VAKIOITUJEN VERKON VALVONTA- JA HALLINTAMENETELMIEN JA -TEKNIIKOIDEN HYÖDYNTÄMINEN TIETOLIIKENNEVERKKOJEN KYBERVALVONNASSA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Riihimäki, tieto- ja viestintätekniikka

Kevät, 2018

Mika Kontio

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Riihimäki

Tekijä Mika Kontio **Vuosi** 2018
Työn nimi Vakioitujen verkon valvonta- ja hallintamenetelmien ja -tekniikoiden hyödyntäminen tietoliikenneverkkojen kybervalvonnassa.
Työn ohjaaja/t Marko Grönfors, Tommi Hytönen

TIIVISTELMÄ

Opinnäytetyön päätavoitteena oli selvittää vakioitujen verkon valvonta- ja hallintamenetelmien ja -tekniikoiden hyödyntämismahdollisuuksia tietoliikenneverkkojen kybervalvonnassa. Työ on tehty kirjallisuustutkimuksena ja siinä oli kaksi tutkimuskysymystä. Ensimmäisenä tutkimuskysymyksenä oli perinteisen verkonvalvonnan ja –hallinnan tuottaman informaation yhdistämismahdollisuudet kybervalvontaan, turvallisuuden tilannekuvan muodostamiseksi. Toisena tutkimuskysymyksenä oli selvittää, mitä muuta tietoa verkkoliikenteestä, verkon aktiivilaitteista, päätelaitteista ja sovelluksista tarvitaan perusteellisen valvontadatan saamiseksi tietoverkkoja valvovaan kybervalvomoon.

Aluksi työssä esitetään verkon valvonnan ja hallinnan teoria standardin X.700 mukaisesti, FCAPS-jaottelulla. Sen jälkeen esitetään esimerkkiverkon kuva, jonka avulla selvitetään verkon valvonnan ja hallinnan menetelmät ja tekniikat. Kybervalvonnan tarve perustellaan työssä teoriaosuuden kautta, jossa todetaan muun muassa tarve tilannekuvalle ja siitä johdettavalle tilanneymmärrykselle turvallisuuden osalta. Esimerkkiverkon avulla havainnollistetaan mahdollisuudet kybervalvonnalle ja esitetään mitä tietoja tietoliikenneverkosta on saatava kattavan turvallisuustilannekuvan saavuttamiseksi. Työssä esitellään myös mahdollisuudet hyödyntää verkon valvonnan ja hallinnan tuottamaa informaatiota kybervalvonnassa. Näitä ovat muun muassa network flow -tyyppinen tieto, konfiguraation hallintatietokanta sekä yhteiskäyttöinen lokipalvelinratkaisu.

Työtä tehtäessä havaittiin, että parhaaseen tulokseen kybervalvonnassa päästään, mikäli valvontaa suorittavalla organisaation osalla on tehtävissään täysi toimintavalta ja hybridimuotoinen kokoonpano, jolloin poikkeamatilanteiden hallintaan voidaan ottaa avuksi verkon valvonnan ja hallinnan asiantuntijoita heidän erityisosaamisalueidensa mukaisesti. Kattavan kybertilannekuvan saamiseksi on kerättävä informaatiota myös tietoliikenneverkkoon liitetyiltä työasemilta ja palvelimilta sekä uhkatietoa organisaation ulkopuolisista lähteistä.

Avainsanat CSOC, Kyber, Kybervalvonta, NOC, SOC
Sivut 45 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and communication technology
Riihimäki campus

Author Mika Kontio **Year** 2018
Subject Possibilities of a cyber security operation center to implement information produced by network management system
Supervisors Marko Grönfors, Tommi Hytönen

ABSTRACT

The main goal for this thesis project was to define standardized network management procedures and techniques, and their abilities to enhance situational awareness of the security operation center. The thesis was written as literature research, and it included two research questions. The first question was to find connection potential for information gathered by a network management system to combine this information with information gathered by the SIEM-system for reaching situational awareness of the security operation center. The second question was to find out what kind of other information was needed to be collected with the SIEM-system.

At first, this thesis presents network management theory based on international standard X.700. This is followed by an example of a network diagram that is used to clarify network management procedures and techniques. The need for cyber situational awareness is presented with theoretical discussion on the need for cyber situational view and understanding the view in the context of cyber security of an organization. The sample network diagram is presented to show the possibilities of cyber security surveillance and the need for information to be gathered. The thesis also presents possibilities to combine information gathered by a network management system with the SIEM-system. Findings included other things: network flow information, the contents of a configuration management database, and possibility to combine information in a cooperative logging system.

Security operation center (SOC) will reach its best results when it has a central and hybrid organization model, with full authority as to managing security incidents and threats in organization. Using this model and authorization SOC can obligate the network management personnel specialists and utilize their skillset for a deeper incident analysis. For a comprehensive situational view, and awareness about security in an organization's network there is also a need for gathering information from workstations and servers, as well as intelligence threats from sources located outside the organization.

Keywords CSOC, Cyber, Cyber Security Operation Center, NOC, SOC
Pages 45 pages

SISÄLLYS

1 JOHDANTO 1

2 VERKON VALVONTA JA HALLINTA 3

2.1 Vikatilanteiden hallinta 4
2.2 Konfiguraatioiden hallinta 6
2.3 Käyttöoikeuksien hallinta 7
2.4 Suorituskyvyn hallinta 8
2.5 Turvallisuuden hallinta 9

3 VERKON VALVONTA- JA HALLINTAJÄRJESTELMÄ 11

3.1 Tietoliikenneverkko 12
3.2 Verkon hallinnan osakokonaisuudet 14
3.3 Verkon aktiivilaitteet 15
3.4 Työasemat ja palvelimet 16
3.5 Verkon valvomo (NOC) 16
3.6 Varautuminen ja toipuminen 17

4 KYBERVALVONTA 19

4.1 Kerättävästä datasta tilanneymmärrykseen 20
4.2 Turvallisuusvalvonta ja päätöksenteko 23
4.3 Turvallisuusvalvonnan maturiteetti 26
4.4 Työkalut tilannekuvan saavuttamiseen 26

5 KYBERVALVONTAJÄRJESTELMÄ 33

5.1 Työasemat 34
5.2 Aktiivilaitteet 35
5.3 Lokitietojen kerääminen 35
5.4 Tietoliikenteen tietojen kerääminen 36
5.5 SIEM -järjestelmä 36
5.6 Turvallisuusvalvomo (SOC) 37
5.7 Varautuminen ja toipuminen 38

6 VAKIOITUJEN VERKON VALVONTA- JA HALLINTAMENETELMIEN JA -TEKNIIKOIDEN HYÖDYNTÄMINEN KYBERVALVONNASSA 40

7 YHTEENVETO 44

LÄHDELUETTELO 46

1 JOHDANTO

Tietoliikenneverkkojen ja sen sovellutusten kehitys on johtanut monimutkaisiin ratkaisuihin runko- ja lähiverkoissa. Tämä on vaikuttanut myös tietoturvaongelmien ja -loukkausten määrän kasvuun vuosituhannen vaihteen jälkeen. Julkisuudessa on uutisoitu valtioiden kehittävän suojauskykyään tietoverkoissa, samaan aikaan useimmat toimijat kehittävät myös tiedustelu- ja vaikuttamiskykyään. Viimeistään Stuxnet-haittaohjelman tultua ilmi vuonna 2010, on käynyt selväksi, että esimerkiksi suurvaltojen valtiollisten toimijoiden kyvykkyydet tietoverkoissa vaikuttamiseen ovat korkealla tasolla. Julkisuudessa aiheesta alettiin käyttää termiä kyberturvallisuus. Tietoturvallisuus ei enää riittänyt käsitteenä kattamaan kuvausta kokonaistietoturvallisuudesta. Tietovuodot muun muassa Yhdysvaltojen ja sen liittolaisten tiedustelu- ja vaikuttamiskyvyistä 2010-luvun alkupuoliskolla johtivat siihen, että maailmanlaajuisesti alettiin kiinnittää huomiota organisaatioihin sekä yhteiskunnalle tärkeisiin kohteisiin kohdistettuihin kyberuhkiin. Suomessa kansallinen kyberstrategia julkaistiin vuonna 2013. Tietoturvallisuuteen Suomessa on valtionhallinnossa kiinnitetty korostetusti huomiota vuosituhannen vaihteesta lähtien, jolloin valtiovarainministeriön alaisuuteen perustettiin valtionhallinnon tietoturvallisuuden ohjausryhmä (VAHTI). Tämän toimijan tehtävänä on ohjeistaa julkishallintoa kyber- ja tietoturvallisuuden hallinnassa. Sittemmin ohjausryhmän nimi on muuttunut julkishallinnon digitaalisen turvallisuuden ohjausryhmäksi. Ohjausryhmän tuottamat ohjeet kyber- ja tietoturvallisuuden parantamiseksi sopivat hyvin myös siviiliorganisaatioiden käyttöön.

Organisaatioilla on mahdollisuus parantaa kilpailukykyään kehittämällä kyber- ja tietoturvallisuuttaan. Vastuullinen toiminta kyberturvallisuuden kehittämiseksi vaatii turvallisuuden tilannekuvan seurantaa organisaation tietoliikenneverkoissa. Tietoliikenneverkoissa tapahtuvista turvallisuuteen vaikuttavista ilmiöistä tietäminen on entistäkin tärkeämpää. Näin luodaan kyky ennakoida tietoliikenneverkon haitallisia tapahtumia mahdollisuuksien mukaan jo etukäteen. Organisaatioissa on kyettävä tunnistamaan tietoliikenneverkkoon kohdistuvat uhat ja riskit niiden toteutumiselle. Tätä kautta organisaation tietoliikenneverkon kyberturvallisuuteen voidaan vaikuttaa vaaditulla tavalla.

Kyberturvallisuus on tietoturvallisuutta laajempi käsite. Kyberturvallisuus ottaa huomioon myös tietoliikenneverkkojen ulkopuoliset tapahtumat ja vaikuttamismahdollisuudet. Kyberturvallisuuden käsitteen kautta voidaan ymmärtää, että tapahtumat tietoliikenneverkoissa voivat ilmetä erilaisina tapahtumina myös fyysisessä maailmassa. Perinteisten tietoliikenneverkkojen valvonnan ja hallinnan toimien lisäksi tarvitaan kattavaa turvallisuusvalvontaa ja suurimmissa organisaatioissa on perustettu turvallisuusvalvomoita (Security Operation Center – SOC). Näiden toimien kattamiseksi on syntynyt myös kaupallista toimintaa, joiden avulla organisaatiot voivat

halutessaan ulkoistaa tietoliikenneverkkojen turvallisuuden valvontaa ja hallintaa erillisiin turvallisuusvalvomoihin.

Tietoliikenneverkkojen turvallisuusvalvonta ei poista tarvetta perinteiselle tietoverkkojen valvonnalle ja hallinnalle. Pienissä organisaatioissa nämä voivat olla yhdistettynä, mutta suurissa organisaatioissa saavutetaan nopeampia toimia turvallisuuden parantamiseen ja turvallisuuspoikkeamiin reagoimiseen perustamalla erillinen turvallisuusvalvomo tai ulkoistamalla toiminta. Toiminnan ulkoistamisessa on haasteensa, kaupalliset palveluntarjoajat valvovat tavallisesti usean eri toimijan verkkoja ja tällöin niiden reaaliaikainen toiminta ja poikkeamiin kohdistuva reagointikyky voidaan kyseenalaistaa.

Tässä opinnäytetyössä keskitytään kehittämään konseptiratkaisua kybervalvontaan ja selvittämään kybervalvonnan mahdollisuuksia suljetuissa IP-verkoissa. Opinnäytetyössä pyritään selvittämään, kuinka perinteisen verkon valvonnan ja hallinnan tuottamaa dataa voidaan hyödyntää myös verkon turvallisuusvalvonnassa. Työssä tietoliikenneverkko kuvataan esimerkinomaisena ja samalla pohditaan ensimmäisenä tutkimuskysymyksenä, kuinka perinteisen verkonvalvonnan ja –hallinnan tuottamaa informaatiota voidaan yhdistää kybervalvontaan tilannekuvan muodostamiseksi. Toisena tutkimuskysymyksenä työssä selvitetään, mitä muuta tietoa verkkoliikenteestä, verkon aktiivilaitteista, päätelaitteista ja sovelluksista tarvitaan perusteellisen valvontadatan saamiseksi tietoverkkoja valvovaan kybervalvomoon.

Suljetulla IP-verkolla tässä työssä tarkoitetaan IP-pohjaista tietoliikenneverkkoa, josta ei ole rajapintaa Internetiin. Käyttäjillä ei siis ole mahdollisuutta internet-selaamiseen tai henkilökohtaisen sähköpostin lähettämiseen. Näiltä osin esimerkiksi yksityisyyden suojaa ei oteta huomioon valvontaratkaisuja mietittäessä. Työn ulkopuolelle rajataan myös työntekijöiden suorittamat toimet kybervalvomossa sekä mahdolliset IoT-laitteet organisaatiossa. Varsinaisia konseptia hyödyntäviä ja todentavia testejä ei ole tehty, työssä haetaan ainoastaan kirjallisuustutkimuksen avulla konseptia kybervalvonnan suorittamiselle teknisten ratkaisujen löytämiseksi. Näkökulma opinnäytetyössä on siis tekninen, liiketoiminnallista näkökulmaa ei työssä käsitellä.

2 VERKON VALVONTA JA HALLINTA

Tietoliikenneverkot ovat nykyään rakenteiltaan ja toiminnoiltaan monimutkaisia kokonaisuuksia. Pelkästään eri aktiivilaitteiden konfigurointi vaatii selkeää näkemystä ja osaamista verkon eri laitteiden toiminnallisuuksista sekä käytetyistä tietoliikenneprotokollista. Laitevalmistajilla on toisistaan eriäviä, omia ratkaisuja ja sovelluksia yksittäisten laitteiden sekä laitekokonaisuuksien hallintaan. Usein nämä ratkaisut ovat standardoimattomia tai standardia on mukautettu soveltumaan laitevalmistajien tarkoituksiin. (Clemm, 2006, 81.) Verkossa tehtävien muutosten yhteydessä suoritetaan aktiivilaitteiden konfigurointia näiden muutosten toteuttamiseksi. Tietoliikenneverkoissa tarvitaan aktiivista verkonvalvontaa ja –hallintaa. (Abeck ym. 2009, 30.) Tähän toiminteeseen taas tarvitaan verkonvalvontajärjestelmää (Network Management System – NMS). Verkonvalvontajärjestelmällä voidaan ilmaista erilaisia tapahtumia tietoliikenneverkossa.

Tietoliikenneverkkoa valvovaa ja hallinnoivaa organisaation osaa kutsutaan verkon valvomoksi (Network Operation Center – NOC) tai verkon hallintakeskukseksi (Network Management Center – NMC). Aihealueen englanninkielisessä kirjallisuudessa on pääosin siirrytty NOC-nimitykseen, myös ITIL:ssä. Tietoverkon valvomolla on perinteisesti käytössään hallintaasema ja hallintasovellus, jonka avulla tietoa kerätään ja esitetään valvomossa toimivalle henkilöstölle (Abeck ym. 2009, 34). Hallintasovelluksella voi olla useita eri tasoja, joiden avulla tietoa kerätään verkon eri osista (Element Management Systems – EMS) toistensa kanssa samankaltaisista laitteistoista. (Abeck ym. 2009, 34) Mikäli aktiivilaitteissa on toteutettu standardoitu ja strukturoitu konfigurointiprotokolla, esimerkiksi SNMP, ei hallintatasoja ole järkevää lisätä. (Abeck ym. 2009, 35.) Valvottavia ominaisuuksia voivat olla muun muassa palvelinten toiminta-aika ja levytilan käyttö, tietoliikennekapasiteetin käyttö tietyllä yhteysvälillä ja aktiivilaitteiden tilatietoja (Abeck ym. 2009, 16; Nathans 2015, 5-6). Verkonvalvonta ja –hallinta käsittää tietoverkon ylläpidolliset toimet ja ongelmatilanteiden ratkaisut. Tietoliikenneverkkoa valvovan ja ylläpitävän toimijan osalta tämä vaatii näkyvyyttä kohdeverkkoon eli informaation keräämistä tietoverkon toiminnasta sekä mahdollisuutta vaikuttaa verkon toimintaan. Erilaisia ongelmatilanteita pyritään välttämään analysoimalla kerättyä tietoa tietoverkon ja siihen liitettyjen laitteiden toiminnasta sekä tarpeen mukaan muuttamalla toiminnallisuutta, esimerkiksi aktiivilaitteiden konfiguraatiota. (Abeck ym. 2009, 30.) Valvomot kykenevät selvittämään ongelmia ja niihin johtaneita syitä, analysoimaan eri vaihtoehtoja ongelman ratkaisemiseksi sekä ratkaisemaan teknisiä ongelmia asiantuntijoiden avulla (Abeck ym. 2009, 13-21).

Normaalitilanteessa tietoliikenneverkon osajärjestelmä toimii suunnitellusti, tällöin saatu tieto on informatiivista, vaikka

verkonvalvontajärjestelmä antaisi ilmoituksen muutoksesta. Varoitus ilmaisee, että tietty järjestelmän osa ei toimi kuten sen pitäisi. Tyypillisesti tällöin on ylitetty jokin tietty ennalta asetettu valvonnallinen raja-arvo, joko järjestelmän osassa tai valvontajärjestelmässä. Varoitus voidaan antaa esimerkiksi tietoliikenneverkon aktiivilaitteen prosessorin kuormituksen noustessa yli 80 prosenttiin. Poikkeamailmoitus annetaan vikaantumistapauksessa ja tällöin tarvitaan välittömiä toimenpiteitä häiriötilanteen ratkaisemiseksi. (Davies 2016, Service Operation.) OSI –mallin tietojenkäsittelyjärjestelmän hallinnoinnin viitekehyksen mukaisia tietoliikenneverkon valvonnan ja hallinnan toiminteita ovat:

- Vikatilanteiden hallinnointi
- Konfiguraatioiden hallinnointi
- Käyttöoikeuksien hallinnointi
- Suorituskyvyn hallinnointi
- Turvallisuuden hallinnointi

(Abeck ym. 2009, 13; ISO/IEC 7498-4 1989, 2).

2.1 Vikatilanteiden hallinta

Vikatilanteiden hallinnoinnilla pyritään varmistamaan, että tietoliikenneverkon osajärjestelmät ja sen palvelut ovat käyttäjien käytettävissä sekä pitämään katkosten pituudet minimissä. Vikatilanteiden hallinnoinnin pääosia ovat:

- Tietoliikenneverkon tarkkailu
- Vikojen ja ongelmatilanteiden selvittäminen
- Lokitiedon kerääminen tietoliikenneverkon toiminnasta
- Ongelmien tiketöinti
- Ennakoiva toiminta.

(Clemm, 2006, FCAPS: The ABC’s of Management.)

Vikatilanteiden hallinnan onnistumiseksi tietoliikenneverkon ylläpitäjällä on oltava näkymä kokonaisjärjestelmän toiminnasta, jonka avulla voidaan todeta verkon toimivan suunnitellusti. Tärkeimpänä tehtävänä valvontajärjestelmää käyttävällä valvojalla on vikailmoitusten hallinnointi. Valvojan on kyettävä valvontajärjestelmän avulla tunnistamaan ongelmat ja aloittamaan vikatilanteen ratkaisutoimenpiteet. (Clemm, 2006, FCAPS: The ABC’s of Management.)

Vikatilanteiden hallinnan onnistumiseksi virhelokien keräämisellä on suuri merkitys. Virhelokien seuraamisella pystytään jäljittämään ja tunnistamaan vikatilanteiden aiheuttaja sekä puuttumaan vikatilanteeseen. Vikatilanteeksi käsitetään toiminnallisuuksien puutteellisuus, järjestelmän osan toimimattomuus ja palveluiden saatavuuden ongelmat. Tietoa ongelmista saadaan tietoliikenneverkon osajärjestelmien tuottamista lokitiedoista, verkonvalvontajärjestelmästä ja käyttäjiltä. (Abeck ym. 2009, 16.)

