Organisaation tieto- ja kyber-havainnointikyvykkyys

Turvallisuusjohdon koulutusohjelma

Kehitysprojektin raportti

Mika Leino

Insta DefSec Oy

Tampere 25.7.2020

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Havainnointi on tärkeä osa tieto- ja kyberturvallisuutta, koska se mahdollistaa oikea-aikaisen hyökkäyksiin reagoinnin. Turvallisuutta kehitettäessä olisi tarpeen voida mitata tämän hetkinen kyky havaita hyökkäyksiä tai niiden yrityksiä. Havainnointikyvyn mittaaminen on kuitenkin hyvin vaikeaa, koska kaikkia hyökkäyskeinoja ei tunneta, eikä ole varmuutta valvontakoneiston hyvyydestä.

Tässä työssä tutustutaan tieto- ja kyberturvallisuuden uhkiin, hyökkäyksiin ja havainnointikeinoihin sekä havainnointikykyä ja -kyvykkyyttä käsitteleviin viitekehyksiin. Työssä ei rajauduta pelkästään perinteisiin verkko- ja päätelaiteturvallisuuden osa-alueisiin, vaan tarkasteluun on otettu myös laitteisto-, henkilö- ja tilaturvallisuusnäkökulmat.

Julkisesti saatavilla olevia valmiita ratkaisuja havainnointikyvyn ja -kyvykkyyksien mittaamiseen ja arviointiin on niukalti ja menetelmissä on puutteita. Tässä työssä esitellään lähestymistapa, jolla havainnointikyvykkyyden mittaaminen olisi mahdollista toteuttaa.

Abstract

Detection is a crucial part of the cybersecurity, because it enables timely response to attacks. When developing security, it would be necessary to be able to measure current ability to detect attacks or their attempts. However, measuring the ability to detect is very difficult because all attack techniques and the quality of the monitoring mechanisms are not known.

This paper explores cybersecurity threats, attacks, and detection means, as well as frameworks for detection performance and capability. The work is not limited to the traditional aspects of network and terminal security, but also includes hardware, human and physical security aspects.

There are few publicly available ready-made methods for measuring and evaluating detection performance and capability and there are shortcomings in these methods. This paper presents an approach that would make it possible build detection capability metrics for an organisation.

Sisältö

1 Johdanto

Turvallisuutta luodaan estämällä uhkia toteutumasta ja jos niitä toteutuu, ne pyritään torjumaan siten, että vaurioiden suuruus minimoituu. Turvallisuuteen liittyvät myös ennakointi ja havaitseminen. Koska uhkilla on taipumus toisinaan toteutua, ennakoinnilla huolehditaan siitä, että niihin kyetään reagoimaan oikein. Uhkan havaitsemista tarvitaan torjuntatoimien käynnistämiseksi oikea-aikaisesti.

Havainnointi on keskeinen osa kybertilannekeskusten, turvallisuusoperaatiokeskusten ja hälytysvalvomoiden toimintaa ja organisaatioiden kybertilannetietoisuutta ja turvallisuushäiriöiden hallintaa. Turvallisuushäiriöitä voidaan havaita ja käsitellä hyvinkin määrämuotoisin ja tehokkain menetelmin, mutta taustalla jäytää silti ajatus, oliko tässä kaikki vai jäikö jotain huomaamatta? Onko meillä tällä hetkellä sellaiset laitteet ja järjestelmät, joilla uhkat havaitaan? Mikä on varmuus, että uhka havaitaan? Pitäisikö investoida havaitsemisen kehittämiseen? Miten investoinnit kohdistetaan? Nämä ovat muutamia kysymyksiä, joita voi herätä, kun esimerkiksi katsotaan organisaation haittaohjelmahavaintojen määriä tilannekatsauspalavereissa.

Havainnointikyky kertoo siitä, miten hyvin havaitsemisessa onnistutaan. Samalla se kertoo riskitasosta, joka liittyy uhkien havaitsemiseen. Riskitason tuntemalla voidaan tehdä päätöksiä riskin pienentämiseksi tai hyväksymiseksi. Havainnointikyky vaati kyvykkyyksiä ja riskien pienentäminen vaatii kyvykkyyksien kehittämistä.

Tässä työssä havainnoinnilla tarkoitetaan organisaation omaisuuteen liittyvien uhkien havainnointia. Otsikon mukaisesti työ käsittelee etupäässä tietotekniikkaan liittyvää turvallisuustapahtumien havainnointia, mutta käsittelee lisäksi henkilö- ja tilaturvallisuutta, jotka liittyvät vahvasti tieto- ja kyberomaisuuden turvaamiseen.

Työ tavoitteena on edistää kokonaisvaltaisen havainnointikyvykkyyden kehittämistä tunnistamalla havainnointikyvykkyyden elementtejä ja esittelemällä keinoja havainnointikyvykkyyden tason mittaamiseksi.

Tämän työn ensisijaisena tavoitteena on kuvata keinoja, miten organisaation havainnointikyvyn ja -kyvykkyyden taso voidaan määrittää. Aiheen taustoittamiseksi tutustutaan tarkemmin havainnoitaviin asioihin eli uhkiin ja hyökkäyksiin (luku 2), havainnointikyvykkyyden edellytyksiin, menetelmiin ja välineisiin (luku 3) sekä tietoturvan mittaamiseen (luku 4). Taustoituksen jälkeen kuvataan havainnointikyvykkyyden mittaamiseen liittyvää problematiikkaa ja olemassa olevia viitekehyksiä havainnoinnin tason arviointiin ja mittaamiseen sekä rakennetaan malli, jonka mukaan organisaatio voi luoda itselleen kyvyn arvioida omaa havainnointikykyään ja kyvykkyyttään.

2 Uhkat

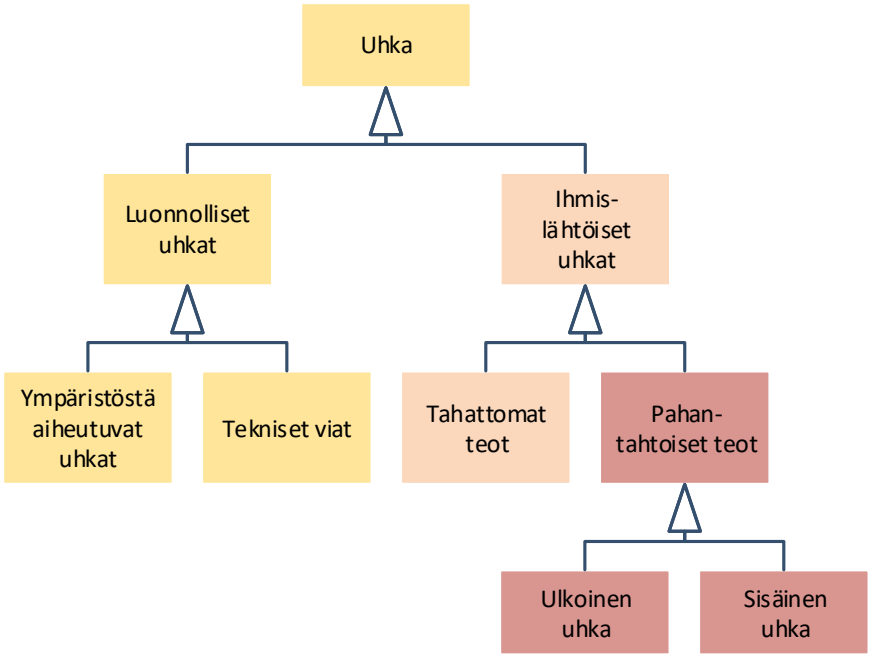
Uhkat ovat suojattavaan omaisuuteen negatiivisesti vaikuttavia tekijöitä. Mitä aikaisemmin uhka havaitaan, sitä paremmin siihen voidaan vastata ja sitä pienemmät ovat negatiiviset vaikutukset.

Tässä luvussa käydään läpi mitä uhkat ovat ja miten uhkat toteutuvat. Lisäksi pohditaan myös mitä hyökkääjät tavoittelevat ja miltä pahantahtoisilta toimilta organisaatiot haluavat suojautua.

2.1 Uhkan määritelmä

Tieto- ja kyberturvallisuudessa uhkalla tarkoitetaan eri asioita riippuen viitekehyksestä. Uhkaa voidaan pitää riskin kaltaisena mahdollisena tapahtumana tai skenaariona, joka aiheuttaa negatiivisia seurauksia (ISO/IEC 27032 2012). Toisissa yhteyksissä uhkalla tarkoitetaan jonkinlaista negatiivisia tapahtumia aiheuttavaa olosuhdetta, lähdettä tai tekijää. Voidaan esimerkiksi sanoa, että avoimet langattomat verkot, salakuuntelu tai lennokit ovat uhkia (BSI 2013; ETSI GS ISI 001-2 2015). Uhkalla voidaan tarkoittaa myös pahantahtoista toimijaa, henkilöä tai ryhmittymää, esimerkiksi aktivistiryhmää tai valtiollista toimijaa (Garcia 2008; Duggan et al. 2007).

Kuva 1 esittää julkaisun (ETSI GS ISI 001-2 2015) mukaista uhkien luokittelua, jossa uhkat jaetaan sen mukaan miten ne aiheutuvat. Pääjako tapahtuu ihmislähtöisiin ja ei-ihmislähtöisiin uhkiin. Ihmislähtöiset uhkat jaetaan edelleen tahattomiin ja pahantahtoisiin uhkiin. Malli tuo esille myös jaon sisältä tuleviin ja ulkoisiin uhkiin.



Kuva 1 Uhkien luokittelu

Vaikka tässä työssä keskitytään erityisesti pahantahtoisten tekojen havaitsemiseen, yleisesti ottaen *uhkalla* tarkoitetaan negatiivisen vaikutuksen aiheuttavaa tekijää riippumatta siitä, onko taustalla luonnollisia tapahtumia vai erilaisin tarkoitusperin varustettuja henkilöitä. Jos uhkan tekijä on pahantahtoinen taho, henkilö tai ryhmittymä, käytetään tekijästä nimitystä *uhkatoimija*, *toimija* tai *hyökkääjä*.

Uhkatoimija on pahantahtoinen taho, jolla on tietty poliittinen, sosiaalinen tai henkilökohtainen päämäärä, ja jolla on tietyt kyvykkyydet ja tarkoitusperät viranomaisten, yksityisten organisaatioiden tai sosiaalisten normien vastustamiseen (Duggan et al. 2007).

Tavallisesti puhutaan *ulkoisista uhkista*, mutta suojautumisen ja havaitsemisen kannalta haastavimpia ovat *sisäiset uhkat*. Sisäisen uhkan toimijat ovat luotettuja henkilöitä, joilla on valmiiksi pääsy kohteeseen tai lähelle kohdetta. Lisäksi sisäisillä uhkatoimijoilla on mahdollisesti tietoa turvajärjestelyiden toteutuksesta ja mahdollisesti niissä olevista heikkouksista ja haavoittuvuuksista. Sisäiset uhkatoimijat voidaan jakaa edelleen passiivisiin ja aktiivisiin. Passiiviset toimijat eivät itse toteuta vahingollista tekoa, vaan toimittavat pahantahtoiselle toimijalle joko tahattomasti tai pakotettuna tietoa vahingollisen teon toteuttamiseksi. Aktiiviset toimijat ovat sen sijaan itse mukana tiedonkeruussa ja vahingollisen teon toteutuksessa. (IAEA 2008)

Uhka-arviointi on prosessi, jolla pyritään tunnistamaan uhkatoimijoita ja niiden ominaisuuksia. Uhka-arvioinnista käytetään myös nimitystä uhkatiedustelu. Uhkatoimijoiden ominaisuuksia ovat muun muassa toimijan sitoutuminen, kyky toimia huomaamattomasti, kärsivällisyyden aste, teknisen osaamisen määrä ja laatu sekä kyky soluttautua kohteeseen (jolloin toimijasta tulee sisäinen uhka) (Mateski et al. 2012). Uhkatoimijoiden tunnistamista ja uhkatoimijoiden ominaisuuksien analysoinnista käytetään myös nimitystä uhkatiedustelu (Roberts & Brown 2017).

2.2 Suojattava omaisuus

Suojattava omaisuus koostuu organisaatiolle elintärkeistä asioista, joihin voi kohdistua erilaisia uhkia. Tietoturvallisuudesta puhuttaessa suojattavia kohteita ovat tyypillisesti organisaation tietojärjestelmät ja niissä olevat tiedot, mutta laajemmin tarkasteltuna suojattavia kohteita ovat myös muun muassa organisaation toiminta, fyysinen omaisuus, henkilöstö, tietämys ja maine.

Uhkat voivat aiheuttaa erilaisia vahingollisia seurauksia suojattavaan omaisuuteen sen lajista riippuen. Tieto-omaisuuden osalta uhka voi vaarantaa luottamuksellisuutta, eheyttä ja saatavuutta. Vastaavasti fyysisen omaisuuden tapauksessa uhkana ovat varkaus ja sabotointi. Alla olevassa taulukossa (ks. Taulukko 1) on esitetty tyypillisimpiä suojattavia kohteita ja niihin kohdistuvia uhkia.

Taulukko 1 Esimerkkejä suojattavista kohteista, niihin kohdistuvista uhkista sekä mahdolliset seuraavista kohteista

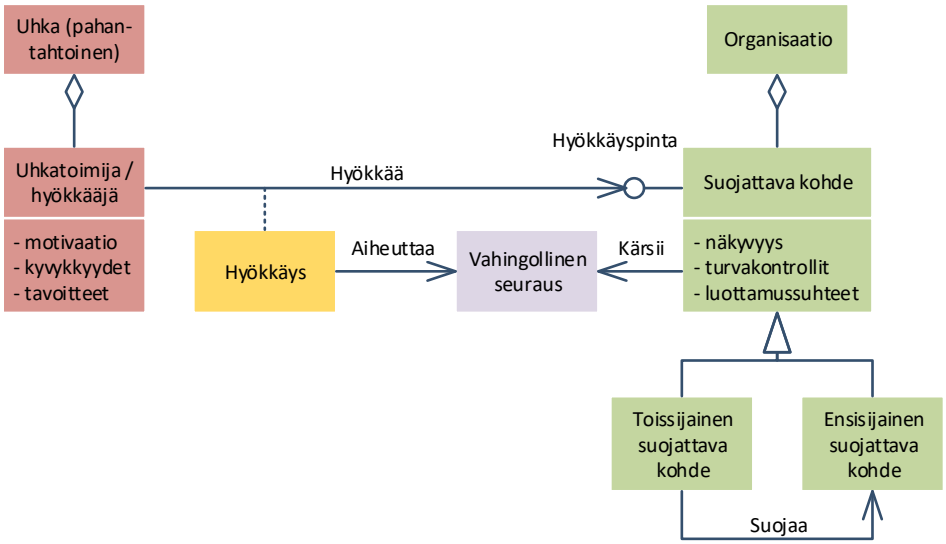
Suojattava kohde	**Uhkan tavoite / vahingollinen seuraus**	**Uhkan toteutumisen mahdollistava seuraava kohde**
Tietoverkot • tietoliikenneyhteydet tietoliikennelaitteet	Tietojen paljastuminen Tietoeheyden menetys Saatavuuden menetys	Tiedot ja tietojärjestelmät Alueet ja tilat
Tiedot ja tietojärjestelmät • käyttöjärjestelmät • ohjelmistot • tietokannat tiedot	Tietojen paljastuminen Tietoeheyden menetys Saatavuuden menetys Kybervaikuttaminen	Tietoverkot Alueet ja tilat Henkilöt
Laitteistot • työasemat palvelimet	Tietojen paljastuminen jne. Fyysisen eheyden menetys Kybervaikuttaminen	Tietoverkot Tiedot ja tietojärjestelmät
Alueet ja tilat fyysinen omaisuus	Varkaus Sabotaasi	Laitteistot Tietoverkot

Suojattava kohde	Uhkan tavoite / vahingollinen seuraus	Uhkan toteutumisen mahdollistava seuraava kohde
Henkilöt yrityksen työntekijät	Tietojen paljastuminen Vaikuttaminen Varkaus Identiteettivarkaus	Tietoverkot Tiedot ja tietojärjestelmät Laitteistot Alue ja tilat

Suojattavat kohteet voidaan luokitella *ensisijaisiin* ja *toissijaisiin* perustuen sen merkitykseen organisaatiolle itselleen (ETSI GS ISI 001-2 2015), mutta vastaava jako voidaan myös tehdä uhkan kautta tarkasteltuna. Ensisijaiset kohteet ovat niitä, joihin uhkatoimija ensisijaisesti pyrkii vaikuttamaan. Toissijaiset kohteet voivat toimia välineinä tai reitteinä ensisijaiseen kohteeseen. Esimerkiksi rakennuksen oven (toissijainen kohde) murtamalla toimija pääsee tiloihin, joissa on arvokkaita esineitä (ensisijainen kohde). Toinen esimerkki on tilanne, jossa henkilöltä (toissijainen kohde) udellaan tietoa, esimerkiksi salasanan (toissijainen kohde), jonka avulla toimija voi toteuttaa tietomurron (ensisijainen kohde).

2.3 Hyökkäys

ISOn määritelmän mukaan "Hyökkäys on yritys tuhota, paljastaa tai varastaa turvattava kohde, muuttaa sitä, tehdä se toimimattomaksi, päästä siihen luvatta" (ISO/IEC 27032 2012). Tässä työssä *hyökkäys* kuvataan uhkatoimijan etenemiseksi suojattavaa omaisuutta kohti tarkoituksenaan tuottaa aikomansa vahingollisen seurauksen. Kuva 2 esittää uhkan ja hyökkäyksen suhdetta organisaation suojattavaan kohteeseen.



Kuva 2 Uhkan suhde suojattavaan kohteeseen: hyökkäys

Suojattavan kohteen reunalla tai rajapinnassa olevat kohdat, joiden kautta hyökkääjä voi luvattomasti päästä kohteeseen ja aiheuttaa vahingollisia seurauksia kohteelle, kutsutaan *hyökkäyspinnaksi* (Ross et al. 2019).

Turvallisuudella tarkoitetaan keinoja, joilla uhka eristetään suojattavasta omaisuudesta. Turvallisuus toteutetaan erilaisilla hallinnollisilla ja teknisillä turvakontrolleilla eli hallintakeinoilla. Turvallisuutta heikentävät suojattavan kohteen näkyvyys, erilaiset tavat päästä kohteeseen käsiksi (hyökkäyspinta) sekä suojattavan kohteen käsittelyyn tai saavutettavuuteen liittyvät luottamussuhteet. (Herzog 2010)

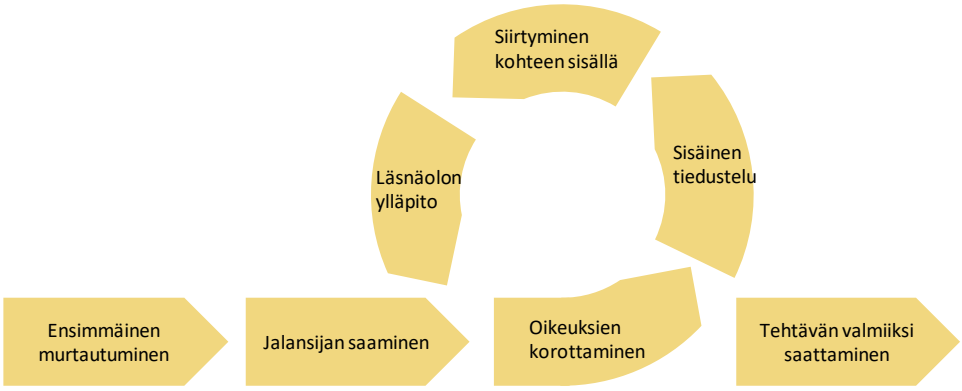
2.4 Hyökkäyksen eteneminen

Systemaattisesti toteutettu hyökkäys voidaan jakaa vaiheittaisiin askeliin, joilla hyökkääjä etenee kohti tavoitettaan. Kullakin vaiheella on merkityksensä hyökkääjälle ja vastaavasti suojaustoimia voidaan kohdentaa kutakin vaihetta varten (Velazquez 2015). Tästä hyökkäyksen tai tunkeutumisen vaiheittaisesta etenemisestä käytetään englanninkielessä laajalti nimitystä Kill Chain. Tämän alun perin sotilaspuolella käytetyn termin kyberturvallisuuteen lanseerasi Lockheed-Martin (Hutchins et al. 2010). Suoran suomennoksen, tappoketjun sijaan tässä työssä käytetään vähemmän raflaavaa nimitystä *hyökkäyksen elinkaari* tai *hyökkäyksen vaiheet*.

