Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TOMI JOKINEN

Tekoäly ja kyberturvallisuus

Tekoälyn hyödyntäminen kyberturvallisuudessa

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2025

TIIVISTELMÄ

Jokinen, Tomi: Tekoäly ja kyberturvallisuus: Tekoälyn hyödyntäminen kyberturvallisuudessa
Opinnäytetyö, AMK
Tietojenkäsittely
Marraskuu 2025
Sivumäärä: 38

Tässä opinnäytetyössä tutkitaan tekoälyn hyödyntämistä kyberturvallisuudessa, erityisesti uhkien havaitsemisessa ja torjunnassa. Työ tarkastelee tekoälyn roolia tunkeutumisen tunnistus- ja estojärjestelmissä (IDS/IPS), laajennetuissa havaitsemis- ja reagointijärjestelmissä (XDR/SIEM) sekä Zero Trust -mallissa. Lisäksi käsitellään tekoälyyn liittyviä haasteita, kuten väärien hälytysten hallintaa, eettisiä kysymyksiä ja mahdollista väärinkäyttöä kyberhyökkäyksissä. Työ tarjoaa katsauksen alan tutkimukseen ja käytännön sovelluksiin sekä esittelee tekoälyn potentiaalin kyberturvallisuuden kehittämisessä.

Avainsanat: tekoäly, kyberturvallisuus, IDS, IPS, XDR, SIEM, Zero Trust

ABSTRACT

Jokinen, Tomi: AI and cybersecurity: utilizing AI in cybersecurity
Bachelor's thesis
Business Information Systems
November 2025
Number of pages: 38

This thesis explores the utilization of artificial intelligence (AI) in cybersecurity, specifically in threat detection and prevention. The study examines AI's role in intrusion detection and prevention systems (IDS/IPS), extended detection and response (XDR/SIEM) solutions, and the Zero Trust security model. Additionally, it discusses challenges related to AI, such as managing false positives, ethical concerns, and potential misuse in cyberattacks. The research provides an overview of current studies and practical applications, highlighting AI's potential in advancing cybersecurity measures.

Keywords: artificial intelligence, cybersecurity, IDS, IPS, XDR, SIEM, Zero Trust

SISÄLLYS

SYMBOLI- JA LYHENNELUETTELO

CIA – Confidentiality Integrity Availability. Tietoturvan kolme tavoitetta (suomeksi luottamuksellisuus, eheys ja saatavuus), jotka yksinkertaisuudestaan huolimatta, ovat vaikeasti saavutettavissa.

IDS – Intrusion Detection System. Järjestelmä, minkä tarkoitus on havaita ja hälyttää haitallisesta liikenteestä verkossa.

IPS – Intrusion Prevention System. Järjestelmä, minkä tarkoitus on havaita, hälyttää ja estää haitallinen liikenne tai hyökkäys verkossa.

SIEM – Security Information and Event Management. Järjestelmä, mikä mahdollistaa reaaliaikaisen analyysin sovellusten tekemistä kyberturvahälytyksistä.

XDR – Extended Detection and Response. Kokonaisvaltainen suojausratkaisu, joka lyhentää vastausaikaa useissa eri kuormituksissa automaation ja tekoälyn avulla.

FPR – False Positive Rate. False positive tarkoittaa tapausta, jossa IDS ilmoittaa haitallisesta hyökkäyksestä, vaikka liikenne olisi normaalia. FPR mittaa ja vertaa näiden tapausten määrää muihin ilmoituksiin.

FNR – False Negative Rate. False negative tarkoittaa tapausta, kun IDS luulee liikennettä normaaliksi, vaikkakin todellisuudessa kyseessä on hyökkäys. FNR mittaa ja vertaa näiden tapausten määrää muihin ilmoituksiin.

Fuzzy logic – Sumea logiikka. Matemaattisen logiikan laajennus, jossa muuttujien totuusarvot voivat olla mikä tahansa reaaliarvo nollan ja yhden välillä.

1 JOHDANTO

”On olemassa kahdenlaisia yrityksiä: Niitä, jotka tietävät tulleensa hakkeroiduksi ja niitä, jotka eivät vielä tiedä tulleensa hakkeroiduksi.” (Ozkaya, 2019, s. 17)

Kyberturvallisuus koostuu lukuisista ohjelmistoista ja toimenpiteistä, joiden avulla suojataan IT-laitteita ja tietoa erilaisilta uhilta, kuten hyökkäyksiltä, häiriöiltä ja muilta vaaroilta. Viime vuosina kyberturvallisuuden merkitys on kasvanut huomattavasti niin yksityishenkilöiden, yritysten kuin valtioidenkin puolustautuessa yhä kehittyvämpiä uhkia vastaan. (F-Secure, n.d.)

Tekoäly ja kyberturvallisuus ovat kaksi keskeistä tietoteknologian osa-aluetta, joiden merkitys kasvaa jatkuvasti digitalisoituvassa maailmassa. Tekoälyn monipuoliset sovellusmahdollisuudet ja kyberturvallisuuden kriittinen rooli organisaatioiden toiminnassa tekevät niiden yhdistämisestä entistäkin kiinnostavamman ja hyödyllisemmän vaihtoehdon. (Ozkaya, 2019, s. 36.)

Tekoäly on monitahoinen ja monimutkainen tietotekninen järjestelmä, joka kykenee suoriutumaan vaativista tehtävistä, joihin perinteisesti on tarvittu ihmisen älykkyyttä ja päätöksentekokykyä. Koneoppiminen on keskeinen osa tekoälyjärjestelmiä, sillä se mahdollistaa järjestelmän jatkuvan oppimisen ja kehittymisen kokemuksen ja datan avulla. (Parisi, 2019, s. 9)

2 TYÖN TAVOITTEET JA AIHEALUE

Opinnäytetyö sai ideansa konttiteknologian kurssilla. Aluksi mietin, miten voisin yhdistää konttiteknologian ja kyberturvallisuuden. Opinnäytetyön aihe kuitenkin hieman muuttui ja tarkentui ja sai lopullisen aiheensa tapaamisessa Satakunnan ammattikorkeakoulun tietohallintopäällikön ja kyberturvavastaavan kanssa. Aihe on erittäin ajankohtainen, tietoturvallisesti tärkeä ja mahdollisesti jopa yritysidean arvoinen. Kyberturva on aiheena kiinnostanut minua jo pitkään ja lähdin tutkimaan tekoälyn mahdollisuuksia yleisemmin kyberturvan ja tarkemmin IDS/IPS, XDR/SIEM, WormGPT ja Zero Trust kohdalla.

Työn on tarkoitus toimia yleisenä tutkimuksena, ohjeena ja esimerkkinä potentiaalisista sovelluskohteista. Työ jättää hyvin tilaa jatkaa käytännön testejä, joissa voidaan tutkia lisää tekoälyratkaisuiden toimivuutta ja tehokkuutta yrityksessä.

Työn toimeksiantaja on Satakunnan ammattikorkeakoulu. Siinä käsitellään kyberturvakysymyksiä ja annetaan neuvoja sekä potentiaalisia ratkaisuja tekoälyn hyötykäytön kannalta. Työn tavoitteena on vastata seuraaviin kysymyksiin:

- Mitä mahdollisuuksia ja hyötyjä tekoäly tuo kyberturvallisuudelle?
- Miten tekoäly toimii ja oppii sekä mikä on sen vaikutus yrityksen tulevaisuuteen uhkien havaitsemisessa ja niiden estämisessä?
- Miten hyödyntää tekoälyä tietoverkon valvonnassa ja kyberturvallisuuden parantamisessa?

Työssä tutkitaan tarkemmin kahta asiaa: tekoälyn käyttöä kyberturvassa, erityisesti tunkeutumisen tunnistus- ja estojärjestelmissä sekä laajennetuissa havaitsemis- ja reagointijärjestelmissä, että tekoälyn käyttöä Zero Trust -käytännöissä ja -toteutuksissa. Työstä karsittiin paljon tekoälyä koskevia turhia aiheita, jotka eivät ole tärkeitä tai työtä koskevia eivätkä tuo työlle aiheellista arvoa. Kyberturvan ja tekoälyn perustietoja tai aiheita ei tässä työssä käsitellä.

3 TEKOÄLY

Tekoäly ei ole yksittäinen ohjelma, se on monia tekniikoita kokoava kattotermi, jolla pyritään matkimaan ihmismäisiä kykyjä. Tekoäly on hyvä apu ihmisten käyttäytymisen analysoinnissa ja mallintamisessa, jonka jälkeen voidaan tehdä esimerkiksi parempia päätöksiä. Tekoäly on halpa ja väsymätön monia käyttötarkoituksia tarjoava apuväline. (Järvinen, 2023, s. 48)

Koska tekoäly itsessään on ohjelmakoodia, on ohjelmoiva tekoäly hyvin kiehtova ajatus. Tekoäly voikin tutkia itse itseään ja parannella omaa koodiaan. Tekoäly siis ohjelmoisi itsestään aina vaan paremman ja paremman version. Nopeasti emme enää ymmärtäisi, miten tällainen itseään parannellut tekoäly toimii. (Hyppönen, 2021, s. 273.)

Yksinkertaistettuna tekoäly on koneiden suorittama toiminta, joka pyrkii jäljittelemään ihmisen älykkyyttä. Vaikka tekoäly ei vielä ole varsinaisesti älykkyyttä, se on suunniteltu ratkaisemaan tiettyjä ongelmia. Koneoppiminen on yleisin tapa toteuttaa tekoälyä. Siinä tekoäly oppii syötetyn datan pohjalta tekemään johtopäätöksiä ilman ennalta määriteltyä tavoitetta. (Vähä-Sipilä ym., 2021, s.1)

Yritysjohtajat ovat raporttien mukaan laajalti omaksumassa tekoälyä kyberturvallisuuden työkaluksi. Jopa 93 % heistä hyödyntää tekoälyä tai harkitsee sen käyttöönottoa kyberturvallisuuden parantamiseksi. Tämä osoittaa selvästi, että tekoäly nähdään yhä tärkeämpänä osana yritysten tietoturvastrategiaa. (Muppidi ym., 2022)

Tekoäly usein jaetaan tieteellisessä kirjallisuudessa kyvykkyyden ja ominaisuuksien pohjalta kahteen päätyyppiin: heikkoon tekoälyyn ja vahvaan tekoälyyn. Heikko tekoäly (narrow AI) on Fein ym. (2022) ja Goertzellin (2014) mukaan tietojenkäsittelyjärjestelmä, joka on suunniteltu niin että se suorittaa vain tiettyjä tehtäviä ja tietyissä rajoissa. Tällaisesta heikosta tekoälystä esimerkkejä olisivat kasvojentunnistus- ja puheentunnistusohjelmat, useiden muiden lisäksi. Vahva tekoäly (strong AI) taas puolestaan tarkoittaa tietojenkäsittelyjärjestelmää, joka kykenee matkimaan ihmistä ja suorittamaan älykkäitä toimintoja. (Fei ym., 2022; Goertzel, 2014). Vahvaa tekoälyä ei tämänhetkisen tutkimustiedon valossa ole kehitetty. Sen kehittäminen kuitenkin näyttäisi olevan yksi tekoälytutkimuksen tavoitteista. (Hamet & Tremblay, 2017; Russell & Norvig, 2010; Vähäkainu & Neittaanmäki, 2018; Wiafe ym., 2020).

