakseen tästä lisääntyneen liikenteen analysoinnista ja valvonnasta lisää henkilöstöä tai laitteistoa. Yrityksen kyberturvan vaatimukset saattavat nousta, ja investoinnit myös tekoälyn tukemiseen voivat olla välttämättömiä. Tekoäly pystyy kuitenkin adaptoitumaan tilanteeseen ja kasvamaan siinä ohessa tehden siitä mahdollisesti kustannustehokkaan ratkaisun. (Watson 2024.) Aikaisemmin mainittu automatisointi ja sen avulla resurssien vapautuminen ovat myös hyvä tapa pienentää yrityksen kuluja. Työn aikana olen monesti korostanut tekoälyn potentiaalia tehostaa yrityksen kyberuhkien havaitsemista, mutta, jos siinä samassa voidaan tehdä säästöjä, aina parempi.

9 Ongelmat & haasteet

9.1 Koulutus & Data

Tekoäly on tuonut ja tulee tuomaan paljon apua kyberturvallisuuteen, mutta niin kuin käytännössä kaikessa muussakin, piilee siinäkin haasteita ja huolenaiheita. Yksi isoimmista haasteista tekoälyn kanssa on se, että kyberhyökkäykset kehittyvät jatkuvasti. Se tarkoittaa sitä, että tekoälyä pitää kouluttaa jatkuvasti, jotta se pystyy tunnistamaan uusia hyökkäystapoja tehokkaasti. Jos tekoälyä ei kouluta se voi johtaa tarpeettomiin hälytyksiin ja pahimmillaan oikea hyökkäys voi päästä huomaamatta tekemään vahinkoa. (Marchal, Nawrotek & WithSecure 2024, 16–17.)

Tekoälyä kouluttaessa on myös hyvä muistaa, että data millä tekoälymalleja koulutetaan, tulee olla laadukasta. Virheellisen datan käyttö voi johtaa vastaavasti siihen, että tekoäly jättää huomioimatta aidon uhan esim. haittaohjelman, mutta hälyttää täysin turvallisesta tiedostosta. (Sangfor Technologies 2024.) Näitä kutsutaan myös vääriksi positiivisiksi ja vääriksi negatiivisiksi. Koulutuksessa käytettävän materiaalin tulee olla laadukasta, mutta sitä pitää olla myös riittävästi. Eikä vain samanlaisia esimerkkejä, vaikka vanhoista hyökkäyksistä. Monimuotoisten datasettien hyödyntäminen mahdollistaa sen, että tekoäly voi tunnistaa hyvin useita uhkia sekä tunnistaa minkälaiset skenaariot voisivat indikoida uhkaa. Jos dataa on paljon, mutta siinä ei ole esimerkiksi palvelunestohyökkäyksistä mitään, miten tekoäly voisi tunnistaa sen? (Paloalto Networks 2024b.)

Haasteena onkin se, että dataa on riittävästi, se kattaa tarpeeksi tietoa erilaisista uhista, joita tekoäly voi kohdata (Paloalto Networks 2024b). Tämä on melko kriittistä edellä mainittujen väärien positiivisten välttämiseksi. Tekoälyn kouluttamisessa tärkeää on siis jatkuvuus sekä koulutusmateriaalin laatu. Toisen elementin puuttuminen johtaa tekoälyn tehokkuuden heikkenemiseen.

Koulutuksen lisäksi yrityksillä on ollut haasteita tekoälyn optimoinnissa omiin järjestelmiinsä. Tekoälyn optimoimista on vaikea kopioida jostain muualta, koska jokaisella yrityksellä on oma IT-infrastruktuurinsa. Jos optimointi jää heikoksi, se voi vaikuttaa luonnollisesti itse tekoälyn kykyyn uhkien tunnistamisessa. Optimointi voi tuottaa haasteita, mutta ongelmaksi voi nousta myös henkilökunnan osaamisen puute tekoälyn suhteen. On täysin ymmärrettävää, että osaamista ei välttämättä jokaisesta yrityksestä löydy ainakaan sillä tasolla, että se saataisiin toimimaan parhaimmalla mahdollisella tavalla. (Pratt 2024.)

