Tietoverkkohyökkäys

Uhkaperusteinen vastakeinojen ominaisuuksien määrittäminen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Kevät 2022

Simo Toivonen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka, insinööri — Tiivistelmä

Tekijä Simo Toivonen — Vuosi 2022

Työn nimi Tietoverkkohyökkäys: Uhkaperusteinen vastakeinojen ominaisuuksien määrittäminen

Ohjaaja Marko Grönfors

Opinnäytetyön aiheena oli tutkia uhkaperusteista tietoverkkohyökkäyksiltä suojautumista hyödyntämällä MITRE organisaation D3FEND- ja ATT&CK-viitekehyksiä. Työn tavoitteena oli saavuttaa geneerinen kuva valitusta menetelmästä valitsemalla uhkatiedon pohjalta tutkimuskohteeksi offensiivinen ATT&CK-tekniikka ja määrittämällä tekniikalle vastakeinojen ominaisuudet, jolla pyritään estämään tai kompensoimaan tekniikan hyödyntämisen mahdollisuuksia kohdeympäristössä.

Teoriaosuudessa tarkasteltiin työn aiheen kannalta olennaisia asioita tietoturvauhkista, uhkatiedosta, suojautumisen mekanismeista ja hyödynnetyistä viitekehyksistä. Käytännön osuudessa toteutettiin työn aiheen ja tavoitteen kannalta olennainen tapaustutkimus.

Tutkimus osoitti työhön valitun menetelmän soveltuvan tietoverkkohyökkäyksiltä suojautumiseen tarvittavien vastakeinojen ominaisuuksien määrittelyyn hyvin, mutta määritetyt ominaisuudet ovat hyvin geneerisiä ja niiden hyödyntäminen kohdeympäristössä vaatii laaja-alaista ammattitaitoa sekä jatkotutkimusta. Lopputuotos saavutti opinnäytetyölle asetetut tavoitteet määritellyn laajuuden puitteissa.

Avainsanat tietoturvauhka, tietoverkkohyökkäys, vastakeino, ATT&CK, D3FEND

Sivut 26 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technologies — Abstract
Author Simo Toivonen — Year 2022
Subject Cyber attack: Threat-based characterization for countermeasures
Supervisors Marko Grönfors

The aim of this thesis was to research threat-based defense against cyber-attacks by utilizing the MITRE Corporation's D3FEND and ATT&CK frameworks. The goal of this work was to obtain a generic view of the chosen method by selecting an offensive ATT&CK technique based on threat information and to determine the necessary countermeasure properties to prevent or compensate for the use of the technique in the target environment.

The theoretical part examined the subjects relevant to the aim of the thesis, such as cyber threats, threat information, defense mechanisms and utilized frameworks. In the practical part, a case study related to the subject and aim of the thesis was conducted.

The research showed that the method chosen for the thesis is well suited for defining the properties of countermeasures required to defend against cyber attacks, but the determined properties are very generic and their utilization in the target environment requires extensive professional skills, as well as further research. The final output achieved the goals set for the thesis within the defined scope.

Keywords cyber threat, cyber attack, countermeasure, ATT&CK, D3FEND
Pages 26 pages

Sisällys

Taulukot

Kuvat

1 Johdanto

Vuosikymmeniä ihmisiin, prosesseihin ja teknologiaan tehtävien investointien jälkeen tietoturvapäälliköitä ja -asiantuntijoita vainoaa edelleen kysymys tieto- tai kyberturvasta. Kuinka voit varmistaa suojataanko organisaation tietoja nykyisten resurssien puitteissa parhaalla mahdollisella tavalla? Huolimatta kaikesta kaupallisiin teknologioihin käytetystä rahasta sekä yrityksestä täyttää standardit ja päivittää haavoittuvuudet, tapahtuu silti tietomurtoja, tietoturvakontrollit pettävät ja vastakeinot eivät pysty estämään tietojen varastamista tai tuhoamista. Tapahtumien kulku voidaan muuttaa keskittymällä todennäköisimpiin organisaatiota uhkaaviin tietoverkkohyökkäyksiin. (Reiber & Wright, 2021, s. v) Uhkilta ei voida suojautua täydellisesti, mutta suunnitelmallisesti määritellyt ja käyttöönotetut vastakeinot voivat tehdä ison vaikutuksen kyvykkyyteen suojautua tietoverkkohyökkäyksiltä eli Sanastokeskus TSK ry:n (2018, s. 30) mukaisesti tietoverkon kautta tapahtuvalta teolta ”jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön”.

Tämän opinnäytetyön aiheena on tutkia tietoverkkohyökkäyksiltä suojautumiseen tarvittavien vastakeinojen ominaisuuksien määrittelyä uhkaperusteisesti, hyödyntämällä yhdysvaltalaisen MITRE organisaation kehittämiä ATT&CK- ja D3FEND-viitekehyksiä. Työn tavoitteena on saada geneerinen kuva aiheen mukaisesta menetelmästä ja sen käytännön hyödyistä tutkimalla uhkatiedon pohjalta valittavaa offensiivista tekniikkaa sekä tekniikalta suojautumiseen tarvittavia vastakeinojen ominaisuuksia.

Aihetta ja tavoitetta tukevaksi uhkatiedon lähteeksi valikoitui opinnäytetyön suunnitteluvaiheessa yhdysvaltalaisen MITRE Engenuity -säätiön CTID-organisaation tuottama geneerinen uhkatietoraportti, koska työn tavoitteen kannalta ei ole olennaista sitoa tutkimusta konkreettiseen organisaatioon tai kohdeympäristöön. Epäkohtien välttämiseksi on kuitenkin mainittava, että kohdeympäristö ja -organisaatio on järkevää, ellei välttämätöntä huomioida hyödynnettäessä tutkimuksenmukaista menetelmää tietoverkkohyökkäyksiltä suojautumiseen todellisissa suunnittelu- tai kehityskohteissa.

Opinnäytetyön abstraktiotason ja lähestymiskulman tietoturva- tai kyberuhkilta suojautumiseen määrittää ATT&CK- ja D3FEND-viitekehykset. Työn tietoperusta sekä rakenne rajautuu tukemaan työn tavoitetta ja siten kattaa vain murto-osan mahdollisista tietoturva- ja kyberuhkilta suojautumisen menetelmistä.

Opinnäytetyön aihe valikoitui tarpeesta kehittää omaa osaamista ja kyvykkyyttä ratkaista tietoverkkohyökkäysten aiheuttamien tietoturvauhkien muodostamia suojautumisen suunnittelun, kehityksen sekä näiden priorisoinnin haasteita uhkaperusteisesti globaalissa organisaatiossa. Opinnäytetyöllä ei ole tilaajaa ja aiheen räätälöinti on toteutettu täysin oman mielenkiinnon ja kehityshalun pohjalta.

Tapaustutkimusta ohjaaviksi tutkimuskysymyksiksi määritin:

- Miten kehitysvaiheessa oleva D3FEND-viitekehys soveltuu tietoverkkohyökkäyksiltä suojautumiseen tarvittavien vastakeinojen ominaisuuksien määrittelyyn?
- Mitä lisäarvoa ATT&CK-viitekehyksen käyttäminen D3FEND-viitekehyksen rinnalla antaa vastakeinojen ominaisuuksien määrittelylle?
- Miten uhkatietoon perustuva lähestymiskulma hyökkäyksiltä suojautumiseen vaikuttaa D3FEND-viitekehyksen käyttöön?

Opinnäytetyö jaetaan kolmeen teoriaosuuden lukuun sekä tapaustutkimukseen. Teoriaosuuden ensimmäinen luku käsittelee tutkimuksen kulmakivenä toimivaa tietoturvauhkaa, suojautumisen mekanismeina käytettäviä vastakeinoja sekä niiden määrittämiseen tarvittavaa uhkatietoa. Toinen ja kolmas luku syventyy uhkien ja vastakeinojen ominaisuuksien määrittelyyn käytettäviin viitekehyksiin sekä tapaustutkimuksessa käytettävään uhkatiedon lähteeseen. Työn käytännön osuus syventyy tapaustutkimukseen, jolla pyritään saavuttamaan työlle annettu tavoite sekä antamaan työn aiheen ja tavoitteen kannalta olennainen tietopohja johtopäätöksille ja pohdinnalle.

2 Uhka

Tietoturvalla tarkoitetaan Sanastokeskus TSK ry:n (2018, s. 15) määritelmän mukaan toimia, joilla varmistetaan, että tiedot

- ovat hyödynnettävissä haluttuna ajankohtana (saatavuus)
- vastaavat alkuperäistä tietoa (eheys)
- eivät joudu kolmansien osapuolien käsiin (luottamuksellisuus).

Tietoturvauhka ja kyberuhka termejä käytetään suomenkielisissä julkaisuissa useasti synonyymeinä, vaikka niiden käsitepiirteet eroavat toisistaan. Sanastokeskus TSK ry:n (2018, s. 25) mukaan molemmat käsitteet ovat haitallisia tapahtumia tai kehityskulkuja, jotka toteutuessaan vaarantavat tietyn tarkoitteen. Tietoturvauhka kohdistuu tietoturvaan eli tiedon saatavuuteen, hyödynnettävyyteen ja luottamuksellisuuteen, kun vastaavasti kyberuhka kohdistuu esimerkiksi tietojärjestelmiin perustuvaan ydinvoimalan ohjausjärjestelmään, elintarvikkeiden kuljetus- ja logistiikkajärjestelmään, liikenteen ohjausjärjestelmään tai pankki- ja maksujärjestelmään, tai siitä riippuvaiseen toimintoon (Sanastokeskus TSK ry, 2018, s. 25). Opinnäytetyössä käytetään myös termiä uhka kuvaamaan geneerisesti mahdollista tietoturva- tai kyberuhkaa.