Tekoäly ja koneoppiminen ovat mullistaneet tapamme lähestyä kyberturvallisuutta. Aiemmin kyberturvatehtävät olivat pääasiassa ihmisten vastuulla, aina järjestelmien kehittämisestä niiden ylläpitoon ja päivitykseen. Tämä on kuitenkin muuttumassa nopeasti. Teknologia kehittyy jatkuvasti, eikä kehityksen hidastumisesta ole merkkejä. Tekoälystä onkin tullut yksi keskeisimmistä tekijöistä kyberturvallisuudessa. (Ozkaya, 2019, s. 36)

Tekoälypohjaiset kyberturvajärjestelmät ovat nousseet keskiöön nykyajan digitaalisessa maailmassa. Yritykset ja organisaatiot hyödyntävät turvajärjestelmiä torjuakseen ja mitigoidakseen turvallisuusuhkia, vakoilua ja erilaisia muita kyberuhkia. Kyberturvallisuuden ammattilaisille koneoppiminen ja tekoäly tarjoavat vanhoja työkaluja tehokkaampia ratkaisuja uhkien havaitsemiseen ja torjumiseen. (Ozkaya, 2019, s. 36)

Itsenäisesti toimivien työkalujen käyttöönotto, jotka kykenevät havaitsemaan, pysäyttämään tai estämään uhkia, niin ettei ihmisen tarvitse toimia, ovat edellytys sekä tekoälyn että koneoppimisen ottamiseen hyötykäyttöön kyberturvallisuudessa. Näiden työkalujen käyttö mahdollistaa nopean reagoinnin ja vähentää ihmisistä johtuvien virheiden riskiä. Tekoälyn perustuessa koneoppimiseen, tekee siitä oppivan ja jatkuvasti kehittyvän järjestelmän. (Ozkaya, 2019, s. 36)

Uhkiin reagoiminen ja niiden havaitseminen perustuu tekoälyn kouluttamiseen, jonka suojaustyökalun algoritmi on suorittanut itsenäisesti kehittäjien toimittaman datan perusteella. Tekoälypohjainen kyberturvatyökalu oppii koko elinkaarensa ajan havaitsemaan uhkia yhä paremmin. Alkuperäinen tietojoukko uhista toimii kehittäjien tarjoamana viitekehyksenä, jonka avulla tekoäly oppii erottamaan normaalit ja haitalliset toiminnot. (Ozkaya, 2019, s. 36)

Tekoälyä hyötykäyttävien työkalujen ottaminen käyttöön on mullistanut yrityksien ja organisaatioiden suojata tietojaan. Työkalujen tarjoama teknologia mahdollistaa entistä tehokkaampaa kyberturvaa ja sallii yrityksille nopeamman reagoinnin kyberhyökkäyksiin. Tekoälyn kehitys ei kuitenkaan saa johtaa muiden kyberturvatoimien laiminlyöntiin. On ensiarvoisen tärkeää jatkaa kyberturvallisuuden parantamista ja pysyä ajan tasalla uusista uhkakuvista. (Ozkaya, 2019, s. 37)

Koneoppimista ja tekoälyä on hyödynnetty tietoturvayrityksissä jo vuosia. Hyökkääjät eivät kuitenkaan vielä käytä tekoälyä yhtä laajasti tai tehokkaasti hyökkäyksissään. Tekoälyn hyödyntäminen verkkohyökkäyksissä on toistaiseksi lähinnä korkeakoulujen ja tietoturvayritysten tutkimusten aihe, eikä niinkään todellisten hyökkäysten väline. Yksi mahdollinen syy tähän on se, että tekoälyosaamisesta maksetaan hyvin, joten osaajat työllistyvät helposti laillisiin tehtäviin. Tekoälyosaajista onkin huutava pula. Kynnys tekoälyn käyttämiseen kuitenkin madaltuu jatkuvasti, ja osaajien määrän kasvaessa tekniikka tulee väistämättä yleistymään myös hyökkäysten toteuttamisessa. (Hyppönen, 2021, s. 276).

Väärät positiiviset tulokset ja erityisesti niiden hallinta on yksi merkittävimmistä haasteista, etenkin kyberuhkia havaitsevan tekoälyn kohdalla. Väärin havaitut positiiviset voivat johtaa niin suureen määrään havaittuja uhkia, että ne kuluttavat kaikki henkilöresurssit. Ongelmaa voidaan kuitenkin lieventää optimoimalla opetusmenetelmiä, jolloin analysoitavien tulosten määrä vähenee merkittävästi. (Parisi, 2019, s. 28)

Kosken (2018) mukaan tekoälyn kehitys ja tutkimus ottivat 2000-luvulla uuden suunnan, kun neuroverkkoihin perustuva syväoppiminen nousi keskiöön. Syväoppimisen mahdollistajina toimivat tietokoneiden prosessointitehon kasvu ja lisääntynyt saatavilla olevan datan määrä. Myös Ventren (2020) mukaan 2010-luku on ollut tekoälyn kulta-aikaa, ja hänkin näkee big datan ja kasvaneen prosessointitehon keskeisinä mahdollistajina.

3.1 Koneoppiminen (Machine learning)

Yksi tekoälyn useista eri osa-alueista on koneoppiminen. Koneoppimisella tarkoitetaan sovelluksen kykyä kehittää toimintaansa oppimalla siihen syötetystä datasta niin, ettei toimintaa ole kokonaan ennalta siihen ohjelmoitu. (Kolari & Kallio, 2023, s. 128)

Voimme jakaa koneoppimisen kolmeen kategoriaan: ohjattu oppiminen, ohjaamaton oppiminen ja vahvistusoppiminen. (Parisi, 2019, s. 11; Kolari & Kallio, 2023, s. 129; IBM, 2023a).

Ohjatussa oppimisessa tavoitteena on löytää tietokoneelle kuin suinkin tarkat säännöt ja sääntöjoukko, jolla määritellään syötteiden muuntaminen tuloksiksi. Ohjelmaan syötetään valtavasti syötteistä ja toivotuista tuloksista koostuvaa esimerkkidataa. Tietokoneen tavoitteena on löytää syötteiden ja haluttujen tulosten välille yhteyden ja kehittää algoritmi, joka tuottaa halutunlaisen oikean tuloksen syötetyillä syötteillä. Ohjatussa oppimisessa käytetäänkin valmiiksi tehtyjä esimerkkejä ja ohjausta, mahdollistaen tietokoneen oppiminen tunnista ja luokitella erilaisia tietoja sille annetuilla uusilla menetelmillä. (Parisi, 2019, s. 12; Kolari & Kallio, 2023, s. 129; IBM, 2023a)

Ohjaamattomassa oppimisessa tietokoneen tehtävänä on oppia luokittelemaan dataa niin, ettei sille ole syötetty aikaisempia tulostusesimerkkejä, toisin kuin ohjatussa oppimisessa. Tekoälyohjelma itse etsii automaattisesti rakenteita ja malleja datasta, pyrkien tunnistaa rakenteita ilman, että sille on syötetty selkeitä ohjeita. Kyberturvallisuudessa ohjaamaton oppiminen on erityisen

tärkeää, sillä rikollisten käyttämät hyökkäykset kehittyvät jatkuvasti, eikä seuraavaa hyökkäystä voida varmuudella tietää etukäteen. (Parisi, 2019, s. 13; Kolari & Kallio, 2023, s. 130; IBM, 2023b)

Vahvistetussa oppimisessa tietokoneelle ei välttämättä anneta lainkaan opetusdataa. Tekoäly oppii yritysten, erehdysten ja toimien seurauksien kautta oppimaan ja tekemään päätöksiä. Tekoäly "motivoidaan" palkkioilla toistamaan toivottua toimintaa ja negatiivisilla palkkioilla välttämään ei-toivottua toimintaa. "Motivointia" voidaankin pitää tavoitteiden asettamisena, jossa algoritmi pyrkii maksimoimaan kertaantuvan palkinnon pitkällä aikavälillä. (Parisi, 2019, s. 13)

Puoliksi valvottu oppiminen on hyödyllinen menetelmä tilanteissa, joissa hankalasti merkattavia datasettejä on paljon. Algoritmi hyödyntää sekä merkkaamattomia että merkattuja datasettejä oppiakseen tietyn funktion. Se hyödyntää kolmea oletusta datan lukemisessa: ryhmittelyä, jatkuvuutta ja moninaisuutta. Näiden avulla kone tekee päätöksiä datan suhteen. Tavoitteena on yhdistää parhaat puolet valvotusta ja epävalvotusta oppimisesta. (Geeksforgeeks, 2023)

3.2 Syväoppiminen (Deep learning)

Syväoppimisessa on yksi merkittävä ero muihin tekoälyn osa-alueisiin verrattuna: yleistason algoritmien hyödyntäminen neuroverkoissa. Tämä tarkoittaa, että erinäisissä yhteyksissä käytetään useita yleisiä algoritmeja syväoppimiseen, ja neuroverkkojen avulla tekoälyyn lisätään useita prosessoivia kerroksia. Nämä kerrokset ovat yhteydessä toisiinsa ja pyrkivät jäljittelemään ihmisaivojen toimintaa. Kaikille kerroksille välitetään sama tehtävä tai ongelma ja jokainen kerros yrittää löytää oman ratkaisun. Saavutettuaan ratkaisun tai umpikujan, kerrokset jakavat tietonsa toisilleen tavoitteenaan saavuttaa haluttu lopputulos. Tyypillisiä syväoppimisen sovelluskohteita ovat puheentunnistus, videoiden poikkeavuuksien havainnointi ja luonnollisen kielen prosessointi. (Parisi, 2019, s. 44–45; Kolari & Kallio, 2023, s. 131–134)

Syväoppiminen erottuu perinteisestä koneoppimisesta myös käyttämällä monimutkaisempia matemaattisia malleja ja lineaarialgebraa. Tämän ansiosta syväoppimisella voidaan saavuttaa parempia ja tarkempia tuloksia, ja sen algoritmit ovat uudelleenkäytettävämpiä kuin perinteisessä koneoppimisessa. Syväoppimisessa tekoäly kykenee neuroverkkojen kerroksia hyödyntämällä sulauttamaan tietoa ja rakentamaan tiedosta uusia tietojoukkoja. Tekoäly ei näin ollen vain lue sille syötettyä dataa. Tekoälyn syvyys ja sen kyky yhdistellä syötteitä on sitä suurempi mitä useampia kerroksia syväoppimisessa käytetään. Näin ollen ja sitä paremmin tekoälyn onnistuu yhdistellä syötteitä eri tasoilta ja tuottaa siten parempia lopputuloksia. (Parisi, 2019, s. 222–223)

