Juri Ihanus

SISÄPIIRIUHKAN HYÖKKÄYSKETJU – SISÄPIIRIUHKAN HYÖKKÄYSVAIHEIDEN MALLINTAMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Ihanus, Juri
Sisäpiiriuhkan hyökkäysketju – sisäpiiriuhkan hyökkäysvaiheiden mallintaminen
Jyväskylä: Jyväskylän yliopisto, 2023, 67 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Tässä tutkielmassa tutkittiin sisäpiiriuhkaa ja sen hyökkäysvaiheita. Organisaatioihin ja niiden käyttämään tietoon kohdistuu monenlaisia uhkia, joista osa syntyy organisaatioiden sisältä. Organisaation omaisuuteen luvallisen pääsyoikeuden saaneita yksilöitä voidaan kutsua sisäpiiriläisiksi. Sisäpiiriläisten toimenpiteet voivat aiheuttaa haittaa organisaatiolle, jolloin puhutaan sisäpiiriuhkasta. Sisäpiiriuhka voi olla joko tahatonta tai pahantahtoista. Kyberturvallisuuden alalta löytyy useita malleja pahantahtoisten hyökkääjien tekemien hyökkäysten mallintamiseen. Sisäpiiriuhkan osalta malleissa on kuitenkin puutteita, mikä tekee tutkielmasta tärkeän. Tutkielman päätavoitteena oli kehittää malli, jolla voidaan kuvata tietoon kohdistuvan sisäpiiriuhkan hyökkäysvaiheita. Tutkielmassa analysoitiin julkisista lähteistä saatavilla olevia sisäpiiriuhkan tapausaineistoja laadullisen sisällönanalyysin keinoin. Analyysin tavoitteena oli selvittää, millaisia vaiheita sisäpiiriuhkan hyökkäyksissä oli. Analyysissä käytettiin hyödyksi aiempaa teoriaa kyberhyökkäysten vaiheista. Analyysin tuloksia hyödynnettiin kehittämällä uusi malli, joka kuvaa tietoon kohdistuvan sisäpiiriuhkan hyökkäysvaiheita. Uuden mallin kehittäminen tehtiin kehittämistutkimuksen keinoin ja mallin toimivuutta verrattiin olemassa oleviin hyökkääjien toimenpiteitä kuvaaviin malleihin. Tutkimuksessa havaittiin, että aiemmat mallit eivät kykene kattavasti kuvaamaan sisäpiiriuhkan hyökkäysvaiheita. Uuden mallin avulla voidaan kuvata sisäpiiriuhkan hyökkäysvaiheita kattavammin ja mallia voidaan hyödyntää sisäpiiriuhkan hallinnassa organisaatioissa.

Asiasanat: sisäpiiriuhka, hyökkäysketju, MITRE ATT&CK, Unified Kill Chain

ABSTRACT

Ihanus, Juri
Insider threat kill chain – modeling the attack phases of insider threat
Jyväskylä: University of Jyväskylä, 2023, 67 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

This study examined insider threat and the attack phases involved in insider threat cases. Organizations need to protect their information assets from multiple different threat actors, including those from within the organization. Individuals who have been given authorized access to the assets of an organization can be called insiders. Insiders can cause damage to an organization through their actions. The potential for such actions is called "insider threat". Insider threat can be either malicious or unintentional. The field of cyber security has multiple models which illustrate phases of malicious attacks on organizations. Such models are known to have issues regarding insider threat, which makes this study important. The main purpose of this study was to create a model which illustrates the attack phases of insider threat targeting information assets. In the study, a qualitative analysis was conducted on publicly available insider threat case studies. The purpose of the analysis was to find out what kind of phases are involved in attacks caused by insider threat, utilizing previous theory on cyber-attack phases. The results of the analysis were used in developing a new model for insider threat attacks targeting information assets. The development of the new model was conducted through design science research, and the model was evaluated against earlier attack models. The study found that the coverage of earlier models regarding insider attack phases was lacking. The new model has better coverage of all the phases of insider attack phases and the model can be utilized in insider threat management in organizations.

Keywords: insider threat, kill chain model, MITRE ATT&CK, Unified Kill Chain

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Nykypäivänä organisaatiot käsittelevät ja hyödyntävät yhä enemmän dataa ja tietoa. Tietoa hyödynnetään mm. päätöksenteossa, liiketoimintaprosessien tukena sekä kriittisen tärkeänä osana liiketoimintaa, esimerkiksi aineettoman omaisuuden osalta. Tiedon tullessa tärkeämmäksi osaksi organisaatioiden toimintaa, myös tietoturvallisuuden merkitys tulee tärkeämmäksi. Kyberrikollisuudesta syntyneiden vahinkojen määrä onkin raporttien mukaan kasvanut vuosi vuodelta (Federal Bureau of Investigation, 2022). Tietoon kohdistuu erilaisia uhkia, kuten organisaation ulkopuolisten kyberrikollisten tekemät hyökkäykset. Organisaatioiden tulisi huomioida ulkoisten uhkien lisäksi myös organisaation sisältä tulevat uhkat. Perinteisesti tietoturvallisuudessa keskitytään ulkoisilta uhkilta suojautumiseen, mutta alan raporttien mukaan myös sisäpiiriuhkan rooli ja siitä johtuvat vahingot ja tapausmäärät ovat kasvaneet merkittävästi viime vuosien aikana (Ponemon Institute, 2020). Sisäpiiriuhkan kasvavasta roolista hyökkäyksistä voidaan päätellä, että sitä ei kyetä hallitsemaan riittävän tehokkaasti.

Sisäpiiriuhka voidaan määritellä potentiaalina sille, että yksilö, jolla on luvallinen pääsy organisaation omaisuuteen, käyttää pääsyoikeuttaan, joko pahantahtoisesti tai tahattomasti, siten että siitä voi aiheutua vahinkoja organisaatiolle (Costa, 2017). Tämä lyhyt määritelmä kuvaa osaset, joista sisäpiiriuhka koostuu:

1. yksilö, jolla on luvallinen pääsy (sisäpiiriläinen)
2. omaisuus, johon uhka kohdistuu
3. yksilön tarkoitusperät tai aikeet
4. vaikutukset (vahingot)

Uhka on monitahoinen, ja kukin yllä mainittu osanen voidaan pilkkoa pienempiin osiin. Ylätasolla sisäpiiriläisten luokittelu tehdään usein yksilön tarkoitusperien mukaan pahantahtoisiin ja tahattomiin tekijöihin. Määritelmässä yksilöllä voidaan tarkoittaa esimerkiksi työntekijää, yhteistyökumppania tai jotain muuta tahoa, jolle organisaatio on jakanut pääsyoikeuksia. Omaisuudella voidaan tarkoittaa esimerkiksi tuotekehitysdataa, järjestelmiä, henkilöresursseja tai muita organisaatiolle tärkeitä resursseja. Uhkan monitahoisuus tekee sen hallitsemisesta haastavan ongelman. Sisäpiiriuhkan haastavuus on tunnistettu

alalla, ja se on nimetty yhdeksi hankalimmista tietoturvallisuuteen liittyvistä ongelmista (INFOSEC Research Council, 2005). Sisäpiiriuhkan erityispiirteenä on, että pelkät tekniset turvatoimet eivät riitä uhkan torjumiseen ja havainnointiin, vaan tarvitaan myös ei-teknisiä indikaattoreita, kuten tekijän käyttäytymisessä tapahtuvia muutoksia (Cappelli, Moore & Trzeciak, 2012, p. 14).

Kyberhyökkäyksien mallintamiseen on käytetty usein niin kutsuttuja hyökkäysketju-malleja Hyökkäysketjujen tarkoitus on kuvata hyökkääjän toimenpiteitä kuvaamalla hyökkääjän toimenpiteitä hyökkäyksen eri vaiheissa. Hyökkäysketju-malleja on monenlaisia ja niitä on tehty eri tarkoituksia varten. Esimerkiksi Lehto (2022) kuvasi kehittyneiden APT-hyökkäjien käyttämiä hyökkäysvaiheita hyökkäysketjun muodossa. Kyberalalla hyvin tunnetut viitekehykset ja hyökkäysketjut keskittyvät usein ulkopuolisiin hyökkääjiin, eikä sisäpiiriläisten hyökkäyksiin liittyviä erikoispiirteitä välttämättä ole huomioitu riittävästi. Alalla suosittu MITRE ATT&CK-viitekehys kuvaa todellisissa kyberhyökkäyksissä havaittuja hyökkääjien käyttämiä tekniikoita ja taktiikoita. Tätä viitekehystä voidaan joiltain osin soveltaa myös sisäpiiriläisten hyökkäyksiin (Hlavek, Folk, Sundar, & Baker, 2022), mutta malli ei ota kantaa esimerkiksi uhkan tunnistamiseen ja lieventämiseen etukäteen, eikä huomioi kattavasti sisäpiiriuhkan ulottuvuuksia teknisten järjestelmien ulkopuolella. Hyökkäysketjumallit (engl. kill chain) kuten Cyber Kill Chain (Lockheed Martin, 2022) ja Unified Kill Chain (Pols, 2017) käsittelevät hyökkäyksiä korkealla abstraktiotasolla, ja niiden soveltaminen sisäpiiriuhkan hallitsemiseen voi olla haastavaa.

Sisäpiiriuhkan ulottuvuuksien on hahmotettu tutkimuksen keinoin ja kehittämällä erilaisia malleja. Uhkaa on esimerkiksi luokiteltu systemaattisen kirjallisuuskatsauksen keinoin (Homoliak, Toffalini, Guarnizo, Elovici, & Ochoa, 2020). Uhkan psykologisia ulottuvuuksia on myös tutkittu esimerkiksi kartoittamalla uhkan yhteyksiä negatiivisiin persoonallisuuspiirteisiin (Maasberg, Warren & Beebe, 2015). Eräässä tutkimuksessa kerättiin myös yksilöiden käyttäytymiseen liittyviä teknisiä ja sosiaalisia indikaattoreita (Dupuis & Khadeer, 2016). Uhkan hahmottamiseksi on luotu viitekehyksiä, joista esimerkkinä voidaan mainita uhkan eri ulottuvuuksien hahmottamiseen käytettävä viitekehys, joka luotiin todellisten hyökkäysten pohjalta (Nurse ym., 2014).

Sisäpiiriuhkasta johtuvat hyökkäykset eroavat ulkopuolisten toteuttamista hyökkäyksistä merkittävästi, ja niiden torjunta -ja havainnointikeinot voivat olla myös monin osin erilaisia. Esimerkiksi sisäpiiriläisen tietoisesti tekemä hyökkäys voi saada alkunsa jostakin negatiivisesta kokemuksesta työpaikalla, jolloin uhkan mallintamisessa on huomioitava myös ihmiskäyttäytymiseen liittyviä ulottuvuudet. Uhkan torjuminen ja sopivien kontrollien valitseminen on haastavaa, koska organisaation on löydettävä tasapaino luottamuksen ja kontrollin välillä. Liiallisten kontrollikeinojen käyttäminen voi vaikeuttaa työntekoa ja aiheuttaa tyytymättömyyttä työntekijöissä, kun taas liiallinen luottamus heikentää kyvykkyyttä havaita uhkien kehittymistä (Cappelli, Moore & Trzeciak, 2012, p. 46).

1.1 Tutkimusongelmat

Tutkimusta suunnitellessa tehtiin olettamus, että nykyisissä kyberturvallisuuden hyökkäysmalleissa voi olla sisäpiiriuhkaan liittyviä puutteita. Tutkimusta lähdettiin suunnittelemaan tämän olettaman pohjalta. Tutkielman päätutkimusongelma on:

- Millaisella mallilla voidaan kattavasti kuvata tietoon kohdistuvan sisäpiiriuhkan hyökkäysvaiheet?

Päätutkimusongelman tukena vastataan myös seuraaviin apututkimuskysymyksiin:

- Millä tavalla sisäpiiriuhkan hyökkäyksiä on tapahtunut?
- Millaisilla malleilla kyberhyökkäyksien vaiheita voidaan kuvata?

1.2 Tutkielman sisältö

Tutkielman toisessa luvussa esitellään lyhyesti joitakin kyberturvallisuuden alalla käytettyjä hyökkäysmalleja sekä sisäpiiriuhkaan liittyviä hyökkäysmalleja. Tutkielman kolmannessa luvussa esitellään sisäpiiriuhkan perusmääritelmiä, erilaisia luokitteluja sekä joitakin sisäpiiriuhkan torjumiseen ja havaitsemiseen käytettäviä menetelmiä. Tutkimuksen neljäs luku koostuu tutkimusmenetelmien ja aineiston esittelystä sekä tutkimuksen luotettavuuden arvioinnista. Viidennessä luvussa käydään läpi tutkielman sisällönanalyysin ja kehittämistutkimuksen eteneminen ja esitellään ja tulkitaan tutkimuksen eri vaiheissa saatuja tuloksia. Kuudennessa luvussa pohditaan tutkimuksen tuloksia, niiden merkitystä ja jatkotutkimusaiheita.

2 KYBERTURVALLISUUDEN JA SISÄPIIRIUHKAN HYÖKKÄYSMALLEJA

Tässä luvussa kuvataan malleja, joita käytetään kyberhyökkäysten kuvaamiseen. Hyökkäysmalleja voidaan hyödyntää hyökkäyksien vastatoimien suunnittelussa ja analysoinnissa. Perinteisissä poikkeamankäsittelyn malleissa poikkeaman vastatoimia suoritetaan usein vasta poikkeamien seurauksena, ja löydetään jokin korjattava vika tai haavoittuvuus, josta poikkeama johtui (Mitropoulos, Patsos & Douligeris, 2006, s. 1). Perinteiset poikkeamankäsittelyn mallit useimmiten keskittyvät enemmän ympäristössä oleviin haavoittuvuuksiin kuin ympäristöön kohdistuviin uhkiin. Perinteisissä malleissa havaittiin puutteita tutkijoiden toimesta, kun kehittyneiden APT-uhkatoimijoiden (engl. Advanced Persistent Threat) tekemiä kyberhyökkäyksiä yleistyivät ja niitä tutkittiin tarkemmin (Hutchins, Cloppert & Amin, 2010). APT-hyökkääjillä on käytössään voimakkaita kyvykkyyksiä ja merkittävästi resursseja, joilla ne voivat saavuttaa tavoitteensa hyödyntämällä useita eri hyökkäysvektoreita, ja ne voivat käyttää hyökkäyksiinsä paljon resursseja ja aikaa (National Institute of Standards and Technology, 2011). APT-hyökkäyksistä puhutaan joskus myös ”kohdistettuina hyökkäyksinä” (Sanastokeskus TSK ry, 2018).

APT-hyökkäyksistä saatujen tietojen perusteella Lockheed Martinin tutkijoiden toimesta kehitettiin vaiheittaiseen hyökkäysketjuun perustuva malli, jonka tarkoituksena on keskittyä haavoittuvuuksien paikkaamisen lisäksi myös uhkien lieventämiseen (Hutchins Cloppert & Amin, 2010). Hyökkäysketjulla tarkoitetaan vaiheittaista mallia, jonka avulla voidaan hahmottaa hyökkäyksen vaiheita ja hyökkääjän toimenpiteitä hyökkäyksen eri vaiheissa. Hyökkäysketjumallin avulla voidaan suunnitella vastatoimia hyökkäyksen eri vaiheissa ja voidaan esimerkiksi hahmottaa mahdollisia puutteita vastatoimien kattavuudessa. Mallien vaiheita voidaan hyödyntää myös digitaalisessa forensiikassa ja uhkatiedon jakamisessa. Hyökkäysketjuun perustuvia malleja käytetään myös sotilaskäytössä, esimerkiksi Yhdysvaltain ilmavoimat ovat käyttäneet ”F2T2EA”-hyökkäysketjua (US Air Force, 2021, s. 27). Sotilaskäytössä hyökkäysketjuissa on usein ajatuksena, että hyökkäys voidaan katkaista, kunhan estetään hyökkääjän toiminta jossakin ketjun vaiheessa. Tietoturvallisuuden tutkimuksessa vaiheittaisia

malleja on hyödynnetty esimerkiksi Willisonin ja Siposen (2009) tutkimuksessa sisäpiiriuhkan torjuntakeinojen hahmottamiseksi. Vaiheittaisia malleja on käytetty eri aloilla ja monia tarkoituksia varten. Kyberturvallisuuden kontekstissa hyökkääjän toimintaa kuvaavia vaiheittaisia malleja on kehitetty viime vuosien aikana useita. Hyökkäysketjujen lisäksi toinen kyberturvallisuuden alalla käytetty malli on niin kutsuttu ”hyökkäysmatriisi” (engl. attack matrix), jossa kuvataan hyökkääjän käyttämiä tekniikoita (engl. techniques), jotka luokitellaan taktiikoiden (engl. tactics) alle. Taktiikat voivat kuvata suurin piirtein samaa abstraktiotasoa kuin hyökkäysketju -malleissa kuvatut vaiheet (Pols, 2017).

Kyberhyökkäyksien monimuotoisuuden takia hyökkäysmalleja on kehitetty useita, tässä luvussa esitellään seuraavat mallit:

1. Lockheed Martin Cyber Kill Chain (CKC)
2. Bryant Kill-Chain (BKC)
3. MITRE ATT&CK
4. Unified Kill Chain (UKC)
5. Insider Threat Cyber Kill Chain
6. Insider Attack Matrix

Edellä olevan listan neljä ensimmäistä mallia kuvaavat kyberhyökkäyksiä yleisemmin tai APT-uhkaan keskittyen, viimeiset kaksi mallia keskittyvät sisäpiiriuhkaan. Sisäpiiriuhkasta kerrotaan tarkemmin luvussa 3.

2.1 Lockheed Martin Cyber Kill Chain (CKC)

Lockheed Martinin tutkijat kehittivät APT-uhkien tutkimushavainoihin vastatakseen uhkatietoon perustuvan mallin, joka tunnetaan nykyään nimellä ”Cyber Kill Chain” tai lyhyemmin CKC. CKC:tä pidetään usein alkuperäisenä kyberhyökkäyksiä kuvaavana hyökkäysketjumallina (Bryant & Saiedian, 2017). Lockheed Martinin tutkijat kritisoivat perinteisiä haavoittuvuuksiin keskittyviä malleja ja pyrkivät mallillaan mahdollistamaan haavoittuvuuksien hallinnan lisäksi myös uhkien hallinnan (Hutchins, Cloppert & Amin, 2010).

CKC:n vaiheet ovat seuraavat:

1. Tiedustelu (engl. reconnaissance): hyökkäyksen kohteiden tutkiminen, tunnistaminen ja valinta
2. Aseistautuminen (engl. weaponization): valmistelevat toimenpiteet hyökkäystä varten, mm. infrastruktuurin valmistelu, haittaohjelmakoodin luominen
3. Toimittaminen (engl. delivery): haitallisen koodin tai vastaavan toimittaminen ympäristöön
4. Hyväksikäyttö (engl. exploitation): toimitetun kohteen käyttäminen ympäristössä
5. Asennus (engl. installation): takaoven asentaminen ympäristöön pysyvän jalansijan luomiseksi
6. Komento ja hallinta (engl. command and control (C2): komento- ja hallintakanavan luominen ja käyttö

7. Toiminnot päämäärässä (engl. actions on objectives): hyökkääjän tavoittelemat toimenpiteet, esimerkiksi tiedon varastaminen

Vaiheet on kuvattu oheisessa kuvassa (Kuva 1). Ymmärtämällä hyökkäyksen vaiheet, puolustaja voi suunnitella toimenpiteitä, voidaan havaita, estää, häiritä, heikentää, harhauttaa tai tuhota hyökkääjän tekemiä toimenpiteitä (Hutchins ym., 2010).

Kuva 1 Lockheed Martin Cyber Kill Chain (Hutchins, ym., 2010)

CKC-mallin mukaan hyökkääjän on käytävä läpi kaikki ketjun vaiheet, ennen kuin se voi saavuttaa haluamansa päämäärän. Lockheed Martinin tutkijoiden mukaan CKC-malli haastaa perinteisen käsityksen siitä, että hyökkääjän on löydettävä vain yksi heikkous puolustuksessa päästäkseen päämääriinsä. Mallin mukaan hyökkääjän on kuitenkin onnistuttava kaikissa hyökkäyksen vaiheissa, ja puolustajalla voi olla kyvykkyys keskeyttää hyökkäys ennen kuin hyökkääjä pääsee kulkemaan koko ketjun loppuun asti (Hutchins ym., 2010, s. 6-7).

Lockheed Martinin malliin on kohdistettu kritiikkiä asiantuntijoiden toimesta. Mallin on sanottu vahvistavan vanhanaikaista nk. ”kovaan ulkokuoreen” ja haittaohjelmien torjuntaan perustuvaa ajattelua. Mallin on myös sanottu keskittyvän tunkeutumisen estämiseen sen sijaan, että pyrittäisiin havaitsemaan ja torjumaan ympäristön sisällä toimivia uhkia (Engel, 2014). Kritiikkiä on kohdistettu myös mallin heikkoon kykyyn torjua sisäpiiriuhkaa, koska sisäpiiriläisten ei tarvitse seurata mallin mukaista hyökkäysketjua alusta alkaen (Reidy, 2013).

2.2 Bryant Kill Chain (BKC)

CKC-mallissa havaittiin puutteita puutteita erityisesti ympäristöissä, joissa useilta sensoreilta koottua dataa käsitellään tietoturvapoikkeamien tutkinnassa (Bryant & Saiedian, 2017, s. 2). CKC-mallin vaiheiden ja sensoreilta saatujen tapahtumatietojen yhdistely johtaa tutkijoiden mukaan manuaalisiin ratkaisuihin, joista seuraa epäjohdonmukaisuuksia. Näihin ongelmiin ratkaisuna tutkijat kehittivät uuden hyökkäysketjun, jota tutkijat kutsuivat nimellä ”Bryant Kill-Chain” (BKC) (Bryant & Saiedian, 2017).

BKC:ssä on seitsemän vaihetta kuten Lockheed Martinin mallissakin, mutta joitakin vaiheita on nimetty uudelleen tai siirretty. Mallin vaiheet on kuvattu oheisessa kuviossa (Kuva 2). BKC:n vaiheet ovat seuraavat (Bryant & Saiedian, 2017):

1. Tiedustelu (engl. reconnaissance): hyökkäyksen kohteiden tutkiminen, tunnistaminen ja valinta
2. Toimittaminen (engl. delivery): haitallisen koodin toimittaminen kohteena olevaan ympäristöön

3. Asennus (engl. installation): takaoven asentaminen ympäristöön pysyvän jalansijan luomiseksi
4. Käyttöoikeuksien korottaminen (engl. privilege escalation): käyttöoikeuksien laajentaminen, siten että saadaan tavallista laajemmat oikeudet järjestelmiin
5. Tunkeutumisen laajentaminen (engl. lateral movement): jalansijan laajentaminen ympäristössä, muihin yhdistettäviin järjestelmiin tunkeutuminen
6. Toiminnot päämäärässä (engl. actions on objectives): hyökkääjän tavoittelemat toimenpiteet, esimerkiksi tiedon varastamisen käynnistäminen
7. Tiedon varastaminen (engl. exfiltration): hyökkääjälle kiinnostavan tiedon siirtäminen hyökkääjän haltuun, esimerkiksi salattua verkkoyhteyttä hyödyntäen

Tutkijat havaitsivat, että uudella mallilla oli helpompi luokitella lokitapahtumia hyökkäysvaiheiden alle johdonmukaisesti. Tapahtumatietoja voitiin yhdistellä mallia käyttämällä tehokkaammin tietoturvatiedon ja -tapahtumien hallintajärjestelmässä (SIEM) ja manuaalisia toimenpiteitä saatiin vähennettyä (Bryant & Saiedian, 2017, s. 11-13). BKC:n avulla voitiin tutkijoiden mukaan suorittaa myös paremmin järjestelmällistä tutkintaa kyberhyökkäyksistä jääneiden lokijälkien pohjalta.

Kuva 2 Bryant Kill-Chain (Bryant & Saiedian, 2017)

CKC-mallin 5. vaihe ”asennus” tapahtuu BKC-mallissa jo vaiheessa 3. Lisäksi malliin on lisätty kokonaan uusina vaiheina ”käyttöoikeuksien korottaminen”, ”tunkeutumisen laajentaminen” ja ”tiedon varastaminen”. Mallissa on jätetty pois CKC-mallin vaihe ”aseistautuminen”, koska tutkijoiden mukaan puolustaja ei voi havaita tätä vaihetta ja se nähtiin tarpeettomaksi. Mallissa keskitytään enemmän hyökkääjän suorittamiin toimiin suojattavassa ympäristössä kuin CKC-malissa. Hyökkääjän toimenpiteistä voi jäädä tutkittavia lokijälkiä, ja malli soveltuu siten CKC-mallia paremmin käytettäväksi tunkeutumisten tutkinnassa käytännössä (Bryant & Saiedian, 2017).

2.3 MITRE ATT&CK

MITRE ATT&CK on yhdysvaltalaisen, voittoa tavoittelemattoman Mitre-yrityksen kehittämä viitekehys, johon kerätään hyökkääjien käyttämiä tekniikoita ja taktiikoita käytännössä tapahtuneiden kyberhyökkäysten pohjalta. ATT&CK-viitekehyksessä tekniikat on luokiteltu yhden tai useamman taktiikan alle.

Taktiikalla tarkoitetaan hyökkääjän taktista tavoitetta, eli syytä sille miksi hyökkääjä tekee tiettyjä toimenpiteitä. Tekniikalla tarkoitetaan toimenpiteitä, joita hyökkääjä suorittaa saavuttaakseen jonkin taktisen maalin (Strom, 2018).

ATT&CK-viitekehyksen taktiikat ovat seuraavat (MITRE, 2022a):

- Tiedustelu (engl. reconnaissance): hyökkääjä kerää tietoa tulevia operaatioita varten
- Resurssien kehittäminen (engl. resource development): hyökkääjä luo resurssit hyökkäyksen tukemiseksi
- Alustava jalansija (engl. initial access): hyökkääjä yrittää luoda jalansijan ympäristöön
- Suorittaminen (engl. execution): hyökkääjä yrittää suorittaa haitallista koodia
- Jalansijan säilyttäminen (engl. persistence): hyökkää yrittää säilyttää jalansijansa
- Käyttöoikeuksien korottaminen (engl. privilege escalation): hyökkääjä yrittää saavuttaa korkeamman tason käyttöoikeudet
- Turvatoimien välttely (engl. defense evasion): hyökkääjä yrittää vältellä havaituksi tulemista
- Pääsytietojen haltuunotto (engl. credential access): hyökkääjä yrittää varastaa käyttäjätunnuksia ja salasanoja
- Kohteiden etsiminen (engl. discovery): hyökkääjä yrittää tutkia ympäristöä ja löytää kiinnostavia kohteita
- Tunkeutumisen laajentaminen (engl. lateral movement): hyökkääjä yrittää liikkua ympäristössä
- Tiedon kerääminen (engl. collection): hyökkääjä yrittää kerätä sille kiinnostavaa tietoa
- Tiedon varastaminen (engl. exfiltration): hyökkäjä yrittää varastaa tietoa
- Vaikutukset (engl. impact): hyökkääjä yrittää muokata, häiritä tai tuhota järjestelmiä tai tietoja

ATT&CK-viitekehyksessä ei ole asetettu taktiikoita aikajärjestykseen hyökkäyksen etenemisen kannalta, minkä takia edellä oleva listakaan ei ole numeroitu. Taktiikoita tutkimalla voidaan havaita, että osa taktiikoista on samoja kuin aiemmin esiteltyjen hyökkäysketjujen vaiheet. Viitekehyksessä tekniikat on ryhmitelty taktiikoiden alle ja osa tekniikoista on jaettu useampaan alitekniikkaan. Tekniikoita on viitekehyksessä yhteensä 193 ja alitekniikoita 401 (MITRE, 2022b). Tekniikat ovat taktiikoihin verrattuna alemmalla abstraktiotasolla ja kuvaavat hyökkääjän toteuttamia käytännön toimia järjestelmässä. Esimerkiksi ”Vaikutukset”-taktiikan alla löytyy muun muassa levyjen ylikirjoitus (engl. disk wipe) ja järjestelmän sammutus tai uudelleenkäynnistys (engl. system shutdown/reboot) (MITRE, 2019a). Taktiikoita ja tekniikoita on luokiteltu Mitren toimesta hyökkäysmatriiseiksi. Matriiseissa on kuvattu tietynlaisen kohteen tai ympäristön relevantit taktiikat ja tekniikat. Tällä hetkellä matriiseja on kolmessa kategoriassa: yritykset (engl. enterprise), mobiili (engl. mobile) ja teollisuuden ohjausjärjestelmät (engl. ICS).

ATT&CK-viitekehyksen avulla voidaan kehittää keinoja hyökkääjien toiminnan havaitsemiseksi ympäristöissä ja viitekehyksessä käytettyä sanastoa voidaan hyödyntää uhkatiedon jakamisessa. Tästä on hyötyä esimerkiksi tiettyihin uhkaryhmittymiin liittyvien tekniikoiden, taktiikoiden ja menettelytapojen eli TTP-tietojen (engl. techniques, tactics and procedures) jakamisessa (Strom, 2018).

2.4 Unified Kill Chain (UKC)

Unified Kill Chain (UKC)-malli esiteltiin Paul Polsin toimesta vuonna 2017. Malli kehitettiin hyödyntäen laadullisia tutkimusmenetelmiä ja kehittämistutkimusta. UKC-mallin tavoitteena on yhdistellä MITRE ATT&CK-mallin taktiikoita ja Lockheed Martinin CKC-malliin kehitettyjä parannusehdotuksia yhdeksi malliksi (Pols, 2017). UKC-mallin kehittämisessä käytettiin esimerkiksi tapauskuvauksia APT-hyökkäyksistä ja simuloiduista hyökkäyksistä todellisiin organisaatioihin (Pols, 2017, s. 13-14).

UKC-mallin kehittäneessä tutkimuksessa havainnoitiin yhteneväisyyksiä MITRE ATT&CK-mallin taktiikoiden ja hyökkäysketjumallien vaiheiden välillä. Mallissa yhdisteltiin hyökkäysketjumalleissa esitellyt vaiheet ja ATT&CK-mallin taktiikat yhdeksi ketjumaiseksi malliksi. Tutkimuksessa hyödynnettiin aiemmin tässä luvussa esiteltyä BKC-mallia sekä muita alkuperäiseen CKC-malliin tehtyjä parannusehdotuksia (Pols, 2017, s. 27–28).

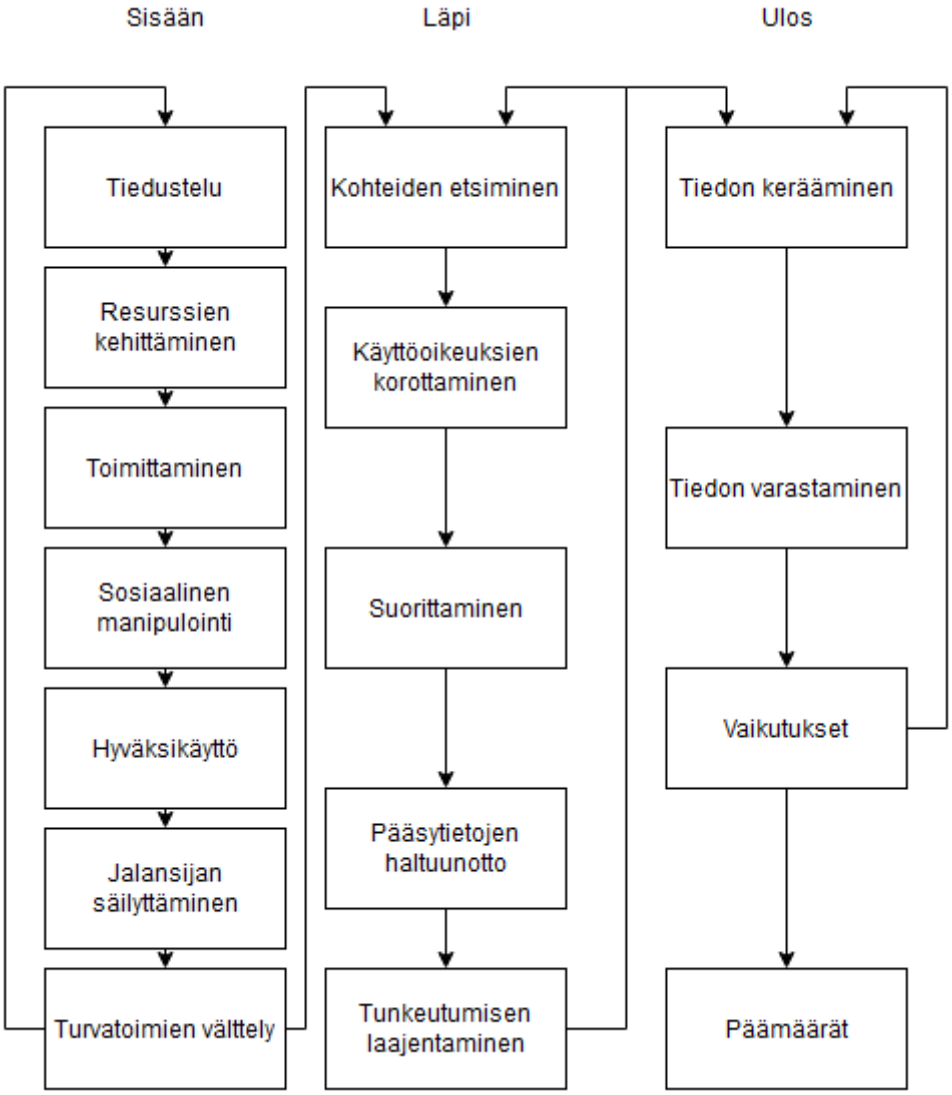
UKC-malliin kuuluu 18 erillistä vaihetta, jotka ovat listattuna alla (Pols, 2017):

1. Tiedustelu (engl. reconnaissance): kohteiden tutkiminen, tunnistaminen ja valinta aktiivisen ja passiivisen tiedustelun keinoin
2. Aseistautuminen (engl. weaponization), myöhemmin korvattu vaiheella ”resurssien kehittäminen” (engl. resource development) (Pols, 2022): valmistelevat toimenpiteet hyökkäystä varten, mm. infrastruktuurin valmistelu, haittaohjelmakoodin luominen
3. Toimittaminen (engl. delivery): aseistetun kohteen toimittaminen ympäristöön
4. Käyttäjän (sosiaalinen) manipulointi (engl. social engineering): henkilöiden (käyttäjien) manipuloiminen hyökkääjän tarkoitusperien mukaisesti
5. Hyväksikäyttö (engl. exploitation): toimitetun kohteen käyttäminen ympäristössä
6. Jalansijan säilyttäminen (engl. persistence): toimintaa, jolla hyökkääjä pyrkii säilyttämään jalansijansa ympäristössä
7. Turvatoimien välttely (engl. defense evasion): hyökkääjän toimet, joilla pyritään välttämään havainnointia ja muita suojakeinoja
8. Komento ja hallinta (engl. command and control (C2): komento- ja hallintakanavan luominen ja käyttö

9. Kauttatunnelointi (engl. pivoting): liikenteen tunnelointi jonkin järjestelmän läpi, että saavutetaan muutoin hyökkääjän tavoittamattomissa olevia kohteita
10. Ympäristön tutkiminen (engl. discovery): ympäristössä olevien kohteiden tutkiminen ja löydösten tekeminen
11. Käyttöoikeuksien korottaminen (engl. privilege escalation): käyttöoikeuksien laajentaminen, siten että saadaan tavallista laajemmat oikeudet järjestelmiin
12. Suorittaminen (engl. execution): hyökkääjän hallitseman koodin tai ohjelman ajaminen järjestelmässä
13. Pääsytietojen haltuunotto (engl. credential access): tunnusten haltuunotto ja käyttö hyökkääjän toimesta
14. Tunkeutumisen laajentaminen (engl. lateral movement): jalansijan laajentaminen ympäristössä, muihin yhdistettäviin järjestelmiin tunkeutuminen
15. Tiedon kerääminen (engl. collection): hyökkääjälle kiinnostavan tiedon tunnistaminen ja kerääminen ympäristöstä
16. Tiedon varastaminen (engl. exfiltration): hyökkääjälle kiinnostavan tiedon siirtäminen hyökkääjän haltuun, esimerkiksi salattua verkkoyhteyttä hyödyntäen
17. Kohdejärjestelmän manipulointi (engl. target manipulation), myöhemmin korvattu vaiheella ”Vaikutukset” (engl. impact) (Pols, 2022): kohdejärjestelmän manipulointi siten että hyökkääjä pääsee lähemmäs päämääriään
18. Päämäärät (engl. objectives): Hyökkäyksen sosiotekniset tavoitteet

UKC-mallin 18 vaihetta voidaan ryhmitellä kolmeen kategoriaan: alustava jalansija (engl. initial foothold), verkossa levittäytyminen (engl. network propagation) ja toiminnot päämäärässä (engl. actions on objectives). Alustavan jalansijan luomisessa hyökkääjä pyrkii pääsemään sisään kohdeympäristöön. Verkossa levittäytymisessä hyökkääjä toimii ympäristön sisällä ja pyrkii lähemmäs päämääräänsä. Hyökkääjän päästyä käsiksi kohteeseensa, se pyrkii suorittamaan toimintoja, joilla se saavuttaa päämääränsä (Pols, 2017).

UKC-mallia on myöhemmin kehitetty siten, että vaiheet muodostavat kolme kierrosmaista rakennetta. Vaiheita on myös muutettu siten, että vaihe 17 ”kohdejärjestelmän manipulointi” on korvattu uudemmassa julkaistussa versiossa vaiheella ”vaikutukset” (engl. impact), jolloin saadaan kuvattua myös sabotaasitoimet. Lisäksi ”aseistautuminen” vaihe on korvattu vaiheella ”resurssien kehittäminen” (engl. resource development). Päivitetty malli on esitetty oheisessa kuvassa (Kuva 3). Malli on kuvattu kolmena kierroksena, joita hyökkääjän toimenpiteet seuraavat hyökkäyksen edetessä. Mallin ensimmäinen kierros ”Sisään” (engl. In) kuvaa hyökkääjän pääsyä järjestelmään sisälle, toinen kierros ”Läpi” (engl. Through) kuvaa hyökkääjän etenemistä kohdeympäristössä ja kolmas kierros ”Ulos” (engl. Out) kuvaa hyökkääjän toimia päämäärässä (Pols, 2022).



Kuva 3 UKC-mallin rakenne (Pols, 2022)

UKC-malli yhdistää MITRE ATT&CK-mallin taktiikoita ja aiemmin esitellyissä hyökkäysketjumalleissa esiteltyjä hyökkäysvaiheita. Lisäksi UKC-mallissa kuvataan toistuvia toimenpiteitä kierrosmaisesti, koska hyökkääjä saattaa toistaa joitakin vaiheita hyökkäyksen edetessä kohti päämäärää.

2.5 Sisäpiiriuhkaan liittyviä hyökkäysmalleja

Reidy (2013) esitteli Black Hat 2013 -tietoturvakonferenssissa mallin sisäpiiriuhkan hyökkäysketjusta. Esityksessään hän arvosteli Lockheed Martinin CKC-mallin toimimattomuutta sisäpiiriuhkien torjumisessa. Reidyn esittelemässä mallissa kuvattiin sisäpiiriuhkalle seuraavat vaiheet:

1. Rekrytointi tai käännekohta (engl. recruitment / tipping point)

2. Etsiminen ja tiedustelu (engl. search / recon)
3. Hankkiminen ja kerääminen (engl. acquisition / collection)
4. Varastaminen ja toiminta (engl. exfiltration / action)

Sisäpiiriuhkaan liittyy Reidyn (2013) mukaan myös vahvasti operaatioturvallisuus, eli sisäpiiriläinen pyrkii peittelemään varsinaista toimintaansa muilta. Sisäpiiriläisten käyttämiä operaatioturvallisuuden keinoja ovat esimerkiksi salauksen käyttäminen, viestinnän peitteleminen ja tiedon varastaminen pienissä erissä. Reidyn esittelemässä mallissa painotetaan sitä, että sisäpiiriuhkan toimijat käyttävät harvoin kyberhyökkäyksissä käytettyjä työkaluja ja tekniikoita. Reidy mainitsee esityksessään, että sisäpiirin hyökkääjät eivät ole käytä teknisesti haastavia menetelmiä, kuten ”hakkerointia”, vaan hyökkääjät hyödyntävät heille myönnettyjä pääsyoikeuksia ja toimivat lähes kuin normaali käyttäjä (Reidy, 2013).

Tutkimusyhtiö G-Research hyödynsi Reidyn (2013) esittelemää mallia omassa tutkimuksessaan, jossa selviteltiin sisäpiiriläisten käyttämiä tekniikoita ja taktiikoita käytännön tapauskuvauksia analysoimalla (Read, Alamir, Dugdale, Stride & Lobo, 2021). Tutkimuksessa käsiteltiin noin 50 sisäpiiriuhkan tapauskuvausta, joiden perusteella luotiin malli hyökkääjien käyttämistä tekniikoista ja taktiikoista. Mallin rakenteessa käytettiin inspiraationa MITRE ATT&CK-viitekehystä. Tutkijat nimesivät mallin ”Insider Attack Matrix” (tässä tutkielmassa lyhennettynä IAM). G-Researchin tutkijoiden mallissa kuvatut taktiikat ovat seuraavat:

- Rekrytointi tai käännekohta (engl. recruitment / tipping point)
- Etsiminen ja tiedustelu (engl. search / reconnaissance)
- Turvatoimien välttely (engl. defense evasion)
- Tiedon kerääminen (engl. data collection)
- Aseistautuminen (engl. weaponise)
- Varastaminen (engl. exfiltrate)
- Vaikutukset (engl. impact)
- Jälkitoimet (engl. aftermath)

G-Researchin tutkijat uskovat, että malli voi auttaa sisäpiiriuhkan havaitsemisessa, torjunnassa ja vastatoimissa ja mainitsevat myös, että malli on varsin keskeneräinen ja vaatii jatkokehitystä. (Read ym., 2021). Osa tutkimuksessa tapauskuvauksista on myös fiktiivisiä, mikä vähentää tutkimuksen luotettavuutta.

3 SISÄPIIRIUHKA

Organisaatiot pyrkivät turvaamaan omaisuutensa ja toimintansa erilaisilta uhkilta. Uhkat voivat olla organisaation ulkopuolella olevia toimijoita, esimerkiksi kyberrikollisryhmiä tai APT-ryhmiä. Osa organisaatioihin kohdistuvista uhkista tulee kuitenkin organisaation sisältä, jolloin puhutaan sisäpiiriuhkasta. Tässä luvussa esitellään sisäpiiriuhkan määritelmiä, käydään läpi sisäpiiriuhkan eri ulottuvuuksia, esitellään sisäpiiriuhkan kategorisointia ja vastakeinoja sisäpiiriuhkan torjumiseksi ja havaitsemiseksi.

3.1 Perusmääritelmät

Sisäpiiriuhkan tutkimuksessa on havaittu haasteelliseksi sisäpiiriuhkan määrittäminen selkeästi (Homoliak ym., 2020). Haasteena on ollut erityisesti rajaus sisäpiiriläisen ja ulkopuolisen toimijan välillä, ja sen rajaaminen, milloin ulkopuolisesta toimijasta tulee sisäpiiriläinen ja toisin päin. Esimerkiksi verkkoon tunkeutuva ulkopuolinen, joka kykenee riittävän tarkasti jäljittelemään sisäpiiriläistä, voidaan Neumannin (2010) mukaan määritellä sisäpiiriläiseksi. Joissakin kaupallisissa tutkimuksissa lasketaan sisäpiiriuhkaksi myös tilanteet, joissa ulkopuolinen taho käyttää sisäpiiriläiseltä varastamiaan tunnuksia (Ponemon Institute, 2022). Sisäpiiriuhkan määrittelyssä oleellisimpia tahoja on Carnegie Mellon yliopiston ohjelmistotekniikan instituutin CERT-yksikkö (tässä tutkielmassa jatkossa ”CERT”) (Homoliak ym., 2020), joka ylläpitää tietokantaa sisäpiiriuhkan tapausaineistoista, jossa on tutkimuksen tekohetkellä yli 3000 tapausta. CERT-yksikön käyttämä sisäpiiriuhkan määritelmä esitellään luvussa 3.1.2.

3.1.1 Sisäpiiriläinen

Yhdysvaltain kyberturvallisuuden ja infrastruktuurin turvallisuuden virasto CISA (tässä tutkielmassa jatkossa ”CISA”) määrittää sisäpiiriläisen henkilönä, jolla on, tai oli, luvallinen pääsyoikeus tai tietoa organisaation resursseista, joihin luetaan muun muassa henkilöstö, tilat, informaatio, laitteisto, tietoverkot ja

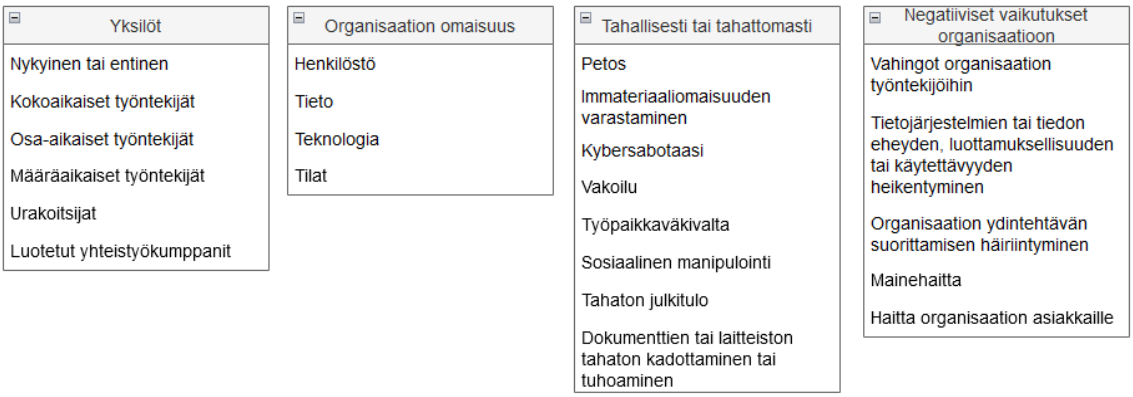
järjestelmät (Cybersecurity & Infrastructure Security Agency CISA, 2022). Probst (2008) määrittää sisäpiiriläisen henkilönä, jolle on oikeutetusti valtuutettu oikeus päästä käsiksi, edustaa tai päättää yhdestä tai useammasta organisaation rakenteeseen kuuluvasta omaisuudesta. Joskus käytetään rajatumpaa määritelmää, esimerkiksi Pfleeger (2010) määrittää sisäpiiriläisen henkilöksi, jolla on oikeutettu pääsy organisaation tietokoneisiin ja verkkoihin. Pfleegerin (2010) määritelmässä korostuu tietotekniikka, kun taas useissa muissa määritelmissä puhutaan myös omaisuudesta, joka on irrallaan tietotekniikasta, esimerkiksi henkilöstö tai tilat.

3.1.2 Sisäpiiriuhka

Sisäpiiriuhkan määritelmänä voidaan käyttää Carnegie Mellon University:n (CMU) ohjelmistotekniikan instituutin CERT-yksikön määritelmää:

> Sisäpiiriuhka – potentiaali sille, että yksilö, jolla on tai on ollut valtuutettu pääsy organisaation kriittisiin resursseihin, käyttää pääsyään joko pahantahtoisesti (engl. maliciously) tai tahattomasti toimiakseen tavalla, joka voisi vaikuttaa organisaatioon negatiivisesti (Costa, 2017).

CERT on tehnyt paljon sisäpiiriuhkaan liittyvää tutkimusta ja se toimii läheisessä yhteistyössä Yhdysvaltain viranomaisten, yksityisten yritysten ja akateemisen yhteisön kanssa. CERT on kerännyt muun muassa tietokannan, jossa on yli kolme tuhatta sisäpiiriuhkaan liittyvää tapauskuvausta ja tehnyt useita hyvin tunnettuja julkaisuja aiheeseen liittyen (Carnegie Mellon University, 2022). Oheinen määritelmä on tiivis ja se voidaan jakaa helpommin ymmärrettäviin osiin. Joitakin määritelmässä esiteltäviä ulottuvuuksia on kuvattu oheisessa kuviossa (Kuva 4). Kuviossa ei ole kuvattuna kaikkia mahdollisia ulottuvuuksia määritelmälle, vaan joitakin yleisiä esimerkkejä. Kuviosta voidaan havaita, että sisäpiiriuhkaan liittyvät yksilöt voivat olla esimerkiksi yrityksen työntekijöitä, yhteistyökumppaneita, tai muita tahoja, jotka saavat jonkin asteisen pääsyoikeuden organisaatioon. Sisäpiiriuhkan kohteena oleva omaisuus voi koostua esimerkiksi aineellisesta tai aineettomasta omaisuudesta tai henkilöstöresursseista. Tekijän tarkoitusperät voivat olla tahattomia tai tahallisia ja niihin voi liittyä suunnitelmallisuutta, mutta teot voivat myös olla spontaaneja. Organisaatio voi kärsiä tekojen seurauksista erilaisin tavoin. Seurauksien kriittisyys organisaatiolle voi vaihdella. Vakavat vaikutukset voivat jopa aiheuttaa organisaation toiminnan pysyvän heikentymisen tai keskeytymisen, kun taas lievemmät vaikutukset voivat olla korjattavissa toimivalla viestinnällä (esimerkiksi lievä mainehaitta).



Kuva 4 Sisäpiiriuhkan määritelmän ulottuvuuksia (Costa, 2017)

Sisäpiiriuhkan piiriin kuuluu monenlaisia toimijoita, uhkan kohteita, tekijän tarkoitusperiä ja erilaisia vaikutuksia. Uhkan monimuotoisuuden takia sen hallitseminenkin vaatii organisaatiolta monipuolisia toimia, eikä sisäpiiriuhkaa voida hallita pelkästään teknologian avulla (Cappelli, Moore & Trzeciak, 2012, s. 14). Sisäpiiriuhkan havaitsemista ja torjuntaa käsitellään tarkemmin luvussa 3.3.

3.2 Sisäpiiriuhkan luokittelu

Sisäpiiriuhkaa voidaan luokitella uhkan eri ominaisuuksien perusteella. Usein käytetään luokittelua sisäpiiriläisen aikeiden perusteella, esimerkiksi pahantahtoisiin ja tahattomiin. Luokittelua on myös tehty muilla perusteilla, kuten profiloimalla tapauksia tai tekijöitä. Homoliak ym. (2020) perehtyivät muun muassa erilaisiin sisäpiiriuhkan taksonomioihin, ja päätyivät luokittelemaan sisäpiiriuhkat pahantahtoisiin ja tahattomiin. Probst (2010) luokittelee sisäpiiriuhkan kahteen kategoriaan: luottamuksen pettäneisiin tekijöihin ja niihin, jotka eivät pettäneet luottamusta. Hayden (1999) luokittelee sisäpiiriuhkan neljään kategoriaan: petturit, kiihkoilijat, selailijat ja hyväntahtoiset. CERT:n määritelmä (Costa, 2017) on koottu siten, että se sisältää sekä pahantahtoiset että tahattomat toimijat. Tässä tutkielmassa erottelu tehdään pahantahtoisiin ja tahattomiin toimijoihin.

3.2.1 Tahaton sisäpiiriuhka

Tahattomalla sisäpiiriuhkalla tarkoitetaan sellaista tilannetta, jossa uhka toteutuu siten, että sisäpiiriläisellä ei ole pahantahtoisuutta tai tarkoitusta aiheuttaa vahinkoa. Tahaton sisäpiiriuhka sisältää sekä tapaukset, joissa sisäpiiriläinen aiheuttaa vahinkoa joko teoillaan tai tekemällä jättämisellään (Insider Threat Team, CERT, 2013). Tekemättä jättämisellä voidaan aiheuttaa vahinkoa esimerkiksi laiminlyömällä prosesseja, kuten vieraiden tunnistaminen organisaation tiloissa tai seuraamalla tuhoamiskäytänteitä huonosti.

CERT:in sisäpiiriuhkan tutkimusryhmä (2013) kuvaa raportissaan neljä tahattoman sisäpiiriuhkan tyyppiä, joihin lähes kaikki heidän analysoimansa tapaukset kuuluvat:

- DISC eli tahaton julkaiseminen (engl. accidental disclosure): arkaluonteinen tieto päätyy julkisesti verkkosivustolle, sitä käsitellään väärin tai se lähetetään väärälle taholle esimerkiksi sähköpostilla
- UIT-HACK eli vahingollinen koodi (engl. malicious code): ulkopuolisen tahon sähköinen sisääntulo sosiaalisen manipuloinnin kautta (kohdistettu kalastelu, luvattomat ulkoiset mediat) ja haitta- tai vakoiluohjelmien suorittaminen
- PHYS eli väärin toteutettu tai vahingossa tehty fyysisten tallenteiden hävittäminen
- PORT eli kadotetut kannettavat ja ohjeislaitteet, kuten ulkoiset mediat, älypuhelimet, kannettavat tietokoneet

Inhimilliset virheet ovat suurin syy tahattomaan sisäpiiriuhkan toteutumiseen. Raportissa tuodaan edellä mainittujen kategorioiden lisäksi esille muita inhimillisiä tekijöitä, päätöksentekoon vaikuttavia asioita, psykososiaalisia ja sosiokulttuurillisia tekijöitä sekä organisaatioon liittyviä tekijöitä (Insider Threat Team, CERT, 2013, s. 19–21).

3.2.2 Pahantahtoinen sisäpiiriuhka

Pahantahtoiseen sisäpiiriuhkaan liittyy sisäpiiriläinen, joka hyödyntää omaa pääsyoikeuttaan aiheuttaen tahallisesti vahinkoja organisaatiolle (Cappelli, Moore & Trzeciak, 2012). Tietoteknisessä ympäristössä toimivat tahalliset sisäpiiriuhkat voidaan luokitella kolmeen kategoriaan (Cappelli ym., 2012):

- IT-sabotaasi (engl. IT sabotage): tapaukset, joissa sisäpiiriläinen hyödyntää tietotekniikkaa tehdäkseen vahinkoa organisaatiolle tai yksilölle
- Petos (engl. fraud): sisäpiiriläinen käyttää IT:tä muokatakseen, lisätäkseen tai poistaakseen organisaation tietoa henkilökohtaisen hyödyn tavoittelemiseksi tai varastaa tietoa, joka johtaa identiteettivarkauteen
- Aineettoman omaisuuden varastaminen (engl. theft of IP): sisäpiiriläinen käyttää IT:tä varastaakseen yritykseltä sen omistamaa yksityisomistuksellista tietoa, tähän kategoriaan kuuluu myös teollisuusvakoilu

CERT:n julkaisemassa (2022, s. 3) ohjeessa sisäpiiriuhkan torjumiseksi mainitaan edellisten lisäksi vielä kolme kategoriaa, joihin voi kuulua pahantahtoiseksi luokiteltavia sisäpiiriuhkia:

- Luvallisen pääsyoikeuden väärinkäyttö (engl. misuse of authorized access)
- Kansalliseen turvallisuuteen liittyvä vakoilu (engl. national security espionage)
- Työpaikkaväkivalta (engl. workplace violence)

Homoliak ym. (2020) esittelevät tutkimuksessaan muitakin tapoja luokitella pahantahtoista sisäpiiriuhkaa, muun muassa ”itsemotivoidut”, ”rekrytoidut” ja ”asetetut” sisäpiiriläiset. Itsemotivoidut sisäpiiriläiset päättävät itse toimia henkilökohtaisista syistä, rekrytoidut sisäpiiriläiset ovat kolmannen osapuolen suostuttelemia tai palkkaamia ja asetetut sisäpiiriläiset on asetettu pahantahtoisen ulkopuolisen organisaation toimesta tiettyyn asemaan, jossa voidaan toteuttaa suunniteltuja päämääriä (Homoliak ym., 2020). CISA:n (2022) mukaan pahantahtoiset uhkat voivat johtua esimerkiksi oman edun tavoittelusta, henkilökohtaisten vääryyksien kokemuksista tai juonittelusta kolmansien osapuolien kanssa.

3.3 Sisäpiiriuhkan havaitseminen ja torjunta

Sisäpiiriuhkan hallitseminen ei onnistu pelkästään teknologian keinoin. Uhkan monitahoisuuden vuoksi sen torjumiseen tarvitaan monenlaisia keinoja, mukaan lukien hallinnollisia toimenpiteitä, teknisiä kontrolleja ja kovennettuja prosesseja. Sisäpiiriuhkan torjunnan tulisi kattaa sekä organisaation fyysinen että sähköinen toimintaympäristö (Cappelli ym., 2012, s. 213). Sisäpiiriuhkaan vaikuttaa yhdistelmä teknisiä, käyttäytymiseen liittyviä sekä organisatorisia haasteita, joita voidaan ratkoa esimerkiksi toimintaperiaatteilla, menettelytavoilla ja teknologioilla (CERT National Insider Threat Centre, 2022).

3.3.1 Käyttäytymiseen liittyvät riski-indikaattorit

Sisäpiiriuhkaan liittyvää riskikäyttäytymistä on kartoitettu tutkijoiden toimesta, ja sitä voidaan havainnoida sekä teknisin keinoin että henkilöiden, esimerkiksi työntekijöiden, toimesta (Greitzer, Kangas, Noonan, Dalton & Hohimer, 2012). Yksilön osalta sisäpiiriuhkan riskiin vaikuttavia tekijöitä ovat muun muassa sisäpiiriläisen persoonallisuuteen liittyvät piirteet, tunnetilat, taloudellinen tilanne sekä organisatoriset ja kulttuurilliset vaikuttimet (Dupuis & Khadeer, 2016). Edellä mainitut tekijät voivat korottaa riskiä, että sisäpiiriläinen motivoituu tekemään vahinkoa organisaatiolle. Yksilön käyttäytymisessä voidaan havaita muutoksia, jotka voivat viestiä kohonneesta sisäpiiriuhkan riskistä. Henkilön käyttäytymiseen liittyviä riski-indikaattoreita ovat esimerkiksi (Greitzer ym., 2012):

- närkästyminen
- palautteen torjuminen
- vihaisuus
- vetäytyminen
- piittaamattomuus auktoriteetista
- heikko suorituskyky
- kohonnut stressitaso
- hyökkäävä käyttäytyminen
- henkilökohtaiset vaikeudet

- itsekeskeisyys
- luottamattomuus
- toistuvat poissaolot

Pelkästään henkilön käyttäytymisen perusteella on vaikeaa lähteä tekemään voimakkaita toimenpiteitä, kuten työsuhteen päättämistä tai pääsyoikeuksien rajaamista. Väärin mitoitettuna kurinpitotoimenpiteet voivat aiheuttaa suurempaa vahinkoa kuin riski, jota niillä torjutaan. Päätöksenteon tueksi tarvitaan usein tietoa yksilön käyttäytymisestä teknisessä ympäristössä. Tähän voidaan käyttää teknisesti kerättyä dataa (esimerkiksi lokitietoja). Sisäpiiriuhkan torjunnassa päätöksentekijöillä on oltava ymmärrystä sekä kyberturvallisuudesta, henkilöstöasioista että hallinnollisista asioista (Greitzer ym., 2012). Sisäpiiriuhkan torjumisessa tarvitaan siis sekä teknisiä että psykososiaalisia havaintoja ja kontekstin ymmärrystä.

Tekninen havaintokyky on tärkeässä roolissa sisäpiiriuhkan havaitsemisessa, sillä suuri osa nykypäivän organisaatioiden toiminnasta tapahtuu sähköisessä ympäristössä. Teknistä voidaan luoda seuraamalla käyttäjien käyttäytymistä teknisessä ympäristössä ja valvomalla potentiaalisia riski-indikaattoreita. Teknisesti havaittavia riski-indikaattoreita ovat esimerkiksi (Kont, Pihelgas, Wojtkowiak, Osula & Trinberg, 2015, s. 33-36):

- viestintä kilpailijoiden kanssa
- epäilyttävien tietoliikenneprotokollien käyttö
- kiellettyjen sovellusten asentaminen tai käyttö
- haittaohjelmahavainnot
- epätavalliset kirjautumisajat ja -tavat

Riski-indikaattorien seuraaminen vaatii yksilön käyttäytymisen seuraamista jollakin tasolla. Sisäpiiriuhkaa havainnoidessa onkin tärkeää huomioida lakien asettamat rajoitteet ja kunnioitettava sisäpiiriläisen yksityisyyttä ja tietosuojaa. Työntekijöiden yksityisyyden ja tietosuojan huomioiminen osana organisaation kulttuuria luo työntekijöiden ja organisaation väille luottamusta ja osaltaan voi myös vähentää tahattomien tietovuotojen määrää (CERT National Insider Threat Centre, 2022).

3.3.2 Tekniset kontrollit

Perinteiset tietotekniset kontrollit luovat toimivan pohjan, jolle voidaan rakentaa myös sisäpiiriuhkan hallintaan tarvittavaa kyvykkyyttä. Sisäpiiriuhka kykenee kiertämään joitakin teknisiä kontrolleja, koska kyseiset uhkatoimijat käyttävät usein niille annettuja työtehtäviin tarvittavia pääsyjä, jolloin monet perinteiset kontrollit kuten palomuurisäännöt ja käyttöoikeuksien rajaaminen eivät välttämättä ole tehokkaita sisäpiiriuhkan hallinnassa. Sisäpiiriuhkan hallintaan erityisesti soveltuvia teknisiä kontrolleja tai työkaluja ovat muun muassa (Trzeciak & Costa, 2018):

- käyttäjän aktiviteettien monitorointi (engl. user activity monitoring, UAM):

- tietovuodon ehkäiseminen (engl. data loss prevention, DLP)
- tietoturvatiedon ja -tapahtumien hallintajärjestelmä (engl. security information and event management, SIEM)
- analytiikka, mm. poikkeamien havaitsemiskyky, riskien pisteytys, ennakoiva analytiikka
- digitaalinen forensiikka, mm. tekojen tutkiminen jälkikäteen järjestelmiin jääneistä tapahtumajäljistä

Sisäpiiriuhkan hallitsemiseksi voidaan koota yhteen yksilöiden tietotekniseen käyttäytymiseen liittyviä riski-indikaattoreita. Indikaattorit voidaan liittää ympäristössä toimiviin teknisiin kontrolleihin ja sitä kautta muodostaa teknistä havainnointikykyä sisäpiiriuhkaa vastaan. Kontrollien toimivuuden todentaminen voidaan tehdä esimerkiksi havainnoimalla aukkoja prosesseissa tai suorittamalla simuloituja hyökkäystestejä ympäristöön. Uhkan hallinnassa on tärkeää, että kontrollien valinnassa huomioidaan organisaation tehtävän kannalta kriittisimmän omaisuuden turvaaminen. (Trzeciak & Costa, 2018)

3.3.3 Henkilöstöturvallisuus ja hallinnolliset kontrollit

Teknisten kontrollien lisäksi sisäpiirin uhkan hallitsemiseksi tarvitaan myös muita kontrollikeinoja. Sisäpiiriuhkan hallitseminen alkaa heti sisäpiiriläisen työsuhteen alkuvaiheessa ja päättyy vasta kun sisäpiiriläisen kaikki pääsyoikeudet organisaation omaisuuteen on poistettu. Suomessa sisäpiiriuhkan vähentämiseksi työsuhteen alussa on melko laajasti käytössä Suojelupoliisin turvallisuusselvitykset (Suojelupoliisi, 2019, s. 24). Selvitysten avulla voidaan huomioida potentiaalisen sisäpiiriläisen taustat ennen rekrytointipäätöstä. Sisäpiiriuhkan hallintaan voidaan käyttää hallinnollisia kontrolleja. Näitä ovat esimerkiksi toimintalinjaukset, menettelytavat, turvallisen käytön ohjeet ynnä muut turvallisuuteen liittyvät käytännöt organisaatiossa. Hallinnollisten kontrollien avulla voidaan luoda malli normaalista toiminnasta, jolloin poikkeamien havainnoinnista tulee helpompaa (Trzeciak & Costa, 2018). Esimerkiksi turvallisen käytön ohjeita voidaan kirjoittaa siten, että järjestelmien käyttö ja siihen liittyvät prosessit tehdään aina tietyllä tavalla ja normaalista poikkeaminen huomataan. Toisena esimerkkinä kriittisissä prosesseissa voidaan vaatia, että yksi henkilö ei pääse suorittamaan toimenpiteitä, vaan tarvitaan aina toinenkin henkilö, joka mahdollistaa tekemisen esimerkiksi antamalla käyttöoikeudet tai fyysisen pääsyn tilaan.

4 TUTKIMUSMENETELMÄT JA AINEISTON ESITTELY

Tämän tutkielman tarkoituksena on tuottaa malli, joka soveltuu sisäpiiriuhkatoimijoiden hyökkäysten mallintamiseen. Tutkimusmenetelmäksi valikoitui kehittämistutkimus (design science, DS) sekä laadullinen sisällönanalyysi. Kehittämistutkimus valittiin menetelmäksi, koska hyökkäysmalleissa on havaittu olevan puutteita sisäpiiriuhkaan liittyen. ja menetelmä soveltuu uusien ratkaisujen kehittämiseen olemassa oleviin ongelmiin. Kehittämistutkimuksen tueksi analysoitiin sisäpiiriuhkaan liittyviä tapauskuvauksia laadullisen sisällönanalyysin keinoin. Sisällönanalyysi tehtiin teoriaohjattuna, eli siinä hyödynnettiin olemassa olevaa teoriaa ja tutkimustietoa.

4.1 Aineistonkeruumenetelmät ja aineiston esittely

Tutkielman aineistonkeruuta tehtiin kolmessa vaiheessa. Ensimmäisessä vaiheessa etsittiin tietoa sisäpiiriuhkaan liittyen, toisessa vaiheessa kyberhyökkäysmalleihin liittyen ja lopuksi kerättiin sisäpiiriuhkan tapauskuvauksia. Ensimmäisessä vaiheessa hakusanoina käytettiin esim. ”insider threat”, ”model”, ”categorization”, ”detection”, ”monitoring” ja ”information security” sekä näiden hakusanojen yhdistelmiä. Toisessa vaiheessa hakusanoina käytettiin esim. ”cyber security”, ”kill chain”, ”attack model” ja näiden yhdistelmiä.

Ensimmäisessä ja toisessa vaiheessa haut kohdistettiin tieteellisten julkaisujen hakukoneisiin, kuten Google Scholar, ACM Digital Library, Elsevier ScienceDirect ja IEEE Xplore. Tutkittavia artikkeleita valikoitiin otsikoiden ja viitteiden määrän perusteella. Hakutuloksia ei käyty systemaattisesti läpi loppuun asti, vaan tuloksista poimittiin ensimmäisten 20–30 artikkelin joukosta tutkimuksen kannalta relevantilta vaikuttavia artikkeleita. Artikkeleita tutkittiin läpi ja niiden lähdeluetteloiden kautta voitiin myös löytää lisää aiheeseen liittyvää aineistoa. Artikkeleiden lisäksi käytettiin joitakin akateemisia ja viranomaisjulkaisuja

kuten Carnegie Mellon -yliopiston CERT-yksikön julkaisuja ja Yhdysvaltain Cybersecurity and Infrastructure Agencyn materiaalia.

Kolmannessa vaiheessa tutkielmaa varten kerättiin julkisista lähteistä tapauskuvauksia sisäpiiriuhkatoimijoiden suorittamista hyökkäyksistä. Tapauksia etsittiin ensin kirjallisuudesta ja Internetistä. Internet-hauissa hyödynnettiin aluksi hakukoneita (esim. Google, DuckDuckGo) ja uutissivustoja (mm. BleepingComputer). Aineistoon ei hyväksytty uutissivustoilla esitettyjä tapauskuvauksia, vaan niiden perusteella etsittiin joko viranomaisjulkaisua tai tutkimuslähteitä aiheesta. Hakukoneissa tapauksien löytämiseksi onnistuneesti käytettiin termejä kuten ”insider threat”, ”case study” ja ”espionage” sekä näiden yhdistelmiä.

Merkittävä määrä aineistosta löytyi Yhdysvaltain puolustusministeriön alaisen Center for Development of Security Excellence -keskuksen (CDSE) julkaisuista. CDSE:n julkaisemia tapauksia päätyi tutkielman aineistoon 65 kappaletta. Tärkeäksi kirjallisuuslähteeksi aineistojen kannalta muodostui Carnegie Mellon -yliopiston CERT-yksikön julkaisema ”The CERT Guide to Insider Threats”, josta tutkimukseen otettiin 38 tapauskuvausta. Lisäksi Yhdysvaltain oikeusministeriön (Department of Justice) sivustoilta löytyi eri osavaltioiden oikeuden julkaisemina tiedotteina 23 tapausta. Tapauksien löytämiseen käytettiin oikeusministeriön sivustolla olevaa hakua hyödyksi (hakusanoina mm. ”espionage”, ”insider”). Loput tapaukset löydettiin mm. FBI:n ja Yhdysvaltain merisotaopiston (Naval War College) sivustojen kautta.

Aineiston keruun aikana tarkistettiin kukin tapauskuvaus alustavasti, että siinä on riittävästi tietoa analyysia varten. Useimmat löydetyt tapaukset oli kuvailtu riittävällä tarkkuudella, että niistä voitiin tunnistaa tekijöiden taktiikoita. Tapauskuvauksista tarkistettiin myös päällekkäisyyttä vertailemalla sopivia yksityiskohtia. Samaa tapausta käsittelevät kuvaukset käsiteltiin analyysissa yhtenä tapauksena. Tapauksia käytiin myös pinnallisesti läpi siten, että saatiin varmasti aineistoon mukaan yleisimmät sisäpiiriuhkan kategoriat (CERT National Insider Threat Centre, 2022):

- IT-sabotaasi
- Aineettoman omaisuuden varastaminen
- Petos
- Luvallisen pääsyoikeuden väärinkäyttö
- Kansalliseen turvallisuuteen liittyvä vakoilu
- Työpaikkaväkivalta

Yhteensä analysoitavaksi kelpuutettiin alustavasti 128 tapausta. Tapauksia voidaan löytää edellä kuvatuilla menetelmillä enemmänkin, mutta tutkimuksen tavoitteiden ja resurssien kannalta määrä arvioitiin riittäväksi. Yksittäisten tapauksien lisääminen analyysiin ei todennäköisesti enää tuottaisi uusia havaintoja, kun huomioidaan tapausten kokonaismäärä.

4.2 Laadullinen sisällönanalyysi

Tutkielmassa toteutettiin laadullinen sisällönanalyysi kerätylle tapausaineistolle. Laadullisessa sisällönanalyysissa keskitytään siihen, mitä asioita ja teemoja aineistossa esiintyy, ja se perustuu tutkijan tekemään koodaukseen, jossa tunnistetaan ja nimetään aineistossa esiintyviä elementtejä (Vuori, ei pvm). Aineistossa esiintyvien elementtien tunnistamista ja nimeämistä kutsutaan ”koodaukseksi”. Koodaus voidaan tehdä käyttää aiempaa teoriaa, jolloin teoriassa esiintyvistä käsitteistä johdetaan koodeja, tai tutkija voi itse keksiä koodeja, yrittäen käyttää vähemmän olemassa olevaa teoriaa hyödykseen (Illinois Library, 2020). Teorian hyödyntämisessä tulisi löytää tutkimuksen kannalta sopiva tasapaino. Uusien löydösten tekeminen voi olla vaikeaa, mikäli teoriaan takerrutaan liikaa, ja aiemman teorian täysi välttteleminen voi johtaa siihen, että tietoaineistoa ei saada yhdistettyä tutkimuskysymyksiin (Ryan & Bernard, 2003).

Tässä tutkielmassa sisällönanalyysin tuloksia käytettiin uuden mallin kehittämiseen ja aiempien hyökkäysmallien sopivuuden arviointiin sisäpiiriuhkatapausten hyökkäysvaiheiden kuvaamisessa. Tutkielmassa käytettiin teoriaohjattua sisällönanalyysia, jossa aineiston koodaamiseen käytetyt käsitteet johdettiin teoriasta. Teoriapohjana käytettiin hyökkäysmalleja, joita on kuvattu tarkemmin luvussa 2. Mikäli analyysin aikana havaittiin, että joitakin hyökkääjän toimia ei voida koodata, kirjattiin havainnot ylös ja pyrittiin keksimään puutteista yhteisiä tekijöitä, joiden perusteella voitiin keksiä uusia koodaukseen käytettäviä käsitteitä. Tutkimuseettisistä syistä suorat viittaukset tapausaineistoihin jätettiin pois tutkielman kirjoitetusta osuudesta, koska tapauskuvaukset sisältävät rikoksiin tuomittujen yksityishenkilöiden nimiä. Alkuperäiset tapauskuvaukset on löydettävissä soveltamalla luvussa 4.1 kuvattuja aineistonkeruumenetelmiä, lisäksi tutkielman työmuistiinpanoina käytetyt tapauskuvausten tiivistelmät löytyvät liitteestä 1.

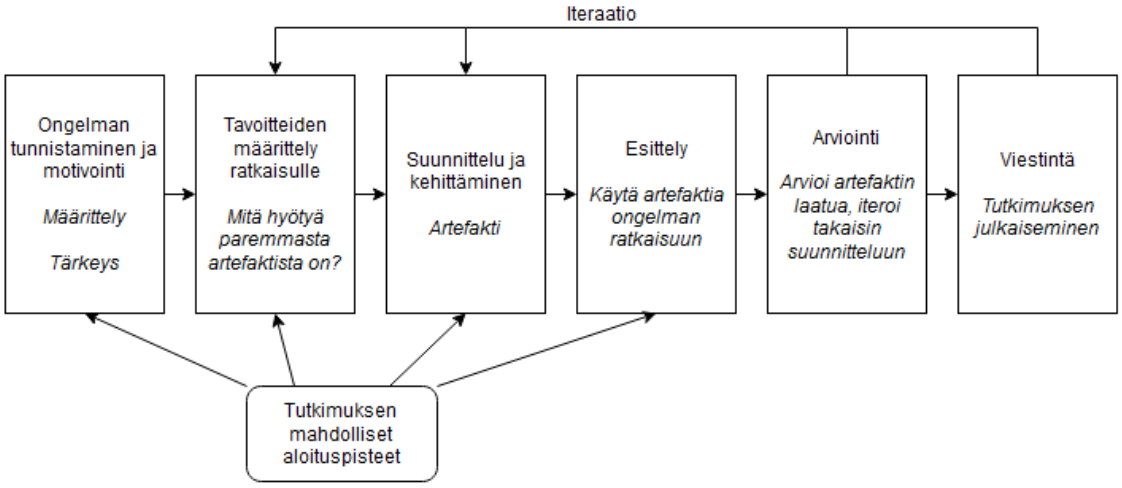
4.3 Kehittämistutkimus

Kehittämistutkimuksen tavoitteena on tuottaa hyödyllinen ratkaisu (artefakti) johonkin määriteltyyn ongelmaan. Kehittämistutkimuksessa seurataan prosessia, jonka aikana määritellään ongelmia, suunnitellaan artefakteja, arvioidaan artefaktien toimintaa sekä tarvittaessa iteratiivisesti kehitetään niitä ja viestitään tuloksista relevanteille tahoille (Hevner, March, Park & Ram, 2004). Kehittämistutkimuksen artefaktilla voidaan tarkoittaa esimerkiksi menetelmiä, malleja, ohjelmistoja tai muita tutkimuksen tuottamia konstruktioita.

Tutkimuksessa käytettiin tietojärjestelmätieteen alalle suunniteltua kehittämistutkimusmetodologiaa (engl. Design science research methodology, DSRM). Menetelmä kehitettiin alunperun, koska alalla ei ollut selkeää hyvin tunnettua viitekehystä, jonka pohjalta kehittämistutkimusta voitaisiin tehdä. DSRM-menetelmässä on kuusi vaihetta (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007):

1. Ongelman tunnistaminen ja motivointi
2. Tavoitteiden määrittely ratkaisulle
3. Suunnittelu ja kehittäminen
4. Esittely
5. Arviointi
6. Viestintä

Prosessiin liittyy myös läheisesti iterointi, jonka avulla voidaan palata aiempiin vaiheisiin kehittämään parempia ratkaisuja ongelmaan. Menetelmässä tutkimuksen aloituskohtina voidaan käyttää prosessin vaiheita 1,2,3 ja 4. Prosessi on kuvattu oheisessa kuviossa (Kuva 5). Tarkemmin tässä tutkielmassa käytettävä menetelmä on kuvattu myös erillisessä kuviossa (Kuva 6). Kyseisessä kuviossa on kuvattu eri vaiheissa tehtävät tärkeimmät toimenpiteet tai tuotokset.



Kuva 5 DSRM-menetelmä (Peffers ym., 2007)

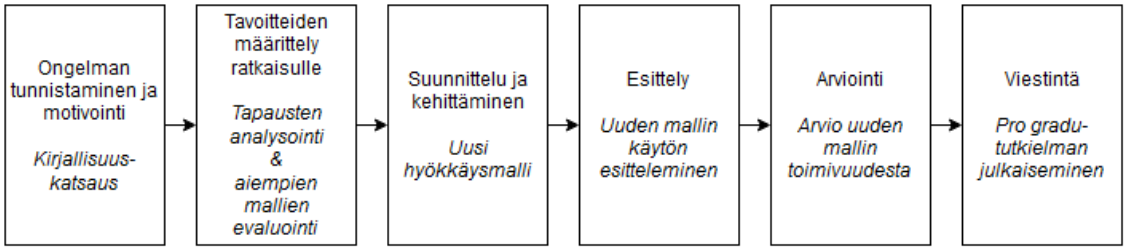
DSRM-menetelmän ensimmäisessä vaiheessa määritellään tutkimusongelma ja perustellaan, miksi ongelma on tärkeää ratkaista. Menetelmässä ongelma on syytä pilkkoa osiin, että voidaan hahmottaa ongelman ja tarvittavan ratkaisun ulottuvuudet. Hyvillä perusteluilla tutkija ja tutkimuksen yleisö ovat motivoituneita kehittämään ratkaisua ja hyväksymään tulokset. Ensimmäisessä vaiheessa vaaditaan tietoa ratkaistavan ongelman tilasta sekä ongelmanratkaisun tärkeydestä. (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

Tässä tutkielmassa ongelman tunnistaminen ja motivointi perustuu tutkielman johdantoon ja kirjallisuuskatsaukseen sekä osittain myös laadullisen sisällönanalyysin tuloksiin. Kirjallisuuskatsauksessa käsitellään olemassa olevia kyberturvallisuuden ja sisäpiiriuhkan mallintamiseen tehtyjä hyökkäysmalleja. Kirjallisuuskatsauksessa esitellään sisäpiiriuhkan perusmääritelmät, luokittelutavat sekä havaitsemiseen ja torjuntaan käytettävät menetelmät. Näiden avulla saadaan selkeys ongelman tilasta sekä ongelman tärkeydestä ja ratkaisun mahdollisista hyödyistä.

Menetelmän toisessa vaiheessa määritellään tavoitteet ratkaisulle, joka kehitetään prosessissa. Tavoitteiden tulee perustua ongelman määrittelyyn, ja ne

voivat olla joko kvantitatiivisia tai kvalitatiivisia. Toisessa vaiheessa vaaditaan tietoa ongelmien ja olemassa olevien ratkaisujen tilasta, sekä niiden tehokkuudesta. (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007)

Tässä tutkielmassa menetelmän toisessa vaiheessa hyödynnetään tutkimuksessa tehtävän laadullisen sisällönanalyysin tuloksia. Analyysin perusteella saadaan tietoa siitä, kuinka hyvin olemassa olevat mallit soveltuvat todellisen maailman sisäpiiriuhkatapausten mallintamiseen. Tutkielmassa luotavan mallin tulee ylittää olemassa olevien mallien kyvykkyys, eli uuden mallin tulee kyetä kuvaamaan sisäpiiriuhkan hyökkäysvaiheita laajemmin kuin aiemmat mallit.



Kuva 6 Tutkielman tutkimusmenetelmä

Menetelmän kolmannessa vaiheessa suunnitellaan artefakti ongelman ratkaisemiseksi. Artefaktin suunnittelussa määritellään toiminnallisuus ja arkkitehtuuri, sekä luodaan se. Artefaktin luomiseksi vaaditaan tietoa ja ymmärrystä ongelmaan ja sen ratkaisuun liittyvästä teoriasta (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

Tässä tutkielmassa menetelmän kolmannessa vaiheessa hyödynnetään laadullisen sisällönanalyysin tuloksia sekä sisällönanalyysissa käsiteltyjä tapauskuvauksia. Analyysin ja tapauskuvausten perusteella kehitellään hyökkäysmalli, joka soveltuu sisäpiiriuhkan hyökkäystapausten vaiheiden mallintamiseen. Sisällönanalyysin tuloksien lisäksi hyödynnetään alan kirjallisuudesta löytyvää teoriapohjaa, jota on esitelty tutkimuksen kirjallisuuskatsauksessa.

Menetelmän neljännessä vaiheessa esitellään luodun artefaktin käyttöä määritellyn ongelman ratkaisemiseksi. Tämä voidaan tehdä esimerkiksi kokeellisesti, simuloimalla, tapaustutkimuksen keinoin tai muulla sopivalla tavalla. Esittelyä varten tarvitaan riittävä osaaminen artefaktin käytöstä ongelman ratkaisemiseksi.

Menetelmän viidennessä vaiheessa arvioidaan kehitetyn ratkaisun toimivuus. Tässä vaiheessa verrataan ratkaisulle määritettyjä tavoitteita esittelyssä havaittuja tuloksia vasten. Arvioinnissa tarvitaan ymmärrystä tarpeellisista mitattavista ominaisuuksista ja analyysitekniikoista. Ongelman ja artefaktin ominaisuudet määrittävät arvioinnin muodon. Arviointi voi sisältää vertailua toisessa vaiheessa tehtyihin tavoitteisiin, kvantitatiivisia mittaustuloksia, kyselytuloksia tai järjestelmien suorituskykytietoa. Käytännössä mitkä tahansa sopivat empiiriset tai loogiset todisteet voivat soveltua tapauskohtaisesti. Tämän vaiheen jälkeen voidaan arvioida, onko tarpeellista kehittää artefaktia lisää, mikäli

tutkimuksen luonne mahdollistaa iteroinnin. (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007)

Tässä tutkielmassa artefaktin toiminta esitellään kuvaamalla mallin vaiheiden yhdistäminen sisäpiiriuhkan tapauskuvauksiin. Esittelyn tuloksia verrataan muiden mallien toimivuuteen ko. tapauksen vaiheiden mallintamisessa. Vertailun pohjalta voidaan arvioida täyttääkö luotu malli sille asetetut tavoitteet.

Lopuksi menetelmän kuudennessa vaiheessa viestitään ongelma ja sen tärkeys sekä artefaktin käyttö, suunnitteluperiaatteet sekä hyödyllisyys relevantille yleisölle, esimerkiksi alan ammattilaisille tai tutkijoille. Tässä tutkimuksessa viestintä sisältää tämän kirjoitetun tutkielman liitteineen. Tulosten julkaisemisen kannalta erityisesti tutkielman yhteenveto sisältää tutkielman aikana tehdyt keskeisimmät havainnot ja mahdolliset jatkotutkimuskohteet. Kehittämistutkimuksen vaiheiden tulokset on kuvattu tarkemmin tutkielman luvussa 5.

4.4 Tutkimuksen luotettavuus

Tutkimuksen aineisto on koottu luotettavista lähteistä, pääosin tieteellisistä, vertaisarvioiduista artikkeleista ja viranomaisjulkaisuista. Tutkimuksessa pyritään avaamaan mahdollisimman selkeästi käytetyt menetelmät, johtopäätökset ja aineistot tutkimuseettiset vaatimukset ja rajaukset huomioiden. Aineiston laadullisessa analyysissä on hyödynnetty olemassa olevaa teoriaa ja tutkimusaineiston tiivistelmät ja käytetty koodaus on avattu tutkimuksessa tarkasti, että saadaan riittävä läpinäkyvyys tutkimuksessa tehtäviin päätelmiin. Tutkimuksen menetelmät, havainnot ja perustelut sekä tutkimuksen tulokset pyritään esittämään mahdollisimman selkeästi julkaisualustan rajaukset huomioiden.

5 ANALYYSI JA TULOKSET

Tässä luvussa käydään läpi kehittämistutkimuksen eri vaiheissa tehdyt toimenpiteitä ja niistä syntyneitä tuloksia. Tutkimusmenetelmät on kuvattu luvussa 4. Tässä luvussa käydään läpi tapausaineistojen analyysin tulokset, olemassa olevien hyökkäysmallien arviointi, uuden hyökkäysmallin kehittäminen, esittely ja evaluointi. Luvussa käydään samalla myös läpi, miten eri tutkimusvaiheet vastaavat tutkimuskysymyksiin.

5.1 Tapausaineistojen analyysi

Tässä tutkielmassa käsiteltäviin tapausaineistoihin koodattiin teoriasta johdettuja hyökkäysvaiheita. Teoriapohjana analyysille käytettiin olemassa olevia hyökkäysmallit, joita on kuvattu tarkemmin luvussa 2. Analyysin aikana voitiin lisätä uusia koodaukseen käytettäviä käsitteitä, mikäli havaittiin, että koodauksessa on selkeitä puutteita. Koodauksessa käytetyt lopulliset hyökkäysvaiheet on kuvattu tutkielman liitteessä 2. Hyökkäysvaiheet numeroitiin analyysia varten tiedon käsittelyn helpottamiseksi.

Liitteessä 2 kuvatut sisällönanalyysin käsitteet, tai koodit, on johdettu aiemmista kyberhyökkäysmalleista, joilla voidaan mallintaa kyberhyökkäyksiä. Hyökkäysvaiheiden kokoaminen teoriasta vastaa yhdessä tutkimuksen kirjallisuuskatsauksen kanssa apututkimuskysymykseen:

> Millaisia vaiheita kyberhyökkäysmalleissa on käytetty?

Liitteen taulukkoon tehty koonti sisältää kaikki vaiheet kirjallisuuskatsauksessa käsitellyistä malleista, jotka tunnistettiin selvästi erillisiksi hyökkäysvaiheiksi. Joitakin vaiheita yhdisteltiin niiden samankaltaisuuden takia. Vaiheiden koonti aloitettiin ottamalla mukaan kaikki Unified Kill Chain -mallin (UKC) hyökkäysvaiheet. UKC-malli on kuvattu tarkemmin tämän tutkielman luvussa 2.4. Liitteen 2 numerot 1–18 vastaavat mallin sisältämiä hyökkäysvaiheita. UKC-malli valittiin pohjaksi sen takia, että malliin on koottu hyökkäysvaiheita muista luvussa 2

esitellyistä hyökkäysketjumalleista (Lockheed Martin Cyber Kill Chain ja Bryant Kill Chain). UKC-mallin vaiheiden tueksi käsitteitä poimittiin myös Insider Attack Matrix -mallista (Liite 2 numerot 19–20) sekä MITRE ATT&CK-viitekehyksestä (Liite 2 numerot 2 ja 21). Analyysissa yhdisteltiin ATT&CK-viitekehyksen taktiikka ”resurssien kehittäminen” ja muissa malleissa käytetty ”aseistaminen” yhdeksi vaiheeksi (vaihe 2) niiden samankaltaisuuden vuoksi. Näin on tehty myös UKC-mallin päivitetyssä versiossa (Pols, 2022).

Aineistoon tutustumisen aikana havaittiin, että tapauksissa toistuu aiemmin tunnistamaton vaihe ”Tiedon toimittaminen”, joka lisättiin koodeihin analyysiin perustuen (Liite 2 numero 22). Tiedon toimittaminen on usein sisällytetty aiemmissa malleissa tiedon varastamisen alle. Tapauskuvauksia analysoitaessa havaittiin, että tiedon toimittaminen on selkeästi erillinen vaihe, jota ennen tieto on varastettu organisaation ympäristöstä, mutta sitä ei ole vielä toimitettu kolmansien osapuolien käsiin. Havaintoa tukee se, että aineistossa oli tapauksia, joissa tekijä oli jo varastanut tiedon organisaatiosta, mutta jäi kiinni ollessaan matkalla toimittamaan tietoa ulkopuolisille (esim. tapaus 69). Taktiikat, jotka voidaan katsoa vastaavan hyökkäysvaiheita (Pols, 2017, ss. 11-12), voidaan määritellä syyksi sille, että hyökkääjä tekee joitakin toimenpiteitä (MITREb, 2022). Useissa tapauksissa sisäpiiriläishyökkääjä pyrkii ensin varastamaan tiedon, jonka jälkeen hyökkääjä pyrkii toimittamaan tiedon eteenpäin kolmannelle osapuolelle. Näin ollen ”tiedon toimittaminen” voidaan tulkita omaksi, erilliseksi vaiheekseen.

Hyökkääjien toimenpiteitä tulkittiin tapauskuvauksista ja yhdistettiin hyökkäysvaiheisiin. Tapauskohtainen erittely tapauksista ja niihin liitetyistä koodeista löytyy taulukkomuodossa tämän tutkielman liitteessä 1. Analyysin aikana kirjoitettiin kustakin tapauksesta myös lyhyt tiivistelmä, joista ilmenee tapauksen sisältö. Tiivistelmät löytyvät myös tutkielman liitteessä 1. Tiivistelmässä keskityttiin kuvaamaan hyökkääjän suorittamia toimenpiteitä ja jätettiin pois yksityiskohdat, joilla on vähemmän merkitystä tutkimuskysymysten kannalta. Tällaisia yksityiskohtia olivat esimerkiksi valtioiden, organisaatioiden ja tekijöiden nimet, sijainnit sekä tekijöille annetut tuomiot.

Analyysin aikana havaittiin, että koodaus soveltuu heikosti osaan tapauksista. Hankalasti koodattaviin tapauksiin lukeutuivat esimerkiksi väkivaltarikokset, terrorismi ja salakuljetus sekä tapaukset, joissa tekijän motiivi oli epäselvä. Näiden havaintojen, ja päätutkimuskysymyksen takia rajattiin aineistosta pois sellaiset tapaukset, joissa hyökkäys ei sisällä tieto- tai kyberturvallisuuteen liittyviä elementtejä ja sellaiset tapaukset, joissa tekijä vaikutti toimivan tahattomasti. Tahattomuus esiintyi aineistossa esimerkiksi siten, että organisaatio ei pyrkinyt rankaisemaan tekijää millään tavalla teon jälkeen, eikä tekijällä vaikuttanut olevan selkeää motiivia aiheuttaa vahinkoa. Rajausten jälkeen tapauksia jätettiin analyysin ulkopuolelle yhteensä 24 kappaletta, eli lopulliseen analyysiin tapauksia jäi 104 kappaletta.

Analyysin lopuksi laskettiin yhteen, kuinka monta kertaa kutakin koodia käytettiin analyysin aikana. Yhteenlasketut koodien käyttökerrat on listattu tutkielman liitteessä 2 sarakkeessa ”Käyttökerrat analyysissä”. Analysoimalla

tapausaineistoaineisto ja laskemalla eri hyökkäysvaiheiden määrät, voitiin vastata apututkimuskysymykseen:

> Millä tavalla sisäpiiriuhkan hyökkäyksiä on tapahtunut?

Taulukon perusteella voidaan todeta, että kaikkia koodeja ei käytetty analyysissä. Analyysin perusteella aineistossa esiintyvät hyökkäysvaiheet kuvaavat vastauksen edellä mainittuun apututkimuskysymykseen. Huomattiin myös, että jotkin vaiheet olivat paljon yleisempiä kuin toiset. Erityisesti teknisemmät hyökkäyksen aikana tehtävät toimenpiteet kuten käyttöoikeuksien korottaminen, jalansijan laajentaminen sekä haittaohjelmien käyttöön liittyvät vaiheet olivat harvinaisia, mutta niitäkin esiintyi.

5.2 Aiempien mallien arviointi

Tutkimuksessa arvioitiin aiempien mallien soveltuvuus sisäpiiriuhkan hyökkäysvaiheiden mallintamiseen. Malleja arvioimalla voidaan määrittää vaatimukset kehittämistutkimuksessa luotavalle mallille. Arvioitavat mallit on kuvattu tarkemmin luvussa 2. Mallien sopivuutta arvioitiin vertaamalla mallien sisältämiä hyökkäysvaiheita sisällönanalyysissä havaittuihin käsitteisiin. Vertailun avulla voidaan arvioida, kuinka kattavasti aiemmat mallit kuvaavat hyökkääjän suorittamia toimenpiteitä sisäpiiriuhkan tapauksissa. Mallien arviointi on kuvattu oheisessa taulukossa (Taulukko 1). Taulukossa kukin malli ja analyysi on omassa sarakkeessaan. Taulukossa on merkitty ”X”, mikäli rivillä oleva vaihe esiintyy sekä sarakkeessa olevassa mallista että analyysissä havaituissa hyökkäysvaiheissa. Mikäli vaihe esiintyy vain mallissa, mutta ei analyysissä, on merkintä ”-”. Jos vaihe löytyy analyysissä, mutta puuttuu mallista, on merkitty ”*”. Tyhjällä solulla on merkitty vaihetta, joka ei esiinny analyysissä eikä mallissa.

Arviointiin otettiin mukaan kaikki luvussa 2 esitellyt hyökkäysmallit, pois lukien Reidy (2013), jonka mallin kaikki hyökkäysvaiheet ovat sisällytettynä G-Researchin kehittämässä Insider Risk Matrix-mallissa (IAM). Vertaamalla kunkin mallin vaiheita sisällönanalyysissa havaittuihin hyökkäysvaiheisiin, voidaan todeta, että yksikään malli ei sisällä kaikkia vaiheita. Sisällönanalyysissä käytettiin yhteensä 17 eri koodia, jotka vastaavat mallien hyökkäysvaiheita. Puuttuvien vaiheiden määrä kussakin arvioitavassa mallissa:

- CKC: 11 puuttuvaa vaihetta
- BKC: 11 puuttuvaa vaihetta
- UKC: 3 puuttuvaa vaihetta
- ATT&CK: 6 puuttuvaa vaihetta
- IAM: 8 puuttuvaa vaihetta

CKC- ja BKC-mallissa on merkittäviä puutteita. UKC-malli kehitettiin mm. paikkaamaan CKC-mallin ja sen johdannaisten puutteita (Pols, 2017), mutta

analyysin perusteella siinäkin on puutteita (rekrytointi tai käännekohta, jälkiseuraukset, tiedon toimittaminen). UKC-malli sisältää tiedon toimittamisen osana tiedon varastamista, mutta ei huomioi sitä erillisenä vaiheena. ATT&CK-viitekehyksessä on vastaavat puutteet kuin UKC-mallissa, ja lisäksi siitä puuttuu vaiheet ”toimittaminen”, ”sosiaalinen manipulointi” ja ”hyväksikäyttö”. ATT&CK-viitekehyksessä toimittamiseen ja hyväksikäyttöön liittyvät tekniikat on listattu muiden taktiikoiden alla, esimerkiksi ”suorittaminen” (MITRE, 2019b) ja ”alustava jalansija” (MITRE, 2019c) taktiikoiden alla. Sosiaalista manipulointia käsitellään viitekehyksessä vain phishingin osalta (MITRE, 2022c). IAM-mallissa havaittiin useita puutteita. Yksi selittävä tekijä on, että mallissa on luokiteltu muissa malleissa hyökkäysvaiheina tai taktiikoina olevia asioita alemmalle abstraktiotasolle. Esimerkiksi käyttöoikeuksien korottaminen on IAM-mallissa aseistautuminen-taktiikan alainen tekniikka, kun se muissa malleissa on erillinen hyökkäysvaihe tai taktiikka. IAM-mallin puutteet ovat kuitenkin selkeitä, erityisesti sosiaalinen manipulointi ja tiedon toimittaminen puuttuvat mallista.

Taulukko 1 Hyökkäysmallien arviointi sisällönanalyysiä vasten

Numero	Nimi	CKC	BKC	UKC	ATT&CK	IAM	Analyysi
1	Tiedustelu	-	-	-	-	-	
2	Resurssien kehittäminen	X	*	X	X	X	X
3	Toimittaminen	X	X	X	*	*	X
4	Sosiaalinen manipulointi	*	*	X	*	*	X
5	Hyväksikäyttö	X	*	X	*	*	X
6	Jalansijan säilyttäminen	X	X	X	X	*	X
7	Turvatoimien välttely	*	*	X	X	X	X
8	Komento ja hallinta	-		-			
9	Kauttatunnelointi			-			
10	Kohteiden etsiminen	*	*	X	X	X	X
11	Käyttöoikeuksien korottaminen	*	X	X	X	*	X
12	Suorittaminen	*	*	X	X	*	X
13	Pääsytietojen haltuunotto	*	*	X	X	*	X
14	Tunkeutumisen laajentaminen		-	-	-		
15	Tiedon kerääminen	*	*	X	X	X	X
16	Tiedon varastaminen	*	X	X	X	X	X
17	Vaikutukset	X	X	X	X	X	X
18	Päämäärät			-			
19	Rekrytointi tai käännekohta	*	*	*	*	X	X
20	Jälkiseuraukset	*	*	*	*	X	X
21	Alustava jalansija				-		
22	Tiedon toimittaminen	*	*	*	*	*	X

Aiempien mallien puutteita voidaan vielä korostaa vertaamalla niitä yksittäisiin tapauksiin esimerkinomaisesti. Esimerkkinä käytettiin tapausta numero 14 (Liite 1). Sisällönanalyysissä tapaukselle koodatut hyökkäysvaiheet ja aiempien mallien kattavuus on kuvattuna oheisessa taulukossa (Taulukko 2). Taulukkoon on merkitty merkillä ”X” kunkin mallin vaiheet, jotka havaittiin tapauksessa, ja merkillä ”*” vaiheet, jotka puuttuvat mallista, mutta esiintyivät tapauksessa. Merkki ”-” merkitsee vaiheet, jotka löytyvät mallista, mutta eivät analyysistä. Tapauksen tiivistelmässä mainitaan:

> Työntekijä vietti sapattivuoden ja palasi töihin eri rooliin. Palattuaan latasi yrityssalaisuuksia firman verkosta. Manipuloi IT-ylläpidon antamaan itselleen laajemmat pääsyoikeudet järjestelmiin ladatakseen lisää tietoja. Toimitti varastettua dataa kilpailijalle ja tallensi sitä kolmannen osapuolen järjestelmiin. Irtisanoutui sisäisen tutkinnan alkaessa. Perusti uuden yrityksen toisen samassa firmassa työskennelleen tekijän kanssa hyödyntäen varastettua tietoa. Toinen tekijä jäi kiinni kannettavan tietokoneen kanssa, jossa löytyi varastettuja tietoja. Tutkinnassa selvisi, että varastettuja tietoja oli myös lähetetty sähköpostilla ja tallennettu pilvipalveluihin.

Analyysissä tulkittiin, että tekijät ovat selkeästi motivoituneita tekemään haittaa (rekrytointi tai käännekohta). Tekijä manipuloi kuvauksessa muita henkilöitä päämääriensä saavuttamiseksi (sosiaalinen manipulointi). Tekijä haki varastettavaa tietoa järjestelmistä (kohteiden etsiminen) ja keräsi niitä (tiedon kerääminen). Tietoja siirrettiin luvattomasti sähköpostilla ja lataamalla niitä pilvipalveluihin (tiedon varastaminen). Tekijä myös toimitti tietoja kilpailevalle yritykselle (tiedon toimittaminen). Tutkinnan alettua tekijä perusti uuden yrityksen, jossa hyödynsi varastettua tietoa (jälkiseuraukset).

Taulukko 2 Mallien vertailu (Tapaus 14)

Numero	Nimi	CKC	BKC	UKC	ATT&CK	IAM	Tapaus 14
1	Tiedustelu	-	-	-	-	-	
2	Resurssien kehittäminen	-		-	-	-	
3	Toimittaminen	-	-	-			
4	Sosiaalinen manipulointi	*	*	X	*	*	X
5	Hyväksikäyttö	-		-			
6	Jalansijan säilyttäminen	-	-	-	-		
7	Turvatoimien välttely			-	-	-	
8	Komento ja hallinta	-		-			
9	Kauttatunnelointi			-			
10	Kohteiden etsiminen	*	*	X	X	X	X
11	Käyttöoikeuksien korottaminen		-	-	-		
12	Suorittaminen			-	-		
13	Pääsytietojen haltuunotto			-	-		
14	Tunkeutumisen laajentaminen		-	-	-		
15	Tiedon kerääminen	*	*	X	X	X	X
16	Tiedon varastaminen	*	X	X	X	X	X
17	Vaikutukset	-	-	-	-	-	
18	Päämäärät			-			
19	Rekrytointi tai käännekohta	*	*	*	*	X	X
20	Jälkiseuraukset	*	*	*	*	X	X
21	Alustava jalansija				-		
22	Tiedon toimittaminen	*	*	*	*	*	X

Taulukosta 3 voidaan havaita, että yksikään aiempi hyökkäysmalli ei ole riittävän kattava kuvaamaan kaikkia tapauskuvauksessa esiteltyjä hyökkäysvaiheita. Yksittäinen tapaus toimii käytännön esimerkkinä korostamaan aiempien hyökkäysmallien puutteita. Tarkemmin esitelty tapauskuvaus myös selkeyttää sisällönanalyysissä tehtyä koodaamista. Vastaavaa taulukointia ja tarkempaa tapauksen esittelyä ei tehty jokaiselle tapaukselle erikseen tutkimusresurssien rajallisuuden vuoksi. Kaikki analyysissä käsitellyt tapaukset on kuvattu

tarkemmin tutkielman liitteessä 1, jonka kautta voidaan tutustua tapausten tiivistelmiin ja niihin koodattuihin vaiheisiin.

5.3 Uuden mallin kehittäminen

Uuden mallin kehittämisessä otettiin lähtökohdaksi mallille edellisessä vaiheessa asetettu vaatimus siitä, että sen on oltava kattavampi kuin aiempien mallien sisällönanalyysiin verrattuna. Uuden mallin kehittämisellä pyrittiin myös vastaamaan päätutkimuskysymykseen:

> Millaisella mallilla voidaan kattavasti kuvata tietoon kohdistuvan sisäpiiriuhkan hyökkäysvaiheet?

Mallille asetettiin vaatimuksena, että sen tulee olla kattavampi sisäpiiriuhkan hyökkäysvaiheiden kuvaamiseen kuin vertailussa käytetyt muut mallit. kattavuusvaatimus saavutettiin yksinkertaisesti siten, että malliin otettiin mukaan kaikki vaiheet, joita sisällönanalyysissä käytettiin. Seuraavassa listassa on esiteltynä mallin kehittämiseen otetut vaiheet, niiden lyhyet kuvaukset ja esimerkkejä hyökkääjien käyttämistä tekniikoista. Vaiheiden kuvaukseen otettiin pohjaksi sisällönanalyysissä käytetyt määritelmät (Liite 2) joita laajennettiin analyysissä käsiteltyjen tapauskuvausten perusteella:

- Aseistautuminen/Resurssien kehittäminen: Toimenpiteet, joilla hyökkääjä yrittää kehittää resursseja toimintansa tukemiseksi. Resurssit voivat olla kyvykkyyksiä, laitteita, ohjelmistoja tai muuta teknistä infrastruktuuria.
- Toimittaminen: Toimenpiteet, joilla hyökkääjä pyrkii toimittamaan tekniseen ympäristöön työkaluja, joita käytetään hyökkäyksen myöhemmissä vaiheissa. Työkaluilla voidaan tarkoittaa esimerkiksi haittaohjelmia.
- Sosiaalinen manipulointi: Toimenpiteet, joilla hyökkääjä pyrkii manipuloimaan muita henkilöitä toimimaan siten, että siitä on hyötyä hyökkääjälle. Manipulointi voi tapahtua esimerkiksi suostuttelemalla.
- Hyväksikäyttö: Toimenpiteet, jotka joilla hyökkääjä pyrkii hyödyntämään ympäristössä olevaa haavoittuvuutta. Haavoittuvuuksia hyödyntämällä hyökkääjä voi esimerkiksi asentaa ympäristöön ohjelmistoja, jotka hyödyttävät hyökkääjää.
- Jalansijan säilyttäminen: Toimenpiteet, joilla hyökkääjä pyrkii säilyttämään jalansijansa ympäristössä. Jalansijan säilyttäminen voidaan tehdä esimerkiksi luomalla takaovia tai käyttäjätunnuksia ympäristöön.
- Turvatoimien välttely: Toimenpiteet, joilla hyökkääjä pyrkii välttelemään kiinnijäämistä. Turvatoimien välttely voi olla esimerkiksi

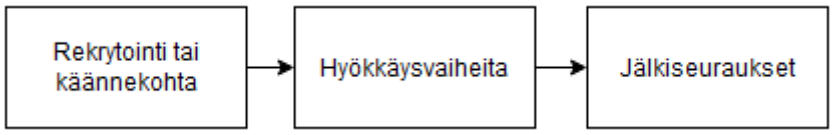
tiedon salaamista, viestinnän peittelyä, todisteiden tuhoamista (esim. ylikirjoitus, lokien hävittäminen) tai valvonnan raja-arvojen alapuolella toimimista (esim. tiedon siirtäminen pienissä erissä ym.)

- Kohteiden etsiminen: Toimenpiteet, joilla hyökkääjä pyrkii etsimään ympäristöstä kiinnostavia kohteita. Kohteita voivat olla esimerkiksi ympäristön tekniset komponentit, tiedostot tai fyysiset asiakirjat.
- Käyttöoikeuksien korottaminen: Toimenpiteet, joilla hyökkääjä pyrkii saamaan laajemmat käyttöoikeudet ympäristössä. Käyttöoikeuksien laajentaminen voidaan tehdä esimerkiksi hyödyntämällä ympäristössä olevia haavoittuvuuksia.
- Suorittaminen: Toimenpiteet, jotka johtavat hyökkääjän hallitsemien ohjelmistojen tai koodin ajamiseen ympäristössä. Hyökkääjä voi suorittaa esimerkiksi salasanan murtamiseen käytettäviä ohjelmia tai ympäristön toiminnalle haitallisia skriptejä.
- Pääsytietojen haltuunotto: Toimenpiteet, joilla hyökkääjä pyrkii ottamaan haltuun pääsytietoja. Hyökkääjä voi esimerkiksi ottaa käyttöön muiden tunnuksia murtamalla salasanoja, tai saamalla muutoin tunnuksia käyttöön työtehtäviensä aikana.
- Tiedon kerääminen: Toimenpiteet, joilla hyökkääjä pyrkii keräämään hyökkäyksen kohteena olevaa tietoa ympäristöstä. Keräämisessä voidaan käyttää hyödyksi esimerkiksi hyökkääjän käytössä olevaa työasemaa tai jotain muuta sähköistä tietosäilöä. Kerääminen voi tapahtua myös paperimuodossa, jolloin tietoa usein tulostetaan hyökkääjän toimesta.
- Tiedon varastaminen: Toimenpiteet, joilla hyökkääjä pyrkii kuljettamaan tiedon luvattomasti pois organisaation ympäristöstä. Tiedon varastaminen voidaan tehdä sähköisessä muodossa esimerkiksi tietoliikenneyhteyksiä (sähköposti, pilvipalvelut yms.) tai fyysisiä siirtomedioita (USB-muistit, CD/DVD, muut ulkoiset muistivälineet) hyödyntäen. Fyysisessä muodossa tieto varastetaan useimmiten paperille tulostettuna.
- Vaikutukset: Hyökkääjän toimet, joilla manipuloidaan kohdejärjestelmää hyökkääjän maalien mukaisesti. Vaikutukset voivat olla esimerkiksi kohteen sammuttaminen, poistaminen tai muokkaaminen.
- Rekrytointi tai käännekohta: Tapahtumat, jotka johtavat siihen, että sisäpiiriläinen motivoituu tekemään haitallisia tekoja. Motivoitumisen syynä voi olla esimerkiksi merkittäväksi koetut tapahtumat, kuten tehtävien muutokset, työsuhteen päättyminen tai sisäpiiriläisen henkilökohtaisen elämän suuret muutokset. Syynä voi olla myös kolmannen osapuolen tekemä rekrytointi, jolloin motivaattorina toimii usein jonkinlaiset palkkiot rekrytoivalta taholta. Sisäpiiriläinen voi olla myös alun perin organisaatioon tullessaan motivoitunut tekemään haitallisia tekoja, kuten esimerkiksi taparikolliset.
- Jälkiseuraukset: Tekijän käyttäytymisessä tapahtuvat muutokset, joita voidaan havaita tekojen jälkeen. Jälkiseuraukset voivat olla

esimerkiksi yllättävää matkustamista, epänormaalia rahankäyttöä tai haitallisten tekojen ylpeää esittelemistä muille.

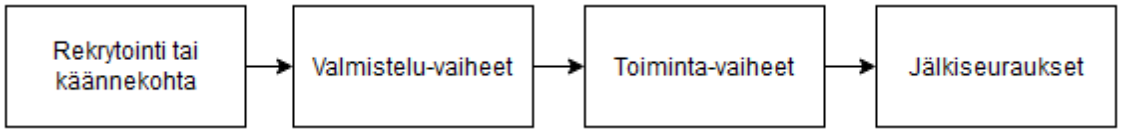
- Tiedon toimittaminen: Toimenpiteet, joilla hyökkääjä pyrkii toimittamaan varastamansa tiedon kolmannelle osapuolelle. Toimittaminen voidaan tehdä esimerkiksi kuljettamalla tiedot fyysisesti johonkin sovittuun paikkaan tai siirtämällä tiedot kolmannen osapuolen ulottuville sähköisesti esimerkiksi välityspalvelimen kautta.

Malliin sisällytettävien vaiheiden ajallista järjestystä hyökkäyksessä hahmotettiin tutkimalla analysoitujen tapauskuvausten tiivistelmiä. Tapauskuvauksia tutkimalla havaittiin, että jotkin vaiheet tapahtuvat hyvin usein peräkkäin. Esimerkiksi tiedon etsiminen, tiedon kerääminen, tiedon varastaminen ja tiedon toimittaminen tapahtuvat usein peräkkäisessä järjestyksessä, kuten esimerkiksi liitteen 1 tapauksissa 14, 19 ja 61. Lisäksi havaittiin, että tapauksien lähtökohtana on lähes aina tekijän motivoituminen haitallisten tekojen tekemiseen, eli hyökkäysvaiheena ”rekrytointi tai käännekohta”. Jälkiseuraukset-vaihe taas on usein analysoiduissa tapauksissa viimeisenä vaiheena, esimerkiksi tapauksissa 12, 62 ja 94. Näiden havaintojen avulla voitiin osa vaiheista laitaa järjestykseen. Kronologisen järjestyksen avulla voidaan ymmärtää, kuinka pitkällä hyökkääjä on tavoitteidensa saavuttamisessa. Alustava kronologinen järjestys on kuvattu oheisessa kuvassa (Kuva 7).



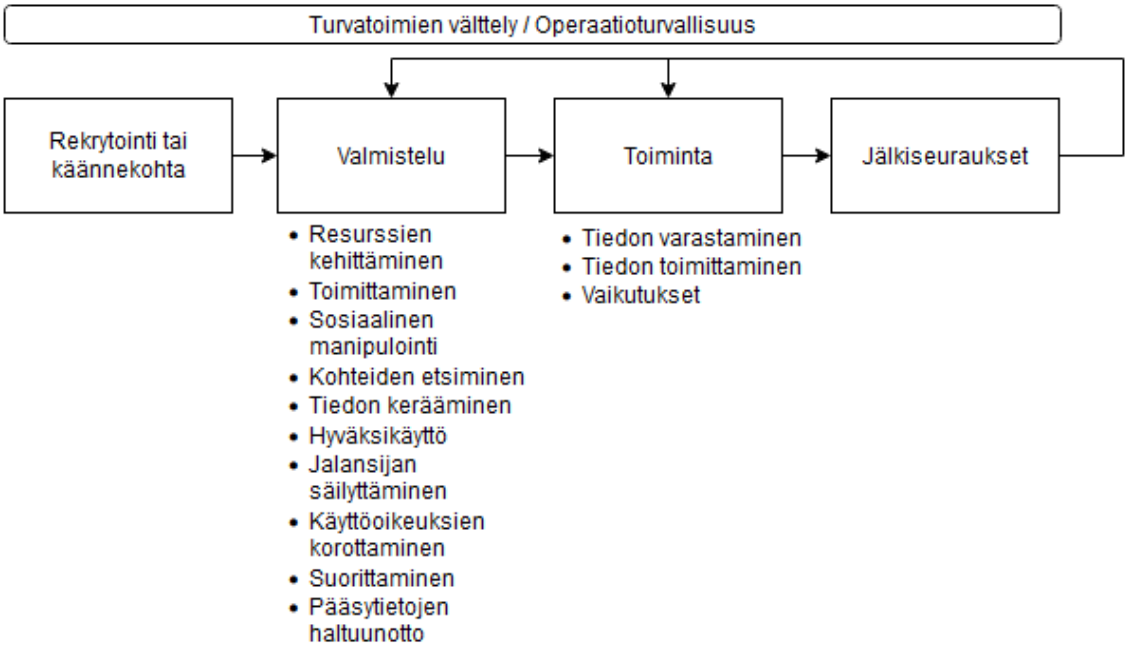
Kuva 7 Alustava hyökkäysketju

Tapauksissa havaittiin myös, että esimerkiksi ”vaikutukset” ja ”tiedon varastaminen” eivät esiintyneet samassa tapauksessa kertaakaan. Luvussa 3.2.2 kuvatut sisäpiiriuhkan kategoriat vastaavat jossain määrin tätä havaintoa. IT-sabotaasitapaukset johtavat onnistuessaan vaiheeseen ”vaikutukset”, kun taas tiedon varastamiseen liittyvät tapaukset kuuluvat usein kategorioihin ”petos” ja ”aineettoman omaisuuden varastaminen”. Onnistuneissa hyökkäyksissä ennen jälkiseurauksia tapahtuu usein joko tiedon varastaminen ja toimittaminen tai vaikutukset (vrt. IT-sabotaasi, petos, aineettoman omaisuuden varastaminen). Tätä ennen tapahtuvat vaiheet voidaan tulkita valmisteluksi varsinaista hyökkääjän tavoittelemaa toimintaa varten. Näiden havaintojen avulla saadaan muodostettua oheisen kuvan mukainen hyökkäysketju (Kuva 8), jossa on ryhmiteltynä valmistelu- ja toiminta-vaiheet. Valmistelu-vaiheessa tekijä pyrkii työskentelemään kohti ”toiminta”-vaiheita, jossa varsinainen tavoiteltu toiminta (esim. tiedon varastaminen tai vaikutukset) tapahtuu.



Kuva 8 Ryhmitelty hyökkäysketju

Tutkimalla tapauksia ryhmitellyn hyökkäysketjun avulla havaittiin, että jotkin hyökkäysvaiheet sopivat hyvin valmistelu-vaiheeseen ja toiset taas toiminta-vaiheeseen. Tiedon varastaminen, tiedon toimittaminen ja vaikutukset kuuluvat luontevasti toiminta-vaiheeseen. Valmistelu-vaiheeseen voidaan ryhmitellä vaiheet, joilla tekijä pyrkii kohti toiminta-vaihetta. Tiedon varastamiseen tähtäävissä tapauksissa tekijä usein valmistelee tiedon varastamista esimerkiksi etsimällä ja keräämällä tietoja (kohteiden etsiminen, tiedon kerääminen), kuten esimerkiksi tapauksissa 19, 53 ja 61. Tapausaineistossa tekojen valmisteluun käytettiin myös enemmän teknisiä taitoja vaativia menetelmiä, kuten tapauksissa 38, 104 ja 118. Tapauksissa esiintyy usein myös kiinnijäämisen välttelyä ja operaatioturvallisuuden harjoittamista eri keinoin mm. salatulla viestinnällä, tietojen ylikirjoittamisella (esim. tapaus 20), ”burner”-laitteiden käytöllä (esim. tapaus 46), tietojen luovuttamisen salailulla (esim. tapaus 79) ja monin muin keinoin. Tällaiset toimet on analyysissä koodattu ”turvatoimien välttelyn” alle. Turvatoimien välttely ei näytä sopivan sinällään valmistelu-vaiheeseen tai toiminta-vaiheeseen, vaan sitä harjoitetaan koko hyökkäyksen ajan. Vastaava havainnon toi esille myös Reidy (2013), jonka esittelemää sisäpiiriuhkan hyökkäysketjua esiteltiin lyhyesti luvussa 2.5. Tietyissä tapauksissa (19 ja 78) on havaittavissa myös syklisyyttä, eli hyökkääjä voi palata valmistelu- tai toiminta-vaiheeseen suoritettuaan hyökkäyksen, mikäli hyökkääjä haluaa jatkaa toimintaa. Näiden havaintojen avulla saadaan muodostettua hyökkäysketju, joka on esitetty oheisessa kuvassa (Kuva 9).



Kuva 9 Sisäpiiriuhkan hyökkäysketju

Mallin avulla voidaan hahmottaa millaisia toimia sisäpiiriuhkan toimijat tekevät pyrkiessään kohti päämääriään. Hahmottamalla hyökkäyksen vaiheet, voidaan tutkia tapauksia tehokkaammin ja suunnitella toimenpiteitä organisaation suojaamiseksi sisäpiiriuhkalta. Mallin sisältämä ryhmittely valmistelun ja toiminnan välillä korostaa havainnoinnin tärkeyttä jo valmistelun aikana, että tekijä ei pääse etenemään organisaatiolle haitallisempaan toiminta-vaiheeseen asti.

5.4 Uuden mallin esittely

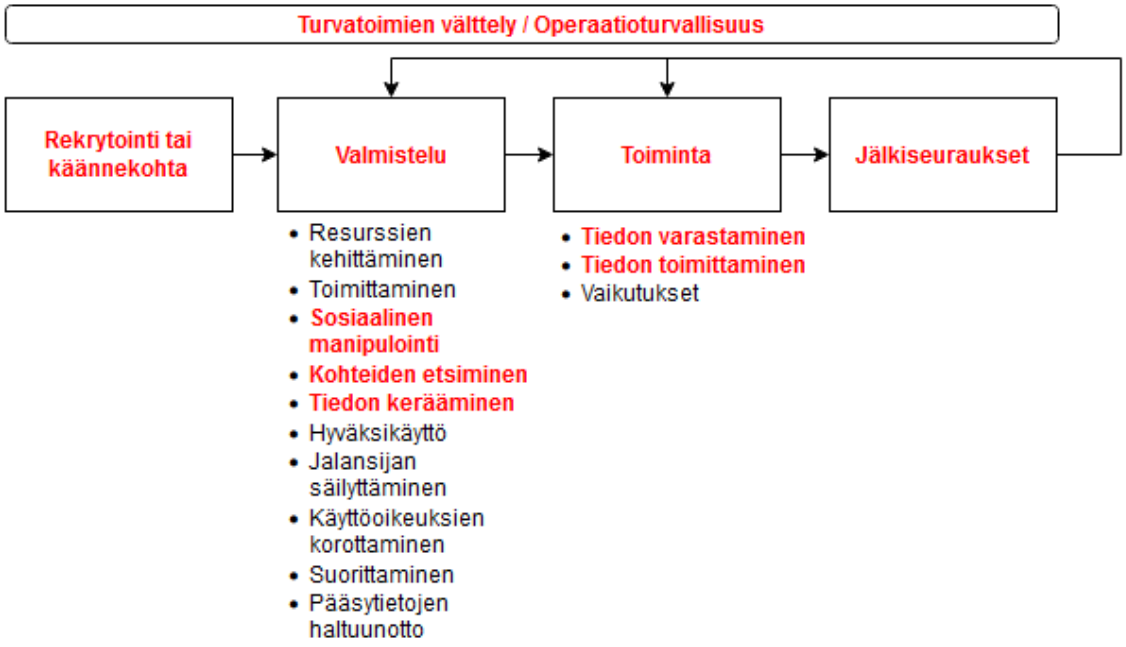
Tutkimuksessa kehitetyn mallin avulla voidaan kuvata pahantahtoisen sisäpiiriuhkan hyökkäyksen vaiheet. Yksittäisen hyökkäyksen vaiheita kuvatessa, mallista valikoidaan kyseiseen hyökkäykseen soveltuvat vaiheet, sillä kaikkien vaiheiden esiintyminen yksittäisessä hyökkäyksessä on erittäin harvinaista. Mallin avulla voidaan myös arvioida suojamenetelmien kattavuutta sisäpiiriuhkaa vastaan. Hyökkäyksen vaiheittainen eteneminen mahdollistaa turvatoimien suunnittelun siten, että hyökkäys voidaan katkaista aiemmissa, vähemmän haitallisissa vaiheissa. Tässä osiossa esitellään, miten yksittäisen sisäpiiriuhkan hyökkäystapauksen voi analysoida tutkimuksessa kehitetyn mallin avulla.

Mallin käyttö esitellään kuvaamalla yksittäinen tapaus esimerkinomaisesti mallin avulla. Esimerkkinä käytetään liitteen 1 tapausta numero 77. Tapauksen 77 sisällön tiivistelmä on seuraava:

> Luovutti turvallisuusluokiteltuja tietoja työpaikaltaan vieraan valtion edustajille. Vieraan valtion tiedustelupalvelu rekrytoi tekijän ja tekijä toimitti tietoa rahaa vastaan. Osa tiedoista kerättiin vieraan valtion pyynnöstä, mutta tekijällä oli myös aktiivinen rooli tiedon

tarjoajana. Yritti rekrytoida toisenkin työntekijän ja neuvoi miten tietoja voi lähettää jäämättä kiinni. Toinen työntekijä ilmiantoi tekijän.

Tapauskuvauksessa on selkeästi tunnistettavissa useita mallissa käytettäviä vaiheita, joiden avulla voidaan luoda tämän yksittäisen hyökkäyksen hyökkäysketju. Oheisessa kuvassa (Kuva 10) on tapauksessa 77 tunnistettavat vaiheet punaisella, lihavoidulla tekstillä.



Kuva 10 Tapaus 77 hyökkäysvaiheet

Tapauksessa havaittiin selkeästi, että teot käynnistyvät tekijän rekrytoinnista vieraan valtion tiedustelupalvelun toimesta (rekrytointi tai käännekohta). Tekijä valmistautui etsimällä ja keräämällä ympäristöstä tietoa (kohteiden etsiminen, tiedon kerääminen). Tekijä varasti tietoja ja toimitti niitä vieraan valtion edustajille (tiedon varastaminen, tiedon toimittaminen). Tapauksen tiivistelmästä on tulkittavissa myös syklisyys, koska tekijä jäi kiinni yritettyään saada toisenkin työntekijän organisaatiosta mukaan toimintaan (sosiaalinen manipulointi). Turvatoimien välttely voidaan tulkita tiivistelmästä, koska tekijä kertoi toiselle työntekijälle menetelmiä tiedon lähettämisestä ilman kiinnijäämisen pelkoa. Jälkiseuraukset kuvaavat mallissa muutoksia tekijän käyttäytymisessä, joka tässä tapauksessa ilmenee yrityksenä rekrytoida toinen työntekijä.

5.5 Uuden mallin arviointi

Mallille asetettiin tavoitteeksi, että se kykenee kuvaamaan aiempia malleja kattavammin sisäpiiriuhkan tapauksia. Kattavuutta voidaan arvioida vertaamalla tapauskuvauksille tehtyyn sisällönanalyysiin (Taulukko 3). Taulukkoon on

merkitty merkillä ”X” kunkin mallin vaiheet, jotka havaittiin tapauksessa, ja merkillä ”*” vaiheet, jotka puuttuvat mallista, mutta esiintyivät tapauksessa. Merkki ”-” merkitsee vaiheet, jotka löytyvät mallista, mutta eivät analyysistä. Taulukosta voidaan todeta, että malli täyttää sille asetetut tavoitteet, ja sisältää kaikki tapauskuvauksista sisällönanalyysin kautta johdetut hyökkäysvaiheet.

Taulukko 3 Sisäpiiriuhkan hyökkäysketjun arviointi

Numero	Nimi	CKC	BKC	UKC	ATT&CK	IAM	Sisäpiiriuhkan hyökkäysketju	Analyysi
1	Tiedustelu	-	-	-	-	X		
2	Resurssien kehittäminen	X	*	X	X	X	X	X
3	Toimittaminen	X	X	X	*	*	X	X
4	Sosiaalinen manipulointi	*	*	X	*	*	X	X
5	Hyväksikäyttö	X	*	X	*	*	X	X
6	Jalansijan säilyttäminen	X	X	X	X	*	X	X
7	Turvatoimien välttely	*	*	X	X	X	X	X
8	Komento ja hallinta	-		-				
9	Kauttatunnelointi			-				
10	Kohteiden etsiminen	*	*	X	X	X	X	X
11	Käyttöoikeuksien korottaminen	*	X	X	X	*	X	X
12	Suorittaminen	*	*	X	X	*	X	X
13	Pääsytietojen haltuunotto	*	*	X	X	*	X	X
14	Tunkeutumisen laajentaminen		-	-	-			
15	Tiedon kerääminen	*	*	X	X	X	X	X
16	Tiedon varastaminen	*	X	X	X	X	X	X
17	Vaikutukset	X	X	X	X	X	X	X
18	Päämäärät			-				
19	Rekrytointi tai käännekohta	*	*	*	*	X	X	X
20	Jälkiseuraukset	*	*	*	*	X	X	X
21	Alustava jalansija				-			
22	Tiedon toimittaminen	*	*	*	*	*	X	X

Taulukosta voidaan havaita, että tutkimuksessa suunniteltu malli kuvaa kattavammin sisäpiiriuhkan tapausten vaiheita sisällönanalyysiin perustuen. CKC-mallissa puutteet ovat merkittäviä ja monimuotoisia, samoin BKC-mallissa. Näiden mallien puutteita yritettiin paikata UKC-mallilla. Taulukossa esiteltyjä tuloksia tulkitsemalla nähdään, että UKC-malli sisältää sisäpiiriuhkaan liittyviä puutteita. UKC-mallista puuttuu kokonaan sisäpiiriläisen kääntyminen sekä jälkiseuraukset, jotka ovat erityisesti sisäpiiriuhkaan liittyviä vaiheita. ATT&CK-viitekehyksessäkin on vastaavia puutteita. Lisäksi viitekehyksestä puuttuu sosiaalinen manipulointi erillisenä taktiikkana sekä joitakin teknisiä vaiheita kuten toimittaminen ja hyväksikäyttö. IAM-mallissa, joka on kehitetty erityisesti sisäpiiriuhkan mallintamiseen, ei huomioida sisäpiiriuhkan toimijoiden potentiaalista kykyä hyödyntää teknisiä taitojaan suojausten kiertämiseksi. Näitä puutteita kuvastaa IAM-mallista puuttuvat vaiheet 3, 5, 6, ja 11–13. IAM-mallista puuttuu myös sosiaalinen manipulointi erillisenä taktiikkana.

Uuden mallin arvioimiseksi esitellään myös yksittäinen esimerkki ja vertailu aiempiin malleihin. Kyseinen esimerkki ei ole osa aiemmin tehtyä sisällönanalyysia, vaan erillinen tapaus, johon sovelletaan samankaltaista analyysiä. Arvioinnissa käytetyn esimerkkitapauksen tiivistelmä:

> Tekijä toimi sosiaalisen median ylläpitäjänä. Erään valtion edustajat lahjoivat tekijää mm. rahalla ja arvoesineillä. Lahjuksia saatuaan tekijä etsi ja keräsi valtiota kiinnostavien käyttäjien yksityistietoja ja luovutti niitä useaan otteeseen valtion edustajille. Tekijä teki saamistaan arvoesineistä myynti-ilmoituksia Internetiin ja matkusti ulkomaille tapaamaan valtion edustajia. Tekijä yritti peitellä saamiaan maksuja käyttämällä lähisukulaisen nimissä avattua pankkitiliä ja pieniä siirtosummia.

Tiivistelmästä voidaan havaita selkeästi, että tekijä rekrytoitiin (rekrytointi tai käännekohta). Tekijä etsi tietoja, keräsi ja luovutti niitä useita kertoja (kohteiden etsiminen, tiedon kerääminen, tiedon varastaminen). Tekijän Internetiin laittamat myynti-ilmoitukset, ulkomaanmatkat ja erikoiset maksutapahtumat voidaan tulkita käyttäytymisen muutoksiksi tekojen jälkeen (jälkiseuraukset). Tekijä pyrki myös peittelemään jälkiään (Turvatoimien välttely/Operaatioturvallisuus). Tapaukselle koodatut vaiheet ja vertailu eri mallien kesken on kuvattu oheisessa taulukossa (Taulukko 4). Taulukkoon on merkitty merkillä ”X” kunkin mallin vaiheet, jotka havaittiin tapauksessa, ja merkillä ”*” vaiheet, jotka puuttuvat mallista, mutta esiintyivät tapauksessa. Merkki ”-” merkitsee vaiheet, jotka löytyvät mallista, mutta eivät analyysistä.

Taulukko 4 Esimerkkitapauksen vertailu mallien kesken

Numero	Nimi	CKC	BKC	UKC	ATT&CK	IAM	Sisäpiiriuhkan hyökkäysketju	Esimerkki
1	Tiedustelu	-	-	-	-	-		
2	Resurssien kehittäminen	-		-	-	-	-	
3	Toimittaminen	-	-	-			-	
4	Sosiaalinen manipulointi			-			-	
5	Hyväksikäyttö	-		-			-	
6	Jalansijan säilyttäminen	-	-	-	-		-	
7	Turvatoimien välttely	*	*	X	X	X	X	X
8	Komento ja hallinta	-		-				
9	Kauttatunnelointi			-				
10	Kohteiden etsiminen	*	*	X	X	X	X	X
11	Käyttöoikeuksien korottaminen		-	-	-		-	
12	Suorittaminen			-	-		-	
13	Pääsytietojen haltuunotto			-	-		-	
14	Tunkeutumisen laajentaminen		-	-	-			
15	Tiedon kerääminen	*	*	X	X	X	X	X
16	Tiedon varastaminen	*	X	X	X	X	X	X
17	Vaikutukset	-	-	-	-	-	-	
18	Päämäärät			-				
19	Rekrytointi tai käännekohta	*	*	*	*	X	X	X
20	Jälkiseuraukset	*	*	*	*	X	X	X
21	Alustava jalansija				X			
22	Tiedon toimittaminen	*	*	*	*	*	X	X

Taulukosta voidaan havaita, että tässä tutkimuksessa kehitetty malli kykenee kuvaamaan myös tutkielman sisällönanalyysin ulkopuolisen tapauksen hyökkäysvaiheet kattavammin kuin aiemmat hyökkäysketjut. IAM-malli kykenee esimerkkitapauksen osalta kuvaamaan kaikki vaiheet, paitsi erillisen tiedon toimittamisen (vaihe 22). IAM-mallissa on kuitenkin aiemmin mainittuja puutteita, kun verrataan koko sisällönanalyysiin (Taulukko 4).

Malli näyttää arvioinnin perusteella täyttävän sille asetetut vaatimukset. Malliin valitut vaiheet ja rakenne perustuvat tutkimuksessa tehdyn sisällönanalyysiin ja tutkimuksen tapausaineistoon. Tutkimuksessa kehitetty malli, sen esittely ja arviointi vastaavat tutkielman päätutkimuskysymykseen:

> Millaisella mallilla voidaan kattavasti kuvata tietoon kohdistuvan sisäpiiriuhkan hyökkäysvaiheet?

6 POHDINTA JA YHTEENVETO

Tutkimuksen tarkoituksena oli selvittää, miten tietoon kohdistuvat sisäpiiriuhkan hyökkäykset etenevät käytännössä. Tutkimuksen alussa tehtiin oletamus, että sisäpiiriuhkatoimijoiden käyttämissä taktiikoissa on selkeästi havaittavia eroja verrattuna organisaatioiden ulkopuolisten uhkatoimijoiden suorittamiin hyökkäyksiin. Tutkimuksessa kehitettiin erityisesti tietoon kohdistuvia sisäpiiriuhkan hyökkäysvaiheita kuvaava malli, johon sisältyy uudenlainen yhdistelmä hyökkäysvaiheita. Malli sisältää kattavasti vaiheita, joita havainnoitiin todellisten tapauskuvausten perusteella.

Tutkimus osoitti, että yleisesti kyberhyökkäyksiin käytettävät mallit eivät kuvaa riittävän kattavasti sisäpiiriuhkan käyttämiä taktiikoita. Kyberhyökkäysketjujen puutteellisuus sisäpiiriuhkan osalta on huomattu (Pols, 2017, s. 20-21; Reidy 2014) ja sisäpiiriuhkan taktiikoita ja tekniikoita on kartoitettu ja mallinnettu (Read, Alamir, Dugdale, Stride & Lobo, 2021), mutta aiemmat mallit havaittiin tutkimuksessa silti puutteellisiksi. Aiemmissa kyberhyökkäysmalleissa puutteet painottuivat vaiheisiin, jotka voivat usein tapahtua organisaation toimintaympäristön ulkopuolella, kuten rekrytointi ja tiedon toimittaminen. Aiemmissa sisäpiiriuhkaan erikoistuneissa malleissa puuttui erityisesti kyberympäristössä tehtävät teknisesti vaativiin toimenpiteisiin, kuten käyttöoikeuksien korottaminen ja pääsyoikeuksien haltuunotto. Tämän tyyppiset toimenpiteet olivat tässäkin tutkimuksessa harvinaisia, mutta niitä esiintyi silti, eli nekin kuuluvat sisäpiiriuhkatoimijoiden käyttämiin taktiikoihin. Aiemmissa sisäpiiriuhkan hyökkäysmalleissa on mahdollisesti ollut käytössä suppeampi aineisto tai erilainen sisäpiiriuhkan määritelmä, jonka seurauksena hyökkääjän teknisemmät toimenpiteet ovat jääneet mallien ulkopuolelle.

Tutkimuksessa havaittiin erillinen hyökkäysvaihe ”tiedon toimittaminen”. Tämä on uusi havainto, jota ei ole käytetty aiemmissa malleissa. Aiemmissa malleissa hyökkäysketju päättyy tiedon osalta usein tiedon varastamiseen. Tämä voi johtua siitä, että tiedon varastamisen jälkeen aiemmissa malleissa on kenties oletettu, että tieto on menetetty ja hyökkääjä on jo saavuttanut viimeisen maalinsa, eikä hyökkäys ole enää organisaation vastatoimien piirissä. Tiedon toimittaminen erillisenä vaiheena on uusi löydös, joka laajentaa hyökkäysmalleissa olevien

vaiheiden kuvauksia ja mahdollistaa hyökkääjän toimien tarkemman hahmottamisen hyökkäysketjun loppupäässä.

Tutkimuksessa käytetty tapausaineisto perustuu pitkälti Yhdysvalloissa tapahtuneisiin tapauksiin, mikä saattaa aiheuttaa rajauksia yleistettävyyden kannalta, mikäli kulttuurilla on vaikutusta sisäpiiriuhkan toimintaan. Tulosten yleistettävyyttä rajaa myös se, että tapauskuvaukset ovat julkisia, eli ne sisältävät vain sellaista aineistoa, mitä julkaisevat tahot haluavat julkaista. Sisäpiiriuhkaan liittyvät tapaukset saattavat sisältää sensitiivisiä yksityiskohtia, jotka jäävät tapauskuvausten ulkopuolelle. Tällaisilla yksityiskohdilla voi olla merkitystä hyökkäysvaiheiden kartoittamisen kannalta. Tutkimuksessa käytetty abstraktiotaso todettiin kuitenkin sopivaksi, ja tapauskuvauksiin oli useimmiten helppo liittää analyysissä käytettäviä käsitteitä.

Analyysissä jouduttiin tekemään joitakin tulkintoja hyökkääjän toimenpiteistä. Esimerkiksi tiedon varastamisen yhteyteen liitettiin usein tiedon kerääminen, vaikka siihen liittyvää mainintaa ei erikseen esiintynyt aineistossa. Tieto on kuitenkin jotenkin kerättävä, että sen voi varastaa, joten tulkinta on looginen. Tulkinnoilla voi olla vaikutusta siihen, kuinka usein kutakin käsitettä käytettiin analyysivaiheessa. Tutkimuksessa kehitetyssä mallissa ei kuitenkaan huomioitu käyttökertojen lukumäärien eroja, vaan malliin kelpuutettiin tutkimuksessa kaikki vaiheet, joita käytettiin analyysissa edes kerran. Mallissa saattaa kuitenkin olla puutteita, koska tutkimuksen tapausaineisto on rajallinen. Malliin hyväksyttiin vain aineistossa ilmenneitä hyökkäysvaiheita eli mallista voi puuttua vaiheita, joita sisäpiiriuhka voisi potentiaalisesti hyödyntää.

Tutkimuksen tulokset osoittavat, että yleisesti käytössä olevia kyberhyökkäysmalleja hyödyntämällä ei kyetä mallintamaan sisäpiiriläisen toteuttamaa hyökkäystä riittävän kattavasti. Tutkimuksessa tehtyjä havaintoja ja tuloksia voidaan hyödyntää käytännössä sekä sisäpiiriuhkan tapausten kuvaamisessa, että sisäpiiriuhkan hallinnassa organisaatiossa. Havaintoja voidaan hyödyntää myös yleisemmin tietoon kohdistuvien hyökkäysten tai kyberhyökkäysten mallintamisessa. Tutkimuksessa käytettyä tutkimusmenetelmää, jossa yhdistellään DSRM-menetelmään tapausaineistojen analyysi, voidaan käyttää muidenkin uhkatyyppien hyökkäysketjujen kartoittamiseen.

Sisäpiiriuhkan mallintaminen ei ole kehittynyt samalle tasolle kuin esimerkiksi ulkopuolisten kyberhyökkäysten mallintaminen. APT-toimijoiden toimenpiteitä voidaan mallintaa esimerkiksi luvussa 2.3 kuvatun MITRE ATT&CK-viitekehyksen avulla. ATT&CK sisältää tekniikoita, jotka kuvaavat hyökkääjien toimintaa alemmalla abstraktiotasolla kuin taktiikat tai hyökkäysketjujen hyökkäysvaiheet. Sisäpiiriuhkaa voisi myös tutkia matalammalla abstraktiotasolla, koska hyökkääjän tekniikoiden tuntemisesta on selkeää käytännön hyötyä. Jatkotutkimusaiheena voisikin olla tarkempien, tekniikoita sisältävien tapauskuvauksien kartoittaminen esimerkiksi haastattelututkimuksien keinoin. Tekniikoiden kartoittaminen vaatii todennäköisesti tarkempia kuvauksia tapauksista, kuin mitä tässä tutkimuksessa käytettiin. Haasteena tarkempien sisäpiiriuhkan kuvausten saatavuudessa on tiedon sensitiivisyys.

Eräänä jatkotutkimusaiheena voidaan kartoittaa sopivia vastatoimia sisäpiiriuhkan toimintaa vastaan. Vastatoimien kartoittamisessa voidaan ottaa malliksi esimerkiksi MITRE:n kehittelemä D3FEND-viitekehys. Vastatoimien suunnittelua voidaan tehdä tehokkaammin, kun on tiedossa hyökkääjän käyttämiä menetelmiä, kuten tässä tutkimuksessa kartoitetut hyökkäysvaiheet.

Uhkien hallitseminen ja turvatoimien suunnittelu ja oikea mitoittaminen on tärkeä edellytys monien organisaatioiden toiminnalle. Tutkimuksessa käsiteltävä sisäpiiriuhka on yksi uhkista, joita kohdistuu organisaatioihin. Sisäpiiriuhka voi ominaisuuksiensa takia tuottaa merkittäviä tai jopa korvaamattomia vahinkoja organisaatioille ja niiden toimintaedellytyksille. Sisäpiiriuhkan hallinta vaatii laajaa ymmärrystä sekä teknisistä että henkilöstöön ja lakeihin liittyvistä asioista. Sisäpiiriuhkatoimijoiden taktiikoiden ja hyökkäysvaiheiden ymmärtäminen on tärkeä askel uhkan hallinnassa. Ymmärtämällä sisäpiiriuhkan luonne ja toiminta, voidaan mitoittaa vastatoimia tehokkaammin ja parantaa organisaation tietoturvan tilaa.

LÄHTEET

Bryant, B. D. & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security, 67*, 198-210. doi:10.1016/j.cose.2017.03.003

Cappelli, D. M., Moore, A. P. & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes.* Addison-Wesley Professional.

Carnegie Mellon University. (2022). Our Research: Insider Threat. Haettu 20. marraskuuta 2022 osoitteesta https://www.sei.cmu.edu/our-work/insider-threat/index.cfm

CERT National Insider Threat Centre. (2022). Common Sense Guide to Mitigating Insider Threats, Seventh Edition. Carnegie Mellon University, Software Engineering Institute. Haettu 21.9.2022 osoitteesta https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=886874

Costa, D. (2017, 7. maaliskuuta). CERT Definition of 'Insider Threat' - Updated . Haettu 20.11.2022 osoitteesta https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Cybersecurity & Infrastructure Security Agency CISA. (2022, 4. elokuuta). Defining Insider Threats. Haettu 20.11.2022 osoitteesta https://www.cisa.gov/defining-insider-threats

Dupuis, M. & Khadeer, S. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. *RIIT '16: Proceedings of the 5th Annual Conference on Research in Information Technology* (ss. 35-40). Association for Computing Machinery. doi:10.1145/2978178.2978185

Engel, G. (2014, 18. marraskuuta). Deconstructing The Cyber Kill Chain. Haettu 20.11.2022 osoitteesta https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain

Federal Bureau of Investigation. (2022). *Internet Crime Report 2022.* Haettu 20.4.2022 osoitteesta https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C. & Hohimer, R. E. (2012). Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. *45th Hawaii International Conference on System Sciences*, (ss. 2392-2401). doi:10.1109/HICSS.2012.309

Hayden, M. V. (1999). *The Insider Threat to U.S. Government Information Systems.* The National Security Telecommunications and Information Systems Security Committee. Noudettu osoitteesta https://www.hsdl.org/?view&did=18530

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), ss. 75-105. doi:https://doi.org/10.2307/25148625

Hlavek, A., Folk, S., Sundar, S. & Baker, J. (2022, 7. helmikuuta). Launching a community-driven insider threat knowledge base. Haettu 19.11.2022 osoitteesta https://medium.com/mitre-engenuity/launching-a-community-driven-insider-threat-knowledge-base-20a249acb2f

Homoliak, I., Toffalini, F., Guarnizo, J. Elovici, Y. & Ochoa, M. (2020). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys, 52*(2), 1-40. doi:10.1145/3303771

Hutchins, E. Cloppert, M. & Amin, R. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *6th Annual Conference on Information Warfare and Security.*

Illinois Library. (2020). *Qualitative Data Analysis: Coding*. Haettu 9.4.2023 osoitteesta LibGuides at University of Illinois: https://guides.library.illinois.edu/qualitative/coding

INFOSEC Research Council. (2005). *Hard Problem List.* Haettu 19.11.2022 osoitteesta https://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf

Insider Threat Team, CERT. (2013). Unintentional Insider Threats: A Foundational Study. doi:10.1184/R1/6585575.v1

Kont, M. Pihelgas, M. Wojtkowiak, J. Osula, A.-M. & Trinberg, L. (2015). *Insider Threat Detection Study.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. Haettu 21. marraskuuta 2022 osoitteesta https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Lehto, M. (2022). APT Cyber-attack Modelling : Building a General Model. *Proceedings of the17th International Conference on Cyber Warfare and Security. 17*, ss. 121-129. Albany, New York, USA: Academic Conferences International Ltd. doi:https://doi.org/10.34190/iccws.17.1.36

Lockheed Martin. (2022). *The Cyber Kill Chain*. Noudettu 19.11.2022 osoitteesta: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Maasberg, M. Warren, J. & Beebe, N. L. (2015). The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits. *2015 48th Hawaii International Conference on System Sciences*, (ss. 3518-3526). doi:10.1109/HICSS.2015.423

MITRE. (2019a). *Impact, Tactic TA0040*. Noudettu 22.4.2023 osoitteesta https://attack.mitre.org/tactics/TA0040/

MITRE. (2019b). *Initial Access, Tactic TA0001*. Noudettu 24.4.2023 osoitteesta https://attack.mitre.org/tactics/TA0001/

MITRE. (2019c). *Execution, Tactic TA0002*. Noudettu 24.4.2023 osoitteesta https://attack.mitre.org/tactics/TA0002/

MITRE. (2022a). *MITRE ATT&CK*. Noudettu 15.3.2023 osoitteesta https//attack.mitre.org/

MITRE. (2022b). *Tactics - Enterprise*. Noudettu 15.3.2023 osoitteesta https://attack.mitre.org/tactics/enterprise/

MITRE. (2022c). *Phishing – Technique T1566*. Noudettu 24.4.2023 osoitteesta https://attack.mitre.org/techniques/T1566/

Mitropoulos, S. Patsos, D. & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security, 25*(5), 351-370. doi:10.1016/j.cose.2005.09.006

National Institute of Standards and Technology. (2011). NIST Special Publication 800-39 Managing Information Security Risk. Noudettu 20.11.2022 osoitteesta https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Neumann, P. G. (2010). Combatting Insider Threats. Teoksessa C. Probst, J. Hunker, D. Gollmann & M. Bishop, *Insider Threats in Cyber Security Advances in Information Security, vol 49* (ss. 17-44). Boston, MA: Springer. Noudettu osoitteesta https://doi.org/10.1007/978-1-4419-7133-3_2

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. & Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks. *2014 IEEE Security and Privacy Workshops*, (ss. 214-228). doi:10.1109/SPW.2014.38

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Pfleeger, S. L., Predd, J. B., Hunker, J. & Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *IEEE Transactions on Information Forensics and Security, 5*(1), ss. 169-179. doi:10.1109/TIFS.2009.2039591

Pols, P. (2017, 7. joulukuuta). The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks. Haettu 22.11.2022 osoitteesta https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf

Pols, P. (2022). The Unified Kill Chain: Raising resilience against advanced cyber attacks. Noudettu 22.11.2022 osoitteesta https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Ponemon Institute. (2020). *Cost of Insider Threats Global Report.* Haettu 9.12.2022 osoitteesta https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf

Ponemon Institute. (2022). *Cost of Insider Threats Global Report 2022.* Haettu 22.4.2022 osoitteesta https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

Probst, C. W., Hunker, J., Bishop, M. & Gollmann, D. (2008). Summary -- Countering Insider Threats. *Dagstuhl Seminar Proceedings*, *8302*, ss. 1-18. doi:10.4230/DagSemProc.08302.2

Probst, C., & Hunker, J. (2010). The Risk of Risk Analysis And its Relation to the Economics of Insider Threats. Teoksessa T. Moore, D. Pym & C. Ionnidis, *Economics of Information Security and Privacy* (ss. 279-299). Boston: Springer. Noudettu osoitteesta https://doi.org/10.1007/978-1-4419-6967-5_14

Read, D., Alamir, A., Dugdale, S., Stride, N. & Lobo, D. (2021). Introducing the Insider Attack Matrix. G-Research. Haettu 20. marraskuuta 2022 osoitteesta https://www.gresearch.co.uk/blog/article/introducing-the-insider-attack-matrix/

Reidy, P. (2013). Combating the Insider Threat at the FBI: Real World Lessons Learned. *Black Hat USA 2013*. Haettu 20.11.2022 osoitteesta https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf

Ryan, G. W. & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods, 15*(1), 85-109. doi:https://doi.org/10.1177/1525822X02239569

Sanastokeskus TSK ry. (2018). Kyberturvallisuuden sanasto. Huoltovarmuuskeskus. Haettu 18. marraskuuta 2022 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Strom, B. (2018, 3. toukokuuta). ATT&CK 101. Haettu 20.11.2022 osoitteesta https://medium.com/mitre-attack/att-ck-101-17074d3bc62

Suojelupoliisi. (2019). *Suojelupoliisin vuosikirja 2019.* Haettu 21.11.2022 osoitteesta https://supo.fi/documents/38197657/40760236/SUPO_Vuosikirja_2019_FI_saavutettava.pdf/1955990c-85f9-57bc-1f54-6c578779add0/SUPO_Vuosikirja_2019_FI_saavutettava.pdf?t=1603804256355

Trzeciak, R. (2011, 15. elokuuta). The CERT Insider Threat Database. Haettu 12. 11.2022 osoitteesta https://insights.sei.cmu.edu/blog/the-cert-insider-threat-database/

Trzeciak, R. & Costa, D. (2018). A Framework to Effectively Develop Insider Threat Controls. *RSA Conference 2018*. San Francisco, California, USA. Haettu 21.11.2022 osoitteesta https://www.rsaconference.com/Library/presentation/USA/2018/a-framework-to-effectively-develop-insider-threat-controls

US Air Force. (2021, 12. marraskuuta). Air Force Doctrine Publication 3-60 Targeting. Haettu 21.11.2022 osoitteesta https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

Vuori, J. (ei pvm). *Laadullinen sisällönanalyysi*. (Tampere: Yhteiskuntatieteellinen tietoarkisto) Haettu 9.4.2023 osoitteesta Laadullisen tutkimuksen verkkokäsikirja: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/

Willison, R. & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133-137. doi:10.1145/1562164.1562198

LIITE 1 TAPAUSKUVAUSTEN KOODAUS JA MUISTIINPANOT

Tapaus-numero	Hyökkäysvaiheet	Työmuistiinpanot
4	15,16,19,20	Tekijät latasivat omille koneilleen teknisiä tuotekuvauksia, liikesalaisuuksia. Keräsivät yhdessä tietoa riittävästi, että voivat tehdä itse tuotteita kilpailevassa yrityksessä.
5	4,7,17,19,20	Tekijät loivat väärillä tiedoilla veronpalautushakemuksia ja keräsivät itse rahat. Hakemukset tehtiin tiettyjen rahallisten rajojen alla, että hyväksyntä ei vaadi esimiehen toimia. Tekijä onnistui uuden järjestelmän suunnitteluvaiheessa vaikuttamaan järjestelmäsuunnitteluun siten, että petosten tekeminen oli mahdollista
7	2,7,12,15,16,19,22	Tekijä suostui luovuttamaan vieraan valtion tiedustelupalvelua esittävälle poliisille tietoja. Latasi piirustuksia järjestelmistä ja luovutti niitä. Kehitti tarkan suunnitelman, johon kuului ohjelmistokomponentti, jolla voitiin kiertää organisaation turvatoimia, joka mahdollistaa tietojen lataamisen ilman että turvallisuuskomponentit havaitsevat sitä. Pyysi agenttia hankkimaan itselleen pienen kameran, jolla hän voisi kuvata laivastotukikohdassa. Henkilöllä kaksi kansalaisuutta, alkuperäisen kotimaan lähetystö oli aiemmin perunut tekijän kansalaisuuden, että soluttautuminen onnistuisi helpommin.
8	7,10,15,16,19,20,22	Toimitti ystävälleen tietoja, joiden perusteella ystävä osasi vältellä rikostutkintaa, joka kohdistui häneen. Etsi tietoa järjestelmistä vuosien ajan, useissa eri tutkinnoissa. Yritti piilotella jälkiään, kehotti ystäväänsä poistamaan sähköposteja ja vaihtamaan osoitetta jne. Neuvoi ystävää petosten tekemisessä ja kiinnijäämisen välttelyssä. Sai vaihdossa rahaa ja mm. matkoja, prostituoituja, viinaa, ilmaisia klubi-iltoja.
9	15,16,19,22	Tapasi ulkomaalaisen naisen konferenssissa, jonka kanssa tekijällä kehittyi romanttinen suhde. Jakoi tietoa naiselle useita kertoja. Vei kotiinsa turvaluokiteltuja asiakirjoja. Lähetti tietoja myös sähköpostilla.
10	15,16,19,22	Sai selville vaikutusoperaatiosta liittolaismaahan, josta suuttui. Myi tuhansia asiakirjoja vieraalle valtiolle. Käytti ystäväänsä apuna tiedon toimittamiseen.
11	4,15,16,19,22	Taloudellinen intressi vieraan valtion yritykseen. Yritys pyysi tietoa tekijältä. Tekijä luovutti tietoa vieraalla valtiolle kolmannen valtion alueella. Valehteli taustaselvityksissä ja matkoihin liittyvissä haastatteluissa. Yritti rekrytoida toisenkin työntekijän mukaan. Tutkinnassa löytyi mm. rekisteröimättömiä aseita, USB-muistivälineitä, joissa varastettuja tiedostoja.
12	15,16,19,20,22	Valtion työntekijä, useita ulkomaan tehtäviä. Sai lahjuksia vieraiden valtioiden edustajilta (rahaa, matkoja, lomia, opintoja, asunto ym.). Ei raportoinut kontaktia

		vieraan valtion edustajiin. Peitteli ulkomaanmatkoja ja kontakteja. Jakoi vieraalle valtiolle asiakirjoja. Suoritti ostoksia ja matkusteli enemmän kuin mitä tunnetuilla tulonlähteillä pitäisi olla mahdollista.
13	17,19	IT-ylläpitäjä, sai potkut. Otti luvattoman etäyhteyden omalla tietokoneellaan firman ympäristöön eri tunnuksilla. Poisti käyttäjätunnuksia ja tiedostoja mikä aiheutti häiriötä yrityksen toiminnalle.
14	4,15,16,19,20,22	Työntekijä vietti sapattivuoden ja palasi töihin eri rooliin. Palattuaan latasi yrityssalaisuuksia firman verkosta. Manipuloi IT-ylläpidon antamaan itselleen laajemmat pääsyoikeudet järjestelmiin ladatakseen lisää tietoja. Toimitti varastettua dataa kilpailijalle ja tallensi sitä kolmannen osapuolen järjestelmiin. Irtisanoutui sisäisen tutkinnan alkaessa. Perusti uuden yrityksen toisen samassa firmassa työskennelleen tekijän kanssa hyödyntäen varastettua tietoa. Toinen tekijä jäi kiinni kannettavan tietokoneen kanssa, jossa löytyi varastettuja tietoja. Tutkinnassa selvisi, että varastettuja tietoja oli myös lähetetty sähköpostilla ja tallennettu pilvipalveluihin.
17	3,4,15,16,19,22	Valtion työntekijä. Lähetty kohdistetun kalasteluviestin saman organisaation työntekijöiden osoitteisiin. Kalasteluviestissä haittakoodia. Tarkoituksena oli vahingoittaa järjestelmiä ja varastaa tietoa. Jäi kiinni asioidessaan peitetehtävissä toimivan poliisin kanssa ja lähetettyään poliisin luoman toimimattoman viruksen kohteille. Oli aiemmin kerännyt listoja työntekijöistä, joita tarjosi rahaa vastaan vieraille valtioille.
19	10,15,16,19,22	Paljasti turvallisuusluokiteltua tietoa ulkopuolisille toimittajille. Romanttinen suhde erääseen toimittajaan, joka julkaisi tekijän vuotamien tietojen perusteella artikkeleita. Keräsi tietoa, joka ei kuulunut omiin työtehtäviin. Vuoti tietoa tekstiviestien, sosiaalisen median suoraviestien ja puhelinkeskusteluiden kautta toimittajille. Otti vastaan tietopyyntöjä ja haki tietoja toimittajien pyyntöjen mukaisesti järjestelmistä.
20	7,17,19	IT-ylläpitäjä. Pyysi huoltoikkunan siirtoa, johon ei suostuttu. Suoritti huoltokatkon väärään aikaan ilman lupaa. Sai puhuttelun, jatkoi väärään aikaan tehtyä huoltokatkoa silti. Haukkui kollegansa puhelimessa ja kiukutteli työpaikalla saatuaan pakkoloman. Pakkoloman aikana sai potkut. Vaihtoi verkkolaitteiden ylläpitotunnusten salasanat ja yritti piilottaa pahat tekonsa ylikirjoittamalla työkannettavansa potkut saatuaan.
21	7,16,19,20,22	Keräsi turvallisuusluokiteltuja asiakirjoja töistä ja lähetti toimittajalle. Pyrki välttämään tutkintaa käyttämällä mm. Tor-verkkoa ja tulostamalla ja ylikirjoittamalla tiedostoja. Toimittajien paljastettua tiedot yleisölle, tekijä puhui aiheeseen liittyvissä tapahtumissa.

27	15,16,19,22	Työntekijä, joka koki, ettei etene urallaan ja kärsi taloudellisista ongelmista. Pyrki myymään ulkomaille ohjelmistoteknologiaa ja tietoa. Jäi kiinni yrittäessään myydä tietoa peiteoperaatiossa toimivan viranomaisen kanssa, jonka luuli olevan vieraan valtion tiedustelu-upseeri. Toimitti tiedot USB-muistilla.
28	15,16,19	Pyrki loikkaamaan vieraaseen valtioon ja paljastamaan turvallisuusluokiteltua tietoa toimittajille. Keräsi tietoja ja valmistautui kuljettamaan sitä toimittajalle.
30	7,15,16,19,22	Yritti viedä vieraaseen valtioon työnantajaltaan varastettua sotilasjärjestelmiin liittyvää tietoa. Lähetti tietoa mm. sähköpostilla. Mainosti omaa sensitiivistä osaamistaan vieraalle valtiolle työnhaussa. Yritti lähettää ulkomaille kontillisen salaista materiaalia, sisältäen dataa, asiakirjoja ja piirustuksia. Sähköisessä viestinnässä kannusti vastapuolta hävittämään todisteita.
31	17,19	Sai potkut, palasi kotimaahansa. Hakkeroi työnantajansa järjestelmiä ja teki vahinkoja. Kuvauksessa epäselvää, mitä tarkoitetaan "hakkeroinnilla" tässä tapauksessa. Onko varsinaisesti sisäpiiriläinen, jos kyseessä on entinen työntekijä, ja ei käyttänyt sisäpiiriläisellä olevaa tietoa? Toki kostonhimo perustui entiseen työsuhteeseen, mutta hyökkäys on kuin ulkopuolisen tekemä, varmasti kuitenkin kohteen valinta perustui aiempaan työsuhteeseen.
33	15,16,19,22	Luovutti turvallisuusluokiteltua tietoa ulkopuoliselle taholle (bloggaaja/toimittaja). Keräsi tiedostot muutamien kuukausien aikana.
34	15,16,19,20,22	Latasi tuotekehitystietoa työnantajan tietokannasta työkoneelleen ja siirsi tiedot henkilökohtaiselle tietokoneelleen USB-mediaa ja sähköpostia hyödyntäen. Käytti tietoja omistamassaan yrityksessä ulkomailla ja pyrki myymään niitä eteenpäin, jonka kohdeorganisaatio lopulta huomasi.
35	16,19,20,22	Kilpaileva yritys ex-työntekijän, joka toi mukanaan yritys-salaisuuksia (ml. valokuvia, prosessikuvauksia). Kilpaileva yritys pyrki myymään tietoja eteenpäin ulkomaille. Tietoja pyrittiin peittelemään tutkinnan vaikeuttamiseksi.
37	15,16,19,20,22	Luovutti turvallisuusluokiteltua tietoa vieraan valtion käsiin. Ei kertonut kontakteista vieraan valtion virkamiehiin, väärensi dokumentteja ulkomaanmatkoista ja kehitti vieraan valtion kansalaisiin suhteita (ml. prostituoidut) yms.
38	3,13,15,16,19	Väärinkäytti ylläpitotunnuksiaan ja otti haltuunsa muiden työntekijöiden tunnuksia ja salasanoja asentamalla keylogger- ohjelmistoja, joilla luki muiden salasanoja. Käytti tunnuksia päästäkseen käsiinsä henkilökohtaisiin tietoihin (mm. valokuvat, sosiaalinen media). Kirjautui luvattomasti muiden tunnuksilla useita kertoja ja etsi

		erityisesti naishenkilöiden sensitiivisiä kuvia. Keräsi tietoja omassa käytössä olevalle työasemalleen.
39	4,15,16,19,20,22	Pyrki varastamaan yrityssalaisuuksia (dataa, asiakirjoja, prosessiteknologiaa ym.) ja toimittamaan niitä vieraaseen valtioon. Teki yhteistyötä ainakin neljän muun henkilön kanssa, jotka olivat työntekijöitä ja ex-työntekijöitä yrityksessä. Matkusteli ulkomaille myymään tietoa. Lahjoi muita työntekijöitä antamaan itselleen tietoa.
41	15,16,19,22	Pyrki myymään turvallisuusluokiteltua tietoa vieraalle valtiolle, jäi kiinni peiteoperaatiossa olevalle poliisille. Paljasti järjestelmiä, joihin hänellä oli pääsyjä ja keräsi pyydettyjä tietoja ulkopuoliselle. Motiivina raha, kärsi taloudellisista ongelmista mm. peliongelmien takia.
42	15,16,19	Keräsi kotiinsa terabittejä turvallisuusluokiteltua tietoa vuosikymmenien ajalta, ei merkkejä tiedon luovuttamisesta eteenpäin.
43	15,16,19,22	Turvallisuusluokiteltua tietoa vuodettiin organisaatiolle, jonka yksi tekijöistä oli perustanut. Motiivina seliteltiin, että tiedustelutieto on liian rajatun joukon saatavilla, minkä takia henkilöt päättivät siirtää tietoa toisen organisaation ulottuville.
44	15,16,19,20,22	Jakoi vieraalle valtiolle salaista tutkimustietoa lahjuksia vastaan. Lahjuksiin kuului mm. vierailevan professorin titteli, rahaa, toimisto ja asunto. Antoi vieraan valtion edustajille pääsyjä tiloihin, joihin ei pitäisi päästä. Peitteli jälkiään vuosia.
46	7,15,16,19,20,22	Toimitti työpaikalta keräämiään turvallisuusluokiteltuja tietoja vieraan valtion agenteille rahaa vastaan. Matkusti ulkomaille viemään ko. asiakirjoja. Keräsi pyydettyjä tietoja organisaation ympäristöstä, siirsi niitä ulkoiselle medialle, matkusti ulkomaille ja luovutti ne vieraan valtion agentille. Maksut tehtiin käyttäen lähisukulaisen tiliä, käytössä oli myös nk. "burner"-puhelin ja muita viestintävälineitä. Teki keräämistä ja varastamista toistuvasti, ja matkusti toistuvasti luovuttamaan tietoja.
47	13,15,16,19,20,22	Murtautui teknisesti edellisen työnantajansa tiedostopalvelimelle varastaakseen tietoja. Tiedot sisälsivät yrityssalaisuuksia. Jäi kiinni sen jälkeen, kun oli lähettänyt lähes identtisen tarjouksen potentiaaliselle asiakkaalle, kuin millaisia kohdeyritys oli käyttänyt. Tekninen murto tehtiin ottamalla haltuun työntekijän sähköpostitunnus, jonka kautta tiedot ladattiin. Kohdeyrityksellä oli käytössä dokumenttijaoissa jonkinlainen "kiertävä tunnus" (rotating account credential), johon tekijä myös pääsi käsiksi sähköpostitunnuksen kautta.
49	15,16,19,20,22	Suostui luovuttamaan peitetehtävissä olevalle poliisille turvallisuusluokiteltua tietoa rahaa vastaan. Luuli että poliisi on vieraan valtion tiedustelupalveluiden edustaja. Poliisi oli aiemmin tutkinnassa havainnut merkkejä, että tekijä oli valmis luovuttamaan tietoja ulkomaille.

		Tekijällä ei ollut enää pääsyä tietoihin, tiedot luovutettiin osittain tekijän omasta muistista. Tekijä oli myös ottanut haltuunsa joitakin turvallisuusluokiteltuja asiakirjoja, joita löydettiin hänen kotoaan. Tiedot toimitettiin 'dead-drop' tyylisesti, mediana salattu USB-muisti.
50	15,16,19	Teki kopioita turvallisuusluokitelluista asiakirjoista (sekä paperilla että sähköisesti). Siirsi tietoja mm. kotikoneelleen, jossa ne vaarantuivat. Ei näyttöä, että olisi myynyt tietoja, selitteli oikeudessa tekojaan mm. etätöiden tekemisellä ylennystä varten ja ansioluettelon päivittämisellä. Teki teot aivan tietoisesti ja tahallaan, useamman vuoden aikana.
52	17,19	Työsuhteen päättymisen jälkeen käytti vanhaa tunnustaan tuhotakseen pilvipalvelussa olevia yrityksen palvelimia.
53	10,15,16,19	Haki työsuhteensa aikana tietoa turvallisuusluokitelluista tietokannoista ja kopioi tietoa henkilökohtaisiin vihkoihin, jotka tekijä vei kotiinsa työpaikaltaan.
54	15,16,19,22	Luovutti vieraalle valtiolle turvallisuusluokiteltua tietoa. Luovutus tehtiin kolmannen osapuolen verkkosivujen salasanasuojatun osion kautta, johon tekijä laittoi tiedot ja vastaanottaja kävi myöhemmin lataamassa ne sieltä.
56	15,16,19	Latasi turvallisuusluokiteltuja tietoja kotikoneelleen ja siirsi sitä ulkoisille medioille. Selvitteli keinoja ylikirjoittaa tietoja sisäisen tutkinnan aikana ja muutteli tai poisti turvallisuusluokittelu-merkintöjä asiakirjoista.
58	13,17,19	IT-ylläpitäjä. Sai haltuunsa muiden käyttäjien tunnuksia työtehtäviensä hoitamista varten. Sai ylennyksen, mutta ei pärjännyt uusissa tehtävissä, palautettiin vanhoihin tehtäviin. Työn laatu heikkeni ja sai potkut, eikä palauttanut firman työkannettavaa. Kirjautui yrityksen järjestelmiin useina päivinä omia ja muiden työntekijöiden tunnuksia hyödyntäen, poisti tiedostoja ja vaihtoi tunnuksien salasanoja.
59	15,16,19,22	Vei organisaation kannettavan tietokoneen ulkomaille ilman lupaa. Työasemassa luokiteltua tietoa, jonka vienti ulkomaille oli kiellettyä. Irtisanoutui ulkomailla ja palattuaan valehteli kannettavan viennistä ulkomaille. Lopulta tunnusti.
60	15,16,19,20	Irtisanoutui ja kertoi kollegalle, että on menossa ulkomaalaiselle kilpailijalle töihin. Yritys teki sisäisen tutkimuksen järjestelmiin tekijän osalta. Tekijä oli ladannut satoja luottamuksellisia asiakirjoja, joihin hänellä ei ollut työhön perustuvaa syytä. Tekijä oli siirtänyt tiedostot ulkoiselle medialle. Tekijä palautti ulkoisen median, jota oli osittain ylikirjoittanut sitä ennen.
61	10,15,16,19,22	Tekijällä oli romanttinen suhde yrityksen ulkopuoliseen henkilöön, joka myöhemmin pyysi turvallisuusluokiteltuja tietoja tekijältä. Tekijä haki tietoja ja luovutti niitä ulkopuoliselle.

62	15,16,19,20,22	Peiteoperaatiossa oleva poliisi esitti vieraan valtion tiedustelupalvelua. Tekijä suostui luovuttamaan turvallisuusluokiteltuja tietoja poliisille. Käytti salattua viestintää ja harjoitti operaatioturvallisuutta toiminnassaan. Tekijä oli kerännyt tietoja jo etukäteen ja vasta työsuhteen päätyttyä pyrki aktiivisesti ottamaan yhteyttä vieraaseen valtioon.
63	15,16,19,22	Menetti rahansa pörssissä ja otti yhteyttä vieraaseen valtioon rahan toivossa. Kuvasi turva-alueita ja teki piirustuksia turvallisuusjärjestelyistä valtion kiinteistössä. Yritti toimittaa tietoja, mutta vieras valtio kieltäytyi ottamasta tietoja vastaan, kun tekijä yritti toimittaa niitä.
64	15,16,19,22	Tekijä oli korkeassa asemassa yrityksessä, joka toimi valtion alihankkijana. Yritys sai haltuunsa vientirajoitettua tietoa. Yritys myytiin ulkomaiselle omistajalle. Yritys luovutti kaupan jälkeen vientirajoitettua tietoa ulkomaille.
65	15,16,19,22	Valtion vastaisen ideologian kannattaja. Asensi työtietokoneelleen luvattoman viestintäsovelluksen ja etsi internetistä tietoa, joka voisi auttaa jälkien peittelyssä. Käytti luvattomia ulkoisia muistivälineitä tiedonkäsittely-ympäristöön ja keräsi turvallisuusluokiteltua tietoa. Luovutti tietoa kolmannelle osapuolelle (uutistoimisto)
66	15,16,19,20,22	Kommunikoi vieraan valtion kanssa, ollessaan töissä kohdeyrityksessä. Haki ulkomaille töihin ja kuvaili hakemuksessa osaamistaan sillä tasolla, että osaamisen oli pakko perustua yrityssalaisuuksien käyttöön. Haki internetistä tietoa yrityssalaisuuksien luvattomaan paljastamiseen rangaistavuuteen liittyen. Irtisanouduttuaan kopioi yrityssalaisuuksia ulkoiselle medialle ja pyrki poistumaan maasta. Lentokentällä ulkoinen media havaittiin poliisien toimesta. Pidätettiin myöhemmin palattuaan lähtömaahan.
67	15,16,19,20,22	Varasti työpaikaltaan yrityssalaisuudeksi luettavaa lähdekoodia. Yritti myydä tietoa peiteoperaatiossa oleville poliiseille, jotka esittivät ulkomaalaisen kilpailevan yrityksen edustajia. Esitteli myös kyvyn peitellä lähdekoodia siten, että se ei ole enää tunnistettavissa alkuperäisen yrityksen omistamaksi.
68	15,16,19,22	Varasti työpaikaltaan yrityssalaisuuksia ja pyrki toimittamaan niitä ulkomaille. Oli saanut vastineeksi rahaa, asunnon, työpaikan ym. Pidätettiin ollessaan matkalla ulkomaille, mukanaan mm. ulkoisia muistivälineitä, joissa varastettua dataa, omaisuutta yms.
69	15,16,19,22	Tekijät varastivat työpaikalta yrityssalaisuudeksi laskettavaa tutkimustietoa, jonka pyrkivät toimittamaan ulkomaille. Olivat perustaneet yrityksen ulkomaille ja olivat mukana useammassa vieraan valtion projektissa ulkomailla yrityksen kautta.
71	15,16,19,22	Yrityksen työntekijä varasti liikesalaisuuksia ja vei niitä vieraan valtion edustajille. Tekijä oli todisteiden mukaan

		ollut yhteyksissä vieraaseen valtioon vuosikymmenien ajan.
72	15,16,19,22	Toimitti turvallisuusluokiteltavia tietoja vieraalle valtiolle. Heikosti yksityiskohtia.
73	15,16,19,22	Jakoi ulkopuoliselle turvallisuusluokiteltua tietoa. Oli romanttisessa suhteessa ulkopuolisen kanssa, joka oli vieraan valtion kansalainen. Lähetti tietoja sähköpostilla. Säilytti kotonaan turvallisuusluokiteltuja asiakirjoja ilman lupaa. Asiakirjoja oli noudettu ulkopuolisen henkilön pyyntöjen mukaisesti.
75	15,16,19,20,22	Toimitti rahaa vastaan turvallisuusluokiteltua tietoa vieraan valtion käsiin. Keräsi tietoa työnsä kautta ja säilöi tietoa myös kotonaan. Matkusteli ulkomaille, mahdollisesti viemään ko. tietoja. Suoritti myös rahanpesua peitefirmojen kautta ja kiersi veroja. Käytti rahojaan näkyvästi.
76	7,15,16,19,20,22	Toimitti terroristijärjestöön liittyvälle peiteyritykselle turvallisuusluokiteltua tietoa. Toimitustapoja mm. salasanasuojatut dokumentit, ulkoiset mediat, sähköposti. Käytti viestinnässä kiertoilmaisuja ja pyrki pitämään yllä operaatioturvallisuutta. Todisteina tekijää vastaan käytettiin mm. nauhoitettuja puhelinkeskusteluita.
77	4,15,16,19,20,22	Luovutti turvallisuusluokiteltuja tietoja työpaikaltaan vieraan valtion edustajille. Vieraan valtion tiedustelupalvelu rekrytoi tekijän ja tekijä toimitti tietoa rahaa vastaan. Osa tiedoista kerättiin vieraan valtion pyynnöstä, mutta tekijällä oli myös aktiivinen rooli tiedon tarjoajana. Yritti rekrytoida toisenkin työntekijän ja neuvoi miten tietoja voi lähettää jäämättä kiinni. Toinen työntekijä ilmiantoi tekijän.
78	15,16,19,20,22	Luovutti turvallisuusluokiteltuja tietoja työpaikaltaan vuosikymmenien ajan vieraalle valtiolle rahaa vastaan. Käytti mm. salattua viestintää, peitenimeä, "dead drop"-toimituksia ja muita tekniikoita toiminnan peittelemiseen. Lopulta organisaation sisäinen tutkinta otti tekijän tarkempaan monitorointiin ja seurantaan, jonka perusteella saatiin kerättyä riittävät todisteet pidättämistä varten. Seuranta mm. paljasti "dead dropin" ja muuta epäilyttävää käytöstä.
79	7,15,16,19,22	Peiteoperaatiossa oleva poliisi kontaktoi tekijää esittäen vieraan valtion edustajaa. Tekijä suostui luovuttamaan turvallisuusluokiteltuja tietoja rahaa vastaan. Tietojen luovutus tehtiin fyysisesti ”dead drop”-menetelmällä, mediana salattu muistitikku.
80	19	Tekijänä vieraan valtion kansalainen, joka pyrki rekrytoimaan kohdeorganisaation työntekijän. Työntekijän oli tarkoitus toimittaa haittaohjelma organisaation tietoverkkoon. Haittaohjelman avulla oli tarkoitus varastaa organisaation tietoa. Työntekijä kuitenkin ilmiantoi

		tekijän. Koodattuna tapaus pysähtyy rekrytointiin, joka epäonnistui, loppuja vaiheita ei tapahtunut.
81	19,20	Luovutti turvallisuusluokiteltua tietoa vieraan valtion edustajille rahaa vastaan. Rekrytoitiin vieraan valtion tiedustelupalvelun toimesta tekijän muutettua ulkomaille työsuhteen päätyttyä. Tuotti asiakirjoja vieraalle valtiolle, jotka sisälsivät turvallisuusluokiteltua tietoa. Tiedon keräämistä työsuhteen aikana ei siis varsinaisesti tehty, koko suhde vieraan valtion tiedustelun kanssa syntyi vasta työsuhteen jälkeen, eikä ollut merkkejä että tieto olisi varastettu fyysisessä tai sähköisessä muodossa, vaan tietoa tuotettiin tekijän muistista.
82	10,15,16,19	Otti vastaan tehtäviä vieraan valtion edustajilta. Keräsi tietoa ko. tehtävien mukaisesti ja kokosi tietoja luovuttaakseen ne vieraan valtion edustajille.
83	7,15,16,19,20	Luovutti turvallisuusluokiteltuja tietoja vieraan valtion tiedustelupalvelun edustajalle, jonka oli tavannut ulkomailla. Vei paperiset asiakirjat työpaikalta ja skannasi ne ulkopuolella ulkoiselle medialle. Skannauksen tekeminen tallentui valvontakameraan ulkopuolisen yrityksen tiloissa. Silppusi paperiset asiakirjat, mutta ulkoinen media löytyi vielä. Tietoja oli tarkoitus viedä ulkomaille älylaitteen muistissa.
84	15,16,19,20	Tekijät varastivat yrityssalaisuuksia kahdesta eri yrityksestä ja perustivat ulkomailla oman yrityksen, jossa voisivat hyödyntää varastamiaan tietoja.
85	15,16,19	Varasti yrityssalaisuuksia kahdelta eri työnantajaltaan. Irtisanoutumistaan edeltävänä päivänä tekijä latasi tuhansia tiedostoja ja kopioi niitä henkilökohtaiselle kovalevylle. Tekijä käytti yrityssalaisuuksia hyötyäkseen niistä itse rahallisesti. Sisäisen tutkinnan käynnistyttyä yrityksessä, tekijä yritti hävittää ja piilottaa varastamiaan tietoja ja niitä sisältäviä medioita.
86	15,16,19	Varasti työnantajaltaan yrityssalaisuuksia. Salaisuudet sähköisessä muodossa, tuhansia tiedostoja. Tavoitteena luovuttaa tiedot vieraalle valtiolle ja saada vieraasta valtiosta työpaikka.
87	15,16,19,22	Kontaktoi vierasta valtiota ja yritti myydä yrityssalaisuuksia. Poliisin aloittama peiteoperaatio keräsi riittävät todisteet pidätystä varten. Peiteoperaation aikana tekijä keräsi pyydettyjä tietoja ja luovutti niitä.
88	7,15,16,19,20,22	Useita tekijöitä. Yrityssalaisuuksia varastettiin ulkomailla toimivan yrityksen käyttöön, vieras valtio myös mukana toiminnassa. Useampi työntekijä kohdeyrityksessä osallistui. Yksi tekijöistä siirtyi vieraan valtion omistamaan yritykseen ja rekrytoi sen jälkeen muita työntekijöitä kohdeyrityksestä, jotka latasivat yrityssalaisuuksia mukaansa. Salaisuuksia tallennettiin mm. ulkoisille medioille ja pilvipalvelussa olevaan tiedostosäilöön. Tekijät

		yrittivät peitellä jälkiään tuhoamalla ja ylikirjoittamalla todistusaineistoa.
89	15,16,19,20,22	Varastivat työpaikaltaan yrityssalaisuuksia ja perustivat yrityksen, jossa valmistivat kilpailevia tuotteita ulkomailla hyödyntäen varastettua tietoa.
90	15,16,19,20,22	Loikkasi vieraaseen valtioon ja paljasti turvallisuusluokiteltua tietoa. Keräsi ja valmisteli tietoa työsuhteensa aikana loikkausta varten.
91	17,19	Yrityksen ainoa IT-ylläpitäjä. Irtisanoutui yllättäen, jolloin yritys kieltäytyi maksamasta palkkaa viimeiseltä kahdelta päivältä. Tekijä kieltäytyi antamasta yritykselle hallussaan olevia järjestelmien ylläpitotunnuksia, jotka vain hän tiesi. Irtisanoutumisen jälkeen sabotoi yrityksen järjestelmiä.
92	17,19	Tekijä oli mukana kohdeyritykseen verkkolaitteiden asennuksia tekevässä tiimissä, josta hänet poistettiin. Tekijä sai tietoa yrityksestä mukanaolonsa aikana. Tekijä tunkeutui yrityksen vierastiloissa olevan vierastyöaseman kautta verkkolaitteisiin ja poisti tunnuksia yrityksen verkkolaitteista koko valtion laajuudella. Kuvauksessa huonosti yksityiskohtia, miten tekniset toimenpiteet suoritettiin.
93	4,17,19,20	IT-työntekijä loi valetilin organisaation sähköpostiin. Tilasi sähköpostin avulla arvokkaita laitteita kotiosoitteeseensa ja myi niitä internetissä.
94	10,12,15,16,19,20	IT-ylläpitäjä käytti salasanan murto-ohjelmaa, jolla sai haltuunsa satoja salasanoja palvelimelle. Salasanojen avulla sai pääsyn aineistoon, josta keräsi suuren määrän henkilötietoja. Tekijä kerskui teollaan IRC-kanavalla. Tutkinnassa tekijän kotoa löytyi ulkoisia medioita, joihin henkilötietoja oli tallennettu.
95	15,16,19	Yrityksen työntekijät, joiden työsuhde oli äskettäin lopetettu, latasivat vanhoilla tunnuksillaan yrityssalaisuuksia yrityksen palvelimelta. Työntekijät kokivat omistavansa osan yrityssalaisuuksista henkilökohtaisesti. Teot paljastuivat selkeästi lokeista.
97	17,19	Tekijä johti tuotteen lähdekoodin kehittämistä ja laiminlöi vastuitaan dokumentoinnin ja varmuuskopioinnin osalta tarkoituksellisesti, jopa kertoen tämän kollegoilleen. Ennen siirtoa muihin työtehtäviin, tekijä tuhosi kannettavalla tietokoneella olevat tiedot, mukaan lukien ainoan kopion lähdekoodista, jonka jälkeen tekijä irtisanoutui. Lähdekoodin kopio löytyi lopulta salattuna tekijän kotoa.
98	4,15,16,19	Tekijä pyysi yritykseltään lupaa tehdä etätöitä, joka kiellettiin. Tekijä sanoi irtisanoutuvansa ja sai työpaikan kilpailevasta yrityksestä. Ennen viimeistä työpäivää, työntekijä meni työpaikalle normaalien työaikojen ulkopuolella ja suostutteli huoltomiehen päästämään itsensä tiloihin, joihin tekijällä ei ollut luvallista pääsyä. Tekijä

		pyrki varastamaan tietoa tilassa olevalta koneelta, mutta jäi kiinni kesken teon. Viimeisenä päivänään yritti vielä viedä mukanaan CD-levyllä tietoa, mutta jäi kiinni.
99	17,19	Tekijä manipuloi tietokannassa olevia maksutietoja rahallisen hyödyn saamiseksi. Työntekijällä oli rikollista taustaa ja taustaselvitys oli jätetty tekemättä.
100	4,17,19	IT-ylläpitäjä irtisanoutui ja poisti tutkimustietoa organisaation järjestelmistä. Työsuhteen päättymisen jälkeen suostutteli toisen työntekijän päästämään itsensä sisälle yrityksen tiloihin yrityksen toiminnan sabotoimista varten.
101	13,17,19	Tekijä suuttui kollegoiden käytöksestä, eikä yritys puuttunut asiaan valituksista huolimatta. Työpanos heikkeni ja tekijä siirrettiin alempiin työtehtäviin. Lopulta irtisanoutui. Irtisanoutumisen jälkeen yhdisti yrityksen järjestelmiin, käytti toisen työntekijän tunnuksia yhteyden muodostamiseen ja poisti kriittistä tietoa järjestelmistä ja kaatoi lopulta järjestelmän.
102	15,16,17,19,20	Tekijällä oli riitoja yrityksen johdon kanssa. Irtisanoutui, kopioi yrityssalaisuuksia ulkoiselle medialle ja poisti niitä yrityksen järjestelmistä. Tuhosi myös varmuuskopioita ja tarjoutui korjaamaan tuhonsa rahallista korvausta vastaan.
103	17,19	Tekijän työsuhde oli riitautumisen takia keskeytetyssä tilassa. Kulkuoikeuksia ei poistettu ajoissa, ja tekijä tunkeutui yrityksen tiloihin. Tekijä sammutti tiloissa ollessaan yrityksen tietojärjestelmiä.
104	6,11,17,19	Tekijä irtisanoutui ja alkoi lähettelemään uhkaavia sähköpostiviestejä yrityksen työntekijöille. Tekijällä oli edelleen pääsy työnantajan järjestelmiin asiakkaana. Tekijä käytti tietämystään järjestelmästä korottaakseen pääsyoikeuksiaan. Yritys havaitsi tämän ja sulki tunnukset, mutta tekijä oli ehtinyt luomaan uusia tunnuksia, joita käytti järjestelmän manipulointiin ja tietojen poistamiseen
105	15,16,19,20	Tekijä latasi palvelimelta salasanatietokannan, ja ryhtyi ajamaan Internetistä lataamaansa salasanan murtoon käytettävää työkalua tietokantaa vasten. Tekijä kerskaili ylläpitäjälle, että hän tietää ylläpitotunnuksen salasanan.
106	7,17,19	Tekijä muokkasi yrityksen ohjelmistoa saadakseen ohjelmiston käyttäjänä rahallista etua ja voidakseen kiertää ohjelmistoon rakennettuja rajoitteita. Tekijää ei havaittu sisäisessä auditoinnissa, koska työntekijän ja auditoijien esimies oli sama.
107	17,19	Tekijä muokkasi yrityksen käsittelemiä hakemuksia siten, että sai siitä itse rahallista etua. Tekijällä oli liian suuret oikeudet hakemustietokantaan, mikä mahdollisti tiedon manipuloinnin.
108	3,4,12,13,17,19	Tekijä suuttui työnantajalle riittämättömistä bonuksista. Tekijä käytti toisen työntekijän lukitsematonta

		tietokonetta ja muokkasi yrityksen tuotteen ohjelmistokoodia siten, että koodi aiheuttaa häiriön useiden kuukausien päästä. Tekijä irtisanoutui ennen häiriön syntymistä.
109	15,16,17,19	Tekijä luovutti organisaation tietokannasta tietoa ulkopuoliselle maksua vastaan. Tekijä myös myöhemmin muokkasi tietokantaa rahallisen hyödyn motivoimana.
110	3,4,12,17,19	Tekijä suuttui riittämättömistä bonuksista ja manipuloi yrityksen järjestelmää siten, että tiettynä ajanhetkenä poistetaan yrityksen tietoja ja kaadetaan järjestelmiä. Tekijä irtisanoutui ennen ko. ajankohtaa.
111	17,19	Tekijä sai ylennyksen, mutta epähuomiossa tekijälle jäi myös alemman roolin oikeudet järjestelmiin. Tämän seurauksena tekijä saattoi tehdä hakemuksia ja hyväksyä niitä itse saaden rahallista hyötyä.
112	17,19	Tekijä toimi ohjelmistokehittäjänä. Muutettuaan toiselle paikkakunnalle, organisaation oli päätettävä työsuhde tekijään. Tekijä jatkoi organisaation ulkoisena konsulttina töiden tekemistä organisaatiolle. Edut eivät olleet samat, mikä suututti tekijän. Tekijä poisti kehittämänsä sovelluksen ja muitakin kehitettäviä sovelluksia etäyhteyden yli, muokkasi lokeja peittääkseen jälkiään ja vaihtoi ylläpitotunnuksien salasanoja. Tekojen jälkeen hän irtisanoutui.
113	2,12,17,19	Tekijä toimi pitkään IT-ylläpitäjänä yrityksessä. Yritys laajentui ja tekijä harmistui pienemmästä merkityksestään yritykselle ja alkoi sabotoimaan projekteja. Tekijä valmisteli ajastetun skriptin, joka tuhosi yrityksen tietoja.
114	7,17,19	Tekijä muokkasi yrityksen valvontajärjestelmää siten, että se ei enää lähettänyt hälytyksiä. Muokkauksen jälkeen tekijä varasti yritykseltä myös rahaa.
115	2,3,12,15,167,19,22	Tekijä asensi toisen työntekijän tietokoneelle keylogger-ohjelmiston, jolla keräsi luottamuksellista tietoa. Tiedot tekijä lähetti lakimiehille, jotka keräsivät todisteita yritystä vastaan.
116	2,3,5,12,15,16,19,22	Tekijät juonivat ulkopuolisen henkilön kanssa varastaakseen yrityssalaisuuksien tekijöiden työnantajalta. Ulkopuolinen lähetti haittaohjelmalla varustetun sähköpostiviestin, jonka tekijä avasi. Haittaohjelma asensi keylogger-ohjelmiston, jonka avulla tekijät lähettivät tietoa ulos ympäristöstä kilpailevalle yritykselle.
117	7,15,16,19,22	Työnantaja tarjosi tekijälle töitä ulkomailla, josta tekijä kieltäytyi ja haki töihin kilpailijalle. Tekijä latasi yrityssalaisuuksia alkuperäisen työnantajansa järjestelmistä kuukausien ajan, kunnes irtisanoutui. Valtavat latausmäärät havaittiin vasta jälkikäteen. Alkuperäinen yritys ilmoitti kilpailijalle, joka palautti tiedot. Tietoja löytyi myös paperimuodossa tekijän kotoa. Tekijä yritti peitellä jälkiään silppuamalla dokumentteja ja hävittämällä ulkoisia medioita.

118	3,12,15,16,19	Tekijä oli toiminut yritykselle konsulttina. Tekijä ajoi useita kertoja yrityksen verkossa salasanan murtamiseen käytettäviä ohjelmistoja. Myöhemmin tekijä asensi kehittyneemmän salasanojen murtamiseen käytetyn sovelluksen yrityksen järjestelmiin. Ohjelman avulla tekijä siirsi käyttäjien salasanoja yrityksen ulkopuoliseen tietokoneeseen. Yritys havaitsi myöhemmin, että tekijällä oli edelleen tunnuksia järjestelmässä ja tutkinta aloitettiin.
119	4,17,19	Tekijä suostutteli esimiehensä antamaan itselleen korotetut käyttöoikeudet yrityksen järjestelmiin. Tekijä sai korotetuilla oikeuksilla manipuloitua järjestelmää siten, että pystyi tekemään tilauksia ja hyväksymään niitä. Tekijä sai tällä rahallista hyötyä.
120	17,19	Tekijä irtisanoutui ja aiheutti jälkikäteen ikävyyksiä yritykselle manipuloiden yrityksen järjestelmiä. Tapauskuvauksessa jää epäselväksi, miten tekijä onnistui tuottamaan yritykselle ikävyyksiä.
121	6,13,15,16,19	Tekijän pääsyjä rajattiin työnantajan järjestelmiin ja hän irtisanoutui. Tekijä asensi takaoven itselleen ja käytti sitä lähdekoodin ja salasanatiedostojen lataamiseen. Teko havaittiin suurien latausmäärien takia.
122	17,19	Tekijän työsuhde katkaistiin. Seuraavana päivänä hän hyödynsi etäyhteyttä, jota ei ollut suljettu ja tuhosi yritykselle tärkeitä tiedostoja.
123	17,19	Tekijä sai potkut, mutta onnistui vielä kirjautumaan etänä yrityksen järjestelmiin. Tekijä sammutti yrityksen tärkeimmän palvelimen, mikä aiheutti vahinkoja.
124	13,17,19	Tekijä oli päättänyt työsuhteensa yritykseen, mutta meni töihin tytäryhtiöön. Tytäryhtiön tietoverkon kautta tekijä oli saanut pääsyn useisiin yrityksen järjestelmiin. Teko havaittiin, kun tekijä kirjautui yrityksen ylläpitäjän tunnuksilla ja käytti niitä toisen työntekijän sähköpostin lukemiseen. Tekijä peitteli jälkiään teknisesti poistamalla historiatietoja. Tekijä oli poistanut joitakin ohjelmistoprojektin muutoksia. Kuvauksesta jää epäselväksi, miten tekijä sai haltuunsa ylläpitäjän ja muiden tunnuksia.
125	17,19	Tekijä tunkeutui urakoitsijan kulkulätkällä yrityksen tiloihin, joissa hallittiin ympäristön tietoverkkoja. Kohteen turvajärjestelyt perustuivat täysin fyysiseen suojaukseen. Tekijä kaatoi järjestelmät ja varasti paikalliset sekä off-site varmuuskopiot käyttäen samaa kulkulätkää.
126	17,19	Tekijä oli saanut potkut organisaatiomuutoksen seurauksena. Tekijä käytti jaettua tunnusta ja poisti yrityksen järjestelmistä ohjelmistoja.
127	4,17,19	Tekijä muokkasi yrityksen tietokantoja siten, että sai rahallista hyötyä. Tekijä tuhosi lokitietoja sisäisen tutkinnan alettua ja pyysi alaistaan poistamaan varmuuskopioita. Tekijä myös pyysi toista alaistaan tuomaan itselleen varmuuskopioita, joita ei löydetty tutkinnassa.

128	15,16,19,20,22	Tekijä latasi yrityssalaisuuksia USB-muistille ja säilöi sitä kotonaan. Tekijä luovutti tietoja yrityksen toiminnasta toimittajille irtisanoutumisen jälkeen.

LIITE 2 SISÄLLÖNANALYYSIN KOODIT JA YHTEENVETO

Hyökkäysvaihe	Numero	Alkuperäinen termi	Määritelmä	Käyttökerrat analyysissä
Tiedustelu	1	Reconnaissance	Ympäristön tutkiminen ulkopuolelta	0
Resurssien kehittäminen	2	Resource development	Valmistelevat toimenpiteet hyökkäystä varten, mm. infrastruktuurin valmistelu, haittaohjelmakoodin luominen	4
Toimittaminen	3	Delivery	Kohteen (esim. haittakoodi) toimittaminen ympäristöön	5
Sosiaalinen manipulointi	4	Social Engineering	Henkilöiden manipulointi hyökkääjän tarkoitusperien mukaisesti	11
Hyväksikäyttö	5	Exploitation	Toimitetun kohteen ajaminen ympäristössä, haavoittuvuuksien hyväksikäyttö	1
Jalansijan säilyttäminen	6	Persistence	Toimintaa, jolla hyökkääjä pyrkii säilyttämään jalansijansa ympäristössä	2
Turvatoimien välttely	7	Defense Evasion	Hyökkääjän toimet, joilla pyritään välttämään kiinnijäämistä	10
Komento ja hallinta	8	Command and Control	Komento- ja hallintakanavan luominen ja käyttö	0
Kauttatunnelointi	9	Pivoting	Liikenteen tunnelointi jonkin kohteen kautta siten, että hyökkääjä saavuttaa muutoin tavoittamattomissa olevia järjestelmiä	0
Kohteiden etsiminen	10	Discovery	Hyökkääjälle kiinnostavien kohteiden etsiminen ympäristöstä	5
Käyttöoikeuksien korottaminen	11	Privilege Escalation	Käyttöoikeuksien laajentaminen siten, että hyökkääjä saa tavallista korkeammat oikeudet järjestelmään	1
Suorittaminen	12	Execution	Hyökkääjän hallitseman ohjelman tai koodin ajaminen järjestelmässä	7
Pääsytietojen haltuunotto	13	Credential Access	Tunnusten haltuunotto ja käyttö hyökkääjän toimesta	6
Tunkeutumisen laajentaminen	14	Lateral Movement	Jalansijan laajentaminen ympäristössä muihin järjestelmiin tunkeutumalla	0
Tiedon kerääminen	15	Collection	Hyökkääjälle kiinnostavan tiedon kerääminen ja kokoaminen ympäristöstä	69
Tiedon varastaminen	16	Exfiltration	Tiedon siirtäminen hyökkääjän haltuun esimerkiksi verkkoyhteyttä tai fyysistä mediaa hyödyntäen	71
Vaikutukset	17	Impact	Toimenpiteet, joilla hyökkääjä manipuloi, häiritsee tai tuhoaa kohdejärjestelmää tai siinä olevaa tietoa	33
Päämäärät	18	Objectives	Hyökkäyksen sosiotekniset tavoitteet	0
Rekrytointi tai käännekohta	19	Recruitment / Tipping point	Sisäpiiriläinen motivoituu tekemään haitallisia toimenpiteitä.	104
Jälkiseuraukset	20	Aftermath	Hyökkääjän käytöksessä havaittavat muutokset hyökkäyksen onnistumisen jälkeen	32
Alustava jalansija	21	Initial Access	Hyökkääjä muodostaa alustavan jalansijan ympäristöön	0
Tiedon toimittaminen	22		Hyökkääjä toimittaa varastetun tiedon kolmannelle osapuolelle	47