Tästä seuraakin kysymys, tuoko tekoäly, joka ei toimi täydellä potentiaalillaan riittävästi arvoa yrityksille? Vai tuottaako se silloin enemmän virheellisiä hälytyksiä ja työllistää ihmisiä turhaan? Tulevaisuudessa osaamista varmasti tuleekin löytymään ja optimointi erilaisiin digitaalisiin ympäristöihin voi onnistua helpommin ja siitä voi nousta korvaamaton työkalu taistelussa uusia hyökkäyksiä vastaan. Mutta se voi tällä hetkellä tuottaa ongelmia, jos osaamista ei löydy.

Osa saattaa yliarvioida tekoälyn tämänhetkisen kyvykkyyden. Odotukset voivat olla myös liian korkealla tekoälyn osaamiseen lähitulevaisuudessakin (Pratt 2024). Isommilta yrityksiltä saattaisi löytyä osaamista tai tarvittavat resurssit ostaa osaaminen. Mutta pienemmillä yrityksillä voi olla ongelmia osaamisen sekä resurssien suhteen. (Skillfloor 2024.)

9.2 Etiikka & Läpinäkyvyys

Muita yleisiä haasteita mitä on liitetty tekoälyyn, on esimerkiksi sen eettisyys. Sen käyttö on herättänyt kysymyksiä muun muassa yksityisyydestä ja sen mahdollisesta puutteesta,

tietoturvasta sekä väärinkäytöstä. Eettisyyden lisäksi tekoälyn läpinäkyvyyttä on kyseenalaistettu. (Skillfloor 2024.)

Eniten on mietitty sitä, millä perusteella tekoäly tekee ratkaisuja. Tekoäly algoritmien pitäisi olla läpinäkyvämpiä. (Skillfloor 2024.) Tekoälyn tekemiin ratkaisuihin pitäisi pystyä luottamaan. Luottamus kärsii kuitenkin, jos sen tekemän ratkaisun syytä ei tiedetä (Skillfloor 2024). Ei tiedetä minkä tiedon/tapahtuman pohjalta kukin ratkaisu/toimi on tehty. On vaikeampi ymmärtää, oliko ratkaisu oikea vai ei. Huolta on herättänyt myös tekoälyn kyky toimia ilman mitään valvontaa. Epäilyksiä löytyy, ettei se kykene suoriutumaan tehtävistään yhtä hyvin ilman, että sitä valvoo ihminen, johtaen virheiden määrän kasvuun. (Watson 2024.) Mikäli tekoäly ei tuota jonkin tyyppistä raporttia tai analyysiä toiminastaan, virheet saattavat kasvaa, aiheuttaen vain lisää harmia ja töitä. Virheisiin liittyy myös aikaisemmin mainitsemani datan laatu. Jos data on jotenkin puolueellista tai harhaanjohtavaa johonkin suuntaan, ovat myös tekoälyn ratkaisut puolueellisia ja harhaanjohtavia (Watson 2024).

Tekoälyn tekemä ratkaisu on sen mielestä aina oikea. Vaikka sillä on potentiaalia soveltaa sille koulutettua sisältöä, se osaa kuitenkin vain sen mitä sille on koulutettu. Sen tekemät ratkaisut voi olla hyvä kyseenalaistaa, jos se ei anna mitään näyttöä, että se on todella toiminut tilanteessa oikein. Ilman sitä yritykset luottaisivat sokeana tekoälyyn. Ihmisen on edelleen hyvä olla mukana päätöksenteossa (Watson 2024). Tekoälyä on myös haastettu siitä, että tuoko se mitään lisäarvoa yrityksille muuta kuin sen, että se suorittaa jonkun tehtävän. Esimerkiksi, tuoko se jotain uutta tietoa kyberuhista. Sen tämänhetkistä kykyä tunnistaa zero-day hyökkäyksiä on myös kyseenalaistettu. Kyseenalaistaminen pohjautuu siihen, että sitä ei ole luotu tämän tyyppiseen tehtävään. (Pratt 2024.) Zero-day hyökkäyksien tunnistamisen on haastavaa ja sen takia se, että sitä on kyseenalaistettu ei sinänsä yllätä. Huoli tekoälyn tekemistä ratkaisuista on ymmärrettävää, sillä niillä voi olla merkittäviä vaikutuksia.