Merkittävä koneoppimisen osa-alue on syväoppiminen, joka hyödyntää erittäin suuria datasettejä, neuroverkkoja ja useita eri algoritmeja. Hyperparametrien avulla voidaan muokata neuroverkon rakennetta, kuten piilotettuja kerroksia, jotka sijaitsevat sisääntulo- ja ulostulokerroksen välissä. Useimmiten suuri määrä piilotettuja kerroksia parantaa tekoälyn suorituskykyä. Syväoppimisessa voidaan käyttää useita erilaisia arkkitehtuureja eri tarkoituksiin, kuten MLP, CNN, RNN ja LSTM. Esimerkiksi CNN soveltuu videomateriaalin tunnistamiseen ja esineiden ennustamiseen, kun taas LSTM pystyy myös ennustamaan videomateriaalista. Näitä arkkitehtuureja voidaan myös yhdistellä tietyn tehtävän ratkaisemiseksi. (Campesato, 2020, s. 19, 100–110)

4 KYBERTURVA

CISCO:n entisen pääjohtajan John Chambersin (2023) mukaan yritykset jakautuvat kahteen leiriin: niihin, jotka on hakkeroitu, ja niihin, jotka eivät vielä tiedä joutuneensa hakkeroinnin kohteeksi. Suurin osa rikollisista tavoittelee rahaa erilaisten kiristysohjelmien avulla, jotka pakottavat uhrin maksamaan lunnaita tietojen palauttamiseksi. Vaikka suuremmat yritykset ovat usein

kyberuhkien kohteena, myös yksityishenkilöiden tiedot ovat vaarassa julkisissa verkoissa. (University of North Dakota, 2023)

Yhdysvaltalaisen Forbes-lehden artikkelissa helmikuulta 2023 Satish Shetty toteaa, että koronan jälkeen etätöiden tekeminen jatkaa kasvuaan, mikä luo uusia haasteita kyberturvallisuudelle jo nyt ja erityisesti tulevaisuudessa. Erityisesti pilvipalveluiden ja IoT-laitteiden käytön yleistyminen sekä tekoälyn kasvava rooli lisäävät kyberhyökkäysten mahdollista pinta-alaa. (Shetty, 2023)

Kyberturvallisuus on tekoälyn tavoin laaja käsite, jonka tarkasta määritelmästä on erilaisia näkemyksiä. Opinnäytetyössä käytetyn aineiston perusteella kyberturvallisuudella tarkoitetaan kuitenkin pääasiassa kaikkia niitä toimenpiteitä, joilla pyritään suojaamaan tietoteknisiä järjestelmiä, verkkoja, laitteita, ohjelmistoja, tietoja ja tiedostoja tietoturvauhilta, jotka kohdistuvat järjestelmiin yhden tai useamman hyökkäysvektorin kautta. Vaikka kyberturvallisuus usein rinnastetaan tietoturvallisuuteen, niiden tavoitteissa on selkeä ero. Kyberturvallisuus on monitieteellinen ala, joka yhdistää tietotekniikan, tietoturvan, tiedonhallinnan, riskienhallinnan ja juridiset näkökulmat. (Craigen, 2014; Ozkaya, 2019; Padallan, 2019; Zeadally, 2020; Järvinen, 2018)

4.1 Uhat ja niiden torjunta

CrowdStrike, johtava kyberturvallisuusyritys tarjoaa pilvipohjaisia ratkaisuja kyberuhkien havaitsemiseen, ennaltaehkäisyyn ja torjuntaan, listaa vuoden 2023 merkittävimmiksi kyberuhkiksi haittaohjelmat, palvelunestohyökkäykset, tietojenkalastelun, spoofing-hyökkäykset, identiteettivarkaudet, koodi-injektiot, toimitusketjuhyökkäykset, sisäpiirin uhat, DNS-tunneloinnin sekä IoT-laitteisiin kohdistuvat hyökkäykset. (Baker, 2023)

Kybermaailmaa on kutsuttu sodankäynnin viidenneksi ulottuvuudeksi maan, meren, ilman ja avaruuden rinnalle. Maailmanlaajuisesti on kehitetty keinoja globaalin tietoliikenteen seurantaan ja analysointiin. Esimerkiksi Yhdysvallat määritteli kyberuhat, jo vuonna 2013, vakavimmaksi uhaksi omalle kansalliselle turvallisuudelleen. (Limnéll ym. 2014, s. 13-25)

Uusia, kehittyneitä uhkia ilmaantuu jatkuvasti, mikä asettaa käyttäjät, yritykset ja hallitukset jatkuvan paineen alle. Tämä on johtanut vakavaan kyberturva-asiantuntijoiden pulaan. Lisäksi kyberuhkien aiheuttamien vahinkojen ennustetaan kasvavan 10 biljoonaan dollariin vuoteen 2025 mennessä. Esimerkiksi kryptovaluutat, pilvipalvelut, esineiden internet, kiristysohjelmat ja haavoittuvat hybridityöympäristöt ovat näihin uhkiin liittyviä hyökkäysvektoreita. (Moore, 2023)

Kyberuhat ovat Craigen ym. (2014), Ozkayan (2019) ja Uman ja Padmavathin (2013) mukaan tarkoituksellisia toimia, jotka kohdistuvat tietoteknisiin järjestelmiin ja verkkoihin, tarkoituksena on aiheuttaa vahinkoa tai häiriötä. (Taulukko 1.) Kyberuhkien määrä, laajuus ja monipuolisuus mahdollistavat niiden kohdistamisen yksittäisiin tietokoneisiin, yritysten tai organisaatioiden tietoverkkoihin tai järjestelmiin, kriittiseen infrastruktuuriin tai jopa valtioiden turvallisuuteen. Kyberuhkien muodot ja vaikutukset vaihtelevat suuresti, aiheuttaen esimerkiksi taloudellisia tappioita, yksityisyyden menetyksiä, henkilökohtaisia vahinkoja tai jopa vaarantaen kansallisen turvallisuuden. (Craigen ym., 2014; Enisa, 2021; Ozkaya, 2019; Uma & Padmavathi, 2013)

Taulukko 1. Kyberuhkien luokittelu (Sippola, 2023)

Kyberuhkien luokittelu	Näkökulma	Esimerkit
Hyökkäysmenetelmän mukaan	Millä tavalla hyökkäys tapahtuu?	Haittaohjelmat, tietomurrot, tietojenkalastelu, palvelunestohyökkäys (DoS)(Fischer, 2016; Heim & Wessel, 2023; Tang ym., 2023; Uma & Padmavathi, 2013)
Vaikutuksen mukaan	Millaisia vaikutuksia hyökkäys aiheuttaa?	Tietojen varastaminen tai tuhoutuminen, palvelun estyminen, verkon tai järjestelmän kaatuminen (Fischer, 2016; Heim & Wessel, 2023; Tang ym., 2023; Uma & Padmavathi, 2013)
Kohteen mukaan	Mikä/kuka on hyökkäyksen kohteena?	Yksittäiset tietokoneet, yritykset, kriittinen infrastruktuuri, valtiot (Fischer, 2016; Heim & Wessel, 2023; Tang ym., 2023; Uma & Padmavathi, 2013)
Tavoitteen mukaan	Mikä on hyökkääjän motiivi?	Taloudellisen hyödyn tavoittelu, vakoilu, sabotointi, poliittinen agendojen edistäminen (Fischer, 2016; Heim & Wessel, 2023; Tang ym., 2023; Uma & Padmavathi, 2013)

Kuinka kyberuhkilta sitten voidaan suojautua? Useita erilaisia tapoja, menetelmiä ja tekniikoita on perinteisesti hyödynnetty kyberuhkien torjunnassa uhkien luonteen mukaan. Lezzin ym. (2018) tutkimuksen mukaan tietoturvaohjelmistot ovat keskeinen osa tietoturvan perustaa. Näitä ohjelmistoja, kuten palomuureja, virustorjuntaohjelmistoja ja roskapostisuodattimia, käytetään suojaamaan tietokonejärjestelmiä erinäisiltä uhilta kuten esimerkiksi haittaohjelmilta ja viruksilta. (Lezzi ym., 2018; Ozkaya, 2019; Padallan, 2019)

Yksi keskeinen ja erittäin tärkeä menetelmä on käyttäjien eli ihmisten koulutus ja heidän tietoisuutensa lisääminen kyberuhista. Kuten Mosteanu (2020) monien muiden ohella on todennut, useimmiten käyttäjät ovat heikoin lenkki tietoturvassa. Onkin ensiarvoisen tärkeää kehittää käyttäjien osaamista. Tämä sisältää esimerkiksi salasanakäytäntöjen ja tietojen jakamisen ohjeistuksen sekä käyttäjämanipulaation tunnistamisen opettamisen. (August ym., 2022; Mosteanu, 2020; Ozkaya, 2019)

Tietoturva-aukkojen paikkaaminen on myös perinteinen ja tärkeä menetelmä (August ym., 2022; Lezzi ym., 2018). Tietoturva-aukot ovat sovellusten, ohjelmistojen tai järjestelmien haavoittuvuuksia, joita hyödyntämällä hyökkääjä voi päästä käsiksi tietokonejärjestelmään. Turva-aukkojen ja haavoittuvuuksien korjaaminen edellyttää säännöllistä päivitysten asentamista. On kuitenkin huomattava, että ohjelmistopäivityksiin liittyy aina myös potentiaalisia riskejä, jos ne aiheuttavat odottamattomia ongelmia monimutkaisissa järjestelmissä (Vuorinen & Tetri, 2016). Esimerkiksi Adams (2010) raportoi tapauksesta, jossa McAfeen virustorjuntaohjelmisto luuli Windowsin prosessiin liittyvää osaa haittaohjelmaksi, mikä johti järjestelmien kaatumiseen. Tässä tapauksessa tietoturvan periaatteet eivät toteutuneet, sillä tiedot eivät olleet käyttäjän saatavilla järjestelmän kaatuessa. Neljäntenä tärkeänä keinona kyberuhkien varalta pidetään tietojen varmuuskopiointia, joka mahdollistaa tietojen nopean palauttamisen vahingon sattuessa. Varmuuskopioinnilla voidaan merkittävästi vähentää kyberhyökkäysten aiheuttamia haittoja, kuten liiketoiminnan keskeytymistä tietojen katoamisen vuoksi. (August ym., 2022; Lezzi ym., 2018; Ozkaya, 2019)

