MAANPUOLUSTUSKORKEAKOULU

PERUSYHTYMÄN JOHTAMISJÄRJESTELMÄN KYBERVALVONTA

Pro gradu -tutkielma

Yliluutnantti
Henri Ojala

Sotatieteiden maisterikurssi 9
Maasotalinja

Huhtikuu 2020

MAANPUOLUSTUSKORKEAKOULU

Kurssi Sotatieteiden maisterikurssi 9	Koulutusohjelma Maavoimat
Tekijä Yliluutnantti Henri Ojala	
Opinnäytetyön nimi **Perusyhtymän johtamisjärjestelmän kybervalvonta**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Maanpuolustuskorkeakoulun kirjasto
Aika Huhtikuu 2020	**Tekstisivuja** 63 **Liitesivuja** 14

TIIVISTELMÄ

Nykypäivänä ei enää puhuta siitä, joutuvatko organisaatiot kyberhyökkäysten kohteiksi. Nykyhetkessä täytyy olettaa, että kyberhyökkäys pääsee jossain vaiheessa läpi kohteeseen. Tällöin täytyy ajatella milloin, miten ja millä voimakkuudella organisaatioon kohdistetaan kyberhyökkäys. Tämän tutkimuksen tarkoituksena oli selvittää kuinka perusyhtymän johtamisjärjestelmää tulisi valvoa kybertoimintaympäristössä. Lisäksi tutkimuksessa selvitettiin millaisia hyökkäystekniikoita hyökkääjät käyttävät ja kuinka ne havaitaan. Tarkoituksena oli myös tarkastella kybervalvomon rakennetta, henkilöstöä sekä yleisimpiä toimintatapoja kybervalvonnan kannalta.

Tutkimuksen päätutkimusmenetelmänä oli laadullisen tutkimuksen mukainen kirjallisuuskatsaus. Sisällön analysointi toteutettiin aineistolähtöisesti. Kybervalvontaa ilmiönä tutkittiin syvän puolustuksen -teorian kautta. Kyberturvallisuudessa syvän puolustuksen -teoria tarkoittaa sitä, että tietojärjestelmiä suojataan monilla eri tasoilla. Taso-ajattelun kautta puolustaja luo itselleen mahdollisimman monia keinoja, joiden avulla mahdollinen hyökkääjä kyetään havaitsemaan. Tässä tutkimuksessa syvän puolustuksen kerroksina käytettiin henkilöstöä ja toimintatapoja, tietoverkkoa sekä laitteita.

Tutkimuksen perusteella kybervalvomojen keskeisimmät palvelut valvonnan kannalta ovat reaktiiviset ja proaktiiviset palvelut. Poikkeaman hallinta, uhkatiedustelu sekä uhkametsästys liittyvät keskeisesti edellä mainittuihin palveluihin. Tutkimuksessa havaittiin kymmenen erilaista tehtävää henkilöstölle, joita tarvitaan tehokkaan kybervalvonnan toteuttamiseen. Henkilöstön tehtävät jakaantuivat tasaisesti palvelujen kesken.

Tutkimuksessa käytettiin kyberhyökkäyksien mallintamiseen MITRE:n tuottamaan ATT&CK-taulukkoa. Sen perusteella voidaan todeta, että suurin osa valvottavista kohteista liittyivät syvän puolustuksen -teorian mukaiseen laitekerrokseen. Tietojärjestelmien erilaiset prosessit ovat valvonnan keskiössä lähes kaikissa ATT&CK-taulukon hyökkäysvaiheissa. Tietoverkon valvonta on kyberhyökkäysten osalta selvästi pienemmässä osassa. Valvontaan käytettäviä keskeisiä työkaluja ovat laite- ja verkkopohjaiset tunkeutumisen esto- ja havainnointijärjestelmät sekä keskitetyt lokienhallintajärjestelmät.

Kirjallisuuskatsauksen perusteella voidaan päätellä, ettei Yhdysvaltojen perusyhtymissä ole tehokasta kybervalvontaa, vaan se korkeintaan tukeutuu alueelliseen kyberkeskukseen valvonnan osalta. Ammattitaitoisen henkilöstön puutteen vuoksi on todennäköistä, ettei perusyhtymään ole mahdollista luoda täydellistä kybervalvomoa. Yksinkertaisen kybervalvomon toteutus perusyhtymätasolle on kuitenkin mahdollista. Perusyhtymässä olevan kybervalvomon avulla alueelliset kyberkeskukset saisivat arvokasta tietoa taktiselta tasolta kybervalvontaan liittyen. Omien tietojärjestelmien tunteminen on ensiarvoisen tärkeää tehokkaan valvonnan toteuttamiseksi.

AVAINSANAT
perusyhtymät, johtamisjärjestelmät, kybervalvonta, kyberturvallisuus, SIEM, IDPS, uhkatiedustelu, uhkametsästys, tietoturvapoikkeamat, verkkohyökkäykset, kybervalvomot

SISÄLLYS

PERUSYHTYMÄN JOHTAMISJÄRJESTELMÄN KYBERVALVONTA

1. JOHDANTO

Nykypäivänä ei enää puhuta siitä, joutuvatko organisaatiot kyberhyökkäysten kohteiksi. Nykyhetkessä täytyy olettaa, että kyberhyökkäys pääsee jossain vaiheessa läpi kohteeseen. Tällöin täytyy ajatella milloin, miten ja millä voimakkuudella organisaatioon kohdistetaan kyberhyökkäys. [1, s. 9; 2, s. 7; 3, s. 1]

Kyberturvallisuuteen liittyvät hyökkäykset ovat lisääntyneet, ja ne ovat kehittyneet monipuolisiksi ja tuhovoimaisiksi. Uuden tyyppisiä tietoturvapoikkeamia ilmestyy lisää jatkuvasti. Ennakoivat toimenpiteet voivat vähentää poikkeamien määrää, mutta kaikkia poikkeamia ennakointi ei kuitenkaan poista. Poikkeaman hallinnan suorituskyky on erittäin tärkeä, jotta tietoturvapoikkeamat kyetään havaitsemaan riittävän nopeasti, niiden vaikutukset saadaan minimoitua, oman järjestelmän heikkouksia vähennettyä ja saadaan palautettua palvelut takaisin normaaliksi. [3, s. 1; 4, s. 1]

Yhdysvaltojen asevoimat on tunnistanut, että sen tietojärjestelmiin kohdistuu jatkuva kyberuhka. Yhdysvallat näkee uhkaksi kaikki toimijat, joilla on kyky ja tahto vahingoittaa Yhdysvaltojen tietojärjestelmiä. Uhkan aiheuttajia voivat olla valtiolliset toimijat, ei-valtiolliset toimijat, rikolliset sekä sisäpiiriläiset. Toimijoiden tavoitteet voivat vaihdella suuresti sotilaallisista tavoitteista aina kiusantekoon. [5, s. 31]

Tulevaisuudessa verkkoon yhdistetyt laitteet lisääntyvät. Tämä tarjoaa hyökkääjälle enemmän mahdollisuuksia hyökkäyksen toteuttamiseen. On myös huomioitava, että erilaisten kyberhyökkäysten toteuttaminen on suhteellisen halpaa verrattuna konventionaaliseen vaikuttamiseen. [6, s. 47]

Yhdysvaltojen asevoimat on listannut *Cyberspace and Electronic Warfare Operations* -ohjesääntöönsä hyökkäysesimerkit, joita asevoimat pitävät uhkana (Liite 1). Taulukkoon on listattu esimerkkeinä palvelunestohyökkäys, tietoverkon penetrointi, haittaohjelmat ja elektromagneettisen spektrin käytön estäminen sekä häirintä.

Jotta tietojen luottamuksellisuudesta, eheydestä sekä saatavuudesta voidaan varmistua perusyhtymän johtamisjärjestelmässä, täytyy sen tietojärjestelmiä valvoa jatkuvasti. Yhdysvaltojen armeija julkaisee ohjesääntönsä julkisina asiakirjoina. Tietojärjestelmän valvontaan liittyviä ohjeita niistä ei ole havaittavissa.

Tietojärjestelmien valvonta ei ole uusi asia. Ensimmäinen kybervalvomo käynnisti toimintansa vuonna 1988. Kybervalvomon toiminta aloitettiin Morris-madon takia, joka levisi ympäri Internetiä. [3, s. 19]

Tässä pro gradu -tutkielmassa perusyhtymällä tarkoitetaan itsenäiseen taisteluun kykenevää sotilasosastoa. Itsenäisellä tarkoitetaan sitä, että se kykenee suorittamaan tehtävän ilman ylemmän johtoportaan tukea. Perusyhtymässä on oltava kaikki sen tarvitsemat aselajit edustettuna, kuten jalkaväki-, pioneeri-, tykistö-, viesti-, tiedustelu- ja huoltojoukot.

Perusyhtymän johtamisjärjestelmällä tarkoitetaan yleisesti sen johtamisjärjestelmähenkilöstöä, viestijärjestelmää, tietojärjestelmiä, johtamispaikkoja, johtamisen prosesseja sekä prosessien tuotteita ja varamenetelmiä. [7, s. 11] Tutkimuksessa käsitellään viesti- ja tietojärjestelmien valvontaa.

Kybervalvonnalla tarkoitetaan tietojärjestelmien valvontaa, jonka tavoitteena on tietoturvapoikkeamien havaitseminen ja niiden vaikutusten pienentäminen valvottavassa kybertoimintaympäristössä. Sitä toteuttaa erillinen valvontaan nimetty osasto, esimerkiksi kybervalvomo (Cyber Security Operations Center, CSOC).

1.1. Tutkimuksen tarkoitus, rakenne ja tutkimuskysymykset

Tämän tutkimuksen tarkoituksena on selvittää, millä tavoilla perusyhtymän johtamisjärjestelmää tulee valvoa kyberturvallisuuden näkökulmasta. Tutkimuksen pääkysymys on:

- Kuinka perusyhtymän johtamisjärjestelmää tulee valvoa?

Tutkimukseen on laadittu alakysymyksiä, jotka tukevat päätutkimuskysymystä. Laaditut alakysymykset ovat seuraavat:

1. Millainen on perusyhtymän johtamisjärjestelmä ja perusyhtymän kyberoperaatioiden suorituskyky?
2. Miten tietojärjestelmiä valvotaan kyberturvallisuuden näkökulmasta?

3. Millainen on kybervalvomo, ja millaisia palveluita se tuottaa?
4. Millaisia tekniikoita hyökkääjät käyttävät tietojärjestelmissä ja kuinka niitä valvotaan?

Tutkimuksessa on viisi asialukua. Tutkimuksen toisessa luvussa tarkastellaan perusyhtymää ja sen johtamisjärjestelmää sekä kybertoimintaympäristöä. Luvussa selvitetään, millainen on taisteluosaston johtamisjärjestelmä sekä sen kyberoperaatioiden suorituskyky. Luku vastaa tutkimuksen ensimmäiseen alakysymykseen.

Tutkielman kolmannessa luvussa käsitellään tutkimuksessa käytetty teoria. Lisäksi luvussa keskitytään tietojärjestelmien valvontaan, jota lähestytään teknisten työkalujen kautta. Luvussa kerrotaan, millaisilla työkaluilla hyökkäystekniikoita voidaan havaita. Luvussa vastataan alakysymykseen kaksi.

Neljännessä luvussa esitellään kybervalvomojen rakenne ja toiminta. Luvussa selvitetään, millainen henkilöstökokoonpano tarvitaan tehokkaaseen kybervalvontaan, millaisilla toimintatavoilla kybervalvontaa toteutetaan ja millaisia palveluita kybervalvomot tuottavat. Luvussa vastataan tutkielman kolmanteen alakysymykseen.

Tutkimuksen viidennessä luvussa tutkitaan MITRE:n ATT&CK-taulukkoa ja sen kuvaamaa kyberhyökkäyksen rakennetta. Luvussa käsitellään hyökkäykset vaiheittain ja kootaan tärkeimmät valvottavat kokonaisuudet hyökkäystekniikoiden osalta. Luvun lopuksi tätä tietoa verrataan toisessa asialuvussa käsiteltyihin valvonnan menetelmiin ja muodostetaan yhteenveto hyökkäystekniikoiden valvonnasta. Tutkimuksen neljänteen alakysymykseen vastataan tässä luvussa.

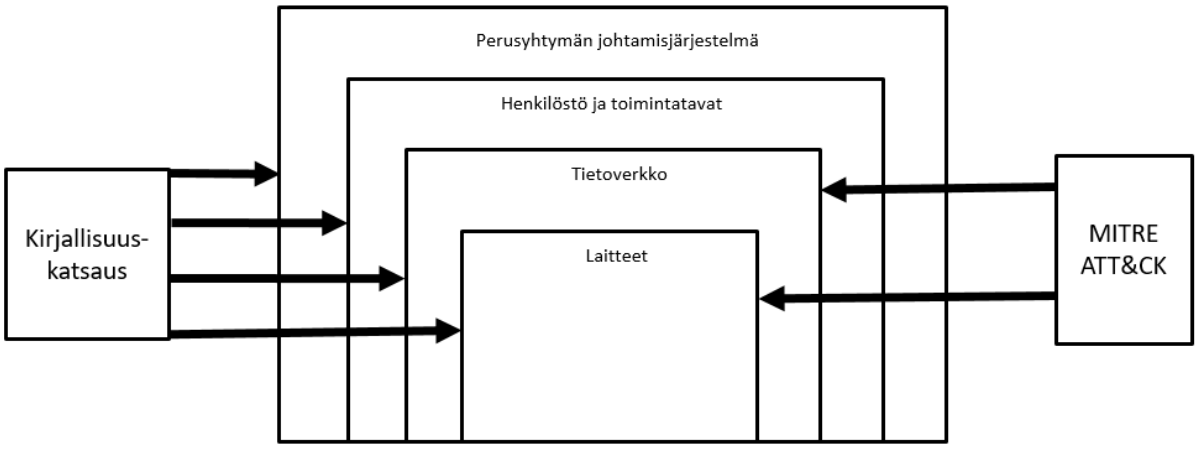
Tutkielman viimeisessä luvussa tehdään johtopäätökset aiempien lukujen perusteella. Luvussa arvioidaan sitä, kuinka kybervalvontaa tulisi suorittaa perusyhtymässä, jotta se olisi mahdollisimman tehokasta. Lisäksi luvussa analysoidaan sitä, millaisia haasteita kybervalvonnan suorituskyvyn luominen todennäköisesti aiheuttaa perusyhtymätasolla. Lopuksi arvioidaan tutkielman luotettavuutta ja pohditaan mahdollisia jatkotutkimusaiheita. Luvussa vastataan tutkielman päätutkimuskysymykseen.

1.2. Tutkimusmenetelmät ja rajaukset

Tutkimuksessa käytetään päätutkimusmenetelmänä laadullisen tutkimuksen mukaista kirjallisuuskatsausta, jonka avulla on kyetty hahmottamaan tutkittavan aihealueen kokonaisuus. Kirjallisuuskatsaus sopii hyvin päätutkimusmenetelmäksi, koska tutkimuksen eri aihealueista on saatavilla runsaasti tietoa Internetistä. Sisältö on analysoitu aineistolähtöisen sisällönanalyysin mukaisesti.

Tutkimuksessa käytetään syvän puolustuksen -teoriaa. Yhdysvaltojen asevoimat ovat järjestäneet kyberpuolustuksensa teorian mukaisesti [5, s. 17]. Se tarkoittaa periaatetta, jossa tietojärjestelmiä suojataan useissa eri pisteissä, useilla erilaisilla työkaluilla ja toimintatavoilla [8, s. 7; 9, s. 388]. Tutkimuksessa käytetyt syvän puolustuksen kerrokset ovat henkilöstö, toimintatavat, tietoverkko ja laitteet. Teoria on esitelty kattavammin luvussa kolme.

Tietoverkko- ja laitekerroksen valvonnan teorian tarkasteluun ja analysointiin on käytetty kirjallisuuskatsauksen lisäksi MITRE:n ATT&CK-taulukkoa. Se on avoimesti saatavilla oleva tietopankki, jossa kuvataan kyberhyökkääjän mahdollisesti käyttämiä tekniikoita [10]. Lisäksi taulukossa kuvataan, millaisiin eri vaiheisiin kyberhyökkäys voidaan jakaa [10; 11]. Tutkimuksen viitekehys on esitetty kuvassa 1.



Kuva 1: Tutkimuksen viitekehys

Kirjallisuuskatsaus on aloitettu käsiteanalyysillä, jonka avulla on perehdytty aihealueen keskeisimpiin käsitteisiin. Käsitteiden määrittämiseen on pääsääntöisesti käytetty Sanastokeskuksen tuottamaa Kyberturvallisuuden sanastoa vuodelta 2018.

Käsitteiden määrittämisen jälkeen on tutkittu kirjallisuuskatsauksen avulla perusyhtymän johtamisjärjestelmää. Tutkimuksessa käsitellään Yhdysvaltojen asevoimien johtamisjärjestelmää, koska siitä on parhaiten saatavilla tietoa julkisista lähteistä. Perusyhtymän johtamisjärjestelmän tutkimisella on kyetty asettamaan kybervalvonta tutkittavaan viitekehykseen.

Kirjallisuuskatsausta on käytetty lisäksi kybervalvomon toimintatapojen ja henkilöstön selvittämiseen. Kirjallisuuskatsauksessa esille nousseita toimintatapoja ovat poikkeaman hallinta, uhkatiedustelu ja uhkametsästys. Katsauksen lopuksi henkilöstöstä ja eri toimintatavoista on muodostettu yhteenveto. Kirjallisuuskatsausta jatkettiin tietoverkon ja laitteiden osalta, joka käytännössä tarkoitti eri teknisten valvontatyökalujen ominaisuuksien ja käyttöperiaatteiden tarkastelua.

Kirjallisuuskatsauksen avulla muodostettua tietopohjaa eri valvontatyökaluista käytettiin MITRE:n ATT&CK-taulukon analysoinnin tukena. Taulukossa oli tutkimuksen tekohetkellä 319 erilaista hyökkäystekniikkaa. Taulukkoa päivitetään jatkuvasti. Taulukkoa on tarkasteltu 7.1.2020 mennessä tapahtuneiden hyökkäystekniikoiden osalta.

Tutkielmassa ei keskitytä siihen, miten hyökkäys pääsee sisälle perusyhtymän tietojärjestelmiin, koska sillä ei lopulta ole merkitystä valvonnan näkökulmasta. Tutkielmassa oletetaan, että hyökkäys pääsee läpi perusyhtymän johtamisjärjestelmään.

Isojen kybervalvomojen toiminta on erittäin laaja-alaista. Kybervalvomojen toiminnasta ei pääsääntöisesti käsitellä kuin valvontaa sekä sitä välittömästi tukevia toiminteita. Esimerkiksi lakeihin liittyvät toiminteet on rajattu pois (valvomon lakimiehet ja lakeihin liittyvät prosessit).

1.3. Aineiston esittely

Ensimmäisessä asialuvussa käytettiin aineistona pääasiassa Yhdysvaltojen asevoimien ohjesääntöjä. Lisäksi käytettiin lisäksi Ison-Britannian vastaavia ohjesääntöjä. Johtamisjärjestelmän periaatteita selvitykseen käytettiin lisäksi viestijärjestelmien valmistajien tekemiä oppaita, ohjeita ja Janes-tietokantaa.

Tutkielman laajimpien kyberturvallisuuteen liittyvien kokonaisuuksien tutkimiseen (tietoturvapoikkeamien hallinta, kybervalvomot) käytettiin National Institute of Standards and Technology:n (NIST) ja SANS-instituutin tuottamia tutkimusraportteja. NIST on Yhdysvaltain kauppaministeriöön (United States Department of Commerce) kuuluva virasto, jonka tehtävänä on edistää innovaatioita ja teollisuuden kilpailukykyä [12]. NIST:n yhtenä tutkimuskohteena on tieto- ja kyberturvallisuus [12]. SANS-instituutti on voittoa tavoittelematon yritys, joka on erikoistunut kyber- ja tietoturvallisuuskoulutuksiin [13].

Valvontatyökalujen tutkimiseen on käytetty pääasiassa erilaisia oppikirjoja tai jo edellä mainittujen instituutioiden raportteja. Oppikirjoista mainittakoon David Nathansin toimittama *Designing and Building a Security Operations Center* ja Michael E. Whitmanin sekä Herbert J. Mattordin toimittama *Principles of Information Security*. Lisäksi on käytetty eri tietoturvayhtiöiden tuottamia raportteja ja ohjeita.

Tutkimuksen viidennessä luvussa on käytetty MITRE:n ATT&CK-taulukkoa tehokkaan valvonnan määrittämiseen. ATT&CK-taulukossa on kuvattu kehittyneen hyökkäyksen mahdolliset eri vaiheet ja niissä käytettävät hyökkäystekniikat. Yhdysvaltalainen MITRE on voittoa tavoittelematon yritys, joka hallinnoi eri tutkimus- ja kehittämiskeskuksia. Liittovaltio rahoittaa yrityksen toimintaa. Yhtenä MITRE:n osana toimii *National Cybersecurity FFRDC.* [14]

Tutkimuksessa käytettyihin käsitteisiin on käytetty mahdollisuuksien mukaan Sanastokeskuksen tuottamaa Kyberturvallisuuden sanastoa. Kuitenkaan kaikkia termejä ei ole avattu sanastossa, jolloin tutkimuksessa on käytetty esimerkiksi Wikipedian, Finton tai Techterm:n määritelmiä.

2. PERUSYHTYMÄN JOHTAMISJÄRJESTELMÄ JA KYBEROPERAATIOT

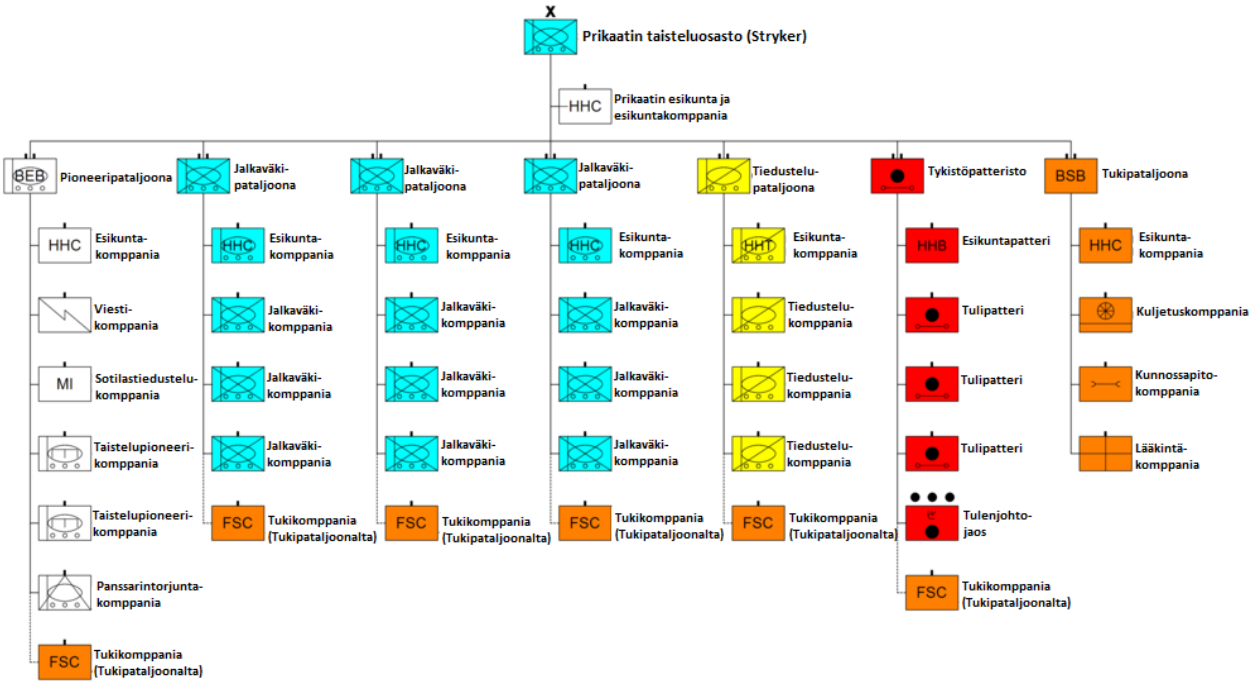
Prikaatin taisteluosasto on Yhdysvaltojen maavoimien perusyhtymä. Yhdysvaltalaisia prikaateja on kolmenlaisia, jotka ovat jalkaväkiprikaati, Stryker-prikaati ja panssariprikaati. Prikaatin nimi kuvaa käytettävää pääkalustoa. [15, s. 15]

Prikaateista uusin joukkotyyppi on Stryker-prikaati, jota myös käytetään esimerkkinä tässä työssä. Se on keskiraskas jalkaväkiprikaati, joka on tarkoitettu tunkeutumaan uudelle taistelualueelle, erityisesti ilmakuljetuksilla. Tehtävätyypistään johtuen sillä todennäköisesti on käytössään uudenaikaisin johtamisjärjestelmä. [16, s. 50]

Prikaatin ylempänä johtoportaana toimii divisioona (tai Joint Task Force). Ylempään johtoportaaseen voi kuulua enintään kuusi prikaatia. Johtoporras käskee prikaatille tehtävän, toiminta-alueen sekä sitä tukevat elementit. [15, s. 15]

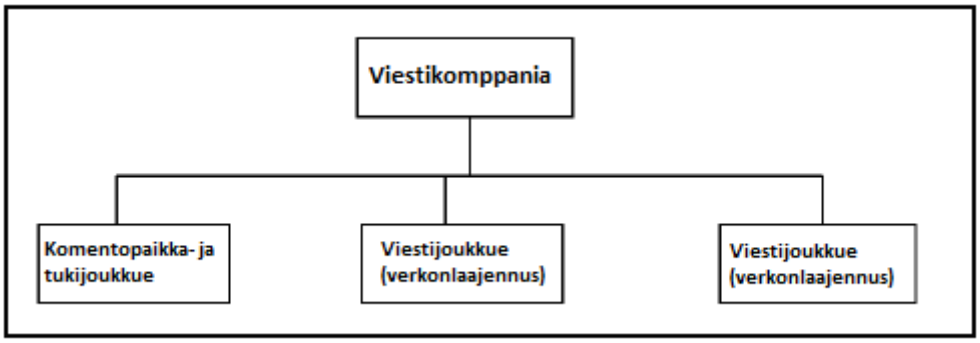
Jokainen prikaati sisältää tykistö-, tiedustelu-, viesti-, pioneeri- sekä huoltojoukkoja, taistelevien joukkojen lisäksi. Johtoporras tukee tarvittaessa prikaatia esimerkiksi helikoptereilla, taistelupanssarivaunuilla, jalkaväellä, tykistöllä, ilmatorjunnalla, pioneereilla tai viestijoukoilla. Tuen ansiosta prikaati kykenee suoriutumaan monista erityyppisistä tehtävistä. [15, s. 15]

Stryker-prikaati on nopean toiminnan joukko, jonka rungon muodostaa moottoroitu jalkaväki. Operatiivisesta luonteestaan johtuen prikaati kykenee toimimaan tehokkaasti eri tyyppisissä maasto- ja sääolosuhteissa. Prikaati taistelee kolmen jalkautetun jalkaväki pataljoonan voimalla. Jokaiseen pataljoonaan kuuluu kolme komppaniaa, jotka jaetaan kolmeen joukkueeseen. Prikaatin tykistöpatteristoon kuuluu neljä patteria (esikuntapatteri ja kolme tulipatteria). [15, s. 21] Seuraavassa kuvassa on esitetty Stryker-prikaatin organisaatio [15, s. 23; 17].