Ongelmaksi tekoälyn kanssa voisi tulevaisuudessa nousta se, että siihen luotettaisiin liikaa. Luotettaisiin täysin siihen, että se tunnistaa kaikki uhat. Vaikka aikaisemmin puhuin siitä, kuinka tekoäly voi vapauttaa resursseja ja pienentää kuluja sen avulla, ei sen käyttöön ottaminen ole kuitenkaan ilmaista. Kuten mainitsin, se vaatii kouluttamista, optimoimista, hallinnointia ja osaamista. Sitä ei kaikkialta löydy ja yleensä arvokas osaaminen, jonka saatavuus voi olla heikko, on kallista. Tekoäly ratkaisut saattavat tarvita melko isoa prosessointikapasiteettia toimiakseen tehokkaasti. Se voi vaatia lisää laitteistoa tukemaan sen toimintaa. Useasti ihmiset näkevät vain hyödyt, unohtaen esimerkiksi tässä tulevat mahdolliset piilevät kulut. (Palotalto Networks 2024b.)

9.3 Hyökkäykset

Yksi isoista yleisistä huolenaiheista ovat mahdolliset hyökkäykset, jotka saattavat kohdistua tekoälyjärjestelmiin. Hyökkäykset tekoälyjärjestelmiin, jotka osallistuvat uhkien

tunnistamiseen ovat vakava uhka. (Skillfloor 2024.) Tekoäly nojaa täysin sille syötettävään dataan uhkien tunnistamisessa. Onnistuessaan hyökkääjä voi päästä manipuloimaan dataa mitä käytetään koulutusmateriaalina ja syötetään tekoäly algoritmeille. Se voi puolestaan johtaa pahimmillaan siihen, että tekoäly ei enää kykene erottamaan mikä tiedosto on turvallinen ja mikä ei, mikä aiheuttaa uhan ja mikä ei. (Paloalto Networks 2024b.)

Tekoälypohjaisten ratkaisujen kannalta vaarallinen hyökkäys on Data poisoning attack eli datan manipulointi. Dataa voidaan manipuloida siten, että se voi antaa täysin harhaanjohtavia hälytyksiä sekä päästää esimerkiksi selkeän haittaohjelman tunnistuksen läpi, vaarantaen siten koko yrityksen kyberturvallisuuden. (National Cyber Security Centre 2024.) Tähän liittyy myös aikaisemin puhuttu liika luottamus/riippuvuus tekoälystä. Jos tekoäly on pienemmässä roolissa mahdollisesti vain tehostamassa perinteisten järjestelmien toimintaa, ei sen datan manipulaatio välttämättä aiheuta ihan niin kriittistä uhkaa, jos muut järjestelmät toimivat täysin ja tunnistavat uhan.

Toinen potentiaalinen uhka tekoälylle ovat Prompt injection hyökkäykset. Tällöin hyökkääjä antaa tekoälylle syötteen, jonka tarkoituksena on saada se paljastamaan jotain tietoa mitä sen ei pitäisi paljastaa. Tieto voisi liittyä esimerkiksi siinä piilevään haavoittuvuuteen, mitä tietoturvatiimi ei ole vielä löytänyt. Sillioin hyökkääjä pääsisi hyödyntämään tietoa ja mahdollisesti aloittamaan hyökkäyksen yritystä vastaan. (National Cyber Security Centre 2024.) Tekoälyyn saattaa kohdistua myös hyökkäyksiä, joiden tarkoitus ei ole sekoittaa sen toimintaa vaan päästä käsiksi dataan. Tekoälypohjaiset järjestelmät käyvät läpi dataa, mikä saattaa sisältää arkaluontoista materiaalia. Hyökkäyksen tarkoituksena voi olla myös pääsy käsiksi tähän arkaluontoiseen materiaaliin. (Terranova Security 2023.)

10 Tulevaisuus

Tekoäly on kehittynyt viime vuosien aikana, mutta onko vastaavaa odotettavissa myös tulevaisuudessa? Tekoäly omaa ison potentiaalin, mutta tuleeko se ikinä täyttämään sen odotuksia ja nousemaan merkittäväksi avuksi kyberturvallisuuteen? Sen kehityksen odotetaan jatkuvan ja sen käytön lisääntyvän tulevaisuudessa, mutta siihen on liitetty myös epäilyjä. Etenkin generatiivista tekoälyä pidetään lupaavana (Pratt 2024). Generatiivinen tekoäly keskittyy siis uuden sisällön luomiseen kuten kuvien, koodin, videoiden jne (Scapicchio & Stryker 2024). Se on muun muassa hyvä hahmottamaan erilaisten tapahtumien sarjaa ja missä järjestyksessä mitäkin on tehty. Tätä kykyä ymmärtää tapahtumien sisältöä voitaisiin tulevaisuudessa hyödyntää käyttäytymismallien sekä uhkien tunnistamisessa. (Pratt 2024.) Siitä voisi tulla hyvinkin tehokas tunnistamaan poikkeavaa käytöstä, koska sillä olisi hyvä käsitys missä järjestyksessä normaalisti jokin asia tehdään ja mitä resursseja käyttäjät hyödyntävät milloinkin.