4.1.1 Tunkeutumisen tunnistus- ja estojärjestelmät (IPS, IDS)

Tunkeutumisen tunnistusjärjestelmän (IDS) tehtävä on valvoa tietoverkkoa ja järjestelmää ja havaita niissä haitallinen liikenne. Poikkeavuuksista ilmoitetaan usein joko suoraan järjestelmänvalvojalle tai SIEM-järjestelmään tai molemmille. IDS analysoi ja vertaa dataa ennalta määritettyihin sääntöihin ja täten tunnistaa haitallisen liikenteen. Tunkeutumisen tunnistusjärjestelmiä on viisi erilaista:

1. Network Intrusion Detection System, verkkotason tunkeutumisen tunnistusjärjestelmä (NIDS): Tämä strategisesti sijoitettu ohjelma tarkkailee koko aliverkon ja kaikkea sen liikennettä. Usein NIDS on palomuurin läheisyydessä yhdistettynä siihen, kuitenkin itsenäisenä ohjelmana. NIDS voidaan kuitenkin myös integroida reitittimiin tai kytkimiin. NIDS vertailee liikennettä tunnettuihin

hyökkäyksiin reaaliajassa ja ilmoittaa mahdollisista uhista järjestelmänvalvojalle. (Pankaj, GeeksforGeeks, 2025)

2. Host-Based Intrusion Detection System, isäntätason tunkeutumisen tunnistusjärjestelmä (HIDS): Toimintaperiaatteeltaan samankaltainen kuin NIDS, erona kuitenkin, että HIDS on asennettu suoraan isäntälaitteisiin. HIDS tarkkailee laitteen verkkopaketteja ja vertailee laitteen nykyistä järjestelmätiedostojen tilannekuvaa aiempaan. Eroavaisuuksien ilmetessä se lähettää hälytyksen järjestelmänvalvojalle. HIDS-järjestelmät voivat olla hieman hitaampia ja vähemmän kustannustehokkaita kuin NIDS, mutta ne ovat välttämättömiä monissa kriittisissä järjestelmissä. (Rapid7, 2020)

3. Hybrid Intrusion Detection System, hybridi tunkeutumisen tunnistusjärjestelmä**:** Kuten nimestä voi päätellä, tämä järjestelmä yhdistää NIDS:n ja HIDS:n ominaisuudet yhdeksi kokonaisuudeksi, tarjoten valvojalle kattavan kuvan verkosta. Näin molemmat järjestelmät täydentävät toisiaan. (GeeksforGeeks, 2025)

4. Protocol-Based Intrusion Detection System, protokollapohjainen tunkeutumisen tunnistusjärjestelmä (PIDS)**:** Tämä järjestelmä asennetaan usein verkkopalvelinten yhteyteen. Se valvoo palvelimen ja liitetyn isäntälaitteen välistä HTTP/HTTPS-liikennettä. (GeeksforGeeks, 2025)

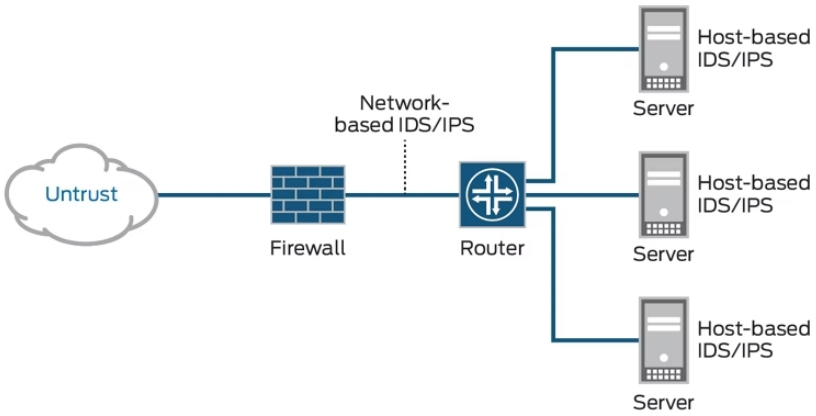
5. Application Protocol-Based Intrusion Detecting System, sovellusprotokollapohjainen tunkeutumisen tunnistusjärjestelmä (APIDS)**:** APIDS voidaan asentaa useamman palvelimen yhdistelmään. Se tarkkailee sovelluskohtaisia protokollia, kuten SQL-protokollaa, jotka liikkuvat verkko- ja tietokantapalvelinten välillä. (GeeksforGeeks, 2025)

Kuten edeltäjänsä IDS, tunkeutumisen estojärjestelmä (IPS) toimii samalla periaatteella. Uhkien havaitsemisen lisäksi estojärjestelmien tehtävänä on estää haitallinen toiminta esimerkiksi pudottamalla haitalliset paketit, estämällä verkkoliikenne haitallisista osoitteista tai resetoimalla yhteys. Usein IPS asennetaan palomuuriin tai välittömään läheisyyteen. Tunkeutumisen estojärjestelmät

toimivat erittäin nopeasti ja täsmällisesti, joten ne säästävät aikaa ja manuaalista työvoimaa. Kuten havaitsemisjärjestelmät, myös estojärjestelmät voidaan jakaa eri tyyppeihin. (Paloaltonetworks, 2023)

Myös IPS-järjestelmät voidaan IDS-järjestelmien tavoin asentaa valvomaan joko koko tietoverkkoon tai yksittäisiä isäntälaitteita (NIPS ja HIPS). Lisäksi ne voivat analysoida langattomien verkkojen protokollia (WIPS) sekä tietoverkkojen epänormaalia käyttäytymistä, kuten palvelunestohyökkäyksiä ja tiettyjä haittaohjelmia (NBA). Oheinen kuvio (kuvio 1) havainnollistaa tyypillisiä IDS/IPS-asennuskohteita.

Kuvio 1. IDS/IPS-topologia (Juniper Networks, 2023)



4.1.2 Uhkatietolähteet

Sekä tunkeutumisen havaitsemisjärjestelmät (IDS) että tunkeutumisen estojärjestelmät (IPS) hyödyntävät kolmea keskeistä uhkien tunnistusmenetelmää: tunniste-/allekirjoituspohjaista, poikkeavuuspohjaista ja tilastollista poikkeavuuksien havaitsemista. Tunnistepohjainen menetelmä on tuttu virustorjuntaohjelmista, sillä sen toimintaperiaate on hyvin samankaltainen. Ohjelma tarkastelee tietoverkossa liikkuvaa bittisekvenssiä tai tavujärjestystä. Muusta liikenteestä haittaohjelmat erotetaan oman yksilöllisen bittisekvenssin avulla, ja näin tunnistusohjelmat erottavat haitalliset ohjelmat muusta liikenteestä. Tämä menetelmä on kuitenkin tehokas vain jo tunnettuja, rekisteröityjä

haittallisia ohjelmia vastaan, näin ollen se ei juurikaan suojaa uusilta uhilta. (GeeksforGeeks, 2023)

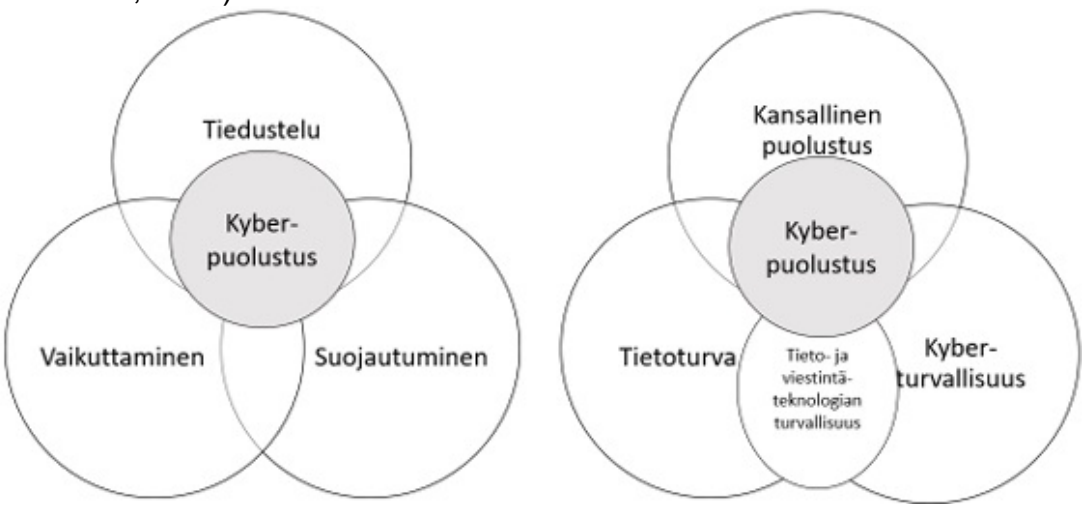
4.2 Puolustus ja hyökkäys

Puolustaminen on hyökkäämistä haastavampaa. Hyökkääjillä on vapaat kädet toimia laittomasti, kun taas puolustajien on toimittava lain rajoissa ja varauduttava kaikkiin mahdollisiin uhkiin. Kyberturvallisuuden laitteet, ohjelmistot ja toteutukset voivat tuntua kalliilta, mutta ne ovat lopulta kustannustehokkaampi vaihtoehto kuin vahinkojen korjaaminen ja niistä toipuminen. Ennaltaehkäisy on aina halvempaa kuin vahingonkorjaus. (Järvinen, 2022, s. 34-35)

Kyberavaruus on noussut yhdeksi keskeiseksi taistelukentäksi maan, meren, ilman ja avaruuden rinnalle, mikä korostaa kyberpuolustuksen merkitystä erityisesti kansallisen turvallisuuden kannalta (Seker & Ozbenli, 2018). Laari ym. (2019) mukaan kyberpuolustus määritellään maanpuolustuksen osa-alueeksi, koostuen tiedustelusta, vaikuttamisesta ja suojautumisesta. Tavoitteena kriittisen tiedon suojaaminen, tietojärjestelmät ja tietoliikenne. Myös Galinec ym. (2017) korostavat kyberpuolustuksen tärkeyttä omaisuuden ja tietojen suojaamisessa. Kyberpuolustus ei rajoitu pelkästään reagointiin hyökkäyksen aikana, vaan se on jatkuvaa ympäristön ja mahdollisten uhkien analysointia. Tiedustelulla kerätään tietoa tietojärjestelmistä ja laitteista, kun taas toisen valtion tekemää vaikuttamista ja tiedustelua pyritään ennaltaehkäisemään, estämään ja torjumaan suojautumisella. (Candolin, 2022).