Valvontajärjestelmän ja sen käyttäjien antamat vikatilanneilmoitukset on kyettävä dokumentoimaan, tämä luo tarpeen tiketöintijärjestelmälle (Davies 2016, Service Operation). Tähän järjestelmään kirjataan muun muassa vian kuvaus, ilmenemisaika, ilmoittaja ja tehdyt toimet vian ratkaisemiseksi. Tarpeen mukaan tiketöintijärjestelmään järjestetään mahdollisuus ilmoitusten priorisoinnille. (Davies 2016, Service Operation.) Samaa tiketöintijärjestelmää käytetään valvontajärjestelmästä saatujen hälytysten kirjaamiseen. Tiketöintijärjestelmää päivittää kulloinkin vuorossa oleva tietoliikenneverkon valvoja. Tiketöinti voi olla automatisoitua verkonvalvontajärjestelmän tuottamien hälytysten osalta. (Subramanian 2010, Network Operations and NOC.) Vikatilanteiden analyysien perusteella saadaan esimerkiksi tietoliikennejärjestelmän testausta varten tarvittavaa dataa. Vikatilanteista toipumisen edistämiseksi valvontajärjestelmä voidaan rakentaa sellaiseksi, että se tuottaa historiatiedon perusteella automaattista informaatiota samankaltaisten ongelmien ratkaisuista (Subramanian 2010, Network Operations and NOC). Tietoliikenneverkon osajärjestelmän vikatilanteesta kerätyllä lokitiedolla ja tiketöintijärjestelmään tuotetun kuvauksen avulla ongelma voidaan toistaa testiympäristössä ja tarvittaessa puuttua merkityksellisiin ongelmiin vielä tietoliikennejärjestelmän elinkaaren ylläpitovaiheessa (Abeck ym. 2009, 16). Lokitietoa on kerättävä myös tietoliikenneverkon osajärjestelmien normaalitilanteesta, koska toimintoja on kyettävä tarkastelemaan historiatietona myöhemmässä vaiheessa (Abeck ym. 2009, 16). Mikäli kerätään ainoastaan virhelokia, on vikatilanteiden vertaaminen normaalitilanteiden toiminteisiin järjestelmässä haastavaa. Vikatilanteiden hallintatoimiin liittyen voidaan suorittaa konfiguraatioiden hallinnointiin liittyvä ITIL-muutoksenhallintaprosessin mukainen hätämuutostehtävä.

Lokitiedon kerääminen tietoliikennejärjestelmän eri osista tehdään usealla eri tasolla. Informatiivisesta lokitiedosta voidaan nähdä esimerkiksi koska aktiivilaite on uudelleenkäynnistynyt. Lokijärjestelmään tallennettujen tietojen perusteella voidaan hakea merkityksiä verkossa ilmenneille asioille. Aikaleiman perusteella voidaan tarkastella esimerkiksi, onko aktiivilaite käynnistynyt itsekseen uudelleen vai onko se tehty verkonvalvonnan toimesta tai ajastetusti. Lokitietoa voidaan kerätä myös järjestelmäkehitystä varten. (Chuvakin, Schmidt & Phillips, 2012, Log data basics.) Linux- ja unix -järjestelmissä kerätään erillistä asetusta käyttämällä niin sanottua debug –tietoa syslog –tiedon yhteyteen (Ubuntu 2015). Varoitustieto lokeissa kertoo, että järjestelmän tai sovelluksen suorittamisessa havaitaan virheitä, mutta tämä ei haittaa vielä toimintaa. Virhetieto lokissa kertoo ilmenneestä osajärjestelmän tai sovelluksen virhetilasta. Usein virhetieto on ylimalkaista ja sen juurisyiden selvittämiseen täytyy järjestelmän lokitietoa käydä läpi perusteellisemmin. Hälytykset lokitiedoissa kertovat häiriötilasta, jossa järjestelmän osan tai sovelluksen toiminta on mahdollisesti pysähtynyt kokonaan. (Chuvakin ym. 2012, Log data basics.) Lokitiedon keräämistä tietoliikenneverkon eri laitteissa voidaan säätää monin tavoin, myös kerättävän tiedon tarkkuutta voidaan säätää.

Lokitietoa voidaan kerätä järjestelmän eri osista paikallisesti säilytettävänä kyseisessä laitteessa, on kuitenkin suositeltavampaa toimittaa lokitieto ulkoiselle palvelimelle. Tällä saavutetaan etua lokitiedon analysoinnissa, jolloin se voidaan keskittää usean yksittäisen paikan sijaan yhteen paikkaan sekä lisätä samalla säilytysvarmuutta lokitiedon ylläpidon osalta. (Chuvakin ym. 2012, Log data basics.) Lokitiedon toimittaminen ulkoiselle palvelimelle tehdään yleisimmin UDP –protokollayhteyttä käyttäen. Osa kaupallisista ja avoimen lähdekoodin ratkaisuista tukee myös TCP-protokollan käyttöä, jonka avulla voidaan varmistaa protokollatasolla tietoliikennepakettien perillemeno. Perustoiminnallisuudeltaan yhteydet ulkoiselle lokipalvelimelle ovat asiakas - palvelin –yhteyden kaltaisia. Käytetyin tapa palvelimelle kerättävälle lokidatan muodolle on syslog-protokolla, joka on standardoitu ratkaisu lokidatan keräämiseen. Syslog-dataformaattia käytetään tavallisimmin linux- ja unix-ympäristöissä kerättävälle lokitiedolle. Myös Windowsista ja useimmista laitekohtaisista käyttöjärjestelmistä löytyy tuki syslog-dataformaatille. Verkonvalvontaan ja hallintaan kehitettyä SNMP-protokollaa on joissain tapauksissa sovellutettu myös lokitiedon toimittamiseen. Suurin ero syslog- ja SNMP-protokollilla on SNMP:lla siirrettävän MIB-tietokannan strukturoitu muoto ja sisältö verrattuna pelkistettyyn syslog-dataformaattiin. Yleisimmäksi tavaksi lokidatan tallentamiseen palvelimelle on viedä kerättävä data tietokantaohjelmistoon. (Chuvakin ym. 2012, Log data basics.) Tämä toiminnallisuus vaatii datasisällön muokkaamista tietokantaan viemiseksi. Räätälöidyissä ratkaisuissa syslog –muotoinen tieto voidaan muokata tietokannan skeeman mukaiseksi ennen sen lähettämistä lokipalvelimelle tai kirjoittaa se suoraan käytettävän skeeman mukaiseksi.

2.2 Konfiguraatioiden hallinta

Konfiguraatioiden hallinnoinnilla käsitetään tietoliikenneverkon laitteistojen ja palveluiden hallintaa. Näiden hallinnointiin kuuluu muun muassa asetusparametrien asettaminen ja muuttaminen, laitteistojen ja palveluiden nimeäminen, alustaminen, tilatietojen monitorointi sekä konfiguraatiotietojen päivittäminen muutosten yhteydessä. (ISO/IEC 7498-4 1989, 2.) Usein voidaan asettaa erilaisia hälytysten ja varoitusten raja-arvoja sekä tarvittaessa suodattaa tietoliikenneverkosta valvontajärjestelmään saatavaa tietoa (Abeck ym. 2009, 15). Tietoliikenneverkon ylläpitoa voidaan helpottaa vakioimalla konfiguraatioiden hallinta mahdollisimman pitkälle saman tyyppisten ja saman laitevalmistajan laitteiden osalta. Tällöin käytetään konfiguraatioiden hallintajärjestelmää (Configuration Management System – CMS). ITIL-prosessikehyksessä määritelmän nimenä käytetään palveluomaisuuden- ja konfiguraationhallintaa (Service asset and configuration management - SACM). (Abeck ym. 2009, 16; Davies 2016, Service Transition Processes.) Konfiguraatioiden hallintajärjestelmän tueksi on oltava konfiguraatiotietokanta (Configuration Management Database – CMDB), johon jokaiselle tietoliikenneverkon laitteelle perustetaan oma tietue (Davies 2016, Service Transition Processes). Konfiguraatiotietokannasta ilmenee jokaiselle laitteelle vähintään konfiguraation identifioiva

tunniste, kategorisoiva nimi, IP-osoitteistus, fyysinen sijoituspaikka, käytön aikainen konfiguraatiotiedosto ja alustuskonfiguraatiotiedosto. Tietoihin voidaan lisätä myös käyttöjärjestelmä versiotietoineen, asennetut ohjelmistot ja niiden versiot, laitteen fyysinen kokoonpano sekä uudelleenasennusta nopeuttava ajantasainen levykuva. (Davies 2016, Service Transition Processes.) Konfiguraatioiden hallintaan kuuluu olennaisena osana muutosten hallinta, joka luokitellaan seuraavasti:

- Hätämuutos (Emergency changes)
- Normaali muutos (Normal changes)
- Standardimuutos (Standard changes).

Hätämuutokset ovat tehtäviä, jotka on suoritettava mahdollisimman nopeasti. Näitä voivat olla esimerkiksi tietoliikenneverkon laajavaikutteiset häiriöt tai osajärjestelmien tietoturvapäivitykset. Hätämuutoksiin liittyvä muutoksenhallinta voidaan tarvittaessa tehdä ilman varsinaista tuotantoverkon ulkopuolista testaamista, mikäli sen luonne sitä vaatii. ITIL:n muutoksenhallintaprosessissa on olemassa erillinen menettelytapa, jolla hätämuutokset käsitellään. Normaalimuutokset ovat puolestaan tehtäviä, jotka omaavat kohtuullisen riskin. Normaalimuutokset noudattavat muutoksenhallintaprosessin määriteltyjä vaiheita. Standardimuutokset ovat matalariskisiä ja ennalta hyväksyttyjä muutoksia, eivätkä edellytä erillistä muutospyyntöä. Standardimuutoksia seurataan käyttäen palvelupyyntöä, näitä voivat olla esimerkiksi salasanan vaihto asiakkaalle, uuden päätelaitteen toimittaminen asiakkaalle tai ennalta määritellyn ohjelmiston asentaminen asiakkaan koneelle. Standardimuutoksista on yleensä olemassa menettelytapa- tai työohje. (Davies 2016, Service Transition Processes.)

2.3 Käyttöoikeuksien hallinta

Käyttöoikeuksien hallinnointiin (Accounting management) kuuluu ISO/IEC 7498-4 standardissa kirjanpito, jolla tarkoitetaan asiakkaalta tehtävän laskutuksen pohjatiedoksi kerättävää dataa (ISO/IEC 7498-4 1989, 3). Nykyisissä tietoliikenneverkoissa veloitusten suorittaminen siirretyn datan tai käytetyn yhteysajan pohjalta on käytössä internetin palveluntarjoajien myydessä sovelluksia, sovellusalustoja tai palvelintilaa, sekä mobiiliverkkojen liittymissä. Accounting management –termiin alkuperäisessä ISO/IEC 7498-4 –standardissa kuuluu resurssien käytön kirjanpito laskutusta varten. Käyttöoikeuksien hallinta on tärkeä osa-alue yksiselitteisen kirjanpidon ja laskutuksen järjestämiseksi. Käyttäjäoikeuksia standardissa käsitellään ainoastaan accounting management –termiin liittyen. (ISO/IEC 7498-4 1989, 3.) Tästä syystä on luontevaa suljetun IP-verkon osalta käsitellä käyttöoikeuksien hallinta tähän termiin liittyvänä.

Käyttöoikeuksien hallinnoinnilla taataan tietoturvallisuuden luottamuksellisuuden, eheyden ja saatavuuden toteutumista. Käyttöoikeuksien hallintaan kuuluu

- Käyttäjähallinta
- Autentikointi
- Käyttövaltuushallinta
- Kirjanpito.

(Davies 2016, Service Operation Processes.)

Käyttäjien tunnistamiseksi perustetaan keskitettyyn käyttäjien tunnistamiseen käyttäjärekisteri, joka voi olla esimerkiksi tietokanta. Käyttäjiä lisätään ja poistetaan tietoliikenneverkon käyttöpolitiikan mukaisesti. Käyttäjät on tunnistettava tietoliikenneverkon resurssien käytön yhteydessä, koska tietoliikenneverkon resurssien käyttö on pystyttävä kiistämättömästi osoittamaan. Käyttäjiä varten perustetaan rooliperusteisia käyttöoikeusryhmiä, jotka helpottavat käyttöoikeuksien hallintaa. Saman tyyppisissä rooleissa työskenteleviä käyttäjien oikeuksia voidaan käsitellä helpommin kokonaisuutena. (Osmanoglu 2013, Roles and rules.) Yksittäisten käyttäjien poiketessa käyttöoikeusryhmän tarpeista, voidaan muutokset tehdä kyseiselle käyttäjälle. Tarvittaessa käyttäjältä voidaan myös poistaa tarpeettomia resurssien käyttöoikeuksia. (Osmanoglu 2013, Roles and rules.) Käyttövaltuushallinnan avulla käyttäjille taataan pääsy heidän rooliensa perusteella tarvittaviin resursseihin keskitetyn käyttäjähallinnan kautta (Osmanoglu 2013, Key considerations). Tämä vaatii lokitiedon keräämistä käyttäjien kirjautumisesta ja resurssien käytöstä. Lokitietoa kerätään mahdollisimman kattavasti. Tällöin voidaan kiistämättömästi osoittaa yksittäisen käyttäjän toimet ja mahdolliset väärinkäytökset tietoliikenneverkon resurssien käyttämisen osalta. (Osmanoglu 2013, Identity and access intelligence: a risk-based approach.) Lokitiedon auditointi on tehtävä säännöllisin väliajoin ongelmien ja mahdollisten väärinkäytösten tunnistamiseksi (Osmanoglu 2013, Enforcement).

2.4 Suorituskyvyn hallinta

Suorituskyvyn hallinnointi mahdollistaa tietoliikenneverkon toiminnan seuraamisen. Tietoliikenneverkon suorituskykyä tarkkaillaan palvelun laadun takaamiseksi. Seurattavia kohteita ovat muun muassa tietoliikennetilastot, resurssien saavutettavuus ja verkon tietoliikennepaketeille aiheutuneet viiveet. Tietoja kerätään verkon eri osien aktiivilaitteilta, joko suoraan laitteiden antamina tietona tai sijoittamalla erillinen keräävä ja analysoiva suorittava yksikkö verkon eri osiin. Analysointia suorittava yksikkö voi olla esimerkiksi sensorilaite, joka kerää tarvittavat tiedot ja suorittaa analyysin tai aktiivilaitteeseen sijoitettava ohjelmisto. Usein aktiivilaitteista itsestään löytyy mahdollisuus saada tilastotietoa sen kautta liikkuvasta datasta. Tietoliikenneverkon suorituskykyyn liittyvät tiedot ovat tärkeitä verkon kokonaistoiminnallisuuden kannalta sekä erilaisten häiriötilanteiden syitä etsittäessä. Kerättävä tilastotieto on hyödyksi myös tietoliikenneverkon tulevaisuuden muutoksia suunniteltaessa. Kerättävistä tiedoista voidaan muodostaa automaattisesti säännöllisiä raportteja verkonvalvonnan ja –hallinnan hyödynnettäväksi. Tyypillisesti tietoliikenneverkon suorituskyvystä säilytetään kattavasti historiatietoa mahdollista myöhempää käyttöä

varten. (Abeck ym. 2009, 17-19; Subramanian 2010, Network Operations and NOC.)

2.5 Turvallisuuden hallinta

Tietoliikenneverkon sekä sen resurssien käyttämisen turvallisuutta taataan organisaatiolle tärkeän tiedon suojaamiseksi. Käsiteltävä tieto, tietoliikenneverkon laitteet ja niiden väliset yhteydet suojataan luottamuksellisuuden ja eheyden takaamiseksi. Saatavuutta edistetään verkonvalvonnan ja –hallinnan muilla osa-alueilla. Organisaatiossa tieto luokitellaan vähintään kahdenlaiseksi tiedoksi: julkiseksi ja salaiseksi. Salaiseksi luokitellaan tieto, josta voi olla organisaation toiminnalle merkittävää haittaa sen paljastuttua. Merkittävä haitta on esimerkiksi liiketoiminnalle aiheutuva haitta, jonka tieto paljastuttuaan aiheuttaa. Mikäli kyse on julkishallinnon organisaatiosta, tietoa luokitellaan neljään eri tasoon. Nämä tasot ovat: suojaustaso I-IV (Tietoturvallisuusasetus 681/2010). Julkishallinnon tietoliikenneverkon turvallisuustason määrittelee järjestelmissä käsiteltävän tiedon suojausluokitus (Puolustusministeriö 2015).

Tietoliikenneverkon turvallisuuden hallinnointiin kuuluu:

- Uhka-arvion tekeminen
- Turvallisuuspolitiikan luominen ja käyttöönotto
- Käyttäjähallinnan ja pääsynvalvonnan järjestelyt
- Luottamuksellisuuden ja eheyden takaaminen
- Turvallisuuden seuranta ja raportoiminen turvallisuustilanteesta

(Abeck ym. 2009, 17).

Turvallisuuden kehittämiseksi tietoliikenneverkon osalta tarvitaan uhkien tunnistamista uhka-arvion ja -analyysin kautta. Uhka-analyysin pohjalta tehdään riskien arviointia, jossa tarkastellaan mahdollisten uhkien toteutumista. Riskitason laskeminen hyväksyttäväksi tehdään riskianalyysin kautta. Tällöin selvitetään, mitä toimenpiteitä organisaatiossa tarvitaan turvallisuustason nostamiseksi. (Abeck ym. 2009, 21.) Esimerkiksi julkishallinnossa tietoliikenneverkkojen kyberturvallisuutta kehitetään KATAKRI:n (Kansallinen tietoturvallisuuden arviointikriteeristö) avulla. KATAKRI keskittyy tiedon luokittelun kautta antamaan vaatimukset turvaamiselle suojaustasokohtaisesti (Puolustusministeriö 2015, 3). Näitä vaatimuksia ei kuitenkaan tule käyttää suoraan esimerkiksi järjestelmäkehityksen tietoturvavaatimuksina, vaan ohjeina ja tarkastuslistoina. Myös tietoturvastandardeja on saatavilla, esimerkiksi ISO 27000 –standardikokonaisuus tuo tietoturvan hallintajärjestelmän organisaation käyttöön ja sertifiointiprosessin myötä tietoturvallisuuden tasoa voidaan nostaa organisaation koko toiminnan osalta. ISO 27000 –standardiperheen 27033 käsittelee tietoliikenneverkon turvallisuutta. (Harris & Maymi 2016, Security frameworks.) Mikäli haetaan ainoastaan tietoliikenneverkon turvallisuuden nostoa, ei kuitenkaan ole järkevää lähteä toteuttamaan vaativaa ja resursseja sitovaa sertifiointiprosessia. Standardointi on prosessina vaativa. Jos

organisaatiolla tai sen turvallisuudesta vastaavalla henkilöstöllä ei ole kokemusta, on syytä käyttää ulkopuolista konsultointiapua. KATAKRI puolestaan on järkevä valinta vastaamaan tietoliikenneverkon ja sen resurssien turvallisuuden kehittämiseen. Jatkuvuus- ja toipumissuunnittelua ei ole otettu käsiteltävässä OSI-mallin tietojenkäsittelyjärjestelmän hallinnoinnin viitekehyksessä huomioon. Jatkuvuus- ja toipumissuunnittelu ovat kuitenkin tärkeitä osa-alueita, jotka on otettava huomioon verkonvalvontaa ja –hallintaa suunniteltaessa. OSI:n mukainen viitekehys on yksinkertainen ja helposti ymmärrettävä, jossa osa-alueiden toiminnot voivat ikävä kyllä mennä ajoittain ristiin (Subramanian 2010, FCAPS: The ABCs of management).