Luontaisen kielen kehitys voi auttaa organisaatioita myös kyberturvallisuudessa. Tekoälyn kehityksen avulla tulevaisuudessa se voi pystyä luomaan hyvinkin arkisella kielellä tehtyjä raportteja kyberuhista. Raportit voisivat sisältää tietoa uhan vakavuudesta sekä sen mallista, miten se pyrkii ohittamaan puolustuksen. Se voisi jopa raportoida tarvittavista vastatoimista, jotta uhka saadaan kiinni välittömästi. Tämä voisi toimia myös toiseen suuntaan siten, että tekoälypohjaisille työkaluille voitaisiin tehdä kyselyjä hyvinkin arkisilla kysymyksillä ja saada sitä kautta lisää informaatiota. Tekoäly voisi kertoa hyvinkin tarkkaan mitä tapahtuu. (Pratt 2024.)

Nämä asiat ovat varmasti mahdollisia nimenomaan tulevaisuudessa. Tekoäly eivätkä välttämättä teknologiat muutenkaan ole vielä valmiita näin vaativiin tehtäviin. Mutta tämän tyylinen kehitys missä tekoälyn kanssa voisi keskustella sen tekemistä löydöksistä voisi helpottaa informaation keräämistä ja ymmärtämistä, jos työkalulta voidaan suoraan kysyä asioita ja se antaisi selkeitä vastauksia mitkä kaikki organisaation sisällä ymmärtäisivät, vaikka heillä ei olisi sen isompaa ymmärrystä aiheesta muuten. Se voisi parantaa myös luottamusta tekoälyn tekemiin ratkaisuihin, kun ne on selvennetty täysin, mitä, miksi, milloin, ja sen lisäksi kerrottu vielä toimet aiheuttaneesta uhasta yksityiskohtaisesti (Skillfloor 2024). Analysoinnin lisäksi, tekoäly voisi tulevaisuudessa ennustaa ja ennakoida kyberuhkia ja hyökkäyksiä (Pratt 2024). Tämä perustuu juuri generatiivisen tekoälyn kykyyn ymmärtää tapahtumia ja niiden tapahtumisjärjestystä. Tämän avulla se voisi tunnistaa uhkia hyvissä ajoin tietyistä merkeistä, mitä esimerkiksi haittaohjelma aiheuttaa. Sen avulla tietoturvatiimit voisivat ennakoida tulevaa ja olla valmiimpia vastaamaan siihen (Pratt 2024).

Syväoppimisen kehittymistä pidetään yhtenä tärkeänä osana tekoälyn tulevaisuutta. Tekoälyn tunnistuksen kehitys ja tehokkuus voivat nousta sen myötä aivan uudelle tasolle. Uudelle tasolle tarkoittaa tässä tilanteessa sitä, että tekoäly tunnistaisi uhkia, jotka käyttäytyvät hyvin hienovaraisesti. (Skillfloor 2024.) Eli ne eivät aiheuta heti selkeitä merkkejä kuten esimerkiksi porttiskannaus tai palvelunestohyökkäys voi aiheuttaa. Haasteena tällä hetkellä tämän tyyppisten uhkien kanssa on se, että tekoäly ei välttämättä ole vielä sillä tasolla, että niiden tunnistaminen olisi tehokasta. Ja tehoton/virheellinen tunnistus voi johtaa monesti isompaan määrään vääriä hälytyksiä.

Vaikeammin havaittavien hyökkäyksien lisäksi tulevaisuudessa tekoälyä voidaan käyttää myös tunnistamaan ns. yksinkertaisempia hyökkäyksiä kuten kalasteluviestejä (Paloalto Networks 2024c). Niin yrityksiä kuin yksityishenkilöitä piinaavat tietojenkalasteluviestit voivat olla helpompia tunnistaa. Kuten Kuviossa 3 esitetään, näitä viestejä ja niissä olevia linkkejä klikkaillaan edelleen melko paljon ja useat kyberhyökkäyksetkin lähtevät liikkeelle kalasteluviesti kampanjasta. Jos jatkossa tekoäly pystyisi tunnistamaan ja tarvittaessa blokkaamaan haitallisen viestin ennen kuin se päätyy edes työntekijän nähtäville, säästyttäisiin tai ainakin vaikeutettaisiin hyökkäyksien toteuttamista (Paloalto Networks 2024c). Tämän lisäksi työssä

monesti mainitut Zero-Day hyökkäykset voivat olla myös paremmin tunnistettavissa tulevaisuudessa (Sangfor Technologies 2024). Nämä ovat kuten mainittu useasti, erittäin haastavia tunnistettavia ja se vaatisi todennäköisesti tekoälyltäkin melkoisen harppauksen eteenpäin, jotta sitä voitaisiin hyödyntää sillä osa-alueella.