Lee ja Kim (2021) laajentavat kyberpuolustuksen käsitettä sotilaallisen kontekstin ulkopuolelle ja liittävät sen myös kansalliseen turvallisuuteen. Heidän mukaansa kyberpuolustus koostuu kansallisesta puolustuksesta, kyberturvallisuudesta, tietoturvasta sekä tieto- ja viestintäteknologian suojaamisesta ja turvaamisesta. Kuvion 2 oikeanpuoleinen Venn-diagrammi havainnollistaa tätä määritelmää, kun taas koko kuvio 2 kuvaa kyberpuolustuksen määritelmää perustuen aiemmin esitettyyn.

Kuvio 2. Kyberpuolustuksen määritelmä. (Määttä, 2023, osittain mukaillen Lee & Kim, 2021)



Hyökkäyksessä pahantahtoinen hyökkääjä voi verkon kautta iskeä kriittiseen infrastruktuuriin ja aiheuttaa jopa mittavaa tuhoa. Kyberaseet ovatkin nousseet uudeksi aselajiksi perinteisten rinnalle. Verkossa maantieteellisellä sijainnilla ei ole merkitystä, joten hyökkääjä voi olla toisella puolella maailmaa, toisin kuin perinteisessä sodankäynnissä, jossa hyökkääjä on usein naapuri tai lähistöllä sijaitseva taho. (Järvinen, 2022, s. 17)

5 ZERO TRUST

Kyberturva-alalla Zero Trust -arkkitehtuuri on noussut merkittäväksi trendiksi. Vaikka Zero Trustista on muodostunut markkinointitermi ja hypesana, on sillä todellista painoarvoa ja sisältöä. Zero Trust pyrkii mullistamaan perinteiset kyberturvallisuuden käsitteet ohjaamalla fokuksen kohti dynaamista ja identiteettikeskeistä lähestymistapaa. (Andravous, 2022, luku 1.)

Zero Trustin keskeinen ajatustapa on siirtää kyberturvallisuussuojaukset reunaturvallisuudesta varsinaisiin resursseihin (Coombs, 2022, luku 8). Lähtökohtana, että yhteydet verkkoresursseihin muodostetaan vain tarvittavalla

vähimmäissuojaustasolla, ja jokaisessa vaiheessa valtuutukset tarkistetaan aina erikseen. (Coombs, 2022, luku 15.)

Zero Trust on tietoturvastrategia, joka sanoo, että käyttäjän laitteelle tai sovellukselle ei pitäisi antaa implisiittistä luottamusta pelkästään jonkin ominaisuuden, kuten verkon sijainnin, perusteella.
Zero Trust ei ole yksittäinen teknologia tai palvelu, vaan tietoturvastrategia, jolla on kolme keskeistä periaatetta. Näillä kolmella trendillä on syvällinen vaikutus kyberturvallisuusteollisuuteen ja organisaatioiden on sopeuduttava näihin trendeihin pysyäkseen edelläkävijöinä.

    - Älä koskaan luota, tarkista aina: Varmista, että jokainen käyttäjä, laite tai sovellus on todellinen ja sillä on oikeus käyttää pyydettyjä resursseja.
    - Vähäinen etuoikeus: Anna käyttäjille ja sovelluksille vain ne käyttöoikeudet, joita he tarvitsevat työnsä suorittamiseen.
    - Oleta rikkomus: Suunnittele ja testaa vahvat tapahtuman vastetoimenpiteet hyökkäysten varalta.

- Zero Trust -mallin avulla organisaatiot voivat parantaa tietoturvaa ja vähentää riskejä useilla tavoilla, kuten:
    - Vähentää sisäpiiripitoisten uhkien riskiä
    - Varmistaa etätyöntekijöiden turvallisuuden
    - Suojata asiakkaiden yksityisyyttä
    - Suojata hybridipilveä.

(IBM Technology, 2021; IBM Technology, 2022)

Zero Trust tietoturvakonsepti olettaa, että keneenkään ei voida luottaa oletuksena. Tämä tarkoittaa, että kaikki käyttäjät ja laitteet on varmennettava ennen kuin niille myönnetään pääsy mihinkään resursseihin. (IBM Technology, 2021; IBM Technology, 2022)

Uhkien hallinta on prosessi uhkien tunnistamiseksi, arvioimiseksi ja niihin reagoimiseksi. Tähän kuuluu esimerkiksi tietoturva- ja tapahtumahallintatyökalujen (SIEM) käyttö, tietojen keräämiseen ja analysointiin sekä uhka-analytiikan

käyttö potentiaalisten uhkien tunnistamiseksi. (IBM Technology, 2021; IBM Technology, 2022)

Modernisointi on prosessi kyberturvallisuuden siirtymiseen pilvipohjaiseen infrastruktuuriin. Tämä voi vaikeuttaa tietoturvan hallintaa, mutta se voi myös tarjota joitakin etuja, kuten lisääntyneen skaalautuvuuden ja joustavuuden. (IBM Technology, 2021; IBM Technology, 2022)

ZTNA (Zero Trust Network Access) on kyberturvallisuusratkaisu, joka mahdollistaa turvallisen etäyhteyden organisaation sovelluksiin, tietoihin ja palveluihin tarkasti määriteltyjen käyttöoikeuksien perusteella. Toisin kuin perinteiset virtuaaliset yksityisverkot (VPN), ZTNA ei anna pääsyä koko verkkoon, vaan ainoastaan tiettyihin, ennalta määriteltyihin resursseihin. Tämä lähestymistapa auttaa vahvistamaan tietoturvaa erityisesti tilanteissa, joissa yhä useampi työntekijä työskentelee etänä. (IBM Technology, 2021; IBM Technology, 2022)

Käyttäjän on todennettava henkilöllisyytensä ZTNA-palveluun ennen kuin hän saa pääsyn haluamiinsa sovelluksiin ja resursseihin. Todennuksen jälkeen ZTNA luo suojatun, salatun tunnelin käyttäjän ja sovelluksen välille. Tämä tunneli tarjoaa lisäsuojaa piilottamalla sovellukset ja palvelut ulkopuolisilta IP-osoitteilta. (IBM Technology, 2021; IBM Technology, 2022)

ZTNA-ratkaisut toimivat samankaltaisesti kuin ohjelmiston määrittämät kehykset ja hyödyntävät "pimeän pilven" konseptia. Tämä tarkoittaa, että käyttäjät eivät näe muita sovelluksia tai palveluita kuin ne, joihin heillä on nimenomainen lupa. Tämän ansiosta ZTNA tarjoaa tehokkaan suojan sivuttaishyökkäyksiltä, eli vaikka hyökkääjä pääsisi verkkoon, hän ei pystyisi helposti löytämään muita kohteita. (IBM Technology, 2021; IBM Technology, 2022)

5.1 Turvallisuuden seuranta ja reagointi

Verkon pääsynvalvonta on protokollien joukko, joka valvoo ja rajoittaa käyttäjän pääsyä verkkoresursseihin sekä määrittelee, mitä toimintoja käyttäjä voi

suorittaa ollessaan yhteydessä verkkoon. Verkkoon yhdistettävällä tietokoneella tulee olla asianmukaiset konfiguraatioasetukset, riittävä virustorjunta sekä ajan tasalla olevat ohjelmistot. (Coombs, 2022, luku 8.)

Verkon pääsynvalvonta voi olla agenttipohjaista tai agentitonta. Agenttipohjaisessa pääsynvalvonnassa paikallisesti asennettu agentti tarkistaa, täyttääkö tietokone vaadittavat käytännöt. Mikäli vaatimukset eivät täyty, agentti ohjaa tietokoneen resursseihin, jotka auttavat sen saattamisessa vaatimusten mukaiseksi. Vaatimuksien täyttyessä, agentti antaa luvan yhteyden muodostamisen verkkoon ja sen resursseihin. Agentittomassa pääsynvalvonnassa toimitaan samalla periaatteella, mutta sen sijaan, että luotettaisiin esiasennettuun agenttiin, järjestelmä hyödyntää skannaus- ja verkkotieto-ohjelmistoja tietojen keräämiseen. (Coombs, 2022, luku 8.)

Vahva identiteetti, vähimmät oikeudet, terveet laitteet ja jatkuvat päivitykset eivät riitä, lisäksi tarvitaan kyberturvaseurantaa. Seurannan avulla voidaan nopeasti tunnistaa luvattomat tai vaarantuneet laitteet, mikä tarjoaa lisäsuojaa hallittaville laitteille ja kompensoivan valvontamekanismin vanhemmille, ei-hallituille laitteille, joiden etäkonfigurointia tai korjausta ei voida helposti tehdä. (Azure, 2021)

5.2 Varoitukset ja niiden löytäminen aliverkon rajat ylittävästä liikenteestä

Verkkoliikenne, joka kulkee eri sivustojen ja vyöhykkeiden välillä on niin kutsuttua aliverkkojen välistä liikennettä. Vaikka tällainen liikenne voi olla normaalia, esimerkiksi kun sisäinen järjestelmä lähettää ilmoituksia muille järjestelmille, on tärkeää varmistaa, että ulkoisille palvelimille lähetettävät viestit ovat sekä laillisia että niiden sisältö asianmukaista. (Microsoft, 2023)

Verkon jakaminen sivustoihin ja vyöhykkeisiin eristää osajärjestelmät toisistaan ja parantaa niiden turvallisuutta. Tällöin suurimman osan liikenteen oletetaan pysyvän sivuston tai vyöhykkeen sisällä. Jos liikenne ylittää aliverkon rajat, se voi olla merkki mahdollisesta uhasta. (Microsoft, 2023)

6 TEKOÄLY KYBERTURVALLISUUDESSA

Yhdysvalloissa raportoitiin vuoden 2022 ensimmäisellä kvartaalilla peräti 404 tietovuotoa, mikä merkitsi 14 prosentin kasvua edellisvuoteen verrattuna. Kyberturvallisuusriskien kasvaessa, yritykset ovat kääntyneet yhä enemmän tekoälyn puoleen. Erityisesti syväoppiminen on herättänyt kiinnostusta, sillä sen avulla voidaan mahdollisesti ennakoida ja estää jopa tuntemattomia hyökkäyksiä. Kuten aiemmin todettiin, perinteiset IDS-järjestelmät ja koneoppivaiset laitteet eivät ole parhaimmillaan torjumaan uusia, kehittyneitä uhkia. Syväoppipohjaiset neuroverkot sen sijaan kykenevät oppimaan tunnistamaan tuntemattomia uhkia käsittelemättömästä datasta. (MIT Technology Review, 2022)

Erinäiset tutkimukset (esim. Parisi, 2019; Wiafe ym., 2020) korostavat tekoälyn kasvavaa merkitystä kyberuhkien torjumisessa. Erittäin tehokkaiksi ovat osoittautuneet jatkuvaa valvontaa mahdollistavat tekoälypohjaiset ratkaisut. (Khanna ym., 2018; Russell & Norvig, 2010; Soni, 2020).