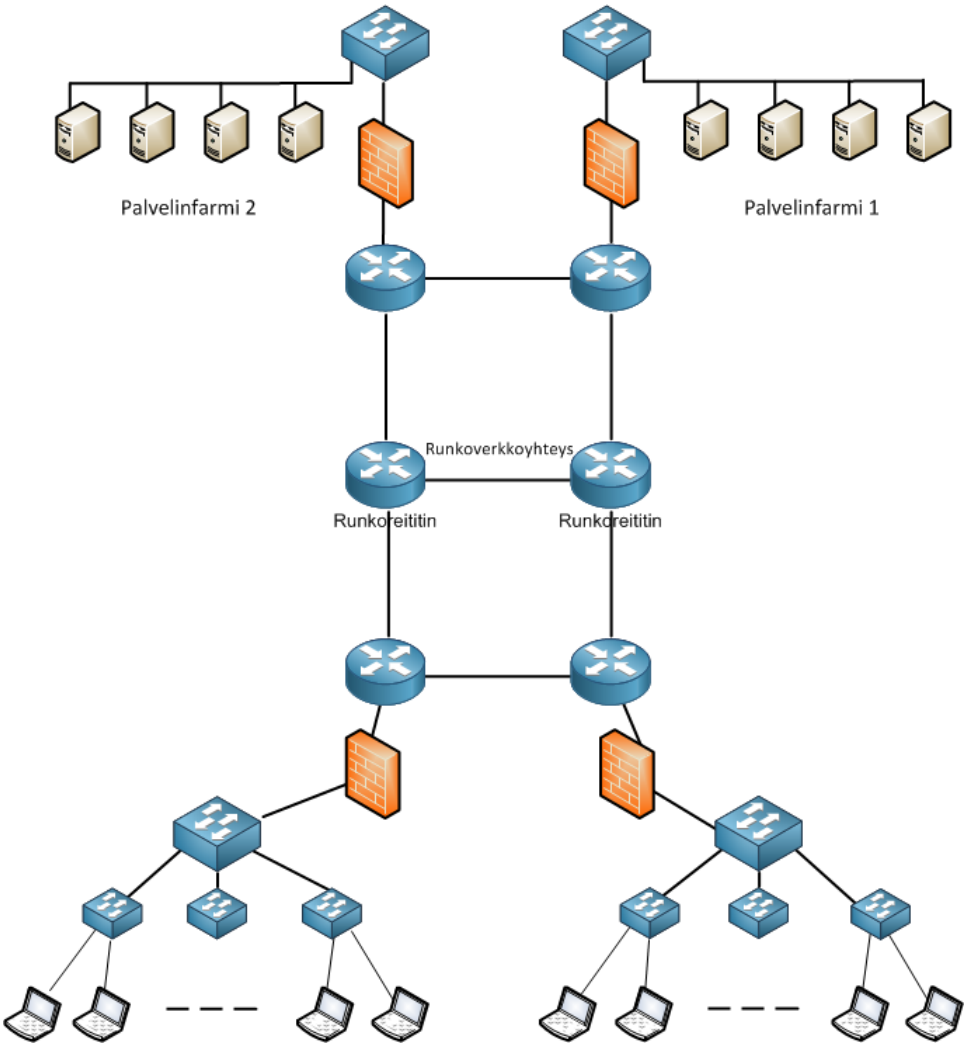
3 VERKON VALVONTA- JA HALLINTAJÄRJESTELMÄ

Tässä kappaleessa käsitellään verkon valvonta- ja hallintajärjestelmää kuvassa 1 kuvatun ja esimerkkinä toimivan tietoliikenneverkon kautta. Kuvassa 2 esimerkkiverkkoon on sijoitettu verkon valvonnan- ja hallinnan järjestelmän osat. Verkon valvonta- ja hallintajärjestelmällä kerätään tietoa aktiivisesti ja passiivisesti. Aktiivinen kerääminen on kiertokyselyin (pollaus) suoritettavia toimia tietoliikenneverkon aktiivilaitteilta ja tietoliikenteestä selvitettävää network flow -tyyppisen tiedon keräämistä. Passiivinen kerääminen tapahtuu SNMP-agentin toimittaessa tietoa tietoliikenneverkon aktiivilaitteelta palvelimen suuntaan, esimerkiksi SNMP TRAP -viestit.

Verkon valvomossa (NOC) tilannekuva visualisoidaan valvontaa suorittavalle henkilöstölle. Valvomon henkilöstöllä on usean eri tason tehtäviä, jolloin tehtävien mukaisesti tarvitaan myös eritasoisia näkymiä tilannekuvasta. Verkon valvonta- ja hallintajärjestelmä tarjoaa myös mahdollisuuden kerätyn tiedon syvempään tarkasteluun asiantuntijoille. Järjestelmästä voidaan ottaa myös automaattisia raportteja organisaation eri osille analysoituina toimitettavaksi. Verkon valvomosovelluksesta on näkymä konfiguraationhallintapalvelimen (CMDB) sisältöön, jolloin sen sisältämiä tietoja tietoliikenneverkon laitteista voidaan hyödyntää ongelmatilanteiden ja esimerkiksi päivitystarpeiden selvittelyssä. Tietoliikenneverkon ajantasainen dokumentaatio tallennetaan osaksi konfiguraationhallintapalvelimen sisältöä, tällä tavalla dokumentaatio on helposti hyödynnettävissä ongelmatilanteita ratkaistaessa sekä päivitettävissä muutoksenhallintatoimenpiteiden yhteydessä.

Verkon valvomossa käytetään tiketöintijärjestelmää, johon tuodaan valvontajärjestelmän (NMS) tuottamia automaattisia hälytystietoja ja kirjataan valvojan toimesta esimerkiksi käyttäjiltä saadut vikailmoitukset. Tiketöintijärjestelmä on siis osa NMS-järjestelmää ja se tarjoaa myös historiatiedon perusteella ratkaisuehdotuksia ilmenneisiin vika- ja hälytysilmoituksiin hallinnoinnin helpottamiseksi.

Verkon valvonnan ja hallinnan suunnittelun yhteydessä tulee selvittää reunaehdot perustettavalle valvontajärjestelmälle. Selvitetään muun muassa valvomon käyttöön tarvittavat tiedot tietoliikenneverkosta, valvonnan päivittäinen suoritustarve, suorituskykyvaatimukset tietoliikenneverkolle ja henkilöstötarve sekä organisaation osaan sijoitettavan henkilöstön osaamistarpeet.



Kuva 1. Esimerkkikuva tietoliikenneverkosta.

3.1 Tietoliikenneverkko

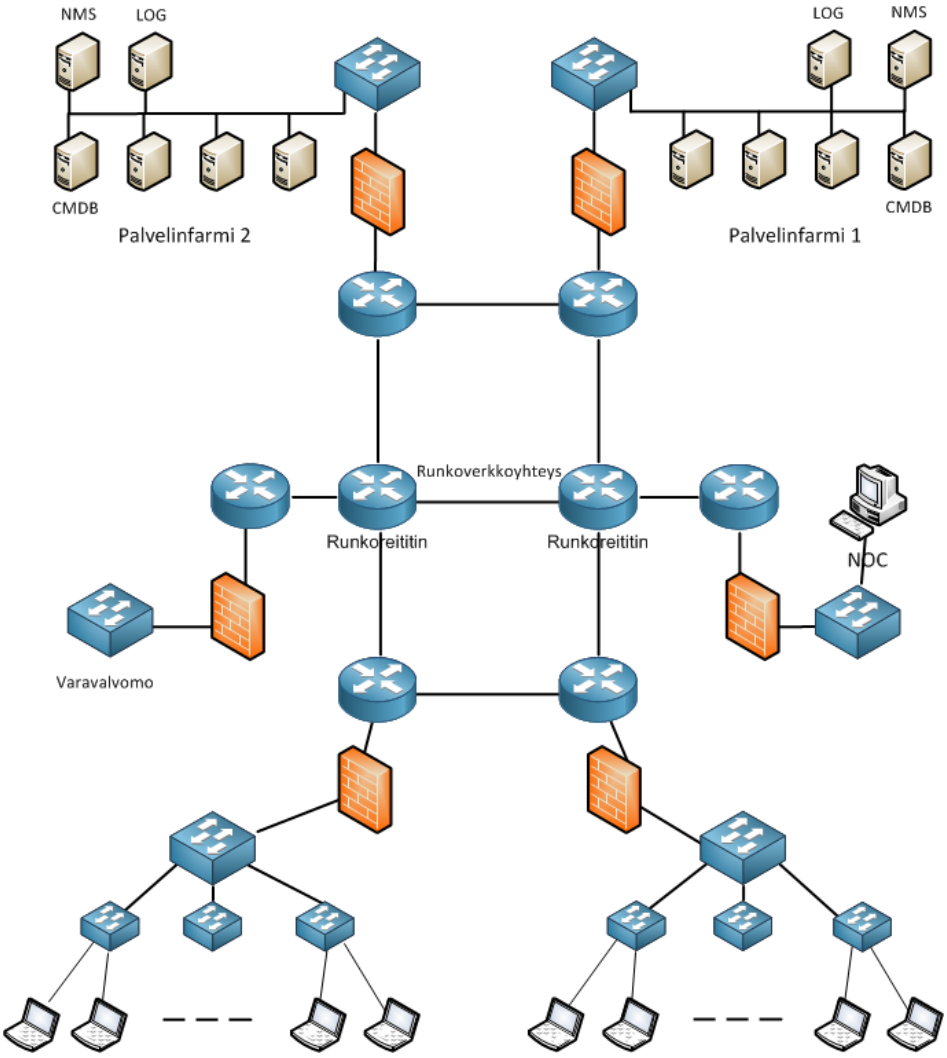
Kuvassa 1 on esitetty yksi esimerkki tietoliikenneverkosta ja myöhemmin työssä kuvataan verkon valvonta- ja hallintajärjestelmä sekä kybervalvontajärjestelmä. Kuvan 1 tietoliikenneverkoratkaisussa työasemien autentikoinnissa ei ole keskitettyä autentikointipalvelua, eli esimerkiksi active directory -tyyppistä käyttäjä- ja laitehallintaa.

Esimerkkinä käytettävä tietoliikenneverkko resursseineen on kuvitteellinen organisaation suljettu verkko, josta ei ole rajapintoja julkisiin verkkoihin. Palvelinfarmi 1 koostuu tietoliikenneverkon käyttäjille tarjotuista palveluista, näitä voivat olla esimerkiksi intranet (www-palvelin), tiedostopalvelin, sähköpostipalvelin (sisäinen sähköposti) ja nimipalvelin (DNS). Organisaatiolla voi olla käytössään myös esimerkiksi aikapalvelin, jonka avulla tuotetaan aktiivilaitteille, palvelimille ja työasemille tarvittavaa aikapalvelua. Suljetussa tietoliikenneverkossa aikapalvelu voidaan tuottaa esimerkiksi GPS-järjestelmän avulla (Wikipedia 2018b). Tällä tavalla saadaan tuotettua esimerkiksi verkonvalvontadataan liitettävillä aikaleimoilla

kaikkialla verkossa synkronoitu aikatieto, jolloin kerätyn tiedon luotettavuus kasvaa. Palvelinfarmi 2 toimii varajärjestelmänä, jossa sijaitseville palvelimille tiedot replikoidaan palvelinfarmista 1. Varajärjestelmänä käytetty palvelinfarmi 2 toimii siten, että mahdollisen yhteyskatkoksen tapahtuessa siirrytään automaattisesti käyttämään siellä sijaitsevia instansseja palveluista. Tämä tarkoittaa samalla sitä, että näin parannetaan varautumisen ja toipumisen nopeutta verkon resurssien osalta. Tällöin palvelinfarmissa 2 on oltava organisaation toinen aikapalvelin.

Kuvassa 1 merkityt runkoreitittimet esittävät nimensä mukaisesti organisaation tietoliikenneverkon runkoverkkoa. Kuvassa niitä on vain kaksi, mutta kuvan voidaan ymmärtää skaalautuvan runkoverkon osalta myös suuremmaksi, jolloin siihen kuuluvia reitittimiä olisi enemmän. Tällöin luonnollisesti myös lähiverkkojen määrä kasvaa kuvaan verrattuna. Runkoverkko rakennetaan tyypillisesti siten, että sillä kyetään vikasietoisuuteen esimerkiksi yhden reititinvälin yhteyden katketessa. Seuraava reititintasa on organisaation eri osien liityntäreititin, jolla organisaation maantieteellisesti eri sijainneissa olevat osat liitetään runkoverkkoon. Mikäli organisaation yksi alueellinen sijainti on laaja, voidaan rakentaa kuvan mukainen rakenne, jossa runkoverkkoon liitytään organisaation osan reunareitittimellä ja yhteydet lähiverkkojen välille varmennetaan. Kytkimet sijaitsevat tässä tapauksessa esimerkiksi rakennuksen talojakamossa, toimien runkokytkimenä, josta runkoverkon yhteyttä kyetään jakamaan rakennusten kerrosjakamoihin sijoitettuihin kytkimiin. Kerrosjakamoiden kytkimistä yhteys viedään työasemille tarkoitettuihin työpisterasioihin. Tyypillisesti nykyään kaapelointeja rakennettaessa ainoastaan yhteydet kerrosjakamoilta työpisterasioihin ovat kuparikaapeloinnein tehtyjä. Reitittimien väliset yhteydet rakennetaan valokuidulla. Rakenne perustuu eurooppalaiseen yleiskaapelointistandardiin, EN50173. (EN 50173-1/2011.)

Palomuureilla suodatetaan lähiverkkoon saapuvia ja sieltä lähteviä yhteyksiä. Palvelinfarmien yhteydessä sijaitsevilla palomuureilla voidaan tarvittaessa rajoittaa liikennöintiä, joka kohdistuu palvelimilta muualle kuin toiseen palvelinfarmiin. Näitä voivat olla esimerkiksi tarpeettomat yhteydenavauspyynnöt, mikäli palvelimen ei odoteta aloittavan yhteyksiä vaan ainoastaan vastaavan yhteyspyyntöihin. Palomuureilla voidaan suodattaa myös palvelimille kohdistuvia yhteydenavauspyyntöjä, jotka kohdistuisivat sellaisiin tietoliikenneportteihin, joita palvelimilla ei pitäisi olla käytössä. Reitittimillä voidaan tehdä tietoliikenteen suodatusta pääsylistojen (Access control list - ACL) avulla, jolloin voidaan estää verkossa esimerkiksi sinne kuulumattomien IP-osoitteiden reitittymistä sekä suodattaa ei-halutut protokollat tietoverkon liikenteestä. Reitittimiltä voidaan myös tuottaa network flow -tyyppistä tietoa verkon valvonnan ja hallinnan tarpeisiin.



Kuva 2. Verkon valvonnan ja hallinnan lisääminen tietoliikenneverkkoon.

3.2 Verkon hallinnan osakokonaisuudet

Yleisimpiä verkon valvonnassa ja hallinnassa käytettyjä dataformaatteja ovat CORBA, MIB ja XML. Verkon valvonnassa yleisimmän aseman protokollana on kuitenkin ottanut SNMP, sen strukturoitujen metodien vuoksi. (Abeck ym. 2009, 53.) Tästä syystä on luontevaa keskittyä MIB:n sisältöön, joka on yleisimmin käytetty dataformaatti SNMP-protokollan yhteydessä (Abeck ym. 2009, 35). MIB (Management information base) on standardoitu tapa esittää tietoja laitteen tilasta. MIB muodostuu tietokannasta, johon haluttuja laitteen tietoja kirjoitetaan kerättäväksi eteenpäin. MIB-tietokanta on siis tarkoitettu luettavaksi ja kirjoitettavaksi. MIB-tietokannan rakenne määritellään ISO:n ASN.1-standardin avulla. ASN.1:n alainen SMI-standardi (Structure of management information - SMI), joka on kuvattu RFC 2578:ssä kuvaa varsinaisen rakenteen. ASN.1 määrittelee myös koodausmahdollisuudet (Basic encoding rules – BER) siirtotielle siirrettävälle datalle. Tätä säännöstömahdollisuutta hyödyntämällä voidaan vaikuttaa muun muassa datan määrään siirtotiellä. (Clemm 2006, 38.) MIB -tietokanta muodostuu muuttujista eli olioista, joita voidaan osoittaa

tunnisteella (Object identifier – OID). Jokaisella oliolla on ennalta määritelty tietotyyppi ja käsittelyn yhteydessä olioon osoitetaan numerosarjalla, esimerkiksi 1.3.6.1.2.1.1.3, joka tarkoittaa järjestelmän ylläoloaikaa (SysUpTime). OID siis osoittaa muuttujan sijainnin MIB-tietokannassa. Verkon valvonnassa ja hallinnassa käytetään yleensä tietokannan osia Management- ja Privat-haarasta (Abeck ym. 2009, 37). Private-haaran alla olevaan Enterprises-haaraan tietokantaa laitevalmistajat saavat koostaa laitespesifisiä muuttujia. Yleisten tietokantahaarojen hallinta on tyypillisesti ongelmatonta. Laitevalmistajaspesifisten haarojen hallintaan tarvitaan hallintapalvelimelle tietokantaosa, joka on rakenteeltaan samanlainen kuin kyselyn kohteena olevassa laitteessa. (Abeck ym. 2009, 65.) Asia tulee tiedostaa laitehankintojen yhteydessä ja tiedot laitevalmistajakohtaisesta MIB -tietokantaosasta on selvitettävä valvonnan ja hallinnan onnistumiseksi.

SNMP-protokolla (Simple network management protocol) on verkon valvonnassa ja hallinnassa yleisin käytetty protokolla. OSI-mallissa tämä protokolla on tasolla 7, eli sovelluskerroksella. Protokollaa voidaan käyttää mekanismina MIB-tietokannan muuttujien lukemiseen ja kirjoittamiseen kohdelaitteella. Yleisimmin sitä käytetään UDP-protokollan avulla, mutta SNMP tukee myös TCP-protokollaa. UDP ei tilattomana protokollana varmista tietoliikennepakettien perille pääsyä TCP-protokollan tapaan. Mikäli tarvitaan tietoliikennepakettien perillepääsyn varmuutta, on käytettävä TCP-protokollaa tai rakennettava sovellustasolla kuittausmenettely UDP:llä saapuville tietoliikennepaketeille. SNMP on asiakas – palvelin -protokolla, jolloin esimerkiksi kiertokyselyä (pollaus) laitteille suorittava asiakassovellus (NMS) ottaa yhteyden hallittavan laitteen ohjelmistoon (SNMP -agentti) ja antaa sille pyyntöjä. Kyselyt kohdistetaan MIB -tietokantaan ja siellä sijaitseviin muuttujiin OID-identifioinnin mukaisesti luettaessa sieltä tietoja. Pyydetyt tiedot siirretään NMS -palvelimelle palvelinfarmiin. SNMP mahdollistaa MIB:ssä olevien muuttujien lukemisen joko yksitellen tai useampia tietoja kerralla. Kirjoittamismahdollisuutta voidaan käyttää esimerkiksi jonkin tietyn prosessin käynnistämiseen hallittavalla laitteella. Verkon valvontaan ja hallintaan liitetty laite voi lähettää tietoja automaattisesti esimerkiksi uudelleen käynnistymisestä tai jonkin raja-arvon ylittymisestä TRAP -viestillä NMS -palvelimelle. (Abeck ym. 2009, 40-41.) SNMP -protokollasta on olemassa kolme versiota, alkuperäinen versio kehitettiin 1980-luvulla. Kahdessa ensimmäisessä versiossa on merkittäviä turvallisuuspuutteita, joten käyttöön suositellaan ainoastaan viimeisintä, kolmatta versiota. (Abeck ym. 2009, 42.)

3.3 Verkon aktiivilaitteet

Tietoliikenneverkon aktiivilaitteilta tietoa kerättäessä on kyettävä selvittämään jo suunnitteluvaiheessa reaaliaikaisuuden tarve. Jatkuva tietojen kysely laitteilta voi aiheuttaa merkittävän kasvun liikenteeseen ja pahimmillaan se voi pienikapasiteettisilla yhteyksillä olla rajoittava tekijä varsinaiselle verkon hyötyliikenteelle. Suunnitteluvaiheessa tulisi pystyä

hahmottamaan esimerkiksi verkon tietoliikenteestä kerättävän datan osalta, missä hyödyllisimmät ja kattavimmat paikat keräämiselle sijaitsevat. Jokaiselta yhteysväliltä ei välttämättä tietoja kannata kerätä, vaan ainoastaan keskeisimmistä pisteistä. Asiakas – palvelin -malli ei ole paras mahdollinen keräämistapa network flow -tyyppisen tiedon keräämiseen sen luoman tietoliikennekuorman ja kohdelaitteen muodostuvan kuormituksen vuoksi. Tästä syystä aktiivilaitteissa, joista tietoliikenteeseen liittyvää tietoa kerätään, pitäisi pyrkiä keräämään tietoa paikallisesti ja toimittamaan ne palvelinfarmin lokipalvelimelle (LOG) syslog-muotoisena, tietyin väliajoin tai ennalta asetetun raja-arvon ylittyessä. (Abeck ym. 2009, 53, 80, 89, 109.) Pelkkää statistiikkatietoa voidaan kerätä MIB -tietokantaan, tällaista tietoa ovat muun muassa IP-pakettien määrä tietyllä verkkosovittimella tai siirretyn tiedon määrä byteinä (Abeck ym. 2009, 80). Statistiikkatietoa hyödyntämällä voidaan varautua muun muassa tulevaisuudessa tarvittavaan kapasiteetin lisäämiseen aktiivilaitteiden osalta.