Tietoturva- ja kyberuhkia muodostaa useat aiheuttajat. National Institute of Standards and Technology (NIST) eli Yhdysvaltojen kansallinen standardi- ja teknologianinstituutti (2012, s. D-2) jakaa uhkien aiheuttajat neljään kategoriaan, vihamieliset, tapaturmaiset, rakenteelliset sekä ympäristölliset aiheuttajat. Opinnäytetyön kannalta oleellinen kategoria on taulukon 1 mukaiset vihamieliset aiheuttajat eli uhkatoimijat, jotka standardi- ja teknologiainstituutin (2012, s. D-2) mukaan pyrkivät hyväksikäyttämään kohde organisaation riippuvuutta tietojärjestelmiin ja -verkkoihin. Bordeu ja Graubart (2016, s. 8) jakavat uhkatoimijoiden motiivit neljään ryhmään, raha (esim. varkaus, kiristäminen), geopoliittinen hyöty (esim. sotilaallinen, terrorismi), uhkatoimijan hyöty (esim. jalansija tietoverkossa) ja henkilökohtainen motiivi (esim. huomio).

Taulukko 1. Vihamieliset aiheuttajat (National Institute of Standards and Technology, 2012, s. D-2)

Uhkatoimija	Asema
Yksilö	Ulkopuolinen Sisäpiiriläinen Luotettu sisäpiiriläinen Etuoikeutettu sisäpiiriläinen
Ryhmä	Ad hoc Vakiintunut
Organisaatio	Kilpailija Toimittaja Kumppani Asiakas
Valtiollinen	

Euroopan parlamentin (2022) julkaiseman uutisen mukaan tällä hetkellä merkittävimmän tietoturvauhan organisaatioille muodostaa kiristyshaittaohjelma. Microsoft (2021) jakaa tyypillisimmät tietoverkkohyökkäyksen vaiheet neljään ennen kiristyshaittaohjelman asennusta:

1. jalansijan saavuttaminen: esimerkiksi tietojenkalastelun, varastettujen käyttäjätunnusten tai haavoittuvien ohjelmistojen avulla
2. käyttöoikeuksien kaappaaminen: esimerkiksi laitteen muistista
3. tunkeutumisen laajentaminen: esimerkiksi kaapattujen käyttäjätunnusten avulla
4. jalansijan säilyttäminen: esimerkiksi hyväksikäyttämällä ajastettuja toimintoja
5. toteutus: kiristyshaittaohjelman asentaminen.

Toteutuessaan kiristyshaittaohjelma vaikuttaa tiedon saatavuuteen salaamalla tarkoituksenmukaisesti laitteella olevia tietoja ja esittämällä lunnasvaatimuksen tietojen palauttamiseen tarvittavasta salauksenpurkuavaimesta (Sanastokeskus TSK ry, 2018, ss. 15, 32). Rahan voidaan olettaa olevan pääsääntöinen motiivi uhkatoimijoille, jos

tietoverkkohyökkäyksen tavoitteena on asentaa kiristyshaittaohjelma organisaation laitteisiin. Tässä opinnäytetyössä keskitytään mahdollisten tietoverkkohyökkäysten muodostamiin uhkiin.

2.1 Uhkatieto

Yhdysvaltojen kansallinen standardi- ja teknologianinstituutin (2016, s. 2) mukaan mikä tahansa tietoturvauhkilta suojautumaan auttava tieto voidaan luokitella uhkatiedoksi. Standardi- ja teknologiainstituutin (2016, s. iii) esimerkkejä uhkatiedosta ovat:

- tunnistetiedot, kuten IP-osoite, haittaohjelman tiiviste tai URL-osoite
- taktiikat, tekniikat ja menetelmät, joita uhkatoimija käyttää tietoverkkohyökkäyksessä
- uhkatietoraportit eli tiettyyn kontekstiin rikastettu, analysoitu tai aggregoitu uhkatieto
- kansallisten kyberturvallisuuskeskuksien antamat varoitukset.

Uhkatiedot voidaan Correan (n.d.) mukaan jakaa taulukon 2 mukaisesti kolmeen kategoriaan. Kategoriat erottavat uhkatiedon luonteen ja kenelle uhkatieto on tarkoitettu.

Taulukko 2. Uhkatiedon kategoriat (Correa, n.d.)

Kategoria	Kuvaus	Kohde
Strateginen	Uhkatietoa, joka pyrkii avaamaan ajankohtaisia uhkatrendejä ja määrittämään trendien taustalla olevia uhkatoimijoita ja heidän motiivejansa.	Päätöksentekijä
Taktinen	Teknistä uhkatietoa, joka pyrkii avaamaan hyökkäysten yksityiskohtia ja käytettyjä taktiikoita, tekniikoita ja menetelmiä.	Tietoturva-ammattilainen
Operatiivinen	Enimmäkseen koneluettavaa uhkatietoa, jonka perusteella pyritään esimerkiksi havaitsemaan haittaohjelmia.	Tekniset suojausratkaisut

Uhkatieto voi olla peräisin monesta eri lähteestä. Taulukko 3 kuvaa Samtani, Abate, Benjamin ja Li (2019, s. 5) listaamia yleisimpiä uhkatiedon lähteitä.

Taulukko 3. Uhkatiedon lähteet (Samtani;Abate;Benjamin;& Li, 2019, s. 5)

Lähde	Kuvaus	Ulkonen vai sisäinen	Esimerkki	Hyöty
Julkisten lähteiden tiedustelu (OSINT)	Avoimista lähteistä kerättävää tietoa	Ulkonen	Haavoittuvuus/ hyväksikäyttö/ uhkatieto syötteet, sosiaalinen media, pimeä verkko, julkiset lausunnot	Tarjoaa kattavan näkymän organisaatioon kohdistuviin ulkoisiin uhkiin
Sisäinen uhkatieto	Organisaation sisäisistä järjestelmistä kerättävää tietoa	Sisäinen	Teknisten suojausratkaisuiden tai muiden laitteiden lokitiedot	Tarjoaa tietoa organisaation sisäisistä toiminnoista
Henkilö-tiedustelu (HUMINT)	Henkilöltä suoraan kerättävää tietoa	Molemmat	Suora vuorovaikutus uhkatoimijan kanssa	Tarjoaa tarkkaa tietoa uhkatoimijasta
Vasta-tiedustelu	Hyökkääjälle asetetusta ansasta kerättävää tietoa	Molemmat	Hunajapurkki	Tarjoaa tietoa hyökkääjien käyttämistä työkaluista ja menetelmistä
Valmis uhkatieto (FINTEL)	Jakeluvalmista uhkatietoa	Molemmat	Kaupalliset uhkatietoraportit tai syötteet	Tarjoaa valmiiksi analysoitua uhkatietoa

Tässä opinnäytetyössä keskitytään uhkatietoraporttiin perustuvaan taktiseen ja tilastolliseen uhkatietoon (FINTEL) eli uhkatoimijoiden eniten tietoverkkohyökkäyksissä käyttämiin taktiikoihin, tekniikoihin ja menetelmiin.

2.2 Vastakeinot

Organisaatioiden perinteinen menetelmä tietoturva- tai kyberuhkilta suojautumiseen perustuu tietoverkkohyökkäyksen indikaattorien ymmärtämiseen ja linnoittamiseen, jossa tavoitteena on rakentaa korkeampia muureja esimerkiksi täyttämällä standardien määrityksiä, korjaamalla konfiguraatioita, päivittämällä ohjelmistoja, ottamalla käyttöön kaupallisia suojausratkaisuja ja havaitsemalla hyökkäyksiä organisaation tietoverkosta uhkatietoon perustuvien tunnistetietojen avulla. Perinteistä menetelmää voidaan pitää välttämättömänä, mutta tehottomana. (Reiber & Wright, 2021, s. 4)

Nykyaikaisena tietoturva- tai kyberuhkilta suojautumisena voidaan pitää menetelmää, jossa uhkatieto ohjaa suojautumista ja tapoja, joilla voidaan ennakoida, estää ja havaita tietoverkkohyökkäyksiä sekä reagoida niihin. (Reiber & Wright, 2021, s. 4; The Mitre Corporation, n.d. -a) Opinnäytetyössä käsitellään suojautumisen mekanismina Kaloroumakisin ja Smithin (2021, s. 1) määrittelemiä vastakeinoja.

Kaloroumakis ja Smith (2021, s. 1) määrittelee vastakeinoiksi minkä tahansa prosessin tai teknologian, joka on kehitetty estämään tai kompensoimaan tietoverkkohyökkäyksiä. Tietoturva-arkkitehdin on ymmärrettävä tarkalleen mitä ja miten organisaation valitsemat vastakeinot ehkäisevät tai havaitsevat tietoverkkohyökkäyksiä sekä mitkä ovat keinojen rajoitteet (Kaloroumakis & Smith, 2021, s. 1).

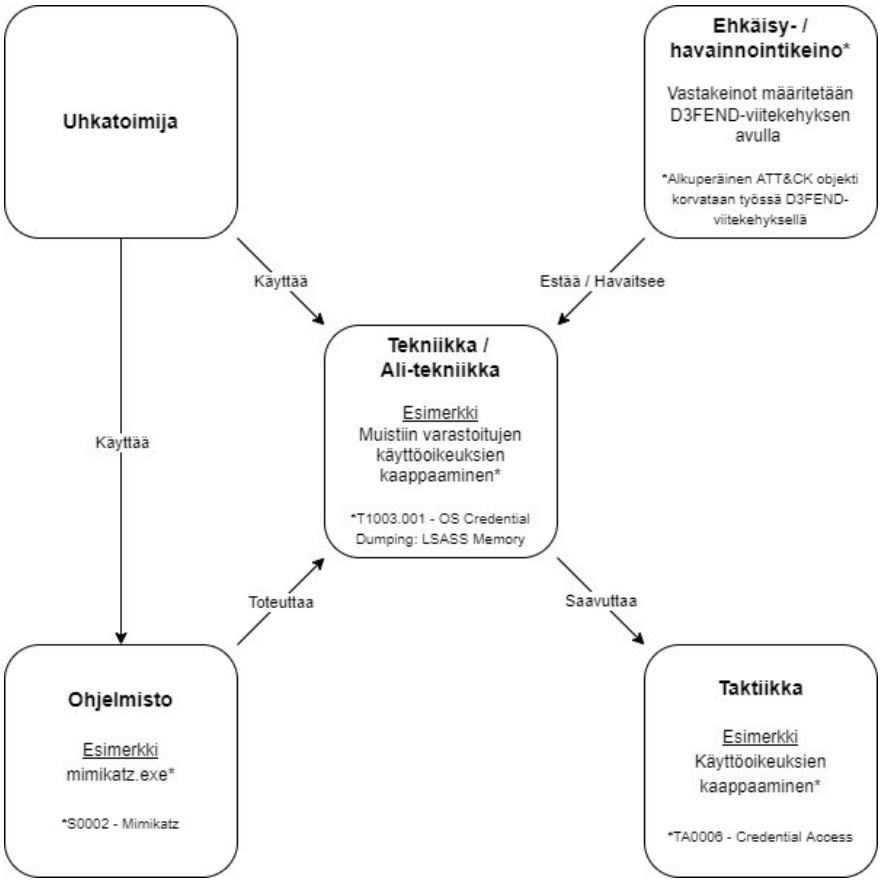
3 MITRE

The MITRE Corporation on vuonna 1958 perustettu yhdysvaltalainen liittovaltion rahoittama, voittoa tavoittelematon tutkimus- ja kehitysorganisaatio (Reiber & Wright, 2021, s. 6). Organisaatio toimii yleisen edun hyväksi ja ratkaisee ongelmia turvallisemman maailman puolesta. Organisaatiolla on rooleja tieto- ja kyberturvan lisäksi muun muassa puolustus-, ilmailu- ja tiedustelu sfääreissä (The MITRE Corporation, n.d. -c; n.d. -d).