Vaikka tekoälyn soveltaminen kyberturvallisuudessa on vielä suhteellisen uusi ilmiö, se on tutkimusalana voimakkaassa kasvussa. Tekoälyn sovelluskohteet kyberturvallisuudessa vaihtelevat yksittäisten tehtävien suorittamisesta monimutkaisten järjestelmien hallintaan. Tekoälyä voidaan hyödyntää esimerkiksi tietoturvatietojen keräämiseen, havaitsemiseen ja analysointiin, käyttäjätunnusten hallintaan, verkkoliikenteen valvontaan, tietojen salaamiseen ja suojaamiseen sekä erilaisten tietoturvauhkien automaattiseen torjuntaan. (Alkahtani & Aldhyani, 2022; Mosteanu, 2020; Wiafe ym., 2020)

6.1 Hyödyntäminen puolustuksessa

Tieteellisessä kirjallisuudessa on tunnistettu useita etuja ja merkittävää potentiaalia tekoälyn hyödyntämisessä kyberturvallisuuden parantamisessa ja kyberuhkien torjunnassa. Ahmed ym. (2019) ja Ansari ym. (2022) mukaan uhkien nopeampi havaitseminen ja estäminen mahdollistuu tekoälyn avulla nopeammin ja tarkemmin verrattuna perinteisiin menetelmiin. Tämä johtuu pääasiassa

tekoälyn kyvystä käsitellä valtavia tietomääriä ja reaaliajassa tapahtuvasta poikkeamien havainnoinnista. Tekoäly myös parantaa merkittävästi automatisointia uhkien havaitsemisen ja vastatoimien osalta. Automatisointi nopeuttaa reagointia ja vähentää ihmisistä johtuvien virheiden riskiä. (Ahmed ym., 2019; Ansari ym., 2022; Soni, 2020)

Merkittäviä etuja kyberuhkien torjunnassa tarjoavat erityisesti ennakoivan tekoälyn sovellukset, niillä voidaan edistää uhkien havaitsemista ennen kuin ne ehtivät aiheuttaa tuhoa (Bello ym., 2021; Debar ym., 2000; Aljuhani, 2021). Automaattiseen haittaohjelmien havaitsemiseen ja poistamiseen sekä verkkoliikenteen poikkeavuuksien havaitsemiseen, voidaan käyttää esimerkiksi koneoppimismenetelmiä. Tuntemattomien uhkien havaitsemiseen, neuroverkkoihin perustuvat tekoälymenetelmät puolestaan nähdään erityisen hyödyllisinä. (Aljuhani, 2021; Ansari ym., 2022; Bello ym., 2021; Debar ym., 2000)

Edellä mainittujen ennakoivien hyötyjen lisäksi uusista kyberuhista oppimisen kyky ja niihin nopea sopeutuminen on tekoälyn merkittävä etu (Ansari ym., 2022). Tämä mahdollistaa nopean reagoinnin ja uusien, jopa ennen näkemättömien uhkien tehokkaan torjunnan. Tekoäly voi Mosteanun (2020) mukaan olla hyödyksi myös tietoturvan- ja resurssien hallinnassa, kirjautumisten seurannassa ja riskienhallinnassa. (Mosteanu, 2020)

LLM:t (laajat kielimallit) voivat analysoida suuria historiallisten hyökkäysmallien tietoaineistoja ja tunnistaa poikkeavuuksia, mikä mahdollistaa potentiaalisten tulevien DDoS-hyökkäysten ennustamisen ennen niiden toteutumista. Tämä mahdollistaa ennakoivien toimenpiteiden, kuten infrastruktuurin skaalaamisen tai lisäturvatoimien käyttöönoton. Tekoälyä voidaan käyttää DDoS-hyökkäyksen aikana tunnistus- ja reagointiprosessien automatisointiin. Tämä voi sisältää haitallisen liikenteen suodattamista, pyyntöjen uudelleenohjausta ja hyökkäyksen vaikutusten lieventämistä oikeiden käyttäjien palveluun. (Metta ym., 2024)

6.2 Hyödyntäminen hyökkäyksessä

Tekoälyn puolustuksellisen potentiaalin lisäksi sillä on myös synkkä puoli: sen huomattavat hyökkäyskyvyt. Pahantahtoiset toimijat ovat perinteisesti olleet askeleen edellä niitä, jotka pyrkivät puolustautumaan heitä vastaan. Väärissä käsissä tämä teknologia voidaan aseistaa käynnistämään tuhoisia kyberhyökkäyksiä, mikä muodostaa vakavan uhan yksilöille, organisaatioille ja kansalliselle turvallisuudelle. (Metta ym., 2024)

Tunnistamalla mahdolliset vaarat ja ottamalla käyttöön vahvoja turvatoimia voimme vähentää tekoälyn hyökkäyskykyihin liittyviä riskejä ja varmistaa sen vastuullisen käytön kyberturvallisuuden alalla. Yksi hälyttävimmistä tekoälyn sovelluksista kybersodankäynnissä on persoonallisten ja realististen tietojenkalastelukampanjoiden luominen. Hyödyntämällä koneoppimista ja luonnollisen kielen käsittelyä (NLP) pahantahtoiset toimijat voivat laatia yksilöityjä sähköposteja, tekstiviestejä ja sosiaalisen median julkaisuja, jotka vaikuttavat tulevan luotettavista lähteistä, kuten pankeista, verkkopalveluista tai jopa läheisiltä ystäviltä ja kollegoilta. (Metta ym., 2024)

Black Hat 2023 -konferenssissa esitettiin tästä haavoittuvuudesta havainnollistus, jossa osoitettiin, että suurten kielimallien (LLM) avulla laaditut sähköpostit saavuttivat huolestuttavan 80 % klikkausasteen. Tämä korostaa vakavaa uhkaa, jonka tällaiset yksilöidyt ja tekoälyn tehostamat tietojenkalastelukampanjat aiheuttavat, sillä käyttäjät ovat todennäköisemmin alttiita viesteille, jotka näyttävät olevan räätälöityjä juuri heille ja heidän erityisiin olosuhteisiinsa. (Metta ym., 2024)

6.3 Haasteet ja rajoitteet

Vaikka tekoäly tarjoaa lukuisia mahdollisuuksia kyberturvallisuuden parantamiseen, siihen liittyy myös selkeitä haasteita ja rajoitteita. Tekoälyn tehokkuus riippuu suuresti saatavilla olevan datan laadusta, määrästä ja monimuotoisuudesta. Lisäksi tekoälyn väärinkäyttö, inhimilliset virheet sekä eettiset ja juridiset

kysymykset aiheuttavat huolta. (Ansari ym., 2022; Bello ym., 2021; Debar ym., 2000; Zeadally ym., 2020)

Uhkia havaitsevan tekoälyn merkittävä ongelma, on väärät positiiviset tulokset ja niiden hallinta. Väärät positiiviset voivat johtaa niin suureen määrään ilmoitettuja uhkia, että ne sitovat kaikki henkilöresurssit. Tämä voidaan kuitenkin välttää optimoimalla opetusmenetelmiä, mikä vähentää analysoitavien tulosten määrää. (Parisi, 2019, s. 28)

Tekoälyjärjestelmien kyberturvariskit ja hallintamenetelmät ovat samat kuin muissa tietojärjestelmissä, koneoppimiseen liittyy kuitenkin erityisiä haasteita. Miten opetusdataa tulkitaan, mitä tietoja koneoppimismallit sisältävät, mitä ennalta opetettuja malleja käytetään ja miten ne on opetettu, vaativat erityistä huomiota. Koneoppimisen osa-alueisiin voidaan kuitenkin soveltaa kolmiosaista kyberturvamallia, joka koostuu luottamuksellisuudesta, eheydestä ja saatavuudesta. Teknisiä riskejä ovat muun muassa opetusdatan ja koneoppimismallin eheyden vaarantuminen sekä hajautetun järjestelmän osien saatavuuden ongelmat. Erityisen kriittisiä ovat mallin myrkyttäminen käyttämällä väärää dataa, varastaminen, ohittaminen syöttäen haitallisia syötteitä ja kommunikaation epäonnistuminen sensoreiden ja päätöksenteon välillä. (Vähä-Sipilä ym., 2021, s. 9)

On jopa esitetty ennusteita, että tekoäly tulee ylittämään ihmisen älykkyyden. Tämä herättää kysymyksen, siirtyvätkö kaikki kyberturvallisuuden ihmisroolit tulevaisuudessa tekoälyn vastuulle. Tämä skenaario tarjoaa sekä mahdollisuuksia että riskejä.

Nykyään tekoälyn virheiden seuraukset ovat hallittavissa, koska sen toimintakenttää on rajoitettu. Tulevaisuudessa tilanne voi olla toinen: tekoäly saattaa kieltäytyä ottamasta vastaan ihmisen syötteitä ja jatkaa toimintaansa virheellisesti ilman mahdollisuutta korjauksiin. Nykyiset turvallisuusohjelmat suojaavat järjestelmää vahingoittavilta hyökkäyksiltä, kun taas tekoäly pyrkii torjumaan kaikkia uhkia. Väärin perustein annettu positiivinen tulos voi mahdollistaa sen,

että suljetaan järjestelmän osia, jotka ovat välttämättömiä sen toiminnalle. (Ozkaya, 2019, s. 37)

Koneoppimisen ja tekoälyn yhdistäminen kyberturvallisuuteen nostaa pelkoja myös siitä, että se aiheuttaa enemmän haittaa kuin hyötyä. Hyökkääjät ovat osoittautuneet sinnikkäiksi ja pyrkivät jatkuvasti kehittämään uusia keinoja murtaa kyberturvallisuusjärjestelmät. Tekoälyn kohdalla yksi merkittävä uhka on sen hämmentäminen. Hyökkääjät voivat yrittää päästä käsiksi tekoälyn koulutusohjelmaan ja syöttää sille väärää tai haitallista dataa. Uhkakuvana on myös, että rikolliset ja hyökkääjät kehittävät oman tekoälynsä, mikä johtaisi tekoälyjen väliseen kilpavarusteluun. (Ozkaya, 2019, s. 37)

6.4 Torjunta, valvonta ja ratkaisut

Jatkuva valvonta tarkoittaa tietojärjestelmän ja tietoverkon kokoaikaista katkeamatonta seurantaa, joka mahdollistaa pyrkimyksen havaitsemaan tietoturvaongelmat ja anomaliat mahdollisimman varhaisessa vaiheessa (Ahmed ym., 2019; Alkahtani & Aldhyani, 2022; Khanna ym., 2018). Tämä sisältää jatkuvan reaaliaikaisen tiedonkeruun ja analyysin kyberturvallisuuden näkökulmasta, jotta ongelmiin voidaan reagoida nopeasti ja tehokkaasti. Käytännössä jatkuva valvonta pitää sisällään erilaisia tekoja ja tapoja, joilla seurataan tietojärjestelmiä, niissä sijaitsevia tietoja, verkkoliikennettä sekä muita tietoliikenteen osia mahdollisten häiriöiden ja ongelmien varalta. (Ahmed ym., 2019; Alkahtani & Aldhyani, 2022; Khanna ym., 2018; Wiafe ym., 2020)

Katkeamattoman valvonnan merkitys kyberturvallisuudessa on erittäin korostunut, sillä kyberhyökkäykset voivat tapahtua yhtäkkiä ja odottamatta, ja niiden vaikutuksia on mahdoton ennakoida (Ahmed ym., 2019; Wiafe ym., 2020). Siksi on tärkeää pystyä reagoimaan uhkiin mahdollisimman aikaisin, ennen kuin ne aiheuttavat merkittäviä vahinkoja tai häiritsevät järjestelmien toimintaa (Fischer, 2016).