Verkon aktiivilaitteet liitetään konfiguraatiotietokantaan (CMDB), jolloin verkon valvonnassa ja hallinnassa voidaan hyödyntää laitteisiin liittyvää tietoa ja tarvittaessa esimerkiksi palauttaa alkuperäinen konfiguraatiotiedosto laitteeseen sekä ohjelmistojen ja käyttöjärjestelmien päivitystarvetta selvitettäessä. Lokitietoa aktiivilaitteista kerätään muun muassa järjestelmävirheiden osalta. Järjestelmävirheistä laitteet voivat ilmoittaa automaattisella TRAP-viestillä NMS:lle, varsinainen lokitieto löytyy syslog -muodossa kerättynä ja valmiina analysoitavaksi erillisellä palvelinfarmiin 1 sijoitetulla lokipalvelimella (LOG).

3.4 Työasemat ja palvelimet

Tyypillisesti verkon valvontaa ja hallintaa ei uloteta työasemille saakka. Työasemilla olevat antivirusohjelmat voidaan ohjata kirjoittamaan tietonsa paikalliseen syslog-tietoon (Linux) tai event logiin (Windows), josta tieto siirretään muun tarpeellisen lokitiedon mukana palvelinfarmilla 1 sijaitsevalle lokipalvelimelle (LOG). Lokipalvelimelta tiedot ovat hyödynnettävissä siihen käytettävillä analysointiohjelmilla (NMS).

Palvelimet voidaan ottaa verkon valvontaan mukaan, mikäli organisaatiossa halutaan sovellustason valvontatietoa palveluista. Tällöin palvelimien on toimittava SNMP-agentteina ja kerättävä tarvittavaa tietoa MIB-tietokantaan NMS:lle toimitettavaksi. Lokidataa kerätään valvonnan ja hallinnan tarpeiden mukaisesti lokipalvelimelle (LOG).

3.5 Verkon valvomo (NOC)

Verkon valvomoon tuotetaan näkymää NMS:llä kerätyn tiedon osalta. Näytöllä oleva informaatio voi koskea tietoliikenneverkon aktiivilaitteiden välisten yhteyksien toiminnasta, yksittäisten aktiivilaitteiden tietoja sekä hälytys- ja varoitustietoja. Valvomon toimintaan kulminoituu NMS-

järjestelmällä koostettujen tietojen esittäminen verkon valvonnan ja hallinnan onnistumiseksi. Ratkaisevassa asemassa on siis kerätty data, joka pyritään visualisoinnin avulla esittämään informaationa valvomossa toimivalle henkilöstölle. Kerättyyn dataan on pystyttävä kohdistamaan syvällisempää tarkastelua esimerkiksi vikatilanteissa asiantuntijoita varten. Tietotarpeita on siten useamman tasoisia, ei ainoastaan valvomopäivystäjän näkymän koostamista varten. (Abeck ym. 2009, 96.) NMS:n suorittamat kyselyt, niiden saamat vastaukset ja aktiivilaitteiden lähettämät TRAP-viestit tulisi kyetä salaamaan luottamuksellisuuden ja eheyden takaamiseksi (Abeck ym. 2009, 78).

Tiketöintijärjestelmä on merkittävä osa vikatilanteiden hallintaa. Kaikki ilmenneet ongelmat ja niiden ratkaisemiseksi suoritettavat toimenpiteet on kyettävä jäljittämään. Tiketöintijärjestelmään kerätystä tiedosta muodostetaan yhteenliittymiä ja niissä suoritetuista ratkaisuista tarjotaan vaihtoehtoja uusille ilmeneville vikatilanteille.

Verkon valvomoon järjestetään tarpeelliset yhteydet tietoliikenneverkon laitteiden konfiguroimiseksi, tämä voi tarkoittaa esimerkiksi selainyhteyttä (http) tai SSH -työkaluja konfiguroinnin suorittamiseksi turvallisina etäistuntoina, tällöin yhteydet salataan ja käyttäjät autentikoidaan turvallisuuden takaamiseksi. Etäyhteystarpeet otetaan huomioon tietoliikenneverkon ja aktiivilaitteiden suunnittelu- ja rakennusvaiheessa. Räätälöidyissä laite- ja ohjelmistoratkaisuissa tarpeet viedään mukaan vaatimusmäärittelyyn.

Tietoliikenneverkon suorituskyvyn takaamiseksi kerätään ajastettua tietoa suorituskykyvaatimusten kohtaamisesta ja tarvittaessa tehdään konfigurointitoimenpiteitä tietoliikenneverkon aktiivilaitteille niiden toiminnan mukauttamiseksi vallitsevaan tilanteeseen. Tietoliikenneverkon muutosten ja aktiivilaitteiden uusimisen yhteydessä huolehditaan konfiguraatiotietokannan ja kattavan dokumentaation ajantasaisuudesta. Konfiguraatiotietokannan sisältämän tiedon on pysyttävä eheänä ja ajantasaisena sen tärkeyden vuoksi. (Abeck ym. 2009, 78.) NMS ja konfiguraatiotietokanta on suojattava erottamalla ne esimerkiksi palomuurin avulla muusta verkosta, näin taataan kerättyjen tietojen eheyden säilyminen (Abeck ym. 2009, 84). Konfiguraatiotietokantaa hyödynnetään muun muassa päivitystarpeita selvitettäessä ja yksittäisten laitteistojen tietoja tarvittaessa. Aika ajoin NMS:llä saatavaa tietoa verifioidaan, tämä voidaan suorittaa esimerkiksi käyttämällä säännöllisesti tietoliikenneanalysaattoreita vertailutiedon saamiseksi kerätylle tiedolle (Abeck ym. 2009, 109).

3.6 Varautuminen ja toipuminen

Varavalvomon käyttöönottomahdollisuus on yksi varautumisen kulmakivistä. Mikäli joudutaan luopumaan varsinaisista valvomotiloista, otetaan varautumisessa huomioon valvomon sijoittamismahdollisuus maantieteellisesti eri paikkaan organisaatiossa. Mahdollinen siirtyminen suunnitellaan

varautumisen kokonaissuunnittelun yhteydessä, tämä otetaan huomioon myös erilaisia toimenpidelistoja tehtäessä, jolloin luodaan listat erilaisista toimenpiteistä siirron onnistumiseksi. Toimintojen onnistumiseksi ne vastuutetaan henkilökohtaisilla vastuilla, jolloin jokaisen organisaation osan jäsenen tulisi tietää tehtäväkenttänsä tarkasti. Siirtymisen toimintaa on syytä harjoitella säännöllisesti, jolloin mahdolliset ongelmakohdat paljastuvat ja suunnitelmia sekä toimenpidelistoja voidaan kehittää. Samalla voidaan todeta varavalvomon valmiusaste siirtymisen toteuttamiseksi.

Ongelmatilanteisiin varautuminen edellyttää ajantasaista dokumentaatiota tietoliikenneverkosta niin fyysisiltä osilta kuin loogisten verkkokuvienkin osalta. Konfiguraatiotietokantaan kerätään erilaisten skenaarioiden avulla esimerkiksi vaihtoehtoisia konfiguraatiotiedostosisältöjä runkoverkon reitittimien osalta, jolloin yhden tai useamman yhteysvälin katketessa voidaan tehdä tarvittavia reititysmuutoksia nopeasti. Samanlaista toimintatapamallia voidaan hyödyntää myös esimerkiksi varavalvomon käyttöönottotilanteessa. (Subramanian 2010, Network Operations and NOC.)

Palvelinfarmi on kahdennettu siten, että palvelinfarmi 1 toimii pääasiallisena palvelintilana. Palvelinfarmiin 2 replikoidaan tiedot palvelinfarmista 1, siirtyminen poikkeamatapahtuman yhteydessä palvelinfarmin 2 käyttöön tapahtuu automaattisesti. Varautumisessa voidaan hyödyntää myös tallennettavan tiedon erottamista varsinaisesta toiminnallisuutta suorittavasta palvelimesta. Erillinen tallennuspalvelimen tuominen NMS:n yhteyteen lisää toimintavarmuutta, jolloin rautaongelmien yhteydessä ei menetetä NMS:n tallentamaa tietoa yksittäisessä palvelinfarmissa.

4 KYBERVALVONTA

Moderni yhteiskunta perustuu digitaalisiin järjestelmiin. Vuosituhannen alussa tehdyn selvityksen mukaan jo tuolloin taltioidusta tiedosta 90 prosenttia oli digitaalisessa muodossa ja ainoastaan painettuna tuotetun tiedon osuus oli enää noin kolme promillea (Tilastokeskus 2002). Useat koko yhteiskuntaa palvelevista tietojärjestelmistä ovat vaikutukseltaan merkittäviä ja kokonaisjärjestelmien osiin vaikuttaminen realisoituu ilmiöinä myös fyysisessä maailmassa. Tästä huolimatta tällä hetkellä ei ole yhteisesti hyväksyttyä, laajasti käytettyä ja laitevalmistajia sitovaa kyber- tai tietoturvastandardia. Laitevalmistajia velvoittava, CE-merkintää sähkölaitteissa vastaava säätely tietoturvallisuusominaisuuksien osalta puuttuu kokonaan. Julkisuudessa käydään aika-ajoin voimakasta keskustelua kybersodankäynnistä. Säätelytilanne on samanlainen myös siihen liittyen. Osa suurvalloista on sisällyttänyt sodankäynnin doktriiniinsa toiminnan tietoliikenneverkoissa ja sen, että niiden kautta kohdistuvaan hyökkäykseen voidaan vastata perinteisen sodankäynnin keinoin. Perinteistä sodankäyntiä säätelee Geneven sopimus, mutta kybersodankäyntiä koskettava säännöstö puuttuu. (Carr 2011, The legal status of cyber warfare.) Useat NATO:n jäsenvaltioista ja rauhankumppanuusmaista ovat osallistuneet Tallinn Manual –prosessiin, jonka nykyinen, voimassa oleva tuotos on nimeltään ”Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations”. Kyseisessä asiakirjassa pyritään määrittelemään, kuinka tällä hetkellä voimassaolevia kansainvälisiä lakeja voidaan soveltaa kybertoimintaympäristöön.

Tietoliikenneverkoissa ja tietojärjestelmissä tarvitaan kybervalvontaa. Organisaatiolle ja sen tietoliikennejärjestelmän käyttäjille on taattava tietoliikenneverkon ja siellä käsiteltävän tiedon luottamuksellisuus, eheys ja saatavuus. Tietoliikenneverkkojen toimintaa uhkaavat useat tekijät. Rikolliset ja rikollisjärjestöt hakevat mittavaa rahallista hyötyä. Erilaisilla aatteellisilla ja löysästi toisiinsa sitoutuneilla ryhmittymillä voi olla omista lähtökohdistaan syy, jonka vuoksi yhteiseen vastustajaan kohdistetaan haitallisia toimia tietoliikenneverkoissa. Näiden lisäksi tunnistetaan valtiolliset tekijät, kuten eri valtioiden tiedustelupalvelut sekä sotilaalliset toimijat, kun kyseessä on esimerkiksi tietoliikenneverkon resursseihin tai niiden kautta vaikuttaminen kohteeseen. Vaikuttamisella tarkoitetaan kohdejärjestelmän luottamuksellisuuteen, eheyteen ja saatavuuteen vaikuttamista, esimerkiksi saattamalla se vikatilaan, tukkimalla tietoliikenneyhteydet suurella tietoliikennepakettien määrällä tai muuttamalla ja varastamalla tietoa tietoliikenneverkon laitteilta. Tietoliikenneverkon kautta fyysiseen maailmaan vaikuttaminen voi olla esimerkiksi yhteiskunnalle elintärkeisiin toimintoihin lamauttavalla tavalla kohdistuva toiminta. Yhteiskunnalle elintärkeitä toimintoja Suomessa ovat:

1. Valtion johtaminen
2. Kansainvälinen ja EU-toiminta

3. Puolustuskyky
4. Sisäinen turvallisuus
5. Talouden, infrastruktuuri ja huoltovarmuus
6. Väestön toimintakyky ja palvelut
7. Henkinen kriisinkestävyys

(Yhteiskunnan turvallisuusstrategia 2017, 14).

Jokaiseen näistä haitallisesti vaikuttamalla pystytään heikentämään yhteiskunnan toimintaa normaali- ja kriisitilanteissa. Fyysisesti tällaisia järjestelmiä on muun muassa teollisuudessa laaja kirjo, vanhimmat järjestelmistä voivat olla jopa 1980-luvulta. Osin järjestelmät ovat sellaisia, että fyysistä järjestelmää, esimerkiksi tehtaan liukuhihnaa, ohjataan ohjelmoitavalla logiikalla. Nykyään nämäkin ovat yleisesti liitettyinä moderniin tietoliikenneverkkoon ethernet-liitännällä, jolloin niiden toimintaan voidaan vaikuttaa haitallisesti tietoliikenneverkon kautta. Tämän vuoksi nekin tulisi liittää osaksi organisaatioiden turvallisuusvalvontaa.

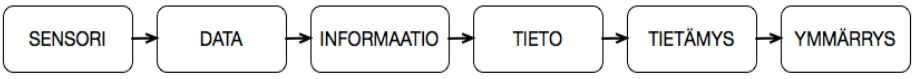
4.1 Kerättävästä datasta tilanneymmärrykseen

Tietoliikenneverkossa vaikuttamiseen on Lockheed-Martinin Cyber Kill Chain -mallin mukaisesti tunnistettavissa seitsemän eri vaihetta. Tiedustelulla (reconnaissance) pyritään löytämään mahdolliset kohteet, joihin vaikuttaminen on hyökkääjän tavoitteisiin pääsemiseksi edullisinta. Tiedusteluvaiheessa pyritään kohteiden lisäksi kartoittamaan hyödyntämiskelpoisia haavoittuvuuksia. Aseistamisen (weaponization) vaiheessa kehitetään valitun haavoittuvuuden hyödyntämiseen tarvittavat työkalut, esimerkiksi kohdistettu haittaohjelma. Valmistettu haittaohjelma toimitetaan valituilla keinoilla kohdejärjestelmään jakeluvaiheessa (delivery), esimerkiksi ulkoista muistilaitetta käyttäen. Hyväksikäyttövaiheessa (exploitation) haittaohjelma käynnistetään kohdejärjestelmässä ja hyödynnetään valittua haavoittuvuutta. Käynnistäminen tapahtuu joko hyökkääjän toimin tai kohdeorganisaation työntekijää käyttäen. Mikäli käytössä on esimerkiksi troijalainen, joka asentaa hyötykuormanaan tulleen etähallintaohjelman (Remote Access Tool – RAT) päästään seuraavaan vaiheeseen, joka on kontrollivaihe (command and control). Tällöin etähallintaohjelma ilmoittautuu internetiin sijoitetulle kontrollipalvelimelle, saadakseen toimintaohjeita ja ilmoittaakseen olemassaolostaan. Hyödyntämisvaiheessa (actions on objectives) kontrollipalvelimelta voidaan etäkäyttää haittaohjelman saastuttamaa työasemaa haluttujen toimintojen suorittamiseksi kohdeorganisaation tietoverkossa ja tarvittaessa tehdä toimia jalansijan ylläpitämiseksi kohdejärjestelmässä. (Hutchins, Cloppert & Amin 2011, 4-5.)

Cyber Kill Chainin tapainen toimintojen ketju on kyettävä tunnistamaan turvallisuusvalvonnan suunnittelussa ja pyrittävä kykyyn vastata vihamieliseen toimijaan koko toimiketjun läpi. Haitallisuuteen tähtäävä toiminta on pyrittävä mahdollisuuksien mukaan estämään jo sen alkuvaiheissa, minimoimalla hyökkäyspinta-alaa omien, turvallisuutta edistävien toimien avulla. (Hutchins ym. 2011, 6-7.) Näihin toimiin kuuluvat teknisten toimien

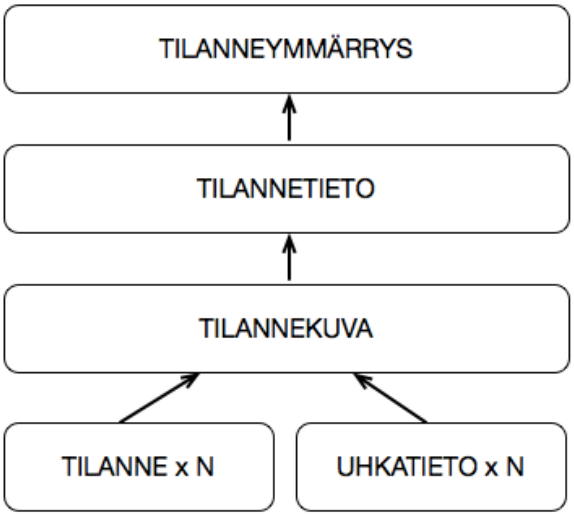
lisäksi luonnollisesti myös hallinnolliset toimet, kouluttaminen ja fyysisen turvallisuuden toimet. Uhka-arvion ja riskianalyysin perusteella pyritään kokonaisjärjestelmän osalta tilaan, jossa jäännösriski uhkien toteutumiselle on hyväksyttävällä tasolla. Tähän hyväksyttävään kokonaistilaan päästään kehittämällä suojaus- ja valvontaratkaisuja sekä organisaation toimintamalleja ja -prosesseja. Henkilöstön kouluttamisen avulla saadaan nostettua koko organisaation turvallisuustietoisuutta uhkiin varautumiseksi ja käyttäjien kykyä havaita haitallisia toimintoja käyttämissään tietojärjestelmissä ja työasemissa (Zimmerman 2014, 38).

Havaitakseen tietoliikenneverkkoon ja sen resursseihin kohdistuvan haitallisen toiminnan turvallisuusvalvontaa suorittavalla organisaation osalla on oltava tieto vallitsevasta tilanteesta. Tällöin puhutaan tilannetietoisuudesta (situational awareness). Tilannetietoisuuden takaamiseksi tarvitaan turvallisuuden valvontajärjestelmä, jonka avulla kerätään tietoa tapahtumista tietoliikenneverkossa ja kyetään visualisoimaan tiedon perusteella koottu informaatio valvontaa suorittavalle henkilöstölle. Tilannetietoisuuden kehittyminen kerättävästä lokidatasta tapahtuu seuraavaa tiedon arvoketjua hyödyntäen:



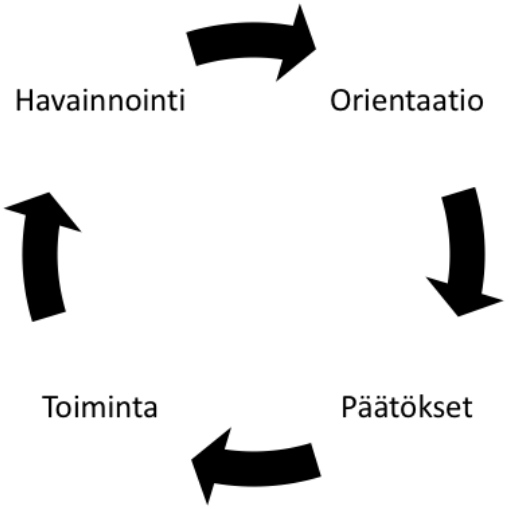
Kuva 3. Tiedon arvoketju.