Kuva 2: Stryker-prikaatin organisaatio

Prikaatin pioneeripataljoonan viestikomppanian tehtävänä on suunnitella, valvoa, ylläpitää sekä suojata viestiverkko prikaatin vastuualueella. Lisäksi yksikkö liittää prikaatin ylemmän johtoportaan verkkoon sekä suoraan Yhdysvaltain puolustusministeriön verkkoon (Department of Defense Information Network, DODIN). [6; 15] Seuraavassa kuvassa on esitelty viestikomppanian organisaatio. [18, s. 25]



Kuva 3: Viestikomppanian organisaatio

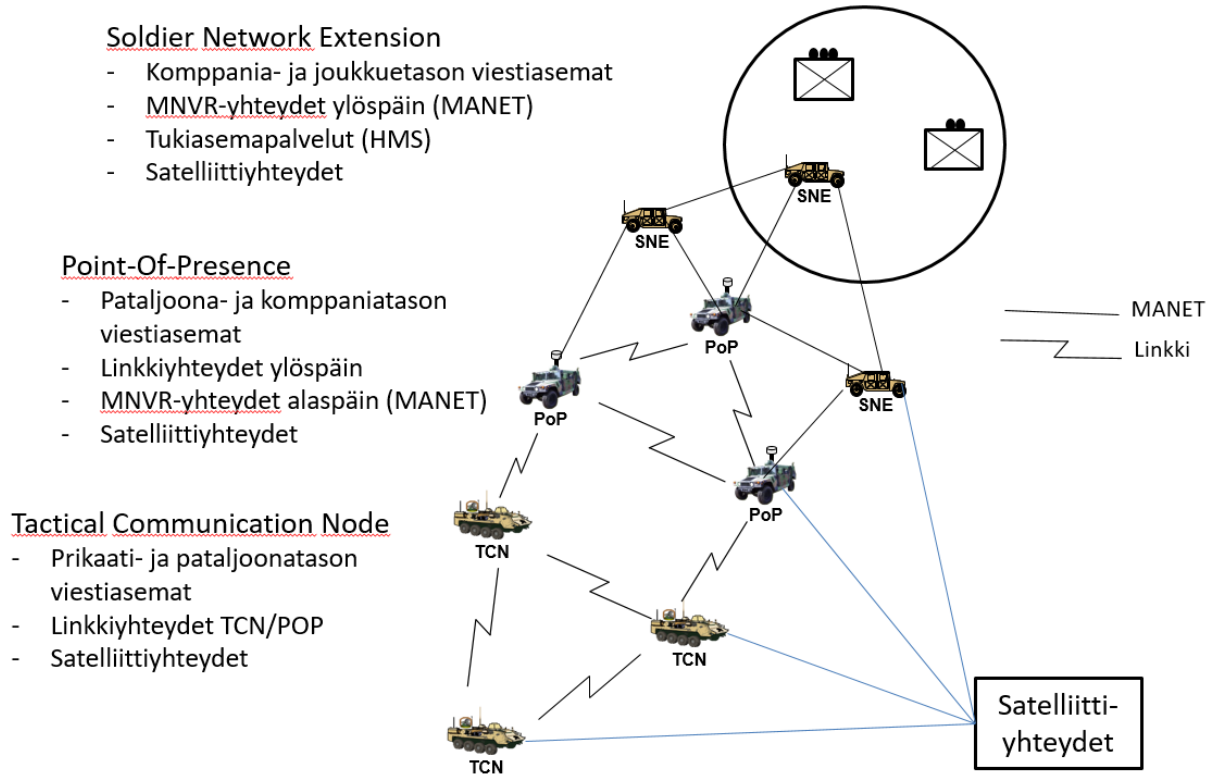
Yksikköön kuuluu kaksi verkkoa laajentavaa joukkuetta sekä tukijoukkue. Toinen verkkoa laajentavasta joukkueesta tukee prikaatin pääkomentopaikkaa ja toinen taktista komentopaikkaa. Ne muodostavat linkkiyhteydet komentopaikkojen välille ja laajentavat verkkoa lähemmäs taistelevia joukkoja. Tukijoukkuetta käytetään erilaisiin verkon tukipalveluihin ja komppanian komentopaikan perustamiseen. [6; 18, s. 24 - 26]

2.1. Yhdysvaltojen puolustusministeriön tietoverkko ja prikaatin johtamisjärjestelmä

Yhdysvaltojen puolustusministeriön tietoverkon (Department of Defense Information Networks, DODIN) tarkoituksena on mahdollistaa puolustusministeriön alaisten laitosten turvallinen viestintä. Tietoverkkoon kuuluvat viestintään tarvittavat tilat, laitteet, tieto- ja viestintäpalvelut. Tietoverkon osajärjestelminä ovat esimerkiksi maavoimien (Army) LandWarNet, laivaston (Navy) FORCEnet ja ilmavoimien (Air Force) C2 Constellation. [6, s. 37 - 38] Prikaatin johtamisjärjestelmä WIN-T (Warfighter Information Network -Tactical) on osa Yhdysvaltojen maavoimien tietoverkkoa (LandWarNet) [19].

Prikaatin WIN-T-johtamisjärjestelmä on rakennettu verkostokeskeisen sodankäynnin periaatteiden mukaan. Johtamisjärjestelmä ulottuu ryhmätasolta prikaatiin asti. Prikaatin johtamisjärjestelmä on pääosin integroitu suoraan ajoneuvoihin, jolloin se siirtyy ongelmitta paikasta toiseen. Näin ollen se ei ole riippuvainen paikallisesti infrastruktuurista. Satelliittiyhteydet tuovat joustavuutta yhteyksien muodostamiseen. Johtamispaikkojen ja viestiasemien väliset yhteydet kyetään tilanteen mukaan muodostamaan langallisesti tai langottomasti. [16; 20; 21]

Johtamisjärjestelmä on yhteensopiva Yhdysvaltojen liittolaisten, kaupallisten järjestelmien ja vanhojen järjestelmien kanssa sekä puolustushaarojen välillä. IP-tekniikalla on keskeinen rooli yhteensopivuuden suhteen. WIN-T-järjestelmän avulla kyetään siirtämään ääntä, videota sekä dataa. Järjestelmä tukee niin paketti- kuin piirikytkentäistä tekniikkaa. [16, s. 64 - 65] Olen laatinut alle yksinkertaistetun periaatekuvan WIN-T-johtamisjärjestelmästä [20; 21]. WIN-T-johtamisjärjestelmään kuuluu muitakin asematyyppejä kuin kuvassa esitetyt [21].



Kuva 4: Stryker-prikaatin WIN-T-johtamisjärjestelmän periaatekuva

Tactical Communications Nodet (TCN) muodostavat runkoverkon prikaatin alueelle. TCN-asemien avulla prikaati liitetään ylemmän johtoportaan verkkoon sekä turvataan nopeat tiedonsiirtoyhteydet tärkeimpiin pataljooniin. Lavetteina viestiasemilla ovat kuorma-autot. Liikkeellä oltaessa TCN:t kykenevät muodostamaan MANET-verkon, johon käytetään HNR-laitteita (Highband Networking Radio). Paikallaan oltaessa asemat muodostavat linkkijänteet toisten vastaavien asemien kanssa. Linkkijänteet käyttävät NATO Band 3:aa ja 4:aa. Satelliittiyhteyksien avulla prikaati kyetään liittämään Yhdysvaltojen puolustusministeriön verkkoon (DODIN). [20; 21; 22]

Point of Presence -asemat (POP) laajentavat verkkoa lähemmäs taistelevia joukkoja. POP-asemat on selkeästi suunniteltu liikkuvammiksi kuin TCN:t. Tämä käy ilmi alustoista joihin POP-asemat kyetään asentamaan. Tällä hetkellä järjestelmää on asennettu MATV:een (MRAP-All-Terrain-Vehicle), Humveehen ja Strykereihin. [20; 21]

Soldier Network Extension -asemia (SNE) käytetään lähimpänä taistelevia joukkoja, ja ne tarjoavat tilannekuvaa yksiköihin. Asemia on asennettu samoihin ajoneuvoihin kuin POP-asemia. [20; 21]

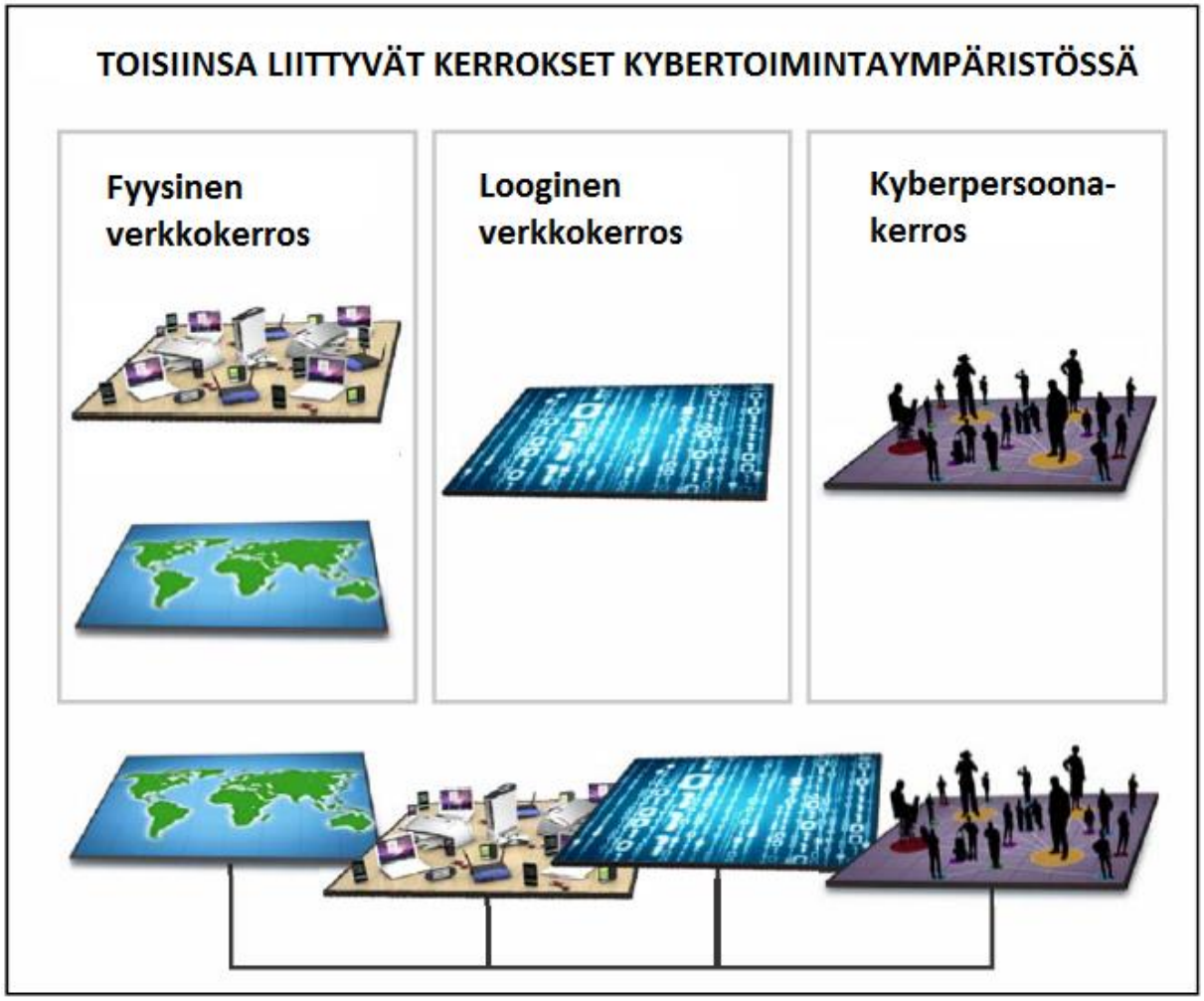
MNVR-radioiden (Mid-Tier Networking Vehicular Radio) tarkoituksena on muodostaa rajapinta ylemmän ja alemman taktisen verkon välille [23]. Rajapinta sijaitsee todennäköisesti komppaniatasolla. MNVR sisältää kaksi eri radiota, jotka käyttävät eri aaltomuotoja rajapinnan muodostamiseen [23].

Tukiasemapalveluihin käytetään ajoneuvoasenteisia AN/PRC-158- sekä kädessä pidettäviä AN/PRC-163-radioita. Radio mahdollistaa niin puheen kuin datan lähetyksen. [24]

2.2.Kybertoimintaympäristö

Yhdysvaltojen asevoimien näkemyksen mukaan kybertoimintaympäristö käsittää Internetin, tietoliikenneverkot, tietokonejärjestelmät ja niihin sulautetut prosessorit ja ohjaimet. Voidaan siis puhua kokonaisuudesta, joka käsittää toisistaan riippuvaisten tietojärjestelmien infrastruktuurin ja niihin sisältyvän datan. Yhdysvaltojen asevoimien termi kybertoimintaympäristölle on *cyberspace*. [25, s. 100] Tutkimuksessa käytetään termiä kybertoimintaympäristö, koska termi on Sanastokeskuksen tekemän kyberturvallisuussanaston mukainen, ja se tarkoittaa samaa asiaa kuin Yhdysvaltojen asevoimien *cyberspace* [26, s. 21].

Kybertoimintaympäristö jaetaan Yhdysvaltojen näkemyksen mukaan kolmeen kerrokseen, jotka ovat fyysinen verkkokerros, looginen verkkokerros ja kyberpersoonakerros. Ison-Britannian näkemys kybertoimintaympäristöstä on periaatteiltaan samankaltainen, jakaantuen kuitenkin kuuteen eri kerrokseen (liite 2), kolmen sijasta. Ison-Britannian näkemyksen mukaan kyberpersoonakerros voidaan jakaa vielä kolmeen erilliseen osa-alueeseen (social, people, persona) ja fyysinen verkkokerros voidaan jakaa kahteen erilliseen (network, real). [25, s. 22 - 23; 27, s. 6 - 9] Tutkimuksen kannalta kolmen kerroksen malli on kuitenkin mielestäni riittävä. Malli on esitelty seuraavassa kuvassa [25, s. 23].



Kuva 5: Kybertoimintaympäristön kerrokset

Fyysiseen verkkokerrokseen kuuluvat erilaiset verkkolaitteistot ja -infrastruktuuri, kuten tietokoneet, erilaiset muistit, verkkolaitteet ja langalliset sekä langattomat yhteydet. Fyysisen kerroksen suojaamiseen tarvitaan fyysistä suojaa, jotta kyetään estämään fyysinen vahinko tai luvaton pääsy järjestelmään. Luvattoman pääsyn kautta hyökkääjä pääsee esimerkiksi loogiseen verkkokerrokseen. [25, s. 22 - 23]

Looginen verkkokerros perustuu erilaisiin ohjelmistoihin, joiden avulla ohjataan fyysisen kerroksen komponentteja. Kyseessä voi olla esimerkiksi internetsivu, jota säilytetään usealla eri palvelimella ympäri maailmaa. Sivustoon saadaan kuitenkin yhteys muodostettua, mikäli tietokoneesta on internet-yhteys sekä -selain. Mikäli sivustoon saadaan yhteys, sitä vastaan voidaan myös hyökätä. [25, s. 24]

Kyberpersoonakerroksella tarkoitetaan jonkin yksilön tai jonkin kokonaisuuden sähköistä identiteettiä kybertoimintaympäristössä. Nämä identiteetit voivat pitää sisällään sähköposti-osoitteita, sosiaalisen median tilejä, muiden web-palveluiden identiteettejä, IP-osoitteita sekä matkapuhelinnumeroita. Yhdellä yksilöllä voi olla useita eri kyberpersoonia ympäri internetiä. Toisaalta yhdellä kyberpersoonalla saattaa olla useita eri käyttäjiä, esimerkiksi järjestelmänvalvojan käyttäjätunnus ja salasana voivat olla useamman ylläpitäjän hallussa. Kyberpersoonat voivat olla todella monimutkaisia monien eri sijaintiensa takia. [5, s. 23 - 24; 25, s. 24]

2.3.Kyberoperaatiot

Suurin osa Yhdysvaltojen asevoimien teknisistä järjestelmistä on jollain tavalla verkottuneita. Tietoverkkojen ja ohjelmistojen monimutkaisuus sekä heikot turvallisuusratkaisut verkkosuunnittelussa ja sovellusten kehittämisessä, tekevät kybertoimintaympäristöstä haavoittuvaisen erilaisille hyökkäyksille. Lisäksi esimerkiksi normaalien käyttäjien huolimaton toiminta lisäävät tietojärjestelmien haavoittuvuutta entisestään. Kyberoperaatioilla pyritään vähentämään riskien määrää, joka mahdollistaa asevoimille saatavilla olevat, luotettavat ja eheät tietojärjestelmät. [5, s. 25 - 29]

Kyberoperaatiot toteutetaan kybertoimintaympäristössä. Niiden tarkoituksena on käyttää kybertoimintaympäristöä operaation tavoitteiden saavuttamiseksi. [25, s. 36; 27, s. 53] Yhdysvaltojen näkemyksen mukaan kyberoperaatiot jaetaan karkeasti hyökkäys-, puolustus- sekä Puolustusministeriön tietoverkko-operaatioiksi. Jako ei ole kuitenkaan todellisuudessa näin yksinkertainen vaan kyberoperaatiossa voi olla esimerkiksi puolustus- ja tietoverkko-operaatioiden osia. [25, s. 36] Henkilöstöä käytetään dynaamisesta eri operaatiolajien kesken [25, s. 40].

Ison-Britannian kyberoperaatiot jaetaan neljään luokkaan (hyökkäys, puolustus, tiedustelu ja valmistelu). Erot Yhdysvaltojen kanssa liittyvät lähinnä operaatioluokkien jakoon ja operaatioiden nimityksiin. Periaatteet ovat kummallakin maalla samat. [25, s. 36; 27, s. 53 - 63]

Yhdysvaltojen Puolustusministeriön tietoverkko-operaatioiden tarkoituksena on suojata, laajentaa, huoltaa sekä ylläpitää Puolustusministeriön kybertoimintaympäristöä. Edellä mainitut toimet sisältävät ennakoivia toimenpiteitä, joiden avulla pyritään vähentämään ja poistamaan haavoittuvuuksia, joita hyökkääjä voisi käyttää hyväkseen. Haavoittuvuuksia ovat esimerkiksi heikot salasanat, päivittämättömät järjestelmät ja salaamaton data. Tietoverkko-operaatioiden avulla varmistutaan tietojärjestelmien luottamuksellisuudesta, käytettävyydestä ja eheydestä. [25, s. 36 - 40]

Huomionarvoista on se, että tietoverkko-operaatiot ulottuvat taktisiin verkkoihin asti. [25, s. 36] Tämä tarkoittaa käytännössä myös prikaatin WIN-T-johtamisjärjestelmää. Onnistuneet tietoverkko-operaatiot luovat perustan onnistuneille puolustus- ja hyökkäysoperaatioille kybertoimintaympäristössä [28, s.30].

Puolustuksellisten kyberoperaatioiden tavoitteena on suojata käskettyä verkkoa välittömiltä kyberuhkilta. Tarkoituksena näillä operaatioilla on säilyttää omien joukkojen kyky toimia kybertoimintaympäristössä vapaasti sekä suojata dataa, tietoverkkoja ja muita kybertoimintaympäristöön liitettyjä laitteita. Verkon palauttaminen turvalliseen tilaan on osa puolustuksellista kyberoperaatiota. Suurin ero tietoverkko-operaatioihin on se, että puolustuksellisilla operaatioilla pyritään estämään uhkat, jotka ovat jo murtautuneet tai ovat murtautumassa järjestelmään. [25, s. 37 - 38]

Yhdysvaltojen armeija käyttää syvän puolustuksen -periaatetta puolustaessaan tietoverkkojaan. Periaate tarkoittaa sitä, että verkkoa valvotaan ja suojataan monessa eri pisteessä, monilla eri tavoilla. Armeija käyttää tietoverkkojensa valvomiseen mm. virustorjuntaohjelmistoja, verkkosensoreita, tunkeutumisen esto- ja havainnointijärjestelmiä. Lisäksi puolustusta tuetaan fyysisellä suojalla. [5, s. 17 - 29]

Puolustukselliset kyberoperaatiot jaetaan toiminnallisesti kahteen eri osaan, sisäiseen ja ulkoiseen puolustukseen. Suurin osa puolustuksellisista operaatioista liittyy sisäiseen puolustukseen. Siihen kuuluu olennaisena osana proaktiivinen uhkametsästys. Lisäksi sisäistä puolustusta toteutetaan aktiivisesti muokkaamalla, suojaamalla, reitittämällä ja eristämällä hyökkäyksen kohteena olevaa verkkoa. Tällä tavoin verkko pyritään pitämään käytettävissä tärkeimmille joukoille häiriötilanteissa. [5, s. 18; 25, s. 37 - 38]

Ulkoisen puolustuksen toimenpiteet viedään nimensä mukaisesti suojattavan tietojärjestelmän ulkopuolelle, ilman ulkopuolisen verkon omistajan lupaa. Nämä toimet saattavat sisältää toimia joiden avulla vahingoitetaan tai tuhotaan vastustajan järjestelmiä. Kohteena ulkoisessa puolustuksessa on kohde joka uhkaa tai on uhkaamassa suojattavaa tietojärjestelmää. [25, s. 38]

Kolmas kyberoperaatiomuoto on hyökkäyksellinen. Sen tarkoituksena on projisoida voimaa oman tietoverkon ulkopuolelle. Kuten ulkoisen puolustuksen tapauksessa, myös hyökkäykselliset operaatiot voivat nostaa voimankäytön fyysisen vahingoittamisen tai tuhoamisen tasolle. [25, s. 39]

2.4. Prikaatin kyky kybertoimintaympäristössä

Omien joukkojensa komentajat armeijakuntatasosta prikaatitasoon ovat vastuussa oman tietojärjestelmänsä puolustuksesta. Tämä tarkoittaa sitä, että aselavetin käyttäjienkin on kyettävä suojaamaan oma järjestelmänsä kyberuhkilta [25, s. 42]. Tällä tarkoitetaan todennäköisesti ainoastaan ennakoivia toimenpiteitä, jotka ovat osa tietoverkko-operaatioita.

Kaikkia maavoimien kyberoperaatioita ohjaa *Army Cyber Operations And Integration Center*. Se johtaa alueellisia kyberkeskuksia. Komentajat voivat pyytää tukea alueelliselta kyberkeskukselta, mikäli heillä itsellään ei ole kykyä suorittaa käskettyä tehtävää. Edellä mainittujen keskusten tuki on kuitenkin kriittinen prikaatin kyberoperaatioiden onnistumiselle. [5, s. 51 - 53]

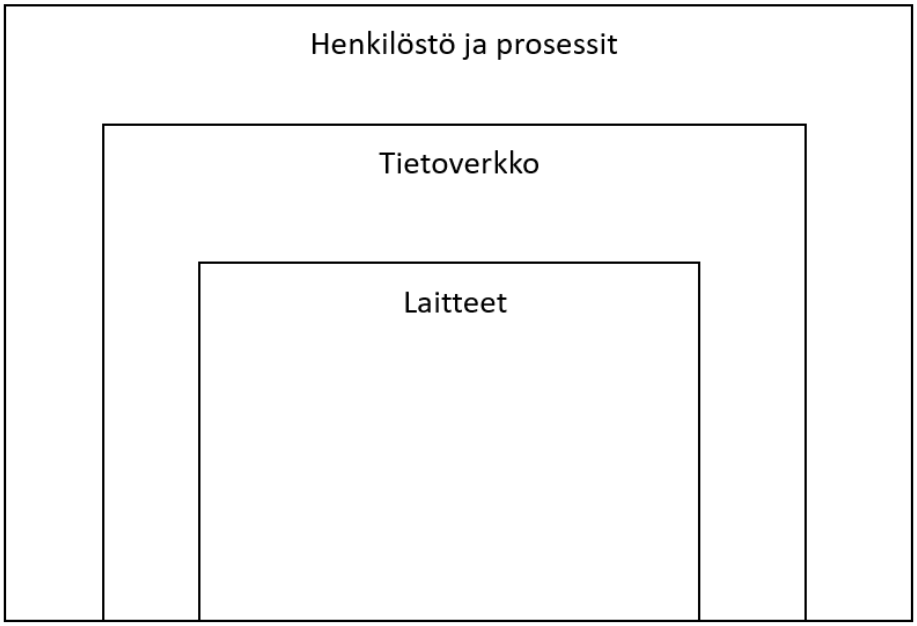
Prikaatin komentajalla on mahdollisuus suunnitella kyberoperaatioita. Komentajan tärkein tuki näiden operaatioiden suunnitteluun ja toteutukseen on esikuntansa elektronisen sodankäynnin henkilöstö, tiedusteluosasto, viestiosasto ja viestikomppania. On kuitenkin hyvä huomioida, että kyberoperaatioiden suunnittelu ei rajoitu pelkästään näihin toimijoihin [5, s. 51 - 60].

3. VALVONNAN TEKNINEN TOTEUTUS

3.1. Syvän puolustuksen teoria

Syvällä puolustuksella tarkoitetaan tietojärjestelmien suojaamisen periaatetta. Sen mukaan tietojärjestelmiä suojataan usealla eri kybertoimintaympäristön tasolla. Kantavana ajatuksena mallissa on se, että yksittäinen turvallisuusratkaisu ei ole riittävä, vaan tarvitaan useita erilaisia ratkaisuja. [8, s. 7; 9, s. 388]

Malleja on saatavilla useita erilaisia, jotka painottavat eri osa-alueita tai ovat yksityiskohteisempia kuin toiset. [9, s. 267; 29, s. 52; 30; 31; 32] Tässä tutkimuksessa syvän puolustuksen kerrokset ovat henkilöstö ja toimintatavat, tietoverkko ja laitteet (kuva 6).



Kuva 6: Syvän puolustuksen kerrokset

3.1.1 Henkilöstö ja toimintatavat

Organisaation kyberturvallisuudesta tulisi vastata koulutettu ja ammattitaitoinen kyberturvallisuuden henkilöstö. On kuitenkin huomioitava, että tämän lisäksi jokaisen tietokoneen käyttäjän tulisi olla tietoinen kyberturvallisuuteen liittyvistä ohjeistuksista ja toimintatavoista [4, s. 24]. [9, s. 59]

Ammattitaitoisen henkilöstön lisäksi tehokkaan puolustuksen toteuttamiseen tarvitaan selkeät toimintatavat. Poikkeaman hallinta, uhkametsästys ja uhkatiedustelu ovat tehokkaan kybervalvonnan kannalta keskeisessä osassa. Henkilöstö ja edelle mainitut toimintatavat käsitellään seuraavassa asialuvussa.

3.1.2 Tietoverkkokerros

Tietoverkkoturvallisuuteen liittyen verkon päätepisteet tulisi konfiguroida siten, että lähtökohtaisesti kaikki liikenne on kielletty mutta kuitenkin erikseen määritellyt yhteydet toimivat [4, s. 24]. Tietoverkon puolustus voidaan jakaa vielä kahteen alakategoriaan, jotka ovat ulkoverkko ja sisäverkko [33].

Ulkoverkolla tarkoitetaan paikkaa, jossa organisaation valvonta ja hallinta loppuvat. Tästä pisteestä alkavat epäluotettavat yhteydet tai esimerkiksi muiden palvelun tarjoajien verkot. Tällä tasolla tavoitteena on estää kaikki ylimääräinen liikenne tietoverkkoon ja valvoa läpi päästettyä tietoliikennettä. [29, s. 52]

Ulkoreunan puolustus toteutetaan yleensä palomuureilla, jotka ovat olennainen osa kybervalvomojen toimintaa, koska niiden avulla saadaan selvitettyä mitä liikennettä suojattavassa tietoverkossa on [8, s. 2; 34, s. 23]. Muita ulkoreunan työkaluja ovat esimerkiksi VPN-yhteydet sekä välityspalvelimet. [9, s. 240 - 241; 29, s. 52; 30]

Sisäverkko voidaan jakaa useisiin eri aliverkkoihin. Turvallisuuteen liittyviä työkaluja tällä tasolla ovat esimerkiksi erilaiset verkkopohjaiset tunkeutumisen esto- ja havainnointijärjestelmät, verkon käyttöoikeuksien hallintaohjelmat (Network Access Control, NAC) sekä datan häviämisen estojärjestelmät (data loss prevention systems). Näiden järjestelmien keräämät lokit ja niiden tekemät hälytykset ovat tärkeitä turvallisuuden kannalta. [29, s. 53; 30] Hälytyksistä saatuja tietoja voidaan käyttää epänormaalin verkkoliikenteen havaitsemiseen, joka aiheutuu haittaohjelmista, datan varastamisesta tai muista haitallisista toimista. [4, s. 27 - 28]

Datan häviämisen estojärjestelmillä valvotaan verkosta siirtyvää dataa. Valvonnan tarkoituksena on varmistua siitä, että datan kuuluukin siirtyä pois valvottavasta verkosta, lähettäjällä on oikeudet siirtää dataa sekä siitä, että data siirtyy luotettavaan paikkaan. [29, s. 53]

Verkon käyttöoikeuksien hallintaohjelman tarkoituksena on valvoa tietoverkossa olevia laitteita ja niiden konfiguraatioita. Yksinkertaisuudessaan ohjelma estää päivittämättömien laitteiden pääsyn verkkoon. [35]

Vaikuttaa kuitenkin siltä, että valvontatyökaluista kaikkein tärkein on verkkopohjainen tunkeutumisen esto- ja havainnointijärjestelmä. [36; 37, s. 88 - 92] Muut työkalut ovat luokiteltavissa puolustusta yleisesti tukeviksi sovelluksiksi. [38, s. 328]

3.1.3 Laitekerros

Laitetason puolustuksella tarkoitetaan palvelimien ja työasemien suojaamista. Tällä tasolla puolustus toteutetaan esimerkiksi virustorjuntaohjelmistoilla, laitepohjaisilla tunkeutumisen esto- ja havainnointijärjestelmillä sekä käyttöjärjestelmän kovennuksilla. [4, s. 24; 9, s. 239; 29, s. 53; 30] Kuten tietoverkkokerroksen valvontaankin liittyen, myös laitekerroksen valvonnan pääasiallisena työkaluna vaikuttaisi olevan tunkeutumisen esto- ja havainnointijärjestelmät [36; 37, s. 88 - 92; 38, s. 328].

Tässä tutkimuksessa laitetaso on jaettu neljään eri alakategoriaan, jotka ovat käyttöjärjestelmä, prosessit, tiedostot ja forensiikka. Käyttöjärjestelmä ohjaa tietokoneen eri komponentteja, ohjelmien resursseja ja tuottaa yleisimmät palvelut eri ohjelmille. Käyttöjärjestelmään kuuluvia valvontakohteita ovat esimerkiksi käyttöjärjestelmän ohjelmointirajapinta, rekisterit, komponenttien firmware ja kernel-ytimen ajurit.

Prosesseilla tarkoitetaan tietokoneessa ajettavia ohjelmia. Tämä voi tarkoittaa esimerkiksi pientä tietokoneen taustalla pyörivää tehtävää, kuten tapahtumien käsittelijää tai isompaa sovellusta, kuten internetselainta. Kaikki prosessit koostuvat, joko yhdestä tai useammasta säikeestä. [39; 40]

Forensiikalla tarkoitetaan sähköisten jälkien analysointia tietokoneissa, tavoitteena löytää tiedon eheyteen tai luottamuksellisuuteen kohdistuneet väärinkäytöt. [41; 42] Jälkien analysointi toteutetaan usein vertaamalla tunnettua hyvälaatuista vedosta tämän hetken tilanteeseen. [43]

3.2. Tunkeutumisen esto- ja havainnointijärjestelmät

Tunkeutumisen esto- ja havainnointijärjestelmät ovat tarkoitettu tietojärjestelmien valvonnan työkaluiksi. Niiden avulla kyetään havaitsemaan tietoturvapoikkeamia. Tunkeutumisen esto- ja havainnointijärjestelmästä käytetään usein lyhennettä IDPS, joka tulee englannin kielen sanoista *Intrusion Detection and Prevention System*. Muita käytettyjä lyhenteitä ovat IDS (Intrusion Detection System, tunkeutumisen havainnointijärjestelmä) ja IPS (Intrusion Prevention System, tunkeutumisen estojärjestelmä). IDS järjestelmä keskittyy ainoastaan tunnistamaan uhkat ja ilmoittamaan niistä järjestelmän ylläpitäjälle, kun taas IPS toimii aktiivisesti ja myös estää mahdolliset uhkat automaattisesti. Tunkeutumisen estojärjestelmän voidaan siis ajatella olevan tietynlainen lisäosa normaaliin havainnointijärjestelmään. [37, s. 15 - 17; 38, s. 293; 9, s. 293]

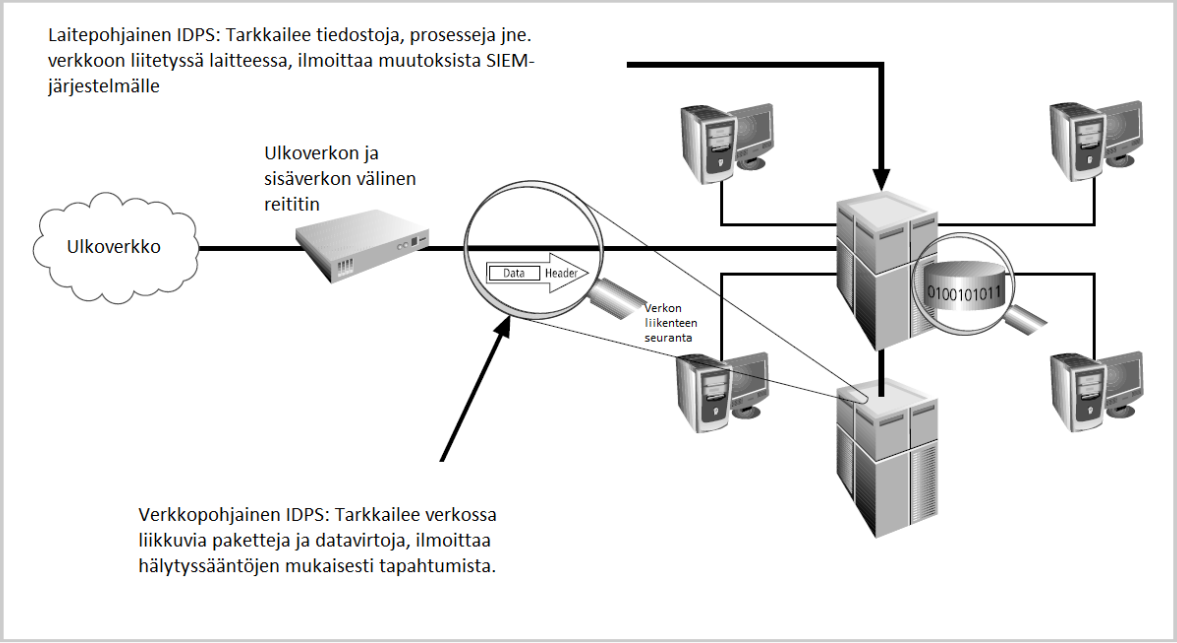
IDPS-ohjelmistoja käytetään perinteisten palomuurien sekä virustorjuntaohjelmien rinnalla. Ne täydentävät verkon puolustusta, tuottamalla ja varastoimalla tietoja tietojärjestelmistä sekä muokkaamalla kohdeympäristöä. Niillä ei siis ole tarkoitus korvata virustorjuntaohjelmia ja palomuureja vaan lisätä tietoturvallisuutta entisestään. [38] On kuitenkin syytä huomioida, että jotkin IDPS:t voidaan konfiguroida siten, että ne estävät verkkoliikennettä kuten palomuurit. Lisäksi ne voidaan konfiguroida tunnistamaan tiedostoja, jotka ovat epäilyttäviä. [37]

Monissa hyökkäyksissä hyökkääjä suorittaa tiedustelua kohteeseen ennen varsinaista iskua. IDPS-järjestelmällä on mahdollista havaita tämän tyyppiset tiedustelut ennakolta. [37; 38]

IDPS mahdollistaa hyökkäysten seurannan keräämällä dataa järjestelmästä. Dataa voidaan lähettää SIEM-järjestelmälle, jossa kerätty data käsitellään. Datan avulla kyetään mahdollisesti selvittämään, onko toteutunut tietoturvatapahtuma todellinen poikkeama vai ei. Lisäksi kerättyä dataa voidaan käyttää hyökkäyksistä oppimisen tukena. Kerätystä datasta voidaan esimerkiksi selvittää minkä haavoittuvuuden kautta hyökkääjät ovat päässeet järjestelmään. Lisäksi kerätyn datan ansiosta hyökkääjän on todella haastavaa saada peitettyä jälkensä hyökkäyksen jälkeen. [9, s. 304; 37, s. 16; 38]

3.2.1 Verkko- ja laitepohjaiset IDPS-järjestelmät

IDPS-ohjelmistot voidaan luokitella useilla eri tavoilla. Niiden jako voidaan tehdä joko niiden sijainnin tai havainnointitekniikan mukaan. Mikäli IDPS-ohjelmistot luokitellaan niiden sijainnin mukaan, yleinen jako tapahtuu verkkopohjaiseen (Network-based) ja laitepohjaiseen (Host-based) tunkeutumisen esto- ja havainnointijärjestelmään. [37, s. 17 - 21] Verkko- ja laitepohjaisen IDPS:n toimintaperiaatteet ovat esitetty kuvassa 7. [38]



Kuva 7: Verkko- ja laitepohjaisen IDPS:n toimintaperiaatteet

Verkkopohjaiset (network-based) tunkeutumisen esto- ja havainnointijärjestelmät valvovat tiettyä verkon osaa havaitakseen epäilyttävää verkkoliikennettä. Lisäksi ne analysoivat verkon ja sovellusten käyttämiä protokollia havaitakseen epänormaalia käyttäytymistä. Kun järjestelmä havaitsee hyökkäyksen, ilmoittaa se siitä järjestelmänvalvojalle. [9, s. 302 - 303; 37, s. 20]

Verkkopohjainen järjestelmä tulisi asettaa jokaiseen verkkosegmenttiin, joka keskustelee toisen segmentin kanssa ja joiden välillä liikkuu data. Nämä IDPS:t mahdollistavat verkkoliikenteen seurannan kaiken datan osalta, joka kulkee solmukohdan läpi. [29, s. 53] Prikaatin johtamisjärjestelmätasolla tämä voisi tarkoittaa esimerkiksi sitä, että verkkopohjainen IDPS sijoitetaan pisteeseen, joka erottaa prikaatin verkon divisioonan verkosta. Tai vaihtoehtoisesti sekä pääkomentopaikalle että taktiselle komentopaikalle.

Verkkopohjaisia järjestelmiä ovat myös langaton (wireless) ja verkkokäyttäytymisen analysointiin (NBA, Network Behaviour Analysis) perustuvat IDPS-järjestelmät. Langattoman ja NBA -järjestelmän toimintaperiaatteet ovat erilaisia verrattuna puhtaaseen verkkopohjaiseen järjestelmään. [37, s. 20 - 21]

NBA tarkkailee kohdeverkossa liikkuvaa dataa ja pyrkii tunnistamaan datavirrasta normaalista poikkeavaa liikennettä, kuten esimerkiksi palvelunestohyökkäyksiä ja haittaohjelmia. Langaton järjestelmä nimensä mukaisesti valvoo langatonta tiedonsiirtoa. [37, s. 21; 38, s. 297 - 299]

Laitepohjainen (host-based) IDPS valvoo tiettyä tietokonetta tai palvelinta. Tällainen järjestelmä kykenee valvomaan esimerkiksi verkkoliikennettä (ainoastaan valvottavan laitteen osalta), järjestelmälokeja, käytettäviä prosesseja, sovellusten sekä tiedostojen käyttöä ja niiden konfiguraatioiden muokkaamista. Usein laitepohjaiset järjestelmät sijoitetaan kriittisimpiin laitteisiin, kuten palvelimiin joissa on arkaluontoista tietoa. [37, s. 21] Järjestelmä kykenee valvomaan kohdejärjestelmässä salauksesta purettavia tiedostoja, joita verkkopohjainen järjestelmä ei kykene salauksen johdosta valvomaan. [9, s. 304; 38]

3.2.2 IDPS-järjestelmien havaintotekniikat

IDPS-ohjelmistot voidaan jakaa havainnointitekniikan mukaan tunnisteisiin (signature-based), poikkeavuuksiin (anomaly-based) ja protokollaan (stateful protocol analysis) perustuviin tunkeutumisen esto- ja havainnointijärjestelmiin. [37, s. 17 - 21; 38]

Tunnisteisiin perustuva (signature-based) havainnointijärjestelmä tarkkailee tiettyjä ennalta määritettyjä hyökkäystapoja verkkoliikenteestä. Tätä tekniikkaa käytetään laajalti, koska monet hyökkäykset ovat samankaltaisia keskenään. Haasteena tässä tekniikassa on se, että uusia hyökkäystapoja täytyy jatkuvasti päivittää IDPS-järjestelmän kirjastoon. Uudenlaisia hyökkäyksiä ei havaita, mikäli niitä ei ole päivitetty järjestelmän kirjastoon. Toinen merkittävä heikkous tämän kaltaisissa ohjelmistoissa on se, että todella hitaasti toimivassa hyökkäyksessä IDPS ei havaitse mitään normaalista poikkeavaa. Tämä johtuu siitä syystä, että IDPS tarkastelee suhteellisen lyhyitä ajanjaksoja. Jos IDPS asetetaan seuraamaan pidemmän aikavälin tapahtumia tästä seuraa se, että sovellus vie huomattavasti enemmän tietokoneen muistia ja prosessointitehoa. [9, s. 302; 38]

Poikkeavuuksiin perustuva (statistical anomaly-based) havainnointijärjestelmä kerää näytteen normaalista verkkoliikenteestä. Tämän jälkeen ohjelma vertaa tätä perustasoa sen hetkiseen verkkoliikenteeseen ja arvioi onko liikenteessä jotain mikä ei sinne kuulu. IDPS vertailee esimerkiksi näinä kahtena ajankohtana käytetty laitemuistia, prosessorin kuormitusta, verkossa liikkuvien pakettien tyyppejä tai niiden määrää. Tämän kaltaisessa tunnistuksessa on huomattava ero tunnisteisiin perustuvaan järjestelmään verrattuna, koska poikkeavuuksiin perustuvassa järjestelmässä huomataan myös uudentyyppiset hyökkäykset. Tämä tosin vaatii huomattavasti enemmän suorituskykyä itse laitteelta. [9, s. 303; 38]

Protokollatunnistukseen (Stateful Protocol Analysis) perustuva havainnointijärjestelmä toimii hieman samaan tapaan kuin poikkeavuuksiin perustuva järjestelmä. Se tarkkailee liikennettä ja vertaa sitä normaaliin liikenteeseen. Tämän tyyppinen havainnointijärjestelmä kuitenkin toimii, nimensä mukaisesti, protokolla tasolla. Tämä tarkoittaa sitä, että verkkoliikenteessä siirtyviä paketteja seurataan IDPS:n toimesta ja pyritään niistä löytämään tunkeutumisen merkkejä. [38]

3.2.3 IDPS:n vastatoimet tietoturvatapahtumaan

IDPS-järjestelmän vastatoimet voidaan jakaa passiivisiin ja aktiivisiin. Passiivisesti toimivalla IDPS:llä tarkoitetaan tilannetta jossa ohjelmisto ilmoittaa epäillystä tunkeutumisesta järjestelmänvalvojalla (IDS, Intrusion Detection System). Tätä seuraavat toimenpiteet hoitaa järjestelmänvalvoja analysoidun tiedon perusteella. Aktiivisissa toimenpiteissä IDPS voi automaattisesti esimerkiksi alkaa kerätä ylimääräistä dataa, muokkaamaan verkkoympäristöä tai tekemään vastatoimia tunkeutujan toimia vastaan (IPS, Intrusion Prevention System). [9, s. 293; 38]

Kun tietoturvatapahtuma havaitaan, organisaation tavoitteet ja IDPS-järjestelmän ominaisuudet määräävät sen, millaisiin vastatoimiin IDPS-järjestelmän avulla ryhdytään. Vastatoimia suunniteltaessa järjestelmänvalvojan on mietittävä, kuinka erilaisiin tietoturvatapahtumiin vastataan. Esimerkiksi palvelunestohyökkäyksen vastatoimena voisi olla esimerkiksi tiettyjen IP-osoitteiden rajoittaminen. Mahdollisia vastatoimenpiteitä voivat olla esimerkiksi: [38, s. 307 - 309]

- Lokitietojen tallennus
- Palomuuriasetuksien muuttaminen
- Haitallisen liitetiedoston poistaminen
- Hyökkääjän käyttäjätunnuksen eristäminen
- Hyökkääjän IP-osoitteen eristäminen

3.2.4 IDPS-järjestelmien vahvuudet ja heikkoudet

IDPS-ohjelmistot ovat tärkeä lisä organisaation tietoturvallisuudelle. On kuitenkin hyvä huomioida IDPS-ohjelmistojen vahvuudet ja heikkoudet. Tällä tavoin organisaatioon kyetään rakentamaan paras mahdollinen suoja, kun ymmärretään missä tilanteissa tunkeutumisen esto- ja havainnointijärjestelmät ovat parhaimmillaan ja missä heikoimmillaan. [9, s. 293 - 305; 38, s. 315 - 316]

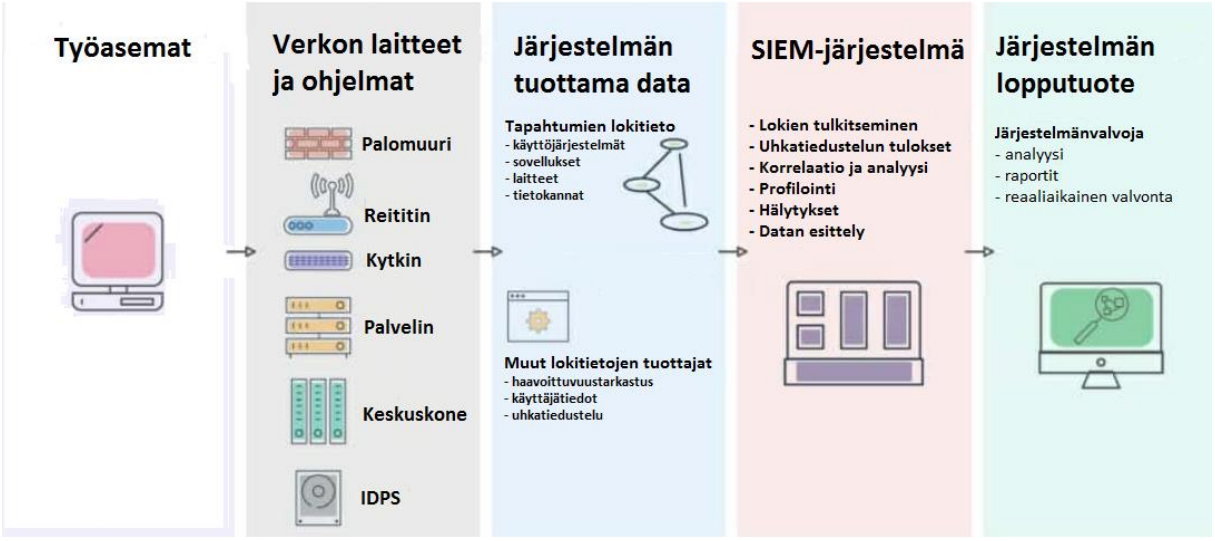
IDPS-ohjelmistojen vahvuudet ovat käyttäjien ja järjestelmien eri tapahtumien tarkkailussa. Ne kykenevät tunnistamaan kaavamaiset hyökkääjät helposti sekä ymmärtämään, milloin verkkoliikenne on normaalia ja milloin verkossa tapahtuu jotain sinne kuulumatonta. [9, s. 293 - 305; 38, s. 315 - 316]

IDPS-ohjelmisto ei sovellu kuitenkaan kaikkiin mahdollisiin tilanteisiin. Se ei voi havainnoida, raportoida sekä vastata hyökkäyksiin, jos verkossa on todella paljon liikennettä. IDPS-ohjelmisto ei kykene itsestään selvittämään hyökkäyksiä vaan se vaatii aina operaattorin. Suurena ongelmana IDPS-ohjelmistoille ovat myös väärät hälytykset (false-positive). On erittäin haastavaa löytää tasapaino hälytyksille siten, että IDPS ei tuota liikaa hälytyksiä mutta se ei myöskään jätä hälyttämättä todellisissa tilanteissa. [9, s. 293 - 305; 38, s. 315 - 316]

IDPS:t ovat tärkeä osa kybervalvomon toimintaa, mutta niiden käyttäminen vaatii myös jatkuvaa päivittämistä. Tällä tavoin IDPS:t kykenevät havainnoimaan tietoturvapoikkeamia mahdollisimman tehokkaasti. [29, s. 53]

3.3. SIEM-järjestelmä ja lokitus

Tunkeutumisen esto- ja havainnointijärjestelmien lisäksi tietojärjestelmien tehokkaaseen valvontaan tarvitaan SIEM-järjestelmä [44, s. 37]. SIEM kirjainyhdistelmä tulee sanoista ”Security Information and Event Management”. SIEM-järjestelmän avulla kyetään yhdistelemään eri tietoteknisten järjestelmien keräämiä turvallisuuteen liittyviä lokeja. Se mahdollistaa kerättyjen lokien jatkokäsittelyn tarjoamalla uutta tietoa yhdistelemällä tietoa monien eri lähteiden lokeista. [29, s. 13; 45; 46] SIM- (Security Information Management) ja SEM- (Security Event Management) ovat käytännössä SIEM-järjestelmän osajärjestelmiä. SIEM-järjestelmän toimintaperiaate on kuvattu seuraavassa kuvassa. [36]



Kuva 8: SIEM-järjestelmän toimintaperiaate

Loki on tallenne tapahtumasta, joka on tapahtunut tietojärjestelmässä. Lokit koostuvat lokimerkinnöistä (log entry). Jokainen näistä merkinnöistä sisältää tietoa tietystä tapahtumasta, joka on toteutunut järjestelmässä (jokainen tapahtuma ei kuitenkaan ole tietoturvatapahtuma). Monet lähteet tuottavat tietoturvallisuuteen liittyviä lokeja, kuten esim. tietoturvaohjelmat, käyttöjärjestelmät, verkon eri laitteet sekä sovellukset. [4, s. 27; 29, s. 13; 36; 47, s. 9; 48]

SIEM-järjestelmä tarjoaa seuraavia toiminnallisuuksia: [29; 36; 44, s. 36; 48]

- Lokien keräys monista eri lähteistä sisältäen mm. tietoverkon, eri tietoturvaohjelmistot, palvelimet, tietokannat ja sovellukset.
- Tiedon säilytys ja haku mahdollistavat pitkän aikavälin seurannan datalle. Järjestelmää voidaan käyttää näin ollen myös kehittyneitä hyökkäyksiä vastaan, jotka vaikuttavat järjestelmässä pitkän ajan kuluessa.
- Hälyttäminen voidaan toteuttaa tiettyjen tapahtumaketjujen seurauksena. Esimerkiksi kirjautuminen järjestelmään käyttäjätunnuksella, joka ei täsmää palomuurin lokissa kirjattuun IP-osoitteeseen. Tai epäonnistuneiden kirjautumisyritysten määrä ylittyy määritetyssä aikaraamissa.
- Käyttöliittymä helpottaa valvontaa suorittavaa operaattoria havaitsemaan poikkeamat tietojärjestelmässä.
- Tietojen yhdistäminen mahdollistaa korrelaation löytämisen eri tietoturvatapahtumien väliltä. Näin useista tietoturvatapahtumista voidaan tarvittaessa muodostaa tietoturvapoikkeama.

SIEM-järjestelmän tarkoituksena on havainnoida ympäristöä ja prosessoida sieltä saatuja tietoja. Järjestelmä prosessoi tehdyt havainnot ja tallentaa kerätyt tiedot myöhempää käyttöä varten. Tietoa SIEM kerää valvottavan järjestelmän tuottamasta lokitiedoista, verkkoliikenteestä sekä tarvittaessa ulkopuolisista lähteistä. [46]

Tiedon prosessointia voidaan tehdä joko automaattisesti tai manuaalisesti. Tavoitteena on pitää manuaalisen analysoinnin osuus mahdollisimman pienenä, jotta suojaaminen pysyy mahdollisimman tehokkaana. [46; 49, s. 2]

SIEM-järjestelmä on sitä hyödyllisempi mitä enemmän tietoja ja havaintoja se kerää. Kuitenkin mitä enemmän havaintoja ja tietoja kerätään, sitä enemmän tarvitaan tallennuskapasiteettia. [44, s. 39; 46]

SIEM-järjestelmä valitaan suoritettavan tehtävän mukaan. SIEM-järjestelmän valintaan vaikuttavat vaadittava havainnointinopeus, tiedon jalostusaste sekä tiedon laaja-alaisuus. Valvomossa tarvitaan laaja-alaista tietoa koko kohdeympäristöstä mahdollisimman nopeasti. Näin ollen havainnoinnin täytyy olla pitkälle automatisoitu. [46] Manuaalisen työn määrä tulee olla suhteutettu henkilöstömäärään.

Organisaation tulisi varmistua siitä, että jokainen lokia tuottava järjestelmä tuottaa riittävän tarkkaa lokia. Mitä tärkeämmästä järjestelmästä on kyse, sitä tarkempia myös lokien tulee olla. [4, s. 27; 29, s. 14]

Lokien käsittely aiheuttaa haasteita, koska lokia tuottavia lähteitä on paljon ja ne tuottavat erittäin paljon lokitietoja [44, s. 39; 47, s. 9]. Lokien keräämisen määrän suhteen kannattaa aloittaa pienestä määrästä ja lisätä kerättäviä lokeja kokemuksen karttuessa sekä tarpeen mukaan [50].

Lokien säilytysaika vaihtelee suojattavan kohteen mukaan. Säilytysaika vaihtelee yleisesti 6 - 24 kuukauden välillä [50]. Mahdolliseen säilytysaikaan vaikuttaa suoraan säilytyskapasiteetti [44, s. 39].

Tietoturvalokien suuresta ja vaihtelevasta määrästä johtuen lokien käsittelyyn täytyy kiinnittää huomiota. Lokien käsittelyyn on luotava selkeä toimintatapa, joka kattaa niiden luonnin, siirron, säilytyksen, analyysin ja hävittämisen [50]. Lokien käsittely on välttämätöntä, jotta voidaan varmistua siitä, että lokit ovat säilöttynä tarvittavilta osin, tarvittavan ajan. Rutiinin omainen lokien analysointi on hyödyllistä tietoturvatapahtumien seurantaan. [47, s. 9]

Olennaisena osana lokien käsittelyyn liittyen on määrittää lokien vaatimukset ja tavoitteet. Mikäli lokien käsittelijöillä ei ole selkeää tavoitetta määritelty, riskinä on, että he ylikuormittuvat suuren datamäärän alle. Kun käsiteltävää dataa on paljon, on oltava selkeät ohjeet siitä mihin keskitytään ja mikä jätetään pienemmälle huomiolle [49]. [47, s. 9 - 10]

On tärkeää tarkastaa säännöllisin väliajoin, että lokien keräämä tieto on tarkoituksenmukaista. Lokit tuottavat erittäin paljon erilaista tietoa, joten on tarkasti määritettävä se tieto, joka on tavoitteiden mukaan tarpeellista. Kaikki lokitiedot keräämällä varastointikapasiteetti ja väärien hälytysten määrät kasvavat erittäin suuriksi. [29, s. 29 - 31] Mikäli lokeja kerätään todella vähän, hyökkäys voi jäädä havaitsematta kokonaan. [44] s. 38

Kerätyistä lokeista tarvittavia tietoja ovat: käyttäjän tunnistetiedot, tapahtuman tyyppi, tapahtuman alkuperäinen paikka, vakavuus, aika, palvelun nimi, protokolla ja käyttäjä. Muita tärkeitä kerättäviä tietoja ovat: [29, s. 13 - 16]

- Kaikki root tai järjestelmänvalvojan tekemät toimenpiteet [4, s. 27].
- Pääsyt lokitietoihin ja niiden käsittely
- Tunnistautumisessa tehtävät toimenpiteet (onnistuneet ja epäonnistuneet) [4, s. 27].
- Järjestelmätasossa tehdyt tiedostojen/vast. luonnit tai poistot

Organisaation tulisi määrittää roolit ja vastuut lokien käsittelystä kaikkien avainhenkilöiden osalta [47, s. 10]. Tämä tarkoittaa esimerkiksi sitä, että tietoturvavastaavat seuraavat turvallisuuteen liittyviä lokeja, kun taas ylläpitäjät heille tarpeellisia lokeja. Kerätyille lokeille on oltava jokin peruste, ja niiden asianmukaisuudesta ja turvallisuudesta on huolehdittava säännöllisesti auditoinneilla. [50]

Lokien käsittelyyn liittyvään infrastruktuuriin kuuluvat laitteet, ohjelmat, tietoverkot ja media, joilla tuotetaan, lähetetään, varastoidaan, analysoidaan ja poistetaan lokitietoja. Organisaation kannattaa muodostaa tehokkaaseen lokien käsittelyyn keskitettyjä lokipalvelimia ja lokien tallennusvälineitä. [47, s. 10]

4. KYBERVALVOMOT JA POIKKEAMAN HALLINTARYHMÄT

Kybervalvomoista ja poikkeaman hallintaryhmistä on käytössä useita eri nimityksiä: CIRC (Computer Incident Response Center), SOC (Security Operations Center), CSOC (Cyber Security Operations Center), CIRT (Computer Incident Response Team) ja CERT (Computer Emergency Response Team). [3, s. 1; 51]

Valvomojen ja ryhmien palveluissa ei ole havaittavissa selkeää yhdenmukaista linjaa. Useissa eri lähteissä toiminteet eroavat toisistaan jonkin verran. Tämä johtuu todennäköisesti siitä, että eri organisaatioilla on erilaiset palvelutarpeet, ja näin ollen eri organisaatiot puhuvat esimerkiksi CSOC:sta tarkoittaen kuitenkin hieman eri asioita. [3; 4; 51; 52]

Kybervalvomo (CSOC ja SOC) vaikuttaisi kuitenkin olevan useimpien lähteiden mukaan kattavin keskusorganisaatio, joka sisältää eniten erilaisia palveluita. Poikkeaman hallintaan keskittyvät ryhmät ja keskukset (CSIRT ja CIRC) ovat näissä määritelmissä vain yksi osa kybervalvomon toimintaa. [1; 4; 51; 52]

Kybervalvomolla tarkoitetaan jatkuvaan kyberuhkien valvontaan, analyysiin, pienentämiseen ja estämiseen keskitettyä osastoa. Tehtävä toteutetaan muun muassa uhkien, poikkeamien ja haavoittuvuuksien hallinnalla, verkon valvonnalla, erilaisilla koulutuksilla ja tietoturvaloukkauksien tutkinnalla. [3, s. 2] Tehokas valvomo on toiminnassa ympärivuorokauden, ja se kykenee tehokkaasti ennakoimaan, estämään ja havaitsemaan erilaiset kyberuhkat ja vastaamaan niihin. [49, s. 1; 51]

Poikkeaman hallintaryhmä (CSIRT ja CIRC) keskittyy nimensä mukaisesti ainoastaan tietoturvapoikkeamien hallintaan. Se tukee kuitenkin valvomon muita toimintoja resurssien antamissa puitteissa. [3, s. 17 - 18]

4.1. Kybervalvomojen yleisimmät palvelut

Kybervalvomot voivat tarjota monipuolisia palveluita. On kuitenkin hyvä huomioida, että esitellyt palvelut eivät kaikki sellaisenaan liity suoranaisesti kybervalvontaan, mutta tukevat kuitenkin organisaation kyberturvallisuutta.

Kybervalvomojen tarjoamat palvelut voidaan jakaa kolmeen kategoriaan. Nämä kategoriat ovat reaktiiviset-, proaktiiviset- ja laadunhallintapalvelut. Seuraavassa kuvassa on esitelty yleisimmät palvelut, joita kybervalvomot tarjoavat. [3, s. 20 - 25; 53; 54; 55]

Reaktiiviset palvelut	Proaktiiviset palvelut	Laadunhallintapalvelut
Varoitukset ja hälytykset Tietoturvatapahtumien käsittely - analysointi - vastatoimet - koordinointi Haavoittuvuuksien hallinta - analysointi - vastatoimet - koordinointi Haitallisten kohteiden hallinta - analysointi - vastatoimet - koordinointi	Ilmoitukset Teknologisen kehityksen seuraaminen Turvallisuusauditoinnit Turvallisuuteen liittyvien työkalujen päivittäminen Tiedottaminen	Organisaation riskien analysointi Organisaation toiminnan turvaaminen ja palautumissuunnitelma Arviointi ja vaatimukset uusien hankintojen osalta Kyberturvallisuuskoulutus

Kuva 9: Yleisimmät tietoturvavalvomojen tarjoamat palvelut

Kybervalvomojen tulee valita tarjoamansa palvelut huolella. Tarjotut palvelut heijastuvat suoraan vaadittaviin resursseihin, kykyihin ja yhteistyökumppaneihin. Tarjotut palvelut tulisivat olla yhteneväiset organisaation muihin tavoitteisiin nähden. [53, s. 1; 54] Perusyhtymätasolla tämä voisi tarkoittaa sitä, että kybervalvomo tai poikkeaman hallintaryhmä tarjoaa vain tiettyjä palveluita, koska alueellinen kyberkeskus hoitaa tietyn osan palveluista.

4.1.1 Reaktiiviset palvelut

Reaktiivisilla palveluilla tarkoitetaan toimenpiteitä, jotka aloitetaan, kun tietoturvatapahtuma havaitaan [3; 53, s. 3; 54]. Tietoturvatapahtumalla tarkoitetaan tilannetta, jolloin suojattavan tietojärjestelmän tietojen tai palveluiden tila on muuttunut ja sen seurauksena tietoturva saattaa vaarantua [26, s. 16]. [4, s. 6]

Reaktiiviset palvelut tuottavat varoituksia ja hälytyksiä [54; 55], jotka levittävät tietoa tunkeutumista järjestelmään, haavoittuvuuksista, viruksista tai esimerkiksi erilaisista huijauksista. Varoituksia ja hälytyksiä tuottavat kybervalvomot kuin valvomon ulkopuolisetkin tahot. [53, s. 3]

Reaktiivisiin palveluihin kuuluu tietoturvatapahtumien käsittely [54; 55]. Siihen kuuluu tietoturvatapahtumien vastaanottaminen, tapahtumien lajittelu, vastatoimet ja analysointi. Vastatoimet pitävät sisällään kohteina olleiden/olevien tietojärjestelmien suojaamisen, järjestelmän korjaamisen sekä päivittämisen. [53, s. 3]

Haavoittuvuuksien hallinta kuuluu osaksi reaktiivisia palveluita [54; 55]. Tämä tarkoittaa haavoittuvuus tietojen saantia laitteista ja ohjelmista, joiden analysoinnilla kyetään korjaamaan haavoittuvuudet suojattavasta järjestelmästä. [53, s. 5]

Haitallisten kohteiden hallinta on osa reaktiivisia palveluita [55]. Haitallisia kohteita voivat olla esimerkiksi virukset, troijalaiset, madot tai komentosarjat. [54] Hallinnalla tarkoitetaan tiedon saantia haitallisesti kohteesta, jota hyökkääjä käyttää tunkeutumisessaan. Tämän jälkeen haitallista kohdetta tarkastellaan ja tarkastelun tuloksena parannetaan kohteen suojausta. [53, s. 5 - 6]

4.1.2 Proaktiiviset palvelut

Proaktiivisten palveluiden avulla kehitetään organisaation infrastruktuuria ja kyberturvallisuuteen liittyviä toimintatapoja. Kehittäminen on tarkoitus toteuttaa ennen tietoturvapoikkeamien ilmaantumista. Lisäksi tavoitteena on pienentää tietoturvapoikkeamien mahdollisia vaikutuksia niiden sattuessa. [54] Lopullisena tavoitteena on estää tietoturvapoikkeamat kokonaan. [3; 53, s. 6] On kuitenkin syytä huomioida, että esitelty palvelutaulukko on vuodelta 2002. Siinä ei ole suoraan huomioitu esimerkiksi nykyhetken vaatimuksia proaktiivisesta uhkametsästyksestä, joka on NIST-organisaation tuottaman kyselyn mukaan yksi keskeinen elementti nykyaikaisten tietoturvahyökkäysten havainnoinnissa [56, s. 15].

Proaktiiviset palvelut tuottavat ilmoituksia haavoittuvuuksiin sekä turvallisuuteen liittyen [54; 55]. Ilmoitukset antavat uutta tietoa siitä, millaisia vaikutuksia uusilla haavoittuvuuksilla tai tunkeutumiseen tarvittavilla työkaluilla on. Ilmoitusten avulla kyetään parantamaan suojautumista uusia uhkia vastaan. [53, s. 6]

Proaktiivisten palvelujen osana kybervalvomot seuraavat uusien kyberturvallisuusratkaisujen kehittymistä, hyökkääjien toimintaa ja näihin kuuluvia trendejä. [54; 55] Näitä tietoja käytetään tulevaisuuden uhkien tunnistamiseen. Näiden toimintojen lopputuloksena tuotetaan ilmoituksia, ohjeita tai suosituksia, jotka painottuvat kyberturvallisuudessa pitkälle tai keskipitkälle aikavälille. [53, s. 6]

Proaktiivisiin palveluihin kuuluu turvallisuusauditoinnit ja -arvioinnit. [54; 55] Tämän avulla selvitetään, vastaako organisaation infrastruktuurin kyberturvallisuus sille asetettuja vaatimuksia. Arviointeja toteutetaan esimerkiksi organisaation infrastruktuuriin ja käytänteisiin liittyen. Lisäksi erilaisilla penetraatiotestauksilla ja järjestelmän skannauksilla voidaan toteuttaa arviointeja. [53, s. 6 - 7]

Infrastruktuurin arvioinnissa arvioidaan manuaalisesti laitteistojen ja ohjelmistojen konfiguraatioita, reitittimiä, palomuureja, palvelimia ja työpöydän laitteita. Arvioinnissa varmistutaan, että ne vastaavat organisaation vaatimuksia. [53, s. 7]

Parhaiden käytänteiden arvioinnissa haastatellaan työntekijöitä ja järjestelmänvalvojia. Tämän tarkoituksena on varmistua, että heidän toimintatapansa vastaavat organisaation käytäntöjä. [53, s. 7]

Penetraatiotestauksessa hyökätään suojattavaan tietojärjestelmään. Lopputuloksena kyetään havaitsemaan pahimmat puutteet organisaation turvallisuudessa. [49, s. 27] Skannauksen avulla tarkastetaan järjestelmän ja verkon haavoittuvuuksia. [53, s. 7]

Olennaisena osana proaktiivisiin palveluihin kuuluu turvallisuustyökalujen, -sovellusten, -infrastruktuurin ja -palveluiden konfigurointi, kehittäminen ja kunnossapito. [54; 55] Tämä voi tarkoittaa päivitysten kehittämistä tai asentamista olemassa oleville sovelluksille. Tai se voi tarkoittaa esimerkiksi uuden liitännäisen kehittämistä haavoittuvuutta vastaan. Kyseiseen toimintaan kuuluu lisäksi ongelmakohtien kertominen esimiehille, liittyen konfiguraatioihin tai työkaluihin. [53, s. 7]

Turvallisuuteen liittyvä tiedottaminen on osa proaktiivisia palveluita. [54; 55] Tiedottamisen avulla levitetään tietoa siitä, kuinka turvallisuutta voidaan organisaatiossa parantaa. [53, s. 8]

4.1.3 Turvallisuuteen liittyvät laadunhallintapalvelut

Laadunhallintapalveluilla tarkoituksena on yleisesti parantaa koko organisaation turvallisuutta [54; 55]. Laadunhallinnassa käytetään hyväksi reaktiivisten ja proaktiivisten palveluiden tuottamaa tietoa. [3; 53, s. 8]

Kybervalvomo osallistuu organisaation riskien analysointiin oman toimintansa osalta [54; 55]. Tämä voi parantaa organisaation kykyä keskittyä todellisiin uhkiin ja näin organisaatio voi tehostaa toimintaansa. Kybervalvomo arvioi uhkien ja hyökkäysten mahdollisia vaikutuksia suojattavaan järjestelmään. [53, s. 9]

Organisaation toiminnan turvaaminen ja palautumissuunnitelma on osa turvallisuuteen liittyvää laadunhallintaa [54; 55]. Kybervalvomo arvioi, kuinka mahdolliset hyökkäykset tulevat vaikuttamaan organisaation toimintaan kokonaisuutena ja kuinka niihin vastataan. Arvion pohjana käytetään jo tapahtuneita tietoturvapoikkeamia ja turvallisuustrendejä. [53, s. 9]

Laadunhallinnassa kybervalvomon tulee laatia arvioita ja vaatimuksia uusien turvallisuusjärjestelmien, verkkolaitteiden tai ohjelmien hankinnasta [54; 55]. Tähän kuuluu myös organisaation uusien turvallisuuteen liittyvien toimintatapojen kehittäminen. [53, s. 9]

Laadunhallinnassa kybervalvomo voi tarjota kyberturvallisuuskoulutusta [54; 55]. Koulutus voi pitää sisällään tietoa siitä, kuinka turvata, havaita, ilmoittaa ja vastata tietoturvatapahtumiin. Tämä voi vähentää onnistuneiden hyökkäyksien määrää tulevaisuudessa ja lisätä mahdollisuutta, että hyökkäykset havaitaan ajoissa ja niistä ilmoitetaan asiaan kuuluvasti. Kun hyökkäykset havaitaan ajoissa, hyökkäyksistä palautumiseen kuluu vähemmän aikaa ja niiden vaikutukset voidaan minimoida. [53, s. 9 - 10]

4.2. Tietoturvavalvomojen henkilöstö

Kybervalvomojen toimintaan liittyy useita erilaisia rooleja. On huomioitava, ettei kaikkia rooleja välttämättä tarvita jokaisessa valvomossa. Lisäksi pienemmissä valvomoissa yksi henkilö voi tehdä mahdollisesti useita eri rooleja tai isommissa toimipisteissä monta henkilöä voi tehdä yhden roolin tehtäviä. [49, s. 5]

Erilaisia analyyseja suorittavia tehtäviä ovat tasojen 1 - 3, haittaohjelmien, forensiikan, uhkatiedustelun analysoijat. Lisäksi henkilöstöön kuuluvat kybervalvomon järjestelmänvalvoja, haavoittuvuusarvioitsija, turvallisuusinsinööri ja kybervalvomon päällikkö. [29, s. 117 - 120; 49, s. 5 - 6; 57, s. 87 - 100]

Tason 1 analysoijaa voidaan ajatella tietoturvatapahtumien lajittelijana. Hänen tehtävänä on pääsääntöisesti valvoa SIEM-järjestelmän antamia hälytyksiä ja päättää mitkä niistä ovat mahdollisia tietoturvapoikkeamia ja mitkä ovat vääriä hälytyksiä. Mikäli järjestelmä antaa tason 1 analysoijan mielestä liikaa false-positive -hälytyksiä, hän voi pyytää turvallisuusinsinööriä säätämään järjestelmää. Mikäli tason 1 analysoija ei kykene määrittämään onko hälytyksessä kyse tietoturvapoikkeamasta vai false-positive -hälytyksestä, hän siirtää käsittelyn ylemmän tason analysoijalle. [29, s. 109 - 111; 44, s. 37; 49, s. 5; 57, s. 94 - 95]

Tason 2 analysoija on tietoturvapoikkeamien käsittelijä. Hän tehtävänään on analysoida hälytyksiä, jotka saapuvat hänelle tason 1 analysoijalta. Tasolla 2 on käytössä enemmän informaatiota hälytyksen selvittämiseksi. Lisäinformaatiota saadaan esimerkiksi järjestelmälokeista, uhkatiedustelusta ja ulkopuolisista lähteistä. Havaitessaan hyökkäyksen tason 2 analysoija siirtää tapahtuman eteenpäin, jossa selvitetään hyökkäyksen laajuus ja vaikutus. Hyökkäys pyritään eristämään sekä poistamaan ja aikanaan hyökkäyksestä pyritään palautumaan. Mikäli kyseessä oli false-positive -hälytys, hän tarvittaessa pyytää turvallisuusinsinööriä hienosäätämään järjestelmää edelleen. [29, s. 109 - 111; 44, s. 37; 49, s. 5]

Tason 3 analysoija vastaa kybervalvomon suorittamasta uhkametsästyksestä. Lisäksi uhkametsästäjä osallistuu korkean prioriteetin tietoturvapoikkeamien hallintaan, koska hän on usein ammattitaitoisin henkilö käsittelemään kehittyneimpiä hyökkäyksiä. Hänen tehtävänään on kehittää uhkametsästyksen perusteella valvontajärjestelmää. [49, s. 6]

Haittaohjelmien analysoijan tehtävänä on haittaohjelmanäytteiden takaisinmallinnus sekä haittaohjelmien perusteellinen tutkinta. Hän osallistuu poikkeamien hallintaan haittaohjelmien osalta. Työnsä tuloksien avulla hän määrittelee uusia IOC:itä. [49, s. 5]

Forensiikka analysoijan tehtävänä on kerätä ja analysoida sähköisiä jälkiä tietojärjestelmissä. Tavoitteena hänellä on löytää tiedon eheyteen tai luottamuksellisuuteen kohdistuneita väärinkäytöksiä. [41; 42] Tehtävä toteutetaan poikkeaman hallinnan osana. Forensiikka tuottaa uusia IOC:itä. [49, s. 5]

Uhkatiedustelijan tehtävänä on toteuttaa uhkatiedustelu sekä sen tuottaman tiedon analysointi. Uhkatietoja kerätään ja analysoidaan mm. avoimista lähteistä sekä muilta turvallisuustoimijoilta. [57, s. 96] Tiedustelun perusteella määritetään uusia IOC:itä. [49, s. 5]

Kybervalvomon järjestelmänvalvoja vastaa valvomon tietoteknisten laitteiden toimivuudesta ja ylläpidosta. Lisäksi hän mahdollisuuksien mukaan automatisoi kybervalvomon toimintoja. Järjestelmänvalvojan tehtävänä on myös valvomon infrastruktuurin ja työkalujen jatkuva dokumentointi. [29, s. 112 - 115; 49, s. 5; 57, s. 98 - 100]

Haavoittuvuusarvioitsijan tehtävänä on arvioida, priorisoida sekä raportoida havaitut haavoittuvuudet. Haavoittuvuusarvioitsijan tehtäviin kuuluu erilaisten tunkeutumis- ja uhkasimulointiharjoituksien järjestäminen, joiden avulla saadaan kuva tietojärjestelmän tämän hetkisestä turvallisuustilanteesta. [49, s. 5; 57, s. 97]

Turvallisuusinsinöörin tehtävänä on kybervalvomon työkalujen käyttöönotto ja integrointi. Hän ylläpitää ja kehittää valvontajärjestelmää. Kybervalvomon koosta riippuen, turvallisuusinsinöörejä voi olla useita, jotka erikoistuvat eri toimintoihin (SIEM, reitittimien turvallisuus jne.). [29, s. 112 - 115; 49, s. 6; 57, s. 98 - 100]

Päällikön tehtävänä on valvoa ja johtaa kybervalvomon toimintaa. Hän laatii valvomon toimintasuunnitelman sekä raportoi esimiehelleen säännöllisesti valvomon toiminnasta. Päällikkö vastaa ja on tietoinen valvomon sen hetkisestä suorituskyvystä. [29, s. 117 - 120; 49, s. 5]

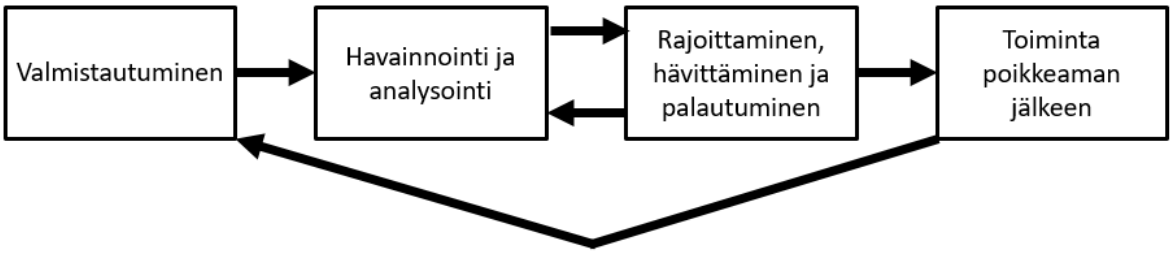
4.3. Tietoturvapoikkeamat ja niiden käsittely

Tietoturvapoikkeamien hallinta kuuluu osaksi reaktiivisia ja proaktiivisia palveluita, ja on näin ollen olennainen osa kybervalvomojen toimintaa. [53, s. 10] Tietoturvapoikkeamalla tarkoitetaan tietoturvatapahtumaa, joka vaikuttaa organisaation toimintaan epäsuotuisasti, vaarantaen tietojen ja palvelujen tietoturvan. [4, s. 6; 26, s. 16]

Tietoturvapoikkeamat voivat vaarantaa organisaation tietojen luottamuksellisuuden, eheyden tai saatavuuden. Tästä syystä on tärkeää, että tietoturvapoikkeamiin vastataan nopeasti ja tehokkaasti heti, kun hyökkäys tapahtuu. Kybervalvomossa, jossa on jatkuva poikkeaman hallinnan kyky, kyetään systemaattisesti vastamaan tietoturvapoikkeamiin. Tämä kyky minimoi vahingot ja palvelukatkokset mahdollisista hyökkäyksistä. Jokainen havaittu tietoturvapoikkeama edesauttaa poikkeaman hallintaryhmän kykyä estää vastaavanlaiset poikkeamat tulevaisuudessa. Tämä toteutetaan konfiguroimalla turvallisuuteen liittyvät työkalut vastaamaan saman tyyppiseen hyökkäykseen tulevaisuudessa. [4, s. 6 - 7; 58, s. 19]

National Institute of Standards and Technology on luonut tietoturvapoikkeaman hallintaan prosessin, joka on jaettu neljään vaiheeseen. Prosessin vaiheet ovat varautuminen, havainnointi ja analysointi, hyökkäyksen rajoittaminen ja palautuminen sekä toiminta poikkeaman jälkeen. [4] s. 21. Huomionarvoista on, että tietoturvapoikkeaman hallinta prosesseja on saatavilla erittäin paljon julkisista lähteistä. Pääpiirteittäin prosessit ovat kuitenkin samankaltaisia [9, s. 233; 29, s. 134 - 137; 58; 59; 60; 61, s. 13].

Tässä tutkielmassa käytetään NIST -organisaation julkaisemaa mallia (kuva 10). Tiedon luotettavuutta on parannettu lisäämällä lähdemerkintöjä samankaltaisista prosesseista.



Kuva 10: Poikkeaman hallinnan vaiheet

4.3.1 Valmistautuminen

Valmistautuminen voidaan jakaa kahteen osaan. Toinen valmistautumisen elementti on poikkeaman hallintakyvyn luominen ja toinen elementti on poikkeamien estäminen. Tietoturvapoikkeamien estämisessä on tarkoituksena varmistua siitä, että laitteet, tietoverkot ja ohjelmat ovat turvattu riittävän hyvin [59, s. 2 - 5; 62, s. 5 - 9]. [4, s. 21]

Mahdollisimman monen tietoturvapoikkeaman estäminen etukäteen on erittäin tärkeää koko organisaatiolle kuin myös poikkeaman hallintaryhmälle. Mikäli poikkeamia ei estetä tehokkaasti, se nopeasti ylikuormittaa poikkeaman hallintaryhmän erilaisilla poikkeamatapauksilla. [4, s. 24; 59, s. 2 - 5]

Valmistautumisessa on tärkeää, että poikkeaman hallintaryhmällä on käytössä riittävät resurssit. Näitä ovat esimerkiksi viestintävälineet, työskentelytilat, poikkeamien analysointiin tarkoitettu kalusto, poikkeamien vaikutusten pienentämiseen tarkoitetut ohjelmat ja muut resurssit. [4, s. 22 - 24; 59, s. 2 - 5; 62, s. 5 - 9]

4.3.2 Havainnointi ja analysointi

Tietoturvapoikkeamien hallintaan kuuluu havainnointi ja analysointivaihe. Valvonnan näkökulmasta kyseinen vaihe on keskeinen. Vaiheen tärkeimpänä tarkoituksena on analysoida, onko havaittu tietoturvatapahtuma todellinen poikkeama vai mahdollisesti jokin turvallisuutta vaarantamaton tapahtuma. [4, s. 26; 58, s. 26; 59, s. 5 - 6; 62, s. 9]

Vaiheen keskeisimpinä elementteinä ovat mahdollisten hyökkäysvektoreiden tiedostaminen sekä tietoturvatapahtumien ja -poikkeamien tunnistaminen, analysointi, dokumentointi ja priorisointi. [4, s. 25 - 34; 59, s. 5 - 6]

Poikkeavat voivat näyttäytyä lukemattomilla eri tavoilla. [59, s. 5 - 6] Tästä syystä on mahdotonta kehittää tarkkoja ohjeita jokaista poikkeamaa varten. Organisaatioiden tulisi valmistautua hoitamaan kaikki mahdolliset poikkeamat jollain tasolla. Organisaation tulisi kuitenkin keskittyä sellaisiin poikkeamiin, jotka käyttävät yleisimpiä hyökkäysvektoreita. Erilaiset poikkeamat vaativat erityyppisiä vastatoimia. [4, s. 26]

4.3.2.1 Tietoturvatapahtumat ja niiden lähteet

Tietoturvatapahtumalla tarkoitetaan merkkiä siitä, että poikkeama saattaa tapahtua tulevaisuudessa, on saattanut tapahtua tai saattaa tällä hetkellä olla tapahtumassa [4, s. 26; 26, s. 16]. Tietoturvatapahtumia ovat esimerkiksi lokien ilmoitukset konfiguraatiomuutoksista, virustorjunnan hälytykset, epäilyttävät tiedostot, epäonnistuneet kirjautumiset tai poikkeava verkkoliikenne [11]. [4, s. 26 - 27] Tietoturvatapahtuma ei kuitenkaan vielä tarkoita sitä, että kyseessä olisi todellinen poikkeama [26].

Mahdollisten poikkeamien havainnointi on haastavaa. Mikäli arvioidaan, että poikkeama on tapahtunut, on arvioitava poikkeaman tyyppi, laajuus ja ongelman suuruusluokka.

Poikkeamia voidaan havaita monilla eri keinoilla, kuten automatisoiduilla havainnointi työkaluilla (verkko- ja laite-IDPS, virustorjunta, manuaalisesti suoraan käyttäjän toimesta jne.). Poikkeamahavaintojen tarkkuus vaihtelevat poikkeamasta ja lähteestä riippuen. [4, s. 26; 58, s. 27 - 28]

Huomionarvoista on myös se, että tietoturvatapahtumia havaitaan normaalisti erittäin paljon. Lisäksi poikkeamiin liittyvän datan tehokkaaseen analysointiin vaaditaan todella syvää teknistä tietämystä aihealueesta. [4, s. 26]

Tietoturvatapahtumia tunnistetaan käyttämällä monia eri lähteitä, kuten tietoturvaohjelmien hälytyksiä, lokeja, uhkatiedustelua ja henkilöstöä. Erilaisia hälytyksiä tuottavia ohjelmia ovat esimerkiksi edeltävässä luvussa käsitellyt tunkeutumisen esto- ja havainnointijärjestelmät sekä SIEM:t. [4, s. 27; 58, s. 27 - 28]

Henkilöt niin organisaation sisältä kuin organisaation ulkopuolelta voivat antaa tapahtumahavaintoja. Organisaation sisältä mm. järjestelmänvalvojat sekä normaalit käyttäjät voivat raportoida tapahtumista. Organisaatiolla on tärkeää olla toimintatapa ulkopuolisten tahojen ilmoittamille tietoturvatapahtumien käsittelylle. Poikkeaman hallintaryhmä päättää muodostuuko tietoturvatapahtumasta tietoturvapoikkeama. [4, s. 28; 58, s. 27 - 28]

4.3.2.2 Poikkeamien analysointi

Tietoturvatapahtumat eivät ole usein kovinkaan tarkkoja. Esimerkiksi tunkeutumisen esto- ja havainnointijärjestelmät tuottavat usein suuren määrän false-positive -hälytyksiä. Poikkeaman havainnoinnin ja analysoinnin tekee vaikeaksi se, että jokainen IDPS:n tuottama hälytys pitäisi tarkastaa. Vääriä hälytyksiä voi tulla tuhansista miljooniin päivässä. Kaikkien näiden väärien hälytysten joukoista pitäisi kyetä löytämään todelliset poikkeamat. Tilannetta hankaloittaa entisestään se, että vaikka tietoturvatapahtuma olisi todellinen, se ei silti tarkoita sitä, että tietoturvapoikkeama olisi tapahtunut [29, s. 134 - 135]. Jotkin tietoturvatapahtumat, kuten palvelinten kaatuminen tai tärkeiden tiedostojen muutokset voivat tapahtua muiden kuin kohdistetun hyökkäyksen takia, esimerkiksi käyttäjän tekemän virheen vuoksi. [4, s. 28]

Joissain tapauksissa ainoa indikaattori tietoturvapoikkeamasta voi olla pieni muutos yhdessä järjestelmän konfiguraatiotiedostossa. Havainnon saaminen tietoturvapoikkeamasta on usein kaikista haastavin tehtävä poikkeaman hallinnassa. Poikkeamien käsittelijät ovat vastuussa tietoturvatapahtumien analysoinnista, jotka usein ovat tulkinnanvaraisia, ristiriitaisia ja puutteellisia. Näiden tietojen pohjalta analysoijien pitäisi muodostaa käsitys siitä mitä on tapahtunut. [4, s. 29]

Vaikka teknisiä ratkaisuja on olemassa jotka tekevät havainnoinnista helpompaa, paras vaihtoehto on muodostaa ammattitaitoinen ryhmä, joka kykenee analysoimaan tietoturvatapahtumia tehokkaasti, ja tekemään tarvittavat toimet poikkeamien hallintaan. Ilman ammattitaitoista henkilökuntaa poikkeamien havainnointi ja analysointi ovat tehottomia. [4, s. 29]

Poikkeaman hallintaryhmän tulisi työskennellä nopeasti analysoidakseen ja vahvistaakseen jokaisen tietoturvatapahtuman. Työskentely tulisi suorittaa ennalta kehitetyn toimintatavan mukaisesti, ja dokumentointi analysoinnin yhteydessä tulisi tehdä kattavasti. Kun poikkeama on tapahtunut, ryhmän tulisi kiireesti toteuttaa esianalysointi, jotta he saavat kuvan siitä mitkä verkot, järjestelmät ja/tai ohjelmat ovat vahingoittuneet, mistä poikkeama on saanut alkunsa sekä kuinka hyökkäys on toteutettu. [4, s. 29; 58, s. 26 - 40; 29, s. 135]

Esianalysoinnin tulisi tuottaa riittävästi informaatiota, jotta ryhmä kykenee priorisoimaan seuraavat toimenpiteensä mahdollisimman tehokkaasti. Toimenpiteitä ovat esimerkiksi poikkeaman eristäminen ja vaikutusten tarkempi analysointi. [4, s. 29; 58, s. 26 - 40; 29, s. 135]

Analysointia edesauttaa järjestelmien profilointi, jonka avulla muodostetaan vertailukohtia, joihin vertaamalla kyetään tunnistamaan muutokset esimerkiksi verkkoliikenteen määrissä tai kriittisissä tiedostoissa. Käytännössä kuitenkin pelkästään profiloinnin avulla poikkeamien havainnointi on erittäin haastavaa. Organisaation tulisi käyttää profilointia yhtenä monista eri toimintatavoista. Järjestelmän normaalin toiminnan tunnistaminen on ensiarvoisen tärkeää poikkeaman hallintaryhmälle, jotta he tunnistaisivat epänormaalin toiminnan analysoinnin yhteydessä [62, s. 11]. [4, s. 29 - 30]

Lokien säilytykseen tulisi luoda selkeä toimintatapa. Poikkeamaan liittyvää tietoa on useissa eri paikoissa, kuten palomuurien, IDPS:n ja ohjelmien lokeissa. Lokien säilyttäminen mahdollistaa tehokkaan poikkeaman analysoinnin, koska lokit voivat paljastaa esimerkiksi hyökkäykseen kuuluvaa tiedustelua. Lokien säilytys on tärkeää, koska on mahdollista, että poikkeama havaitaan jopa useita kuukausia sen jälkeen, kun hyökkäys on aloitettu. [4, s. 29 - 30]

Eri tapahtumien vertailu helpottaa poikkeaman analysointia. Havaintoja poikkeamasta voidaan saada kerättyä useisiin eri tyyppisiin lokeihin. [62, s. 10] Palomuurin lokit voivat esimerkiksi paljastaa hyökkääjän IP-osoitteen, kun taas laitteen lokit voivat sisältää käytetyn käyttäjätunnuksen. Verkkopohjainen IDPS voi havaita, että hyökkäys on toteutettu tiettyä laitetta vastaan, mutta se ei välttämättä tiedä onko hyökkäys onnistunut. Tällöin analysoijan täytyy tutkia laitteen sekä käytettyjen sovelluksien lokeja varmistuakseen hyökkäyksen vaikutuksista [62, s. 10]. [4, s. 29 - 30]

Analysointia helpottaakseen tietojärjestelmän eri laitteet tulisi pitää samassa kellonajassa, jolloin eri kellonaikoja vertaamalla voidaan päätellä hyökkäyksen tarkempi eteneminen [58, s. 31]. Tähän voidaan käyttää esimerkiksi NTP-protokollaa (Network Time Protocol). [62, s. 5] Edellä mainitun vertailun toteuttaminen on erittäin haastavaa, mikäli eri laitteiden kellonajat eroavat toisistaan. [4, s. 29 - 30; 29, s. 14]

Poikkeamien käsittelijöille tulisi luoda tietopankki, joka sisältäisi tietoa jota he mahdollisesti tarvitsisivat poikkeaman hallinnan yhteydessä. Tietopankin tulisi sisältää yleisimpien tietoturvatapahtumien, kuten joidenkin IDPS-hälytysten merkitykset. [4, s. 29 - 30; 62, s. 7]

Hakukoneet voivat helpottaa analysoijien työtä löytää informaatiota epätavallisesti toiminnasta. Huomionarvoista kuitenkin on, että tutkimukseen on hyvä käyttää erilisiä työasemia, jotta minimoidaan organisaatiolle aiheutuvat riskit näiden hakujen toteuttamisesta. [4, s. 29 - 30]

Tietoliikennepakettien analysointi on hyödyllistä. Poikkeamat eivät tarjoa aina riittävästi informaatiota analysoijalle, jotta hän kykenisi ymmärtämään mitä on tapahtumassa. Kerättävien tietoliikennepakettien määrä on suositeltavaa pitää rajattuna, jotta minimoidaan merkityksetön data valvonnan kannalta. Pakettien kerääminen on järkevää toteuttaa ennalta määrätyn kriteeristön mukaisesti. [4, s. 29 - 30]

Datan suodattaminen voi olla järkevää, koska poikkeaman käsittelijöillä ei riitä aika kaikkien hälytysten tutkimiseen. Yksi toimintatapa datan suodattamiseen on sellaisten hälytysten suodattaminen, jotka usein ovat merkityksettömiä. Toinen vaihtoehtoinen tapa on suodattaa kaikki muut paitsi merkittävimmät tapahtumat. On kuitenkin huomioitava, että tässä lähestymistavassa voidaan suodattaa myös todelliset uudentyyppiset hälytykset. [4, s. 29 - 30]

Mikäli poikkeaman hallintaryhmällä ei ole riittävästi osaamista, tulisi sillä olla selkeät yhteyshenkilöt oman organisaation ulkopuolelta, joiden avulla tietoturvapoikkeama saadaan käsiteltyä asianmukaisesti. [4, s. 29 - 30]

4.3.3 Hyökkäyksen rajoittaminen ja hävittäminen sekä palautuminen hyökkäyksestä

Hyökkäyksen rajoittaminen on erittäin tärkeää poikkeamahavainnon alkuvaiheessa. Ilman rajoittamista hyökkäys pääsee leviämään kohteessa, jolloin se syö enemmän resursseja ja sen aiheuttamat vahingot kasvavat. Hyökkäyksen rajoittamisen avulla saadaan aikaa tehdä palautumissuunnitelma. Päätöksenteko on keskeisenä osana rajoittamista. Rajoittamiseen liittyvillä päätöksillä esimerkiksi suljetaan eri järjestelmiä, katkaistaan tietty osa tietoverkosta tai tietyt toiminnallisuudet otetaan pois käytöstä. [58, s. 34 - 36; 59, s. 6 - 7] Päätöksenteko on helpompaa, mikäli organisaatiolla on selkeät toimintatavat valmiina erilaisten tietoturvapoikkeamien rajoittamiseksi. [4, s. 35; 29, s. 135; 62, s. 11 - 12]

On syytä huomioida, ettei hyökkääjän tunnistamiseen poikkeaman hallinnassa lähtökohtaisesti käytetä kovin paljoa resursseja, koska hyökkääjän tunnistaminen on aikaa vievää sekä se ei todennäköisesti edesauta hyökkäyksestä palautumista. [4, s. 37]

Hyökkäyksen rajoittamisen jälkeen, hävitetään hyökkääjän luomat epäedulliset kohteet tietojärjestelmistä. Epäedullisia kohteita voivat olla esimerkiksi hyökkääjän haltuun saamat käyttäjätunnukset tai järjestelmässä olevat haittaohjelmat. Lisäksi rajoittamisen jälkeen pyritään tunnistamaan ja pienentämään kaikki tunnistetut haavoittuvuudet. Kohteiden hävittämisen yhteydessä on erityisen tärkeää, tunnistaa kaikki kohteet joihin on vaikutettu hyökkäyksen aikana, jotta ne voidaan palauttaa turvalliseen tilaan. [4, s. 37; 59, s. 6 - 7; 62, s. 14]

Hyökkäyksestä palautumisessa järjestelmänvalvojat varmistuvat siitä, että järjestelmä toimii normaalisti ja, mikäli mahdollista, haavoittuvuudet paikataan. Palautuminen voi tarkoittaa esimerkiksi varmuuskopioiden käyttöä, saastuneiden tiedostojen korvaamista, päivitysten asentamista, salasanojen vaihtoja, palomuurisääntöjen muokkausta tai pahimmassa tapauksessa koko järjestelmän alustamista. Palautumiseen liittyy myös järjestelmän valvonnan parantaminen hyökkäyksen kohteiden osalta. [4, s. 37; 29, s. 136; 59, s. 6 - 8; 62, s. 14 - 15]

4.3.4 Toiminta poikkeaman jälkeen

Tärkeimpänä toimena poikkeamasta palautumisen jälkeen on oppia poikkeamasta ja parantaa toimintatapoja sekä suojausta tämän osalta. [58, s. 46] Jotta poikkeamasta kyetään oppimaan, on tärkeää, että saastuneista kohteista tallennetaan forensiikkaa varten tarvittavat tiedot [62, s. 12]. [59, s. 7] Erillisen palautetilaisuuden pitäminen on tehokas toimintatapa, joka tulisi pitää muutamia päiviä poikkeamasta palautumisen jälkeen. [4, s. 38]

Palautetilaisuuksista laaditaan pöytäkirja, johon kirjataan tärkeimmät asiat kyseisen poikkeaman osalta. Tämän kaltainen raportointi helpottaa esimerkiksi uusien työntekijöiden kouluttamista. [4, s. 39] Palautetilaisuuksissa tulisi käsitellä seuraavat kokonaisuudet: tietoturvapoikkeaman havaintoaika, ensimmäinen havainto tietoturvapoikkeamasta, poikkeaman laajuus, hyökkäyksen eristäminen ja poistaminen, palautumiseen vaaditut toimenpiteet, vahvuudet sekä kehitettävät asiat. [29, s. 136 - 137; 59, s. 9]

Tapahtuneiden tietoturvapoikkeamien tarkka raportointi mahdollistaa riskien ja uhkien tunnistamisen turvallisuusjärjestelyissä, joiden avulla kyetään parantamaan uhka-arviota. Tarkan raportoinnin avulla kyetään lisäksi tunnistamaan, kuinka hyvin nykyisillä resursseilla poikkeaman hallintaryhmä kykenee toteuttamaan tehtäväänsä. [29, s. 136 - 137; 58, s. 26 - 50; 59, s. 9; 62, s. 15] Mahdollisia mittareita tapahtumien arviointiin ovat esimerkiksi hoidettujen poikkeamien määrä ja poikkeamiin käytetty käsittelyaika. [4, s. 40 - 41]

4.4. Uhkametsästys

Uhkametsästyksellä tarkoittaa hyökkääjien ja haittaohjelmien etsintää ennakoivasti. Tavoitteena uhkametsästyksellä on havaita ja eristää kohdistetut hyökkäykset, jotka ovat väistäneet tai ovat väistämässä olemassa olevat turvallisuusratkaisut. [63, s. 2] Hyökkääjät voivat esimerkiksi hiljalleen varastaa dataa järjestelmästä, seurata luottamuksellista informaatiota tai etsiä käyttäjätunnuksia joiden avulla hyökkääjä pääsee käsiksi erittäin tärkeisiin tietoihin. [64; 65; 66]

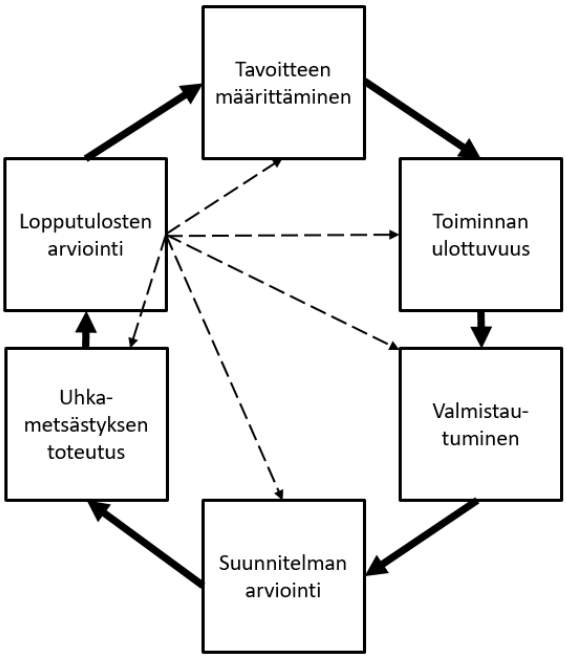
Kybervalvomon tarjoamien palveluiden osalta, uhkametsästys on selvästi ennakoivan toimintansa takia osa proaktiivisia palveluita. Alkuperäinen palvelutaulukko on vuodelta 2002, jolloin on ymmärrettävää, että uhkametsästys ei ole osa sitä. Uhkametsästys vaikuttaisi olevan yleistynyt toimintatavaksi vuoden 2015 jälkeen [63, s. 2; 64; 65; 66].

Uhkametsästyksen suorituskyky on hankittava asteittain organisaatioon. Ensivaiheessa organisaation henkilöstössä pitää olla lajittelun asiantuntija (taso 1) ja poikkeamien käsittelijä (taso 2), jotta uhkametsästys kyetään alusta alkaen toteuttaa mahdollisimman tehokkaasti. On tärkeää, että uhkametsästystä suorittavat henkilöt tuntevat organisaation tietojärjestelmät erittäin hyvin, jotta he kykenevät arvioimaan onko jokin toiminta normaalia vai epänormaalia. [64; 67]

Ennen uhkametsästyksen aloittamista täytyy määritellä tärkeimmät tiedusteluvaatimukset. Vaatimukset määräytyvät organisaation uhka-arvion mukaan. Tärkeimpien tiedusteluvaatimuksien avulla uhkametsästyksen tehokkuus paranee huomattavasti, koska näiden avulla kyetään päättämään mm. mistä mahdollista hyökkääjää etsitään ja mitä hyökkääjä mahdollisesti pyrkii tekemään. Esimerkiksi mikäli uhka-arviona on, että dataa pyritään varastamaan organisaation sisältä, tällöin valvonnan keskiössä on yhtäkkiset muutokset verkkoliikenteen määrissä. [64]

Jotta uhkametsästys olisi mahdollisimman tehokasta, sen toteuttamisessa on käytettävä selkeää toimintatapaa. Uhkametsästys-mallin tarkoituksena on muodostaa toimintatapa, joka soveltuu käytettäväksi eri uhkametsästyksen menetelmien ja työkalujen kanssa. Mallin avulla uhkametsästyksen fokus pysyy paremmin asetetuissa tavoitteissa, eikä resursseja näin ollen kulu niin paljoa toisarvoisiin kohteisiin. Malli tarjoaa henkilöstölle varmistuksen siitä, että uhkametsästys säilyttää analyyttisen eheytensä ja maksimoi eri datalähteiden käytön. [63, s. 2 - 12]

SANS-instituutin tuottama uhkametsästyksen malli pitää sisällään kuusi peräkkäistä vaihetta, jotka ovat tavoitteen määrittäminen, toiminnan ulottuvuus, valmistautuminen, suunnitelman arviointi, uhkametsästyksen toteutus ja lopputulosten arviointi. Malli on esitetty seuraavassa kuvassa. [63] Samansuuntaisia toimintatapoja on havaittavissa myös muista lähteistä [68; 69; 70].



Kuva 11: Uhkametsästys-malli

Tavoitteen määrittämisen yhteydessä organisaation on tunnistettava uhkametsästykseen liittyvät päätavoitteensa. Vaiheen aikana on tärkeää tunnistaa minkä takia uhkametsästystä halutaan ylipäätään suorittaa ja mikä on tavoiteltava loppuasetelma toiminnalle. Tavoiteltavan loppuasetelman tulisi olla linjassa organisaation muiden tavoitteiden kanssa. Lisäksi on tunnistettava missä ympäristössä, millä oletuksilla ja rajoitteilla uhkametsästystä toteutetaan. [63, s. 6 - 7]

Tarve uhkametsästyksen aloittamiselle voi ilmaantua esimerkiksi uhkatiedustelun kautta, jossa on paljastunut uusia hyökkäystapoja organisaation järjestelmiä vastaan tai uhkametsästys aloitetaan tarpeesta tulla tietoisemmaksi ja varmemmaksi omasta ympäristöstä. Tavoitteet antavat yleiset suuntaviivat esimerkiksi painopisteen luonnille eri järjestelmien ja alueiden osalta. Tavoite määrittää lopulta sen, millainen lopputulos uhkametsästyksellä halutaan saavuttaa. Lopputuloksena voi esimerkiksi olla hyökkääjän löytäminen tai haavoittuvuuksien tunnistaminen kohdejärjestelmästä. [63, s. 7]

Tavoitteen määrittämisen jälkeen seuraavana vaiheena on toiminnan ulottuvuuden määrittely. Se voidaan jakaa kahteen alavaiheeseen. Ensimmäisessä alavaiheessa määritetään kohteena oleva järjestelmä ja toisessa alavaiheessa hypoteesit. [63, s. 7]

Ensimmäisenä määritellään järjestelmä sekä palvelut, joita testataan. Sen lisäksi uhkametsästäjät voivat määritellä aliverkon tai -verkot, joita pitää tutkia tunnistettujen palveluiden osalta. Tutkittava alue kapenee entisestään liittämällä mukaan esimerkiksi tietyt laitteet, joilla on tunnistettu olevan merkitystä uhkametsästyksen tavoitteille. Kohteita valittaessa on huomioitava, ettei määriteltyä kohdetta rajata liikaa, jotta tutkittavasta alueesta ei tule liian suppea. Mikäli tutkittavasta alueesta tulee liian pieni, tällöin on todennäköisempää, että hyökkääjän läsnäolo jää huomaamatta kohdeympäristössä. [63, s. 7]

Kun järjestelmä on määritetty, aloitetaan hypoteesin muodostaminen. Hypoteesin avulla uhkametsästäjät tekevät tiettyjä olettamuksia hyökkääjän toiminnasta ja näin ollen pystyvät rajaamaan tutkittavaa järjestelmää pienempiin alueisiin. [63, s. 8; 67]

Valmistautumisvaihe keskittyy analysointi- ja datan keräämissuunnitelman kehittämiseen. Valmistautumissuunnitelma sisältää datan keräämisen lähteet sekä analyysityökalut ja -menetelmät. Suunnitelman täytyy olla linjassa edeltävässä vaiheessa tehtyyn hypoteesiin sekä määritettyyn alueeseen kohdejärjestelmän sisältä. [63, s. 8]

Suunnitelman arvioinnin tarkoituksena on varmistua siitä, että suunnitelma vastaa asetettuja tavoitteita. Uhkametsästyksen toteuttajan voi olla järkevää keskustella toteutettavasta suunnitelmasta oman esimiehensä kanssa varmistaakseen, että suunnitelma tukee tavoitteita. Tässä vaiheessa allokoidaan resurssit, joita tarvitaan suunnitelman toteuttamiseen. Mikäli uhkametsästäjillä ei ole kaikkia tarvittavia resursseja, joita he tarvitsevat suunnitelman toteuttamiseen, tulisi vaiheessa tunnistaa puutteet ja ehdottaa mahdollisia ratkaisuja tunnistettujen puutteiden ratkaisuun. Lisäresurssit voivat tarkoittaa esimerkiksi uusien työkalujen tai ulkopuolisten resurssien hankintaa. Vaiheessa tulisi myös arvioida aikaa jonka uhkametsästys tulee kuluttamaan. Lisäksi tulisi varmistua siitä, että aikaresurssi ja datankeräysresurssit ovat linjassa keskenään, ennen seuraavaan vaiheeseen siirtymistä. [63, s. 9]

Suoritusvaihe aloitetaan, kun uhkametsästyssuunnitelma on hyväksytty. Uhkametsästäjät keräävät tietoja toiminnan ulottuvuuden määrittelyn yhteydessä tehdyistä kohteista. He käyttävät analysointitekniikoita todistaakseen tai kiistääkseen kehitetyn hypoteesin. Analysoijien tulisi kohdistaa työnsä myös muuhun saatavilla olevaan dataan ja käyttää tarvittaessa ylimääräisi analysointitekniikoita joita tarvitaan tavoitteiden saavuttamiseen. [63, s. 9]

Uhkametsästysraportin kirjoittaminen aloitetaan suoritusvaiheen lopussa, kun kaikki analyysit ovat tehty. Valmiin raportin tulisi keskittyä siihen millaiset olivat metsästyksen tulokset sekä siihen saavutettiinko asetetut tavoitteet. Raportin tulisi sisältää ylimääräiset datalähteet, analysointitekniikat ja muut olennaiset tapahtumat ja löydökset uhkametsästyksen aikana. [63, s. 9]

Loppuarviointi on toimintamallin viimeinen vaihe. Sen tarkoituksena on tuottaa analyysi kaikista edeltävistä vaiheista uhkametsästyksen osalta. Analyysin perusteella organisaatio saa palautetta siitä, mikä meni hyvin ja missä on kehitettävää. [63, s. 9 - 10]

4.5. Uhkatiedustelu

Uhkatiedustelun tarkoituksena on tuottaa tarkkaa tietoa mahdollisista tulevista tai jo vaikuttavista kyberhyökkäyksistä. Tämän tiedon avulla hyökkäyksen kohde voi toteuttaa vastatoimia kyseistä hyökkäystä vastaan. Tarkka tieto uhkista hankitaan erilaisten uhkasyötteiden avulla sekä vertamaalla uhkasyötettä oman tietojärjestelmän rakenteeseen. [71, s. 2; 72, s. 91] Uhkatiedustelu vaikuttaa olevan osa proaktiivisia palveluita, vaikka sitä ei sellaisenaan alkuperäisessä palvelutaulukossa esiinny.

Uhkasyötteellä tarkoitetaan mitä tahansa tietoa uhkasta, joka voi auttaa organisaatiota suojautumaan uhkaa vastaan tai havaitsemaan uhkan. Erilaisia uhkasyötteitä ovat IOC:t, hyökkääjien toimintatavat (TTP), turvallisuusilmoitukset, uhkatiedustelun raportit sekä työkalujen konfiguraatio suositukset. [72, s. 92; 73, s. 2 - 3]

IOC:lla tarkoitetaan esimerkiksi haittaohjelmaa tai tapahtumaa, joka viittaa välittömään hyökkäysuhkaan tai siihen, että hyökkäys on jo toteutunut. Se edesauttaa mahdollisten uhkien havaitsemista ja torjuntaa. IOC voi olla esimerkiksi hyökkääjän ohjauspalvelimen IP-osoite, URL joka viittaa haitalliseen sisältöön tai haitallisen sähköpostin otsikkokenttä. [73, s. 2]

Hyökkääjien toimintatavat (TTP) kuvaavat esimerkiksi hyökkääjän taipumusta käyttää tiettyä haittaohjelmaa, suorittaa hyökkäys tietyllä vaiheistuksella tai käyttää hyväksi tiettyä haavoittuvuutta. Lyhenne TTP tulee sanoista taktiikat (Tactics), tekniikat (Techniques) ja menetelmät (Procedures). [72, s. 93; 73, s. 2]

Turvallisuusilmoitukset ovat lyhyitä, teknisiä kuvauksia tämän hetken haavoittuvuuksista ja muista turvallisuuteen liittyvistä asioista. [73, s. 2] Turvallisuusilmoituksia tuottaa Suomessa esimerkiksi Kyberturvallisuuskeskus [74].

Uhkatiedustelun raporteilla tarkoitetaan dokumenttia, joka kuvaa hyökkääjän toimintatavat, kohdejärjestelmät sekä muut uhkatiedot. Raportit parantavat organisaation tilannetietoisuutta. [73, s. 2]

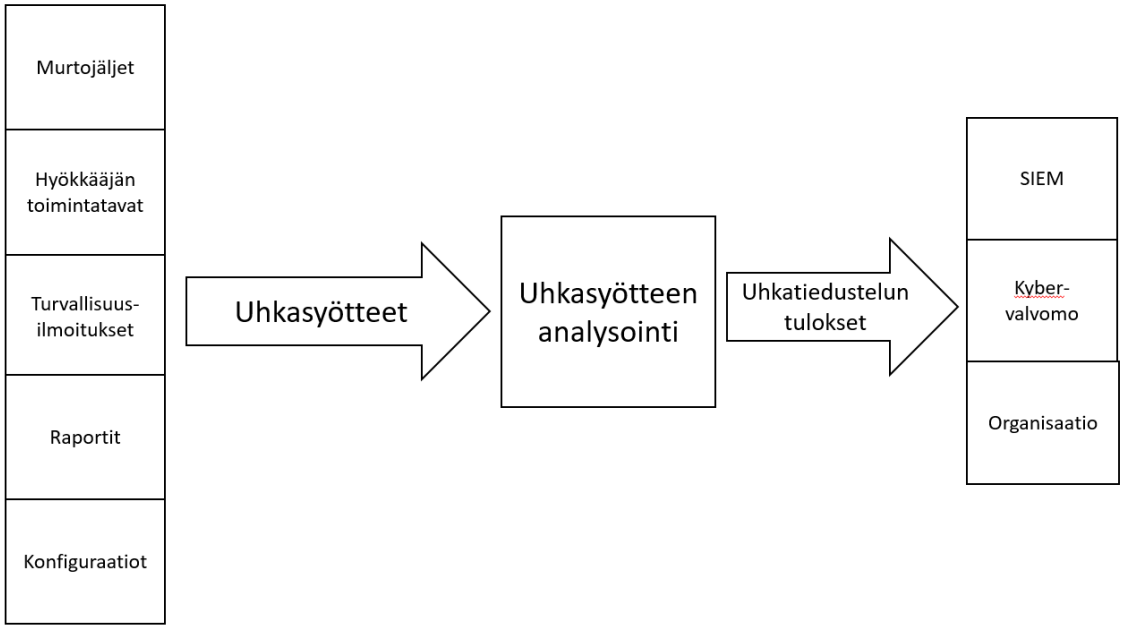
Uhkasyötteet ovat suosituksia siitä, kuinka työkaluja tulisi konfiguroida, jotta mahdolliset uhkat kyetään estämään tai havaitsemaan. Esimerkiksi konfiguraatioihin liittyvät uhkasyötteet voivat sisältää ohjeita, kuinka asentaa ja käyttää piilohallintaohjelmien (rootkit) havaitsemis- ja poistotyökaluja tai kuinka luoda ja muokata palomuurin sääntöjä. [73, s. 2 - 3]

Uhkasyötteistä saatua tietoa täytyy analysoida, jotta siitä saatua tietoa voidaan käyttää tehokkaasti. Analysoidun tiedon perusteella pyritään parantamaan suojattavan järjestelmän valvontakykyä. Käsittelemätön tiedustelutieto ei sellaisenaan tarjoa kybervalvomolle riittävästi tietoa tehokkaaseen valvontaan. Esimerkiksi tieto ainoastaan haitallisesta verkkosivusta ei aiheuta vielä suuria toimenpiteitä valvonnalle. Mutta tehokkaan analysoinnin avulla haitallisesta verkkosivusta saadaan selville esimerkiksi sen käyttämä haittaohjelma. Valvontaa kyetään näin ollen kehittämään, kun tiedetään millainen haittaohjelma leviää kyseisen sivuston kautta. [49, s. 15; 71, s. 2]

Uhkatiedustelun tuottamaa analysoitua tietoa voidaan käyttää monilla eri tasoilla organisaatiossa. Sen avulla kyetään ohjeistamaan esimerkiksi organisaation henkilöitä, jotka eivät työskentele kyberturvallisuuden parissa päivittäin. Tiedustelun tuottama tieto voisi jalostua toimintaohjeiksi ja säännöiksi verkkoympäristöissä. Lisäksi tiedustelun tuottama tieto hyödyttää organisaation ylempää johtoa, kun he saavat tarkempaa kybertilannekuvaa. [71, s. 2 - 3; 75]

Ymmärrys hyökkäystekniikoista sekä niiden mahdollisista indikaatioista on mahdollista saavuttaa yhdistelemällä sisäisiä uhkasyötteitä, ulkoisista lähteistä kerättyjen syötteiden kanssa. Tämä mahdollistaa tehokkaiden puolustusoperaatioiden toteuttamisen kehittyneitä hyökkäyksiä vastaan. [49, s. 15]

Uhkatiedustelulla tarkoitetaan uhkasyötteistä kerättyä, analysoitua ja täydennettyä tietoa, joka on liitetty osaksi teknisiä työkaluja, kybervalvomon ja tarvittaessa muun organisaation toimintaa. [71, s. 2 - 3] Uhkatiedustelun vaikutuksien muodostuminen kybervalvomossa on esitelty seuraavassa kuvassa [49, s. 15; 71; 73].



Kuva 12: Uhkatiedustelun vaikutuksien muodostuminen kybervalvomossa

4.6. Haasteet sekä yhteenveto kybervalvomoista

SANS-instituutti on teettänyt kyselyn eri organisaatioilla, joilla on toiminnassa tietoturvavalvomo. Organisaatioiden suurimmat haasteet liittyivät esimerkiksi henkilöstöön, automaatioon, työkalujen integraatioon, hälytyksien määrään, tilannekuvaan sekä vastustajan tuntemiseen. [49, s. 1; 56]

Haasteet henkilöstön osalta johtuivat ammattitaitoisen henkilöstön pienestä määrästä [56, s. 19]. Tietoturvavalvomoissa vaaditaan osaamista esimerkiksi haittaohjelmien analysoinnista, digitaalisesta forensiikasta ja poikkeaman hallinnasta. Henkilöstön tulisi osata niin tulkita SIEM-järjestelmän keräämää dataa sekä tunnistaa ja määritellä tärkeä informaatio yleisestä datavirrasta. Heidän tulisi myös kyetä muokkaamaan korrelaatiosääntöjä ja vahvistaa saatua dataa lisäämällä se oikeaan kontekstiin. Ilman ammattitaitoista henkilöstöä tämä ei onnistu. [49, s. 2]

Tietoturvavalvomon toiminnassa automaatio on erittäin tärkeässä osassa. Heikko automaatio yhdistettynä edellä mainittuun ammattitaitoisen henkilöstön vähäiseen määrään muodostaa olemassa olevalle henkilöstölle suuren työtaakan. Henkilöstön käyttäminen työtehtäviin joita olisi mahdollista automatisoida, heikentää huomattavasti valvomon tehokkuutta. [49, s. 2; 56, s. 2]

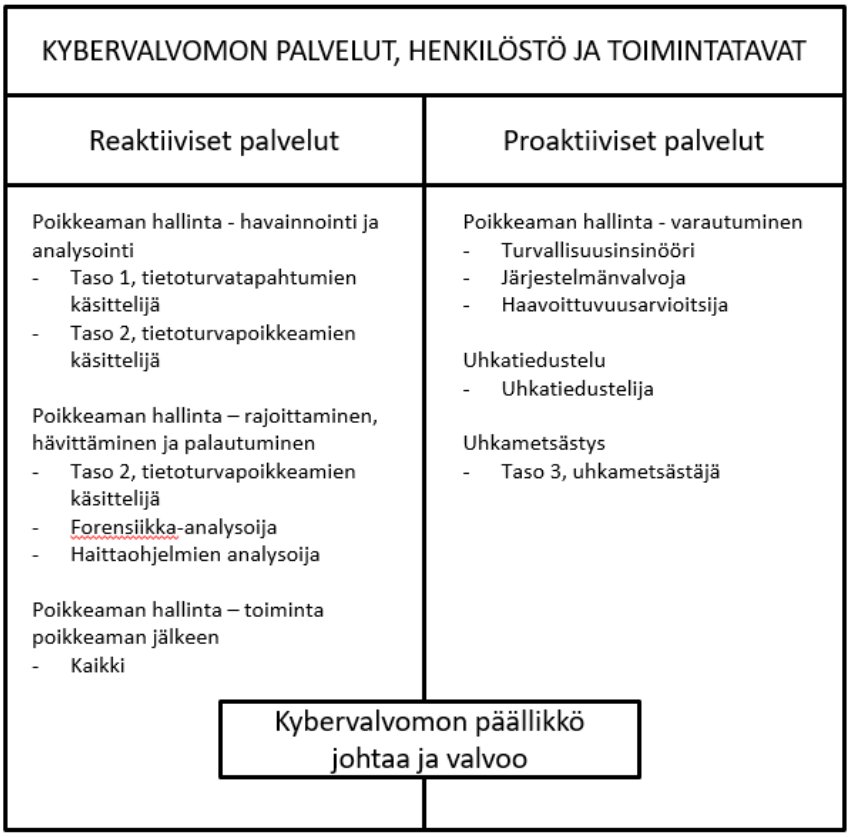
Työkalujen välinen integraatio täytyy olla kunnossa. Tällä tarkoitetaan sitä, ettei valvomon henkilöstön tarvitsisi käyttää useita eri työkaluja työtehtävissään ilman että työkalut keskustelevat keskenään tehokkaasti. Henkilöstön tekemien virheiden mahdollisuus lisääntyy, mikäli heidän tarvitsee vaihtaa työkaluista toiseen tietoja manuaalisesti. Uusien työkalujen käyttöönotossa täytyy ottaa huomioon niiden integrointi vanhoihin ratkaisuihin. [49, s. 2; 56, s. 19]

Tietoturvavalvomon toiminnassa ongelmana ovat myös suuret määrät hälytyksiä, joita tuottavat eri tietoturvatyökalut. SANS-instituutin teettämän kyselyn mukaan hälytyksien määrä on usein niin suuri, että noin puolet hälytyksistä jää kokonaan käsittelemättä. [49, s. 2; 56, s. 19]

Suuresta datamäärästä johtuen tietoturvavalvomot voivat joutua kaventamaan valvottavien laitteiden ja tietoverkkojen määrää. Tästä kuitenkin aiheutuu se, ettei heillä ole tällöin tarkkaa tilannekuvaa koko järjestelmästä. Verkon pääpisteitä, kuten reitittimiä ei usein valvota, koska ne esimerkiksi tuottavat erittäin suuren määrän false-positive -hälytyksiä. Kuitenkin nämä päätepisteet ovat pääkohteita hyökkääjälle ja näin ollen niiden valvominen olisi ensisijaisen tärkeää. [49, s. 2]

Henkilöstön tehokas toiminta on haastavaa, jos valvomon henkilöstö ei kykene tunnistamaan vastustajan tavoitteita, taktiikoita, tekniikoita ja toimintatapoja. Tämä johtuu siitä syystä, että henkilöstö ei kykene priorisoimaan eikä näin ollen luo painopistettä. Tästä yleensä seuraa se, että henkilöstöllä on liian suuri määrä hälytyksiä käsiteltävänä, joka johtaa ylikuormittumiseen ja sitä kautta suorituskyvyn laskuun. Uhkatiedustelun avulla henkilöstö kykenee tunnistamaan paremmin vastustajan tavoitteet, taktiikat ja hyökkäystekniikat. [49, s. 2]

Yhteenvetona voidaan todeta, että valvonnan kannalta keskeisimpiä palveluita ovat reaktiiviset ja proaktiiviset palvelut. Näihin palveluihin liittyy keskeisesti poikkeaman hallinta sekä uhkatiedustelu ja uhkametsästys. Esitelty henkilöstö jakaantuu eri palveluiden alle tasaisesti. Valvonnan kannalta keskeisimmät palvelut, toimintatavat ja henkilöstö on koottu seuraavaan kuvaan.



Kuva 13: Kybervalvomon toiminta valvonnan osalta

5. HYÖKKÄYSVAIHEIDEN VALVONTA

Luvussa tarkastellaan MITRE:n ATT&CK-taulukon avulla, mitä eri asioita tietojärjestelmistä pitäisi valvoa, jotta kyberhyökkäys voitaisiin havaita. ATT&CK-taulukossa on yhteensä 319 erilaista hyökkäystekniikkaa.

Kaikki hyökkäystekniikat ja -vaiheet, joita ATTACK -taulukossa käsitellään perustuvat oikeisiin tapahtumiin. Taulukko on tutkimuksen liitteessä 3. Sivuston esittelemät hyökkäysvaiheet (tactics) kuvaavat hyökkääjän välitavoitteita, jonka hän pyrkii saavuttamaan tietyllä tekniikalla. Jokainen välitavoite on saavutettavissa useilla eri tavoilla, riippuen kohteesta ja sen suojauksesta. Tekniikat kuvaavat tapaa kuinka hyökkääjä saavuttaa välitavoitteensa. [10; 11]

Tutkimuksessa ei käsitellä sitä, kuinka hyökkääjä mahdollisesti pääsisi sisään kohdejärjestelmäänsä. Tästä syystä ATT&CK-taulukon ensimmäistä vaihetta (initial access) ei käsitellä.

ATT&CK-taulukon hyökkäystekniikoiden valvonta on jaettu erilaisiin datalähteisiin [11]. Tässä tutkimuksessa datalähteet ovat jaettu eri alakategorioihin, jotka ovat edelleen jaettu koskemaan tietoverkko- ja laitekerrosta. Käytetyt alakategoriat ovat ulkoverkko, sisäverkko, käyttöjärjestelmä, prosessit, tiedostot, forensiikka, lokit ja työkalut. Eri datalähteiden liittyminen eri alakategorioihin on esitetty tutkielman liitteessä (liite 4). Seuraavassa kuvassa on esitetty tutkimuksessa käytetyt eri alakategoriat sekä niiden linkittyminen tietoverkko- ja laitekerroksiin.

<table>
<tr><th>TIETOVERKKOKERROS</th><th>LAITEKERROS</th></tr>
<tr><td>- ULKOVERKKO
- SISÄVERKKO</td><td>- KÄYTTÖJÄRJESTELMÄ
- PROSESSIT
- TIEDOSTOT
- FORENSIIKKA</td></tr>
<tr><td colspan="2">MOLEMPIIN KERROKSIIN LIITTYVÄT ALAKATEGORIAT</td></tr>
<tr><td colspan="2">- LOKIT
- TYÖKALUT</td></tr>
</table>

Kuva 14: Alakategorioiden jako tietoverkko- ja laitekerrokseen

Luvussa on esitelty ATT&CK-taulukon mukaiset vaiheet ja niiden valvontaan liittyvät keskeiset huomiot. Suluissa olevat numerot tarkoittavat, kuinka monessa eri vaiheen tekniikassa kyseinen valvontatapa esiintyi. Viimeisessä alaluvussa kootaan yhteen ATT&CK-taulukosta saadut keskeisimmät tulokset.

On huomioitava, että yksittäinen hyökkäystekniikka saattaa aiheuttaa valvontaa niin laite- kuin tietoverkkokerroksessa. Tästä esimerkkinä mainittakoon hyökkäystekniikka *Obfuscated Files or Information*, jonka valvonta olisi tehokasta, mikäli valvontaa toteutettaisiin jokaisen alakategorian kautta (prosessit, käyttöjärjestelmä, tiedostot, lokit, forensiikka, työkalut, sisäverkko, ulkoverkko).

5.1. Suoritus (execution)

Suorittaminen tarkoittaa sitä, kun hyökkääjän haittaohjelma ajetaan kohdejärjestelmässä. Vaiheeseen kuuluvia hyökkäystekniikoita ovat mm. Powershell:n, komentosarjojen ja komentokehotteen hyväksikäyttö. Tässä hyökkäysvaiheessa on 34 eri hyökkäystekniikkaa ja kaikki niistä liittyivät suoraan syvän puolustuksen mallin mukaiseen laitekerrokseen. Vain kuusi hyökkäystekniikkaa vaikuttavat myös tietoverkkokerrokseen. [11] Vaiheen valvonta näin ollen painottuu laitekerroksen valvontaan.

Tämän vaiheen valvonnassa näyttäisi painottuvan erilaisten prosessien valvonta (33). Muita lukumäärällisesti isoimpia valvottavia kohteita ovat tiedostot (16) ja käyttöjärjestelmä (12). Tietoverkkokerroksen osalta valvottavat kokonaisuudet ovat kaikki sisäverkossa.

Vaikuttaa täysin loogiselta, että suoritusvaiheessa valvonta painottuu erilaisten prosessien valvontaan. Hyökkääjän suorittaessa haitallisen ohjelmansa, tällöin myös tietokoneessa käynnistyy jonkinlainen prosessi. Mutta huomionarvoista kuitenkin on se, että vaikka kyseessä onkin hyökkääjän haittaohjelman ajaminen kohdejärjestelmässä, valvonta ei silti rajoitu ainoastaan prosessien valvontaan.

5.2. Pysyvyyden varmistaminen (persistence)

Vaihe koostuu tekniikoista joiden avulla hyökkääjä säilyttää pääsyn järjestelmään. Pääsy järjestelmään säilyy, vaikka se uudelleen käynnistettäisiin, kirjautumistietoja muutettaisiin tai jostain muusta syystä jonka takia pääsy järjestelmään katkeaisi. Tekniikoiden avulla pyritään muokkaamaan kohdejärjestelmän konfiguraatioita siten, että pääsy järjestelmään säilyy. [11]

Hyökkäystekniikoita pysyvyyden varmistamiseen ovat esimerkiksi käyttäjätunnuksien, piilotettujen kansioiden ja tiedostojen hyväksikäyttö. Erilaisia hyökkäystekniikoita on vaiheeseen listattu 62. Niistä lähes kaikki (61) liittyvät suoraan laitekerroksen valvontaan, kun taas tietoverkkokerroksen valvontaan liittyy ainoastaan seitsemän hyökkäystekniikkaa. [11] Pysyvyyden varmistamisen valvonta keskittyy siis laitekerrokseen.

Erilaiset valvonnan kohteet jakaantuvat tässä vaiheessa tasaisemmin eri kohteisiin kuin edeltävässä suoritusvaiheessa. Valvonnan kohteet painottuvat kuitenkin samoihin asioihin kuin edeltävässä vaiheessa. Pysyvyyden varmistamisen valvonnassa prosessien (47), tiedostojen (37) ja käyttöjärjestelmän (33) valvonta painottuvat. Tietoverkkokerroksen valvonta painottuu sisäverkon valvontaan. [11]

Suurin osa tämän vaiheen tekniikoista on havaittavissa laitekerroksessa. Tämä on ymmärrettävää, koska pysyvyys halutaan saavuttaa nimenomaan erilaisissa laitteissa kohdejärjestelmässä.

5.3. Käyttöoikeuksien laajentaminen (privilege escalation)

Vaihe koostuu tekniikoista joiden avulla hyökkääjä saavuttaa korkeamman käyttöoikeuden tietojärjestelmään. Hyökkääjä voi usein päästä sisälle järjestelmään ja tutkia verkkoa ilman pääsyoikeutta. Saavuttaakseen lopullisen tavoitteensa hyökkääjä tarvitsee korkeammat pääsyoikeudet. Käyttöoikeuksia laajennetaan tavallisimmin hyödyntämällä järjestelmän heikkouksia, konfiguroinnissa tehtyjä virheitä ja haavoittuvuuksia. Laajennettu käyttöoikeus voi olla esimerkiksi järjestelmänvalvojan tunnukset tai peruskäyttäjän tunnukset, jossa on järjestelmänvalvojan kaltaiset oikeudet. Tähän vaiheeseen kuuluvat tekniikat menevät osittain päällekkäin pysyvyyden varmistamiseen liittyvän vaiheen kanssa. [11]

Käyttöoikeuksien laajentamiseen käytetään mm. Windowsin käyttäjähallinnan (UAC, User Account Control) ohittamista sekä ajastettuja tehtäviä (scheduled tasks). [11] Vaiheeseen kuuluvia hyökkäystekniikoita on yhteensä 32, jotka kaikki liittyvät laitekerrokseen. Ainoastaan yksi hyökkäystekniikka liittyy suoraan tietoverkkokerrokseen.

Käyttöoikeuksien laajentamisen valvonnassa painottuvat samat kohteet kuin aiemmissa hyökkäysvaiheissa. Vaihetta valvotaan prosessien (28), tiedostojen (19) ja käyttöjärjestelmän (18) kautta. [11]

Todennäköisesti vaiheen valvonta muistuttaa erittäin paljon edeltäviä vaiheita, koska kaikkien näiden hyökkäysvaiheiden erottaminen toisistaan on haastavaa. Hyökkääjä todennäköisesti toteuttaa kaikki nämä vaiheet samanaikaisesti, jolloin niiden valvontakin on samankaltaista. Pieniä eroja vaiheiden valvontojen välillä löytyy, mutta isossa mittakaavassa samat valvontakohteet säilyvät.

5.4. Suojauksen kiertäminen (defense evasion)

Vaihe sisältää tekniikat joiden avulla hyökkääjä pyrkii välttämään sen, että hänet havaittaisiin hyökkäyksen aikana. Tekniikat pitävät sisällään turvallisuusohjelmien lamauttamisen. Lisäksi ne pitävät sisällään datan ja komentosarjojen hämäämisen tai salaamisen. Hyökkääjä saattaa käyttää myös luotettuja prosesseja hyväkseen piilottaakseen haittaohjelman. [11]

MITRE on listannut suojauksen kiertämiseen yhteensä 69 erilaista hyökkäystekniikkaa. Kuten aiemmissakin vaiheissa, myös suojauksen kiertäminen painottuu laitekerrokselle (67). Kuitenkin verkkokerrokseen painottuvia tekniikoita on 14, jolloin niitä on suhteessa eniten kaikkiin edeltäviin vaiheisiin nähden. [11]

Suojauksen kiertämisen yhteydessä valvottavia kokonaisuuksia laitekerroksella ovat prosessit (54), tiedostot (34) ja käyttöjärjestelmä (24). Verkkokerroksen valvonta painottuu sisäverkkoon (13), kuitenkaan ulkoverkon (5) valvontaa ei voi täysin sivuuttaa. [11]

5.5. Käyttäjätunnusten ja salasanojen hankinta (credential access)

Vaihe koostuu tekniikoista, joiden avulla hyökkääjä pyrkii varastamaan käyttäjätunnuksia ja salasanoja. Hyökkääjä voi pyrkiä tähän esimerkiksi käyttäjätietokantojen kopioinnilla, käyttäjätunnusten kopioimisella suoraan tiedostoista tai näppäintallentimilla. Hyökkääjän havainnointi on todella haastavaa, mikäli hän käyttää oikeita tunnuksia. Oikeat tunnukset mahdollistavat sen, että hyökkääjä voi luoda lisää oikeilta näyttäviä käyttäjätunnuksia järjestelmään, joka voi helpottaa hyökkääjää saavuttamaan tavoitteensa. [11]

Käyttäjätunnusten ja salasanojen hankintaan liittyviä tekniikoita on listattuna yhteensä 21 kappaletta. Vaihe painottuu laitekerroksen valvontaan. Vaiheen eri valvontakohteet jakaantuvat tasaisesti. Kuitenkin tärkeimmät valvottavat kohteet ovat erilaiset prosessit (14) ja käyttöjärjestelmän toiminteet (12). Vaiheessa korostuvat myös eri sovelluksista kerättävät lokit (11). Neljän hyökkäystekniikan osalta tietoverkon valvonta on tärkeässä osassa. Jokaisessa näistä tekniikoista valvonta koskee sisäverkkoa. [11]

Huomionarvoista on, että ainoastaan kolmessa eri hyökkäystekniikassa oli valvottavaksi kohteeksi merkitty käyttäjätunnuksien käytöstä kerätyt lokit. Hyökkääjällä on tarkoituksena todennäköisesti saada käyttöönsä legitiimit käyttäjätunnukset, jolloin niihin liittyvissä lokeissa ei havaita normaalista poikkeavaa toimintaa. Poikkeuksena mahdollisesti tilanteet joissa hyökkääjä tekee käyttäjätunnuksilla jotain normaalin käyttäjän toiminnasta poikkeavaa.

5.6. Ympäristön tutkinta (discovery)

Vaihe pitää sisällään tekniikat joiden avulla hyökkääjä saa tietoa kohdejärjestelmästä. Tekniikat helpottavat hyökkääjää orientoitumaan ympäristöön ennen päätöstä siitä, kuinka hän aikoo toimia järjestelmässä. Tämä mahdollistaa myös sen, että hyökkääjä voi tutkia mitä kaikkea hän voi kontrolloida ja mitä kaikkea ympäristössä on, joista hän voi hyötyä. Usein tietojen keräämiseen käytetään käyttöjärjestelmän omia järjestelmätyökaluja. [11]

Hyökkäysvaiheen tekniikoita ovat esimerkiksi tietoverkon konfiguraation, tietoverkon yhteyksien, järjestelmätietojen sekä eri ohjelmien tutkinta. [11] Vaiheeseen kuuluu yhteensä 23 erilaista hyökkäystekniikkaa, joista kaikki liittyvät jollain tavalla laitekerrokseen. Tietoverkkokerroksen valvontaan liittyy neljä eri tekniikkaa.

Vaiheen tärkeimmät valvottavat kohteet ovat järjestelmän eri prosessit (23). Tietojen keräämiseen käytetään jonkinlaisia työkaluja, jolloin myös prosessien painottuminen on ymmärrettävää. Ympäristön tutkintaan liittyen on tärkeää valvoa myös käyttöjärjestelmää (8), lokeja (6) ja tiedostoja (5). Nämä ovat kuitenkin selkeästi pienemmässä osassa. Tietoverkkokerroksen valvonta jakaantuu tasaisesti sisä- (4) ja ulkoverkkoon (3).

5.7. Liikkuminen ympäristössä (lateral movement)

Vaihe sisältää tekniikat joita hyökkääjä käyttää levittäytyäkseen kohdejärjestelmässä. Jotta hyökkääjä voi saavuttaa tavoitteensa, vaatii se usein verkon tutkimista, jotta hyökkääjä löytää ja saa pääsyn kohteeseensa. Hyökkääjän tavoitteiden saavuttaminen vaatii usein, että hyökkääjä pääsee useiden eri järjestelmien läpi sekä sen, että hyökkääjä saa käyttöönsä useita eri käyttäjätunnuksia. Hyökkääjä saattaa asentaa kohteeseen oman etäkäytön mahdollistavan työkalun, joka mahdollistaa liikkumisen kohdejärjestelmässä. Hyökkääjä voi myös käyttää hankittuja käyttäjätunnuksia ja salasanoja sekä käyttöjärjestelmän alkuperäisiä työkaluja, jotta hän pysyisi paremmin salassa. [11]

Ympäristössä liikkumiseen kuuluvia hyökkäystekniikoita on yhteensä 18. [11] Tietoverkkokerroksen valvontakeinoja käytetään seitsemässä eri tekniikassa ja laitekerroksen valvontaa käytetään jokaisessa hyökkäystekniikassa.

Kuten aiemmissakin vaiheissa, myös ympäristössä liikkumisen valvontaan pääkeinona on prosessien (13) valvonta. Vaiheen valvonnassa korostuvat lisäksi tiedostojen (10) valvonta sekä lokien (10) kerääminen eri kohteista. Käyttäjätunnuksiin liittyvät lokit painottuvat selvästi. [11] Tämä vaikuttaa järkevältä, koska liikkuminen tietojärjestelmässä vaatii todennäköisesti useita eri käyttäjätunnuksia, jolloin tämä on myös nähtävissä käyttäjätunnuksia käsittelevissä lokeissa.

5.8. Datan kerääminen (collection)

Vaihe koostuu tekniikoista joiden avulla hyökkääjä voi kerätä tietoa järjestelmästä. Lähteistä kerätään sellaisia tietoja, joista on hyötyä hyökkääjän tavoitteiden saavuttamiselle. Usein datan keräämisen jälkeen, hyökkääjän seuraava tavoite on datan varastaminen. Tavallisimmat kohteet sisältävät erilaisia asemia, selaimia, ääntä, videota ja sähköposteja. Tavallisin keräystapa pitää sisällään kuvankaappaukset ja näppäimistön syötteet. Lisäksi hyökkääjä voi esimerkiksi kerätä tietoja leikepöydältä. [11]

Vaiheeseen on listattu 13 erilaista hyökkäystekniikka. Datan keräämisen valvonta toteutetaan laitekerroksessa jokaisessa listatussa tekniikassa. Tietoverkkokerrokseen liittyviä tekniikoita on yhteensä neljä. Tekniikat, joiden avulla dataa ohjataan uuteen paikkaan (esim. man in the browser -tekniikka) aiheuttaa sen, ettei tietoverkkokerroksen valvontaa voi täysin unohtaa datan keräämisvaiheessa.

Laitetason valvottavat kohteet liittyvät tässä vaiheessa prosessien (11) ja tiedostojen (9) valvontaan. Tietoverkkokerroksen valvonta keskittyy täysin sisäverkkoon. [11]

5.9. Järjestelmän hallinta (command and control)

Vaiheen tarkoituksena on, että hyökkääjä kykenee kontrolloimaan kohdejärjestelmää. Tämän avulla hyökkääjä voi kommunikoida järjestelmän kanssa joka on ollut hänen kohteenaan. Hyökkääjä pyrkii usein matkimaan normaalia liikennettä, jotta hän ei paljastuisi. Hyökkääjällä on monia mahdollisuuksia järjestelmän hallintaan, riippuen kohdeverkon rakenteesta ja sen puolustuksesta. [11]

Mahdollisia tapoja järjestelmän ottamiseksi hallintaan ovat esimerkiksi porttien, useiden yhteysprotokollien sekä välityspalvelimien hyväksikäyttö. Järjestelmän hallintaan ja ohjaamiseen on MITRE:n ATT&CK-taulukossa 22 erilaista hyökkäystekniikkaa. [11] Kyseisessä hyökkäysvaiheessa hyökkäykset kohdistuvat niin tietoverkko- (22) kuin laitekerrokseen (16).

Vaiheen valvonnassa näyttäisi painottuvan erityisesti tietoverkon valvontaan liittyvät toimenpiteet, kuten pakettien kaappaaminen, prosessien valvonta tietoverkon käytön osalta sekä tietoverkon liikennemäärien valvonta. Pääpaino tietoverkkokerroksen valvonnassa on sisäverkossa (22). [11]

Tietoverkon valvonnan painottuminen tässä vaiheessa on erittäin luonnollista, johtuen siitä, että hyökkääjän täytyy aiheuttaa jonkinasteista verkkoliikennettä, jotta hän kykenee ohjaamaan kohdejärjestelmäänsä halutulla tavalla. On kuitenkin huomionarvoista, että tämän vaiheen toteuttaminen saattaa olla hyökkääjälle erityisen haastavaa perusyhtymän johtamisjärjestelmässä, koska ohjausliikenteen ulottaminen mahdollisesti muusta internetistä irralliseen verkkoon voi olla erittäin haastavaa.

Laitekerroksen valvonta painottuu täysin prosessien (14) valvontaan. Käyttöjärjestelmän (1) ja tiedostojen valvonnalla (2) ei tämän vaiheen hyökkäystekniikoita juurikaan havaita.

5.10. Datan varastaminen (exfiltration)

Vaiheen avulla hyökkääjä varastaa dataa kohdeverkosta. Hyökkääjä pyrkii sulauttamaan varastetusta datasta aiheutuvan tiedonsiirtonsa legitiimiin liikenteeseen. Tekniikat voivat sisältää tiedon pakkaamista sekä salaamista. Jotta hyökkääjä kykenee siirtämään dataa pois kohdejärjestelmästä, vaatii tämä usein edeltävän vaiheen mukaista järjestelmän hallintaa. [11]

MITRE on esitellyt yhdeksän erilaista hyökkäystekniikkaa koskien datan varastamista. Koska kyse on datasta, niin se koskettaa jokaisessa tekniikassa laitekerrosta jollain tasalla. Noin puolessa tekniikoista oli havaittavissa myös tietoverkkokerroksen mukaiseen valvontaan liittyviä toimenpiteitä.

Vaiheen valvonnassa erilaisten prosessien valvonta (8) on tärkeässä osassa. Tiedostojen valvonta (4) on myös tärkeä osa tämän vaiheen valvontaa. Käyttöjärjestelmän valvontaa ei tarvita tämän vaiheen hyökkäystekniikoita vastaan. Tietoverkon valvonta painottuu sisäverkon (5) valvontaan.

Todennäköisesti verkkoliikenteen valvonta on suhteellisen pienessä osassa tässä vaiheessa sen takia, että hyökkääjä pyrkii piilottamaan verkkoliikenteen normaalin liikenteen sekaan. Tämä ei kuitenkaan tarkoita sitä, etteikö verkkoa täytyisi myös tämän vaiheen osalta valvoa.

5.11. Vaikuttaminen (impact)

Vaihe pitää sisällään hyökkäystekniikoita joiden avulla häiritään järjestelmän käytettävyyttä ja vahingoitetaan tietojen eheyttä. Tekniikat voivat pitää sisällään tietojen muuttamista tai tuhoamista. Joissain tapauksissa tiedot voivat näyttää oikealta, mutta todellisuudessa niitä on muokattu siten, että ne hyödyttävät hyökkääjää saavuttamaan tavoitteensa. Näitä tekniikoita voidaan käyttää hyökkääjän lopullisen tavoitteen saavuttamiseen tai näillä tekniikoilla voidaan suojata luottamuksellisuuteen kohdistuneita iskuja. [11]

Vaikuttamisessa käytetään hyökkäystekniikoina mm. käyttäjätunnusten poistamista järjestelmästä, laiteohjelmiston korruptointia ja datan tuhoamista tai muokkaamista. Vaikuttamiseen on luetteloitu 16 erilaista hyökkäystekniikkaa. Suurin osa (13) on havaittavissa laitekerroksen valvonnalla. Tietoverkon valvontaan liittyy viisi erilaista hyökkäystekniikkaa, joissa kaikissa sisäverkon valvonnalla on merkitystä. Lisäksi ulkoverkon (4) valvontaan on kiinnitettävä huomiota. Tämän vaiheen laitekerroksen valvonta suoritetaan prosessien (9), tiedostojen (4) sekä käyttöjärjestelmän valvonnalla (4). [11]

5.12. Yhteenveto

Suurin osa MITRE:n ATT&CK-taulukon hyökkäystekniikoiden mukaisista valvottavasti kohteista liittyivät syvän puolustuksen mukaiseen laitekerrokseen. Erilaisten prosessien valvonta oli keskiössä lähes kaikissa hyökkäysvaiheissa (pl. järjestelmän hallinta).

Järjestelmän hallintaan liittyvässä hyökkäysvaiheessa valvonnan keskiössä on tietoverkkokerros. Huomioitava on, että kaikista hyökkäystekniikoiden valvonnasta vain noin 4% liittyi ainoastaan tietoverkkokerroksen valvontaan. Sisäverkon valvonta painottuu jokaisessa hyökkäysvaiheessa tietoverkkokerroksen osalta. Ulkoverkon valvonnan merkitys on pienempi.

On kuitenkin syystä muistaa, ettei yksittäisen prosessin valvonnalla voida päätellä, että onko kyseessä järjestelmään kohdistuva hyökkäys. Epäilyttävän prosessin käynnistyminen täytyy ajatella enemmänkin johtolankana, jota seuraamalla voidaan päätellä, onko kyseessä todellinen poikkeama vai jokin muu turvallisuutta vaarantamaton tapahtuma. Tämä käy ilmi taulukon hyökkäystekniikoiden valvonnan osalta. Erittäin harvassa hyökkäystekniikassa oli ainoastaan yksi datalähde, jonka kautta hyökkäys voidaan havaita. Tällaisia hyökkäystekniikoita oli yhteensä 23 ATT&CK-taulukon kaikista 319 hyökkäystekniikasta.

Seuraavaan taulukkoon on koottu yhteen luvussa käsitelty keskeinen sisältö. Viimeisessä sarakkeessa oleva prosenttiosuus kertoo, kuinka suuri osuus hyökkäystekniikoista koskee kyseistä valvottavaa kategoriaa. Hyökkäysvaiheiden sulkeissa oleva teksti kertoo, kuinka monta hyökkäystekniikkaa vaiheeseen kuuluu.

Taulukko 1: Yhteenveto hyökkäystekniikoiden valvonnasta eri hyökkäysvaiheissa

Valvottavakohde	Suoritus (yht. 34)	Pysyvyyden varmistaminen (yht. 62)	Käyttöoikeuksien laajentaminen (yht. 32)	Suojauksen kiertäminen (yht. 69)	Käyttäjätunnusten ja salasanojen hankinta (yht. 21)	Ympäristön tutkinta (yht. 23)
Laitetaso	34	61	32	67	21	23
Käyttöjärjestelmä	12	33	18	24	12	8
Prosessit	**33**	**47**	**28**	**54**	**14**	**23**
Tiedostot	16	37	19	34	6	5
Forensiikka	0	2	0	5	0	0
Tietoverkkotaso	6	7	1	14	4	4
Sisäverkko	6	7	1	13	4	4
Ulkoverkko	0	1	0	5	1	3
Molemmat tasot						
Lokit	9	14	11	22	11	6
Työkalut	2	1	1	6	0	0

Valvottavakohde	Liikkuminen ympäristössä (yht. 18)	Datan kerääminen (yht. 13)	Järjestelmän hallinta (yht.22)	Datan varastaminen (yht. 9)	Vaikuttaminen (yht. 16)	Yhteensä (319)	Kuinka suureen osuuteen liittyy taulukon tekniikoista
Laitetaso	18	13	16	9	13	307	96,24 %
Käyttöjärjestelmä	5	6	1	0	6	125	39,18 %
Prosessit	**13**	**11**	14	**8**	**9**	254	79,62 %
Tiedostot	10	9	2	4	4	146	45,77 %
Forensiikka	0	0	7	0	1	15	4,70 %
Tietoverkkotaso	7	4	22	5	5	79	24,76 %
Sisäverkko	7	4	**22**	5	5	78	24,45 %
Ulkoverkko	2	0	10	1	4	27	8,46 %
Molemmat tasot						0	
Lokit	10	3	2	0	8	96	30,09 %
Työkalut	2	2	3	1	2	20	6,27 %

Valvonnan työkalujen osalta painottuvat selkeästi laitepohjaiset tunkeutumisen esto- ja havainnointijärjestelmät. Verkkopohjaiset järjestelmät ovat tärkeitä, mutta niiden osuus kaikista valvottavista kohteista on selkeästi pienempi kuin laitepohjaisilla ratkaisuilla.

6. JOHTOPÄÄTÖKSET

Perusyhtymän johtamisjärjestelmää tulisi valvoa kybervalvomon toimesta. Sen henkilöstöllä tulisi olla selkeät roolit ja valvomon toiminnan tulisi noudattaa etukäteen sovittuja toimintatapoja tehokkaan valvonnan takaamiseksi. Kuitenkin näin laajan kokonaisuuden liittäminen osaksi perusyhtymää ei ole täysin ongelmatonta. Kybervalvomon liittäminen osaksi perusyhtymän organisaatiota asettaa vaatimuksia esimerkiksi perusyhtymän kalustolle, infrastruktuurille, johtamiselle ja huollolle.

Kybervalvomoissa yleisimmin käytössä olevia työkaluja ovat virustorjunnat, palomuurit, tunkeutumisen esto- ja havainnointijärjestelmät sekä keskitetty lokienkeruujärjestelmä (SIEM). Muitakin työkaluja tutkimuksen mukaan on olemassa, kuten erilaiset datan häviämisen estojärjestelmät ja käyttäjähallintasovellukset (UAC).

Valvonnan näkökulmasta vaikuttaa siltä, että tärkeimmät työkalut ovat tunkeutumisen esto- ja havainnointijärjestelmät sekä keskitetty lokienkeruujärjestelmä. Palomuurit, virustorjunnat ynnä muut ovat myös tärkeä osa kyberturvallisuutta, mutta varsinaiseen valvontaan liittyen niillä on toimintaa tukeva rooli.

Valvonta toteutetaan käytännössä asettamalla IDPS- ja SIEM-sovelluksiin erilaisia hälytyssääntöjä, joiden avulla valvontaa suorittavat henkilöt havaitsevat tietoturvatapahtumia ja mahdollisia poikkeamia. SIEM-järjestelmän automatisointi on tärkeää perusyhtymän johtamisjärjestelmässä, johtuen kybervalvontaan osallistuvan henkilöstön vähäisestä määrästä.

Lokien keräys on keskeisessä osassa. Lokien keräämisessä täytyy tasapainotella määrän ja laadun suhteen. Mikäli kerätään vähän lokeja, voidaan todennäköisemmin varmistua siitä, että hälytykset eivät ole vääriä. Mikäli taas kerätään liikaa lokeja, väärien hälytysten määrä kasvaa nopeasti niin suureksi, ettei niiden käsittelyyn ole saatavilla tarpeeksi resursseja.

Yhdysvaltojen Puolustusministeriön tietoverkko-operaatioiden tarkoituksena on estää mahdolliset kyberuhkat. Tämä tarkoittaa poikkeaman hallinnan osalta varautumista. Ohjesääntöjen mukaan tietoverkko-operaatiot ulottuvat taktiselle tasolle asti. Tietoverkko-operaatioiden toteuttaminen ei välttämättä tarkoita kybervalvontaa, koska tietoverkko-operaatioiden toimenpiteet voivat liittyä esimerkiksi tietojärjestelmien päivitysten asentamiseen.

Puolustukselliset kyberoperaatiot pitävät sisällään poikkeaman hallintaan liittyvät vaiheet (pl. varautuminen), uhkametsästyksen sekä todennäköisesti myös uhkatiedustelun. Ohjesäännöistä on pääteltävissä, että puolustuksellisia kyberoperaatioita toteuttavat alueelliset kyberkeskukset, jolloin poikkeaman hallinta on täysin sen varassa, onko prikaatin komentaja pyytänyt tukea toiminnalleen. Todennäköistä on myös se, että vaikka prikaatin komentaja pyytäisikin tukea alueelliselta kyberkeskukselta hän ei sitä välttämättä saa, mikäli muut prikaatit ovat pyytäneet tukea.

Kyberhyökkäys voidaan jakaa useisiin eri vaiheisiin (kuten MITRE:n ATT&CK-taulukossa). Hyökkäyksen täydellinen piilottaminen ilman useiden eri nollapäivähaavoittuvuuksien käyttöä on todennäköisesti erittäin haastavaa. Esimerkiksi järjestelmän hallinta ja ohjaaminen aiheuttavat aina verkkoliikennettä sisäverkossa. Tällä tavalla hyökkäys paljastaa itsensä mahdollisesti myös kybervalvonnalle.

Valvontaan liittyen on ensiarvoisen tärkeää, että kybervalvomon henkilöstö tuntee valvottavan tietojärjestelmän erittäin hyvin. Mikäli esimerkiksi FTP-palvelua ei normaalisti ympäristössä käytetä, sen käyttö on merkki tietoturvatapahtumasta. Jotta kybervalvonta olisi tehokasta, sitä ei voi ulkoistaa kokonaan esimerkiksi alueelliselle kyberkeskukselle, koska se ei todennäköisesti täydellisesti tunne valvottavaa ympäristöä. Mikäli valvontaa suoritetaan alueellisen kyberkeskuksen toimesta, on tietojärjestelmissä oltava selkeät toimintaohjeet siitä, mitä palveluita prikaatin taisteluosaston johtamisjärjestelmässä saa käyttää.

MITRE:n ATT&CK-taulukosta käy kiistatta ilmi, että valvonnan painopiste on erilaisissa laitteissa, kuten esimerkiksi päätteissä tai palvelimissa. Verkkokerroksen valvontaa tarvitaan, mutta sitä tarvitaan selkeästi vähemmän kuin laitteiden valvontaa.

Asevoimien johtamisjärjestelmiä on valvottu perinteisesti erilaisilla valvontaryhmillä, joiden tehtävänä on ollut esimerkiksi linkkijänteiden valvonta vihollisen elektronista vaikuttamista vastaan. Kybertoimintaympäristö laajentaa valvontaa entisestään. Enää ei riitä, että valvotaan verkkoja vaan ajatusmaailma on käännettävä kokonaisvaltaisempaan suuntaan, jossa laitteiden valvonnalla on suuri merkitys.

Poikkeavuuksiin perustuva valvominen on tehokkaampaa kehittyneitä hyökkäyksiä vastaan kuin tunnisteisiin perustuva valvominen. Tämä johtuu siitä, että kehittyneissä hyökkäyksissä ei todennäköisesti käytetä tunnistettuja hyökkäystapoja hyökkäyksien toteuttamiseen vaan esimerkiksi nollapäivähaavoittuvuuksia. En pidä kuitenkaan todennäköisenä, että perusyhtymän johtamisjärjestelmä olisi panos ja tuotos -suhteeltaan järkevä kohde käyttää useita erilaisia nollapäivähaavoittuvuuksia.

Prikaatin johtamisjärjestelmän kaltaisissa ympäristöissä poikkeavuuksien etsiminen on erittäin haastavaa, koska sen johtamisjärjestelmä on suunniteltu erittäin dynaamiseksi. Tämän takia verkkoyhteydet ja tietoliikennemäärät ovat jatkuvassa muutoksessa taisteluvaiheen mukaisesti. Tästä syystä erilaisiin tunnisteisiin perustuvat valvontamenetelmät ovat yksinkertaisempia toteuttaa prikaatin johtamisjärjestelmässä.

SANS-instituutin teettämän kyselyn mukaan eri organisaatiot joissa on kybervalvomo, suurimpana haasteena oli löytää riittävän ammattitaitoista henkilöstöä valvomotoimintaan [56]. Tämä todennäköisesti heijastuu myös prikaatin taisteluosastojen kybervalvontakykyyn.

Yhdysvaltojen armeijan ohjesääntöjen mukaan prikaatin taisteluosastoon ei ole tullut lisähenkilöstöä tukemaan kybervalvontaa. Olen kuitenkin kybervalvontaan liittyen osoittanut, että kyseessä on laajakokonaisuus, johon täytyy olla osoitettuna riittävät henkilöstöresurssit. Prikaatin taisteluosastossa ei näiden lähteiden valossa ole tehokasta kybervalvontaa. Ohjesäännöissä kuitenkin mainittiin siitä, että prikaatin komentaja voi pyytää tukea alueelliselta kyberkeskukselta. Oman arvioni mukaan prikaatin taisteluosaston kybervalvonta on täysin alueellisten kybervalvomojen varassa, jolloin ilman niitä prikaatin johtamisjärjestelmää ei kyetä tehokkaasti valvomaan kyberuhkia vastaan.

Toisaalta yksinkertaisen kybervalvomon toteuttamiseen tarvitaan tämän tutkielman mukaisesti IDPS-järjestelmä, keskitetty lokienkeräysjärjestelmä ja ammattitaitoinen valvontaa suorittava henkilö. Parhaimmillaan tämän koko luokan toiminta ei tarvitse lisähenkilöstöä, vaan prikaatin taisteluosaston sisältä löydetään riittävän ammattitaitoinen henkilö toteuttamaan kybervalvontaa. On kuitenkin syytä muistaa, että tehokas kybervalvonta on kokoaikaista ja siihen liittyy useita eri henkilöitä. Ei voida puhua tehokkaasta kybervalvonnasta, mikäli yksi henkilö ainoastaan toteuttaa kybervalvontaa. Pahimmillaan tämä tapahtuu omien muiden tehtävien ohella.

Tehokas kybervalvonta muodostuu ammattitaitoisen henkilöstön ympärille. Ammattitaitoisesta henkilöstöstä on kuitenkin puutetta, ei ainoastaan asevoimissa vaan myös siviilimarkkinoilla. Lisäksi täydellisen kybervalvomohenkilöstön ja eri toiminteiden ylläpitäminen on erittäin kallista. Tästä johtuen ei ole mielestäni realistista ajatella perusyhtymätasolle täyttä kybervalvomoa, kaikkine henkilöstöineen ja toiminteineen. Mielestäni realistisempi vaihtoehto voisi olla esimerkiksi kahden hengen kybervalvomo, jossa tunnistettaisiin ainoastaan tietoturvatapahtumia. Tietoturvapoikkeamien käsittely, uhkametsästys ja uhkatiedustelu toteutettaisiin esimerkiksi alueellisen kyberkeskuksen toimesta. Tämän kaltainen tehtäväjako aiheuttaisi kuitenkin tiettyjä ongelmia esimerkiksi silloin, kun prikaatin johtamisjärjestelmä ei ole yhteydessä alueelliseen kyberkeskukseen. Tällöin koko poikkeaman hallinnan prosessi suoritettaisiin prikaatin tasolla, johon ei välttämättä annetut resurssit riittäisi.

Joka tapauksessa pienimuotoinenkin valvonta tukisi mielestäni erittäin paljon kybervalvontaa kokonaisuutena, koska toiminta lisäisi asevoimien ymmärrystä siitä mitä tietojärjestelmissä tapahtuu taktiselta tasolta alkaen. Näinkin kevyellä valvonnalla lisäksi annettaisiin viesti mahdolliselle vastustajalle, että perusyhtymätasokaan ei ole täysin sokea. Tämä itsessään jo pienentäisi kyberuhkan toteutumisen mahdollisuutta.

6.1. Tutkimuksen luotettavuus

Subjektiivisuus on suurena riskinä käytettäessä kirjallisuuskatsausta päätutkimusmenetelmänä. Tämä johtuu siitä, että kirjoittaja on valinnut käytettävän aineiston, ja tämän aineiston perusteella kirjoittaja on muodostanut tutkimuksen johtopäätökset. Subjektiivisuutta on pyritty pienentämään käyttämällä tutkimuksessa laajasti eri lähteitä. Päälähteinä keskeisissä aihealueissa on käytetty SANS:n ja NIST:n tuottamia raportteja, ja joita on varmennettu eri oppikirjoilla sekä tietoturvayhtiöiden kirjoituksilla.

Tutkimuksessa käytettiin kirjallisuuskatsauksen lisäksi MITRE:n ATT&CK-taulukkoa erilaisten hyökkäystekniikoiden ja niiden valvonnan tutkimiseen. Taulukon avulla tutkimuksessa on pyritty vähentämään subjektiivisten näkemysten mahdollisuutta, joita kirjallisuuskatsauksessa on voinut syntyä. Kirjallisuuskatsauksessa luotu malli teknisistä työkaluista vastasi hyvin MITRE:n taulukon muodostamiin kyberuhkiin. Eri hyökkäystekniikoiden alakategorioita vastaan löydettiin kirjallisuuskatsauksesta valvontatyökalu.

On tärkeää huomioida, ettei MITRE:n ATT&CK-taulukko ole ainoa kyberhyökkäyksiä kuvaileva malli, mutta verrattuna esimerkiksi Lockheed Martinin Cyber Kill Chainiin, ATT&CK-taulukko syventyy paljon tarkemmin hyökkäyksen teknisiin yksityiskohtiin, ja näin ollen se soveltuu paremmin valvonnan tutkimiseen.

Kyberturvallisuudessa ei ole käytössä yhdenmukaista käsitteistöä. Kyberturvallisuuteen liittyviä samoja termejä käytetään eri lähteissä hieman eri merkityksissä. Tai kahta eri sanaa käytetään siten, että ne tarkoittavat samaa asiaa. Tämän takia tutkimuksessa käytetyt käsitteet ovat pääsääntöisesti Kyberturvallisuussanaston mukaisia.

Tutkimuksen lähdeaineistona on käytetty erittäin paljon englanninkielisiä lähteitä. Tutkimuksessa on pyritty suomentamaan englanninkieliset termit Kyberturvallisuussanaston mukaisiksi käsitteiksi. Kirjoittajan tekemät termien tulkinnat ja niistä tehdyt suomennokset heikentävät tutkimuksen luotettavuutta. Jotkin tutkimuksessa käytetyistä käsitteiden tulkinnoista ovat voineet vääristää alkuperäisen lähteen käsitteiden merkityksiä. Esimerkiksi NIST:n *signs of an incident* -termi on suomennettu tietoturvatapahtumaksi tai tietoturvapoikkeamaksi, riippuen asiayhteydestä.

Kirjoittajalla ei ole juurikaan käytännön kokemusta kybervalvomojen eri teknisten työkalujen käytöstä. Tämä on saattanut aiheuttaa tulkinta virheitä kirjallisuuskatsauksen yhteydessä, joka heikentää tutkimuksen luotettavuutta. Toisaalta käytännön kokemuksen puute voi edesauttaa kirjallisuuskatsauksessa objektiivisen näkemyksen säilyttämistä.

6.2.Jatkotutkimus

Tutkimuksessa annettiin yleiskuvaus kybervalvonnasta ja siihen liittyvistä toimenpiteistä. Tutkimuksessa ei käsitelty pintaa syvemmältä esimerkiksi tunkeutumisen esto- ja havainnointijärjestelmien tai keskitettyjen lokien hallintajärjestelmien käyttöä, vaan pysyttiin perusominaisuuksien kuvailussa. Jatkotutkimus aiheena voisi olla esimerkiksi yksinkertaisen kybervalvomon tutkiminen. Tutkimuksessa voisi tarkastella millainen kybervalvonnan suorituskyky on mahdollista toteuttaa yhdellä operaattorilla taisteluosastossa.

Toisena jatkotutkimusaiheena voisi olla esimerkiksi toimintatapojen kehittäminen perusyhtymän ja alueellisen kyberkeskuksen toiminnan välille. Mahdollisia tutkimuskysymyksiä voisivat olla: mitkä eri poikkeaman hallinnan vaiheet kuuluvat perusyhtymälle, missä vaiheessa perusyhtymä siirtää tietoturvapoikkeaman alueelliselle kyberkeskukselle, miten uhkatiedustelun ja uhkametsästyksen tulokset siirtyvät osaksi perusyhtymän kybervalvontaa?

Tässä tutkimuksessa ei otettu kantaa miten kyberhyökkäys mahdollisesti pääsisi sisään järjestelmään. Jatkotutkimus voitaisiin esimerkiksi tehdä tilaturvallisuuteen liittyen, jossa tutkittaisiin taisteluosaston eri tilaratkaisuja sekä mahdollisia heikkoja kohtia, joista hyökkääjä voisi päästä fyysisesti kiinni järjestelmään. Tämän kaltainen tutkimus todennäköisesti vaikuttaisi myös osiltaan kybervalvonnan rakenteeseen.

KÄSITTEET

False-positive -hälytys: Väärähälytys, joka tapahtuu, kun hälytyksen tekemä työkalu on konfiguroitu tuottamaan hälytyksiä tietyn haitallisen tapahtumaketjun mukaan. Konfiguroitu tapahtumaketju toteutuu kuitenkin legitiimin toiminnan yhteydessä, josta seuraa false-positive -hälytys. [29, s. 18]

Hyökkäystekniikka: termillä viitataan MITRE:n ATT&CK-taulukossa esiintyviin hyökkäystekniikoihin. Tekniikat kuvaavat tapaa kuinka hyökkääjä saavuttaa sen hetkisen tavoitteensa. [10; 11]

IOC: Lyhenne tulee sanoista *indicator of compromise*. Sillä tarkoitetaan merkkiä mahdollisesta tunkeutumisesta tietojärjestelmään. [76]

Kyberhyökkäys: ”Termi viittaa tietoverkkohyökkäystä laajempaan käsitteeseen, sillä kyberhyökkäys voidaan tehdä myös muilla tavoin kuin tietoverkon kautta” [26, s. 30]

Kyberoperaatiot: Kyberoperaatiot toteutetaan kybertoimintaympäristössä. Niiden tarkoituksena on käyttää kybertoimintaympäristöä operaation tavoitteiden saavuttamiseksi. Yhdysvaltojen näkemyksen mukaan kyberoperaatiot jaetaan karkeasti hyökkäys-, puolustus- sekä Puolustusministeriön tietoverkko-operaatioiksi. [25, s. 36]

Kyberpuolustus: ”kyberturvallisuuden maanpuolustuksellinen osa-alue, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä.” [26, s. 22]

Kybertoimintaympäristö: ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö” [26, s. 21]

Kyberturvallisuus: ”Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan” [26, s. 22]

Kyberuhka: ”mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon.” [26, s. 25]

Kybervalvomo: Kybervalvomolla tarkoitetaan jatkuvaan kyberuhkien valvontaan, analyysiin, pienentämiseen ja estämiseen keskitettyä osastoa. [3, s. 2; 49, s. 1; 51]

Perusyhtymän viestijärjestelmä koostuu viestiasemista ja -laitteista, komentopaikoista, viestijoukoista, viestiverkoista, prosesseista sekä erilaisista varamenetelmistä. [7, s. 11]

Suorituskyky: ”Kyky suorittaa tietty toiminta tai saavuttaa tietty vaikutus.” [77]

Tietojärjestelmä: ”Tiedoista ja tietoja käsittelevistä ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoja käsittelevistä ohjelmista ja tietojen käsittelysäännöistä koostuva järjestelmä, jonka tarkoitus on tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Tietojärjestelmän käsite on laaja, eivätkä kaikki sen osa-alueet ole relevantteja kaikissa käyttöyhteyksissä.” [78]

Tietoturvallisuus: ”Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.” [26, s. 15]

Tietoturvapoikkeama: ”yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti.” [26, s. 16]

- ”**Saatavuus** tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. **Eheys** tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja **luottamuksellisuus** sitä, ettei kukaan sivullinen saa tietoa.” [26, s. 15]

Tietoturvatapahtuma: ”tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan” [26, s. 16]

Tietoverkko: ”tietokoneiden ja niiden välisten tiedonsiirtoyhteyksien muodostama kokonaisuus” [79]

Tietoverkkohyökkäys: ”Tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön” [26, s. 30]

Verkostokeskeinen sodankäynti: ”Toimintakonsepti, jonka avulla sensoreita, johtoportaita ja joukkoja johdetaan reaaliaikaisesti. Se perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, modulaarisiin suorituskykyisiin joukkoihin, kansainväliseen yhteensopivuuteen sekä kehittyneeseen johtamisjärjestelmään.” [16, s. 14]

LÄHTEET

[1] Cyril Onwubiko. Cyber Security Operations Centre, Security Monitoring for protecting Business and supporting Cyber Defense Strategy. IEEE: Intelligence & Security Assurance, E-Security Group. 2015. 10 sivua.

[2] Martti Lehto. Kybermaailma ja turvallisuus ITKST41-5. 19.-20.9.2018. Jyväskylän yliopisto. Luentomateriaali. 60 sivua.

[3] Robin Ruefle, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, Samuel J. Perl. Computer Security Incident Response Team Development and Evolution. Carnegie Mellon University. Syys-/Lokakuu 2014. 11 sivua.

[4] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. Computer Security Incident Handling Guide.NIST, Elokuu 2012. 79 sivua. <Näitä voi olla vaikka kuinka pirusti>.

[5] Headquarters, Department of the Army. FM 3-12 Cyberspace and Electronice Warfare Operations. 2017. 108 sivua.

[6] Headquarters, Department of the Army. FM 6-02 Signal Support to Operations. 2014. 68 sivua.

[7] Maavoimien esikunta. Taisteluosaston johtamisjärjestelmä M18 toimintatapaohje STIV. Tammikuu 2017. 71 sivua.

[8] Todd McGuiness. Defense in Depth. SANS Institute. 2001. 11 sivua.

[9] John R. Vacca. Computer and Information Security Handbook. Elsevier. 2009. 877 Sivua. ISBN: 978-0-12-374354-1.

[10] Blake Strom. ATT&CK 101. MITRE. [Viitattu 8.8.2019]. Saatavissa: https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

[11] MITRE. ATT&CK Matrix for Enterprise. [Viitattu 8.8.2019]. Saatavissa: https://attack.mitre.org/.

[12] Wikipedia. National Institute of Standards and Technology. Päivitetty 27.1.2020. [Viitattu 30.1.2020] Saatavissa: https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology.

[13] Wikipedia. SANS Institute. Päivitetty 8.8.2019. [Viitattu 30.1.2020] Saatavissa: https://en.wikipedia.org/wiki/SANS_Institute.

[14] Wikipedia. Mitre Corporation. Päivitetty 11.3.2020 [Viitattu 19.3.2020] Saatavissa: https://en.wikipedia.org/wiki/Mitre_Corporation.

[15] Headquarters, Department of the army. FM 3-96 Brigade Combat Team. 2015. 260 sivua.

[16] Karsikas Jarkko. Maavoimien verkostokeskeisen tiedonsiirtojärjestelmän arkkitehtuuri ja sen toteuttaminen. Yleisesikuntaupseerikurssin tutkielma. Helsinki. MPKK. Heinäkuu 2007. Sotatekniikan laitos. 153 sivua.

[17] Wikipedia. Brigade Combat Team. [Viitattu 24.1.2019] Saatavissa: https://en.wikipedia.org/wiki/Brigade_combat_team.

[18] Headquarters, Department of the Army. FM 6-02.43 Signal Soldiers Guide. 2009. 258 sivua.

[19] Global Security. Warfighter Information Network - Tactical. [Viitattu 29.8.2019]. Saatavissa: https://www.globalsecurity.org/military/systems/ground/win-t.htm.

[20] George J. Allen. MAGTF Communications. Julkaistu 5.5.2009. Saatavissa: https://www.aviation.marines.mil/Portals/11/Documents/DCA_Industry_Day_C4%20(1).ppt.

[21] General Dynamics. Warfighter Information Network -Tactical, Commander's Handbook. 2016. 85 sivua.

[22] Jane's. Warfighter Information Network-Tactical (WIN-T). Päivitetty 18.11.2020. [Viitattu 25.11.2019] Saatavissa: https://janes-ihs-com.mp-envoy.csc.fi/Janes/Display/jmc_4823-jc4il.

[23] Jane's. AN/VRC-118(V)1 Mid-Tier Networking Vehicular Radio (MNVR). Päivitetty 12.4.2018. [Viitattu 25.11.2019] Saatavissa: https://janes-ihs-com.mp-envoy.csc.fi/Janes/Display/jc4il0769-jc4il.

[24] Jane's. Falcon IV family of multi-channel radios (AN/PRC-158/163). Päivitetty 5.11.2019. [Viitattu 25.11.2019] Saatavissa: https://janes-ihs-com.mp-envoy.csc.fi/Janes/Display/jc4il0694-jc4il.

[25] Chairman of the Joint Chiefs of Staff (CJCS). Joint Publication 3-12, Cyberspace Operations. 2018. 104 sivua.

[26] Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry, 2018. 42 s. ISBN 978-952-5608-49-6.

[27] Ministry of Defence; Development, Concepts and Doctrine Centre. Cyber Primer. 2016. 100 sivua.

[28] Chairman of the Joint Chiefs of Staff (CJCS). Joint Publication 6-0, Joint Communication System. 2015. 120 sivua.

[29] David Nathans. Designing and Building Security Operations Center. 1. painos. Elsevier. 257 sivua. ISBN 978-0-12-800899-7.

[30] ScienceDirect. Defense in Depth. [Viitattu 18.2.2020] Saatavissa: https://www.sciencedirect.com/topics/computer-science/defense-in-depth.

[31] Intesar G Ali. Security: Defense in Depth.[Viitattu 20.2.2020] Saatavissa: https://www.slideserve.com/shel/security-defense-in-depth.

[32] MOXA. Three Aspects to Consider When Securing Industrial Automation Control System Networks. [Viitattu 28.2.2020] Saatavissa: https://www.moxa.com/en/articles/three-aspects-for-securing-industrial-automation.

[33] Damian Igbe. What is Defense in depth? Cloud Technology Experts. Julkaistu 12.6.2017 [Viitattu 28.2.2020] Saatavissa: https://www.cloudtechnologyexperts.com/defense-in-breadth-or-defense-in-depth/.

[34] Office of Cybersecurity and Communications. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Department of Homeland Security. Syyskuu 2016. 58 sivua.

[35] Wikipedia. Network Access Control. Päivitetty 30.10.2019. [Viitattu 18.2.2020] Saatavissa: https://en.wikipedia.org/wiki/Network_Access_Control.

[36] Comparitech. 8 Best SIEM Tools: A Guide to Security Information and Event Management. Tim Keary. Päivitetty 27.11.2019. [Viitattu 6.1.2020] Saatavissa: https://www.comparitech.com/net-admin/siem-tools/.

[37] Karen Scarfone, Peter Mell. Guide to Intrusion Detection and Prevention Systems IDPS. NIST 800-94. 2007. 127 sivua.

[38] Michael E. Whitman, Herbert J. Mattord. Principles of Information Security 4th edition. 2012. 658 sivua. ISBN-13: 978-1-111-13821-9.

[39] Techterms. Process.[Viitattu 3.3.2020] Saatavissa: https://techterms.com/definition/process.

[40] Wikipedia. Process (computing). Päivitetty 19.1.2020. [Viitattu 6.3.2020] Saatavissa: https://en.wikipedia.org/wiki/Process_(computing).

[41] Ahlberg Data. IT-forensiikka - forensiikkatutkimukset. [Viitattu 29.1.2020] Saatavissa: https://ahlbergdata.fi/it-forensiikka/.

[42] Ibas. IT-forensiikka eli sähköisen aineiston tutkinta. [Viitattu 29.1.2020] Saatavissa: https://www.ibas.com/fi/it-forensiikka/.

[43] Wikipedia. Computer forensics. Päivitetty: 5.3.2020 [Viitattu 11.3.2020] Saatavissa: https://en.wikipedia.org/wiki/Computer_forensics.

[44] Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot. The Operational Role of Security Information and Event Management Systems. Hewlett-Packard Laboratories. Syys-/Lokakuu 2014. 7 sivua.

[45] Insta. SIEM-järjestelmä on organisaation kyberturvallisuuden hermokeskus. Yrjö Kinnunen. Julkaistu 22.8.2017 [Viitattu 6.1.2020] Saatavissa: https://www.insta.fi/ajankohtaista/siem-j%C3%A4rjestelm%C3%A4-on-organisaation-kyberturvallisuuden-hermokeskus.

[46] Traficom. Vieraskynä: SIEM lokitiedon hyödyntämisessä. Petri Vesamäki. Julkaistu 15.3.2016 [Viitattu 6.1.2020] Saatavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn20160315 1527.html.

[47] Karen Kent, Murugiah Souppaya. Guide to Computer Security Log Management. NIST 800-92. 2006. 72 sivua.

[48] Wikipedia. Security information and event management. Päivitetty 9.1.2020 [Viitattu 11.1.2020] Saatavissa: https://en.wikipedia.org/wiki/Security_information_and_event_management.

[49] Kaspesky. Kaspersky for Security Operations Center. 2018/2019. 33 sivua.

[50] Traficom. Näin keräät ja käytät lokitietoja. Julkaistu/päivitetty 3.12.2019 [Viitattu 8.1.2020] Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja.

[51] Cybersec. A Beginners guide to the Cyber Security Operations Center. [Viitattu 11.9.2019] Saatavissa: https://www.secjuice.com/cybersecurity-operations-center-csoc/.

[52] Wikipedia. Computer emergency response team. Päivitetty: 11.12.2019 [Viitattu 22.1.2020] Saatavissa: https://en.wikipedia.org/wiki/Computer_emergency_response_team.

[53] Carnegie Mellon University, Software Engineering Institute. CSIRT SERVICES. 2017. 12 sivua.

[54] ENISA, European Union Agency for Cybersecurity. CSIRT Services. [Viitattu 17.3.2020] Saatavissa: https://www.enisa.europa.eu/topics/csirt-cert-services.

[55] Pierre Jacobs, Sebastiaan von Solms, Marthie Grobler. E-CMIRC: Towards a Model for the Integration of Services Between SOCs and CSIRTs. Researchgate. Heinäkuu 2016. 12 sivua.

[56] Chris Crowley. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. SANS Institute. 2019. 26 sivua.

[57] Carson Zimmerman. Ten Strategies of a World-Class, Cybersecurity Operations Center. MITRE. 2014. 346 sivua. ISBN: 978-0-692-24310-7.

[58] Chairman of the Joint Chiefs of Staff. Cyber Incident Handling Program. Heinäkuu 2012. 176 sivua.

[59] Patrick Kral. Indicent Handler's Handbook. SANS Institute, Joulukuu 2011. 20 sivua.

[60] Brandie Anderson. Building, Maturing & Rocking a Security Operations Center. Hewlett-Packard. [Viitattu 21.2.2020] Saatavissa: https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Building-Maturing-and-Rocking-a-Security-Operations-Center-Brandie-Anderson.pdf.

[61] Valtiovarainministeriö. Tietoturvapoikkeamatilanteiden hallinta.Elokuu 2017. 66 sivua. ISBN: 978-952-251-834-7.

[62] Don Murdoch. Blue Team handbook: Incident Response Edition. 2. painos. 146 sivua. ISBN-13 978-1500734756.

[63] Dan Gunter. A Practical Model for Conducting Cyber Threat Hunting. SANS Institute. 2020. 16 sivua.

[64] Security Intellegence. A Beginner's Guide to Threat Hunting. Louise Byrne. Julkaistu 12.9.2018 [Viitattu 8.1.2020] Saatavissa: https://securityintelligence.com/a-beginners-guide-to-threat-hunting/.

[65] Wikipedia. Cyber Threat Hunting. Päivitetty 16.1.2020 [Viitattu 17.1.2020] Saatavissa: https://en.wikipedia.org/wiki/Cyber_threat_hunting.

[66] Kirsti Helin. Prikaatikenraali Mikko Heiskanen: Kyberpuolustus on osa nykyaikaista sodankäyntiä.Muuriankkuri. Joulukuu 2019. Sivut 12 - 15. ISSN-L 1459-1480.

[67] Security Boulevard. Threat Hunting Strategies for 2020. Gilad Maayan. Julkaistu 19.11.2019 [Viitattu 8.1.2020] Saatavissa: https://securityboulevard.com/2019/11/threat-hunting-strategies-for-2020/.

[68] Crowdstrike. What is Proactive Threat Hunting? Päivitetty 2019. [Viitattu 8.1.2020] Saatavissa: https://www.crowdstrike.com/epp-101/threat-hunting/.

[69] Panda Security. Getting Know the Threat Hunting Process. Julkaistu 30.11.2018. [Viitattu 5.3.2020] Saatavissa: https://www.pandasecurity.com/mediacenter/security/getting-to-know-the-threat-hunting-process/.

[70] Akashdeep Bhardwaj, Sam Goundar. A framework for effective threat hunting. Network Security. Kesäkuu 2019. Sivut 15 - 19. ISSN 1353 - 4858.

[71] CERT-UK. An introduction to threat intelligence. 2015. 8 sivua.

[72] Vasileios Mavroeidis, Siri Bromander. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. IEEE. 2017. 8 sivua. ISBN: 978-1-5386-2385-5/17.

[73] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. Guide to Cyber Threat Information Sharing. NIST 800-150. 2016. 43 sivua.

[74] Kyberturvallisuuskeskus. [Viitattu 10.3.2020] Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/.

[75] DNSstuff. What Is Threat Intelligence? Definition and Types. Julkaistu 25.10.2019 [Viitattu 17.1.2020] Saatavissa: https://www.dnsstuff.com/what-is-threat-intelligence.

[76] Trend Micro. Indicator of Compromise. [Viitattu 23.3.2020] Saatavissa: https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise.

[77] Pääesikunta, suunnitteluosasto. PVOHJEK-PE Sotilaallisen suorituskyvyn käsitemalli. Asiakirja HO46. Toukokuu 2018. 12 sivua.

[78] Finto. Suomalainen asiasanasto- ja ontologiapalvelu. Tietojärjestelmä. [Viitattu 13.3.2020] Saatavissa: https://finto.fi/tt/fi/page/t79.

[79] Finto. Suomalainen asiasanasto- ja ontologiapalvelu. Tietoverkko. [Viitattu 13.3.2020] Saatavissa: https://finto.fi/tt/fi/page/t38

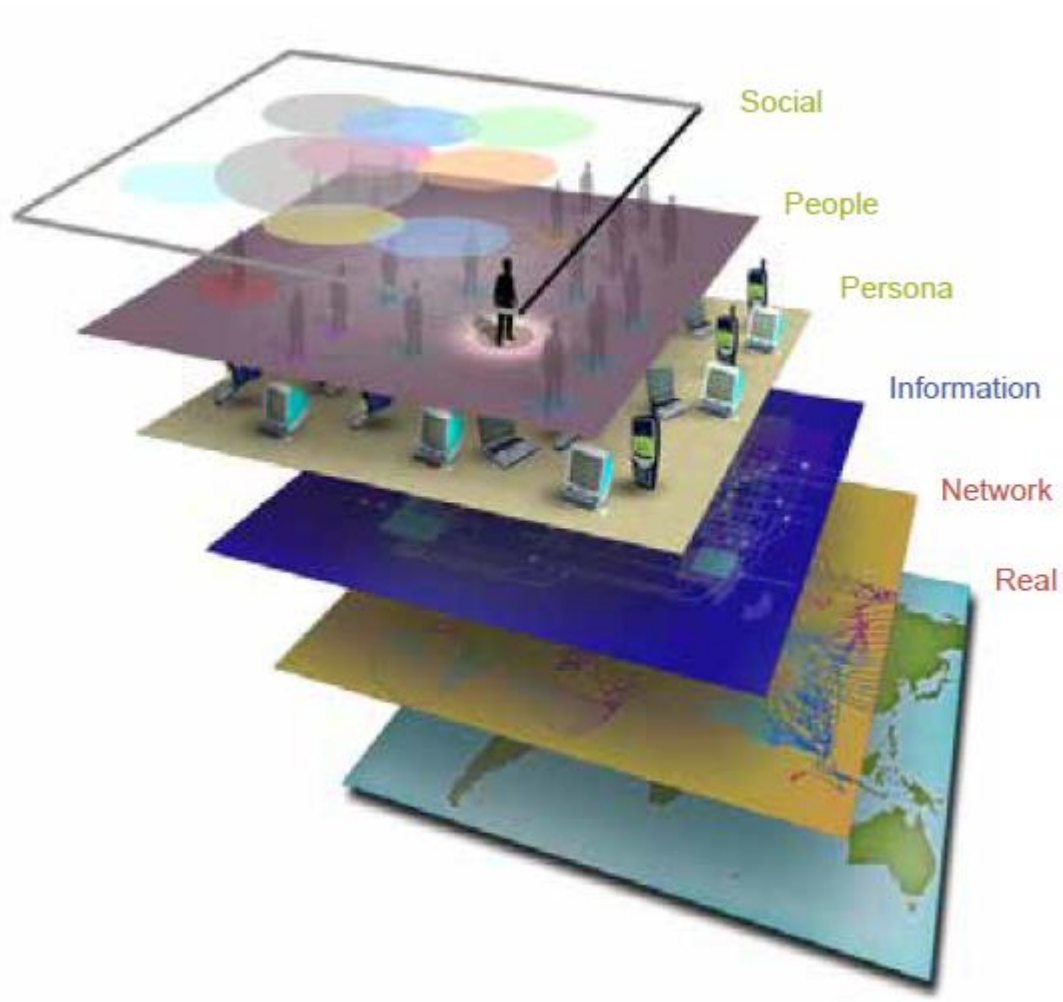
LIITTEET

LIITE 1 - Yhdysvaltojen asevoimien näkemys kyberuhkista

Table 1-1. Sample cyberspace and electronic warfare threat capabilities

Capability	*Methods*	*Indicators*	*First-order effects*
Denial of service attack	Overwhelming a web service, server, or other network node with traffic to consume resources preventing legitimate traffic	Abnormal network performance, inability to navigate web and access sites, uncontrolled spam, and system reboots	Degraded network capabilities ranging from limited operational planning to total denial of use
Network penetration	Man-in-the-middle attacks, phishing, poisoning, stolen certificates, and exploiting unencrypted messages and homepages with poor security features	Unfamiliar e-mails, official looking addresses requiring urgent reply, internet protocol packets replaced, non-legitimate pages with the look of legitimate sites, directed moves from site to site, requests to upgrade and validate information, and unknown links	Uncontrolled access to networks, manipulation of networks leading to degraded or compromised capabilities that deny situational awareness or theft of data
Emplaced malware (virus, worms spyware, and rootkits)	Phishing, spear-phishing, pharming, insider threat introduction, open-source automation services, victim activated through drive-by downloads and victim emplaced data storage devices	Pop-ups, erroneous error reports, planted removable storage media, unknown e-mail attachments, changed passwords without user knowledge, automatic downloads, unknown apps, and degraded network	Spyware and malware on affected systems allow electronic reconnaissance, manipulation, and degrading system performance
Disrupt or deny information systems in the EMS	Prevent friendly antennas from receiving data transmitted in the EMS by using military or commercially available high-powered lasers, high powered microwaves, and repurposed or re-engineered communications systems	Symptoms may not be evident if passive; may manifest as transmission interference, software or hardware malfunctions, or the inability to transmit data	Degraded or complete denial of service in ability to control the EMS denying situational awareness and degrading operational planning

LIITE 2 - Ison-Britannian puolustusministeriön näkemys kybertoimintaympäristön kerroksista



LIITE 3 - MITRE:n ATT&CK-taulukko 1/2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasions
Drive-by Compromise	AppleScript	.bash_profile and . bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP
Spearfishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History
Spearfishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Spearfishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking
	LSASS Driver	Component Firmware	Hooking	Control Panel Items
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow
	Local Job Scheduling	Create Account	Lauch Daemon	DLL Search Order Hijacking
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection
	Scripting	Hypervisor	Scheduled Task	File Deletion
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offset
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass
	Source	LSASS Driver	Sudo Caching	Group Policy Modification
	Space after Filename	Launch Agent	Sudo	HISTCONTROL
	Third-party Software	Launch Daemon	Valid Accounts	Hidden Files and Directories
	Trap	Launchctl	Web Shell	Hidden Users
	Trusted Developer Utilities	Local Job Scheduling		Hidden Window
	User Execution	Login Item		Image File Execution Options Injection
	Windows Management Instrumentation	Logon Scripts		Indicator Blocking
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host
		New Service		Indirect Command Execution
		Office Application Startup		Install Root Certificate
		Path Interception		InstallUtil
		Plist Modification		LC_MAIN Hijacking
		Port Knocking		Launchctl
		Port Monitors		Masquerading
		Rc.common		Modify Registry
		Re-opened Applications		Mshta
		Redundant Access		NTFS File Attributes
		Registry Run Keys / Startup Folder		Network Share Connection Removal
		SIP and Trust Provider Hijacking		Obfuscated Files or Information
		Scheduled Task		Plist Modification
		Screensaver		Port Knocking
		Security Support Provider		Process Doppelgänging
		Service Registry Permissions Weakness		Process Hollowing
		Setuid and Setgid		Process Injection
		Shortcut Modification		Redundant Access
		Startup Items		Regsvcs/Regasm
		System Firmware		Regsvr32
		Systemd Service		Rootkit
		Time Providers		Rundll32
		Trap		SIP and Trust Provider Hijacking
		Valid Accounts		Scripting
		Web Shell		Signed Binary Proxy Execution
		Windows Management Instrumentation Event Subscription		Signed Script Proxy Execution
		Winlogon Helper DLL		Software Packing
				Space after Filename
				Template Injection
				Timestomp
				Trusted Developer Utilities
				Valid Accounts
				Virtualization/Sandbox Evasion
				Web Service
				XSL Script Processing

LIITE 3 - MITRE:n ATT&CK-taulukko 2/2

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	COmmunication Through Removable Media	Data Compressed	Data Encrypted for Impact
Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint denial of Service
Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	System Service Discovery			Standard Non-Application Layer Protocol		
	System Time Discovery			Uncommonly Used Port		
	Virtualization/Sandbox Evasion			Web Service		

LIITE 4 - MITRE:n ATT&CK-taulukon hyökkäystekniikoiden datalähteiden jako alakategorioihin

Yläkategoria	Alakategoria	Valvonnan datalähde
Tietoverkko	Sisäverkko	Packet capture
Tietoverkko	Sisäverkko	Netflow/enclave netflow
Tietoverkko	Sisäverkko	Process use of network
Tietoverkko	Sisäverkko	Host network interface
Tietoverkko	Ulkoverkko	SSL/TLS inspection
Tietoverkko	Ulkoverkko	Web proxy
Tietoverkko	Molemmat	Network protocol analysis
Laitetaso	Käyttöjärjestelmä	MBR
Laitetaso	Käyttöjärjestelmä	VBR
Laitetaso	Käyttöjärjestelmä	Kernel Drivers
Laitetaso	Käyttöjärjestelmä	Component firmware
Laitetaso	Käyttöjärjestelmä	Windows Error Reporting
Laitetaso	Käyttöjärjestelmä	Environment variable
Laitetaso	Käyttöjärjestelmä	API monitoring
Laitetaso	Käyttöjärjestelmä	System Calls
Laitetaso	Käyttöjärjestelmä	Windows Registry
Laitetaso	Käyttöjärjestelmä	WMI objects
Laitetaso	Käyttöjärjestelmä	Access tokens
Laitetaso	Käyttöjärjestelmä	Named pipes
Laitetaso	Prosessit	Process Monitoring
Laitetaso	Prosessit	Process command-line parameters
Laitetaso	Prosessit	Loaded DLL
Laitetaso	Prosessit	DLL monitoring
Laitetaso	Prosessit	User Interface
Laitetaso	Prosessit	Services
Laitetaso	Prosessit	Browser extensions
Laitetaso	Tiedostot	File monitoring
Laitetaso	Tiedostot	Binary file metadata
Laitetaso	Lokit	Authentication Logs
Laitetaso	Lokit	Office 365 account logs
Laitetaso	Lokit	Azure activity logs
Laitetaso	Lokit	AWS Cloudtrail logs
Laitetaso	Lokit	Stackdriver logs
Laitetaso	Lokit	Application logs
Laitetaso	Lokit	Digital certificate logs
Laitetaso	Lokit	Oauth audit logs
Laitetaso	Lokit	Third-party application logs
Laitetaso	Lokit	Office 365 trace logs
Tietoverkko	Lokit	Web logs
Tietoverkko	Lokit	Network device logs
Tietoverkko	Lokit	Web application firewall logs
Laitetaso	Lokit	Windows event log
Laitetaso	Lokit	Powershell logs
Molemmat	Verkko ja käyttöjärjestelmä	DNS records
Molemmat	Verkko ja prosessit	Mail server
Molemmat	Verkko ja prosessit	Email gateway
Laitetaso	Forensiikka	Disk forensics
Laitetaso	Forensiikka	Malware reverse engineering
Laitetaso	Forensiikka	BIOS
Laitetaso	Forensiikka	EFI
Tietoverkko	Työkalut	NIDS
Tietoverkko	Työkalut	Data loss prevention
Molemmat	Työkalut	Sensor health and status
Laitetaso	Työkalut	Antivirus