3.1 ATT&CK-viitekehys

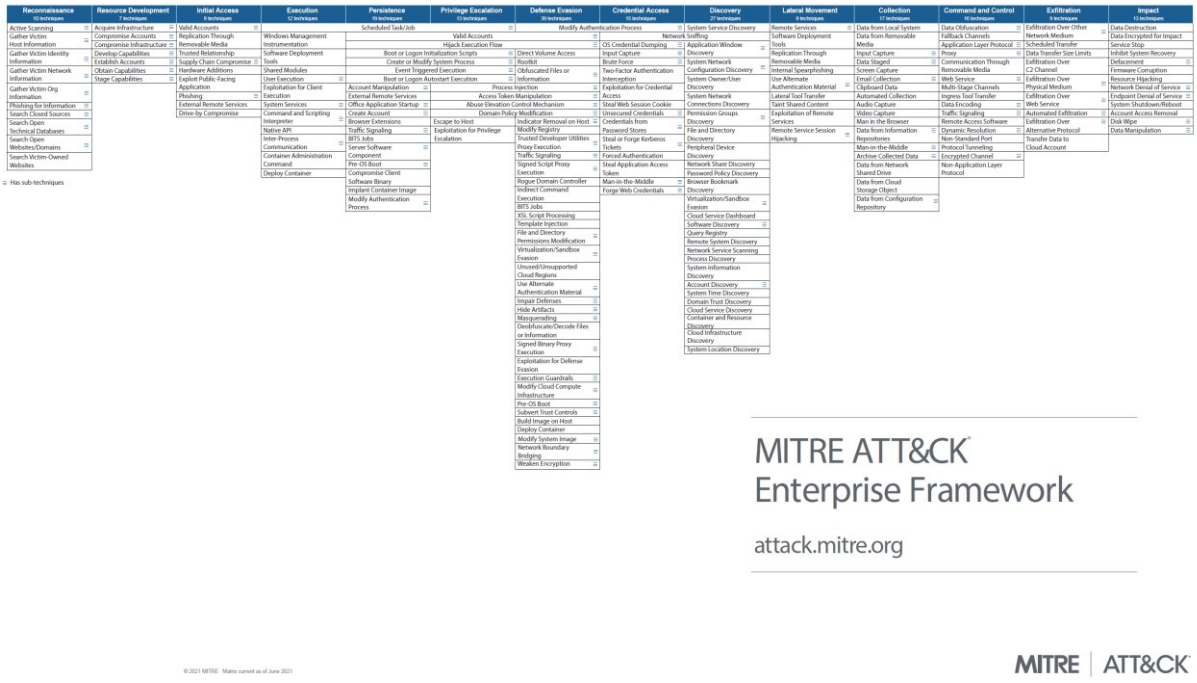
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) -viitekehys on tietoperusta, joka pohjautuu objektimalliin ja objektien välisiin suhteisiin kuvan 1 mukaisella tavalla. Kokonaisuutena ATT&CK kuvaa uhkatoimijoiden tietoverkkohyökkäyksissä käyttämiä offensiivisia ATT&CK taktiikoita eli tavoitteita hyökkäyksessä ja offensiivisia ATT&CK-tekniikoita, joilla tavoite pyritään saavuttamaan. Lisäksi ATT&CK kuvaa tekniikoiden toteuttamiseen mahdollisesti tarvittavia ohjelmistoja ja työkaluja, joita uhkatoimija saattaa käyttää hyökkäyksessä. Sekä ehkäisy- ja havainnointikeinoja, joilla pyritään kompensoimaan tai estämään offensiivisten tekniikoiden käyttöä. (Strom, ym., 2020, ss. 1,17,27) Opinnäytetyössä ATT&CK määrittämät ehkäisy- ja havainnointikeinot korvaan luvussa 3.3 käsiteltävän D3FEND-viitekehyksen tietokaaviolla.

Kuva 1. ATT&CK objektimalli (Strom, ym., 2020, ss. 17-18; Kyberturvallisuuskeskus, n.d.)



Offensiivisten taktiikoiden, tekniikoiden ja alitekniikoiden välisiä suhteita voidaan havainnoida kuvan 2 mukaisesta matriisista. Matriisi mahdollistaa esimerkiksi uhkatoimijakohtaisten taktiikoiden, tekniikoiden, ja alitekniikoiden sekä hyökkäyksessä käytettävien ohjelmistojen ja työkalujen havainnollistamisen lämpökartan muodossa. Matriisi on käytettävissä esimerkiksi MITRE Navigator web-sovelluksessa, mutta sovelluksen hyödyntäminen ei sisälly opinnäytetyön rajattuun aiheeseen, eikä linkity suoranaisesti tutkimukseen.

Kuva 2. ATT&CK Enterprise v10 -matriisi (The MITRE Corporation, 2021a)



ATT&CK ensimmäinen versio luotiin vuonna 2013 MITRE organisaation sisäisen Fort Meade eXperiment (FMX) -projektin tarpeesta kategorisoida kehitysympäristössä uhkatoimijoiden toimintamalleja tietoverkkohyökkäyksissä. Projektin tavoitteena oli kehittää telemetriaan ja toimintamalleihin perustuvaa havainnointikykyä tietoverkossa ja sen osissa. (Strom, ym., 2020, ss. 1-2)

ATT&CK julkaistiin suurelle yleisölle vuonna 2015, jolloin se sisälsi 9 taktiikka ja 96 tekniikkaa. Vuonna 2021 ATT&CK-viitekehys päivittyi versioon 10, joka on edelleen käytössä vuonna

maaliskuussa 2022. Versio 10 sisältää 14 taktiikkaa, 177 tekniikkaa, 348 alitekniikkaa ja jakaantuu kolmeen teknologian määrittämään malliin, Enterprise, Mobile ja ICS. Opinnäytetyö keskittyy käsittelemään ATT&CK Enterprise-mallia, johon sisältyy esimerkiksi Windows-, macOS-, Linux-alustoihin sekä tietoverkkoihin ja pilviteknologioihin liittyviä taulukon 4 mukaisia offensiivisia taktiikoita sekä tekniikoita ja alitekniikoita. (Strom, ym., 2020, ss. 1-2; The MITRE Corporation, 2021d)

Taulukko 4. ATT&CK Enterprise v10 -taktiikat (The MITRE Corporation, n.d. -f; Kyberturvallisuuskeskus, n.d.)

Tunniste	Taktiikka	Tavoite
TA0043	Reconnaissance	Tietoverkkohyökkäyksen suunnittelua tukeva kohteen tiedustelu
TA0042	Resource Development	Tietoverkkohyökkäystä tukevien resurssien kehittäminen
TA0001	Initial Access	Jalansijan saavuttaminen kohdeympäristöön
TA0002	Execution	Haitallisen ohjelmakoodin suorittaminen
TA0003	Persistence	Saavutetun jalansijan säilyttäminen
TA0004	Privilege Escalation	Käyttöoikeuksien laajentaminen
TA0005	Defense Evasion	Suojauksien väistäminen
TA0006	Credential Access	Käyttöoikeuksien kaappaaminen
TA0007	Discovery	Kohdeympäristön sisäinen kartoittaminen
TA0008	Lateral Movement	Tunkeutumisen laajentaminen
TA0009	Collection	Päämäärän kannalta oleellisen tiedon kerääminen
TA0011	Command and Control	Komentokanavan luominen kohdeympäristöön
TA0010	Exfiltration	Tiedon varastaminen
TA0040	Impact	Tiedon tai järjestelmien muokkaus tai tuhoaminen

Tyypillisiä käyttötapauksia ATT&CK-viitekehykselle ovat uhkatoimijan tietoverkkohyökkäyksen simuloiminen, havainnointikyvyn kehittäminen hyödyntämällä uhkatoimijoiden toimintamalleja, suojausratkaisujen nykytilan arviointi, tietoturvavalvomon maturiteetin mittaaminen ja uhkatiedon rikastaminen. (Strom, ym., 2020, ss. 3-4)

ATT&CK-viitekehyksen filosofian muodostaa kolme käsitettä. Ensimmäisenä käsitteenä on uhkatoimijan näkökulma, jolla pyritään siirtymään tietoverkkohyökkäyksiin reagoinnista ennakointiin ja tämän kautta kehittää laitteen, tietoverkon tai -järjestelmän suojausta uhkatoimijan oletetun toimintatavan perusteella. Toisena käsitteenä taktiikat, tekniikat ja alitekniikat perustuvat kokemukselliseen tietopohjaan, joka nojaa vahvasti jaettuun uhkatietoon, kuten uhkatietoraportteihin, tutkimustyöhön, konferensseihin ja sosiaaliseen mediaan. Kolmannen käsitteen muodostaa abstraktiotaso, joka mahdollistaa hyökkääjän oletettujen toimintamenetelmien liittämisen suojautumiseen tarvittaviin vastakeinoihin. (Strom, ym., 2020, ss. 20-23)