Lockheed-Martinin mallissa hyökkäyksen vaiheet ovat:

1. Tiedustelu (reconnaissance), jossa hyökkääjä etsii, tunnistaa ja tutkii potentiaalisia kohteita hyödyntäen eri tietolähteistä saatavaa tietoa.
2. Aseistautuminen (weaponization), jossa hyökkääjä varustautuu esimerkiksi liittämällä haittaohjelman viattomalta näyttävään dokumenttiin tai muuhun tiedostoon.
3. Toimittaminen (delivery), jossa hyökkääjä kuljettaa tavalla tai toisella aseistautumisvaiheessa toteutetun hyökkäysvälineen kohteeseen. Yleisimpiä tapoja ovat sähköpostiliitteet tai USB-muistitikut.
4. Hyväksikäyttö (exploitation), jossa hyökkääjä käynnistää hyökkäysvälineen kohteessa. Väline voi etsiä ympäristön haavoittuvuuksia, seurata käyttäjän toimia tai levitä tietoverkossa.
5. Asennus (installation), jossa muodostetaan etäyhteys tai takaportti pysyvän läsnäolon saavuttamiseksi.
6. Hallinta (command and control), jossa hyökkääjä operoi kohteessa etäyhteyden yli. Erityisesti kohdennetuissa hyökkäyksissä pelkästään automaattisesti toimiva hyökkäysväline ei ole riittävä, vaan tarvitaan manuaalista operoitavuutta.
7. Tavoitteen mukaisen tehtävän suorittaminen (actions on objectives) eli lopulta hyökkääjä kerää tai muuntelee tietoja, sabotoi tietojärjestelmiä, suorittaa kyberoperaation tai siirtyy seuraavaan kohteeseen.

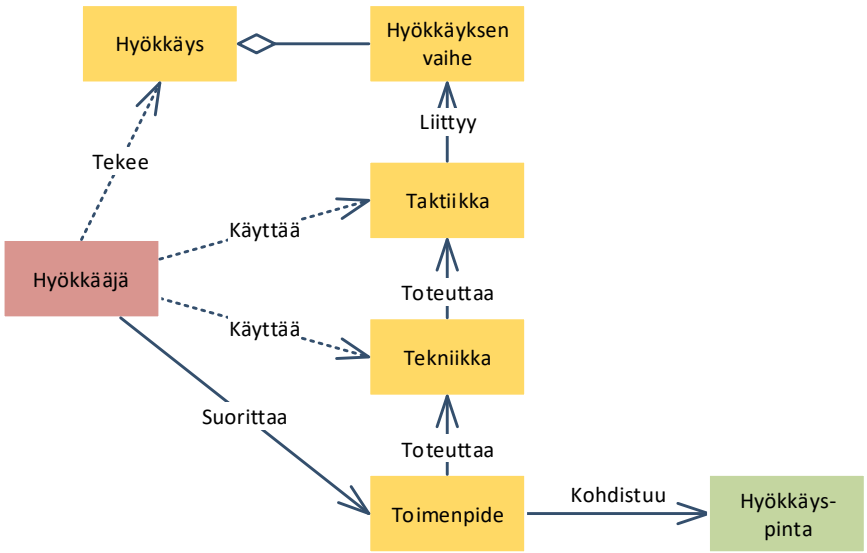
Lockheed-Martinin malliin viitataan melko usein, mutta myös lukuisia muita malleja on kehitelty, joista yhtenä esimerkkinä mainittakoon Mandiant Consultingin hyökkäyksen elinkaari -malli (ks. Kuva 3). Siinä olennaisin lisäys Lockheed-Martinin malliin verrattuna on kuvata eteneminen kohteen sisällä tapahtuvana iteratiivisena oikeuksien noston, tiedustelu, siirtymisen ja läsnäolon vahvistamisen syklinä. Iteratiivisuus tuo esille sen, ettei hyökkäys kybermaailmassa tapahdu niin lineaarisesti kuin mitä Kill Chain antaa ymmärtää, vaan hyökkääjä tyypillisesti joutuu etenemään toissijaisten kohteiden kautta varsinaista hyökkäyksen kohdetta eli ensisijaista kohdetta kohti.



Kuva 3 Mandiant Consultingin iteratiivinen hyökkäysmalli (Bu 2014)

2.5 Hyökkääjän käyttäytymisen mallintaminen

Hyökkäystä ei voi sellaisenaan aistia. Käytännössä hyökkäyksen kohteena oleva organisaatio voi periaatteessa havaita ainoastaan sen hyökkäyspintaan kohdistuvia toimenpiteitä, mutta vaikeutena on erottaa pahantahtoiset toimet normaalista toiminnasta. Ymmärtämällä hyökkäyksen tyypillistä kulkua sekä hyökkääjien käyttäytymistä voidaan mahdollistaa hyökkäyksen tunnistaminen yksittäisten tapahtumien perusteella. Tässä kohdassa hyökkääjän käyttäytymistä tarkastellaan MITREn ATT&CK-mallin kautta käyttäen lähteitä (Strom et al. 2018; MITRE 2019; MITRE 2020b). Muitakin malleja on olemassa, joita on esitetty muun muassa lähteessä (Kwiatkowski & Mouchoux 2018).



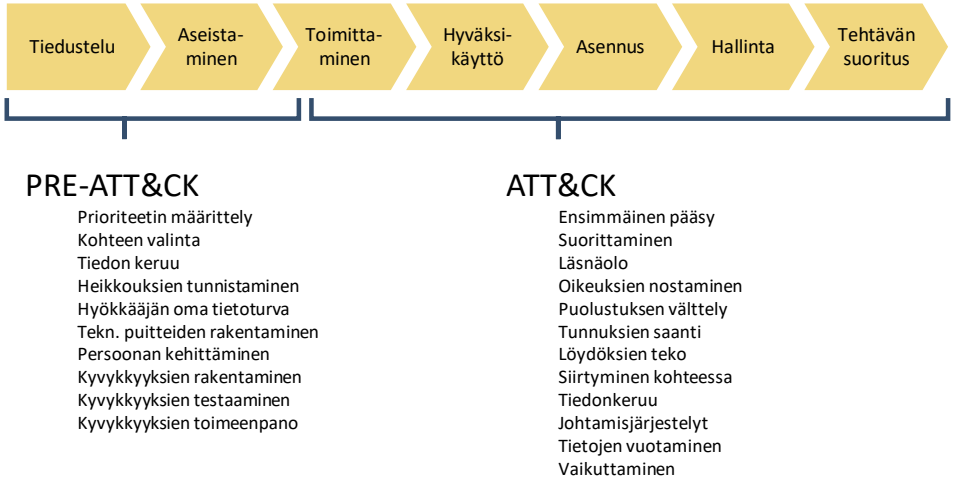
Kuva 4 Hyökkääjän käyttäytymisen mallintaminen

MITREn ATT&CK-mallissa hyökkäys on jaettu *taktiikkoihin* eli hyökkääjän päämääriin hyökkäyksen aikana sekä *tekniikkoihin* ja *toimenpiteisiin*, joita hyökkääjä käyttää saavuttaakseen taktisia päämääriä (ks. Kuva 4). Taktiikoilla ei ole tiettyä perättäistä järjestystä, vaan niitä voidaan pitää pikemminkin hyökkäyksen rakennuspalikoina, jotka voivat eri hyökkäyksissä tapahtua eri vaiheissa. (Pols 2017)

ATT&CK on luotu hyökkääjän käyttäytymisen systemaattista luokittelua varten ja se perustuu todellisiin havaintotietoihin kehittyneistä pitkäkestoisista uhkista (advanced persistent threats, APT). ATT&CK-malli kytkeytyy tiiviisti organisaatiossa yleisesti käytettyihin tietojärjestelmäalustoihin (mm. Windows, Linux) tarjoten yksityiskohtaista tietoa esimerkiksi käytetyistä työkaluista ja kohteena olevista käyttöjärjestelmän versioista. Lisäksi se tarjoaa tietoa mahdollisista keinoista tekniikoiden havaitsemiseksi ja niiltä suojautumiseksi.

Esimerkkinä ATT&CK-mallin tekniikasta mainittakoon siirrettävän tallennevälineen kautta toteutettu tartuttaminen (ks. https://attack.mitre.org/techniques/T1091/). Tältä tekniikalta voi suojautua esimerkiksi minimoimalla USB-muistitikkujen käyttöä ja ottamalla Windowsissa automaattikäynnistysominaisuuden pois päältä.

Varsinaisesti ATT&CK-malli kattaa vain hyökkäyksen elinkaaren toteutusosan vaiheet toimittamisesta tehtävän suorittamiseen. Hyökkäyksen valmisteluun liittyviä taktiikoita ja tekniikoita käsitellään PRE-ATT&CK-mallissa. Yleensä organisaation on vaikea suojautua valmisteluun liittyviltä toimenpiteiltä, koska niitä ei monestikaan tehdä kohdeorganisaation sisällä. PRE-ATT&CK-malli voi kuitenkin auttaa heikkojen signaalien tunnistamisessa, mahdollisten hyökkääjien toimiin varautumisessa ja uhkatilannekuvan muodostamisessa. Kuva 5 esittää ATT&CK ja PRE-ATT&CK -taktiikoita ja niiden sijoittumista hyökkäyksen elinkaareen.



Kuva 5 MITRE ATT&CK ja PRE-ATT&CK -mallien taktiikat suhteessa hyökkäyksen elinkaareen

PRE-ATT&CK-malli kuvaa tekniikoita yleisellä tasolla, koska hyökkääjät voivat käyttää valmistelussa mitä tahansa tietojärjestelmäalustaa. Esimerkkinä hyökkäyksen valmistelevasta tekniikasta on avoimien lähteiden tiedustelu (OSINT, ks. https://attack.mitre.org/techniques/T1247/), joka on helppoa hyökkääjälle, mutta kohdeorganisaation mahdoton tunnistaa.

2.6 Hyökkäysvektorit ja hyökkäysavaruudet

Hyökkäyksen etenemisreittiä tai -tapoja kutsutaan *hyökkäysvektoriksi* (ISO/IEC 27032 2012). Hyökkäysvektoreita ovat siis edellisessä kohdassa kuvatut erilaiset taktiikat, tekniikat ja toimenpiteet. Käytännön esimerkkejä hyökkäysvektoreista ovat siirrettävät tallennusmediat, kalastelusähköpostit, oikeuksien nostot, laitteiston varastaminen, haittaohjelmat jne. (Cichonski 2012; Payne 2007).

MITRE ATT&CK ja PRE-ATT&CK-mallit eivät sisällä täydellistä luetteloa kaikista mahdollisista hyökkäysvektoreista, koska tiedot perustuvat julkisiin lähteisiin ja malleissa keskitytään APT-toimijoihin. Mallit ovat kuitenkin laajennettavissa ja niitä täydennetään koko ajan. (Strom et al. 2018)

ATT&CK-mallia kattavammin hyökkäysvektoreita on luetteloitu muun muassa MITREn CAPEC-tietokantaan. ATT&CK ja CAPEC molemmat kuvaavat hyökkääjien käyttäytymistä. CAPEC luettelee etupäässä sovelluksiin kohdistuvia hyökkäysvektoreita, kun taas ATT&CK keskittyy enemmän tietoverkkoihin ja hyökkäyksen elinkaareen kuvaten taktiikoita, tekniikoita ja toi-

menpiteitä, joita hyökkääjät voivat tehdä. CAPEC sisältää myös joitakin sosiaalisen vaikuttamisen ja toimitusketjuihin liittyviä tekniikoita. (MITRE 2019)

Hyökkäysvektorit voidaan vaikutustapojen mukaan luokitella eri kategorioihin. CAPEC:ssa tekniikat on jaettu *hyökkäysavaruuksiin* (domains of attack), joita ovat ohjelmistot, laitteistot, tietoliikenne, toimitusketjut, sosiaalinen vaikuttaminen ja fyysinen turvallisuus (MITRE 2020a). Luokittelu ei ole poissulkeva, joten yksittäinen tekniikka voi kuulua useampaankin hyökkäysavaruuteen. OSSTMM-menetelmässä CAPEC:n hyökkäysavaruutta kutakuinkin vastaava käsite on *kanava*, joka tarkoittaa kommunikointi- ja vuorovaikutusreittiä, jota hyökkääjä voi hyödyntää (Herzog 2010). Taulukko 2 esittää hyökkäysavaruuksien ja kanavien vastaavuutta.

Taulukko 2 Hyökkäysavaruuksien ja kanavien vastaavuus

Hyökkäysavaruus (CAPEC)	**Kanava (OSSTMM)**	**Hyökkäysavaruus (tämä työ)**
Tietoliikenne	Tietoverkot	Tietoverkot
Ohjelmistot	Tietoverkot	Päätelaitteet (ohjelmistot)
Laitteistot	Tietoverkot	Laitteistot
Toimitusketjut	Fyysinen	Toimitusketjut
Sosiaalinen vaikuttaminen	Ihmiset	Henkilöt
Fyysinen turvallisuus	Fyysinen	Alueet ja tilat
-	Sähkömagneettinen säteily	(Tietoverkot, Alueet ja tilat)
-	Viestiliikenne (esim. puhelinverkot ja modeemit)	Tietoverkot

Jatkossa tässä työssä käytetään hyökkäysavaruus-termiä hyökkäysten vaikutustapojen jaotteluun ja jaottelussa nojaudutaan CAPEC:n määrittämiin hyökkäysavaruuksiin. OSSTMM:n esittelemiä sähkömagneettisen säteilyn ja viestiliikenteen vaikutuskanavia ei sellaisenaan käsitellä tässä työssä. Sähkömagneettiseen säteilyyn sisältyvät muun muassa langaton tiedonsiirto, jota voidaan tarkastella tietoverkkojen yhteydessä, ja hajasäteilyn kaappaaminen, jota osittain voidaan hallita fyysisen turvallisuuden keinoin. Myös viestiliikennettä käsitellään tietoverkkojen yhteydessä.

2.7 Suojautuminen uhkilta

Tässä kohdassa käydään läpi havainnointikyvykkyyden kannalta keskeiset ylätason suojauselementit: turvallisuuden osa-alueet, syvyyssuuntainen puolustus ja turvallisuusoperaatiokeskus.

2.7.1 Turvallisuuden osa-alueet

Hyökkäysavaruus vaikuttaa hyökkäyksen torjuntatapaan. Taulukko 3 kuvaa hyökkäysavaruuksien ja turvallisuuden osa-alueiden välistä vastaavuutta. Turvallisuuden osa-alueilla viitataan tässä yhteydessä Elinkeinoelämän Yritysturvallisuusmalliin (EK 2016). Taulukossa on kuvattu myös vastaava ISO/IEC 27001 -standardin liitteen A mukainen turvallisuuden pääkohta (SFS-ISO/IEC 27001 2017).

Taulukko 3 Turvallisuuden osa-alueet hyökkäysavaruuksittain

Hyökkäysavaruus	**Turvallisuuden osa-alue (EK)**	**ISO/IEC 27001 turvallisuuden pääkohta**
Tietoverkot	Tietoturvallisuus	A.9 Pääsynhallinta A.10 Salaus A.12 Käyttöturvallisuus A.13 Viestintäturvallisuus
Päätelaitteet	Tietoturvallisuus	A.9 Pääsynhallinta A.10 Salaus A.12 Käyttöturvallisuus A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito
Laitteistot	Tietoturvallisuus Toimitila- ja kiinteistöturvallisuus	A. 8 Suojattavan omaisuuden hallinta A.11 Fyysinen turvallisuus ja ympäristön turvallisuus
Toimitusketjut	Tuotannon ja toiminnan turvallisuus	A.15 Suhteet toimittajiin
Henkilöt	Henkilöstöturvallisuus Väärinkäytösten ja poikkeamien hallinta	A.7 Henkilöstöturvallisuus
Alueet ja tilat	Toimitila- ja kiinteistöturvallisuus	A.11 Fyysinen turvallisuus ja ympäristön turvallisuus

2.7.2 Syvyyssuuntainen puolustus

Tämä alakohta perustuu lähteisiin (Garcia 2008; Velazquez 2015).

Syvyyssuuntaisella puolustuksella tarkoitetaan kohteiden suojaamista useilla perättäisillä turvallisuusvyöhykkeillä. Vyöhykkeet voidaan toteuttaa tilaturvallisuuden keinoin tai hallinnollisilla tai teknisillä tietoturvakontrolleilla.

Vyöhykkeiden ansiosta mahdollisella hyökkääjällä on vähemmän tietoa suojausjärjestelykokonaisuudesta, koska sisemmät vyöhykkeet eivät ole ulkoa käsin tarkasteltavissa. Hyökkääminen vaatii myös enemmän valmistautumistyötä, joka nostaa hyökkäyksen aloittamisen kynnystä. Vyöhykkeisyys hidastaa hyökkäystä ja lisää sen epäonnistumisen todennäköisyyttä.

Syvyyssuuntainen puolustus on turvallisuuden toteutuksessa tärkein suunnitteluperiaate, joka liittyy erityisesti havaitsemiseen ja viivytykseen niin fyysisen turvallisuuden kuin tietoturvallisuuden osalta.

Syvyyssuuntaista puolustusta tehostetaan lisäksi suojaustoimien diversiteetillä, toisin sanoen suojaustoimien toteutus tehdään mahdollisuuksien mukaan eri tavalla eri vyöhykkeillä. Diversiteetti voidaan toteuttaa esimerkiksi konfiguroimalla suojaustoimet eri tavoin, käyttämällä esimerkiksi eri valmistajien ratkaisuja tai käyttämällä eri turvallisuuden osa-alueiden ratkaisuja. Konkreettinen esimerkki tästä on rakennuksen fyysinen kuorisuojaus, joka toimii tieto- ja kyberturvallisuuden uloimpana suojauskerroksena.

2.7.3 Turvallisuusoperaatiokeskus (Security Operations Center, SOC)

Tämä alakohta perustuu lähteisiin (Zimmerman 2014; Volksbank et al. 2017).

Tietokoneverkkopuolustus (computer network defence, CND) (Zimmerman 2014) on puolustautumista tietoverkkoihin kohdistuvalta luvattomalta toiminnalta. Puolustukseen sisältyy valvominen, havainnointi, analysointi, vasteen tuottaminen ja palauttaminen. Turvallisuusoperaatiokeskus (security operations center, SOC) on tietokoneverkkopuolustuksesta vastaava elin, joka on määrätty havaitsemaan ja analysoimaan tietoturvahäiriöitä, reagoimaan ja raportoimaan niistä sekä estämään niitä. Vastaava toiminto fyysisen turvallisuuden puolella on hälytyskeskus.

Turvallisuusoperaatiokeskuksen toimintaa kuvataan usein ns. käyttötapauksilla. Käyttötapaus on tietoturvavalvontaskenaario, jonka tarkoituksena on havaita tietoturvauhkan eri ilmenemismuodot. Käyttötapauksissa yhdistyy uhka- ja hyökkäysvektoritietoihin häiriönhallinnan analyysi- ja vastemenetelmät, havaitsemistekniikat, suojattavaan konfiguraatioon ja organisaation liiketoiminnan vaatimuksiin.