Data voidaan ymmärtää tässä kontekstissa yksittäiseksi lokimerkinnäksi, joka on datan lähteen (sensori) tuottamia merkkejä tai bittejä. Data muuttuu informaatioksi, kun se saa hyödynnettävän merkityksen ja muuttuu tiedoksi. Tämä edellyttää automaattista prosessointia kerätyn datan osalta. Data toimitetaan tietosäilöön, jossa se yhdistetään kontekstiin. Tässä tapauksessa konteksti tarkoittaa turvallisuusvalvontaa kohdeympäristön rakenteessa. Työkaluohjelmistoilla, joilla on annetut käsittelysäännöt, jalostetaan tiettyyn tietoliikennejärjestelmän komponenttiin kohdistuvaa informaatiota. Näin data on muuttunut lopulta tiedoksi. Ihmisen käsitellessä tietoa oman kokemusperustansa mukaisesti, se jalostuu tietämykseksi. Kontekstiin liitettynä ihminen puolestaan jalostaa tietämyksensä ymmärrykseksi vallitsevasta tilanteesta muun muassa aiemmalla kokemusperustallaan. (Huotari 2005.) Tällä tavalla saavutetaan kontekstiin liittyvä tilannetietoisuus, joka siis johtaa tilanneymmärrykseen. Tehdäkseen oikeita päätöksiä turvallisuuden valvonnan antaman tiedon perusteella, turvallisuusvalvomon henkilöstön pitää saavuttaa tilannetietoisuuden lisäksi tilanneymmärrys.



Kuva 4. Tilanneymmärryksen kehittyminen.

Turvallisuuden takaaminen vaatii kykyä puuttua tietoliikennejärjestelmän turvallisuuspoikkeamiin, tämän vuoksi tarvitaan tietoa vallitsevasta tilanteesta. Tilannetiedon muodostaminen vaatii tietoliikennejärjestelmän turvallisuuden tilannekuvaa, jonka avulla pystytään tuottamaan tietoa päätöksien tekoa varten. Edellä esitetyn perusteella voidaan sanoa, että tilannekuva muodostuu havaittujen ja automaattisesti koostettujen yksittäisten tilanteiden joukosta sekä uhkatiedoista. Muodostuminen on esitetty kuvassa 4. Tilannekuvan muodostamiseen tarvitaan reaaliaikaista dataa tietoliikennejärjestelmän kaikkien komponenttien tapahtumista OSI-mallin sovelluskerrokselle saakka. Tätä voidaan kutsua jatkuvaksi valvonnaksi. Vaadittavan datan kerääminen, analysointi ja koostaminen ovat haasteita organisaatiolle. Lokitiedon kerääminen tietoliikennejärjestelmän komponenteilta voi organisaatiossa olla hyvinkin strukturoitua, mutta sen varsinainen hyödyntäminen voi jäädä tilanteeseen, jossa turvallisuuspoikkeama on jo ilmennyt ja tarvitaan forensiikkatietoa. (Zimmerman 2014, 38-40.) Olemassa olevia haavoittuvuuksia kartoitetaan haavoittuvuus- ja tunkeutumistestausten, verkkoskannausten ja auditointien avulla, tätä kutsutaan jaksottaiseksi valvonnaksi. Ennakoivan toiminnan takaamiseksi on kerättävä tietoliikennejärjestelmän komponenttien olemassa olevista haavoittuvuuksista sekä uhkatietoa organisaation ulkopuolisista lähteistä. Näitä ovat muun muassa haavoittuvuustiedotteet käyttöjärjestelmistä ja sovelluksista sekä tietoliikenneverkon komponenttien valmistajien tiedotteet laiteohjelmistojen ja rautakokoonpanojen osalta. Ulkopuolisia lähteitä ovat myös haittaohjelmiin liittyvät ilmoitukset, erityisesti nollapäivähaavoittuvuuksiin suunnatut haittaohjelmat. Mediasta tehtävä uutisseuranta voidaan lukea myös tähän kategoriaan. Kaiken kerätyn tiedon perusteella on kyettävä selvittämään havaitun uhkan tai turvallisuuspoikkeaman kohde, laajuus ja riskitaso. (Zimmerman 2014, 19-26.)



Kuva 5. Päätöksenteon OODA-silmukka.

Ilmenneisiin turvallisuuspoikkeamiin ja -uhkiin on kyettävä reagoimaan ja tekemään päätöksiä suojaamisesta sekä vastatoimista. Päätöksenteko tietoliikennejärjestelmän ja sen resurssien osalta voidaan luokitella kahteen eri osaan, manuaaliseen ja automaattiseen. Manuaalinen päätöksenteko tarkoittaa ihmisen muodostamaa tilanneymmärrystä saamansa tilannekuvan avulla ja sen perusteella suoritettavia toimia. Turvallisuuspoikkeamiin puuttumisen runkona pidetään usein John Boydin kehittämää OODA -silmukkaa (kuva 5). OODA jakautuu havainnointiin, saatuun tietoon orientoitumiseen eli analysointiin, päätöksentekoon ja vaadittaviin toimiin turvallisuusuhkaan tai -poikkeamaan puuttumiseksi (Ford 2010). Automaattinen päätöksenteko muodostuu tietoliikennejärjestelmän turvallisuuden mahdollisesti automatisoiduista osista, jolloin kyetään automaattisesti vaikuttamaan tietoliikennejärjestelmän osiin turvallisuuspoikkeamia havaittaessa. Teknisesti tarkasteltaessa turvallisuuspoikkeamiin puuttumista, voidaan toiminta jakaa kahteen eri tyyppiin, tunnisteisiin (signature based) ja epänormaaleihin (anomaly based) tapahtumiin perustuvaan. Tunnisteisiin perustuva toiminta tarvitsee säännöt, joita muodostetaan jo tunnettujen haitallisten toimintojen perusteella. Epänormaaleihin tapahtumiin perustuvassa toiminnassa tarkkaillaan tietoliikenneverkon ja sen resurssien muutoksia normaalitilanteeseen verrattuna, tällöin riittävät muutokset esimerkiksi normaalitilanteen verkkoliikenteessä voivat laukaista hälytyksen turvallisuusvalvomossa. (Zimmerman 2014, 35.)

4.2 Turvallisuusvalvonta ja päätöksenteko

Kybervalvontaa ja päätöksentekoa suorittavat organisaation osat voidaan jakaa viiteen erilaiseen kokoonpanoon, niiden muodostamisen perusteella:

- Turvallisuustiimi
- Sisäinen, hajautettu kokoonpano

- Sisäinen, yhtenäinen keskusmuotoinen kokoonpano
- Sisäinen, hybridikokoonpano
- Koordinoiva kokoonpano

(Zimmerman 2014, 15-16).

Turvallisuustiimin toiminnassa ei ole käytössä varsinaista valvomoa, vaan ongelmia havaittaessa tiimi kerätään organisaatiossa olevista osaajista. Tämä aiheuttaa viiveitä turvallisuuspoikkeamatapahtumien selvittelyssä, koska varsinainen ennakointi puuttuu ja ainoastaan reagoidaan havaittuihin ongelmiin. Formaalia käsittelytapaa turvallisuuspoikkeamiin ei ole, vaan ne käsitellään tapaus kerrallaan. (Zimmerman 2014, 15-16.)

Käytettäessä sisäistä, hajautettua kokoonpanoa turvallisuusvalvomo on olemassa. Toimissa käytettävä henkilöstö työskentelee pääosin kiinteän, vähäisen valvomohenkilöstön apuna, virallisten työtehtäviensä lisäksi. Turvallisuusvalvomossa on tällöin esimerkiksi ainoastaan valvoja, joka tarpeen ilmetessä pyrkii saamaan analyysiapua muilta organisaation osaajilta. (Zimmerman 2014, 16.)

Sisäisen, yhtenäisen keskusmuotoisen turvallisuusvalvomon etuna on kiinteästi sinne sijoitettu henkilöstö. Tällöin valvomossa on valvojan lisäksi jatkuvasti myös osaavaa analysointiin kykenevää henkilöstöä. Näin koostettu turvallisuusvalvonta kykenee tuottamaan valmiiksi analysoitua tilannekuvaa turvallisuudesta ja tuottamaan myös uhka-analyysia organisaation käyttöön. (Zimmerman 2014, 16.)

Hybridikokoonpanoisen turvallisuusvalvomon vahvuutena on kiinteän henkilöstön lisäksi mahdollisuus resurssien hetkelliseen käyttöönottoon organisaation muusta henkilöstöstä, esimerkiksi analysoinnin avuksi. Tällöin turvallisuuspoikkeaman analysointiin ja sen hoitamiseen voidaan ottaa esimerkiksi organisaation kärkiosaaja, jonka osaamisaluetta turvallisuuspoikkeama koskettaa. Tällainen toimintatapa soveltuu hyvin isoihin organisaatioihin, joiden turvallisuuspoikkeamien hallinnassa tarvitaan erityisen yksityiskohtaista osaamista tietyn tietoliikenneverkon resurssin osalta. (Zimmerman 2014, 16.)

Koordinoivan turvallisuustiimin kokoonpano mahdollistaa suurissa organisaatioissa ratkaisun, jossa on useita, esimerkiksi maantieteellisistä syistä muodostettuja erillisiä turvallisuusvalvomoita. Tällöin koordinoivan turvallisuustiimin tarve on saada kokonaistilannekuvaa organisaation turvallisuudesta ja alivalvomot hoitavat valvonnan ja poikkeamienhallinnan omalla vastuualueellaan. Koordinoivan turvallisuustiimin tehtävänä on tällöin toimia konsultoivassa roolissa alivalvomoiden havaitsemien poikkeamien ratkaisun apuna sekä koostaa kokonaistilannekuva ja -analyysi turvallisuustilanteesta. Koordinoivan turvallisuustiimin tehtäväksi jää myös uhka-analyysin suorittaminen koko organisaation osalta, ohjeistaa alivalvomoita ja jakaa uhkatietoa niille ennakoivan toiminnan mahdollistamiseksi. (Zimmerman 2014, 16.)

Organisaatioon perustettavalla tietoverkkojen turvallisuusvalvonnalla on oltava jonkin tasoinen toimivalta tehtäviensä suorittamiseksi. Mikäli turvallisuusvalvomolla ei ole riittävää toimivaltaa, vaan esimerkiksi ainoastaan turvallisuuspoikkeamia havaitseva rooli, on sen haettava lupa kaikkiin yksittäisten poikkeamien hallitsemiseen muualta organisaatiosta. Vaikutusvalta turvallisuuspoikkeamia havaittaessa voi olla myös jakautunutta, jolloin voidaan tehdä esityksiä tai suosituksia poikkeamanhallintaan vaadittavien toimien osalta. Turvallisuusvalvonnalla tulisi organisaatiossa olla tehtävissään täysi toimivalta, jolloin se voi selkeästi velvoittaa organisaation muita osia toimimaan yhteistyössä havaitun turvallisuuspoikkeaman tai -uhkan poistamiseksi. Täyden toimivallan omaavalla turvallisuusvalvonnalla päästään huomattavasti nopeampaan lopputulokseen turvallisuuspoikkeamiin reagoitaessa. Turvallisuusvalvonnan tehtävänä on tukea organisaation johdon päätöksentekoprosessia, tuottamalla sille analysoitua turvallisuustilannekuvaa. Tämä tarkoittaa samalla, että myös poikkeamanhallinnassa suoritettujen toimenpiteiden tulee tukea organisaation toimintaa. Tällöin poikkeamanhallinta ja toimenpiteet eivät voi olla liian aggressiivisia organisaation toiminnan kannalta, vaan tehtävillä toimenpiteillä on kuitenkin oltava yhteinen ymmärrys lopputuloksen kannalta. Turvallisuusvalvonnan toimenpiteet eivät siis saa estää tietoliikenneverkon käyttäjien työtehtävien suorittamista esimerkiksi siten, että merkittävän uhkan havaitessaan turvallisuusvalvonta eristäisi ilman lupaa tietyn verkon osan ohjelmistopäivitysten ajaksi. (Zimmerman 2014, 17.)

Vaikutusvalta voidaan jakaa myös turvallisuusvalvonnan mukaiseen kahtiajakoon turvallisuuspoikkeaman elinkaaren perusteella, näitä ovat reaktiiviset ja proaktiiviset toimet. Reaktiivisilla toimilla tarkoitetaan havaittujen ongelmien poistamista ja ennakoivilla toimilla havaittujen uhkien toteutumisen ehkäisyä. Reaktiivisissa toimissa turvallisuusvalvomon toiminnalla voi olla täysi toimivalta, jolloin esimerkiksi haittaohjelman saastuttama työasema tai koko lähiverkon haara voidaan eristää laajamittaisen leviämisen estämiseksi. Ennakoivien toimien, joita suoritetaan esimerkiksi saadun uhkatiedon perusteella, ei useinkaan ole sallittua rajoittaa tietoverkon resurssien käyttöä yhtä aggressiivisesti. Tällöin toimivaltaa voidaan joutua hakemaan ylemmältä taholta ja järjestelmien pääkäyttäjiltä organisaation sisällä, esitetyn tilannekuvan ja tilanneymmärrykseen perustuvan uhka-analyysin perusteella. Tähän liittyen turvallisuusvalvonnan organisaatiolla on oltava kyky selkeän tilanneraportin tuottamiselle organisaation käyttöön. (Zimmerman 2014, 17-18.)

Vaikutusvalta määrittelee turvallisuusvalvonnan organisaation kyvyn mukautua vastustajan päätöksentekoketjuun. OODA -silmukkaa nopeasti hyödyntävä vastustaja kykenee ketteriin muutoksiin hakiessaan mahdollisuuksia vaikuttaa vastustajan tietoliikennejärjestelmään ja sen resursseihin. Sisäinen, yhtenäinen tai hybridimuotoinen kokoonpano turvallisuusvalvonnan organisaatiolla sekä täysi toimivaltuus takaavat omalta osaltaan

nopeutta päätöksenteossa uhkaa tai haitallista toimintaa vastaan (Zimmerman 2014, 40).

4.3 Turvallisuusvalvonnan maturiteetti

Turvallisuusvalvonnan maturiteetilla tarkoitetaan sen kyvykkyyttä saavuttaa sille tavoitteissa asetetut vaatimukset. Annetut vaatimukset voidaan teknisestä näkökulmasta pilkkoa pieniin kokonaisuuksiin ja tehdä esimerkiksi matriisityyppinen asiakirja, jonka avulla selvitetään toiminnan teknistä kykyä valvoa tietoliikennejärjestelmää ja sen komponenttien toimintaa. Tämän avulla voidaan hahmottaa tekninen kyvykkyyden lisäksi toiminnallinen kyky tavoitteiden saavuttamiseen. (Zimmerman 2014, 81-82.)

Maturiteetti voidaan jakaa kyvykkyydeltään esimerkiksi neljään eri tasoon. Perustasolla turvallisuusvalvonnalla saadaan suoritettua osittainen tai perustoiminta. Edistyneellä tasolla kyky teknisesti ja toiminnallisesti on erittäin hyvä. Mahdollisella voidaan kuvata teknistä kykyä, joka vaatii osaavaa henkilöä kohdistetusti organisaation muusta osasta, esimerkiksi järjestelmäasiantuntijaa tulkitsemaan teknisellä tasalla tuotettua tietoa. Tämä tarkoittaa sitä, että teknisesti tieto saadaan mutta esimerkiksi turvallisuutta valvovan organisaation sisältä syvempi analyysikyky puuttuu. Ei suositeltavalla kuvataan toimintaa, jota ei pystytä hoitamaan teknisten tai muiden rajoitteiden vuoksi. Näitä voivat organisaatiossa olla esimerkiksi yksittäistyöasemat, joita ei niiden sisältämän tiedon arkaluonteisuuden vuoksi haluta kytkeä tietoliikenneverkkoon. Yksittäistyöasemien päivitykset ja lokitietojen kerääminen voidaan suorittaa esimerkiksi fyysisesti lähemmäksi sijoitetun toimijan kautta, yleensä toimenpiteet joudutaan harkitsemaan tapauskohtaisesti. Turvallisuutta valvovan organisaation osan työtä arvioivat toimet voivat myös kuulua tähän luokitukseen, esimerkiksi tunkeutumistestaus, joka tulisi kyetä havaitsemaan turvallisuusvalvonnassa. Testaus- ja auditointitoimet voidaan suorittaa esimerkiksi ostopalveluina ulkoisilta palveluntarjoajilta. (Zimmerman 2014, 81-82.)

Turvallisuusvalvonnan maturiteetin selvittäminen voidaan kytkeä myös organisaation tekniseen kehittämiseen sekä osaamisen kehittämiseen. Jokaisen tavoitteista johdetun yksittäisen kyvykkyysvaatimuksen osalta voidaan selvittää, kuinka se teknisesti hoidetaan sekä millaista osaamista siihen tarvitaan. Osaamisen vaatimukset voidaan verrata turvallisuusorganisaation henkilöstön osaamiseen ja tehdä suunnitelmia mahdollisen osaamisvajeen paikkaamiseksi.

4.4 Työkalut tilannekuvan saavuttamiseen

Työkalut, joilla tuotetaan tietoa kybervalvontajärjestelmälle voivat olla hyvinkin kalliita. Investoinneista huolimatta on muistettava, että käyttäjien itsensä suorittama valvonta ja kyberturvallisuustietoisuus on tärkeää. Tämän vuoksi organisaation henkilöstön kyberturvallisuustietoisuutta on

nostettava koulutusten ja kampanjoinnin avulla. Usein koulutus koetaan ylimääräiseksi kulueräksi organisaatioissa. Kun on kyse organisaation turvallisuudesta ja sen nostamisesta, koulutuksen panos - tuotto –suhde on kohdallaan, on sitten kyseessä käyttäjätason tai turvallisuusvalvonnan parissa työskentelevä henkilöstö. (Zimmerman 2014, 30.)

Kyberpoikkeamille tarvitaan verkonvalvonnan ja hallinnan kaltainen tiketöintijärjestelmä. Etenkin tietoliikenneverkon käyttäjiltä saadut ilmoitukset on nostettava tiketöintijärjestelmään vietäessä prioriteetiltaan korkealle, koska ilmoitettuja ongelmia on jo arvioitu käyttäjien omien toimien kautta tietoliikenneverkon osassa, jossa työntekijät työskentelevät (Zimmerman 2014, 29).

Kybervalvonnan onnistumiseksi on kerättävällä datalla ja sen analysoinnilla suuri merkitys. Kybervalvonta tarvitsee useita eri tekniikoita valvontadatan keräämiseen, koostamiseen, analysointiin ja lopulta esittämiseen oikeassa, ymmärrettävässä muodossa kybervalvomossa työskentelevälle henkilöstölle. Verkon valvonnan ja –hallinnan tuottaman valvontadatan täydentämiseksi tietoliikenneverkkoon voidaan asentaa myös erillisiä sensoreita. Verkosta tulee kyetä tunnistamaan sijainnit, joista saadaan mahdollisimman kattava kuva verkkoresursseihin kohdistuvasta liikenteestä. (Zimmerman 2014, 32.)

Tietoliikennetietojen ja verkon aktiivi- ja päätelaitteiden tietojen keräämisen tarve on kyettävä erottamaan. Tietoliikenneprofiilin selvittämisen lisäksi voidaan käyttää network flow -tyyppistä tietoa, päätelaitteiden käyttöjärjestelmien ja sovellusten toiminnoista puolestaan kerätään syslog-tyyppistä tietoa. Syslog-tietoa ei tulisi käyttää tietoliikennetiedon hankkimiseen ja analysointiin. Pikemminkin se tarjoaa mahdollisuuden selvittää yksittäisen laitteen tasalta tiedot toiminnoista, mikäli tietoliikenneprofiilin perusteella havaitaan epäjohdonmukaisuuksia tai poikkeuksia. (Trost 2009, Compare and contrast.) Kattavan turvallisuusvalvonnan tilannekuvan muodostamiseen tarvitaan

- Kokonaistietoliikennevirran tallenne (Full packet capture)
- Network flow -tieto
- Tietoliikenneprofiili (tilastollinen tieto)
- Tietoliikennepakettien otsikkotieto (protokollatasa)
- Lokitiedot (kattavasti koko verkon osalta)
- Hälytystiedot

(Sanders & Smith 2014, 45-46).