3.2 ATT&CK Sightings

ATT&CK Sightings on pilottiohjelma, jonka tarkoitus on kerätä uhkatietoa tietoverkkohyökkäyksissä hyödynnetyistä offensiivisista ATT&CK-tekniikoista ja tämän avulla auttaa ATT&CK-viitekehyksen käyttäjiä ymmärtämään esimerkiksi mitä offensiivisia tekniikoita käytetään useimmin, kuka niitä käyttää tai miten tekniikoiden käyttö vaihtelee ajan myötä. Tiedon kerääminen jakaantuu kolmeen tyyppiin, suora havainto tekniikasta, suora havainto haittaohjelmasta, epäsuora havainto haittaohjelmasta. Merkittävämpänä tyyppinä voidaan pitää kuvan 3 mukaista esimerkkiä raportoidusta suorasta tekniikkahavainnosta. Esimerkissä nähdään komentorivillä suoritettu komento, joka luo ajastetun toiminnon käynnistämään interaktiivinen komentokehote tiettynä kellonaikana. (The MITRE Corporation, n.d. -e)

Kuva 3. Tietoverkkohyökkäyksestä raportoitu suora havainto ATT&CK-tekniikan hyödyntämisestä (The MITRE Corporation, n.d. -e)


```
{
  "id": "DT-1234",
  "sightingType": "direct-technique-sighting",
  "startTime": "2019-01-01T08:12:00Z",
  "endTime": "2019-01-01T08:12:00Z",
  "detectionType": "human-validated",
  "techniques": [
    {
      "techniqueID": "T1088",
      "startTime": "2019-01-01T08:12:00Z",
      "endTime": "2019-01-01T08:12:00Z",
      "platform": "Windows 10",
      "rawData": [
        "process.create": {"command_line": "at 13:30 /interactive cmd"}
      ]
    }
  ]
}
```


3.3 D3FEND-viitekehys

D3FEND-viitekehys on kehitysvaiheessa oleva tietokaavio, joka jakaantuu geneerisellä tasolla viiteen tietoverkkohyökkäyksiltä suojaavaan taulukon 5 mukaiseen defensiiviseen D3FEND-taktiikkaan sekä versiossa 0.10.0-BETA2 139 defensiiviseen DEFEND perustekniikkaan ja tekniikkaan. ATT&CK-viitekehyksestä poiketen defensiiviset taktiikat eivät sisällä tunnistetta. Defensiiviset taktiikat pyritään toteuttamaan viitekehyksen kannalta keskeisten tekniikoiden avulla, jotka kategorisoidaan perustekniikoiden avulla. (Kaloroumakis & Smith, 2021, ss. 7-8; The MITRE Corporation, n.d. -b; The MITRE Corporation, n.d. -g)

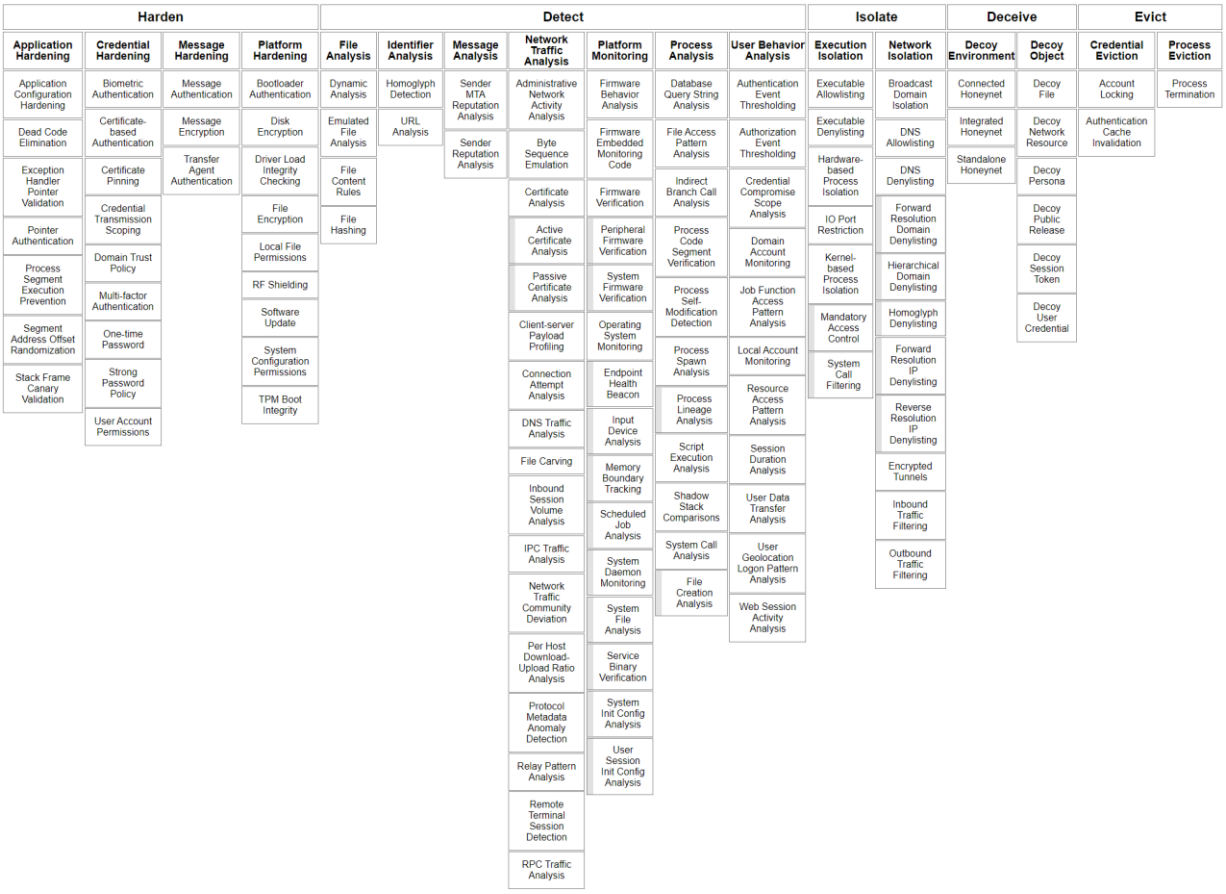
Taulukko 5. D3FEND-taktiikat (The MITRE Corporation, n.d. -h, n.d. -l, n.d. -j, n.d. -k, n.d. -l)

Taktiikka	Kuvaus
Koventaminen (Harden)	Koventamista käytetään pienentämään offensiivisten tekniikoiden hyödyntämismahdollisuuksia. Koventaminen eroaa havaitsemisesta siinä, että se suoritetaan yleensä ennen kuin järjestelmät otetaan käyttöön.
Havaitseminen (Detect)	Havaitsemista käytetään tunnistamaan uhkatoimijan toimintamenetelmiä tietojärjestelmistä ja -verkoista sekä niiden osista.

Eristäminen (Isolate)	Eristämisellä luodaan loogisia tai fyysisiä esteitä järjestelmiin, joilla pyritään vähentämään uhkatoimijoiden mahdollisuuksia tunkeutua syvemmälle kohdejärjestelmään.
Harhauttaminen (Deceive)	Harhauttamista käytetään houkuttelemaan mahdollinen uhkatoimija valvottuun kohdeympäristöön.
Häätäminen (Evict)	Häätämistä käytetään poistamaan uhkatoimija kohdeympäristöstä.

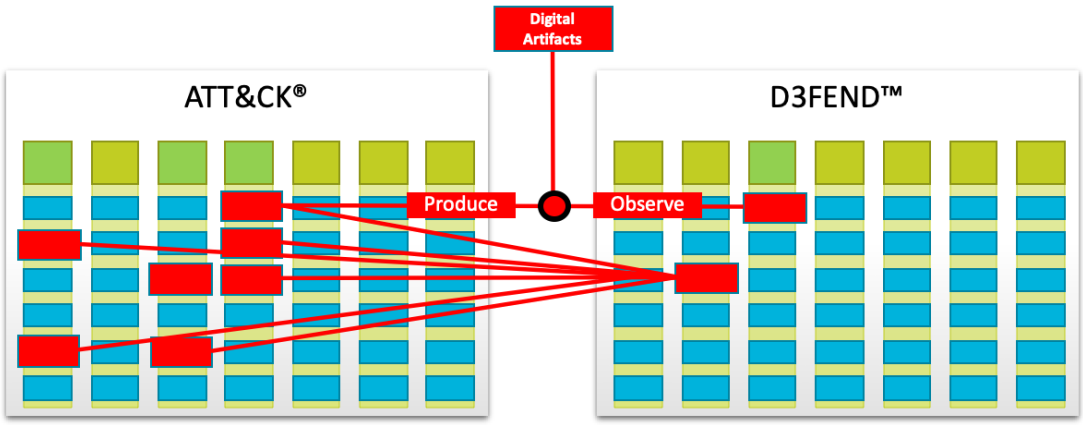
Defensiivisten taktiikoiden, perustekniikoiden ja tekniikoiden välisiä suhteita voidaan havainnoida ja tutkia kuvan 4 mukaisesta D3FEND tietokaavion käyttöliittymästä, jossa jokaisen elementin kautta on mahdollista tarkastella tarkempaa tietoa valitusta elementistä. (Kaloroumakis & Smith, 2021, s. 6)

Kuva 4. D3FEND v0.10.0-BETA2 tietokaavion käyttöliittymä (The MITRE Corporation, n.d. -g)



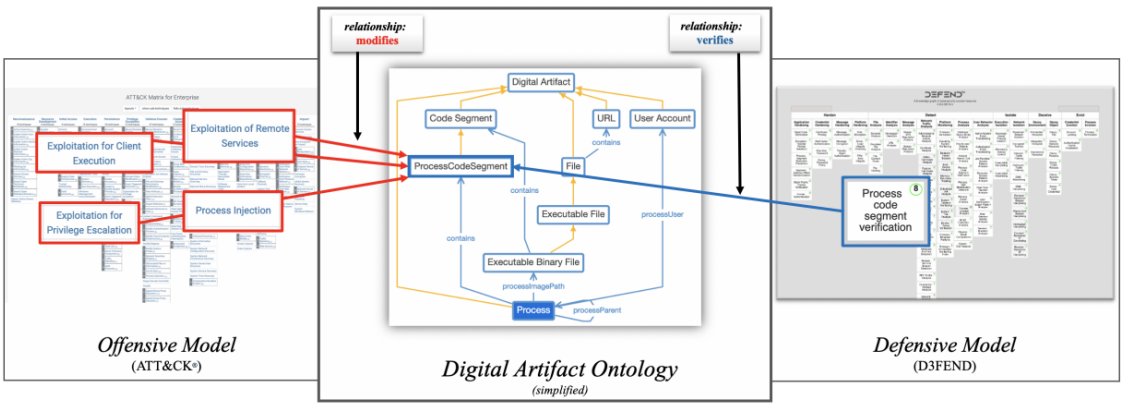
Viitekehyksen avainrakenteen muodostaa kuvan 5 mukainen digitaalinen objekti eli digitaalinen artefakti kuten sähköposti, tietokanta tai dokumentti, johon defensiivinen D3FEND-tekniikka ja offensiivinen ATT&CK-tekniikka on vuorovaikutuksessa. (Kaloroumakis & Smith, 2021, s. 8; The MITRE Corporation, n.d. -m) D3FEND 0.10.0-BETA2-versio viitekehyksestä sisältää 408 digitaalista artefaktia, jotka jakaantuvat ylätason artefakteihin, tiedostoihin, verkkoliikenteeseen ja ohjelmistoihin (The MITRE Corporation, n.d. -m).

Kuva 5. ATT&CK- ja D3FEND-viitekehyksien suhde digitaalisen artefaktin kautta (The MITRE Corporation, n.d. -b)



Kuvan 6 mukainen yksinkertaistettu Digital Artifact Ontology (DAO) -malli havainnollistaa minkälaisen vuorovaikutuksen offensiivinen ATT&CK-tekniikka aiheuttaa digitaaliseen artefaktiin ja miten defensiivisellä D3FEND-tekniikalla pyritään vastaamaan vuorovaikutukseen. (Kaloroumakis & Smith, 2021, ss. 8-9)

Kuva 6. DAO-malli (Kaloroumakis & Smith, 2021, s. 9)



D3FEND-projekti luotiin tarpeesta kehittää viitekehys, jonka avulla pystytään määrittämään tarkasti tietoverkkohyökkäyksiltä suojautumiseen tarvittavien vastakeinojen ominaisuuksia ja komponentteja. Tutkimustyön rahoitti Yhdysvaltojen kansallinen turvallisuusvirasto NSA (National Security Agency). (Kaloroumakis & Smith, 2021, s. 1; The MITRE Corporation, n.d. -b)

D3FEND-viitekehyksen tietoperusta pohjautuu pääasiassa patenttihakemuksiin kyberturvallisuuden teknologioista, jotka on rekisteröity Yhdysvaltojen patentti- ja tavaramerkkivirastoon vuosien 2001 ja 2019 välillä. Kehitystyössä käytettiin myös tietolähteenä olemassa olevia tietopohjia kuten MITRE Cyber Analytic Repository (CAR) sekä muita lähteitä kuten akateemisia julkaisuja. (Kaloroumakis & Smith, 2021, ss. 4-5)

4 MITRE Engenuity

MITRE Engenuity on yhdysvaltalainen MITRE organisaation omistama voittoa tavoittelematon säätiö ja vastakohta tavanomaisen kehitys- ja tutkimusekosysteemin oman edun tavoittelulle sekä voittoa tavoittelevalle päätöksenteolle. Säätiö perustettiin vuonna 2019 tavoitteena yleisen edun tavoittelu ja koko kansan ongelmien ratkaiseminen yhteistyöllä ja tuomalla kilpailijoita yhteen. Säätiö tekee tutkimus- ja kehitystyötä esimerkiksi terveysalan, puolijohdeteollisuuden ja kyber-/tietoturvan parissa. (MITRE Engenuity, n.d. -b)

4.1 Center for Threat Informed Defense

Center for Threat Informed Defense (CTID) on MITRE Engenuity -säätiön perustama yksityisesti rahoitettu voittoa tavoittelematon tutkimus- ja kehitysorganisaatio. Organisaatio on perustettu vuonna 2019 kyberturvallisuusyhteisön palautteen perusteella nopeuttamaan ja ylläpitämään kyber- ja tietoturvauhkilta suojautumisen kannalta kriittisiä julkisia resursseja. (MITRE Engenuity, 2019) Organisaatio kehittää ratkaisuja edistämään uhkatietoon perustuvaa tietoturvauhkilta suojautumista yhteistyössä rahoittavien sekä muiden organisaatioiden kanssa (MITRE Engenuity, n.d. -a).

4.2 Sightings Ecosystem -projekti

CTID-organisaation Sightings Ecosystem -projekti pohjautuu luvussa 3.2 käsiteltyyn MITRE Sightings pilottiohjelman vapaaehtoiseen uhkatietojen keruu menetelmään. Projektissa Sightings-havainnot anonymisoidaan ja koostetaan yhteen uhkatiedon (FINTEL) tuottamiseksi. Projekti tarjoaa analysoitujen havaintojen ja ATT&CK-viitekehyksen avulla laajan käsityksen uhkatoimijoiden toimintamalleista tietoverkkohyökkäyksissä. (MITRE Engenuity, n.d. -c)

5 Uhkaperusteinen vastakeinojen ominaisuuksien määrittäminen

Tapaustutkimus jakaantuu kahteen vaiheeseen. Ensimmäisessä vaiheessa kartoitetaan uhkatiedon pohjalta tutkimukselle kohteeksi offensiivinen ATT&CK-tekniikka ja toisessa vaiheessa valittu offensiivinen tekniikka analysoidaan D3FEND-viitekehyksen avulla vastakeinojen ominaisuuksien määrittämiseksi. Tavoitteena on muodostaa kuva vastakeinojen ominaisuuksista, joita tarvitaan valitulta offensiiviselta tekniikalta suojautumiseen tietoverkkohyökkäyksissä. Tutkimuksen päättää tulokset, joissa pyritään vastaamaan työtä ohjaaviin tutkimuskysymyksiin ja tutkimukselle asetettuun tavoitteeseen.

5.1 Uhkien kartoittaminen

Uhkien kartoittaminen rajautui tutkimuksessa käsittelemään ainoastaan yhtä luvussa 4.2 käsiteltyä uhkatiedon lähdettä eli Sightings Ecosystem -projektia ja tarkemmin määriteltynä kyseisen projektin ensimmäistä 2022 julkaistua uhkatietoraporttia. Kartoittamisen tarkoituksena on valita tutkimuskohteeksi uhkatoimijan käyttämä offensiivinen ATT&CK-tekniikka.

Lähderaportti koostuu yli 800 000 Sightings-havainnosta, jotka on kerätty aikavälillä 1.4.2019 – 31.7.2021. Kerätyt havainnot muodostavat 184 yksilöllistä offensiivista ATT&CK-tekniikkaa ja -alitekniikkaa. Noin 90 prosenttia kerätyistä havainnoista kohdistuu kuuteen offensiiviseen ATT&CK-taktiikkaan ja kuvan 7 mukaisesti viiteentoista offensiiviseen tekniikkaan. Offensiiviset alitekniikat on koostettu sisältymään raportin tulosten statistiikassa

offensiivisiin tekniikoihin. (MITRE Engenuity, 2021, ss. 5,7) Raportissa tilastollisesti eniten käytetyille offensiivisille tekniikoille on määritelty ennaltaehkäisevät NIST SP 800-53 julkaisun mukaiset tietoturvakontrollit ja havainnointiin liittyvä tietopohja SigmaHQ/sigma -projektin sekä MITRE CAR tietopohjan avulla. Edellä mainittuja määrittelyjä ei kuitenkaan hyödynnetä tässä tutkimuksessa.

Kuva 7. Tilastollisesti eniten käytetyt ATT&CK-tekniikat (MITRE Engenuity, 2021, s. 8)

1. Scheduled Task/Job [T1053]
2. Command and Scripting Interpreter [T1059]
3. Hijack Execution Flow [T1574]
4. Proxy [T1090]
5. Masquerading [T1036]
6. Signed Binary/Proxy Execution [T1218]
7. Create or Modify System Process [T1543]
8. Process Injection [T1055]
9. Impair Defenses [T1562]
10. Obfuscated Files or Information [T1027]
11. Remote Services [T1021]
12. Non-Application Layer Protocol [T1095]
13. Windows Management Instrumentation [T1047]
14. Modify Registry [T1112]
15. Ingress Tool Transfer [T1105]

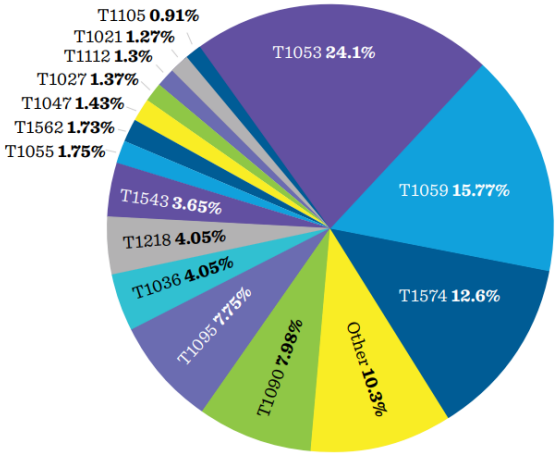
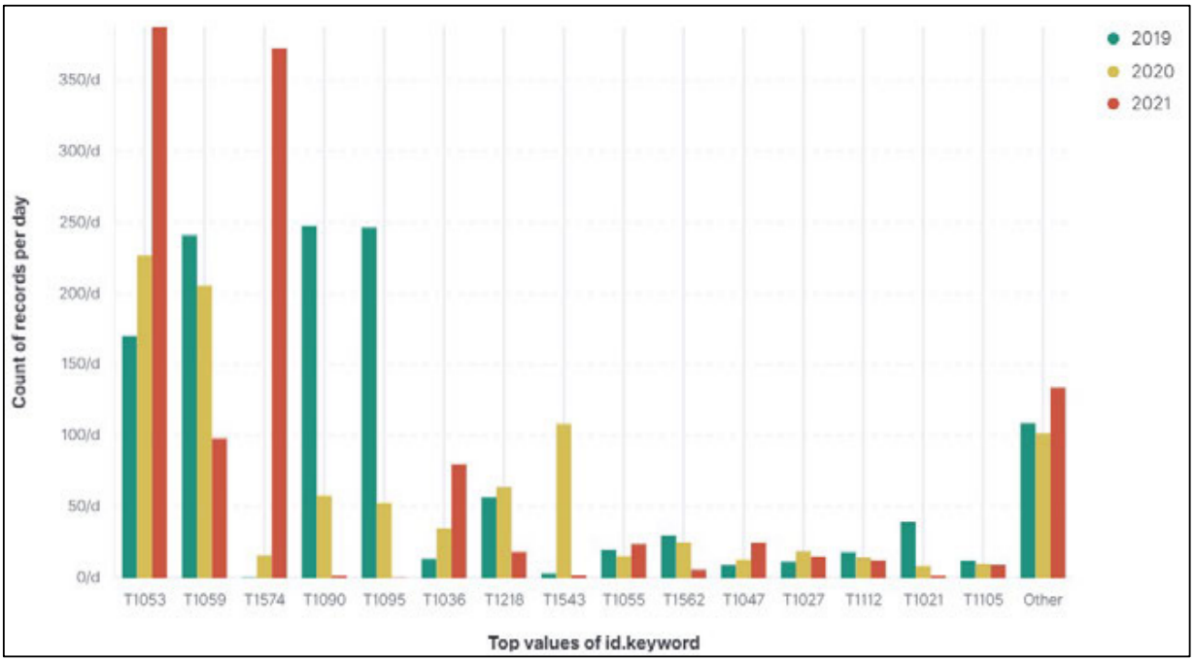


Figure 1 Total Dataset Technique Breakdown

Uhkatietoraportti sisältää myös kerätyille havainnoille tehdyn kuvan 8 mukaisen aikasarja-analyysin. Analyysi kuvaa vuosittaisia muutoksia uhkatoimijoiden käyttämissä offensiivissa ATT&CK-tekniikoissa. Aikasarja-analyysiä ei voida kuitenkaan pitää täysin luotettavana, koska esimerkiksi uhkatoimijoiden käyttämät offensiiviset tekniikat, havainnointikyky sekä ATT&CK-viitekehys kehittyy jatkuvasti. (MITRE Engenuity, 2021, s. 33) Edellä mainituista syistä johtuen aikasarja-analyysille ei annettu painoarvoa tutkimukseen valittavan offensiivisen tekniikan valinnassa.

Kuva 8. Aikasarja-analyysi (MITRE Engenuity, 2021, s. 33)

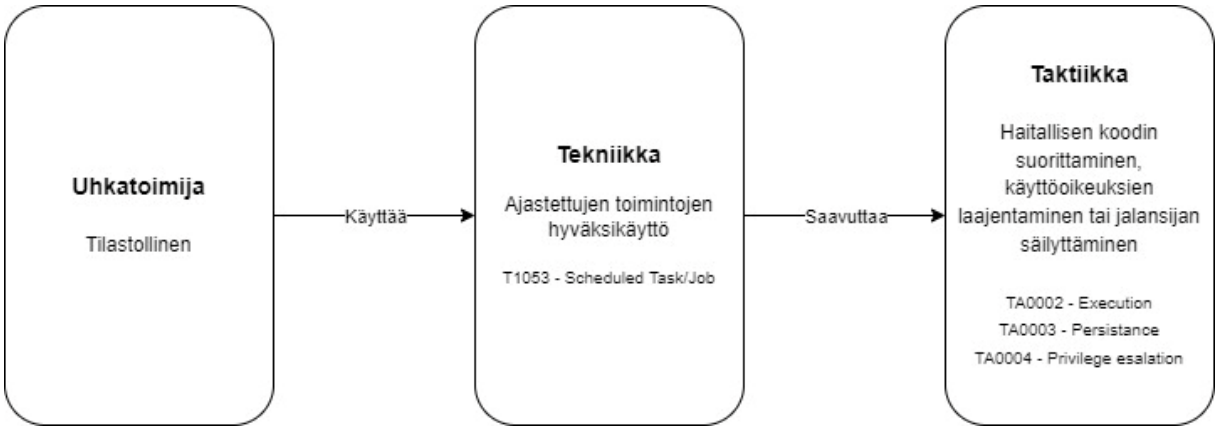


Raportin tuloksien perusteella offensiivinen T1053 Scheduled Task/Job -tekniikka eli ajastettujen toimintojen hyväksikäyttö on tilastollisesti uhkatoimijoiden tietoverkkohyökkäyksissä eniten käyttämä offensiivinen ATT&CK-tekniikka ja tähän perustuen tekniikka valikoitui tutkimuksen kohteeksi. Tapaustutkimuksessa ei huomioitu uhkatietoraportissa laskennallisesti T1053 Scheduled Task/Job -tekniikkaan sisällytettyjä seuraavia alitekniikoita:

- T1053.002 Scheduled Task/Job: At (Windows)
- T1053.003 Scheduled Task/Job: Cron
- T1053.005 Scheduled Task/Job: Scheduled Task

Uhkatoimijat voivat hyväksikäyttää tietoverkkohyökkäyksissä kaikkiin yleisimpiin käyttöjärjestelmiin sisältyviä ajastettuja toimintoja, joilla mahdollistetaan ohjelmien tai komentosarjojen suorittaminen tiettynä ajanhetkenä. Uhkatoimija pyrkii hyväksikäyttämään mekanismia haitallisen koodin suorittamiseen, käyttöoikeuksien laajentamiseen tai jalansijan säilyttämiseen. Tietyin edellytyksin uhkatoimija voi hyödyntää offensiivista ATT&CK-tekniikkaa myös etähallinnan kautta. (The MITRE Corporation, 2021b; Kyberturvallisuuskeskus, n.d.)

Kuva 9. Ajastettujen toimintojen hyväksikäytön yksinkertaistettu objektimalli (The MITRE Corporation, 2021b)



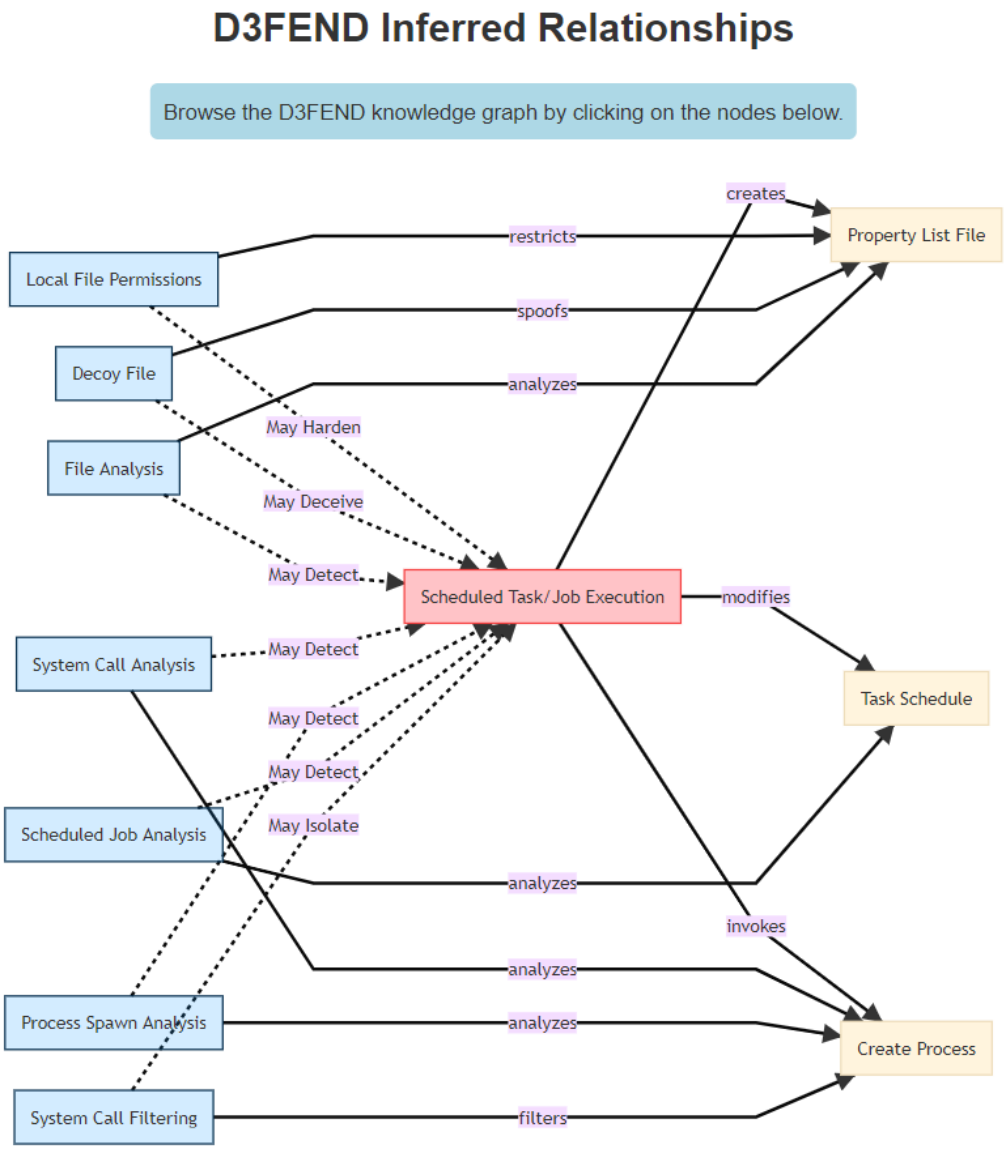
5.2 Vastakeinojen ominaisuuksien määrittäminen

Vastakeinojen ominaisuuksien määrittäminen rajautuu luvun 5.1 perusteella määritettyyn offensiiviseen ATT&CK-tekniikkaan. D3FEND-viitekehyksen avulla on tarkoitus analysoida mihin ajastettujen toimintojen hyväksikäyttö vaikuttaa, miten vaikutus tapahtuu ja miten vaikutuksilta pystytään suojautumaan.

D3FEND-viitekehys määrittää automaattisesti tietokaavioon digitaaliset artefaktit, defensiiviset tekniikat ja offensiivisen tekniikan sekä näiden väliset vuorovaikutukset. Tutkimuksen tarkoituksena on purkaa automaattisesti määritetty tietokaavio osiin sekä analysoida kokonaisuutta osa kerrallaan ja muodostaa analyysin perusteella kuva tarvittavista vastakeinojen ominaisuuksista.

Kuvan 10 mukainen D3FEND tietokaavio havainnollistaa graafisesti mihin digitaalisiin artefakteihin ajastettujen toimintojen hyväksikäyttö eli offensiivisen T1053 Scheduled Task/job -tekniikan käyttäminen aiheuttaa vuorovaikutukset sekä miten kyseiset vuorovaikutukset muodostuvat ja miten defensiiviset D3FEND-tekniikat pyrkivät saavuttamaan taktiset toiminteen eli suojaamaan offensiivisen tekniikan kohteena olevia digitaalisia artefakteja. Tietokaavion perusteella defensiivisten tekniikoiden ja offensiivisen tekniikan välisiä vuorovaikutuksia käsitellään aina muodossa saattaa, koska vuorovaikutuksen toteutumiseen vaikuttaa useat eri tekijät.

Kuva 10. D3FEND tietokaavio ajastettujen toimintojen hyväksikäytöstä (The MITRE Corporation, n.d. -n)



Tietokaaviosta nähdään, että defensiivisiä tekniikoita ja ajastettujen toimintojen hyväksikäyttöä yhdistää kolme taulukon 4 mukaista digitaalista artefaktia. Artefaktien analysoinnin perusteella huomioitavaa on, että PLIST-asetustiedosto liittynee esimerkiksi macOS-käyttöjärjestelmissä käytettävään launchd-prosessiin, joka mahdollistaa muun muassa toimintojen ajastamisen. Muut listatut artefaktit ovat geneerisempiä ja liittyvät suurella todennäköisyydellä myös muihin mahdollisiin käyttöjärjestelmiin.

Suojattavaan kohteeseen kuulumaton artefakti ja siihen liittyvän offensiivisen sekä defensiivisten tekniikoiden vuorovaikutukset voidaan mielestäni tarvittaessa rajata pois vastakeinojen ominaisuuksien määrittelystä, jos rajaaminen nähdään järkeväksi.

Taulukko 6. Digitaaliset artefaktit (The MITRE Corporation, n.d. -n, n.d. -o, n.d. -p, n.d. -q)

Digitaalinen artefakti (IRI)	Kuvaus
d3f:PropertyListFile	PLIST-asetustiedosto on tiedosto, johon voi tallentaa sarjamuotoisia objekteja esimerkiksi OS X, iOS, NeXSTEP, ja GNUstep ohjelmointikehyksissä. Tiedostoja käytetään usein tallentamaan käyttäjän asetuksia.
d3f:TaskSchedule	Ajastettu toiminto on tiettynä aikana tai aikavälein suoritettava toiminto.
d3f:CreateProcess	Prosessin luonti on toiminto, joka lataa ja suorittaa uuden lapsiprosessin. Nykyinen prosessi voi odottaa lapsiprosessin suorituksen päättymistä tai jatkaa suorittamista asynkronisesti.

Tietokaavion mukaan offensiiviselta ATT&CK-tekniikalta suojautuminen jakaantuu seitsemään taulukon 5 mukaiseen defensiiviseen D3FEND-tekniikkaan. Defensiivisten tekniikoiden perusteella pystytään muodostamaan geneerinen kuva, miten offensiiviselta tekniikalta pyritään suojautumaan. Kuitenkin ilman kontekstia defensiiviset tekniikat ovat lähes hyödyttömiä vastakeinojen ominaisuuksien määrittelyssä. Huomion arvoista on, että perustekniikka kategorisoi defensiiviset tekniikat ja tapauskohtaisesti tämän avulla pystytään priorisoimaan jatkoanalyysissä vastakeinojen valintaa, jos merkittävä määrä kartoitetuista defensiivisistä tekniikoista kuuluu esimerkiksi Process Analysis -perustekniikan alle.

Taulukko 7. Suojautumiseen tarvittavat D3FEND-tekniikat ja -perustekniikat (The MITRE Corporation, n.d. -n, n.d. -r, n.d. -s, n.d. -t, n.d. -u, n.d. -v, n.d. -w, n.d. -x)

Tunniste	Tekniikka	Perustekniikka	Kuvaus
D3-LFP	Local File Permissions	Platform Hardening	Paikallisten tiedostojen käyttöoikeuksien rajoittaminen käyttöjärjestelmän toimintojen avulla

D3-DF	Decoy File	Decoy Object	Tiedosto, joka on luotu ansaksi uhkatoimijalle
D3-FA	-	File Analysis	Tiedostoanalyysi on prosessi tiedoston tilan määrittämiseksi. Esimerkiksi: virus, haitallinen, luotettava
D3-SCA	System Call Analysis	Process Analysis	Järjestelmäkutsujen tarkastelu luvattomien prosessien varalta
D3-SJA	Scheduled Job Analysis	Platform Monitoring	Ajastettuihin toimintoihin liittyvien lähdetiedostojen, prosessien, kohdetiedostojen tai kohdejärjestelmien tarkastelu hyväksikäytön havaitsemiseksi
D3-PSA	Process Spawn Analysis	Process Analysis	Prosessin argumenttien tai attribuuttien tarkastelu hyväksikäytön havaitsemiseksi
D3-SCF	System Call Filtering	Execution Isolation	Ytimen API-kutsujen suodattaminen konfiguroitavan referenssilistan avulla

Taulukon 6 avulla muodostuu kokonaiskuva tietokaaviosta, jonka avulla määrittyy suojautumiseen tarvittavat vastakeinojen ominaisuudet. Taulukko kuvaa ensin miten ajastettujen toimintojen hyväksikäyttö on vuorovaikutuksessa taulukon 4 mukaisiin digitaalisiin artefakteihin ja millä defensiivisillä D3FEND-taktiikoilla suojautumista on mahdollista toteuttaa. Taulukon 5 mukaiset defensiiviset tekniikat kuvaavat mitä defensiivisen taktiikan toiminteen toteutuminen vaatii sekä minkälainen vuorovaikutus defensiivisestä tekniikasta kohdistuu digitaaliseen artefaktiin.

Taulukko 8. Tarvittavien vastakeinojen ominaisuudet

Mitä T1053 tekee?	Mihin teko kohdistuu?	Miten teolta pyritään suojautumaan?	Miten suojautuminen toteutetaan?	Mitä suojautuminen tekee?
Luo	PLIST-asetus-tiedosto	Koventaminen	Tiedoston käyttöoikeudet	Rajoittaa
		Harhauttaminen	Houkutintiedosto	Väärentää
		Havainnointi	Tiedostoanalyysi	Analysoi
Muokkaa	Ajastettu toiminto	Havainnointi	Ajastetun toiminnon tarkastelu	Analysoi
Kutsuu	Prosessin luonti	Havainnointi	Järjestelmäkutsun tarkastelu	Analysoi
		Havainnointi	Prosessin luonnin tarkastelu	Analysoi
		Eristäminen	Järjestelmäkutsujen suodatus	Suodattaa

Kokonaisuutena ajastettujen toimintojen hyväksikäytöltä suojautumiseen tarvittavat vastakeinojen ominaisuudet perustuvat teknologioihin tai prosesseihin, jotka mahdollistavat havainnoinnin, koventamisen, ansoittamisen sekä eristämisen taulukon 6 mukaisella tavalla. Vastakeinojen ominaisuuksien määrittelyn perusteella hyväksikäytön havainnoinnin mahdollistava teknologia tai teknologiat ovat avainroolissa suojauduttaessa kyseiseltä tekniikalta.

5.3 Tulokset

Tietoverkkohyökkäyksiltä suojautumiseen vaadittavien vastakeinojen ominaisuuksien uhkaperusteinen määrittely luo selkeät geneeriset tarpeet vastakeinojen valinnalle tai kehitykselle. Prosessi vaatii kuitenkin luotettavan ATT&CK-viitekehykseen sidotun uhkatietolähteen ohjaamaan D3FEND-viitekehyksen avulla tehtävää ominaisuuksien määrittelyä. Tutkimuksen perusteella nähdään kuitenkin tarkoituksenmukaisemmaksi määrittää vastakeinojen ominaisuuksia todennäköisille, kuin epätodennäköisille uhkille. Ilman uhkatietoa vastakeinojen ominaisuuksien määrittelyä saattaisi ohjata summittain valitut offensiiviset ATT&CK-tekniikat, joiden perusteella valittava tai kehitettävä teknologia tai prosessi ei välttämättä kohtaisi todellista tarvetta kohdeympäristössä tai organisaatiossa.

Tutkimuksessa käytetyssä prosessissa täytyy kuitenkin ymmärtää, että analysointi ei ikinä anna absoluuttisesti oikeaa tulosta, koska uhkatoimijat saattavat käyttää tietoverkkohyökkäyksissä myös mitä tahansa muuta kohde ympäristön arkkitehtuurin mahdollistamaa offensiivista ATT&CK-tekniikkaa.

ATT&CK-viitekehyksen hyödyntäminen D3FEND-viitekehyksen rinnalla on kuitenkin äärimmäisen helppoa ja luontevaa kuten on suunniteltu. Itselle kuitenkin herää kysymys tuleeko D3FEND-viitekehys syrjäyttämään jossain määrin tulevaisuudessa opinnäytetyöstä ulosrajatut ATT&CK-viitekehyksen objektimalliin kuuluvat havainnointi- ja ehkäisykeinot vai integroidaanko D3FEND mahdollisesti olemassa olevaan ATT&CK objektimalliin erillisenä kokonaisuutena vai jääkö D3FEND-viitekehys vain omaksi kokonaisuudeksi.

Tapaustutkimuksen avulla määritetyt vastakeinojen ominaisuudet ovat kuitenkin hyvin geneerisiä ja ilman laaja-alaista ammattitaitoa ominaisuuksien sitominen tarvittaviin tai olemassa oleviin teknologioihin tai prosesseihin eli vastakeinoihin on hyvin haastavaa. Myös laajemmassa mittakaavassa esimerkiksi työssä käytetyn uhkatietoraportin pohjalta kaikkien 15 raportoidun offensiivisen ATT&CK-tekniikan analysointi vaatisi merkittävästi työtä, mutta toisaalta mahdollistaisi myös ominaisuuksien priorisoinnin paremmassa mittakaavassa esimerkiksi defensiivisten D3FEND-perustekniikoiden avulla.

6 Johtopäätökset ja pohdinta

Kokonaisuutena opinnäytetyön lopputuotos saavuttaa mielestäni työlle asettamani tavoitteet määritellyn laajuuden puitteissa sekä vastaa työtä ohjanneisiin tutkimuskysymyksiin. Opinnäytetyön pitäminen määrätyssä laajuudessa vaati tiukkaa rajaamista myös työn toteutusvaiheessa, koska D3FEND-, sekä ATT&CK-viitekehykset mahdollistavat useita muitakin käyttötapauksia ja tietoperustan aiheet ovat huomattavasti laajempia, kuin opinnäytetyön tavoitteen kannalta työhön sidotut olennaiset osat. Tapaustutkimuksessa yksittäisen uhkaperusteinen tekniikan analysointi riitti kuitenkin antamaan kuvan prosessista ja sillä saavutettavista tuloksista, mutta kokonaisuutena useamman tekniikan analysointi olisi antanut paremman kokonaiskuvan lähestymistavasta.

Tapaustutkimuksessa määritettyjen ominaisuuksien perusteella toteutettava vastakeinojen valinta tai kehitys olisi johdonmukainen jatkokehityskohde opinnäytetyölle. Jatkokehitys vaatisi kuitenkin kehityskohteeksi konkreettisen tai hypoteettisen organisaation, tai kohdeympäristön sekä merkittävästi enemmän aikaa, kuin työssä käsitelty kokonaisuus.

Erillisen haasteen opinnäytetyölle aiheutti suomen kielen terminologia ja käsitteiden määrittely. Tieto-/kyberturvasta kirjoittaminen suomen kielellä aiheuttaa lähtökohtaisesti aina haasteita, koska monia termejä käytetään ristiin tiedostetusti, tai tiedostomatta ja useille englanninkielisille termeille ei löydy kontekstiin sopivaa yhdenmukaista suomenkielistä käännöstä. ATT&CK- ja D3FEND-viitekehysten käsittelyssä päädyin käyttämään pääsääntöisesti alkuperäisiä englanninkielisiä taktiikoiden ja tekniikoiden nimiä käännösten aiheuttamien sekaannusten välttämiseksi.

Kokonaisuudessaan pidän opinnäytetyötä onnistuneena tuotoksena, vaikkakin tapaustutkimus on omasta mielestä hieman rajallinen, mutta työmäärällisesti kuitenkin vielä järkevässä mittakaavassa. Haastavinta opinnäytetyössä oli luoda kokonaisuus, jossa tietoperusta kättelee tapaustutkimuksen kanssa mahdollisimman hyvällä tasolla.

Lähteet

Bodeau, D. & Graubart, R. (2016). *Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms.* Haettu 11.4.2022 osoitteesta https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf

Correa, A. (n.d.). *What is Cyber Threat Intelligence and how is it used?* Haettu 10.4.2022 osoitteesta https://www.malwarepatrol.net/three-types-of-cyber-threat-intelligence/

Kaloroumakis, P. & Smith, M. (2021). *Toward a Knowledge Graph of Cybersecurity Countermeasures.* Haettu 13.4.2022 osoitteesta https://d3fend.mitre.org/resources/D3FEND.pdf

Kyberturvallisuuskeskus. (n.d.). *Opas tietomurtojen havaitsemiseen.* Haettu 12.4.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Opas-tietomurtojen-havaitsemiseen.pdf

Microsoft Corporation. (20.7.2021). *The growing threat of ransomware.* Haettu 14.4.2022 osoitteesta https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/

MITRE Engenuity. (12.11.2019). *MITRE Engenuity Announces the Center for Threat-Informed Defense.* Haettu 10.4.2022 osoitteesta https://mitre-engenuity.org/blog/2019/11/12/mitre-engenuity-announces-the-center-for-threat-informed-defense/

MITRE Engenuity. (2021). *Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild.* Haettu 10.4.2022 osoitteesta https://f.hubspotusercontent20.net/hubfs/7754670/Center%20for%20Threat%20Informed%20Defense/CTID-Sightings-Ecosystem-Report.pdf

MITRE Engenuity. (n.d. -a). *Our Work.* Haettu 11.4.2022 osoitteesta https://ctid.mitre-engenuity.org/our-work/

MITRE Engenuity. (n.d. -b). *About Us.* Haettu 11.4.2022 osoitteesta https://mitre-engenuity.org/about-us/

MITRE Engenuity. (n.d. -c). *Sightings Ecosystem.* Haettu 22.4.2022 osoitteesta https://ctid.mitre-engenuity.org/our-work/sightings/

National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30 reversion 1: Guide for Conducting Risk Assessments.* Haettu 10.4.2022 osoitteesta https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2016). *NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing.* Haettu 10.4.2022 osoitteesta http://dx.doi.org/10.6028/NIST.SP.800-150

Reiber, J. & Wright, C. (2021). *MITRE ATT&CK for dummies, AttackIQ Special Edition*. Haettu 14.4.2022 osoitteesta https://attackiq.com/lp/mitre-attack-for-dummies/

Samtani, S. Abate, M. Benjamin, V. & Li, W. (2019). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. http://dx.doi.org/10.1007/978-3-319-90307-1_8-1

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden sanasto.* http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Strom, B. Applebaum, A. Miller, D. Nickels, K. Pennington, A. & Thomas, C. (2020). *MITRE ATT&CK: Design and Philosophy.* Haettu 7.4.2022 osoitteesta https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

The European Parliament. (2022). *Cybersecurity: main and emerging threats in 2021 (infographic)*. Haettu 8.4.2022 osoitteesta https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic

The MITRE Corporation. (2021a). *MITRE ATT&CK Matrix Poster.* Haettu 8.4.2022 osoitteesta https://attack.mitre.org/docs/attack_matrix_poster_2021_june.pdf

The MITRE Corporation. (2021b). *Scheduled Task/Job.* Haettu 12.4.2022 osoitteesta https://attack.mitre.org/techniques/T1053/

The MITRE Corporation. (2021d). *Updates - October 2021.* Haettu 14.4.2022 osoitteesta https://attack.mitre.org/resources/updates/updates-october-2021/index.html

The Mitre Corporation. (n.d. -a). *THREAT-BASED DEFENSE*. Haettu 8.4.2022 osoitteesta https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

The MITRE Corporation. (n.d. -b). *About the D3FEND Knowledge Graph Project.* Haettu 10.4.2022 osoitteesta https://d3fend.mitre.org/about

The MITRE Corporation. (n.d. -c). *OUR HISTORY.* Haettu 10.4.2022 osoitteesta https://www.mitre.org/about/our-history

The MITRE Corporation. (n.d. -d). *Corporate Overview.* Haettu 11.4.2022 osoitteesta https://www.mitre.org/about/corporate-overview

The MITRE Corporation. (n.d. -e). *ATT&CK Sightings.* Haettu 11.4.2022 osoitteesta https://attack.mitre.org/resources/sightings/

The MITRE Corporation. (n.d. -f). *Enterprise tactics.* Haettu 9.4.2022 osoitteesta https://attack.mitre.org/tactics/enterprise/

The MITRE Corporation. (n.d. -g). *D3FEND A knowledge graph of cybersecurity countermeasures 0.10.0-BETA-2.* Haettu 15.4.2022 osoitteesta https://d3fend.mitre.org/poster/

The MITRE Corporation. (n.d. -h). *Harden.* Haettu 20.4.2022 osoitteesta https://d3fend.mitre.org/tactic/d3f:Harden/

The MITRE Corporation. (n.d. -i). *Detect.* Haettu 20.4.2022 osoitteesta https://d3fend.mitre.org/tactic/d3f:Detect

The MITRE Corporation. (n.d. -j). *Isolate.* Haettu 20.4.2022 osoitteesta https://d3fend.mitre.org/tactic/d3f:Isolate

The MITRE Corporation. (n.d. -k). *Deceive.* Haettu 20.4.2022 osoitteesta https://d3fend.mitre.org/tactic/d3f:Deceive

The MITRE Corporation. (n.d. -l). *Evict.* Haettu 20.4.2022 osoitteesta https://d3fend.mitre.org/tactic/d3f:Evict

The MITRE Corporation. (n.d. -m). *Digital Artifact Ontology.* Haettu 18.4.2022 osoitteesta https://d3fend.mitre.org/dao

The MITRE Corporation. (n.d. -n). *Scheduled Task/Job Execution - T1053.* Haettu 16.4.2022 osoitteesta https://d3fend.mitre.org/offensive-technique/attack/T1053

The MITRE Corporation. (n.d. -o). *Property List File.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/dao/artifact/d3f:PropertyListFile/

The MITRE Corporation. (n.d. -p). *Task Schedule.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/dao/artifact/d3f:TaskSchedule/

The MITRE Corporation. (n.d. -q). *Create Process.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/dao/artifact/d3f:CreateProcess/

The MITRE Corporation. (n.d. -r). *Local File Permissions.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:LocalFilePermissions/

The MITRE Corporation. (n.d. -s). *Decoy File.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:DecoyFile/

The MITRE Corporation. (n.d. -t). *File Analysis.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:FileAnalysis/

The MITRE Corporation. (n.d. -u). *System Call Analysis.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:SystemCallAnalysis/

The MITRE Corporation. (n.d. -v). *Scheduled Job Analysis.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:ScheduledJobAnalysis/

The MITRE Corporation. (n.d. -w). *Process Spawn Analysis.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:ProcessSpawnAnalysis/

The MITRE Corporation. (n.d. -x). *System Call Filtering.* Haettu 23.4.2022 osoitteesta https://d3fend.mitre.org/technique/d3f:SystemCallFiltering/