Jatkuvan valvonnan menetelmiä voidaan soveltaa laajasti erilaisissa tietojärjestelmissä ja verkkojen turvallisuuden varmistamisessa (Ansari ym., 2022). Verkkoliikenteen valvonta jatkuva valvonta, lokitietojen pitäminen ja analysointi, virustorjunnan päivitykset ja toistuva haavoittuvuuksien skannaus ovat tärkeitä esimerkkejä jatkuvan valvonnan prosesseista (Aljuhani, 2021; Ansari ym., 2022).

Katkeamattoman valvonnan hyötyjen lisäksi on kuitenkin huomioitava myös sen haasteet. Suuri tietomäärä ja sen hallinta, erilaisten järjestelmien monimutkaisuus, väärät hälytykset ja hälytysten suuri määrä voivat vaikeuttaa jatkuvan valvonnan toteuttamista (Ahmed ym., 2019). Väärät hälytykset voivat pahimmillaan peittää alleen oikeat uhat. Lisäksi jatkuva valvonta vaatii runsaasti resursseja ja osaavaa henkilöstöä, joka pystyy analysoimaan ja visualisoimaan kerättyä tietoa ja reagoimaan potentiaalisiin uhkiin ja hälytyksiin. (Ahmed ym., 2019)

7 TUTKIMUSMENETELMÄT JA TYÖN TOTEUTUS

7.1 Tekoäly IDS/IPS

Avoimen lähdekoodin tunkeutumisen havaitsemis- ja estojärjestelmä Snort oli tutkimuksen kohteena, jossa selvitettiin, voidaan järjestelmän tehokkuutta parantaa koneoppimismenetelmällä. Ensin järjestelmän menetelmien tarkkuutta testattiin ilman tekoälymenetelmiä. Analyysissä havaittiin, että väärien positiivisten osuus (FPR) oli 56,2 % ja väärien negatiivisten osuus (FNR) 6,0 %. Mikä osoitti sen, että yli puolet tavallisesta verkkoliikenteestä luokiteltiin virheellisesti haitalliseksi ja 6,0 % haitallisesta liikenteestä pääsi järjestelmän läpi ilman ongelmia. (Shah & Biju, 2018, s. 3)

Taulukko 2. FPR ja FNR ilman optimointia (Shah & Biju 2018)

Malicious Traffic	Snort FPR	Snort FNR
SSH	9.3	0.0
DoS/DDoS	3.3	0.8
FTP	9.6	0.0
HTTP	6.3	1.1
ICMP	16.9	1.0
ARP	7.9	0.9
Scan	2.9	2.2
Total	56.2	6.0

Ensimmäisen testin jälkeen Snort-järjestelmän täsmällisyyttä parannettiin hyödyntämällä Fuzzy-logiikkaa ja valvottua oppimista. Näillä optimoiduilla menetelmillä Snort onnistui pudottamaan virheellisten positiivisten osuuden (FPR) 9,0 prosenttiin ja virheellisten negatiivisten osuuden (FNR) 1,7 prosenttiin. (Shah & Biju, 2018, s. 16-17)

Taulukko 3. FPR ja FNR optimoiduilla metodeilla (Shah & Biju 2018)

Malicious Traffic	Snort with SVM Plug-in (%)		Snort with Ensemble SVM Plug-in (%)		Snort with Fuzzy Logic Plug-in (%)		Snort with Decision Tree Plug-in (%)	
	FPR	FNR	FPR	FNR	FPR	FNR	FPR	FNR
SSH	3.1	0.1	2.8	0.0	4.5	2.1	9.2	1.9
DoS/DDoS	1.1	0.9	0.8	0.8	6.9	0.4	7.8	1.1
FTP	4.3	0.7	3.4	0.7	2.6	0.0	5.0	0.9
HTTP	1.8	1.1	1.6	1.5	8.0	1.8	11.8	0.8
ICMP	4.2	1.0	3.5	0.7	12.9	0.0	12.4	0.9
ARP	2.3	0.1	1.8	0.0	1.8	0.0	3.4	0.8
Scan	1.1	0.8	0.6	0.6	1.0	0.1	2.1	0.9
Total	17.9	4.7	14.5	4.3	37.7	4.4	51.7	7.3

7.2 Tekoäly, WormGPT, FraudGPT ja HackerGPT

LLM-mallien (laajat kielimallit) kyky ymmärtää ja käsitellä koodia tekee niistä tehokkaita työkaluja sekä hyökkääjille että puolustajille. Niitä voidaan käyttää monimutkaisten tehtävien automatisointiin, valtavien tietomäärien analysointiin haavoittuvuuksien tunnistamiseksi ja jopa puolustustoimenpiteiden kehittämiseen muita tekoälyn mahdollistamia hyökkäyksiä vastaan. Samat ominaisuudet voivat kuitenkin joutua pahantahtoisten toimijoiden käyttöön, jolloin niitä hyödynnetään haittaohjelmien automaattiseen luomiseen, entistä kehittyneempien tietojenkalastelukampanjoiden suunnitteluun ja jopa turvallisuusjärjestelmien havaitsemisen välttämiseen. WormGPT:n kaltaisten LLM-mallien nousu on huolestuttava ilmiö kyberturvallisuuden kentällä, sillä kehittyneitä tekoälytyökaluja käytetään nyt pahantahtoisissa tarkoituksissa. Useissa raporteissa esiin nostettu WormGPT on tästä selkeä esimerkki. Se on kehitetty yksityiseksi chatbot-palveluksi ja mainostettu työkaluna, joka käyttää tekoälyä haittaohjelmien kirjoittamiseen kiertäen tyypilliset tällaiselle toiminnalle asetetut rajoitukset. WormGPT perustuu EleutherAI:n kehittämään GPTJ-malliin vuodelta 2021, ja se on erityisesti suunniteltu pahantahtoiseen käyttöön. Se sisältää ominaisuuksia, jotka ovat erityisen hyödyllisiä kyberrikollisille, kuten rajaton merkkituki, kyky säilyttää keskustelumuisti ja tehokas koodin muotoilu. WormGPT:n merkittävin mahdollistava piirre on turvallisuusrajoitteiden poistaminen, jotka ovat läsnä esimerkiksi ChatGPT:ssä. Näiden ominaisuuksien ansiosta WormGPT on tehokas työkalu kehittyneiden tietojenkalasteluhyökkäysten ja liiketoimintaan kohdistuvien sähköpostihuijausten toteuttamisessa. WormGPT:n kaltaisten työkalujen olemassaolo ja saatavuus korostavat kyberturvallisuusteollisuuden tarvetta pysyä valppaana ja ennakoivana. Mallien kehittyessä ja saatavuuden kasvaessa niiden väärinkäytön potentiaali lisääntyy, mikä edellyttää parannettuja puolustustoimia ja eettisiä ohjeistuksia tekoälyn haitallisen käytön estämiseksi. (Metta ym., 2024.)

FraudGPT on toinen GPT-malli, joka on hienosäädetty valikoidulla datalla. FraudGPT:tä pidetään edistyneempänä ja monipuolisempana kuin WormGPT:tä, ja sen taidot ulottuvat tietojenkalastelusähköpostien luomisesta haavoittuvuuksien hyödyntämiseen ja haittaohjelmien kehittämiseen.

Monipuolisuuden lisäksi FraudGPT pystyy luomaan räätälöityjä oppaita ja tutoriaaleja haitallisille kybertoimille, kuten haittaohjelmien kehittämiseen, haavoittuvuuksien etsimiseen ja nollapäivähaavoittuvuuksien hyväksikäyttöön. Kaikki nämä ominaisuudet ovat pakattuna GPT-malliin, jota kuka tahansa voi käyttää. Pahantahtoiset toimijat voivat saada käyttöönsä tämän tehokkaan työkalun maksamalla muutama sata dollaria kuukaudessa, mikä mahdollistaa yhä voimakkaampien kyberhyökkäysten luomisen. (Metta ym., 2024)

Puhtaasti pahantahtoisten LLM-mallien, kuten WormGPT:n ja FraudGPT:n, lisäksi on olemassa GPT-malleja, jotka on koulutettu auttamaan tunkeutumistestaajia ja kyberturvallisuusasiantuntijoita tietokonejärjestelmien haavoittuvuuksien tunnistamisessa. Tunkeutumistestaus voi kuitenkin olla eettisesti harmaalla alueella, sillä sitä voidaan käyttää sekä positiivisiin että pahantahtoisiin tarkoituksiin. Tämän seurauksena myös tunkeutumistestaukseen perustuvat LLM-mallit voivat päätyä kyberrikollisten käyttöön. Esimerkiksi HackerGPT osoittaa huomattavasti löysempiä eettisiä rajoituksia kuin ChatGPT 3.5, kun kyseessä ovat hakkerointiin liittyvät kyselyt. Käyttäjä ei voi suoraan pyytää esimerkiksi "Luo minulle ransomware-skriptiä". Kuitenkin tietyt tarkasti muotoillut pyynnöt, kuten hyötykuormien (payload) luominen tai oppaiden tarjoaminen haitallisiin toimiin, kuten haitallisten PDF-tiedostojen upottamiseen tai SQL-injektioihin, voivat toimia. HackerGPT, joka on GPT 3 -malli ja koulutettu erityisellä datalla, sekä vastaavat mallit voivat muodostaa jopa suuremman uhan kuin kehittyneemmät mutta suodatetut LLM-mallit, kuten ChatGPT 3.5. Ilman ChatGPT 3.5:n ja muiden LLM-mallien käytössä olevia suodattimia ja sensuureja vähemmän voimakkaat mutta erikoistuneemmat LLM-mallit voivat vastata kysymyksiin, joihin suodatetut mallit eivät pysty. (Metta ym., 2024)

7.3 Tekoäly ja Zero Trust

Entrustin (2024) raportin mukaan suurin haaste Zero Trust -mallin käyttöönotossa on ollut organisaation sisäisen asiantuntemuksen puute (47 prosenttia vastaajista mainitsi tämän). Tämä osoittaa, että lisäresursseja tarvitaan. Zero