Kokonaistietoliikennevirralla tarkoitetaan kahden pisteen välisen tietoliikenteen pakettien tallentamista kokonaisuudessaan. Tämä vaatii suurta suoritus- ja tallennuskapasiteettia tallentavalta laitteelta, eikä sitä käytännössä kannata tehdä kuin tarpeen vaatiessa. Tarve tallentamiselle ja analysoinnille voi ilmetä turvallisuusvalvonnassa havaittujen poikkeamaepäilyjen vuoksi, tästä syystä tulisi mahdollisuudet tämän ajoittaiselle

suorittamiselle tulisi taata jo tietoliikenneverkkoja rakennettaessa ja turvallisuusvalvontaa perustettaessa. Tallennusta suunniteltaessa valitaan keskeiset paikat kattavan tietoliikennedatan saamiseksi. Tallentamisessa voidaan käyttää myös suodatussäännöstöjä, jolloin keskitytään esimerkiksi tietyn työaseman avaamiin yhteyksiin. Yleensä tätä tehdään, jos ilmenee tarvetta tarkastella tarkemmin tietyn työaseman avaamia yhteyksiä ja keskittyä pelkästään yhteen avattuun yhteyteen liittyvien tietoliikennepakettien sisältöjä. (Sanders & Smith 2014, 45.)

Network flow -tiedon keräämisellä tarkoitetaan kokonaistietoliikenteen sisällöstä yksittäisten tietoliikennepakettien sisältöä tutkimalla selvitettäviä

- Yhteyden aikaleima
- Tietoliikennevuon lähde- ja kohdeosoitteet
- Tietoliikennevuon lähde- ja kohdeporttiosoitteet
- Tietoliikennevuon käyttämä siirtoprotokolla ja sen tiedot (flags)
- Tietoliikennevuon pakettien määrä
- Tietoliikenneverkossa siirretty data (bytes)

(Trost 2009, Network flows and anomaly detection).

Tietoliikenneprofiililla tarkoitetaan kerätyn tiedon järjestämistä tilastollisesti, analysoimalla kerättyä tietoa ja tulkitsemalla sitä automaattisesti. Selkeät muutokset tilastoissa ja organisaatiossa tarpeettomien protokollien havaitseminen liikenteessä tarkastellaan tarkemmin, esimerkiksi manuaalisen analysoinnin avulla. Tietoliikennepakettien otsikkotiedoista voidaan kerätä protokollatasan tietoa, esimerkiksi http-protokollaan liittyvät GET- ja POST-komennot voivat olla kiinnostavia. Otsikkotietojen perusteella päätellään, millaisia komentoja tietoliikenneprotokollan sisällä suoritetaan ja mahdollisia uhkia analysoidaan sen perusteella. (Sanders & Smith 2014, 45.)

Lokitietoja kerätään, siirretään, seurataan ja suojataan suunnitelmallisesti. Tämän vuoksi käytetään lokitietojen keskitettyyn keräämiseen erillisiä palvelimia, joiden toimintaa valvotaan. Lokitietojen avulla voidaan kyetä turvallisuuspoikkeamien selvittämisessä muodostamaan koko tapahtumaketju sekä hyödyntää niitä uhkatiedon saamiseksi ja ennakoitujen toimien suorittamiseksi. Lokitietojen kattavalla keräämisellä voidaan varmistaa kiistämättömyyttä, todeta tapahtuman suorittaja ja kohde sekä toiminnan kokonaiskulku. Tietojen kerääminen on aikakriittistä toiminnan luotettavaksi selvittämiseksi, tämän vuoksi organisaatioissa käytetään keskitettyä aikapalvelua (NTP-palvelin). Lokitietojen keräämisen yhteydessä ne voidaan luokitella esimerkiksi seuraavalla tavalla:

- Käyttöloki
- Ylläpitoloki
- Muutosloki
- Virheloki

Lokitiedolla on myös elinkaari, joka alkaa lokitiedon muodostamisesta ja päättyy lokitiedon tuhoamiseen tai arkistointiin. (Valtionvarainministeriö 2009, 13-14.) Verkon valvonta ja -hallinta -luvun vikatilanteiden hallinnassa on kuvattu yleisimmin käytetyt protokollat. Lokitietojen toimittamisessa käytetään usein UDP-protokollaa, joka ei takaa tiedon perillepääsyä. Toimittamisvarmuuden takaamiseksi voidaan hyödyntää esimerkiksi vuonna 2008 Rainer Gerhardsin kehittämää RELP-protokollaa, joka toimii TCP -protokollan päällä. RELP on kehitetty alun perin rsyslog-ohjelman tueksi, mutta se on saavuttanut kohtuullisen kattavan aseman. Käyttöjärjestelmistä muun muassa Linux ja Windows saadaan eri työkaluohjelmien avulla tukemaan kyseistä protokollaa. Nykyisellä RELP-toteutuksella ei ole tukea TLS-protokollalle, jolloin siirrettävän lokitiedon salaaminen tietoliikenneyhteydelle vaatii muita toimenpiteitä. (Wikipedia 2018a.) Käytettäessä kaupallista versiota syslog-ng -ohjelmistosta lokien keräämiseen, on mahdollista hyödyntää patentoitua RLTP -protokollaa (Reliable Log Transfer Protocol). Tällä protokollalla on tuki myös TLS -salauksen käyttöön lokitiedon toimittamisessa. (Syslog-ng 2018.)

Hälytystieto tuotetaan tietoliikenneverkon aktiivilaitteissa, työasemissa, palvelimilla ja verkon valvonnan ja hallinnan järjestelmässä analysoidun lokidatan perusteella. Hälytystietoihin liitetään myös palomuurien, IDS-järjestelmien ja antivirus-ohjelmistojen hälytysdata. (Sanders & Smith 2014, 46.) Hälytystietojen liittäminen kerättävään kokonaislokitietoon voidaan tehdä aktiivilaitteilla, työasemassa ja palvelimessa kerättävän lokitiedon kautta tai siirtämällä ne suoraan lokipalvelimelle. Nykyiset antivirusohjelmat kykenevät kirjoittamaan lokitiedon suoraan syslog-muotoon, jolloin ne ovat ilman erillistä käsittelyä hyödynnettävissä (F-Secure 2017a, 6). Mikäli antivirusohjelmissa käytetään keskitettyä hallintaa, kerätty lokitieto voidaan viedä keskitetysti lokitietoihin (F-Secure 2017b, 40).

IDS (Intrusion detection system) on lyhenne, jolla tarkoitetaan tunkeutumisen havaintajärjestelmää tietoliikenneverkossa. Korkealla tasolla tämä voidaan jakaa tietoliikenneverkon tunkeutumisen havaitsemiseen (Network intrusion detection system – NIDS) ja työasemien tunkeutumisen havaitsemiseen (Host intrusion detection system – HIDS). IDS-järjestelmät pyrkivät havaitsemaan haitallista toimintaa analysoimalla tietoliikennesisältöä (NIDS) tai tapahtumia työasemassa (HIDS) ja antamaan niihin liittyviä hälytyksiä. Nykyisten antivirus-ohjelmistojen toiminnallisuudet ovat laajentuneet (Next generation antivirus – NGAV) siten, että useimmin niiden mukana asentuvat myös palomuuri- ja HIDS-toiminnallisuudet. HIDS-toimintoa käytetään työasemissa, palvelimilla ja muilla päätelaitteilla. NIDS-toiminto puolestaan sijoitetaan tietoliikenneverkossa sellaiseen solmupisteeseen, jossa sillä on mahdollisimman kattava tietoliikenteen massa analysoitavanaan.

IDS-toiminne voidaan jakaa kahteen toiminnallisuuden osalta eri tyyppiin. Poikkeuksiin ja epäsäännöllisyyksiin eli käyttäytymiseen perustuvaan tunnistamiseen (Anomaly-based intrusion detection), joka tarkkailee

tietoverkon liikennettä ja sen muutoksia. Tällöin tarvitaan selkeää vertailutietoa tietoverkon liikenteestä normaalitilassa ja pyritään tunnistamaan muutoksia, jotka voivat olla haitallisia. Esimerkiksi verkossa alkaa liikkua SMTP-protokollaa sisältäviä tietoliikennepaketteja huomattavasti tavallista enemmän tai esimerkiksi suuria määriä fragmentoituneita TCP/IP-paketteja. SMTP-protokollan tietoliikennepakettien määrä voi kertoa haittaohjelman leviämistoimenpiteistä ja TCP/IP -pakettien fragmentoituminen yrityksestä ohittaa palomuurilaitteen toiminallisuudet. Liikenteen tunnistaminen perustuu statistiikkaan, johon vaikuttaa verkon normaalitilanteen liikenne. Tämä toimintamalli tyypillisesti aiheuttaa joko liian paljon tai liian vähän hälytyksiä ja riippuu siitä, kuinka hyvin säätäminen kohdeverkkoon on onnistunut. Esimerkiksi network flow -tyyppistä tietoa käytettäessä otetaan näytetietoa verkosta IDS:n oppimiseen ja perustilanteen tiedon keräämiseen noin 30 päivän ajan. Tällöin verrattavaa dataa on kertynyt tarpeeksi tulevaisuuden tarpeisiin. (Trost 2009, Intrusion detection systems.) Tunnisteisiin perustuva toiminta hyödyntää aiemmin tunnistettuja toiminteita ja tietoliikenteen pakettisisältöjä. Tällöin toimintoja verrataan siis IDS-järjestelmään aiemmin luotuihin tunnisteisiin. Tämän toimintamallin vaatimuksena on tunnisteiden kattavuus ja järjestelmää voidaan sanoa yhtä hyväksi kuin sen tunnisteet ovat. Tunnistepohjainen IDS-järjestelmä kärsii selkeästi ajantasaisen tunnistetiedon välittämisen vaikeuksista. Tavallisesti nopeimmillaankin päivittyvät tunnisteet tulevat kolmesta neljään päivään esiintyneiden uhkien jäljessä. (Trost 2009, Network flows and anomaly detection.) Huonosti toteutettuna molemmat toimintamallit aiheuttavat tyypillisesti paljon vääriä positiivisia tai vääriä negatiivisia tunnistustapahtumia, joista edellä mainittu tarkoittaa suurta määrää vääriä hälytyksiä ja jäljemmän vuoksi hälytyksiä jää turvallisuusvalvonnan näkökulmasta saamatta (Trost 2009, Intrusion detection systems).

Network flow -tiedoissa tapahtuvien muutosten selvittämiseksi voidaan käyttää erillisiä sensoreita, nämä voivat olla erillislaitteita tai sovelluksia tietoliikenneverkon aktiivilaitteissa. Sensoreilla täydennetään IDS-järjestelmien antamaa tietoa turvallisuusvalvonnassa tarkkailemalla tietoliikenneyhteyksien sisältöä. Sensorien sijoittamisella on suuri merkitys niiden antaman informaation kannalta, väärä sijoittaminen voi esimerkiksi aiheuttaa tilanteen, jossa haitallisen liikennesisällön selvittäminen estyy esimerkiksi reitittimen antaman lähde- tai kohdeosoitteen vuoksi. Tällöin sensori on sijoitettu väärälle puolelle organisaation osan reunareititintä. (Sanders & Smith 2014, 61.)

Erillisten sensoreiden käyttämiseen on käytännössä kaksi mahdollisuutta, tietoa voidaan kerätä runkokytkimeltä tai sijoittamalla erillinen tietoa keräävä laite keskeiseen paikkaan tietoliikenneverkossa, joka on tyypillisesti verkon ulkoreunalla sijaitsevan palomuurin sisäverkon puolella. Käytettäessä tietoliikenneverkon aktiivilaitetta sensorina, voidaan kerättävää tietoa rikastaa edellä mainittujen lisäksi muun muassa verkkosovittimen tiedoilla. Network flow -tyyppistä tietoa kerätään useista paikoista, jolloin duplikaateilta ei voida välttyä. Tietosäilöön tietoja vietäessä on tehtävä

karsintaa duplikaattien osalta (deduplication). Tehtävän suorittaa joko keräävä sovellus tai tietoliikennevuon analyysiin käytettävä sovellus. Analyysia suorittava sovellus antaa arvokasta tietoa avatuista tietoliikenneyhteyksistä. Kerättäessä tietoja tietosäilöön, on huomioitava duplikaattien toimittamisen mahdollisesti aiheuttama kuormitus tietoliikenneverkolle sekä tietoliikennevuon analyysiin käytettävälle sovellukselle ja järjestelmälle. Network flow -tyyppisen tiedon käsittelyssä on ymmärrettävä, että kahden laitteen välinen interaktio on kaksisuuntaista (duplex). Tällöin sovellustasolla on siis kyettävä yhdistämään kaksi erisuuntaista tietoliikennevuota, jotka kuuluvat samaan ”keskusteluun”. Muussa tapauksessa kerättävät tiedot yksittäisenä tietoliikennevuona eivät anna todellista kuvaa kahden laitteen välisestä interaktiosta ja kokonaistieto avatun yhteyden osalta jää vajaaksi. (Trost 2009, Network flows and anomaly detection.) Tarvittaessa voidaan kerätä myös tietoliikennepakettien hyötydataa analysoitavaksi, yleensä se ei ole tarkoituksenmukaista suuren datamäärän ja tietoliikenneverkon kuormittumisen vuoksi. Saatujen tietojen perusteella tehtävillä jatkoselvityksillä voidaan tarkastella tietoliikenneverkon komponentin sisäistä lokitietoa.

SIEM -järjestelmissä nimitys tulee sanoista Security Incident and Event Management. Kirjallisuudessa nämä toisinaan erotetaan käsitteisiin SIM (Security Incident Management) ja SEM (Security Event Management). SIM-järjestelmänä voidaan ajatella keskitettyä lokienhallintaa ja lokien analyysin perusteella suoritettavien ilmoituksien tuottamista. SEM-järjestelmän toiminnan puolestaan reaaliaikaisen tilannekuvan ja ilmoitusten hallinnan. (Balaji 2017.)

SIEM-järjestelmä tarjoaa tyypillisesti toimintoina
- Kerätyn lokitiedon nopean analysoinnin
- Hälytysten luomisen
- Poikkeaman hallinan ja tiketöinnin
- Forensiikkatiedon muodostamisen analysoimalla lokitietoja
- Riippuvuussuhteiden löytämisen lokitiedoista
- Tietojen yhteen liittämisen ja duplikaattien poiston
- Raportoinnin, näkymät reaaliaikaiseen monitorointiin

(Johnson 2018, SIEM systems).

SIEM-järjestelmän käytössä olevalle lokipalvelimelle kerätään kattavasti tietoliikenneverkon aktiivilaitteiden lokitietoja sekä esimerkiksi network flow -tyyppistä tietoa analysoitavaksi. Käytännössä järjestelmä tarjoaa tietoa jokaiseen tietoliikenneverkon tapahtumaan liittyen. SIEM tarjoaa myös nopean keinon lokitiedon analysointiin riippuvuussuhteiden löytämisen avulla sekä hälytysten muodostamisen annettujen sääntöjen perusteella. Hälytysten perusteella voidaan suorittaa tapahtumaan liittyvien verkon aktiivilaitteiden tai työasemien lokitarkastelua forensiikkaan kuuluvina toimenpiteinä. Tyypillisesti SIEM-järjestelmään yhdistetään myös tietoliikenneverkkoon sijoitettujen IDS-järjestelmien antamat tiedot. Tärkeän

lokitiedon kattavuus koko tietoliikenneverkon osalta ratkaisee SIEM-järjestelmän konfiguroinnin lisäksi sen toiminnan laadun. (Balaji 2017.)

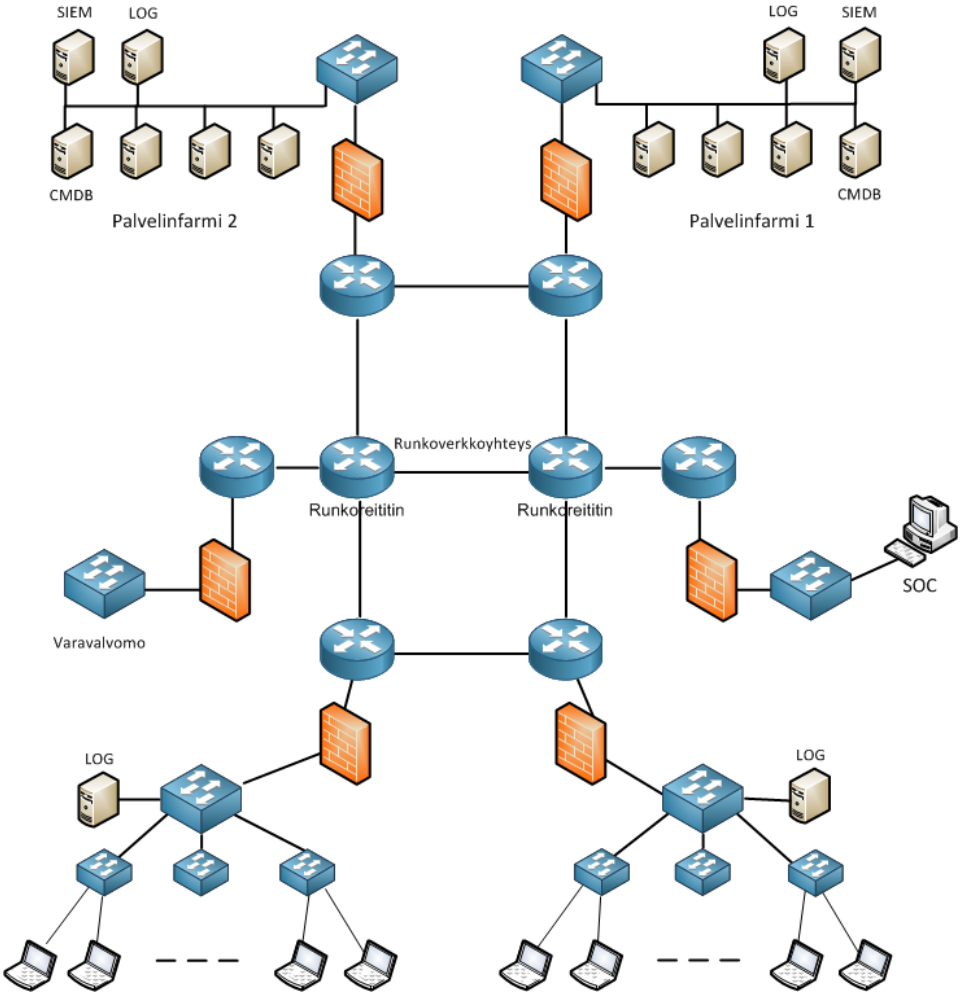
5 KYBERVALVONTAJÄRJESTELMÄ

Tietoliikenneverkon eriyttäminen on yksi mahdollinen ratkaisu verkon suojaamiseen. Yhtenä mahdollisuutena eriytettyihin tietoliikenneverkkoihin haitallisesti vaikuttamiseen tulevaisuudessa voivat olla älykkäät, oppivat haittaohjelmat. Tällaiset haittaohjelmat eivät tarvitsisi varsinaista kohdeverkon ulkopuolella olevaa komentopalvelinta, vaan tietoverkkoon toimittamisen jälkeen tarkkailisivat kohdejärjestelmää oppien sen erityispiirteet ja pyrkisivät tämän jälkeen erilaisiin haitallisiin toimiin. Tietoliikenneprofiilin tarkkailu voi olla yksi tällaisten haittaohjelmien toimista. Isäntäjärjestelmän tietoliikenneprofiilin perusteella haittaohjelma voi tehdä päätöksen verkossa käyttää verkossa isäntäjärjestelmän eniten käyttämää tietoliikenneprotokollaa leviämiseen tai sen keräämään tiedon saamiseksi ulos tietoverkosta. (Rid & McBurney 2012, 6-13.) Stuxnet-haittaohjelman paljastuminen Iranin uraanirikastamon ohjausjärjestelmästä vuonna 2010 osoitti, että julkisista verkoista eriytettyihin verkkoihinkin voidaan kohtuullisella vaivalla kohdistaa haitallisia toimia. Stuxnet oli yksi monista kohdistetuista haittaohjelmista, jotka kuuluivat samaan haittaohjelmaperheeseen, muita tähän kuuluvia olivat muun muassa Dugu, Flame ja Gauss –nimiset haittaohjelmat (IEEE 2013).

Kybervalvontajärjestelmä koostuu useasta eri osasta. Siihen voidaan käsittää kuuluvaksi tietoja analysoiva ja valvomossa tilannekuvaa esittävä SIEM-järjestelmä, lokipalvelin, erilliset sensorit ja IDS-järjestelmät sekä tietoliikenneverkon laitteet, jotka tuottavat valvonnassa tarvittavaa dataa. Kuvassa 6 esitetty kybervalvontajärjestelmä voidaan jakaa kolmeen eri osakokonaisuuteen, joita ovat datan kerääminen, analysointi sekä tilannekuvatiedon esittäminen ja raportointi.