Tekoälyä voitaisiin mahdollisesti hyödyntää tulevaisuudessa myös syväväärennösten (Deepfake) videoiden, kuvien ja äänien tunnistukseen (Paloalto Networks 2024c). Syväväärennökset ovat myös tekoälyn luomaa materiaalia ja niillä voi olla monia eri käyttötarkoituksia. Niillä voidaan pyrkiä rakentamaan erilaisia huijauksia, mutta työn kannalta merkittävämpänä sitä voidaan käyttää tietojenkalasteluun tai käyttäjien manipulointiin (Social Engineering). Sillä voitaisiin huijata yrityksen työntekijöitä lähettämään tietoja tai jopa siirtämään rahaa hyökkääjälle. Vaarallisen syväväärennnöksistä tekee sen, että niitä voi olla jopa vaikea tunnistaa, että onko se edes väärennös vai onko video tai ääni aito. (Fortinet 2024.)

Tekoälyn kehitys on johtanut yhä paremmin luotuihin väärennöksiin, mutta sitä voitaisiin myös hyödyntää niiden tunnistamiseen. Sitä voitaisiin käyttää ja voidaan jo tälläkin hetkellä hyödyntää erilaisissa tunnistustyökaluissa, jotka analysoivat videon tai kuvan ja etsivät niistä merkkejä väärennöksestä (Lenaerts-Bergmans 2024). Merkkejä ovat epäjohdonmukaisuudet, vaikka kasvoissa tai käsissä. Esimerkkinä voisin käyttää, vaikka videota, jossa pää, silmät ja suu liikkuvat mutta kaikki muu pysyy täysin paikallaan pitkän ajan. Vaikka tällaisia työkaluja on jo kehitetty, ei täysin vedenpitävää ratkaisua ole toistaiseksi löytynyt. Eli jokaisen tulee olla hereillä niin sosiaalisessa mediassa ja muissakin ympäristöissä ja olla tietoinen, että tämän tyyppistä materiaalia voidaan levittää eri käyttötarkoituksissa (Lenaerts-Bergmans 2024.) Tekoäly voisi olla tulevaisuudessa käänteentekevä, jos se saataisiin tunnistamaan väärennösten merkit riittävän hyvin.

Tulevaisuudessa tekoälyltä voidaan odottaa myös kehitystä sen kykyyn automatisoida tehtäviä. Työssä on tullut ilmi jo sen potentiaali tehdä niin, mutta tulevaisuus näyttää vasta, kuinka paljon sillä voidaan automatisoida erilaisia tehtäviä sekä kuinka paljon se tehostaa yritysten ja organisaatioiden toimintaa. Sillä voitaisiin automatisoida hälytyksiä ja niihin vastauksia, jos tilanne ei vaadi ihmisen väliintuloa. Automatisoinnin tarkoituksena on nopeuttaa tunnistusprosessia. (Sangfor Technologies 2024.) Tulevaisuudessa voidaan nähdä myös enemmän järjestelmiä, missä on sisäänrakennettuna tekoäly ominaisuudet. Tämän tyyppiset työkalut voisivat olla hyödyllisiä myös siten, että ne voisivat tehdä ehdotuksia järjestelmiin ja niiden säädöksiin esimerkiksi uusien määräysten astuessa voimaan, jotka koskettavat kyseisiä laitteita. (Bourzikas 2024.)