MaGMa-käyttötapauskehikossa (Volksbank et al. 2017) on kolmen tasoisia käyttötapauksia. Ensimmäisen eli ylimmän tason käyttötapaukset vastaavat Lockheed-Martinin mallin mukaisia hyökkäyksen vaiheita. Toisen eli taktisen tason käyttötapaukset tarkentavat ylätason käyttötapauksia kuvaten yksityiskohtaisemmin erilaisia tapoja toteuttaa hyökkäyksen vaiheita. Tällä tasolla käyttötapauksiin liittyy tieto toimijasta. Kolmannella eli alimmalla tasolla käyttötapaukset kytkeytyvät toteutusteknologiaan ja sisältävät konkreettisia valvontasääntöjä hyökkäyksien tunnistamiseksi. MaGMan käyttötapauksien pohjalla on käytetty MITREn ATT&CK-mallia siten, että toisen tason käyttötapaukset vastaavat taktiikoita ja kolmannen tason käyttötapaukset tekniikoita.

3 Havainnot ja havainnointikyvykkyys

Havainnointikyvykkyys on osa turvallisuusjärjestelyitä. Kyky havaita hyökkäys tai sen yritys on olennaista torjumisen ja vaikutusten minimoinnin kannalta.

Aluksi kuvataan mitä havaitseminen ja havainnointikyvykkyys tarkoittavat ja mitkä ovat havainnoinnin tavoitteet. Tämän jälkeen kuvataan havainnointia prosessina ja prosessin vaiheina, jonka jälkeen käydään läpi vaatimuksia prosessin toteuttamiseksi ja havainnoinnin tavoitteiden täyttämiseksi. Luvun loppuosa käsittelee hyökkäyksen tunnistamiseen liittyviä kysymyksiä ja tekniikoita sekä havainnointiprosessin vaiheiden sisältöä ja havaitsemistapoja eri hyökkäysavaruuksissa.

3.1 Määritelmiä

Tapahtumaa, jossa jokin ilmiö havaitaan, kutsutaan havaitsemiseksi. Sanakirjamääritelmien (Collins; Cambridge) mukaan havaitseminen (detection) on jonkun asian huomaamista, aistimista tai selville saamista. Vastaavasti havainnoinnilla (observation) tarkoitetaan jonkin asian tarkkailua tai valvontaa, ja siihen liittyvää havaintojen tekemistä.

Tässä työssä havaitsemisella viitataan aistimiseen eli sensorointiin ja sensoreihin, kun taas havainnoinnilla tarkoitetaan laajempaa kokonaisuutta, joka pitää sisällään havaitsemisen lisäksi havaintojen käsittelyn ja ymmärtämisen. Havaitsemisessa sensorit tuottavat havaintoja määriteltyjen havaitsemiskriteerien mukaisesti. Havainnoinnissa sensorien tuottamista tiedoista voidaan ymmärryksen avulla tulkita tapahtuma pahantahtoiseksi teoksi eli hyökkäykseen liittyväksi toimenpiteeksi.

Myös sanat kyky ja kyvykkyys ovat lähellä toisiaan. ISO-standardeissa, kuten esimerkiksi (SFS-EN ISO 9000 2015) termi kyky viittaa suorituskykyyn, tu-

lostasoon tai suoritustasoon. Vastaavasti kyvykkyydellä tarkoitetaan toimintakykyä, kohteen kykyä toteuttaa tuotos. Yhdistelemällä käsitteet havaitseminen ja havainnointi käsitteiden kyky ja kyvykkyys kanssa saadaan neljä lähes synonyymeiltä vaikuttavaa termiä (ks. Taulukko 4).

Taulukko 4 Havaintojen tuottamiseen tasoon ja edellytyksiin liittyviä määritelmiä

Termi	Määritelmä
Havaitsemiskyky	Sensorin tai sensorien suorituskyky eli miten todennäköisesti kriteerien mukainen tapahtuma havaitaan (tietyllä ajanhetkellä).
Havaitsemiskyvykkyys	Sensoroinnin edellytykset tuottaa havaintoja, esimerkiksi sensoroinnin kattavuus suhteessa suojattavaan omaisuuteen, hyökkäyspintoihin ja hyökkäysavaruuksiin.
Havainnointikyky	Havainnoinnin suorituskyky eli miten todennäköisesti hyökkäys havaitaan (tietyllä ajanhetkellä).
Havainnointikyvykkyys	Voimavarat, edellytykset ja osaaminen hyökkäysten havaitsemiseksi.

Havainnointikyvyllä tarkoitetaan todennäköisyyttä havaita hyökkäys, mikäli sellainen organisaatioon kohdistuu. Havainnointikyvykkyydellä tarkoitetaan tekijöitä ja edellytyksiä eli henkilöresursseja ja välineistöä, joilla havainnointikyky saadaan aikaan.

3.2 Havainnoinnin tavoitteet

Havainnoinnin tarkoituksena on saada indikaatio hyökkäyksestä aina kun sellainen tapahtuu, jotta hyökkäys saadaan torjuttua ja sen tuottamat vahingot saadaan pidettyä mahdollisimman pieninä. Mitä paremmin havainnoinnissa onnistutaan, sitä paremmin voidaan onnistua reagoinnissa. Tämän vuoksi tärkeimmät tavoitteet havainnoinnille on, että se tuottaa tietoa luotettavasti ja riittävän nopeasti. Vaikka havainnointi on välttämätön osa turvallisuutta, se ei ole itseisarvo; havainnointiin käytettävien panostuksien ei tulisi ylittää suojattavan omaisuuden arvoa.

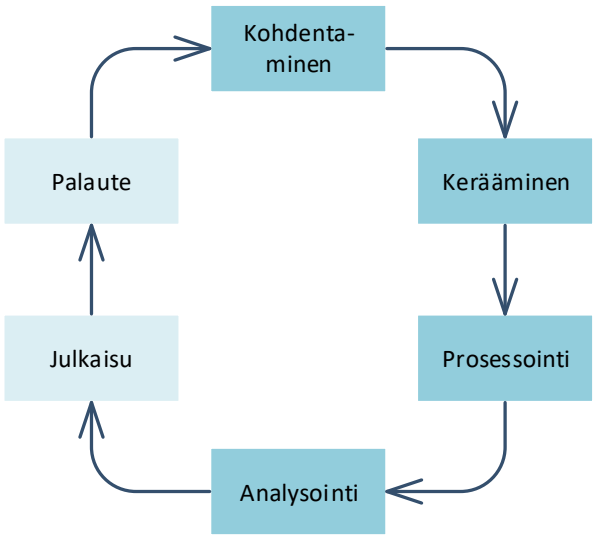
Havainnoinnin tulisi tuottaa mahdollisimman oikeaa tietoa. Tällä tavoitteella on kaksi puolta. Ensinnäkin havainnoinnin tulisi havaita pahantahtoinen toiminta aina, kun sellaista tapahtuu. Toisaalta havainnoinnin tulisi tuottaa havaintoja, jotka mahdollisimman suurella todennäköisyydellä ilmaisevat pahantahtoisen teon tapahtuneen, jotta havainnointiin ja reagointiin käytettävä työmäärä pysyisi kohtuullisena.

Havainnoinnin tulisi tuottaa tiedon hyökkäyksestä mahdollisimman nopeasti, jotta reagointiin jäisi mahdollisimman paljon aikaa. Ensinnäkin hyökkäys tulisi havaita mahdollisimman aikaisessa vaiheessa ja toisaalta havainnoinnin tulisi kyetä tekemään havaintoja mahdollisimman reaaliaikaisesti. Jos uhka havaitaan myöhemmin, kun se on toteutunut, sen välittömiä vaikutuksia ei voi enää estää. Jälkikäteen havaitseminen voi olla kuitenkin hyödyllistä oppimismielessä sekä havainnoinnin ja suojaavien hallintakeinojen kehittämiseksi.

Havainnoinnin tulisi voida toteuttaa mahdollisimman edullisesti ja pienellä vaivalla, koska panostuksia joudutaan tekemään koko ajan kybermaailman monimutkaistuessa, teknologian kehittyessä ja hyökkääjien kyvykkyyksien parantuessa. Raskaat ja kalliit järjestelyt vaikeuttavat kehityksen mukana pysymistä. Lisäksi mitä pienemmällä työllä havaintoja voidaan tuottaa, sen paremmin voidaan onnistua havaintojen paikkansa pitävyydessä ja tuottamisnopeudessa.

3.3 Havainnointiprosessi

Havainnointi on prosessi, jossa kiinnostuksen kohteena olevasta toiminnasta kerätään dataa, joka jalostetaan vaiheittain ymmärrykseksi. Havainnoinnin vaiheittaista etenemistä voidaan tarkastella ns. tiedusteluympyrän kautta. Tiedusteluympyrä on malli, jonka mukaan tiedusteluorganisaatiot tuottavat tietoa päätöksentekoa varten. Tiedusteluympyrästä on olemassa lukuisia eri variaatioita, tässä tapauksessa tarkastellaan kuusivaiheista mallia (Roberts & Brown 2017), ks. Kuva 6



Kuva 6 Tiedusteluympyrä

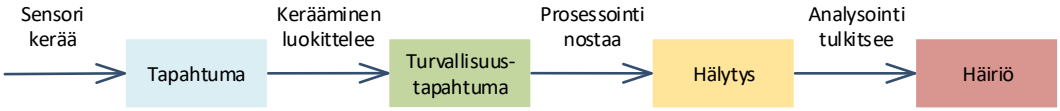
Tiedustelutoimintaa ohjaa tietotarpeet, joiden pohjalta kohdennetaan sensorointia ja havainnointitoimintaa tarkoituksenmukaisella tavalla. Sensorit keräävät kiinnostuksen kohteena olevista ilmiöistä havaintoja, joita tavallisesti pitää prosessoida koneellisesti ennen ihmisen suorittamaa analysointia. Analysoinnin pohjalta tuotetaan tietotuote eli esimerkiksi raportti, joka vastaa tietotarpeeseen. Tietotuotteesta saatu palaute otetaan huomioon tiedustelutoiminnan kohdentamisessa ja muissa ympyrän vaiheissa.

Tiedusteluympyrästä johdettuna havainnointi voidaan kuvata alla olevien vaiheiden perättäisenä etenemisenä:

1. Kohdentamisessa luodaan ja kohdistetaan sensorit sekä sensoreille määritellään havaitsemissäännöt, joiden avulla tunnistetaan mahdollinen pahantahtoinen (tai muuten kiinnostava) toiminta. Tämä edellyttää tuntemusta suojattavista kohteista, organisaation toiminnasta, kohdistuvista uhkista ja hyökkääjien toimintatavoista sekä sensorien ominaisuuksista.
2. Keräämisessä sensorit tarkkailevat kohteina olevia ilmiöitä tai toimintaa, vertaavat esiintyviä tapahtumia havaitsemissääntöihin ja tuottavat niiden pohjalta havaintoja. Tässä vaiheessa havainto luokitellaan turvallisuustapahtumaksi eli sellaiseksi tilaksi, joka viittaa mahdolliseen turvallisuuden vaarantumiseen, tai tilanteeksi, jolla saattaa olla merkitystä turvallisuudelle (SFS-ISO/IEC 27000 2020).
3. Prosessoinnissa havaintoja käsitellään koneellisesti siten, että ihmiselle esitettävä havaintomassa olisi mahdollisimman relevanttia ja informatiivista. Tyypillisesti kerääminen tuottaa helposti valtavia määriä havaintoja, joista jatkokäsittelyyn pyritään suodattamaan vain olennaisimmat. Prosessointi voi tuottaa kriittisistä tai välitöntä käsittelyä vaativista havainnoista hälytyksen hälytysehtojen perusteella.
4. Analysoinnissa tarkastellaan syntyneitä havaintoja ja pyritään arvioimaan, onko kyse todellisesta pahantahtoisesta toiminnasta eli häiriöstä. Analysointi on ihmisvoimin tehtävää työtä, jonka keskiössä on havaintoihin liittyvän kontekstin tuntemus, johon sisältyy muun muassa rinnakkaiset havainnot, havaintojen kehityskulut, uhkatilanne sekä organisaation toiminnan ja suojattavan omaisuuden tila.

5. Julkaisussa raportoidaan havainnoista organisaation johdolle ja muille sidostahoille.
6. Palautevaiheessa analysointitulosten perusteella päivitetään sensoreita ja havaitsemissääntöjä havaintojen laadun ylläpitämiseksi tai parantamiseksi.

Kuva 7 esittää tapahtuman jalostumista ensin turvallisuustapahtumaksi, sitten mahdolliseksi hälytykseksi ja lopulta häiriöksi.



Kuva 7 Tapahtuman jalostuminen tietoturvahäiriöksi

3.4 Havainnointikyvykkyys

Havainnointikyvykkyys tulisi rakentaa siten, että havainnointitavoitteet eli havaintojen oikeellisuus ja tuottamisen riittävä nopeus toteutuvat havainnointiprosessissa. Käytännössä havainnointikyky muodostuu oikeista välineistä, joita käytetään oikein ja joiden tuottamia tuloksia kyetään ymmärtämään.

Havainnoinnin tulisi aina havaita pahantahtoinen teko. Tämä edellyttää havainnoinnin riittävää kattavuutta suhteessa suojattavaan omaisuuteen ja eri hyökkäystapoihin. Tärkeää on myös, että sensorien havaitsemissäännöt on säädetty oikein. Lisäksi sensorien ja muiden havainnointivälineiden tulisi olla mahdollisimman laadukkaita, jotta ne havaitsevat mitä havaitsemissääntöjen puitteissa pitääkin havaita.

Havainnoinnin pitäisi tuottaa mahdollisimman vähän turhia havaintoja. Myös tämä edellyttää laadukkaita havainnointivälineitä ja oikein säädettyjä havaitsemissääntöjä. Tärkeää on myös, että havaintojen prosessointi on tehokasta ja tuottaa mahdollisimman selkeitä ja informatiivisia ilmaisuja analysoijalle.

Havainnoinnin pitäisi tuottaa havainnon mahdollisimman nopeasti. Tämän tavoitteen saavuttamisessa auttaa keräämisen reaaliaikaisuus, havaintojen prosessoinnin korkea automaatioaste ja tehokkuus, analysointivälineiden tehokkuus ja helppokäyttöisyys sekä analysoijien hyvä ammattitaito.

Havainnoinnin tulisi kuluttaa mahdollisimman vähän resursseja. Käytännössä välineiden niin keräys-, prosessointi- kuin analysointivaiheessa tulisi olla mahdollisimman tehokkaita ja edullisia, niiden käyttöönotto sekä käytön aikainen operointi ja ylläpito tulisi olla mahdollisimman vaivatonta. Lisäksi välineistön tuottama tieto mahdollisimman laadukasta ja informatiivista havaintodataa, jotta ihmisvoimin tehtävä työ olisi mahdollisimman vähän kuormittavaa.

Havainnointikyvykkyyden välineistö koostuu etupäässä sensoreista sekä lisäksi prosessointi- ja analysointivälineistä. Lisäksi tarvitaan näitä tukevia tietovarastoja ja tietoliikenneyhteyksiä, joiden ei tulisi muodostaa pullonkaulaa havainnointiin. Välineistöä käsitellään myöhemmin tässä luvussa mutta yhteistä välineille on, että niiden tulisi tarjota riittävän toiminnallisuuden, suorituskyvyn, kapasiteetin ja muunneltavuuden.

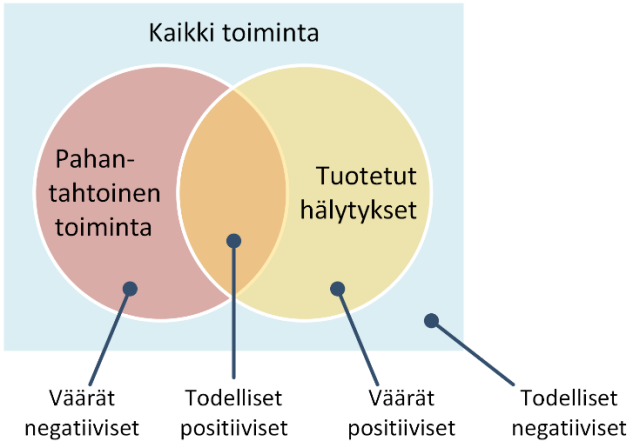
Havainnointikyvykkyys edellyttää tietoa ja osaamista havainnointiprosessin jokaisessa vaiheessa: sensorien kohdentamisessa ja säätämisessä, prosessoinnin kehittämisessä ja analysoinnissa. Havainnointihenkilöstöllä tulee olla tietoa ja osaamista kohteena olevista tietoteknisistä resursseista, tietoverkoista ja tietojärjestelmistä, uhkista ja hyökkäystaktiikoista, -tekniikoista ja -työkalusta sekä havainnointivälineiden ja havainnointitiedon käsittelystä ja hallinnasta. Erilaisia henkilökyvykkyyksiä on lueteltu kattavasti esimerkiksi lähteessä (Newhouse et al. 2017).

3.5 Hyökkäyksen tunnistaminen

3.5.1 Oikeat ja väärät hälytykset

Käytännössä kaikkea pahantahtoista toimintaa ei havaita ja toisaalta on yleistä, että havainnointi tuottaa varsinkin keruuvaiheessa havaintoja, jotka ovat aiheettomia. Kuva 8 esittää asetelmaa, jossa kaikkien tapahtumien joukon sisällä ovat sekä hälytysten että pahantahtoisen toiminnan muodostamat osajoukot. Nämä osajoukot ovat osittain päällekkäin muodostaen neljä eri tapahtumaryhmää:

- Todellinen positiivinen eli todellisesta pahantahtoisesta toiminnasta on tehty havainto.
- Todellinen negatiivinen eli normaalista toiminnasta ei ole tehty havaintoa.
- Väärä positiivinen eli normaalista toiminnasta on tuotettu hälytys.
- Väärä negatiivinen eli pahantahtoinen toiminta on jäänyt havaitsematta.



Kuva 8 Tapahtumien luokittelu (Zimmerman 2014)

Havainnoinnissa tavoitteena on maksimoida todellisten positiivisten määrä suhteessa vääriin negatiivisiin ja vääriin positiivisiin. Hälytyskynnyksen madaltamisella saatetaan pienentää väärien negatiivisten määrää, mutta samalla voidaan tuottaa merkittävästi enemmän vääriä positiivisia, jotka kuormittavat turhaan analysoijia.