Datan kerääminen tehdään verkon aktiivilaitteilla, työasemilla ja palvelimilla. Keräämisen jälkeen data toimitetaan ennalta määritetyssä muodossa lähiverkon lokipalvelimelle, josta se toimitetaan kuvassa 6 esitettyyn palvelinfarmi 1:n analysoitavaksi. Reititinten, palomuurien ja palvelinfarmiin sijoitettujen tietoliikenneverkon palveluita tuottavien palvelinten kerättävä data toimitetaan suoraan palvelinfarmi 1:ssä sijaitsevaan lokipalvelimeen. Tarvittaessa osalle datavirroista voidaan oikeaan muotoon parsiminen suorittaa vasta lokipalvelimella.

SIEM-järjestelmä analysoi palvelinfarmin 1 lokipalvelimelle kerättyä lokitietoa ja tuottaa tilannekuvaa kybervalvomoon (SOC). Kybertilannekuvasta voidaan muodostaa eritasoisia näkymiä organisaation käyttöön. SIEM-järjestelmästä saadaan tuotettua myös määrämuotoisia tilanneraportteja eri tarkoituksiin, esimerkiksi organisaation johdolle esitettäväksi.



Kuva 6. Tietoliikenneverkon turvallisuuden valvonnan ratkaisut.

5.1 Työasemat

Käyttöjärjestelmän tuottaman tavallisen lokitiedon lisäksi kerätään tietoa turvallisuuteen liittyvien tapahtumien osalta, näitä ovat muun muassa kirjautuminen työasemalle, järjestelmätiedostojen muutokset, konfiguraatiomuutokset, sovellusten asentaminen sekä tietoliikenneverkon palveluiden käyttäminen. Antivirus-ohjelmien loki- ja hälytystietojen kirjoittamiselle on kaksi mahdollisuutta, liittäminen suoraan koneen yleislokiin tai toimittaminen suoraan lähiverkon lokipalvelimelle (F-Secure 2017a & 2017b). Windows-työaseman event logista vietäessä lokitietoa palvelimelle, se muutetaan käytettävään syslog-tietomuotoon. Linux-työasemilla lokitiedot kirjoitetaan suoraan syslog-muotoon, jolloin muutoksia dataformaattiin ei tarvita lokipalvelimelle vietäessä. Tarvittaessa lokitietoa voidaan myös rikastaa tunnistamisen helpottamiseksi. Antivirus-ohjelmien myötä työasemille tulee useimmiten käyttöön myös HIDS-toimintoja, näiden tuottamat lokitiedot liitetään myös osaksi lokidataa. Työasemien lokitiedot toimitetaan lähiverkossa sijaitsevalle lokipalvelimelle (LOG). Lähiverkon lokipalvelimelta lokitiedot toimitetaan kokonaisuudessaan kuvassa 6 olevan palvelinfarmin 1 lokipalvelimelle SIEM-järjestelmän analysointia varten.

5.2 Aktiivilaitteet

Lähiverkossa sijaitsevalta lokipalvelimelta lähetettäessä tietoa palvelinfarmin 1 lokipalvelimelle, suoritetaan mahdollisten duplikaattien poisto (deduplication). Duplikaatit on kyettävä tunnistamaan palvelinfarmin 1 lokipalvelimella ja poistettava tarpeettomat. Samalla tietoa voidaan vielä rikastaa tai poistaa valvonnan kannalta turhia tietoja. Lähiverkon sisäisestä tietoliikenteestä kerätään tietoa runkoverkon kytkimeltä SPAN-portin avulla, suunnittelussa otetaan laskennallisesti huomioon kapasiteetin riittävyys. Laskelmissa otetaan huomioon keskimääräinen liikenteen määrä sekä maksimimäärä, joka ilmenee vuorokauden ajankohdista johtuen piikkeinä (Sanders & Smith 2014, 54-55). Hävikkiä voi aiheutua esimerkiksi suuresta liikennemäärästä tai kytkimen rakenteen huonosta laadusta johtuen. Lähiverkon kytkimeltä saatua tietoa analysoimalla voidaan havaita esimerkiksi haittaohjelman leviämisestä tai pyrkimyksestä ottaa yhteyttä komentopalvelimelle johtuvaa liikennettä. Tarvittaessa muutetaan lähiverkon palomuurin säännöstöjä vastaamaan tilannetta ja rajoitetaan liikennettä runkoverkkoon tai eristetään lähiverkko runkoverkosta kokonaan (leviämisen ehkäisy).

Palomuurien toiminnallisuutta tehostetaan IDS/IPS-toiminnoin, jolloin haitallista liikennettä havaittaessa voidaan myös automaattisesti muuttaa säännöstöä ja estää haitallinen liikenne. Palomuuri tuottaa lokitietoa, joka toimitetaan suoraan palvelinfarmin 1 lokipalvelimelle. Haluttaessa varautua kokonaistietoliikenteen tallentamiseen, runkokytkimiltä kerättävän tiedon lisäksi, voidaan jo ennalta sijoittaa palomuurien ja organisaation osien reunareitittimien väliin sensorit (TAP). Nämä voidaan aktivoida tarvittaessa suorittamaan kokonaistietovirran tallentamista, esimerkiksi runkokytkimiltä tallennettavassa tiedossa havaittujen puutteiden jälkeen. Vaihtoehtoisesti tätä tallentamista voidaan ajoittaa viikonaikoihin tai vuorokaudenaikoihin liittyen. Kytkimiltä kerättävä tieto toimitetaan lähiverkossa sijaitsevalle lokipalvelimelle. Reititinverkossa sijaitsevista runko- ja reunareitittimistä tiedot kerätään suoraan palvelinfarmissa 1 sijaitsevalle lokipalvelimelle. Reititinverkon reitittimissä voidaan tarvittaessa suorittaa kybervalvomosta otettavan etäyhteyden avulla kokonaistietoliikenteen tallentamista esimerkiksi tcpdump-komentoa käyttäen. Tällöin analyysi kerätystä datasta voidaan suorittaa manuaalisesti kybervalvomon asiantuntijan toimesta.

5.3 Lokitietojen kerääminen

Lähiverkoista kerättävä lokitieto toimitetaan sinne sijoitetulle lokipalvelimelle (LOG), josta tiedot välitetään (forwarding) palvelinfarmin 1 lokipalvelimelle (LOG). Näin kyetään tarvittaessa ottamaan käyttöön uusi SOC, joka valvoo ainoastaan ko. lähiverkkoa sekä kyetään vikatapauksissa suuntaamaan SIEM -järjestelmälle toimitettava data palvelinfarmiin 2. Palvelinfarmien palvelimet lähettävät lokitietonsa oletusarvoisesti suoraan palvelinfarmin 1 lokipalvelimelle.

5.4 Tietoliikenteen tietojen kerääminen

Reititinten network flow -tyyppinen tieto toimitetaan lokipalvelimelle, jossa se parsitaan syslog-muotoiseksi, rikastetaan tunnistetiedoilla ja tallennetaan hyödynnettävässä muodossa. Runkokytkimeltä kerätään SPAN-tyyppistä (Switched port analyser – SPAN) tietoa, eli peilataan tiettyyn porttiin kaikki kytkimen läpi kulkeva liikenne. Näin SIEM-järjestelmälle saadun tiedon avulla voidaan havaita esimerkiksi lähiverkossa tapahtuvan haittaohjelman leviämisen aiheuttama liikenne. Tämä ratkaisu voi kärsiä pakettihävikistä SPAN-portin läpäisykyvyn tullessa äärirajalle sekä kuormittaa kytkimen suoritustehoa merkittävästi. Vaihtoehtoisesti samaa tietoa voidaan kerätä esimerkiksi palomuureilta tai erillisiltä sensoreilta.

Palomuureilta on mahdollista kerätä TAP-tyyppistä tietoa (Test access point – TAP) ja toimittaa tietoliikenneyhteyksien tieto paikalliselle lokipalvelimelle. Useasta paikasta tietojen kerääminen aiheuttaa päällekkäisyyttä. Tietosäilöön vietäessä nämä duplikaatit tunnistetaan ja poistetaan sekä tarvittaessa yhdistetään kattavamman tiedon saamiseksi tietystä tietoliikennevuosta. Tarvittaessa tietoliikenneverkon keskeisiin osiin sijoitetaan sensoreita (TAP), jotka hoitavat tietoliikenneverkon tietyn osan tarkkailun muodostamalla statistiikkaa ja raportteja. Tietoa voidaan kerätä sensoreilta SNMP-protokollan avulla, konfiguraatiomuutoksilla kyetään tarvittaessa keräämään koko tietoliikennepakettivirta tallennettavaksi ja analysoitavaksi. (Trost 2009, Infrastructure monitoring.)

5.5 SIEM -järjestelmä

SIEM-järjestelmä toimii turvallisuusvalvonnan ytimenä palvelinfarmiin 1 sijoitetulla palvelimella (SIEM) Palvelinfarmi 1:n sijoitetulla erillisellä lokipalvelimella tasataan SIEM-järjestelmän kuormitusta, mahdollistamalla näin mahdollisimman paljon suorituskykyä analyysin suorittamiseen. Palvelinfarmin 1 SIEM-palvelimen tiedot replikoidaan vikatilanteiden varalta palvelinfarmin 2 SIEM-palvelimelle. Lokipalvelimet organisaation eri osien lähiverkoissa tuovat lokitietoa keräävän lisäkerroksen organisaation jokaiseen lähiverkkoon, tällöin taataan mahdollisimman viiveetön lokien kerääminen paikallisesti sekä koottu lokitiedon toimittaminen palvelinfarmissa 1 sijaitsevalle lokitiedon pääpalvelimelle. Yhteydet alipalvelimilta pääpalvelimille voidaan rakentaa esimerkiksi omaa vlan-ratkaisua käyttäen, jolloin runkoverkkoon liikennöitäessä lokipalvelimien liikenne erotetaan virtuaalisesti muusta tietoliikenneverkon liikenteestä. Ratkaisu mahdollistaa tulevaisuudessa myös paikallisen analyysikyvyn rakentamisen, jolloin SIEM-järjestelmälle voitaisiin välittää valmiiksi analysoitua lähiverkon turvallisuustilanteeseen liittyvää tietoa. Tällä ratkaisulla laajassa organisaatiossa mahdollistetaan myös alueellisen SIEM-järjestelmän käyttöönotto, mikäli tulevaisuudessa sellaiseen ilmenee tarvetta. Tämä tarkoittaisi siis myös alueellistettua ratkaisua turvallisuusvalvomon osalta, jolloin organisaation ylemmällä tasolla sijaitseva turvallisuusvalvomo saa uuden, koordinoivan roolin. Koordinoivassa roolissa toimivalle turvallisuusvalvomolle

välitetään tilannekuvaa, mutta varsinaisen turvallisuuden alueellinen johtaminen voidaan suorittaa alivalvomoissa. Päävalvomon tehtäväksi jää silloin esimerkiksi uhkatiedon välittäminen sekä kokonaistilannekuvan koostaminen ja raportoiminen organisaation turvallisuudesta. Tällöin päävalvomosta tarjotaan analyysiapua asiantuntijoiden muodossa alivalvomoille.

Työasemien turvallisuustilannetiedot kerätään SIEM-järjestelmään työaseman lokitiedoista, joihin liitetään myös antivirus-ohjelman hälytykset. Antivirus-ohjelmisto pyritään valitsemaan siten, että se sisältää HIDS-ominaisuudet. Tällöin SIEM-järjestelmälle saadaan kerättyä myös tunkeutumisenhavaintatiedot työasematasalta saakka. Työaseman HIDS-ominaisuudelta saadun tiedon jälkeen voidaan SIEM-järjestelmässä analysoida automaattisesti hälytyksen aiheuttanut toimenpide lokitiedoista ja ryhtyä välittömästi tarvittaviin toimenpiteisiin esimerkiksi eristämällä työasema tietoliikenneverkosta kokonaan.

SIEM-järjestelmään liitetään konfiguraationhallintapalvelin (CMDB), jolloin turvallisuusvalvonnassa kyetään hyödyntämään sen sisältämät tiedot. Tämä mahdollistaa esimerkiksi ulkoisena uhkatietona SIEM-järjestelmään liitetyn haavoittuvuustiedon tietyn sovelluksen version tai käyttöjärjestelmäversion osalta. Näin turvallisuustilannekuvassa voidaan esittää helposti organisaatioon kohdistuvan uhkan laajuus tämän nimenomaisen haavoittuvuustiedon osalta. CMDB:stä saadaan siis tässä tapauksessa tiedot kaikista työasemista organisaatiossa, jota tämä kyseinen uhkatieto koskettaa. CMDB:n tietojen ohella SIEM-järjestelmään liitetään myös ajantasaiset tietoliikenneverkon dokumentaatiot hyödynnettäväksi osana tilannekuvaa ja työkaluiksi poikkeamatilanteiden hallinnassa.

SIEM-järjestelmä mahdollistaa erilaiset näkymät eri tehtävien suorittajille turvallisuusvalvomossa, muun muassa tarkempaan manuaaliseen analysointiin tarvitaan yksityiskohtaisten lokitietojen koostamista tietoliikennejärjestelmän eri osista. Järjestelmällä mahdollistetaan myös poikkeamakohtainen forensiikkatiedon tallentaminen erillisiksi tiedostoiksi tiketöintijärjestelmään kirjattuun yksittäiseen poikkeamatapahtumaan. Tiketöintijärjestelmässä ratkaistuksi merkityt turvallisuuspoikkeamat tallennetaan tulevaisuuden käyttötarpeita varten, näitä tarpeita ovat muun muassa uudet samankaltaiset poikkeamat, joihin tarjotaan ratkaisuvaihtoehtoja aiemmin ratkaistuista poikkeamista.

5.6 Turvallisuusvalvomo (SOC)

Turvallisuusvalvomon käytössä tarvittava tilannekuva ja automatisoitu analyysikyky toteutetaan SIEM-järjestelmällä. Turvallisuusvalvonnassa tarvittava tiketöintijärjestelmä rakennetaan osaksi SIEM-järjestelmää, jolloin sen sisältämät tiedot ovat helposti käytettävissä ja kyetään tarjoamaan valvomohenkilökunnalle valmiita ratkaisuehdotuksia aiemmin ratkaistujen toimien perusteella. Turvallisuusvalvomo rakennetaan omana

organisaation osanaan ja sille tuotetaan tarvittavat tietoliikenneyhteydet palvelinfarmiin 1:n sijoitettuun SIEM-järjestelmään.

Turvallisuusvalvomolla on paras mahdollinen toimintakyky, jos sen kokoonpano on toteutettu kybervalvonta-kappaleessa kuvatulla hybridimallilla ja omaa täydet valtuudet toimintaansa. Turvallisuusvalvomo voi velvoittaa tietoliikennejärjestelmän osan päivityksen tehtäväksi verkon valvontaan ja hallintaan liittyvänä hätätyönä, saatuaan tietyn ohjelmisto- tai käyttöjärjestelmäversion osalta uhkatiedon haavoittuvuudesta. (Zimmerman 2014, 16-17.) Turvallisuusvalvomo tarvitsee tällaisiin tapauksiin liittyen lukuoikeuden CMDB:n sisältämiin tietoihin SIEM-järjestelmän kautta. Varsinaisia muokkausoikeuksia CMDB:n sisältöön turvallisuusvalvomo tai SIEM-järjestelmä ei tarvitse.

Turvallisuusvalvomon tehtäviin kuuluu ulkoisen uhkatiedon hankkiminen ja liittäminen SIEM-järjestelmään (Zimmerman 2014, 19). Tähän tehtävään turvallisuusvalvomo tarvitsee erillisyhteyden internetiin, yhteyttä ei ole esitetty kuvassa 6. Organisaatiota koskettavat uhkat raportoidaan analysoituna tietona ja tiedotetaan tarpeellisille toimijoille organisaatiorakenteessa (Zimmerman 2014, 19). Valvomon päivystäjän toimesta kirjataan käyttäjien ilmoittamat poikkeamahavainnot tiketöintijärjestelmään ja suoritetaan havaintojen priorisointi. Turvallisuusvalvomo mukauttaa SIEM-järjestelmän toiminnallisuudet vastaamaan oikeita turvallisuuspoikkeamia

5.7 Varautuminen ja toipuminen

Varautumisen suunnittelussa pyritään aina ennakointiin reagoinnin sijaan. Mahdollisuus siirtyä käyttämään varavalvomotiloja turvataan varautumisen ja toipumisen huolellisella suunnittelulla. Vika- tai hätäpoikkeustoiminnassa varaudutaan toipumiseen etukäteissuunnittelulla. Tehtyjä suunnitelmia harjoitellaan säännöllisesti erilaisten skenaarioiden avulla ja näiden kautta havaittuja suunnittelupuutteita täydennetään tarpeen mukaan. Skenaarioiden perusteella luodaan toiminnan onnistumiseksi toimenpidelistoja, joita seuraamalla pystytään varmistumaan onnistumisesta. (Yhteiskunnan turvallisuusstrategia 2017.)

Normaalien päivittäisten tehtävien lisäksi kybervalvomon henkilökunnalle annetaan työn tehtäväsisältöjen kautta vastuut varautumisen ja toipumisen suunnitteluun. Toteutuksen osalta säännöllinen harjoittelu varmistaa osaamisen tason. Harjoittelun avulla koko kybervalvontahenkilöstölle hahmottuu esimerkiksi toipumisen ja mahdollisen valvomon siirron vaatima aika. Verkon valvonnan ja hallinnan tapaan palvelinten varmuuskopiointi suoritetaan palvelinfarmista 1 palvelinfarmiin 2 reaaliaikaisena, jolloin katkokset esimerkiksi vikatapauksissa kyetään pitämään mahdollisimman lyhyinä.

Kybervalvonnan varautumisen ja toipumisen suunnitelmissa otetaan huomioon sen toiminnan kannalta kaikkein pahinkin vaihtoehto: valvonnan

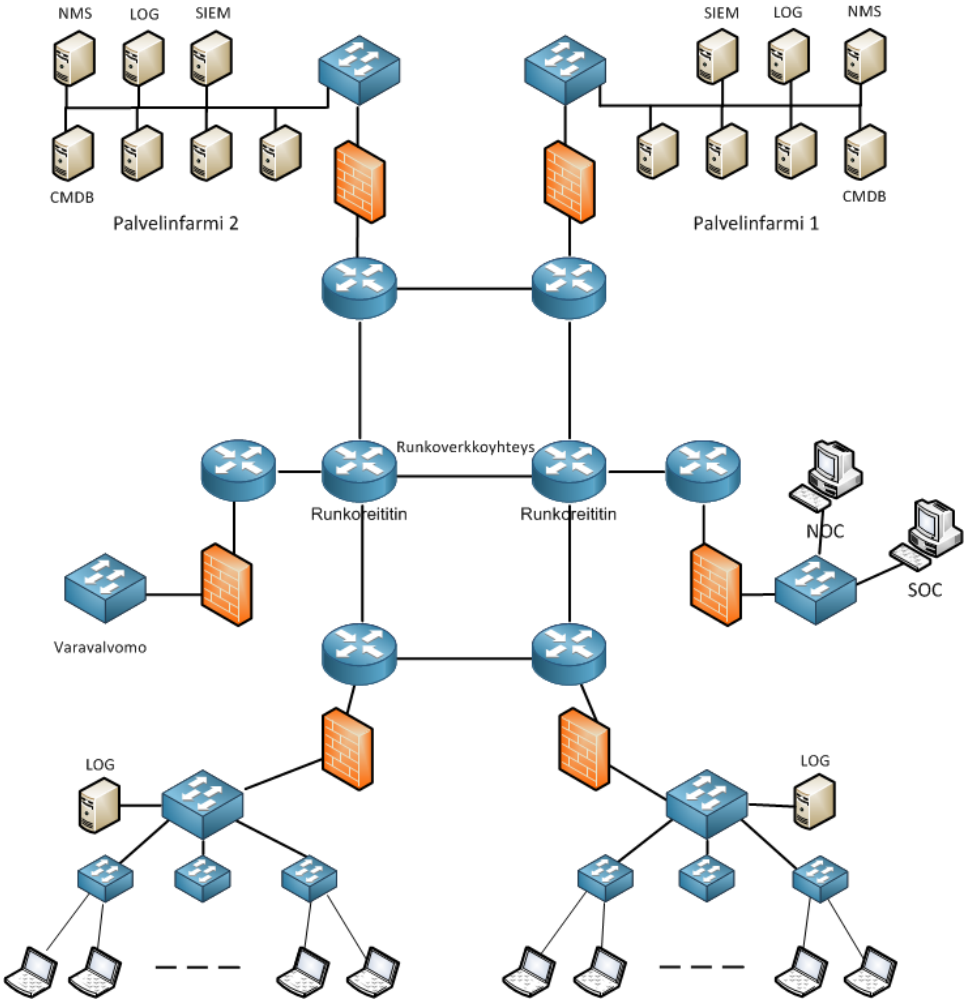
kannalta oleellisimpaan järjestelmään eli SIEM-järjestelmään on tunkeuduttu tai kyetty saastuttamaan haittaohjelman avulla. Suunnitelmiin sisällytetään myös toimet, jotka aloitetaan havaittaessa ongelmia analysoitavan lokitiedon eheydessä tai luottamuksellisuudessa.

6 VAKIOITUJEN VERKON VALVONTA- JA HALLINTAMENETELMIEN JA -TEKNIIKOIDEN HYÖDYNTÄMINEN KYBERVALVONNASSA

Verkon valvonnan ja hallinnan toimet valvomotasalla voidaan käsittää monella tapaa samantyyliseksi kuin kybervalvontaa suorittavassa valvomossa. Molempien vastuulla on tunnistaa, priorisoida, analysoida ja ratkoa ongelmia sekä raportoida tilannetietoa organisaation eri osille. Molemmille toimijoille on selkeä tarve organisaatiossa, lähestymistapa ongelmiin on kuitenkin erilainen. Henkilöstön osaamisalueet eroavat myös selkeästi toisistaan.

Perustavanlaatuisena erona voidaan nähdä ongelmien ja vaikutusten selkeä erilaisuus. Verkonvalvonnassa keskitytään käsittelemään tietoliikenneverkon ongelmatapahtumia ja valvontajärjestelmän tuottamia hälytyksiä. Voidaan käsittää, että verkonvalvonta keskittyy saatavuuden ja suorituskyvyn takaamiseen sekä erilaisten häiriötilojen purkamiseen ja keskeytysaikojen minimoimiseen. Kybervalvonnassa puolestaan keskitytään turvallisuuspoikkeamien havaitsemiseen sekä valvontajärjestelmän tuottamien hälytysten aiheuttajien tunnistamiseen ja poistamiseen. Kybervalvonnan tavoitteena on turvata tietoliikenneverkon resurssien luottamuksellisuutta, eheyttä ja saatavuutta, keskitytään siis turvallisuuden takaamiseen tietoliikenneverkon komponenttien sekä siirrettävän ja tallennettavan tiedon osalta. Tästä syystä esimerkiksi valvonnan yhdistämistä yhdeksi kokonaisuudeksi ei voida suositella. Yhteistyön on oltava saumatonta valvomoiden välillä. Tällöin valvomoiden on luontevaa sijaita erillisinä, mutta fyysisesti lähellä toisiaan, kuten kuvassa 7 esitetään.

Kybervalvonnassa voidaan tarvittaessa hyödyntää verkon valvonnan ja hallinnan asiantuntijoita manuaalisen analysoinnin avustamisessa. Yhtenä mahdollisuutena hyödyntää verkonvalvomoa on hätätyönä teetettävä työasemien tai tietoliikenneverkon aktiivilaitteiden päivittäminen, saatujen uhkatietojen perusteella. Laajuuden päivittämistarpeelle ja organisaation tietoliikenneverkkoon kohdistuvalle uhkalle tässä tapauksessa kybervalvomo saa tietää CMDB:stä, johon sillä on näkymä SIEM-järjestelmän kautta. Sama ajatusmalli toimii esimerkiksi analysoitaessa tietoliikenneverkon aktiivilaitteiden ajantasaisten konfiguraatiotiedostojen sisältöä, CMDB:ltä voidaan tehdä vertailu laitteen käyttämän konfiguraatiotiedoston ja palvelimella sijaitsevan tiedoston välillä. Tällä tavalla voidaan havaita esimerkiksi manipulointi aktiivilaitteen konfiguroinnissa, jonka jälkeen analysointi suunnataan kyseisen laitteen lokitietoihin tapahtumaketjun selvittämiseksi.



Kuva 7. Tietoliikenneverkon kokonaisvalvonta.

Kuvassa 7 nähdään esimerkkinä käytetty tietoliikenneverkko, johon on tuotu sekä verkon valvonnan ja hallinnan ja kybervalvonnan elementit mukaan. Verkon valvontaan ja hallintaan verrattuna kuvaan voidaan nähdä lisätyn lokipalvelimet lähiverkkoihin, SIEM-järjestelmä palvelinfarmiin (SIEM) sekä varsinainen kybervalvomo (SOC).

Lokitiedot sekä tietoliikenteestä kerätyt tiedot voidaan luontevasti sijoittaa samoihin lokipalvelimiin molempien toimijoiden osalta, tällä tavalla kerätty data on käytettävissä analysointiin kummankin toimijan tarpeiden mukaisesti. Näistä erityisesti tietoliikenneprofiili- ja network flow -tiedot soveltuvat molempien käyttöön. Lokipalvelimille tallennettava data muunnetaan syslog-muotoon sen yhtenäistämiseksi. Näin taataan tiedon kattavuus SIEM-järjestelmän käyttöön. Lokipalvelimille sijoitettua dataa käsitellään ainoastaan valvontajärjestelmissä (NMS ja SIEM), jolloin se säilyy muuttumattomana varsinaisessa tietosäilössään. Tallennettava tieto rikastetaan tunnisteiden osalta tarvittavalla tavalla, molempien toimijoiden hyötykäytön takaamiseksi. Lokipalvelimien sisältämä tieto säilytetään organisaation lokipolitiikan mukaisesti tietyn aikaa suoraan hyödynnettävässä muodossa. Tämän ajan jälkeen lokitiedot arkistoidaan siten, että sen palauttaminen analysoitavaksi on tarvittaessa mahdollista. Organisaation

lokipolitiikka määrittää myös arkistoidun lokitiedon lopullisen tuhoamisajankohdan. Lokipalvelimilla nämä toimet rakennetaan suoritettavaksi automatisoidusti.

Lokipalvelimia suunniteltaessa otetaan huomioon relaatiotietokantaohjelmistojen ja palvelinten turvallisuus eheyden ja luottamuksellisuuden takaamiseksi. Organisaatiossa on tiedostettava, että lokitiedon luominen, siirtäminen ja tallentaminen on molempien valvomoiden kannalta tärkeää. Mikäli analysoitavaan lokidataan tai osaan siitä ei voida luottaa, valvomot eivät voi toteuttaa tehtäväänsä uskottavasti. Tästä syystä koko lokitiedon elinkaari on kyettävä turvaamaan riittävällä tavalla. Relaatiotietokantaohjelmistoissa eheyden takaaminen on yksi sen päätehtävistä, taustalla piilee kuitenkin mahdollisuus ongelmiin valvonnan kannalta. Tallennettujen tietojen eheyden lisäksi analysoinnissa on kyettävä tehokkuuteen, suorituskykyisyyteen. Suuren organisaation tietoliikenneverkosta kerättynä lokitietomäärä voi olla kokonaiskooltaan massiivinen, jolloin analysointitoimet vaativat tietokantaohjelmistolta vakaata ja korkeaa suorituskykyä. Tämä on tehtävä, jossa relaatiotietokannat eivät ole kaikkein paras ratkaisu. Relaatiotietokannat on suunniteltu pääasiallisesti muuttuvaa tietosisältöä varten. Tyypillisesti lokitieto ei muutu sen luomisen ja tietosäilöön siirtämisen yhteydessä tehtyjen toimien jälkeen. Lokitieto siis on staattista tietoa tietosäilöön tallentamisen jälkeen. Relaatiotietokantaohjelmistojen kysely- ja lisäystoimet aiheuttavat resurssien käytön kautta viiveitä tietokannan käsittelyyn analysointiohjelmistojen näkökulmasta. Organisaatioissa tulisi vaatimusmäärittelyiden yhteydessä määritellä, käytetäänkö lokipalvelimen tallennusohjelmistona relaatiotietokantaa vai niin sanottua flat file -tyyppistä tiedon tallennustapaa. (Collins 2017, Getting data in one place.)

Kybervalvontajärjestelmä-luvussa kuvattiin lähiverkosta kerättävän lokidatan kerääminen paikalliselle lokipalvelimille ja mahdollisuus jakaa kybervalvonta alijakamoihin, samanlainen toiminta voidaan suunnitella tehtäväksi myös verkon valvonnalle ja hallinnalle. Toimintatapamuutoksen huomioiminen voidaan selittää ensisijaisesti ottamalla huomioon mahdollinen organisaation kasvu ja toissijaisesti varautumisen toimenpiteenä, jolloin voidaan jakaa valvonta pelkästään alueellisiin valvomoihin molempien toimijoiden osalta. Varautumisen ja toipumisen suunnittelua voidaan yhdistää valvomoiden osalta yleisestikin niiden samankaltaisuuksien vuoksi.

Tietoliikenneverkon dokumentaatio on molemmille valvontaa suorittaville organisaatioille tärkeää tietoa, tästä syystä on luontevaa yhdistää ajantasainen tieto molempien toimijoiden käyttöön. Ajantasaisen tietoliikenneverkon dokumentaation ylläpitopaikkana voidaan pitää esimerkiksi konfiguraationhallintapalvelinta (CMDB). Ylläpitovastuu dokumentaatiosta ja konfiguraationhallintapalvelimesta on verkon valvonnan ja hallinnan organisaatiolla, joka huolehtii päivityksistä osana muutoksenhallintaprosessiaan.

Erilaisten älykkäiden ratkaisuiden kehittyessä voidaan suunnitelmissa varautua kybervalvonnan ratkaisuiden kehittyvän siten, että analysointikykyä rakennetaan työasemiin sekä lähiverkkojen lokipalvelinten yhteyteen. Työasemilla automaattisesti tehtävä kattava turvallisuusanalyysi mahdollistaisi jatkossa merkittävän parannuksen lokitiedon vähenemisenä lähi- ja runkoverkon tietoliikenteessä. Ideaalitilanteessa pystytään luottamaan työasemassa tapahtuvaan turvallisuusanalyysiin ja poikkeustapahtuman yhteydessä lähetetään ainoastaan poikkeamakohtainen SNMP TRAP-viesti ongelman indikoimiseksi SIEM-järjestelmälle. Hälytyksen poikkeamatapahtumasta saatuaan SIEM-järjestelmä automaattisesti pyytää lisätiedot työasemasta poikkeamatapahtuman jatkoanalysoinnin tarpeiden mukaisesti. Toimintatapa mahdollistaa tällöin valvonnan myös pienikapasiteettisten tietoliikenneyhteyksien ylitse. Toinen vaihtoehto SIEM-järjestelmän analyysin tekemiselle jatkossa on sijoittaa lähiverkon lokipalvelimen (LOG) yhteyteen SIEM-alijärjestelmä, joka analysoi itsenäisesti lokitietoja lähiverkon osalta ja raportoi havainnoistaan SIEM-pääjärjestelmälle mahdollisimman minimaalisella tietoliikennekuormalla. Keinoälyn kehitysnäkymät tällä hetkellä voivat mahdollistaa tämän kaltaisia toimintamuutoksia jo lähitulevaisuudessa.

7 YHTEENVETO

Opinnäytetyössä tutkittiin mahdollisuuksia vakioitujen verkon valvonta- ja hallintamenetelmien hyödyntämiselle tietoliikenneverkkojen kybervalvonnassa. Työ tehtiin kirjallisuustutkimuksena ja siinä keskityttiin kahteen tutkimuskysymykseen. Ensimmäisenä haettiin perinteisen verkon valvonnan ja hallinnan tuottaman informaation hyödyntämismahdollisuuksia osana kybervalvontajärjestelmän analysoimaa tietomassaa. Tarkoituksena oli löytää kyberturvallisuuden tilannekuvaan, turvallisuuspoikkeamien ja -uhkien analysointiin soveltuvaa tietoa, jota kerätään verkon valvonta- ja hallintajärjestelmän (NMS) toimesta. Toisena tutkimuskysymyksenä selvitettiin, mitä muuta tietoa tietoliikenneverkosta ja sen komponenteista tarvitaan kyberturvallisuuden valvontajärjestelmään (SIEM), jotta organisaatiossa kyetään muodostamaan mahdollisimman kattava turvallisuuden tilannekuva.

Tutkimuksessa löydettiin tietolähteitä, jotka verkon valvonta- ja hallintajärjestelmän lisäksi soveltuvat hyvin myös kybervalvontajärjestelmän käyttöön. Näitä ovat muun muassa network flow -tyyppinen sekä tilastollinen informaatio tietoliikenteestä eli tietoliikenteestä muodostettu kokonaisprofiili. Verkon valvonnan ja hallinnan osana käytetään konfiguraationhallintapalvelinta (CMDB), jonka tiedot ovat tärkeitä esimerkiksi kybervalvonnassa muodostetun uhkatiedon analysoinnissa, organisaatioon kohdistuvan uhkatason selvittämiseksi. Tutkimus ehdottaa myös loki- ja tietoliikennetietojen yhdistämistä yhteiskäyttöiselle, keskitetylle palvelimelle, josta verkon valvonta- ja kybervalvontajärjestelmä suorittavat itsenäiset analyysinsä tietoliikenneverkon tilasta.

Lisäksi kybervalvonnassa tarvitaan kattavaa lokitietoa tietoliikenneverkon aktiivilaitteiden, työasemien ja palvelinten toiminnoista. Lokitietoa kerätään myös aktiivilaitteissa, työasemissa ja palvelimissa toimivien sovellusten toiminnoista. Työtä tehtäessä havaittiin, että kybervalvontaa suorittavan organisaation osan tulee olla keskusmuotoinen hybridimalli ja mahdollisuuksien mukaan omata täysi toimivalta suorittamiinsa tehtäviin. Tällä tavalla kyetään vastaamaan mahdollisimman ketterästi havaittuihin turvallisuusuhkiin ja -poikkeamiin. Ketteryys mahdollistaa kyvyn vastata vastustajan päätöksentekoketjuun, joka tyypillisesti noudattaa John Boydin kehittämää OODA-silmukkaa.

Kirjallisuustutkimuksena suoritettu tutkimus tulisi jatkossa todistaa rakentamalla esimerkkinä esitetty tietoliikenneverkkokokonaisuus. Tällä tavoin olisi mahdollista löytää puutteita tai rajoitteita esitetyille ratkaisuille, etsiä keinoja esiin nouseviin ongelmakohtiin ja löytää oikeat työkaluohjelmistot kybervalvonnan suorittamiseen.

Jatkotutkimuksena aihealueeseen liittyen tulisi tutkia tässä opinnäytetyössä lyhyesti pohditun keinoälyn hyödyntämismahdollisuuksia

valvontainformaation tuottamisketjun alkupäässä. Työasema- ja lähiverkkotasolle viety turvallisuuden analyysikyky voisi laskea merkittävästi tietoliikenneverkon kuormitusta, joka syntyy loki- ja tietoliikennetietojen toimittamisesta keskitettyyn palvelinratkaisuun analysoitavaksi. Toisena jatkotutkimusalueena voidaan esittää kybervalvonnan johtamiseen liittyvä aihe, jonka tutkimus kohdistuisi kybervalvonnan henkilöstön osaamistarpeiden tunnistamiseen. Tämän avulla muun muassa rekrytoinnissa voidaan keskittyä oikeiden osaajien tunnistamiseen sekä rekrytoinnin jälkeiseen osaamisen kehittämiseen.

LÄHDELUETTELO

Abeck, S., Bryskin, I., Evans, J., Farrel, A., Filsfils, C., Hegering, H-G., McCabe, J., Morrow, M., Nadeau, T., Neumair, B., Ramaswami, R., Sivarajan, K., Strassner, J. & Vijayanda K. (2009). *Network Management*. Burlington: Elsevier.

Balaji, N. (2017) SIEM a detailed explanation. Haettu 23.5.2018 osoitteesta https://gbhackers.com/security-information-and-event-management-siem-a-detailed-explanation/

Carr, J. (2011) *Inside cyber warfare, 2nd edition*. Sebastopol: O'Reilly Media.

Chuvakin, A., Schmidt, K., Phillips, C. (2012) *Logging and log management.* Waltham: Syngress.

Clemm, A. (2006) *Network Management Fundamentals*. Indianapolis: Cisco Press.

Collins, M. (2017). *Network Security Through Data Analysis, 2nd edition*. Sebastopol: O'Reilly Media.

Davies, J. (2016) *ITIL Foundation All-in-One Exam Guide*. New York: McGraw-Hill.

EN 50173-1 (2011). *Information technology - Generic cabling systems*. Brussels: CENELEC.

Ford. D. (2010). The OODA Loop. Haettu 6.5.2018 osoitteesta www.danford.net/boyd/essence4.htm

F-Secure. (2017a) *F-Secure Linux Security, Administrator's Guide*. F-Secure.

F-Secure. (2017b) *F-Secure Policy Manager, Administrator's Guide*. F-Secure.

Harris, S., Maymi, F. (2016) *CISSP all-in-one exam guide, 7th edition*. New York: McGraw-Hill.

Huotari, M-L. (2005). *Mitä tieto on*. Haettu 5.5.2018 osoitteesta http://oppimateriaalit.internetix.fi/fi/avoimet/0viestinta/informaatiotutkimus/po1/perusteet/01_mita_tieto_on/

Hutchins, E., Cloppert, M., Amin, R. (2011) *Intelligence driven defence, white paper*. Haettu 5.5.2018 osoitteesta https://lockheedmartin.com/content/dam/lockheedmartin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defence.pdf

IEEE (2013). *The real story of Stuxnet*. Haettu 7.1.2018 osoitteesta https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

ISO/IEC 7498-4. (1989). *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework, First edition*. Geneve: ISO/IEC.

Johnson, A. (2018). *CCNA Cybersecurity Operations Companion Guide*. San Jose: Cisco Press.

Nathans, D. (2015) *Designing and building a security operations center.* Waltham: Syngress

Osmanoglu, E., (2013) *Identity and access management.* Waltham: Syngress.

Puolustusministeriö. (2015) *KATAKRI 2015 tietoturvallisuuden auditointityökalu viranomaisille*. Helsinki: Puolustusministeriö.

Rid, T., McBurney, P., (2012). *Cyber-Weapons*. The RUSI Journal, 157:1.

Sanders, C., Smith, J. (2014) *Applied network security monitoring*. Waltham: Syngress.

Subramanian, M. (2010) *Network Management, second edition*. India: Pearson Education.

Syslog-ng. (2018). Syslog-ng. Haettu 8.5.2018 osoitteesta http://www.syslog-ng.com

Tietoturvallisuusasetus 681/2010. Haettu 5.1.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Tilastokeskus. (2002). *Informaatiosta yhä pienempi osuus hyötykäyttöön*. Haettu 10.5.2018 osoitteesta https://www.stat.fi/tup/tietoaika/tilaajat/ta_07_02_faktuaari.html

Trost, R. (2009) Practical Intrusion Analysis: *Prevention and Detection for the Twenty-First century.* Boston: Addison-Wesley Professional.

Ubuntu (2015). Linux Log Files. Haettu 6.1.2018 osoitteesta https://help.ubuntu.com/community/LinuxLogFiles

Valtioneuvoston periaatepäätös. (2017) *Yhteiskunnan turvallisuusstrategia*. Turvallisuuskomitea.

Valtionvarainministeriö. (2009) *VAHTI Lokiohje*. Helsinki: Edita Prima Oy.

Wikipedia (2018a). Reliable Event Logging Protocol. Haettu 10.5.2018 osoitteesta https://en.wikipedia.org/wiki/Reliable_Event_Logging_Protocol

Wikipedia (2018b). *Network Time Protocol*. Haettu 17.5.2018 osoitteesta https://en.wikipedia.org/wiki/Network_Time_Protocol

Zimmerman, C. (2014) *Ten strategies of a world class cybersecurity operations center.* Bedford: The Mitre Corporation.