Tekoälyn pelätään tulevan ja vievän ison määrän työpaikkoja. Se ei välttämättä täysin pidä paikkaansa, mutta se voi kehittyessään vaikuttaa työpaikkoihin ja vähintään ihmisten työnkuvaan. Kyberturvallisuudessa se voisi tulevaisuudessa juuri mainittujen ominaisuuksien kuten

analysoinnin, automatisoinnin ja tehokkuutensa ansiosta tehdä matalamman tason työtehtäviä kuten verkkoliikenteen analysoinnin jne. Se voi tarkoittaa sitä, että vaatimustaso alalle nousee. Kun yksinkertaisemmat tehtävät jäävät enemmän tekoälyn tehtäväksi, niin sinne ei tarvita välttämättä yhtä paljon henkilökuntaa enää. Silloin ihmiset siirrettäisiin tekemään haastavampia tehtäviä, jotka vaativat myös enemmän kokemusta sekä yleistä osaamista. Osaamista tekoälyn ja koneoppimisen puolelta tullaan varmasti arvostamaan, koska jonkun tulee hallinnoida myös sitä puolta. (Bourzikas 2024.)

Työtehtävien lisäksi saattaa tulevaisuudessa tulla myös muutoksia siihen, miten tietoturvatiimit operoivat. Onko tarvetta valtavaan määrään työntekijöitä, joka työskentelee vuorokauden jokaisena tuntina? Osan työtehtävistä on pakko pyöriä jatkuvasti, mutta tarvitaanko niihin tehtäviin enää niin montaa ihmistä vai pystyisivätkö koneet hoitamaan osan näistä tehtävistä? Ihmisiä voitaisiin tässäkin tilanteessa keskittää kriittisempiin tehtäviin. Tekoälyn mukauttaminen haastaviin it-ympäristöihin tulee kuitenkin olemaan todennäköisesti myös tulevaisuudessa hankalaa. Mitä isommaksi osaksi kyberturvallisuutta tekoäly tulee, sitä enemmän yritykset joutuvat hallinnoimaan dataa. Yritysten ja tietoturvatiimien tulee noudattaa jo olemassa olevia ja tulevaisuudessa vielä uusia lakeja ja säädöksiä liittyen esimerkiksi sen varastointiin ja käyttöön. (Bourzikas 2024.) Tekoälyn kasvu ja sen tuomat tulevaisuuden mahdollisuudet eivät tule ilman haasteita.

11 Johtopäätökset

Opinnäytetyön perusteella voidaan sanoa, että tekoäly omaa merkittävän potentiaalin kyberuhkien tunnistamisessa. Se voisi tuoda tarvittavaa nopeutta ja tehokkuutta tunnistusprosessiin. Tekoälyn isoimmat hyödyt ovat sen nopeus esimerkiksi käydä läpi dataa, tehdä hälytyksiä ja priorisoida kriittisimmät tilanteet. Muita selkeitä hyötyjä ovat esimerkiksi mahdollinen yksinkertaisempien työtehtävien automatisointi ja helposti ymmärrettävien analyysien/raporttien tuottaminen, joita voitaisiin jakaa organisaation sisällä helpommin. Toistaiseksi iso osa sen potentiaalista on kuitenkin vielä tulevaisuudessa. Jotta sen edellä mainittuja ominaisuuksia saataisiin laajemmin käyttöön, pitää ratkaista vielä siihen liittyviä haasteita.

Isoimmiksi haasteiksi voitaisiin nostaa siihen liittyvä jatkuva koulutus, optimointi omiin ympäristöihin sekä sen eettiset ongelmat. Kaikkiin ongelmiin löytyy usein ratkaisu, mutta tässä tapauksessa esimerkiksi koulutuksen osalta se voi olla haastavaa. Erilaisten kyberhyökkäysten määrä on valtava ja siihen kouluttaminen on työlästä. Datan pitää olla laadukasta. Esimerkkejä erilaisista hyökkäyksistä pitää olla valtava määrä. Virheet materiaalissa tai sen puutteellisuus johtavat tehottomaan tunnistukseen. Silloin tekoälyn käytöstä ei hyödytä juurikaan. Optimointi voi olla myös haaste. Jos tekoälystä pyritään samaan todella herkkä tunnistamaan muuten vaikeasti havaittavia hyökkäyksiä, tulee myös vääriä hälytyksiä enemmän. Sen

säätäminen ei välttämättä ole niin yksinkertainen prosessi, kun voisi kuvitella. Myös sen ratkaisuntekoa voidaan kyseenalaistaa, jos se ei tuota jonkinlaista raporttia toiminnastaan. Esimerkiksi minkä tiedon pohjalta joku hälytys on tehty. Ilman tätä tietoa, kukaan ei tiedä oliko ratkaisu oikea. Tekoälyn mielestä se on aina oikein. Mutta se ei ymmärrä sitä, mitä sille ei ole koulutettu. Haasteita siis löytyy vielä.