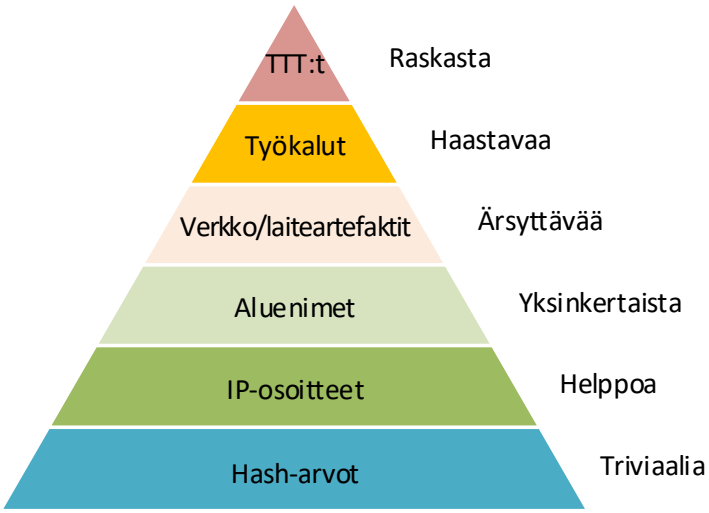
3.5.2 Tunnuspiirteiden ja poikkeamien tunnistaminen

Sensori voi tehdä havainnon joko vertaamalla havaittuja ilmiöitä ennalta määriteltyihin tunnuspiirteisiin tai vertaamalla havaitun ilmiön ominaisuuksia tunnettuun normaalitilanteen ominaisuuksiin. Ensin mainitusta käytetään nimitystä *tunnuspiirrehavainnointi* (signature-based detection) ja jälkimmäisestä *poikkeamahavainnointi* (anomaly detection). Monesti sensorit hyödyntävät molempia tekniikoita. (Zimmerman 2014)

Tunnuspiirrehavainnointi perustuu niin sanottujen *vaarantumisindikaattorien* (indicator of compromise, IOC) käyttöön. Vaarantumisindikaattori on yksittäinen pahantahtoisesta toiminnasta vihjaava tieto, jonka sensori kyke-

nee helposti havaitsemaan. Vaarantumisindikaattoreita ovat esimerkiksi epäilyttävät IP-osoitteet, sähköpostiosoitteet, liitetiedoston nimet tai tiedostoista lasketut hash-arvot. Tunnuspiirrehavainnointi on yleisesti käytetty, koska sen toimintaperiaate on selkeä, havaintojen tuottaminen determinististä ja tehokasta. (Zimmerman 2014)

Tunnuspiirrehavainnointi edellyttää, että sensorille on kerrottava vaarantumisindikaattorit etukäteen tarkasti. Havainnoinnin kannalta vaarantumisindikaattori on sitä parempi, mitä vaikeampi hyökkääjän on sitä muunnella. Kuva 9 esittää hyökkääjän näkökulmasta piirteidensä muuttamisen vaikeusasteita. Matalan tason vaarantumisindikaattoreita on helppo havaita, mutta niitä on hyökkääjän myös vaivatonta muunnella, jolloin ne yleensä vanhenevat nopeasti. Tämä tekee havainnoinnin epävarmaksi ja edellyttää koko ajan ajantasaista uhkatietoa. Mitä korkeammalle abstraktiotasolle noustaan, sitä vaativampaa hyökkääjälle on muuttaa toimintaansa. (Roberts & Brown 2017)



Kuva 9 Tuskan pyramidi (Bianco 2013)

Poikkeamahavainnoinnissa muodostetaan ensin käsitys normaalista ja asiaankuuluvasta käyttäytymisestä, jota käytetään vertailukohtana arvioitaessa myöhemmin tapahtuvaan käyttäytymistä. Havainto luodaan, kun käyttäytymisessä havaitaan poikkeama tallennettuun käyttäytymisprofiiliin.

Poikkeamahavainnointi voi kyetä havaitsemaan niin sanottuja nollapäivähyökkäyksiä eli tilanteita, joita ei ole aiemmin tavattu. Menetelmän huonona puolena on, että sen käyttöönotto vaatii ensin normaalitilan muodostamisen ja tallentamisen, joka vie aikaa ja voi olla haasteellista. Lisäksi menetelmä on monimutkainen ja tuottaa helposti vääriä positiivisia havaintoja, esimerkiksi

jos organisaatio ottaa uusia tietojärjestelmiä tai toimintatapoja käyttöönsä. (Zimmerman 2014)

3.6 Havainnoinnin kohdentaminen

Kohdentamisessa tavoitteena on saavuttaa mahdollisimman kattava ja hyvä havainnointikyky mahdollisimman helpolla ja edullisesti. Havainnoinnin kohdentaminen pitää tehdä siten, että havainnoinnilla katetaan organisaation suojattava omaisuus ja siihen kohdistuvat uhkat. Kohdentamisessa tulee ottaa huomioon organisaatioon kohdistuvat vaatimukset, olemassa olevat turvajärjestelyt ja organisaation toiminta.

Valvonnan kattavuuden varmistamiseksi tulisi olla tarkka kuva suojattavista kohteista, esimerkiksi omaisuusluettelon tai konfiguraatiohallintatietokannan (configuration management database CMDB) kautta. Luettelo voidaan muodostaa käsin tai esimerkiksi verkkoon kytketyt laitteet voidaan etsiä käymällä verkkoa läpi skannaustyökaluin (Zimmerman 2014). Omaisuusluettelossa olisi hyvä olla tiedot suojattavista kohteista riittävällä tarkkuudella. Esimerkiksi ohjelmiston versio- ja päivitystieto kertoo mahdollisista haavoittuvuuksista. Kohdentamisen kannalta oleellista on myös suojattavien kohteiden fyysinen sijainti ja sijoittuminen turvallisuusvyöhykkeille. Lisäksi merkityksellisiä tietoja ovat suojattavien kohteiden kriittisyys organisaatiolle, näkyvyys, saatavuus ja pääsyoikeusjärjestelyt (Herzog 2010).

Havainnoinnin tulisi kattaa erilaiset hyökkäysavaruudet ja -vektorit sekä hyökkäyksen vaiheet. Lisäksi ennakkotiedot hyökkääjien kyvyistä voi auttaa valitsemaan sensorit ja sensorien ominaisuudet siten, että niiden ohittaminen tai huijaaminen on mahdollisimman vaikeaa.

Jotta hyökkäys havaittaisiin mahdollisimman aikaisin, tulisi havainnointi kohdistaa hyökkäyksen tiedusteluvaiheeseen, joka ilmenee mahdollisena epäilyttävänä liikehdintänä organisaation reuna-alueilla. Käytännössä ongelmaksi kuitenkin voi muodostua tiedustelutapahtumien määrä sekä se, että niistä on vaikea tunnistaa todellisia positiivisia hälytyksiä (Roberts & Brown 2017). Havainnointi kannattaakin kohdistaa useampaan hyökkäyksen vaiheeseen ja hyödyntää tietoa siitä, mitä taktiikoita, tekniikoita ja toimenpiteitä hyökkääjät eri vaiheessa käyttävät (Velazquez 2015). Esimerkiksi kohteeseen ujutettu troijalainen tyypillisesti lähettää hallintavaiheessa säännöllisiä vies-

tejä hyökkääjän suuntaan etäohjausyhteyden käynnistämiseksi. Tällainen toiminta voidaan havaita epäilyttävänä ulospäin suuntautuvana liikenteenä tietoliikenneyhteyksissä (Zimmerman 2014).

Organisaatioon kohdistuu ulkoisia ja sisäisiä vaatimuksia, jotka voivat koskea havainnointia. Ulkoisia vaatimuksia ovat lainsäädännön asettamat vaatimukset ja sopimukselliset vaatimukset. Lainsäädäntö ohjaa valvontaa erityisesti ihmisten yksityisyyden suojan kautta, valvonta ei voi olla mielivaltaista. Sopimukset voivat asettaa vaatimuksia esimerkiksi sen suhteen, miten sopimusten alaista omaisuutta tulee valvoa. Organisaatio voi asettaa myös itselleen vaatimuksia politiikkojen kautta. Esimerkiksi riskienhallintapolitiikka voi määrittää hyväksyttävän riskitason, joka voi vaikuttaa havainnoinnin järjestelyihin.

Sensorointi kytkeytyy olemassa oleviin turvajärjestelyihin, turvallisuusvyöhykkeisiin ja turvakontrolleihin. Valvonnan olisi hyvä kattaa eri turvallisuusvyöhykkeet ja varsinkin ulkoraja tulisi varustaa tunkeutumisenilmaisuvälineillä. Sijoittelussa erityisesti tulisi ottaa huomioon vyöhykerajojen potentiaaliset tunkeutumispisteet. Turvakontrollit voivat tarjota keinoja luvattomien pääsy-yritysten havainnointiin. Esimerkiksi tällaisia ovat kulunvalvonta, palomuurit ja IDS/IPS-laitteet. Havainnoinnin kohdentamisessa tulee ottaa huomioon myös olemassa olevan valvontakoneiston puutteet ja kehityskohteet.

Kohdentamista tulisi päivittää aina kun suojattavaan omaisuuteen, uhkakuvaan, turvajärjestelyihin, organisaation toimintaan tai havainnointia koskeviin vaatimuksiin tulee muutoksia.

3.7 Havaintojen kerääminen

Keräämisen tavoitteena on tuottaa havaintoja siltä alueelta, johon kohdentaminen on tehty. Tyypillisesti havaintoja kerätään koneellisesti sensoreilla, mutta myös ihmiset voivat tuottaa havaintoja. Sensoroinnissa tärkeitä tekijöitä ovat sensorien kyky tuottaa olennaisista ilmiöistä havainnoinnin kannalta hyödyllisiä tapahtumia tehokkaasti ja luotettavasti. Esimerkiksi havainnointisääntöjen mukaiset ilmiöt tulisi aina havaita, eikä sensori saisi tuottaa liiaksi kohinaa väärien positiivisten muodossa. Sensorin kykyyn tuottaa havaintoja vaikuttavat sensorin toteutusteknologia, oikeanlainen konfigurointi ja herkkyys häiriötekijöille.

Sensoroinnissa voi toisinaan olla tärkeää myös, se että niiden tulisi mahdollisimman vähän paljastaa itseään hyökkääjälle, koska se voi tällöin siirtää hyökkääjän toimintaa mahdollisesti hankalammin valvottavalle alueelle.

Sensoroinnin tulisi vaikuttaa mahdollisimman vähän organisaation käyttäjien arkeen. Aina tältä ei voida välttyä, esimerkiksi haittaohjelmien havaitsemisvälineen aiheuttama tiedostojen läpikäynti voi aiheuttaa käyttäjille näkyvää työaseman toiminnan hidastumista.

Havaintojen keruun järjestäminen voi olla toisinaan hyvin työlästä tai mahdotonta. Tällaisia tilanteita ovat muun muassa ihmisten välinen kasvotusten tapahtuva kommunikaatio tai organisaation tavoittamattomissa oleva toiminta, esimerkiksi toimitusketjujen tai ulkoistettujen palveluiden osalta.

Tässä kohdassa esitellään keinoja kerätä havaintoja tietoliikenneympäristöissä, päätelaiteympäristöissä, laitteistoissa ja toimitusketjuissa, fyysisissä ympäristöissä sekä ihmisten välisessä toiminnassa. Esitetyt sensorit ja sensoritekniikat eivät muodosta täydellistä ja kattavaa sensorilistaa, koska erilaisia tapoja ja teknologioita niin hyökkäykseen kuin havaitsemiseen kehitetään koko ajan.

3.7.1 Tietoverkot

Keskeisin väline epäilyttävän toiminnan havainnointiin tietoverkoissa on tunkeutumisenhavaitsemisjärjestelmä (intrusion detection system, IDS). IDS-laitteet analysoivat liikennettä ja etsivät epätavallista käyttäytymistä tai epäilyttäviä tapahtumia. IDS-laitteiden toiminta perustuu tavallisimmin tunnuspiirrehavainnointiin, mutta myös poikkeamahavainnointiominaisuuksia on joissain tuotteissa. Monesti IDS tukee molempia havainnointitapoja. Kehittyneimmät IDS:t hyödyntävät koneoppimista poikkeamantunnistuksessa. (Thompson 2018)

Havainnointiin voidaan käyttää myös monia muita tietoliikennekomponentteja. Tietoverkkosensorit voidaan jakaa sen mukaan, tuottavatko ne ensiherätteitä huomiota vaativista tapahtumista vai tuottavatko syvällisempää tai taustoittavaa tietoa hyökkäyksestä analysointia varten. IDS-laitteet ovat esimerkki ensin mainituista sensoreista. Analysointivaiheessa voidaan käyttää

esimerkiksi koko tietoliikenteen keräämiä laitteita, mutta ne eivät sovellu jatkuvaan valvontaan tuottamaan reaaliaikaisia hälytyksiä hyökkäyksistä. (Zimmerman 2014)

Joissain tapauksissa sensori itsessään ei tuota ensiherätteiksi kelpaavia tietoja, mutta prosessointivaiheessa tietojen yhdistelyn ja korreloinnin kautta voidaan tuottaa havaintoja (Zimmerman 2014). Tällaisia sensoreita ovat muun muassa NetFlow-tietoa tuottavat verkkolaitteet, kuten esimerkiksi palomuurit, yhdyskäytävät, nimipalvelimet, reitittimet ja kytkimet, jotka keräävät tietoa normaalin toimintansa ohessa. Tietoliikennelaitteet keräävät tietoa liikenteestä, esimerkiksi lähettäjistä, vastaanottajista, siirretyn tiedon määrästä ja käytetyistä protokollista. (Thompson 2018; Roberts & Brown 2017)

3.7.2 Päätelaitteet

Päätelaitteiden, kuten palvelimien, työasemien ja mobiililaitteiden valvontaa voidaan hyödyntämällä päätelaitteen lokeja, suojausjärjestelmiä, tunkeutumishavaitsemisjärjestelmiä tai tietoliikennettä käsitteleviä komponentteja.

Päätelaitteiden käyttöjärjestelmät keräävät seuranta- ja käyttäjälokeja, joita voidaan käyttää poikkeavan toiminnan tunnistamiseen. Seurantalokeihin jää tietoa muun muassa onnistuneista kirjautumisista ja epäonnistuneista kirjausyrityksistä. Käyttöjärjestelmälokit voivat kertoa esimerkiksi tiedostojen käsittelystä, prosessien luonnista, etäyhteyksien luonnista, käyttöjärjestelmäasetusten muutoksista jne. (Thompson 2018)

Päätelaitteen suojausjärjestelmät ovat kokonaisuuksia, jotka tarjoavat erilaisia suojaus- ja havainnointitoiminnallisuuksia. Tunnetuin lienee haittaohjelmasuojaus, joka havaitsee päätelaitteelle tuodun tai asennetun haittaohjelman (Zimmerman 2014). Toinen esimerkki suojoustoiminnallisuuksista on sallittujen ja kiellettyjen ohjelmien listat ja niiden keskitetty päivittäminen. Päätelaitesuojaus voi myös havaita laitteelle tehtyjä konfiguraatiomuutoksia vaarantumisindikaattoreiden avulla tai vertaamalla laitteen käyttäytymistä normaalitilanteen käyttäytymiseen (Thompson 2018). Vielä yhtenä suojaustoiminnallisuutena mainittakoon tiedon menetyksen estäminen (data loss prevention, DLP), jotka tunnistavat sensitiivisen tiedon ja estävät sen siirtämistä esimerkiksi muistitikulle (Zimmerman 2014).

Päätelaitteen tunkeutumisenhavaitsemisjärjestelmä (host-based intrustion detection system, HIDS) valvoo päätelaitteen verkkoliityntöjen tietoliikennettä vähän vastaavalla tavalla kuin tietoverkkojen IDS-järjestelmät. HIDS-järjestelmän etuna on se, että periaatteessa kykenee tunnistamaan paremmin hyökkäykseen liittyvää tietoliikennettä, koska siitä puuttuu salattu liikenne ja se on kohdistettu kyseiselle päätelaitteelle. HIDS-järjestelmät voivat myös mahdollistaa sisäisen uhkan tunnistamista.

Tietoliikennettä voidaan myös valvota palomuurien ja VPN-tuotteiden avulla (Zimmerman 2014).

3.7.3 Laitteistot

Laitteistot voivat altistua hyökkäyksille valmistuksen ja toimittamisen sekä käytön aikana. Toimitusketjuihin kohdistuvia hyökkäyksiä käsitellään niin laitteistojen kuin ohjelmistojen osalta seuraavassa alakohdassa.

Käytön aikana laitteistot voivat vaarantua silloin, kun ne jäävät valvomatta tai fyysisen turvallisuuden järjestelyt pettävät. Hyökkääjä voi muunnella laitetta tai tehdä siihen lisäyksiä, joiden avulla voidaan esimerkiksi kerätä sensitiivistä tietoa. Hyökkäys voi ilmetä myös laitteen varkautena tai sabotointina. Hyökkäykset voivat kohdistua päätelaitteisiin, tietoverkon kaapelointiin tai tietoliikennelaitteisiin tai tiloihin, joissa laitteistoja sijaitsee.

Havainnointiin voidaan käyttää fyysisen turvallisuuden tarjoamien keinojen lisäksi esimerkiksi tilojen ja laitteiden visuaalista tarkastelua tai ylimääräisen sähkömagneettisen säteilyn ilmaisimia. Verkkoihin kytkettyjä vieraslaitteita voidaan havaita kattavan tietoverkkovalvonnan kautta.

3.7.4 Toimitusketjut

Toimitusketjut voivat muodostaa tavattoman pitkiä ja monihaaraisia verkostoja lähtien mikropiirien ja ohjelmistokirjastojen suunnittelusta aina valmistuksen, integroinnin, kokoonpanon kautta tuotteiden jakeluun. Jokaisessa toimitusketjun portaassa hyökkääjällä voi olla mahdollisuus peukaloida tuotetta tai sen osaa.

Toimitusketjujen turvallisuutta ja erilaisia hyökkäystapoja ja puolustuskeinoja on kuvattu lähteessä (Miller 2013). Hyökkäys voi kohdistua laitteistoon (hardware, HW), ohjelmistoon (software, SW), laiteohjelmistoihin

(firmware, FW) tai järjestelmän tietoihin. Hyökkäys voi toteutua lisäyksen tekemisenä tuotteeseen tai osan korvaamisena, muunteluna tai haittaohjelmana.

Toimitusketjuihin liittyvien hyökkäysten tunnistaminen on tavallisesti hyvin hankalaa, koska organisaatioilla harvemmin on näkyvyyttä toimitusketjun eri vaiheisiin ja tuotteiden sisäiseen rakenteeseen ja toimintaan. Mikäli mahdollista, tulisi pyrkiä luomaan näkyvyys toimittajien tuotantoprosesseihin, henkilöstöön ja alihankkijoihin, ja luomaan keinot havaita niissä hyökkäyksiin viittaavia poikkeamia. Poikkeamien havainnointikykyä voidaan arvioida tuotantoketjuun kohdistuvalla penetraatiotestauksella.

Laitteistoja ja laiteohjelmistoja voidaan valvoa sinetöityjen turvapakkausten tai piilotettujen turvamerkintöjen käytöllä, analysoimalla sähkömagneettista säteilyä tai visuaalisella tarkastelulla. Turvapakkausten ja -merkintöjen käyttö edellyttää mahdollisuutta vaikuttaa toimitusketjun menettelytapoihin. Visuaalisella tarkastelulla sekä lämpö- ja sähkömagneettisen säteilyn analysoinnilla on mahdollista tunnistaa muutokset muuntelemattomaan laitteeseen verrattuna.

Ohjelmistojen valvontaa voidaan tehdä tuotteen toteutusvaiheessa suunnittelu- ja lähdekoodikatselmuksilla. Ohjelmistotoimitusten luotettavuutta voidaan valvoa hyödyntämällä esimerkiksi tarkistussummia, digitaalista allekirjoitusta ja tiedoston salausta. Ohjelmistopäivitysten osalta voidaan todentaa päivityksen lähde ja toimitustapa. Esimerkiksi onko toimitettu päivitys linjassa toimittajan päivitysperusteiden, kuten päivitysvälin tai ajankohdan kanssa.

3.7.5 Fyysinen maailma

Tämä kohta perustuu pääosin lähteeseen (Garcia 2008). Fyysisen turvallisuuden kontrollit jaetaan havaitsemiseen, viivytykseen ja vasteeseen. Havaitseminen pitää sisällään tunkeutumisen havaitsemisen, hälytyskommunikaation ja hälytyksen todentamisen.

Fyysisen turvallisuuden tunnistustekniikat voidaan jakaa ulkoaluesensoreihin, sisäaluesensoreihin ja pääsynhallintaan. Ulkoaluesensoreita ovat infrapunailmaisimet, videokuvailmaisimet ja tutkat sekä erilaiset maahan upotet-

tavat paine- ja värähtelyilmaisimet tai aitoihin asennetut ilmaisimet. Sisäaluesensoreita ovat kuorisuojausilmaisimet, sisäliiketunnistimet, lähitunnistimet, magneettikytkimet, lasirikkoilmaisimet ja muut silmukkapohjaiset ilmaisimet.

Myös pääsynhallinnan järjestelmiä voidaan käyttää havainnointiin ja kerätä tietoa valtuutettujen henkilöiden kulusta ja sijainnista tai yrityksistä päästä alueille tai tiloihin, joihin henkilöllä ei ole valtuutusta.