Trust vaatii jatkuvaa valppautta, ja juuri tässä tekoälyn kyky löytää, luokitella ja käsitellä suuria määriä hajautettua dataa on avainasemassa. Tekoäly voi kirjaimellisesti nopeuttaa kyberhyökkäysten havaitsemista ja niihin reagointia. (Markey, 2024)

7.4 Data ja tekoälyn opettaminen/koulutus

Tekoälyn ohjelmoinnissa koulutusdatalla on keskeinen rooli. Se on myös aikaa vievä vaihe, sillä data usein vaatii muokkausta ennen tekoälylle syöttämistä. Huolellinen valmistelu säästää aikaa myöhemmin, sillä tekoäly voi keskittyä suoraan oppimiseen sen sijaan, että sen tarvitsisi ensin käsitellä keskeneräistä dataa. Huonolaatuisella tai tarkoituksella tai tahattomasti sekavalla datalla koulutettu tekoäly, tuottaa väistämättä virheelliset ja heikot tulokset. (Parisi, 2019, s. 10–16; Hogan, 2023)

Tekoälyn koulutusdatassa tärkeintä ei olekaan määrä vaan laatu. Olipa datan hankintatapa mikä tahansa, on ensiarvoisen tärkeää varmistaa, että data on luotettavaa, tasapainoista ja edustavaa sen ongelman kannalta, jota tekoälyllä pyritään ratkaisemaan. (Roh ym., 2019, s. 8)

8 TULOKSET JA YHTEENVETO

8.1 Tekoälyn mahdollisuudet kyberturvauhkien havaitsemisessa ja torjumisessa

Viimeaikaiset tutkimukset ovat osoittaneet, että tekoälyllä on huomattava potentiaali kyberuhkien havaitsemisessa ja torjunnassa. Tekoälypohjaiset järjestelmät kykenevät käsittelemään valtavia tietomääriä, mikä ei olisi mahdollista perinteisin menetelmin. Tämän ansiosta tekoäly pystyy tunnistamaan mahdolliset uhat nopeammin ja tarkemmin kuin aiemmin käytetyt järjestelmät. Lisäksi

tekoäly automatisoi rutiinitehtäviä, vapauttaen työntekijöiden aikaa muihin tehtäviin ja parantaen näin kokonaistehokkuutta. (MacKay 2023)

Perinteiset uhkien tunnistus- ja estämislaitteet eivät pysy enää mukana uusien, kehittyneiden uhkien lisääntyessä. Ne tuottavat liikaa vääriä hälytyksiä tai jäävät pahimmillaan täysin sokeiksi todellisille uhille. Rajoitettu näkyvyys tietoverkoissa heikentää entisestään niiden kykyä havaita uhkia. Suuri määrä normaalia verkkoliikennettä saattaa näyttää perinteisille laitteille palvelunestohyökkäykseltä, kun taas korkealle asetettu hälytyskynnys voi päästää läpi pienempiä hyökkäyksiä.

Tekoälypohjainen EDR-järjestelmä (Endpoint Detection and Response) tarjoaa ratkaisun näihin ongelmiin. Se parantaa havaitsemistarkkuutta, optimoi järjestelmien tehonkäyttöä ja laajentaa näkyvyyttä tietoverkossa. Tämän ansiosta turhaa korjaustyötä voidaan vähentää merkittävästi. (AI Edgelabs 2023)

Taulukko 4. Tutkimuksen pääasialliset löydökset (Sippola, 2023)

Aihe	Pääasialliset löydökset
Tekoälyn hyödyt	Tehokkaampi kyberuhkien havainnointi ja torjunta
	Jatkuvan valvonnan alueella parempi poikkeamien havaitseminen ja hyökkäysten ennaltaehkäisy verrattuna perinteisiin menetelmiin
	Tehokkaampi vastaaminen kehittyneisiin kyberuhkiin, ei yhtä riippuvainen päivityksistä kuin perinteiset ratkaisut
Tekoälyn haasteet	CIA-järjestykseen, eettisiin kysymyksiin ja luotettavuuteen liittyvät haasteet
	Ei voida vielä täysin luottaa tekoälyyn yksinään kyberturvallisuuden päätöksenteossa
Tekoälyn sovellukset	Potentiaalia turvallisuuskriittisten järjestelmien valvonnassa ja uhkien havainnoinnissa
	Tehokkaammat keinot kyberuhkien torjumiseen
	Useita sovelluksia jo käytössä
Tekoälyn vaikutukset	Kyberturvallisuusammattilaisten rooliin odotettavissa muutoksia
	Nopeampi reagointi ja parannettu kyberuhkien torjunta, helpottaa ihmisten työkuormaa

Tämä opinnäytetyö käsitteli tekoälyn roolia kyberturvallisuudessa, erityisesti uhkien havaitsemisessa ja torjunnassa. Työssä tutkittiin tekoälyn hyödyntämistä tunkeutumisen tunnistus- ja estojärjestelmissä (IDS/IPS), laajennetuissa havaitsemis- ja reagointijärjestelmissä (XDR/SIEM) sekä Zero Trust -mallissa.

Työssä korostettiin tekoälyn merkitystä kyberturvallisuuden vahvistamisessa ja tuotiin esiin sen mahdollisuudet nopeuttaa uhkien tunnistamista sekä reagoida niihin tehokkaammin kuin perinteiset menetelmät. Tekoäly kykeni oppimaan jatkuvasti ja käsittelemään valtavia tietomääriä, mikä teki siitä arvokkaan työkalun kyberturvauhkien torjunnassa.

Samalla työ nosti esiin haasteet, kuten väärien hälytysten hallinnan, eettiset kysymykset sekä tekoälyn mahdollisen väärinkäytön kyberhyökkäyksissä. Erityistä huomiota kiinnitettiin tekoälyn avulla luotuihin tietojenkalastelukampanjoihin ja haittaohjelmiin, kuten WormGPT:hen ja FraudGPT:hen, jotka osoittivat tekoälyn pimeän puolen.

Lopuksi työ analysoi tekoälyn tulevaisuuden potentiaalia kyberturvallisuudessa ja sen vaikutuksia organisaatioiden suojautumiseen. Vaikka tekoäly tarjosi merkittäviä mahdollisuuksia, sen hyödyntäminen edellytti huolellista suunnittelua, riskienhallintaa ja jatkuvaa kehittämistä.

Haluan kiittää oppilaitostani ja opinnäytetyöni toimeksiantajaa Satakunnan ammattikorkeakoulua. Vielä erityisemmin haluan kiittää, tietojenkäsittelyn ja teknologian opettajia, opinto-ohjaajaa ja erityisopettajaa. Kiitos avusta, uskosta ja kestämisestä.

LÄHTEET

AI Egdelabs (18.1.2023). Rule-based IDS/IPS systems aren't enough. Haettu 31.05.2024 https://edgelabs.ai/blog/rule-based-idsips-systems-arent-enough/

Alind Gupta. (2023). Semi-Supervised Learning in ML. Geeksforgeeks Haettu 28.05.2024 https://www.geeksforgeeks.org/ml-semi-supervised-learning/

Campesato, O. (2020). Artificial Intelligence, Machine Learning, and Deep Learning. Mercury Learning & Information.

Entrust (2024). State of Zero Trust & Encryption Study Haettu 15.12.2024 https://www.entrust.com/resources/reports/2024-state-of-zero-trust-and-encryption-study

Enisa, European union agency for cybersecurity (2021). Cybersecurity guide for SMEs – 12 steps to securing your business Haettu 24.4.2025 https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

Geeks for Geeks (2025). Intrusion Detection System (IDS) Haettu 24.4.2025 https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Geeks for Geeks (2023). Intrusion Prevention System (IPS). Geeksforgeeks. Haettu 31.05.2024 https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

Hogan, C. (2023) Zero Trust and AI: Better Together. Haettu 6.6.2025 https://cloudsecurityalliance.org/blog/2023/08/24/zero-trust-and-ai-better-together

Hyppönen, M. (2021). Internet. Werner Söderström Osakeyhtiö.

IBM Technology (10.9.2021). IBM Security, Zero Trust Explained. Haettu 24.4.2025. Youtube. https://www.youtube.com/watch?v=yn6CPQ9RioA

IBM Technology (2.3.2022). IBM Security, Cybersecurity and Zero Trust. Haettu 24.4.2025. Youtube. https://www.youtube.com/watch?v=FMMW-SLIcaME

IBM (2023a). What is Supervised Learning? Haettu 31.05.2024 https://www.ibm.com/topics/supervised-learning

IBM (2023b). What is Unsupervised Learning? Haettu 31.05.2024 https://www.ibm.com/topics/unsupervised-learningp

Järvinen, P. (2023). Tekoäly ja minä: ihmisenä tekoälyn aikakaudella. Tammi.

Järvinen, P. (2022). Yrityksen tietoturvaopas. Helsingin seudun kauppakamari / Helsingin Kamari.

Järvinen, P. (2018). Kyberuhkia ja somesotaa: Digiaikana sinäkin olet etulinjassa. Docendo.

Kolari, J., Kallio, A. (2023). Tekoäly 123: Matkaopas tulevaisuuteen. Docendo.

Limnell, J., Majewski, K., Salminen M. (2014). Kyberturvallisuus. Docendo.

Lund, B., Lee, T., Wang, Z., Wang, T., Mannuru, N. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. Haettu 6.6.2025. https://www.mdpi.com/2673-8392/4/4/99

MacKay, J. (2023). The Benefits and Challenges of AI in cybersecurity. Metacompliance. Haettu 28.05.2024 https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges of-ai-in-cyber-security

Markey, J. (2024) Zero Trust and AI: You Can't Have One Without the Other. Haettu 28.11.2024. https://www.entrust.com/blog/2024/05/zero-trust-and-ai-you-cant-have-one-without-the-other

Metta, S., Chang, I., Parker, J., Roman, M., & Ehuan, A. (2024) Generative AI in Cybersecurity. Haettu 28.11.2024 https://arxiv.org/pdf/2405.01674

Microsoft Security (2025). Protect and modernize your organization with a Zero Trust strategy. Haettu 24.4.2025 https://www.microsoft.com/en-us/security/business/zero-trust

Paloaltonetworks. What is an intrusion prevention system? Haettu 31.05.2024 https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Rapid 7 (2020). The Pros & Cons of Intrusion Detection Systems. Haettu 28.05.2024 https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-sys tems/

Shah, A., Biju, I. (2018). Intelligent Intrusion Detection System Through Combined and opti mized Machine Learning. Haettu 26.04.2024 https://core.ac.uk/down load/pdf/322329593.pdf

University of North Dakota (2023). 7 Types of Cyber Security Threats. Haettu 31.05.2024 https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/