Tekoälyn kehitystä kyberturvallisuudessa on hidastanut koko digimaailman nopea kehitys. Se ei kuitenkaan tarkoita sitä, etteikö siitä voisi tulla pysyvä ja tärkeä osa kyberturvallisuutta tulevaisuudessa. Hyökkääjät tulevat hyödyntämään tekoälyä hyökkäyksissään, joten sen jalostaminen myös osaksi puolustusta olisi varmasti edullista. Nähtäväksi kuitenkin jää miten isoon rooliin tekoäly tulee päätymään tulevaisuudessa ja mitä sen ainakin potentiaalisista hyödyistä saadaan tuotua käyttöön isommalle yleisölle.

Lähteet

Badman, A & Kosinski, M. 2024. What is network detection and response (NDR)? IBM. Viitattu 12.11.2024. https://www.ibm.com/topics/ndr

Bourzikas, G. 2024. Preparing for the future of AI in cyber security. theNET by Cloudflare. Viitattu 28.11.2024. https://www.cloudflare.com/the-net/building-cyber-resilience/preparing-ai-future/

Builtin 2024. Artificial Intelligence. Viitattu 2.8.2024. https://builtin.com/artificial-intelligence

CEO Monthly 2024. The Role of AI on DDoS Detection and Mitigation. Viitattu 8.11.2024. https://www.ceo-review.com/the-role-of-ai-in-ddos-detection-and-mitigation/

Cisco 2024a. What is cybersecurity? Viitattu 20.8.2024. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Cisco 2024b. What is a Cyberattack? Viitattu 21.8.2024. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Cloudflare 2024a. SYN flood attack. Viitattu 6.11.2024. https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Cloudflare 2024b. What is predictive AI? Viitattu 18.11.2024. https://www.cloudflare.com/learning/ai/what-is-predictive-ai/

Dhaliwal, J. The What, Why and How of AI and Threat Detection. McAfee. Viitattu 15.11.2024. https://www.mcafee.com/blogs/internet-security/the-what-why-and-how-of-ai-and-threat-detection/

EC-Council 2023. IDS and IPS: Understanding Similarities and Differences. Viitattu 6.11.2024. https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/

Fortinet 2024. What is a Deepfake? Viitattu 27.11.2024. https://www.fortinet.com/resources/cyberglossary/deepfake

Freed, A. M. 2024. Harnessing the Power of AI-Driven XDR. Cybereason. Viitattu 24.10.2024. https://www.cybereason.com/blog/harnessing-the-power-of-ai-driven-xdr

F-Secure 2024. Mikä on kyberhyökkäys? Viitattu 19.8.2024. https://www.f-secure.com/fi/articles/what-is-a-cyber-attack

F-Secure 2022. Mitä on tietojenkalastelu? Viitattu 5.12.2024. https://www.f-secure.com/fi/articles/what-is-phishing

Grady, J. 2023. How AI benefits network detection and response. TechTarget. Viitattu 13.11.2024. https://www.techtarget.com/searchsecurity/opinion/How-AI-benefits-network-detection-and-response

Huoltovarmuuskeskus 2022. Tekoäly tulee muuttamaan myös kyberhyökkäyksiä. Viitattu 17.7.2024.https://www.huoltovarmuuskeskus.fi/a/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia

IBM 2024. Cost of a Data Breach Report 2024. Viitattu 1.10.2024. https://www.ibm.com/reports/data-breach

IBM 2022. Data breach action guide. Viitattu 1.10.2024. https://www.ibm.com/reports/data-breach-action-guide

IBM 2021. IBM Report: Cost of a Data Breach Hits Record High During Pandemic. Viitattu 1.10.2024. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

IBM 2023. What is a zero-day exploit? Viitattu 14.11.2024. https://www.ibm.com/topics/zero-day

ISO 2024. What is artificial intelligence (AI)? Viitattu 3.8.2024. https://www.iso.org/artificial-intelligence/what-is-ai#toc9

Kaspersky 2024. Mikä on laajennettu tunnistus ja reagointi (XDR)? Viitattu 23.10.2024. https://www.kaspersky.fi/resource-center/definitions/what-is-xdr

Kosinski, M. & Lindemulder, G. 2024. What is Cybersecurity? IBM. Viitattu 20.8.2024. https://www.ibm.com/topics/cybersecurity

Kyberturvallisuuskeskus 2022. Toimintaohje – Palvelunestohyökkäys, 2. Viitattu 6.11.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

Lenaerts-Bergmans, B. 2024. What is a Deepfake Attack? CrowdStrike. Viitattu 27.11.2024. https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/deepfake-attack/?srsltid=AfmBOoq5mgrDJIUMlPepBXP4Vnku6iF3uRjSuKbv8sjhqfY7uGIWiTWW

Marchal, S., Nawrotek, B. & WithSecure. 2024. Tekoälypohjaiset kyberturvallisuusratkaisut. Kyberturvallisuuskeskus, 15–19. Viitattu 18.7.2024.https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Teko%C3%A4lypohjaiset%20kyberturvallisuusratkaisut_FI.pdf

Microsoft 2024a. Mikä kyberhyökkäys on? Viitattu 21.8.2024. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-a-cyberattack

Microsoft 2024b. What is AI for cybersecurity? Viitattu 27.8.2024. https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity#heading-oc4546

Microsoft 2024c. What is Threat Detection and Response (TDR)? Viitattu 6.9.2024. https://www.microsoft.com/en-ca/security/business/security-101/what-is-threat-detection-response-tdr

National Cyber Security Centre 2024. AI and cyber security: what you need to know. Viitattu 30.8.2024. https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know#section_4

Paloalto Networks 2024a. What Is the Role of AI in Threat Detection? Viitattu 12.9.2024. https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection

Paloalto Networks 2024b. What are the Risks and Benefits of Artificial Intelligence (AI) in Cybersecurity? Viitattu 18.11.2024. https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity#benefits

Paloalto Networks 2024c. What are Predictions of Artificial Intelligence (AI) in Cybersecurity? Viitattu 27.11.2024. https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity

Pratt, M. K. 2024. How AI could change threat detection. TechTarget. Viitattu 15.11.2024. https://www.techtarget.com/searchsecurity/tip/How-AI-could-change-threat-detection

Rapid7 2024. Threat Detection and Response. Viitattu 4.9.2024. https://www.rapid7.com/fundamentals/threat-detection/

Sangfor Technologies 2024. Role of Artificial Intelligence (AI) in Threat Detection. Viitattu 2.10.2024. https://www.sangfor.com/blog/cybersecurity/role-of-artificial-intelligence-ai-in-threat-detection

Scapicchio, M & Stryker, C. 2024. What is generative AI? IBM. Viitattu 26.11.2024. https://www.ibm.com/topics/generative-ai

Sennovate 2024. The role of artificial intelligence in detecting phishing attacks. Viitattu 24.9.2024. https://sennovate.com/the-role-of-artificial-intelligence-in-detecting-phishing-attacks/

Sibanda, I. 2023. Why we need advanced malware detection with AI-powered tools. ComputerWeekly.com. Viitattu 23.9.2024. https://www.computerweekly.com/feature/Why-we-need-advanced-malware-detection-with-AI-powered-tools

Skillfloor 2024. AI-Driven Threat Detection: The Future of Cybersecurity. Medium. Viitattu 4.10.2024. https://skillfloor.medium.com/ai-driven-threat-detection-the-future-of-cybersecurity-6293fb8bea01

Smith, G. 2024. Top Phishing Statistics for 2024: Latest Figures and Trends. StationX. Viitattu 28.10.2024. https://www.stationx.net/phishing-statistics/

Terranova Security 2024. AI in Cyber Security: Pros and Cons, and What it Means for Your Business. Viitattu 25.11.2024. https://www.terranovasecurity.com/blog/ai-in-cyber-security

The Big Sleep team. 2024. Project Zero. Google Project Zero. Viitattu 14.11.2024. https://googleprojectzero.blogspot.com/2024/10/from-naptime-to-big-sleep.html

Vectra AI 2024a. Network Detection and Response (NDR). Viitattu 12.11.2024. https://www.vectra.ai/topics/network-detection-and-response

Vectra AI 2024b. Zero Day. Viitattu 14.11.2024. https://www.vectra.ai/topics/zero-day

Watson, K. M. 2024. The Benefits of Cyber Security and AI. PentestPeople. Viitattu 15.11.2024. https://www.pentestpeople.com/blog-posts/the-benefits-of-cyber-security-and-ai

Whitfield, B. 2023. What is the Turing test? Builtin. Viitattu 22.11.2024. https://builtin.com/artificial-intelligence/turing-test

Kuviot

Kuvat