Fyysisen turvallisuuden tunnistamismekanismeihin kuuluvat myös kielletyn materiaalin, kuten aseiden, räjähteiden, luvattomien työkalujen tai suojattavan omaisuuden kuljettamisen havainnointi. Näissä tapauksissa käytetään esimerkiksi läpivalaisulaitteita, metallintunnistimia ja kiellettyjen aineiden tunnistamiseen opetettuja koiria.

Fyysisessä turvallisuudessa käytetään vielä nykyäänkin melko konservatiivista tekniikkaa verrattuna tietoturvatapahtumien havaitsemistekniikkoihin. Uusimpia ovat erilaiset tekoälyä hyödyntävät tunnistus ja -analysointitekniikat, jotka voivat esimerkiksi tunnistaa henkilöitä videokuvasta.

3.7.6 Henkilöt

Organisaation henkilöt voivat olla hyökkäysten kohteena siinä missä laitteistot, järjestelmät ja fyysinen omaisuuskin. Ihmiset ovat lisäksi helppoja kohteita, koska ihmiset ovat koko ajan keskenään vuorovaikutuksessa, ihmisillä on taipumus tehdä virheitä ja ihmisten käyttäytymistä voidaan ohjailla. Tämä kohta perustuu lähteisiin (Mouton 2014; Gragg 2003).

Sosiaalisessa vaikuttamisessa henkilöä manipuloidaan sosiaalisen vuorovaikutuksen keinoin tekemään sellaista, jota henkilö ei vapaaehtoisesti muuten tekisi. Tyypillisiä tavoitteita on saada luottamuksellista tietoa tai pääsyn kohteeseen, joka on ulkopuolisilta rajattu.

Sosiaalinen vaikuttaminen voi perustua suoraan tai epäsuoraan kommunikaatioon. Suora kommunikaatio voi olla yksi- tai kaksisuuntaista. Kommunikointi voi tapahtua kasvotusten tai käyttäen viestintävälineitä, kuten sähköpostia, puhelinta, pikaviestisovelluksia, tallennevälineitä, perinteistä kirjettä, esitteitä tai verkkosivuja.

Henkilöön kohdistuvan manipuloinnin etenemistä on käsitelty kirjallisuudessa. Eräs malli on Kevin Mitnickin esittelemä sosiaalisen vaikuttamisen hyökkäyssykli, joka koostuu neljästä perättäisestä vaiheesta: tutkimustyö, yhteyden ja luottamuksen rakentaminen, luottamuksen hyödyntäminen ja informaation hyödyntäminen. Tutkimusvaiheessa hyökkääjä kerää tietoa kohteesta. Yhteydenluonti- ja luottamuksen rakentamisvaiheessa hyökkääjä käyttää hyväkseen sisäpiiritietoja tai väärää identiteettiä, viittaavat kohteen tuntemiin henkilöihin, esittävät avutonta tai vetoavat arvovaltaan. Luottamuksen hyödyntämisessä hyökkääjä pyytää kohdehenkilöltä tietoa tai palvelusta, tai saa kohdetta pyytämään apua hyökkääjältä. Informaation hyödyntämisessä hyökkääjä on joko päässyt tavoitteeseensa tai jatkaa kohti uutta kohdetta tai tavoitetta.

Sosiaalinen vaikuttaminen perustuu tiettyjen psykologisten periaatteiden hyödyntämiseen vuorovaikutuksessa. Kohteena oleva henkilö voidaan saada *kiihtyneeseen mielentilaan*, jolloin hänen kykynsä tehdä järkeen perustuvia ratkaisuja heikkenee. Henkilöä voidaan *kuormittaa* korostamalla asian kiireellisyyttä, jolloin henkilö ennemmin toimii, kuin jää miettimään teon seurauksia. Henkilölle voidaan tehdä jokin palvelus, jolloin henkilö *vastavuoroisesti* pyrkii korvaamaan sen auttajalleen jollakin tavalla. Henkilön kanssa voidaan luoda *petollinen ystävyyssuhde,* esimerkiksi keskustelemalla yhteisistä kiinnostuksen kohteista tai vihollisista. Henkilön *vastuullisuutta tai moraalia voidaan heikentää* vetoamalla suurempaan hyveeseen. Henkilö voidaan saada tekemään vastoin organisaation hyväksyttyjä käytäntöjä esimerkiksi pelastaessaan ystävän kuvitellulta irtisanomiselta. Hyökkääjä voi käyttää *auktoriteettia* esiintymällä esimerkiksi johtoryhmän jäsenenä. Ihmiset pyrkivät toimimaan *yhdenmukaisesti* vallitsevien käytäntöjen ja muiden organisaation ihmisten toiminnan mukaisesti.

Sosiaalista vaikuttamista voidaan tunnistaa viestiliikennettä valvomalla, esimerkiksi roskapostisuodattimilla, jotka ovat monissa organisaatiossa käytössä. Roskapostisuodattimet tunnistavat potentiaaliset asiattomat viestit ja siirtää ne roskalaatikkoon.

Kasvokkain tapahtuvan sosiaalisen vaikuttamisen havaitseminen onkin sitten vaikeampaa. Ehkä suurin ongelma havainnoinnin kannalta on, että ihmiset eivät itse useinkaan tunnista olevansa mahdollisia kohteita. Käytännössä säännöllinen koulutus on ainoa tapa puolustautua sosiaalisen vaikuttamisen

uhkalta. Ihmisten väliseen vuorovaikutuksen havainnointiin on kehitelty malleja, esimerkiksi sosiaalisen vaikuttamisen havaitsemismalli SEADM (Bezuidenhout 2010).

3.8 Havaintojen prosessointi

Tämä kohta perustuu lähteisiin (Roberts & Brown 2017; Zimmerman 2014).

Sensorien tuottama tieto ei välttämättä ole havainnoinnin kannalta käyttökelpoisessa muodossa. Havaintojen prosessoinnilla pyritään eri sensoreilta tulevasta havaintodatamassasta koostamaan mahdollisimman selkeitä indikaatioita hyökkäyksistä. Havainnoille kohdistettavia yleisimpiä prosessointitoimenpiteitä ovat normalisointi, indeksointi, kääntäminen, rikastaminen, korrelointi, suodattaminen, priorisointi ja visualisointi.

Normalisointi tarkoittaa havaintodatan muuntamista relaatiotietokannoille sopivaan muotoon eli normalisointisääntöjen mukaan data jaetaan omiin tauluihinsa. Tässä yhteydessä eri lähteistä tulevat tiedot pyritään saamaan keskenään mahdollisimman samaan muotoon.

Indeksoinnilla datalle muodostetaan hakua helpottavat rakenteet. Havainnot voidaan indeksoida esimerkiksi osoitteiden ja muiden tunnistetietojen perusteella, joita saatetaan käyttää myöhemmin havaintojen haussa.

Joissain tapauksissa havainto sisältää kirjoitettua tai puhuttua kieltä, jonka ymmärtäminen voi olla tärkeää havainnoinnin kannalta. Tekstin kääntäminen koneellisesti saattaa tuottaa kieliopiltaan ontuvaa kieltä, mutta se voi kuitenkin helpottaa ensiherätteiden tekoa.

Rikastamisessa täydennetään havainnon tietoja esimerkiksi tunnettujen perustietojen (master data) tai muiden tietolähteiden avulla.

Havaintoja voidaan korreloida tunnettuihin vaarantumisindikaattoreihin tai hyökkääjän toimintaa kuvaaviin käyttötapauksiin (Volksbank et al. 2017). Korrelointia voidaan tehdä myös vertaamalla tuloksia historiatietoihin. Korrelointi tuottaa tietoa havainnon merkityksestä.

Suodattamisella pyritään poistamaan ylimääräistä kohinaa havaintomassasta, jotta analysoijalle tulisi esille vain käsittelyä vaativat havainnot. Suodattamisella ei kuitenkaan poisteta havaintoa tietokannasta, jotta niitä voidaan tarvittaessa tarkastella syvällisemmässä analysoinnissa.

Priorisoinnissa havainnoille pyritään määrittämään merkitys ja käsittelyn kiireellisyys havainnon sisältämän tiedon perusteella.

Visualisoinnissa havainnot tarjotaan analysoijalle informatiivisessa muodossa. Visualisointi voidaan toteuttaa erilaisin listoin tai graafisin näkymin, jotka voivat olla käyttäjän tarvittaessa konfiguroitavissa. Visualisointi voi ilmetä myös huomiota herättävinä hälytyksinä, jotka voidaan muodostaa haluttujen hälytyssääntöjen perusteella.

Tyypillinen prosessointiväline on SIEM (security information and event management), joka kykenee vastaanottamaan IDS-tietoja ja keräämään eri muodossa olevia lokitietoja. SIEM-järjestelmää kevyempi ja edullisempi ratkaisu on käyttää lokienhallintajärjestelmää, joka mahdollistaa havaintojen keskitetyn keräämisen, mutta rajallisesti muita prosessointiominaisuuksia.

3.9 Havaintojen analysointi

Tämä kohta perustuu lähteisiin (Roberts & Brown 2017; Zimmerman 2014).

Analyysi tarkoittaa merkityksien, päätelmien ja ennusteiden tekoa kerätyn ja prosessoidun havaintodatan arvioinnin ja jäsentämisen kautta. Analyysi on aina ihmisten tekemää työtä, jossa voidaan joutua toimimaan mahdollisesti puutteellisten ja epävarmojen tietojen pohjalta. Jos analyysi voidaan muotoilla algoritmiksi ja toteuttaa koneellisesti, siitä tulee prosessointia. Joka tapauksessa, vaikka prosessointivälineet olisivat kuinka tehokkaita ja älykkäitä, viime kädessä tarvitaan aina lopulta ihmisen tekemä päätös siitä, että havainto on aiheellinen ja edellyttää jatkotoimenpiteitä (Garcia 2008).

Analysointi voidaan tehdä reaaliaikaisesti sekunti-minuutti -tasolla prosessoinnin tuottamien tulosten pohjalta tai myöhemmin tutkimalla syvällisemmin havaintoa ja siihen mahdollisesti liittyviä tietoja. Reaaliaika-analysoinnissa triviaalimmat ja kiireellisimmät havainnot luokitellaan aiheettomiin tai aiheellisiin eli häiriöihin. Havainto voidaan myös eskaloida syvällisempään

analyysiin, mikäli sen merkitystä ei kyetä heti ratkaisemaan tai se vaatii laajempaa käsittelyä. Syvällisemmässä analyysissä voidaan tutkia laajoja havaintomassoja ja käyttää monipuolisia analysointivälineitä ja se voi viedä aikaa tunneista kuukausiin.

4 Havainnointikyvyn ja -kyvykkyyden mittaaminen

Tässä luvussa perehdytään tietoturvamittareihin, havainnointikyvyn ja -kyvykkyyden mittaamiseen ensin yleisellä tasolla ja sen jälkeen erilaisten viitekehyksien kautta. Lopuksi rakennetaan elementit havainnointikyvyn ja -kyvykkyyden mittaamiseksi.

4.1 Tietoturvan mittaaminen

Tässä kohdassa käydään läpi tietoturvan mittaamisen perusteita, terminologiaa sekä erilaisia mittareita, mittareiden käyttötarkoituksia ja hyvien mittareiden ominaisuuksia. Tämä kohta perustuu pääosin lähteeseen (SFS-ISO/IEC 27004 2016).

4.1.1 Perusteet

Mittaaminen tarkoittaa jonkun kohteen ominaisuuden arvon tai määrän määrittämistä tietyllä ajan hetkellä. Mittari on muuttuja, joka saa arvon mittauksessa. Mittaamista käytetään organisaation toiminnan johtamisessa ja kehittämisessä muun muassa tehokkuuden tai laadun parantamisessa. Mittaustiedot kuvaavat nykytilaa ja kehityssuuntaa, ja ne auttavat näkemään miten hyvin tavoitteet saavutetaan. Mittarien tulisi tuottaa mahdollisimman luotettavaa ja päätöksen tekoa helpottavaa tietoa. Samalla mittaamisen tulisi olla mahdollisimman helppoa ja vähän resursseja kuluttavaa, ettei mittaamisen kustannukset ylitä siitä saatavia hyötyjä. Ihan kaikkea ja mitä tahansa ei siis kannata mitata. Tämä nostaa esille kysymyksiä siitä, miten mittarit tulisi valita ja toteuttaa.

Mittaaminen voi kohdistua joko tekemisen prosessiin tai sen tuottamiin tuloksiin. Tuloksiin liittyvät mittarit kertovat organisaation tilanteesta suoraan, kun taas prosessiin liittyvät mittarit kuvaavat niiden asioiden ominaisuuksia, jotka ovat *edellytyksiä* tulosten aikaansaamiselle. Hyvät tulokset prosessin mittaamisessa eivät välttämättä tarkoita hyviä prosessin tuloksia, mutta on

huomattava, että tuloksiin vaikutetaan prosessin kautta, jonka vuoksi tekemisprosessin mittaaminen on tärkeää.

Tietoturvan tapauksessa mittaaminen kohdistuu joko siihen, miten tietoturvallisuuden prosessit ja tietoturvakontrollit on toteutettu tai siihen, mikä on tietoturvallisuuden taso, toisin sanoen miten hyvin tiedon turvaamisessa ja erityisesti luottamuksellisuuden, eheyden ja saatavuuden turvaamisessa on onnistuttu.

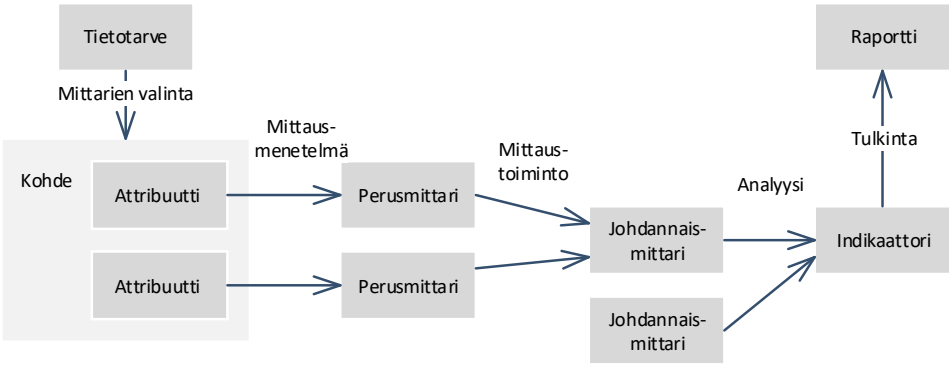
Tietoturvan mittaamisella pyritään vastaamaan muun muassa kysymyksiin: toimimmeko riittävän turvallisesti, mitkä ovat vahvimmat ja heikoimmat kohdat turvallisuudessamme, käytämmekö liian vähän tai liian paljon rahaa tietoturvainvestointeihimme, onko turvallisuusresurssimme oikein kohdennettu jne. (Hinson & Brotby 2016) Kehittääkseen tietoturvaansa systemaattisesti, organisaatio kytkee tietoturvamittarit strategiaansa tai esimerkiksi tietoturvapolitiikassa lausuttuihin tavoitteisiinsa.

4.1.2 ISO/IEC 27004 -standardi

ISO/IEC 27004 -standardi on osa laajempaa kansainvälistä ISO/IEC 27000 -standardiperhettä ja se antaa ohjeita tietoturvan tason sekä prosessien ja hallintakeinojen vaikuttavuuden arvioimiseen. Mittaaminen liittyy ISO/IEC 27001 -standardinmukaisen tietoturvallisuuden hallintajärjestelmän (TTHJ) arviointitoimintaan, johon sisältyvät myös sisäiset auditoinnit ja johdon katselmukset. ISO/IEC 27001 määrittää vaatimukset, joiden mukaan organisaation tulee määrittää mitä sen täytyy seurata ja mitata, ja millä menetelmillä se aikoo seurannan, mittaamisen, analysoinnin ja arvioinnin toteuttaa. Lisäksi tulee määrittää, milloin mittaamiseen liittyviä toimia on tehtävä ja ketkä ovat vastuussa mittaamiseen liittyvien toimien suorittamisesta.

ISO/IEC 27004 -standardissa mittarit jakautuvat kahteen tyyppiin: *suorituskykymittareihin* (performance measures) ja *vaikuttavuusmittareihin* (effectiveness measures). Suorituskykymittarit ilmaisevat missä määrin tietoturvallisuuden prosessit ja hallintakeinot on toteutettu. Vaikuttavuusmittarit ilmaisevat suunniteltujen prosessien ja hallintakeinojen vaikutukset organisaation tietoturvatavoitteisiin. Niillä voidaan ilmaista esimerkiksi kustannushyötyjä tai asiakasluottamusta. TTHJ:n käyttöönotossa tulisi ensin toteuttaa suorituskykymittarit, ja kun niiden osalta tavoitetasoja saavutetaan, tulisi siirtyä enenevässä määrin vaikutusmittarien toteutukseen.

Kuva 10 esittää ISO/IEC 27004 -standardin mukaisen mittaamisen toiminnot ja tietomallin. Mittareiden valinta perustuu *tietotarpeisiin*, jotka määrittävät ketkä tarvitsevat tietoa, mitä tietoa ja mihin käyttötarkoitukseen. Kun tietotarve on selvä, voidaan toteuttaa mittarit eli valitaan kiinnostavien *kohteiden* ominaisuudet eli *attribuutit*, joita mitataan sekä *menettelyt*, joilla mittaustieto kerätään. Kerätty tieto varastoidaan, todennetaan ja analysoidaan. Lopuksi mittarien analyyseistä tuotetaan tietotarpeen mukainen raportti sidostahoille. Raportointi voidaan toteuttaa esimerkiksi tuloskorteilla, jotka koostuvat karkean tason *suoritusindikaattoreista*. Indikaattorit tuotetaan *perusmittarien* ja *johdannaismittarien* perusteella halutun algoritmin avulla.



Kuva 10 Mittauksen toiminnot ja tietomalli ISO/IEC 27004 -standardin mukaisesti

ISO/IEC 27004 -standardi kuvaa varsin kattavasti mitä asioita mittaukseen liittyen tulisi miettiä ja tehdä. Lisäksi se kytkeytyy muuhun standardiperheeseen, joka hyödyllistä silloin, kun organisaatio on toteuttanut ja mahdollisesti sertifioinut ISO/IEC 27001:n mukaisen TTHJ:n. Standardi sisältää myös 37 esimerkkimittaria, joka tarjoaa hyvän lähtökohdan omien mittarien laadintaan.

4.1.3 Hyvän mittarin kriteerit

Hyvän mittarin kriteereitä on kuvattu kirjallisuudessa lukuisia, ks. (Hermann 2007; Jaquith 2007; Chew et al. 2008; Hinson & Brotby 2016; Payne 2007). Eräs tunnetuimmista on SMART, jonka nimi tulee englannin kielisten sanojen alkukirjaimista (Wikipedia 2020; Payne 2007):

- S = specific
- M = measurable
- A = archievable, assignable, attainable jne.
- R = realistic, reasonable, relevant, repeatable, resourced jne.
- T = testable, time-dependent, time-related, trackable, jne.

Vaikka määritelmiä on useita, niissä nousee usein esille seuraavia ominaisuuksia (Barabanov 2011):

- Mittarin tulisi olla merkityksellinen organisaatiolle, johtamiselle ja tavoitteille. Tämä vaatimus kohdistuu niin itse tietosisällölle kuin myös tiedon esitystavalle. Vaikeaselkoinen mittari ei tue päätöksentekoa.
- Mittarin tulisi olla helppo ja edullinen toteuttaa eli sen toteuttamiskustannukset eivät tulisi ylittää siitä saatavia hyötyjä. Jos mittari on raskas, se voi viedä resursseja mittarin hyödyntämiseltä tai vielä huonommassa tilanteessa, tietoturvaprosessien toteuttamiselta.
- Mittarin tulisi tuottaa riittävän usein ja riittävän ajantasaista tietoa. Liian pitkä latenssi tai liian harvoin tuotettavat mittaustulokset vaikeuttavat toimenpiteiden vaikutusten arviointia.
- Mittarin tulisi olla objektiivinen eli sen tulee tuottaa oikeaa ja harhatonta tietoa todellisuudesta. Yleensä tämä tarkoittaa myös sitä, että mittarin tulisi tuottaa kvantitatiivista dataa, numeroarvoja, joilla on jokin yksikkö.
- Mittarin tulisi olla toistettava niin, että tulokset ovat vertailukelpoisia riippumatta siitä, milloin ne mitattu.

4.2 Havainnointikyvyn mittaaminen

Havainnointikyvyn määritelmä on varsin selkeä ja sisältää itsessään jo mittarin määritelmän. Havainnointikyky on todennäköisyys, jolla hyökkäys havaitaan. Havainnointikyky voidaan siis ilmaista lukuarvona, jonka maksimiarvo on 100 %, joka tarkoittaa, ettei yhtäkään hyökkäystä jää havaitsematta. Vaikka määritelmä on hyvin selkeä, miten havainnointikykyä todellisuudessa voidaan mitata? Toteutustapoina tarkastellaan kolmea eri vaihtoehtoa: päättelemällä todellisesta havaintotietovirrasta, testaamalla havainnointikyvykkyyttä tai johtamalla havainnointikyvykkyydestä.

Havainnointi tuottaa jatkuvana virtana tapahtumia, joista osa todetaan positiivisiksi ja osa niistä ilmaisee todellista hyökkäystä eli päätyy häiriöksi. Väärien negatiivisten tapahtumien määrää ei voida suoraan nähdä mistään, mutta yhtenä ratkaisuvaihtoehtona on historiatietojen hyödyntäminen: jälkikäteen havaitut tietomurrot paljastavat ainakin osan vääristä negatiivisista (Volksbank et al. 2017). Ongelmaksi muodostuu se, että näin päätelty mittari kertoo menneisyydestä, mutta ei välttämättä kerro mitään tämän hetken tilanteesta. Toinen ongelma on se, että on mahdollista ja jopa todennäköistä, ettei kaikkia onnistuneita hyökkäyksiä havaita jälkikäteenkään.

Havainnointikykyä voidaan arvioida hyödyntämällä murtotestausta (ETSI GS ISI 005 2015). Murtotestauksia käytetään muun muassa haavoittuvuuksien etsimiseen sekä turvakontrollien ja reagointikeinojen toimivuuden varmistamiseen, mutta yhtenä näkökulmana on testimurtojen havaitseminen. Havainnointikyky voidaan laskea siitä, montako hyökkäystä testijakson aikana havaittiin. Hyvin valmisteltu ja toteutettu testaus voi antaa varsin hyvän käsityksen havainnointikyvykkyydestä, mutta haasteena on toteuttaa todellisia uhkia vastaavia testitapauksia. Lisäksi haasteena on manuaalisesti toteutetun testauksen kertaluonteisuus. Usein testaus on kohtalainen ponnistus, joka toistetaan melko harvoin. Testauksen haasteena on vielä toistettavuus eli testejä ei välttämättä saada suoritettua joka kerta täsmälleen samalla tavalla.

Joissain tapauksissa havainnointikykyä voidaan testata simuloidulla ja koneellisesti ajetulla testidatalla (ETSI GS ISI 005 2015). Simuloinnin toteuttaminen edellyttää sensorilta tai valvottavalta kohteelta rajapintaa, johon on mahdollista syöttää testiaineistoa. Simuloinnin etuna on toistettavuus ja lisäksi testaus voidaan periaatteessa tehdä säännöllisesti. Toisto on samalla myös haaste; miten testiaineistoa ja testausajankohtia varioidaan niin, että testien vertailukelpoisuus säilyy. Yksittäistä sensoria on melko helppo testata, mutta kokonaisvaltaisen tilanteen luonti, jossa hyökkäys hyödyntää eri kohteita ja keinoja, on vaikeampi järjestää.

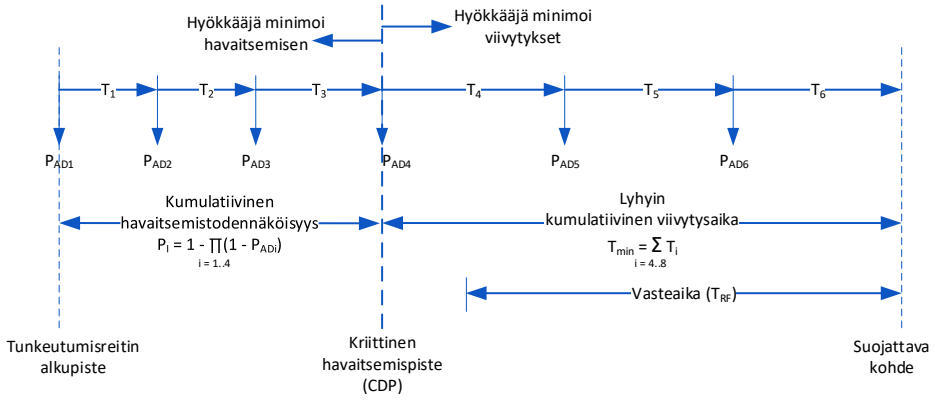
Havainnointikykyä voidaan arvioida havainnointikyvykkyyden perusteella. Mikäli voidaan luoda oikea kuva havainnointikyvykkyydestä, se kertoisi *mihin havainnointikyvyn tasoon olisi mahdollisuus päästä*. Toisin sanoen havainnointikyvykkyys ilmaisisi havainnointikyvyn enimmäisarvon. Havainnointikyvykkyyden tason määrittäminen ei kuitenkaan ole yksinkertainen

tehtävä ja yksiselitteisen vastauksen saaminen ei ole helppoa, kuten seuraavasta kohdassa nähdään. Lisäksi jäljelle jää kysymys ovatko käytettävissä olevat kyvykkyydet täysimääräisessä käytössä eli mikä on havainnointikyvyn todellinen taso.

Käytännön ratkaisu havainnointikyvyn mittaamiseen tai arvioimiseen on hyödyntää useampaa edellä kuvattua tekniikkaa. Isoimmiksi haasteiksi nousevat mittarin reaaliaikaisuus sekä mittarin toteuttamisen hinta.

Havainnointikykyyn liittyy havainnointitodennäköisyyden lisäksi havainnointiin käytettävä aika. Tällä tarkoitetaan aikaa, joka menee hyökkäyksen ensimmäisestä rekisteröidystä tapahtumasta siihen, että se todetaan hyökkäykseksi. Havainnointiajan tulisi olla sen verran lyhyt, että vasteelle jää riittävästi aikaa, toisin sanoen hyökkäys ehditään torjua ennen kuin hyökkääjä suorittaa tavoitteenaan olleen tehtävänsä.

Fyysisessä turvallisuudessa havainnointitodennäköisyydet ja vasteaika sekä hyökkäyksen etenemistä haittaavien viivytysten kestot ovat yleisiä suunnitteluparametreja turvajärjestelyjen suunnittelun arvioinnissa (ks. Kuva 11). Arvioinnissa lähdetään siitä, että hyökkääjän tunkeutumisreitti etenee pisteeltä pisteelle. Siirtyminen pisteiden välillä vie tietyn ajan (T_i) ja jokaisella pisteellä voi olla sensori, joka havaitsee tunkeutumisen tietyllä todennäköisyydellä (P_{ADi}). Lisäksi oletetaan, että vaste vie tietyn ajan (T_{RF}). Vasteajan ja viivytysten kestot määrittävät ns. kriittisen havaitsemispisteen (CDP), jossa hyökkääjä on viimeistään havaittava, jotta se voidaan torjua. Turvajärjestelyjen hyvyys määräytyy todennäköisyydestä, jolla hyökkääjä havaitaan kriittiseen havaitsemispisteeseen mennessä (P_I). (HAEA 2015)



Kuva 11 Fyysisten turvajärjestelyjen suorituskyvyn arviointi

Vaikka malli on tarkoitettu korkean turvallisuustason fyysisten turvajärjestelyjen suunnitteluun, se auttaa hahmottamaan, miten havainnointikyky lasketaan: havainnointi on tehtävä tietyssä aikaikkunassa tai sillä ei ole merkitystä hyökkäyksen torjumisen kannalta. Muilta osin mallin soveltaminen muihin turvallisuuden osa-alueisiin vaatii kuitenkin harkintaa. Fyysisessä turvallisuudessa on mahdollista määritellä kohtalaisella tarkkuudella viivytysten ja vasteen viemät vähimmäisajat, mutta esimerkiksi kyberturvallisuudessa niiden määrittäminen voi olla vaikeaa, kun vielä huomioidaan erilaiset hyökkäystavat ja kohteet.

4.3 Havainnointikyvykkyyden mittaaminen

Havainnointikyvykkyyden taso kuvaa havainnoinnin edellytysten tasoa. Havainnointikyvykkyys on staattisempi muuttuja kuin havainnointikyky, jonka taso riippuu osittain havainnointiin osallistuvien henkilöstön suoritustasosta. Havainnointikyvykkyyden peruselementtejä ovat havainnoinnin oikeellisuus, havainnointihenkilöstön osaaminen ja havainnon muodostamisaika.

Havainnoinnin oikeellisuus koostuu havainnoinnin kattavuudesta ja havainnoinnin tasosta. Kattavuutta tarkastellaan organisaation näkökulmasta - miten kattavasti havainnointi on järjestetty huomioiden suojattavat kohteet, eri tyyppiset uhkat, hyökkäysavaruudet ja havainnointiprosessin vaiheet. Havainnoinnin tasolla tarkoitetaan sitä, miten hyvään havainnoinnin varmuuteen käytetyllä havainnointivälineistöllä on mahdollisuus päästä.

Henkilöstön osaaminen koostuu useasta eri osa-alueesta, esimerkiksi miten hyvin havaintoja osataan tulkita, miten hyvin analysointivälineitä osataan käyttää, mitkä asiat liittyvät toisiinsa jne.

Havainnon muodostamisaika riippuu siitä, onko havainnointi reaaliaikaista, mikä on havainnoinnin automaatioaste ja kuinka toimivia ja tehokkaita analysointivälineet ovat. Muodostamisaika saavuttaa parhaimman arvonsa, jos havainto voidaan jalostaa reaaliaikaisesti havainnoijalle selkeänä hyökkäyksen ilmaisuna, jonka todentaminen on triviaalia.

4.4 Viitekehyksiä

Tässä kohdassa kuvataan viitekehyksiä, joissa on käsitelty havainnoinnin tasoa, havainnointikykyä tai havainnointikyvykkyyttä.

4.4.1 ISO/IEC 27004 -standardin esimerkkimittarit

Aiemmin tässä luvussa esitelty ISO/IEC 27004 -standardi esittelee liitteessä B 36 esimerkkimittaria, joista tietoturvatapahtumien ja -häiriöiden hallintaan liittyvät:

- B.15 Sosiaaliseen manipulointiin varautuminen: Testataan käyttäjien reagointia manipulointiin tähtäävissä hyökkäyksissä. Lasketaan kaavalla A + (1 - B) + C = D, jossa A on linkin napsuttelijoiden osuus, B on asianmukaisesti raportoineiden osuus, C on linkistä saatujen ohjeiden noudattaneiden osuus.
- B.20 Fyysisen kulunvalvonnan vaikuttavuus: Luvattomien pääsyjen määrä tietojärjestelmiä sisältävissä toimitiloissa. Tätä voi verrata turvallisuushäiriöiden kokonaismäärään.
- B.23 Haittaohjelmilta suojautuminen: Havaittujen ja torjumatta jääneiden hyökkäysten lukumäärän kehityssuunta (tulisi olla laskeva tai tasainen).
- B.27 Lokitiedostojen katselmointi: Katselmoitujen lokitiedostojen määrä määritellyllä ajanjaksolla. Tämän arvioimiseksi tulee määrittää kuinka usein mitäkin lokia pitäisi katselmoida (päivittäin - kuukausittain).
- B.29 Tunkeutumistestaus ja haavoittuvuuksien arviointi: Niiden kriittisten tietojärjestelmien prosenttiosuus, joille on suoritettu tunkeutumistestaus tai haavoittuvuuksien arviointi edellisen merkittävän päivityksen jälkeen.
- B.34 Turvallisuushäiriöiden kehityssuunnat: Tietoturvahäiriöiden lukumäärä määritellyllä ajanjaksolla (esim. kuukaudessa), mahdollisesti jaoteltuna häiriöluokittain.
- B.35 Tietoturvatapahtumien raportointi: Ihmisten raportoimien tietoturvahäiriöiden määrä esimerkiksi vuodessa.
- B.37 Haavoittuvuusarvioinnin kattavuus: Niiden järjestelmien, joiden haavoittuvuutta on testattu viimeisen ajanjakson (neljännes vuosi - vuosi) aikana, suhde järjestelmien kokonaismäärään.

Havaintomäärään ja sitä kautta epäsuorasti havainnointikykyyn viittaavia mittareita ovat B.20, B.23, B.34 ja B.35, havainnointikykyä kuvaavia mittareita on ainoastaan B.15 ja havainnointikyvykkyyden tasoon viittaavia mittareita ovat B.27, B.29 ja B.37.

4.4.2 ETSI GS ISI

Information Security Indicators (ISI) on ETSIn (European Telecommunications Standards Institute) teollisuusryhmän standardoima kehikko tietoturvatapahtumien havainnoinnin kvalitatiiviseen ja kvantitatiiviseen arviointiin. ISI:n kehittäminen on aloitettu 2011 ja siihen on osallistunut eri toimijoita Euroopan alueelta (ETSI 2016). Mukana on ollut yritysmaailmasta muun muassa Airbus ja Thales. Standardi viittaa ISO/IEC 27000 -standardisarjaan ja ISO/IEC on ollut mukana standardointityössä tarkkailijana (ETSI 2020).

Havainnointikyvykkyyden näkökulmasta mielenkiintoisimmat ETSI GS ISI -julkaisut ovat:

- ISI 001-1 Indicators; Part 1. Kehikon yleiskuvaus ja indikaattorien esittely.
- ISI 001-2 Indicators; Part 2. Opas operatiivisten indikaattoreiden valintaan.
- ISI 002 Event Model. Tietoturvatapahtumien luokittelumalli.
- ISI 003 Maturity. Menettely tapahtumahavainnoinnin kypsyystason arvioimiseen.
- ISI 005 Event Testing. Havainnointimekanismien vaikuttavuuden testausmenetelmä.

ISI 001-1 antaa yleiskuvan kehikosta ja kuvaa lähes sata erilaista indikaattoria liittyen tietoturvahäiriöihin, haavoittuvuuksiin ja vaikutuksiin. Indikaattorit on järjestetty ISI-002:ssa esitetyn luokittelumallin mukaisesti ja jokaisesta indikaattorista on kuvattu indikaattorin synnyttävät perustapahtumat sekä niiden ominaisuudet, indikaattorin tuottamiseen liittyvät perus- ja johdannaismittarit, indikaattorin arvon muodostuminen, indikaattorin vertailuarvo perustuen eri organisaatioiden kokemuksiin sekä viittaukset ISO/IEC 27001:ssa kuvattuihin hallintakeinokategorioihin. (ETSI GS ISI 001-1 2015)

Kolmannes indikaattoreista liittyy mahdollisiin pahatahtoisiin toimiin. Yhtenä esimerkkinä tällaisesta indikaattorista on IEX_INT.1, joka kertoo ulkopuolta käytettävien palvelimien hyökkäysyritysten määrästä. Indikaattorin perustapahtumina ovat IDS- tai SIEM-järjestelmien havainnot, jotka ilmaisevat järjestelmällistä palvelimien skannausta tai palvelimille lähetettyjä epäi-

lyttäviä pyyntöjä. Indikaattorin kuvauksessa esitetään perustapahtumien ilmaantumistiheyden olevan korkea ja havaitsemisen mahdolliseksi saavuttamistasoksi parhaimmillaan 60 - 70 %.

ISI 001-2 kuvaa muun muassa ISO/IEC 27002 -standardin hallintakeinoihin liittyviä häiriö- ja haavoittuvuusindikaattoreita. Julkaisu kytkee indikaattorit myös COBIT:iin ja ISO/IEC 20000:een. (ETSI GS ISI 001-2 2015)

ISI 002 kuvaa häiriöiden ja haavoittuvuuksien luokittelumallin ja taksonomian. Häiriöt jaetaan ulkoisiin hyökkäyksiin, vikoihin ja poikkeaviin sisäisiin tapahtumiin. Haavoittuvuudet jaetaan toimintatapa-, ohjelmisto- ja konfiguraatiohaavoittuvuuksiin sekä yleisiin turvallisuushaavoittuvuuksiin. Edellä kuvatut kategoriat jaetaan alikategorioihin ja edelleen perheisiin, jotka koostuvat yhdestä tai useammasta indikaattorista. Taksonomia kuvaa häiriöiden ja haavoittuvuuksien tiedot. Esimerkiksi häiriöön liittyviä aihealueita ovat aiheuttaja tai syy, häiriön kuvaus, keinot häiriön aikaansaamiseksi, häiriön tilanne, hyödynnetyt haavoittuvuudet, kohdetyypit, vaikutus tietoturvallisuustavoitteisiin ja vaikutus organisaation toimintaan. (ETSI GS ISI 002 2015)

ISI 003:ssa arvioidaan organisaation havainnoinnin tehokkuutta ja kypsyystasoa kahdeksan KPSI:n (key performance security indicator) kautta. KPSI:t arvioivat organisaation havainnointi- ja reagointikypsyyttä kokonaisuutena ja kertovat kyvystä ja tasosta havaita ISI-001:ssä kuvattuihin indikaattoreihin liittyviä tapahtumia. Kypsyystasoja on yhteensä kolme: tasolla 1 toiminta on vaatimusten mukaista ja tuki forensiikalle on olemassa, tasolla 2 on kyky havaita kattavasti tunnettuja hyökkäyksiä ja reagoida niihin ja tasolla 3 valvonta on kattavaa ja koko organisaatio on tietoinen tietoturvauhkista. KPSI:stä erityisesti 5, 6 ja 8 eli lokien keruu, analysointi ja arkistointi, tietoturvaosaaminen ja -koulutukset sekä tiedon menetyksen estäminen liittyvät selkeästi havainnointikyvykkyyteen. (ETSI GS ISI 003 2018)

ISI 005 kuvaa menettelyn tietoturvatapahtumien havainnointikyvykkyyden arviointiin testaamalla. Testaus voi tuottaa kvantitatiivisia tuloksia kuten esimerkiksi kohdeympäristön havaitsemistaso ja aiheettomien hälytysten määrä tietyllä ajanhetkellä. Testaus voi tuottaa myös kvalitatiivisia tuloksia, kuten esimerkiksi tietoa havaittavista tapahtumatyypeistä. (ETSI GS ISI 005 2015)

Dokumentti tuo esille erilaisia strategioita testauksen suorittamiseksi. Testaus voidaan tehdä eriytetyssä ympäristössä tai normaalisti toiminnassa olevassa ympäristössä. Testaus voidaan tehdä aktiivisesti tai passiivisesti. Aktiivisessa testaustavassa käytetään testidataa, kun taas passiivisessa testaustavassa odotetaan oikean tapahtuman ilmaantumista. Aktiivisessa testauksessa tarvitaan testimateriaalia, joka kuvastaa normaalia ja hyväksyttyä käyttäytymistä. Pelkästään tällaisella materiaalilla voidaan paljastaa paljonko valvontajärjestelmät tuottavat vääriä positiivisia havaintoja. Havainnointikyvykkyyden testaamiseksi testimateriaaliin generoidaan joko erilaisia tietoturvatapahtumia, havaintoja tietoturvatapahtumien mahdollisista vaikutuksista (esimerkiksi tiedostojen muutoksia) tai hälytyksiä, jos tapahtumien generointi tai olemassa olevien järjestelmien käyttö testaukseen on vaikeaa.

Testauksen toteuttamiseksi dokumentti esittää penetraatiotestausta, henkilöstön osallistuttamista tekemään vääriä tai huolimattomia toimenpiteitä, tunnettujen haavoittuvuuksien hyväksikäyttöä ja murtovälineiden käyttöä. Tavallisesti penetraatiotestauksessa testaajalla on vapaat kädet tehdä mitä tahansa onnistuakseen murtautumisessa. Havainnointikyvykkyyden arvioimiseksi penetraatiotestiin pyritään tuottamaan tapauksia, jotka havainnointimekanismien tulisi havaita. Käyttäjien ja erityisesti ylläpitäjien osallistumisella voidaan tuottaa erilaisia tietoturvatapahtumia ja niiden aiheuttamia vaikutuksia. Henkilöstön osallistuttaminen vaatii huolellista valmistelua, jotta ei aiheuta todellista vakavaa varaa tietojenkäsittely-ympäristölle. Havainnointikyvyn testausta voidaan helpottaa käyttämällä kohteessa tunnettuja haavoittuvuuksia sisältäviä järjestelmiä tai hunajapurkkeja (honeypots). Myös tällöin on huolehdittava siitä, ettei kohdeympäristöä samalla altisteta todellisille hyökkäyksille.

4.4.3 SEI Incident Management Capability Assessment

Tämä alakohta perustuu lähteeseen (Dorofee et al. 2018). Software Engineering Instituten (SEI) julkaisema Incident Management Capability Assessment (IMCA) on menetelmä organisaation häiriönhallinnan käytäntöjen arviointiin. Menetelmä on kehitetty alun perin Yhdysvaltain liittovaltion virastojen tietoturvapalveluntarjoajien arviointia varten. Edeltävä versio julkaistiin nimellä Incident Management Capability Metrics v0.1.

Menetelmä arvioi häiriönhallinnan käynnistämiseen, suojautumiseen, havainnointiin, vasteeseen ja ylläpitoon liittyviä kyvykkyyksiä. Kyvykkyydellä

tarkoitetaan ihmisiä, prosesseja sekä teknologiaa, jotka tarjoavat valmiudet tai ominaisuudet jonkun tehtävän suorittamiseen. Menetelmällä ei voida mitata kuinka hyvin häiriönhallintaa suoritetaan, ainoastaan sen, että sitä suoritetaan.

Kyvykkyydet on jaettu perustamiseen, suojautumiseen, havainnointiin, reagointiin ja ylläpitoon. Jokaisella kyvykkyydellä on indikaattoreita, jotka arvioivat kyseisen kyvykkyyden suorituskykyä. Indikaattorit on jaettu kolmeen ryhmään: pakolliset, suositeltavat käytännöt sekä vakiinnuttaminen ja laadunparannukset. Pakollisten indikaattorien tulee täyttyä, jotta kyvykkyys voidaan saavuttaa. Suositeltavat käytännöt parantavat kyvykkyyden tasoa. Vakiinnuttamisella ja laadunparannuksissa varmistetaan toiminnan jatkuvuutta.

Indikaattoreita on neljää lajia: perusedellytykset, kontrollit, aktiviteetit ja laatuindikaattorit. Perusedellytysten tulee täyttyä, jotta kyvykkyyttä voidaan ylipäänsä suorittaa. Kontrollit ohjaavat aktiviteettien toteuttamista. Laatuindikaattorit kertovat vaikuttavuudesta, täysimääräisyydestä, käyttökelpoisuudesta, vakiinnuttamisesta tai muista aktiviteetteihin liittyvistä laatunäkökulmista.

Menetelmällä voidaan arvioita häiriönhallintaa kokonaisuutena tai keskittyen yksittäiseen osa-alueeseen. Kyvykkyyksiä arvioidaan haastatteluilla, demonstraatioilla, tarkkailemalla tai dokumenttikatselmuksilla. Haastattelussa arvioija käy häiriönhallintatiimin kanssa läpi kyvykkyyksiä kysymys-vastaus -periaatteella. Demonstraatioissa arviointitiimi luo kuvitteellisia tilanteita, joita käydään läpi vuorovaikutteisesti häiriönhallintatiimin kanssa. Läpikäynnissä arvioijat tekevät havaintoja kyvykkyydestä reagoinnin, työkalujen käytön tai kysymysten vastausten perusteella. Tarkkailussa arvioija tutkii kohdetiimin toimintaa todellisissa tilanteissa. Dokumenttikatselmuksien kautta saadaan täydentävää tietoa kyvykkyyksistä. Läpikäynnin perusteella indikaattori merkitään saavutetuksi tai täyttymättä jääneeksi.

Havainnointiin liittyvät kyvykkyydet on jaettu kolmeen alikategoriaan: verkon ja järjestelmien tietoturvavalvonta, häiriöinformaation ulkoiset lähteet, uhka- ja tilannetietoisuus. Tietoturvavalvonnalla tarkoitetaan organisaatioon omaa kykyä havaita tietojärjestelmiinsä kohdistuvaa epäilyttävää toimintaa. Ulkoisilla lähteillä tarkoitetaan kykyä vastaanottaa tietoa häiriöistä, joita ulkopuolinen turvallisuusvalvonta tai esimerkiksi yksittäinen käyttäjä raportoi.

Uhka- ja tilannetietoisuudella tarkoitetaan teknologiaseurantaa, avoimien lähteiden valvontaa, konfiguraatioiden ja haavoittuvuuksien läpikäyntiä ja muita proaktiivisen seurannan keinoja.

Verkon ja järjestelmien tietoturvavalvonta -osio koostuu yhdeksästä pakollisesti kontrolli- ja aktiviteetti-indikaattorista, yhdeksästä suositeltavat käytännöt -indikaattorista ja viidestä vakiinnuttaminen ja laadunparannukset -indikaattorista. Esimerkki pakollisesta kontrolli-indikaattorista on, että tulee olla olemassa kriteerit luonnehtia poikkeavia tapahtumia (epäilyttävien porttien, protokollien ja palveluiden käyttöä).

Menetelmä antaa hyvin karkean kuvan havainnointikyvykkyydestä. Koska kyseessä on arviointimenetelmä, se perustuu manuaaliseen työhön, eikä saatu kuva ole reaaliaikainen. Menetelmällä voidaan kuitenkin saada aikaan käsitys perusvaatimusten täyttymisen asteesta ja kehityskohteista. Ansiokasta on myös, että menetelmä tuo esille ihmisten ja prosessien merkityksen kyvykkyydelle.

4.4.4 Management, Growth and Metrics & Assessment (MaGMa)

Tämä alakohta perustuu lähteeseen (Volksbank et al. 2017). Hollantilaisten rahoituslaitosten tiedonvaihtoyhteisön (FI-ISAC) yhteistyönä laatima MaGMa käyttötapauskehikko kuvaa mallin tietoturvavalvontakäyttötapausten tietämyksenvaihtoon. Nimi MaGMa tulee sanoista Management, Growth and Metrics & assessment.

Kehikko kuvaa käyttötapausmallin ja sen käyttämisen lisäksi menettelyt kyvykkyyden ja kypsyyden arviointiin sekä käyttötapauksiin liittyvää mittaristoa. *Kyvykkyydellä* tarkoitetaan tässä yhteydessä SOC:n kykyä havaita uhkia. *Kypsyydellä* tarkoitetaan toiminnan tasaisuutta, toistettavuutta ja tehokkuutta. Mittareilla arvioidaan käyttötapauskehikon vaikuttavuutta eli kykyä tuottaa optimaalista tietoturvavalvontaa.

Kyvykkyys koostuu monitasoisesta havaitsemismekanismeista, kehittyneistä työkaluista ja ammattitaitoisista henkilöistä. Käyttötapauksien tapauksessa kyvykkyyttä voidaan kehittää kehikon kattavuuden eli käyttötapausten määrän suuntaan tai käyttötapausten kattavuuden suuntaan. Käyttötapauksen kattavuutta voi kasvattaa lisäämällä valvottavia kohteita, lisäämällä uusia kohdetyyppejä tai lisäämällä valvontasääntöjä.

MaGMa viittaa CMMI:n määrittämiin kypsyystasoihin: kaoottinen, toistettava, määritelty, hallittu ja optimoiva. Kypsyyteen vaikuttavia tekijöitä ovat muun muassa dokumentointi, standardien käyttö, määritellyt roolit ja vastuut, tekemisen ja tuotosten jäsentäminen, tavoitteiden asettaminen ja mittaaminen.

MaGMa korostaa, ettei ole olemassa yhtä optimaalista kypsyystasoa, vaan se riippuu muun muassa organisaation toiminnasta ja valvontaan liittyvästä ambitiotasosta. Vastaavasti kyvykkyydelläkään ei ole yhtä optimaalista tasoa, joihin kaikkien pitäisi pyrkiä. Laaja käyttötapausten määrä ja kattavuus vaativat paljon ylläpitotyötä. Jos ylläpito jää tekemättä, havaintojen laatu kärsii, ja jos ylläpitoon käytetään paljon aikaa, se voi olla pois analysointiin käytettävästä ajasta.

MaGMan mittaristo koostuu sisäänrakennetuista mittareista, ohjausmittareista ja tulosmittareista. Sisäänrakennetut mittarit tarjoavat tietoa käyttötapauskehikon vaikuttavuudesta. Ohjausmittarit kertovat kehikon hallinnasta. Tulosmittarit keskittyvät kehikon tuottamiin tuloksiin.

Sisäänrakennettuja mittareita ovat tehokkuus, toteutuksen taso, kattavuus, paino ja potentiaali. *Tehokkuus* ilmaisee havaitsemismekanismin kyvystä tehdä havaintoja, esimerkiksi salattua tietoliikennettä ei kyetä kovin tehokkaasti valvomaan, jos salausta ei pystytä purkamaan. Tehokkuus on ominainen havaitsemismekanismille, eikä sitä voida säätämällä tai kattavuutta parantamalla muuttaa. *Toteutuksen taso* kertoo havaitsemismekanismin toteutuksen hyvyydestä, esimerkiksi havaitsemissäännön hienosäätö parantaa toteutuksen tasoa. *Kattavuus* kuvaa kuinka kattavasti havaitsemismekanismi havainnoi ilmiötä. *Paino* on johdettu mittari, joka lasketaan tehokkuuden, toteutuksen tason ja kattavuuden perusteella. *Potentiaali* on myös johdettu mittari, joka lasketaan tehokkuuden ja painon erotuksen perusteella.

Ohjausmittareita ovat kehikkoon kohdistuneiden muutoksien määrä, käyttötapausten määrän kasvu, painon kasvu ja potentiaalin muutos. Ohjausmittarien määrittäminen perustuu kehikon muutosten seurantaan ja käyttötapausten määrään sekä sisäänrakennettujen mittarien arvoihin.

Tulosmittareita ovat hälytysten määrä, häiriöiden määrä, väärien positiivisten suhde ja väärien negatiivisten määrä. Viimeksi mainitulla mittarilla tarkoitetaan häiriöitä, jotka havaitaan häiriönhallintaprosessissa, mutta joita ei havaittu havainnointimekanismeilla.

MaGMa tarjoaa varsin kattavan havainnointia koskevan arviointi- ja mittarikokonaisuuden, jonka pohjalta organisaation kokonaishavainnointikyvykkyys voisi olla mahdollista määrittää. MaGMaan sisältyy excel-väline sisäänrakennettujen mittarien määrittämistä ja käsittelyä varten. Väline tarjoaa erilaisia indikaattoreita, kuten esimerkiksi keskiarvoja tai mittarien arvoja käyttötapauksittain. Mittarien arvot määritetään manuaalisesti, joten menettely ei tarjoa reaaliaikaista tietoa käyttötapauskehikosta. Mittarien käytön haasteena voi olla myös kvantitatiivisten arvojen määrittäminen tehokkuudelle tai toteutuksen tasolle.

4.4.5 SOC-CMM

Tämä alakohta perustuu lähteeseen (Os 2018). SOC-CMM on Rob van Osin Luleån yliopiston tutkimushankkeessa kehittämä turvallisuusoperaatiokeskusten kyvykkyyden ja kypsyyden arviointiin tarkoitettu malli. Malliin sisältyy myös itsearviointityökalu, jota SOC-tiimit voivat käyttää oman toimintansa arviointiin. Mallissa tarkastellaan SOC:n toimintaa viiden osa-alueen kautta: liiketoiminta, ihmiset, prosessi, teknologia ja palvelut. Kukin osa-alue koostuu edelleen aspekteista.

Malli kuvaa viisi kypsyystasoa ja kolme kyvykkyystasoa. Kypsyystasoja käytetään kaikkien osa-alueiden kanssa, mutta kyvykkyystasoja sovelletaan vain teknologia- ja palvelut-osa-alueisiin.

Malli tuottaa tutkakaavion kypsyyksistä ja kyvykkyyksistä. Lisäksi työkalu sisältää nykyisellään myös tulosten esittämisen NISTin Cyber Security Frameworkin esittämiä tietoturvatoimintojen kategorioita vasten.

Tärkeimmät havainnointikyvykkyyteen liittyvät osa-alueet ja aspektit ovat:

- Teknologiat: SIEM- ja IDPS-järjestelmät sekä tietoturva-analytiikka.
- Palvelut: tietoturvavalvonta, tietoturvahäiriöidenhallinta, tietoturva-analysointi ja -forensiikka, uhkatiedustelu, uhkien metsästys, haavoittuvuuksienhallinta, lokienhallinta.

4.5 Viitekehysten vertailua

Viitekehyksissä kuvatut arviointimallit lähestyvät havainnointikykyä ja -kyvykkyyttä eri lähtökohdista. Mallien ominaisuuksia on vertailtu ao. taulukoissa (ks. Taulukko 5, Taulukko 6, Taulukko 7, ja Taulukko 8) ETSI-julkaisuja ISI 001-1, ISI 003 ja ISI 005 tarkastellaan erikseen.

Taulukko 5 kuvaa lyhyesti viitekehyksen keskeisen sisällön ja ajatusmallin.

Taulukko 6 kuvaa millä tavoin viitekehyksessä toteutuu havainnointikyvyn mittaaminen. Vaihtoehtoja ovat päättely havaintovirrasta, testaaminen tai päättely havainnointikyvykkyydestä.

Taulukko 7 kuvaa mitä suureita viitekehys tarkastelee havainnointikyvykkyyteen liittyen eli millä tavoin malli käy läpi havainnoinnin kattavuutta, teknistä kykyä tuottaa oikeita havaintoja, välineiden suorituskykyä ja henkilöstön osaamista.

Taulukko 8 kuvaa viitekehyksen tarjoamien mittarien laatua suhteessa hyvän mittarin kriteereihin: toteutettavuus, ajantasaisuus, objektiivisuus ja toistettavuus. Merkityksellisyyttä ei tässä erikseen arvioida, koska mittarien soveltuvuutta on tarkasteltu taulukoissa 6 ja 7 esitettyjen kohtien kautta.

Taulukko 5 Arviointiviitekehysten vertailua.

Arvioitava asia	ISO/IEC 27004, liite B	ISI Indicators (ISI 001)	ISI Maturity (ISI 003)	ISI Event Testing (ISI 005)	SEI IMCA	MaGMa	SOC-CMM
Mittausmenetelmä vai arviointiprosessi?	Tietoturvamittari-esimerkkejä, joista 8 liittyy havaintoihin ja häiriönhallintaan	Mittaristo häiriöiden ja haavoittuvuuksien havaitsemiseen liittyen	Havainnointikyvykkyyden kypsyyden arviointimenetelmä	Menetelmä havainnointikyvykkyyden testaamiseksi	Menetelmä häiriönhallinnan kyvykkyyksien arvioimiseksi	Käyttötapauskehikko ja siihen liittyvä kyvykkyyden, kypsyyden ja mittaamisen menettely	SOC:n toiminnan kypsyyden ja kyvykkyyden arviointimenetelmä

Taulukko 6 Havainnointikyvyn mittaamisen keinot eri viitekehyksissä

Arvioitava asia	ISO/IEC 27004, liite B	ISI Indicators (ISI 001)	ISI Maturity (ISI 003)	ISI Event Testing (ISI 005)	SEI IMCA	MaGMa	SOC-CMM
Päättely havaintovirrasta	Yksi esimerkkimittari	Perustuu indikaattorin tuottaman arvon vertaamiseen kuvauksessa esitettyyn state-of-the-art -arvoon	Ei	Kyllä	Ei	Kyllä, kun yhdistetään tietoon toteutuneista, mutta ei (ajallaan) havaituista häiriöistä	Ei
Testaaminen	Ei	Ei	Ei	Kyllä	Ei	Ei	Ei
Päättely havainnointikyvykkyydestä	Ei	Ei	Voidaan yhdessä ISI 001:n kanssa mahdollisesti arvioida	Ei	Ei	Ei	Ei

Taulukko 7 Havainnointikyvykkyyden mittaamisen suureet eri viitekehyksissä

Arvioitava asia	ISO/IEC 27004, liite B	ISI Indicators (ISI 001)	ISI Maturity (ISI 003)	ISI Event Testing (ISI 005)	SEI IMCA	MaGMa	SOC-CMM
Kattavuus (eri dimensiot)	Kolme esimerkkimittaria: lokit, kriittiset tietojärjestelmät, tietojärjestelmät yleensä	Ei	Ohjelmistot, laitteet, haavoittuvuudet, käyttäjien pääsy	Riippuu mitä otetaan testaukseen, mutta periaatteessa tietoverkko, päätelaitteet, tilat ja ihmiset	Poikkeamien tunnistuskriteerit, verkot ja järjestelmät, valvontamenettelyt	Käyttötapaukset (hyökkäyksen vaiheet, taktiikat, tekniikat), lokilähteet, havaitsemistekniikka, kohteet (käyttäjät, järjestelmät, sovellukset, tietoverkot, toimipisteet)	Teknologiat (SIEM, IDS, analytiikka)
Tekninen kyky tuottaa oikeita havaintoja (säädöt, laatu)	Ei	Ei suoranaisesti	Ei	Kyllä	Ei	Tehokkuus, toteutuksen taso	Säädetäänkö jatkuvasti, väärien positiivisten aktiivinen poisto
Havainnon muodostamisaika (havainnoinnin reaaliaikaisuus, automaatioaste, välineiden tehokkuus)	Ei	Ei suoranaisesti	Ei	Testaus suoritetaan tietyssä aikaraamissa	Lokianalyysi, korrelaatiovälineet, reaaliaikainen valvonta, automaattiset hälytykset, reaaliaikaisuuskriteerit	Ei	Havainnoinnin reaaliaikaisuus, työkalujen tehokkuus, käyttötaito,
Henkilöiden osaaminen (eri vaiheet, kohteet, uhkat, välineet, havainnot)	Ei	Ei	Kyllä, mutta ei ole eritelty taitoja	Ei suoranaisesti	Välineet, havainnot	Ei	Välineosaaminen, koulutukset yleensä, onko eri rooleihin henkilöitä

Taulukko 8 Viitekehysten mittarien ominaisuuksien vertailua

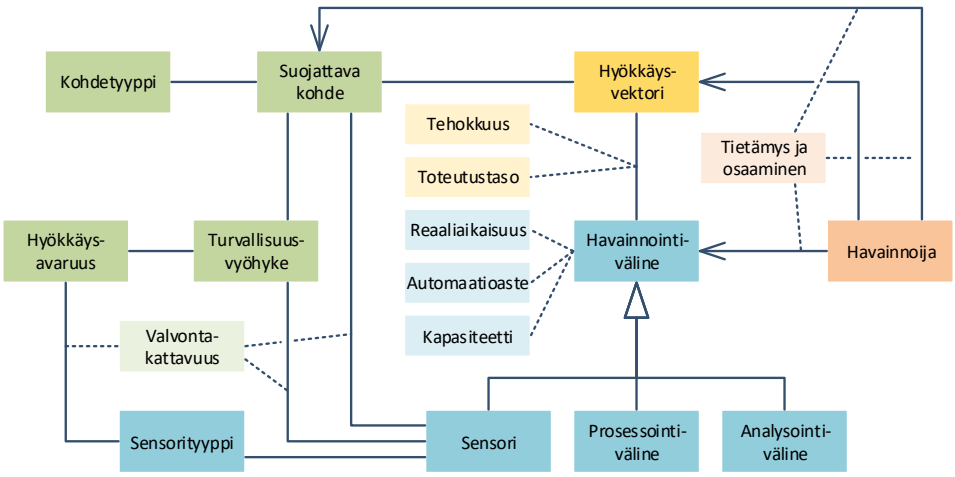
Arvioitava asia	ISO/IEC 27004, liite B	ISI Indicators (ISI 001)	ISI Maturity (ISI 003)	ISI Event Testing (ISI 005)	SEI IMCA	MaGMa	SOC-CMM
Mittarien toteutettavuus (työmäärä)	Matala	Indikaattorien toteuttaminen iso työ, sen jälkeen automaattista ja tulkinta kohtalainen työ	Manuaalinen, melko kevyt	Kohtalaisesti manuaalista työtä joka testauskerralla	Manuaalinen, melko kevyt	Käyttötapauskehikon ja mittarien rakentaminen sekä arvojen määrittäminen kohtalaisen iso työ	Manuaalinen, kohtalainen
Mittarien ajantasaisuus	Päivä - vuosi	Päivä - kuukausi	Arvioinnin toistoväli (kuukausi tai enemmän)	Testien toistoväli (kvartaali tai enemmän)	Arvioinnin toistoväli (kuukausi tai enemmän)	Käyttötapauksiin liittyvät mittarit - arvioinnin toistoväli, hälytyksiin ja häiriöihin liittyvät reaaliaikaisia	Arvioinnin toistoväli (kvartaali tai enemmän)
Mittarien objektiivisuus, kvantitatiivisuus	Kyllä	Kyllä	Kvalitatiivinen	Kyllä	Kvalitatiivinen: indikaattorin ehto täyttyy / ei täyty	Semi-kvantitatiivinen, osittain subjektiivinen	Semi-kvantitatiivinen, subjektiivinen
Mittaamisen toistettavuus, tulosten vertailukelpoisuus	Kyllä	Kyllä	Kyllä	Haastava toteuttaa	Kyllä	Kyllä	Kyllä

4.6 Mittariston kokoaminen

Viitekehysten läpikäynnin yhteydessä voitiin havaita, että yksikään esitetyistä malleista ei tarjoa valmista mittaristoa havainnointikyvyn ja -kyvykkyyden mittaamiseen. Tässä kohdassa kuvataan mittariston muodostaminen ottaen huomioon tässä työssä kuvatut havainnointiin liittyvät näkökulmat sekä hyödyntäen viitekehyksissä esitettyjä hyödyllisiä ratkaisumalleja.

Mittariston kokoamisen lähtötietoina ovat tietotarpeet ja vaatimukset mittareille. Mittariston muodostamiseksi tulee myös tunnistaa mitattavat kohteet ja niihin liittyvät mitattavat ominaisuudet. Tämän jälkeen muodostetaan tietotarpeen tyydyttäviä indikaattoreita, jotka tuotetaan perus- ja johdannaismittareiden kautta.

Tietotarpeena on havainnointikyvykkyyden tason määrittäminen. Kuten aiemmin tässä työssä on ilmennyt, havainnointikyvykkyys koostuu monesta tekijästä, joita kuvattiin muun muassa luvussa 3 ja kohdassa 4.3. Kuva 12esittää havainnointikyvyn elementtejä ja niiden välisiä suhteita. Mitattavia kokonaisuuksia ovat valvonnan kattavuus, tekninen kyky havaita hyökkäys, välineistön suorituskyky ja henkilöstön tietämys ja osaaminen.



Kuva 12 Havainnointikyvykkyyden mittaamisen kohteet ja attribuutit

Taulukko 9 kuvaa havainnointikyvykkyyteen liittyviä mittareita. Jokaisesta mittarista esitetään mittarin kuvaus, mittarin arvoalue ja mittarin arvon muodostuminen. Mittarien toteuttamisessa on pyritty saavuttamaan hyvän mittarin ominaisuudet. Esimerkiksi mittarien tulokset ovat numeroarvoja. Kaikilta osin hyvän mittarien kriteereihin ei täysin päästä: monessa mittarissa joudutaan turvautumaan subjektiivisen arvion määrittämiseen. Tällaisten mittarien

tulosten tarkkuutta voidaan parantaa käyttämällä semi-kvantitatiivista arvoasteikkoa, jossa eri tasojen kriteerit on kuvattu mahdollisimman tarkasti.

Taulukko 9 Havainnointikyvykkyysmittarit

Mittarin kuvaus	Arvoalue	Arvon muodostaminen
Valvontakattavuus		
Hyökkäysavaruudet	0 - 6	Valvottujen hyökkäysavaruuksien määrä eli moneenko hyökkäysavaruuteen on ylipäänsä valvontakykyä
Valvottavat suojattavat kohteet	0 - 100 %	Kuinka suuri osa suojattavista kohteista on valvonnan piirissä kohdetyypeittäin ilmaistuna.
Sensorityypit / hyökkäysavaruus	0 - n	Montako erilaista sensorityyppiä on käytössä kussakin hyökkäysavaruudessa
Havainnointitapa / hyökkäysavaruus	0 - 2	Tunnistetaanko hyökkäysavaruudessa hyökkäykset tunnuspiirteiden ja/tai poikkeavan käyttäytymisen perusteella
Sensorityyppikohtainen kattavuus	0 - 100 %	Kuinka laajasti kyseistä sensorityyppiä käytetään kyseisessä hyökkäysavaruudessa
Turvallisuusvyöhykkeiden hyökkäysavaruudet	0 - 100 %	Suojattavat kohteet sijaitsevat eri turvallisuusvyöhykkeillä. Missä määrin jokaisen turvallisuusvyöhykkeen hyökkäysavaruudet valvottu?
Hyökkäysavaruuksien turvallisuusvyöhykkeet	0 - 100 %	Miten kattavasti eri hyökkäysavaruuksiin liittyvät turva-alueet on valvottu?
Tekninen kyky havaita hyökkäys		
Tehokkuus	0 - 100 %	Arvio välineistön sisäsyntyisestä kyvystä havaita hyökkäysvektori [Volksbank et al. 2017]
Toteutustaso	0 - 100 %	Arvio välineistön havainnointisääntöjen hyvyydestä havaita hyökkäysvektori [Volksbank et al. 2017]
Välineistön suorituskyky		
Havainnoinnin reaaliaikaisuus	0 tai 1	Kyky tuottaa havainto niin, että ehditään torjumaan hyökkäys ennen kuin se suoritetaan loppuun. Arvio tehdään havainnointivälineittäin
Automaatioaste	0 - 100 %	Kuinka pitkälle koneellisesti tuotetaan havainto analysoijalle / hälytysvalvojalle. 0 % = valvoja tekee täysin manuaalisesti havainnon, 100 % = havainto tuodaan esille merkityksen ja tarvittavien lisätietojen kera täydellisesti. Arvio tehdään havainnointivälineittäin
Välineistön suorituskyky ja kapasiteetti	0 - 100 %	Välineen kyky käsitellä kaikki tapahtumat ja säilyttää havaintoja vähintään niin kauan, että hyökkäys voidaan torjua. Arvio tehdään havainnointivälineittäin
Henkilöiden tietämys ja osaaminen		
Sensorin käyttöosaaminen	0 - 100 %	Henkilöstön kyky ottaa käyttöön, säätää ja ymmärtää sensorityypin tuottamia havaintoja
Havaintojen analysointiosaaminen	0 - 100 %	Kyky analysoida välineistön tuottamia havaintoja ja tunnistaa siitä epäilyttävää tai pahantahtoista toimintaa

Mittarin kuvaus	Arvoalue	Arvon muodostaminen
Suojattavien kohteiden tuntemus	0 - 100 %	Ymmärrys valvottavista kohteista. 0 % = ei mitään tietoa suojattavista kohteista, 100 % = kattavat tiedot kohteen merkityksestä organisaatiolle, kohteen normaalista käytöstä ja kohteeseen kohdistettujen hyökkäysten tunnistamisesta

5 Johtopäätökset ja yhteenveto

Havainnointi ja havainnointikyvykkyys on tunnistettu yhdeksi keskeisistä tekijöistä tieto- ja kyberturvallisuudessa. Vaikka panostukset suojaamiseen ja ennaltaehkäisyyn olisivatkin mittavat, jäljelle jää aina jäännösriski, että suojaukset kierretään tai ne pettävät.

Tässä työssä on käyty läpi erilaisia uhkia, hyökkäyksiä ja kykyä havaita niitä. Erilaisia havaitsemisvälineitä ja -mekanismeja on kehitetty runsaasti eri turvallisuuden alueille. Tämän vuoksi on ollut hämmentävää huomata, miten kehittymättömiä menetelmät ja välineistö havainnointikyvyn ja -kyvykkyyden arvioimiseen ovat. Millä muulla tavoin panostuksien vaikutusta havainnoinnin parantamiseksi voisi arvioida?

Työssä käytiin läpi viisi eri viitekehystä havainnointikyvyn ja -kyvykkyyden mittaamiseen tai arviointiin liittyen. Luultavasti eri malleja on olemassa paljon muitakin, mutta välttämättä ne eivät ole julkisesti saatavilla, vaan pysyvät organisaatioiden omana tietona. Yksikään esitetyistä viitekehyksistä ei sellaisenaan tarjoa riittävää pohjaa tieto- ja kyberhavainnointikyvyn ja -kyvykkyyden mittaamiseen, mutta eri menetelmiä yhdistelemällä on mahdollista luoda kattava mittaristo. Tällöin haasteeksi voi muodostua syntyneen mittariston kompleksisuus, jonka käyttö ja ylläpito voivat olla saatuun hyötyyn nähden liian raskaita. Tämä lienee yksi syy, miksi sopivia ja valmiita malleja on niin vähän tarjolla.

Lisäksi tieto- ja kyberhavainnointiin liittyvät mallit tarkastelevat hyökkäysavaruuksia suppeasti keskittyen tietoverkko-, päätelaite-, websovellus- ja sähköpostimaailmaan. Sellaisia malleja, jotka yhdistäisivät perinteisiin tieto- ja kyberhavainnointiin liittyviin mittareihin myös kattavasti fyysisen turvallisuuden, laitteistoturvallisuuden, toimitusketjuturvallisuuden ja henkilöstöturvallisuuden havainnointielementtejä, on vaikea löytää.

Työn lopussa esiteltiin periaatteellinen malli ja mittaristo havainnointikyvykkyyden tason arvioimiseksi. Mittaristo on mahdollista rakentaa hyödyntämällä erilaisia mahdollisesti olemassa olevia luetteloita ja tietokantoja, kuten esimerkiksi omaisuuden hallintaan liittyvää välineistöä tai käyttötapaustietokantaa. Systemaattisella suojattavan omaisuuden, valvontakoneiston ja uhkakuvan mallinnuksella, tietojen keruulla ja tietojen ylläpidolla voidaan luoda ajantasainen kokonaiskuva havainnointiin liittyvistä kyvykkyyksistä. Sivutuotteena saadaan ajantasainen kokonaiskuva nykyisten järjestelyjen suojauksen ja heikkouksien tasosta.

Havainnointikyvyn mittaaminen normaalin toiminnan ohessa luotettavasti on vaikeaa, koska pahantahtoisen toiminnan kokonaismäärää kaikesta toiminnasta ei välttämättä saada selville koskaan. Kohtalaisen hyvän kuvan voi saada testaamalla. Haasteeksi tällöin muodostuu riittävä testausosaaminen, riittävän autenttiset testausjärjestelyt ja -tilanteet sekä testauksen vaatima työmäärä. Havainnointikyvykkyyden taso kertoo miltä osin havainnointikyky on olemassa ja miltä osin se puuttuu. Tätä tietoa voidaan hyödyntää testauksen kohdentamisessa. Testauksen vaatimaa manuaalisen työn määrää voidaan myös keventää jakamalla testaus yksittäisten osa-alueiden ja välineiden testaukseen sekä hyödyntämällä automaattisia testausvälineitä.

Lähdeviitteet

1. Barabanov, Rostyslav, Stewart Kowalski, Louise Yngström. 2011. Information Security Metrics: State of Art. DSV Report series No 11-007.
2. Bezuidenhout, Monique, Francois Mouton, H.S. Venter. 2010. Social Engineering Attack Detection Model: SEADM. IEEE.
3. Bianco, David J. 2013. The pyramid of pain. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (haettu 7.7.2020)
4. BSI. 2013. IT-Grundschutz Catalogues, 13th version. Bundesamt für Sicherheit in der Informationstechnik
5. Bu, Zheng. 2014. Zero-Day Attacks are not the same as Zero-Day Vulnerabilities. FireEye. https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html, (haettu 6.6.2020)
6. Cambridge Dictionary. https://dictionary.cambridge.org/
7. Chew, Elisabeth, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, Will Robinson. 2008. Performance Measurement Guide for Information. NIST 800-55 Rev 1. National Institute of Standards and Technology.
8. Cichonski, Paul, Tom Millar, Tim Grance, Karen Scarfone. 2012. Computer Security Incident Handling Guide. NIST 800-61 Rev 2. National Institute of Standards and Technology.
9. Collins Online English Dictionary. https://www.collinsdictionary.com/dictionary/english
10. Dorofee, Audrey, Robin Ruefle, Mark Zajicek, David McIntire, Christopher Alberts, Samuel Perl, Carly Lauren Huth, Pennie Walters. 2018. Incident Management Capability Assessment. Technical Report. CMU/SEI-2018-TR-007. Carnegie Mellon University (CMU), Software Engineering Institute (SEI)
11. Duggan, D. P., S. R. Thomas, C. K. K. Veitch, and L. Woodard. 2007. Categorizing Threat: Building and Using a Generic Threat Matrix. Albuquerque, NM: Sandia National Laboratories.

12. EK. 2016. Elinkeinoelämän yritysturvallisuusmalli. Elinkeinoelämän keskusliitto.
13. ETSI. 2016. ETSI ISI flyer 2016. European Telecommunications Standards Institute. https://portal.etsi.org/Portals/0/TBpages/ISI/Docs/ETSI ISI flyer 2016.pdf (haettu 23.7.2020)
14. ETSI. 2020. Information Security Indicators - ISG ISI. European Telecommunications Standards Institute. https://portal.etsi.org/TB-SiteMap/ISI/ISI-List-members (haettu 23.7.2020)
15. ETSI GS ISI 001-1 V1.1.2. 2015. Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture. European Telecommunications Standards Institute.
16. ETSI GS ISI 001-2 V1.1.2. 2015. Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1. European Telecommunications Standards Institute.
17. ETSI GS ISI 002 V1.2.1. 2015. Information Security Indicators (ISI); Event Model A security event classification model and taxonomy. European Telecommunications Standards Institute.
18. ETSI GS ISI 003 V1.2.1. 2018. Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection. European Telecommunications Standards Institute.
19. ETSI GS ISI 005 V1.1.1.2015. Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness. European Telecommunications Standards Institute. European Telecommunications Standards Institute.
20. Garcia, Mary Lynn. 2008. The Design and Evaluation of Physical Protection Systems, 2nd Ed, Butterworth-Heinemann.
21. Gragg, David. 2002. A Multi-Level Defense Against Social Engineering. SANS Institute
22. Hermann, Debra. 2007. Complete Guide to Security and Privacy Metrics. Auerbach Publications.
23. HAEA, Hungarian Atomic Energy Authority. 2015. Evaluation of the effectiveness of the physical protection system of nuclear facilities. Hungarian Atomic Energy Authority.
24. Herzog, Pete. 2010. The Open Source Security Testing Methodology Manual. ISECOM.
25. Hinson, Gary, W. Krag Brotby. 2016. PRAGMATIC Security Metrics. Auerbach Publications.

26. Hutchins, Eric M., Michael J. Clopperty, Rohan M. Amin. 2010. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation.
27. IAEA. 2008. Preventive and Protective Measures against Insider Threats (NSS 8). International Atomic Energy Agency.
28. ISO/IEC 27032. 2012. Information technology -- Security techniques -- Guidelines for cybersecurity. International Organization for Standardization / International Electrotechnical Commission.
29. Jaquith, Andrew. 2007. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional.
30. Kwiatkowski, Ivan, Ronan Mouchoux. 2018. Automation and Structural Knowledge in Tactical Threat Intelligence. Kaspersky Labs.
31. Mateski, Mark, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye. 2012. Cyber Threat Metrics. Sandia Report SAND2012-2427.
32. Miller, John F. 2013. Supply Chain Attack Framework and Attack Patterns. The MITRE Corporation.
33. MITRE. 2019. About CAPEC, ATT&CK Comparison. https://capec.mitre.org/about/attack_comparison.html (haettu 6.6.2020)
34. MITRE. 2020. CAPEC, Common Attack Pattern Enumeration and Classification. A Community Resource for Identifying and Understanding Attacks. https://capec.mitre.org/ (haettu 6.6.2020)
35. MITRE. 2020. PRE-ATT&CK Introduction, https://attack.mitre.org/resources/pre-introduction/ (haettu 6.6.2020)
36. Mouton, Francois, Mercia M. Malan, Louse Leenen, H.S. Venter. 2014. Social Engineering Attack Framework. IEEE.
37. Newhouse, William, Stephanie Keith, Benjamin Scribner, Greg Witte. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST 800-181. National Institute of Standards and Technology.
38. Os, Rob van. 2018. SOC-CMM. Measuring Capability Maturity in Security Operations Centers. https://www.soc-cmm.com/downloads/ (haettu 22.7.2020)
39. Payne, Shirley. 2007. A Guide to Security Metrics. SANS Institute
40. Pols, Pauls. 2017. The Unified Kill Chain, Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks. Cyber Security Academy The Hague

41. Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid. 2019. Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST 800-160 Volume 2. National Institute of Standards and Technology.
42. Roberts, Scott, Rebekah Brown. 2017. Intelligence-Driven Incident Response, Outwitting the Adversary. O'Reilly Media.
43. SFS-EN ISO 9000. 2015. Laadunhallintajärjestelmät. Perusteet ja sanasto. Suomen Standardisoimisliitto SFS ry.
44. SFS-ISO/IEC 27000. 2020. Information technology. Security techniques. Information security management systems. Overview and vocabulary. Suomen Standardisoimisliitto SFS ry.
45. SFS-ISO/IEC 27001. 2017. Informaatioteknologia. Turvallisuustekniikat.Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS ry.
46. SFS-ISO/IEC 27004. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Suomen Standardisoimisliitto SFS ry.
47. Strom, Blake E., Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas. 2018. MITRE ATT&CK™: Design and Philosophy. The MITRE Corporation.
48. Thompson, Eric C. 2018. CSIR - How to Contain, Eradicate and Recover from Incidents, Apress
49. Trots, Ryan. 2010. Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century. Addison-Wesley Professional.
50. Velazquez, Chris. 2015. Detecting and Preventing Attacks Earlier in the Kill Chain. SANS Institute.
51. Wikipedia. 2020. SMART criteria. https://en.wikipedia.org/wiki/SMART_criteria (haettu 6.6.2020)
52. Volksbank, Rob van Os de, Floris Ladan, Thomas van Casteren, Robin Toornstra, Robert Metsemakers, Holger Grotenhuis. 2017. MaGMa. A joint use case framework from the Dutch financial sector. FI-ISAC.
53. Zimmerman, Carson. 2014. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation.