TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JONI KORJALA

TIETOTURVALLISUUDEN TILANNEKUVAN JA LOKIEN HALLINNAN KEHITTÄMINEN

Diplomityö

Tarkastaja: yliopisto-opettaja Marko Helenius ja

diplomi-insinööri Joona Kannisto
Tarkastajat ja aihe hyväksytty

Tieto- ja sähkötekniikan tiedekunnan dekaanin päätöksellä 30. elokuuta 2017

TIIVISTELMÄ

JONI KORJALA: Tietoturvallisuuden tilannekuvan ja lokien hallinnan kehittäminen
Tampereen teknillinen yliopisto
Diplomityö, 44 sivua
Syyskuu 2017
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietoturvallisuus
Tarkastajat: yliopisto-opettaja Marko Helenius ja diplomi-insinööri Joona Kannisto

Avainsanat: tietoturva, lokienhallinta, SIEM, IT infrastruktuurin valvonta

Taloudelliset menetykset, jotka kohdistuvat tietojärjestelmien toimintakunnon ja vakauden horjumiseen vaativat proaktiivista työskentelyä ja nopeaa reagoimista muutoksiin ja ongelmatilanteisiin. Keskitetyn hallintajärjestelmän avulla on mahdollista automatisoida ja integroida eri tieto-turvatyökalut samaan paikkaan, josta voidaan keskitetysti valvoa ja hallita ympäristöjä kokonaisuutena. Lokiviestit ja niiden hallinta ovat tärkeässä osassa tieturvallisuuden hallintaa. Niiden merkitys tulee kasvamaan, kun EU:n tietosuoja-asetus tulee sovellettavaksi 25.5.2018 määrittäen uusia velvoitteita rekisterinpitäjille.

Tässä diplomityössä tutkittiin lokien käsittelyä, keskitetyn lokienhallinnan menetelmiä sekä ohjelmistoja, jotka mahdollistavat valvonnan toteutuksen ja ilmoituksien generoimisen ylläpitäjille. Tavoitteena oli löytää kokonaisuus, joka mahdollistaisi työkalut valvonnan ja lokiviestien käsittelyn toteutukseen. Diplomityön tutkimusstrategiana oli kokeellinen tutkimus, jonka avulla pyrittiin saavuttamaan määritetyt tavoitteet.

Diplomityössä toteutettiin erillinen hallintaverkko, johon muutettiin olemassa olevien palvelimien sekä verkkolaitteiden hallintayhteydet. Hallintaverkon avulla päästiin palomuuraamaan sekä hallintayhteyksiä että diplomityössä toteutettuja Nagios-valvontajärjestelmää ja Splunk-keskitettyä lokienhallintajärjestelmää. Määritettyjen kohteiden ja toteutettujen järjestelmien avulla pyrittiin löytämään ympäristön toiminnan kannalta mielenkiintoisia lokiviestejä sekä lisäämään valvottavia kohteita.

Tämän diplomityön tuloksena saavutettiin kokonaisuus, jonka avulla voidaan valvoa laitteiden toimintaa ja kerätä lokiviestejä keskitettyyn paikkaan, josta niiden visualisointi ja analysointi helpottuvat. Valvontanäkymät koettiin hyödyllisiksi ja niiden muunneltavuus antaa mahdollisuuksia jatkokehityksille. Saavutettu kokonaisuus sopii ympäristöön, jossa oman IT-henkilöstön resurssit ovat rajalliset.

ABSTRACT

JONI KORJALA: Improving Information Security Situational Awareness and Event Management
Tampere University of Technology
Master of Science Thesis, 44 pages
September 2017
Master's Degree Programme in Information Technology
Major: Data Security
Examiner: Senior Reseacher Marko Helenius, M.Sc. Joona Kannisto

Keywords: Information Security, Log Management, SIEM, IT Infrastructure Monitoring

Minimizing financial losses from the disruptions and unavailability period of information systems needs proactive maintenance and fast response to incidents. A centralized security information and event management system enables IT infrastructure monitoring and log management. Log messages and their management have important role in information security management. The Significance of Log Management will increase in May 2017 when the new EU General Data Protection Regulation will be enforced.

This thesis discusses log collection, centralized log management, and tools to enable monitoring the status of systems. The monitoring tools can offer visualizations of the system as well as notifications to administrators. The main aim was to discover a collection of tools and systems to monitor IT Infrastructure, and handle log messages centrally. Using experimental study as a research strategy helped to achieve the appointed goals.

In this thesis, a separate management network was deployed. This made it possible to firewall the IT Infrastructure´s management connections and log management solutions. The critical and interesting functionalities were monitored with Nagios, and log messages were analyzed with Splunk.

The result of this thesis is a centralized system for monitoring and handling of log messages from IT infrastructure, which enables log visualization and analysis. The visualization dashboards were discovered to be useful and the versatilities of dashboard configurations gave possibilities for future development. The result is suitable for an environment where the resources of company internal IT staff are limited.

ALKUSANAT

Lokiviestien käsittely ja hyödyntäminen ovat kiinnostaneet minua jo ennen tätä diplomityötä, mutta syvällisempi perehtyminen on jäänyt aiemmin tekemättä. Diplomityön aiheen hauduttelu on aloitettu vuoden 2016 aikana ja tekemisen aloitin 2017 vuoden alussa. Kokopäivätöiden ohessa diplomityöprosessin eteneminen ei ollut kovin vikkelää, mutta haluaisinkin kiittää työni tarkastajaa Joona Kannistoa pitkäjänteisestä ja kannustavasta otteesta diplomityöhöni liittyen.

Tampereella, 23.10.2017

Joni Korjala

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

ASDM	Adaptive Security Device Manager, Ciscon graafinen hallintatyökalu
COBIT	Control Objectives for Information and Related Technologies, ICT-Prosessien viitekehys
CPU	Central Processing Unit, suoritin
ESXi	VMwaren virtualisointikäyttöjärjestelmä
FTP	File Transfer Protocol, tiedonsiirtoprotokolla
GB	Gigatavu
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure, suojattu hypertekstin siirtoprotokolla
IDS	Intrusion Detection System, tunkeutumisenhavaitsemisjärjestelmä
IPS	Intrusion Prevention System, tunkeutumisenestojärjestelmä
IP	Internet Protocol, Internet-protokolla
ISO 27000	ISO 27000 –standardisarja
NTP	Network Time Protocol, aikaprotokolla
PCI-DSS	Payment Card Industry Data Security Standard, kortinhaltijoiden tietojen käsittelyn auditointi
RELP	Reliable Event Logging Protocol, lokiviestien yksi protokolla
SCP	Secure Copy, suojattuun tiedonsiirtoon käytettävä protokolla
SEM	Security Event Management, tietoturvatapahtumien valvonta
SFR	Moduuli Ciscon ASA palomuureissa
SIEM	Security Information and Event Management, Tietoturvatiedon ja tapahtumien hallinta
SIM	Security Information Management, lokienhallinta
SNMP	Simple Network Management Protocol, TCP/IP-verkkojen hallintaprotokolla
SOAP	Simple Object Access Protocol, XML-kieleen pohjautuvat tietojen vaihtamisessa käytettävä protokolla.
SSH	Secure Shell, salattu etäyhteys
TCP	Transmission Control Protocol, tietoliikenneprotokolla
TLS	Transport Layer Security, salausprotokolla
UDP	User Datagram Protocol, tietoliikenneprotokolla
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä
VLAN	Virtual LAN, fyysisen lähiverkon jakaminen loogisesti
VPN	Virtual Private Network, virtuaalinen erillisverkko
WAN	Wide Area Network, laajaverkko
XML	Extensible Markup Language, merkkauskieli

1. JOHDANTO

Tämän diplomityön tavoitteena olivat lokitietojen keskitetyn hallinnan tarpeet ja ongelmiin sekä muutoksiin reagoimisen parantaminen. Tietojärjestelmien toimintakunnon ja vakauden horjumisesta johtuvien taloudellisten menetysten minimoiminen vaatii proaktiivista työskentelyä ja nopeaa reagoimista muutoksiin ja ongelmatilanteisiin. Nykypäivänä tietojärjestelmiin voi kohdistua hyökkäyksiä, joiden seurauksena järjestelmään saatetaan tunkeutua ja tietoja varastaa [1, s. 29]. Tunkeutumisen havaitsemisen tueksi on olemassa erilaisia teknologioita, mutta teknologiat itsessään eivät niitä löydä, vaan tämä vaatii ihmisen osaamista ja havainnointikykyä. [2, s. 20].

Tuotannon tietojärjestelmät koostuvat monista eri osa-alueista ja osa niistä voivat olla elintärkeitä organisaation toiminnan kannalta. Ne saattavat sisältää kriittistä tietoa, jonka menettämiseltä ja varastamiselta tarvitsee suojautua. Organisaatioiden järjestelmät ja sovellukset tulisikin suojata mahdollisimman hyvin, mutta uusien uhkien ilmetessä reagoinnin ja suojautumisen tulee tapahtua nopeasti. [3, s. 249]

Automatisoidut tietoturvatoimenpiteet ovat tärkeässä osassa ja niitä onkin hyvä hyödyntää sellaisissa toiminnoissa, joissa ei vaadita ihmisen toimenpiteitä. Varmistustyöt ovat hyvä esimerkki automatisoidusta prosessista, jossa varmistustyöt tehdään ajastetusti automaattisesti ja huomiot sekä varoitukset lähetetään automaattisesti ylläpitäjille. Suurin hyöty saavutetaan keskitetystä järjestelmästä, joka valvoo useita eri kohteita. [3, s. 250]

Tässä diplomityössä tutkimuksen kohteena ovat lokiviestit ja niiden keskitetty hallinta. Loki on viesti, jonka tietokone, laite tai ohjelmisto generoi jonkin tapahtuman seurauksena. Se voi olla esimerkiksi käyttäjän kirjautuminen järjestelmään tai palomuurin viesti, kun liikenne täsmää pääsylistan ehtoon. Keskitetyn hallintajärjestelmän avulla on mahdollista automatisoida ja integroida eri tietoturvatyökalut samaan paikkaan, josta voidaan keskitetysti valvoa ja hallita ympäristöjä kokonaisuutena. [4, s. 3]

Lokiviestit ja niiden hallinta ovat tärkeässä osassa tieturvallisuuden hallintaa. Niiden merkitys tulee kasvamaan, kun EU:n tietosuoja-asetus tulee sovellettavaksi 25.5.2018, mikä asettaa uusia velvoitteita rekisterinpitäjille. Tämä muutos on hyvä huomioida suunniteltaessa ja toteutettaessa uusia järjestelmiä sekä ylläpidettäessä olemassa olevia. Rekisterinpitäjän on määritettävät käsittelytavat ja toteutukset niin teknisestä kuin organisatorisesta näkökulmasta. Teknisestä näkökulmasta suurimmat vaikutukset kohdistuvat muun muassa tietojärjestelmien tietoturvaan, auditointeihin ja teknisiin rajoituksiin. [5, s. 9, 13]

Tässä diplomityössä pyritään löytämään hyväksi todettuja menetelmiä, joiden avulla liiketoiminnan jatkuvuutta voitaisiin turvata sekä tietoturvallisuuden tietoisuutta parantaa. Tavoitteena on toteuttaa hyväksi todettujen menetelmien perusteella keskitetty lokienhallintajärjestelmä ja laitteiden automaattinen valvonta. Järjestelmien avulla pyritään saamaan hälytyksiä ja näkymiä, joiden avulla saataisiin arvoa lokitiedoista ja tapahtumista verkossa. Järjestelmien avulla pyritään myös helpottamaan lokien seuraamista, koska ilman keskitettyä lokienhallintaa lokiviestit ovat hajallaan sekä eri muodossa riippuen laitteesta ja järjestelmästä, mikä luo haasteita tapahtumaketjujen analysoimiselle. Lokien käsittelyyn ja laitteiden valvontaan pyritään löytämään menetelmiä, jotka ottavat huomioon tietoturvallisuuden näkökulmat. Ennalta määritettynä haasteena on tilanne, jossa ei päästä havaitsemaan mitään poikkeavaa tai hyödynnettävää, jolloin tietoturvallisuuden tapahtumien ja lokitietojen hyödynnettävyyden arviointiin ei saada todellisia tuloksia.

Tämä diplomityö on kokeellinen tutkimus, jonka tavoitteet pyritään saavuttamaan toteutettuna osittain laboratorio-olosuhteissa ja osittain oikeassa tuotantoympäristössä. Käyttöönotettavia järjestelmiä ja olemassa olevien laitteiden hallintayhteyksiä varten toteutetaan erillinen hallintaverkko, jolla pyritään turvaamaan järjestelmiä ja rajoittamaan hyökkäyspintaa sekä saamaan näkyvyyttä verkkojen välille. Valinnat tutkittaville tuotteille tehtiin aiempien kokemuksieni sekä saatavilla olevien konfigurointidokumentaatioiden perusteella. Lisäksi tuotteiden valintaa ohjasi muodostunut teoreettinen viitekehys. Nagiokseen olen tutustunut aiemmin toisessa projektissa, jonka perusteella päädyin hyödyntämään sitä myös tässä diplomityössä. Splunk puolestaan nousi esille teoreettista viitekehystä tehdessä ja lisäksi olen perehtynyt siihen opiskeluiden aikana kurssiharjoituksen tehtävässä. Sekä Nagioksen että Splunkin osalta niihin perehtyminen oli aiemmin jäänyt matalalle tasolla, ja näin ollen niiden lisäperehtymiselle oli tarvetta ja näin niissä olevan potentiaali hyödyntää tämän diplomityön kontekstissa.

Aiemmissa tutkimuksissa ja kirjallisuudessa ilmenee muun muassa lokiviestien suuren määrän käsitteleminen ja siihen liittyviä ohjelmistoja. Söderström̈a ja Moradiana ovat tutkineet artikkelissaan kasvavien lokimäärien hallitsemista keskitetyllä ratkaisulla. Tutkimuksessa löytyi menetelmiä keskitetyn lokienhallintaratkaisun turvaamiseen muun muassa pääsynhallinnan avulla. [6, s. 1249 – 1258] Bumgarner käsittelee kirjassaan Splunk-ohjelmiston käyttöönottoa ja pohtii sen monipuolisuutta. Bumgarnerin mielestä Splunkia voidaan hyödyntää erilaisissa sovelluksissa ja se mukautuu ja skaalautuu [7]. Sigman puolestaan mainitsee kirjassaan Splunkin tehokkaista haku- ja visualisointityökaluista [8]. SANS-instituutin julkaisussa havaitaan, että organisaatioiden verkkojen segmentoinnilla saavutetaan suojauspintaa, hallittavuutta ja näkyvyyttä verkkoihin sekä paremmat lähtökohdat ongelmatilanteiden hallintaan verrattuna verkkoon ilman segmentointia [9, s. 18 – 19].

Diplomityö jakautuu rakenteellisesti seitsemään lukuun, joista luvussa 2 käsitellään tietoturvallisuutta ja tietoturvallisuuden hallintaa yleisesti sekä tietoturvallisuuden tiedon

ja tapahtumien hallintaa. Luku 3 keskittyy lokiviesteihin ja niiden käsittelyyn. Luvussa 4 tutkitaan ympäristöä, jossa kokeellisen tutkimuksen käytännön toteutukset tullaan tekemään sekä esitellään eriytetyn hallintaverkon toteuttamisen vaiheet, jonka avulla pyritään suojamaan käyttöönotettavia järjestelmiä ja laitteiden hallintayhteyksiä. Luku 5 sisältää valvontaohjelmiston ja SIEM-ohjelmiston käyttöönoton, joiden avulla pyritään löytämään ratkaisuja tutkimusongelmiin. Luvussa 6 pohditaan työn tuloksia. Luku 7 on yhteenveto diplomityöstä.

2. TIETOTURVALLISUUS JA TAPAHTUMIEN HALLINTA

Tässä kappaleessa käsitellään tietoturvallisuutta yleisesti ja perehdytään tietoturvallisuuden tiedon ja tapahtumien keskitettyyn hallintaan teknisesti. Tietoturvallisuustiedon ja tapahtumien hallinnan määrittämiseen ja toteutukseen liittyvät kerättävien lokitietojen määrittäminen, jotka pohjautuvat kartoitettujen riskien ja tietoturvapolitiikan pohjalta. Tietoturva-auditoinneissa yhtenä auditoitava kohteena on lokienhallinta, johon sisältyvät lokien säilytys, seuranta ja lokipolitiikka. Ympäristön ja järjestelmien kriittisyys on yksi peruste sille, kuinka paljon suojaamiseen ja ylläpitämiseen panostetaan. Kriittisyyden määrittelyä varten tehdään riskien kartoitusta, jonka perusteella määrittyvät kohdistuvat riskit ja toisaalta niiltä suojautumiseen vaadittavat toimenpiteet.

Tietoturvallisuus on tietojen, järjestelmien ja palveluiden suojaamista sekä normaali että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuus jakaantuu tiedon kolmen ominaisuuden - luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen. Luottamuksellisuuteen pyrkiminen tarkoittaa sitä, että kukaan sellainen henkilö ei pääse käyttämään tietoja, jotka eivät ole hänelle tarkoitettu. Tietojen lukeminen tai muokkaaminen onnistuu vain heiltä, joille on myönnetty oikeus tietoihin etukäteen. Käyttäjät pitää ensin todentaa, jotta valtuutetut käyttäjät voitaisiin tunnistaa. Luottamuksellisuuden saavuttamiseen liittyy oleellisesti todentaminen, jonka tarkoituksena on varmistua siitä, että henkilö, laite tai tiedon alkuperä on juuri se mitä esittääkin. [10, s. 48 – 49]

Tiedon eheys tarkoittaa, että mikään ulkopuolinen taho ei pysty luvatta muokkaamaan tiedon sisältöä, esimerkiksi poistamaan tai tekemään asiattomia muutoksia. Eheydessä voi ilmetä myös tahattomia ongelmia, jos esimerkiksi levylle on tullut vika-alue tai tiedoston sisällä on eheysvika. Eheyden turvaamiseksi käytetään kryptologisia menetelmiä, tarkistussummia, lokitiedostoja, tiedonsiirron protokollia ja erilaisia tarkistusohjelmia sekä sisäisiä tarkistuksia. [10, s. 48 – 49]

Käytettävyydellä tarkoitetaan sitä, että yhteydet, järjestelmät, tiedot ja ohjelmat ovat saatavilla, kun niitä tarvitaan. Tämä koskee myös mahdollisesti useita vuosia vanhoja tiedostoja, joita pitäisi pystyä hyödyntämään, mutta se on käytännössä mahdotonta, kun tiedostoja ei saada auki tarvittavan ohjelman ollessa niin vanha, että se ei toimi nykyisessä koneessa. [10, s. 48 – 49][11, s. 78 – 79]

2.1 Tietoturvallisuuden hallinta

Tietoturvallisuus voidaan jakaa kahdeksaan eri osa-alueeseen helpottamaan suunnittelua, toteutusta ja valvontaa. Nämä kahdeksan osa-aluetta ovat hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja tietoliikenneturvallisuus. Tässä diplomityössä keskitytään tietoturvallisuuden hallinnan osa-alueeseen siltä osin, mitkä liittyvät lokitietojen käsittelyyn.

Hallinnollinen tietoturvallisuus on organisaation tietoturvatoiminnon lähtökohtana ja muodostaa tietoturvallisuuden johtamistoiminnot. Hallinnollinen tietoturvallisuus käsittää muun muassa johdon määrittelemän tietoturvapolitiikan, uhka- ja riskianalyysistä sekä jatkuvuus- ja toipumissuunnitelmasta. Tietoturvapolitiikan määrittelyä varten tehdään uhka- ja riskianalyysejä, jonka perusteella saadaan selville suojattavat kohteet ja suojaamiseen käytettävät resurssit. Käytettävät resurssit liittyvät myös organisaation lokipolitiikkaan, jossa määritellään muun muassa organisaation eri tasojen vastuut, käytettävät menetelmät sekä käsiteltävät lokit. Riippuen organisaation toiminnasta, voi siihen kohdistua viitekehyksien vaatimuksia ja organisaation toimintaa voidaan auditoida. Auditoinneissa yhtenä kohteena voi olla organisaation lokiviestien hallinta. Tietoturvallisuuden viitekehykset ja standardit tukevat organisaation tietoturvallisuuden hallinnan suunnittelua, toteutusta ja seuraamista.

2.1.1 Tietoturvapolitiikka

Organisaation tietoturvapolitiikka ohjaa ja tukee tietoturvallisuuden toteutumista. Siinä määritellään käytännöt, vaatimukset ja tavoitteet, joiden perusteella saadaan lähtökohta suunnittelulle ja toteuttamiselle, joilla organisaation tiedot ja järjestelmät suojataan. Tietoturvapolitiikka on organisaation johdon hyväksymä ja siitä selviää johdon näkemys tavoitteista tietoturvallisuuden suhteen, sisältäen vastuunjaot johdon, ylläpidon ja käyttäjien kesken. [12][13]

Tietoturvapolitiikka on ylin tietoturvallisuuden dokumentti ja sen pohjalta voidaan tehdä alemman tason politiikkoja ja ohjeistuksia, joilla asioiden jalkauttaminen organisaatiossa helpottuisi. Tietoturvapolitiikan olisi hyvä olla kaikkien ymmärrettävässä muodossa. Tietoturvapolitiikan jalkauttamisessa tulisi käyttää tiedottamisen keinoja, jotta organisaation käyttäjä osaisivat noudattaa niitä. Organisaation tietoturvapolitiikan ajantasaisuutta tulisi tietyin väliajoin seurata ja tarkastella, ja sen pitäisi olla linjassa muiden organisaation dokumenttien kanssa. [12]

Tietoturvapolitiikan sisältäessä yleiset käytännöt, vaatimukset ja tavoitteet, joiden pohjalta yrityksen tietoturvallisuutta hallitaan, tehdään organisaatiolle myös tietoturvasuunnitelma, jossa määritellään yksityiskohtaisemmin tavat, joilla saavutetaan tietoturvapolitiikassa määritetyt asiat. Tietoturvasuunnitelma sisältää raportin nykytilanteesta, suosi-

tukset ja vaatimukset tavoitteiden saavuttamiseksi, aikataulutuksen suunnittelujen toimeenpanemiseksi ja suunnitelman säännöllisille tarkastuksille. [12][14]

2.1.2 Riskit ja riskienhallinta

Tietoturvallisuuden yhtenä tärkeänä osana on tietoturvariskien arviointi. Näin ollen tässäkin diplomityössä on hyvä käsitellä riskien ja riskienhallinnan perusteita. Riski on sellaisen tapahtuman, johon liittyy jotain mitä ihminen arvostaa. Riskejä voidaan jakaa esimerkiksi operatiivisiin ja strategisiin riskeihin. Operatiivinen voi olla riski joka vaarantaa tietyn toiminnon ja strateginen puolestaan voi vaarantaa koko yrityksen olemassaolon. Riskit voidaan jakaa myös staattisiin ja dynaamisiin riskeihin, jossa riskit jaetaan muuttumattomiin vakioriskeihin sekä vaihtuviin ja ennustamattomiin riskeihin. [15]

Riskienhallinnassa pyritään määrittelemään etukäteen mahdolliset riskit, jotka voisivat uhata organisaation liiketoimintaa. Riskit voivat olla myös tuntemattomia, jolloin niitä ei pystytä hallitsemaan. Riskien tunnistamisen jälkeen seuraava vaihe on arvioida riskit niiden kahden perusominaisuuden avulla. Riskeille tyypilliset ominaisuudet ovat tapahtumatodennäköisyys ja seurausten vakavuus. Haasteita riskien todennäköisyyksien arvioinnissa on esimerkiksi jokin tapahtuma jota ei ole koskaan tapahtunut, mutta se olisi mahdollinen tapahtua. Riskien seuraustodennäköisyyksien määritys riippuu myös käytettävissä olevan tiedon laadusta ja määrästä. [16]

Riskien arvioinnin jälkeen riskit voidaan asettaa tärkeysjärjestykseen ja sen perusteella määrittää resurssien kohdistaminen. Tulosten pohjalta suunnitellaan mahdollisia kehitystoimenpiteitä, joita ovat riskin välttäminen, pienentäminen, siirtäminen, jakaminen ja pitäminen omalla vastuulla. Riskienhallinta on jatkuva prosessi, jonka tulisi olla läsnä organisaation päätöksenteossa ja toiminnassa. [16]

2.1.3 Tietoturva-auditoinnit, viitekehykset ja standardit

Tietoturvallisuuden hallintaan kuuluu yhtenä osana muun muassa auditoinnit ja jatkuva seuranta. Tietoturva-auditoinnin tarkoitus on puolueettomasti testata organisaation tietoturvallisuuden riittävyyden taso sen etuuksien suojaamiseksi. Salaisen tiedon käsittelemisessä sopimuskumppanien toimintaa tulee valvoa sekä tarpeen mukaan käyttää auditoijaa antamaan toiminnasta lausuntoja. Tietoturva-auditointiprosessin tavoitteena on koostaa organisaatioon kohdistuvat tietoturvariskit, riskeihin varautumisen mahdollisuudet ja havainnot liittyen tietoturvallisuuden eri osa-alueilta. Tietoturva-auditointiprosessi koostuu suunnitteluvaiheesta, kenttätutkimuksesta ja analysoinnista, jonka pohjalta organisaatio saa raportin havaituista asioista ja kehitysehdotuksista. Auditoinnin toteutuksessa apuna käytetään jotain tietoturvastandardia tai ohjeistusta, johon pystytään nojaamaan määritettäessä organisaation tietoturvan tasoa. [17, s. 51][18, s. 20 – 22]

Tietoturvallisuuden toteutusta ja auditointia varten on olemassa erilaisia viitekehyksiä, standardeja ja ohjeistuksia. Organisaation tietojenkäsittelyn hahmottamiseen on olemassa esimerkiksi viitekehys COBIT (*lyh. Control Objectives for Information and Related Technologies*). Tietoturvastandardeja on esimerkiksi ISO 27000 –sarja, joka on keskittynyt tietoturvallisuuden hallintajärjestelmiin. Ohjeistuksia tarjoaa esimerkiksi Suomen valtionvarainministeriö, jolla on ohjeistuksia tieturvallisuuden eri osa-aluiden kehittämistä varten tukevia VAHTI-ohjeita. [19][18, s. 68, 76]

2.2 Tietoturvatiedon ja tapahtumien hallinta

Tietoturvatiedon ja tapahtumien hallinta SIEM (*eng. Security Information and Event Management*) muodostuu kahdesta eri toiminnosta, SIM (*eng. Security Information Management*) ja SEM (*eng. Security Event Management*). SIEM järjestelmän avulla on mahdollista automatisoida ja integroida eri tietoturvatyökalut yhteen ja samaan paikkaan, josta voidaan keskitetysti valvoa ja hallita ympäristöjä kokonaisuutena. [3, s. 253]

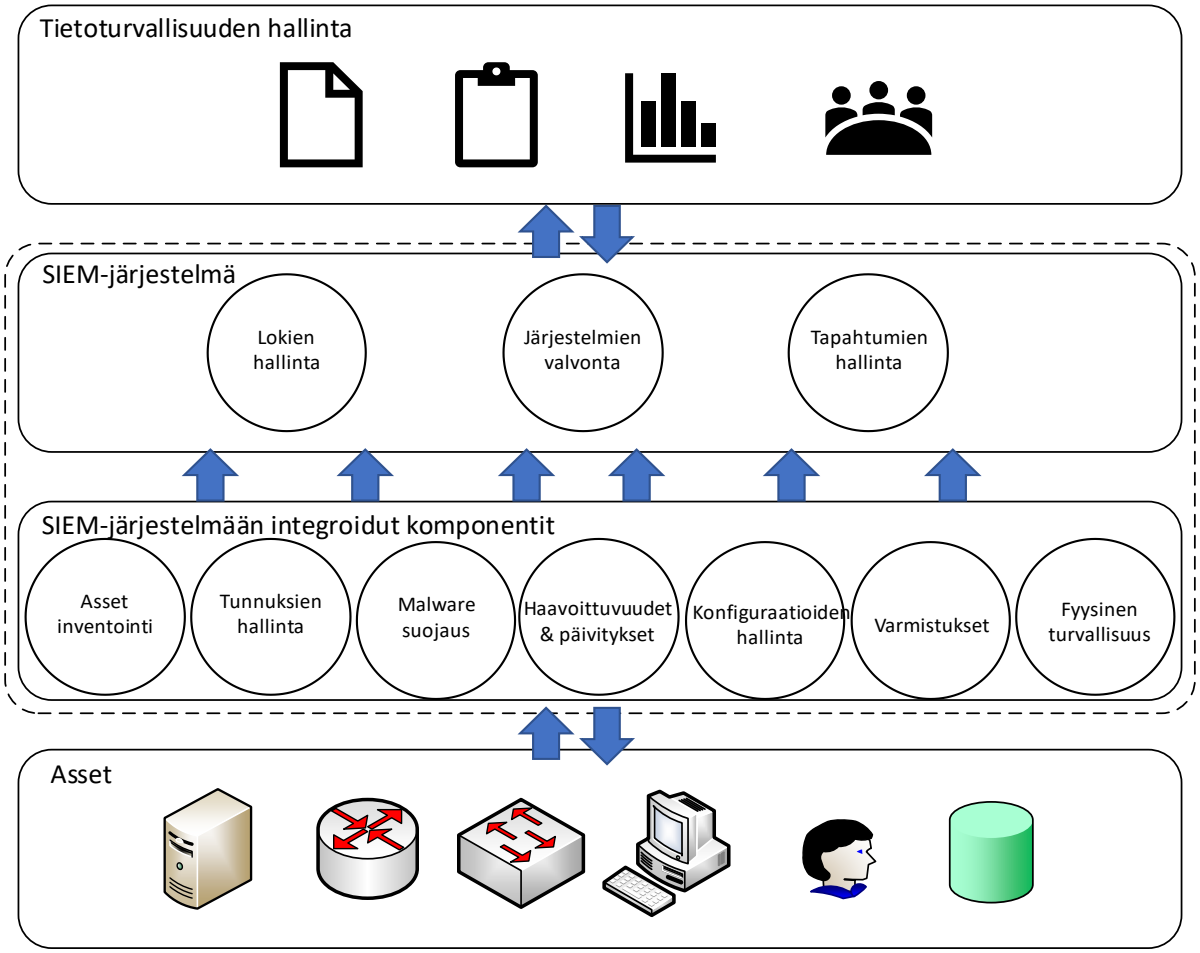
SIM lokienhallinta koostuu lokien keräämisestä eri järjestelmistä ja sovelluksista, raportoinnista ja analysoinnista. Kerätystä lokidatasta ja sen analysoinnista muodostuu vaatimustenmukaisuusraportointi. SEM käsitteenä tarkoittaa reaaliaikaista monitorointia ja tietoturvatapahtumien hallintaa. Siinä prosessoidaan tietoturva- ja verkkolaitteiden sekä järjestelmien ja sovelluksien loki- ja tapahtumadataa reaaliaikaisesti, mikä mahdollistaa tapahtumien riippuvuuksien tarkastelun. [3, s. 253]

Tietoturvallisuustapahtumia voidaan kerätä useista eri laitteista, kuten palomuureista, kytkimistä, reitittimistä, palvelimista ja sovelluksista. Osassa laitteista on mahdollista kerätä laitteen omaan muistiin tapahtumia, toinen vaihtoehto on kerätä useista lähteistä tietoturvallisuustapahtumat keskitettyyn järjestelmään. Tavoitteena ei ole kerätä mahdollisimman paljon dataa vaan, kuinka saadaan relevantein data laitteista kerättyä. [20, s. 296]

SIEM-järjestelmiä on tarjolla usealta eri valmistajalta, esimerkiksi LogRhythm, LogPoint, Splunk, Alien Vault ja IBM:n Honorable Mentrion. Tuotteisiin perehtymisen voi aloittaa esimerkiksi Gartner-arvostelujen kautta, jossa tuotteiden eri ominaisuuksia vertaillaan ja lisäksi asiakkaiden palautteita pääsee lukemaan. Valmistajat tarjoavat myös ilmaisjaksoja tuotteidensa testaamiseksi. [21]

SIEM-prosessi koostuu tietoturvallisuuden hallinnasta, jossa on määritettynä politiikat ja vastuuhenkilöt. Hallinnasta vastaavat pidetään ajan tasalla SIEM-järjestelmän avulla, johon kuuluvat lokien hallinta, järjestelmien valvonta ja tapahtumien hallinta. SIEM-järjestelmään on liitettynä muun muassa laitekannan inventoinnit, tunnusten hallinta, lokien hallinta, varmistukset ja fyysinen turvallisuus. Asset-tasolta, eli laitekannasta datan kerääminen keskitetysti on yksi SIEM-järjestelmän ominaisuuksista. Lokiviestidataa voidaankin kerätä useilla eri menetelmillä riippuen kerättävästä laitteesta, esimer-

kiksi valvottavien laitteiden syslog-datavirrasta, asennettujen agenttien avulla tai esimerkiksi erilaisten API-rajapintojen avulla. Kokonaisuutta kuvaa kuva 1, jossa on havainnollistettu SIEM-järjestelmän koostumus. [3, s. 253, 256 - 259]



Kuva 1. *SIEM-viitekehys, mukaillen [3, s. 256]*

Keräyksen ja analysoinnin seurauksena syntyy raportteja, hälytyksiä ja tietoa vianselvityksen tueksi. Tapahtumaketjut koostuvat paikka- ja kriittisyystiedoista. Analysoinnissa korreloidaan eri tapahtumia ja hyödynnetään aiemmin kerättyä datamassaa, jonka seurauksena voidaan havaita poikkeavuuksia ja syitä tapahtumille. Verkko- ja muiden laitteiden lokien ja tapahtumien kerääminen yhdessä kaikkien poikkeavuuksien kanssa on edellytys kehittyneiden uhkien havainnoinnissa. Näiden yhteen saattamisen ja tapahtuminen riippuvuussuhteiden tarkastelun avulla voidaan havaita tietoturvatapahtuma. SIEM-järjestelmän avulla on mahdollista havaita poikkeamia sekä monitoroida ja verrata niitä ennalta määriteltyihin normaaliarvoihin. [22, s. 190, 192]

Haasteita tapahtumien keräämiselle luovat väärät hälytykset, jolloin hälytyksiä saattaa generoitua tavanomaisesta toiminnasta, jolla ei ole pahantahtoisia pyrkimyksiä. Toisaalta laite saattaa generoida suuren määrän hälytyksiä, jolloin hyödyllisen tiedon löytäminen vaikeutuu. Lisäksi kokonaisuuden hallinnassa haasteita ovat laajasti olemassa olevat teknologia ja lukuisat erilaiset uhat, jotka tekevät kokonaisuudesta monimutkaisen.

Prosessin monimutkaisuutta ja tehokkuutta pyritään parantamaan automatisoimalla mahdollisimman laajasti kontrollointi- ja valvontatehtäviä. Aiemmat tutkimukset ja standardoinnit ovat listanneet tehtäviä, joita voitaisiin automatisoida. [20, s. 296][3, s. 260]

3. LOKIVIESTIT

Tässä kappaleessa käsitellään lokiviestejä, niiden sisältöä, kuljetusta, visualisointia, yleisiä uhkia sekä perehdytään lokipolitiikkaan yleisellä tasolla. Lokien keräystä ja analysointia varten diplomityössä tutkitaan teknisiä ratkaisuja, joiden avulla tietoturvallisuuden seurantaa ja tilannetietoisuutta voitaisiin parantaa. Lisääntyvien uhkien kohdistuminen tietoverkkoihin ja järjestelmiin aiheuttavat lokiviestien lisääntymisen, joka puolestaan lisää lokiviestien käsittelyn määrää sekä monimutkaistaa hyödynnettävien lokiviestien löytämisen. Haasteita aiheutuu esimerkiksi lokiviestien säilytyksestä, suojaamisesta ja analysoinnista. [6, s. 1249]

Hyviä esimerkkejä hyödyllisistä lokitiedoista on esimerkiksi tallennusjärjestelmän ilmoittamat lokit, kun laitteistossa ilmenee ongelma. Jos ongelmiin pystytään reakoimaan tarpeeksi ajoissa, voidaan välttyä suuremmalta katastrofilta. Hyödyllisiä lokeja ovat myös esimerkiksi käyttäjien kirjautumistiedot, joista jää jälki kirjauduttaessa tietojärjestelmään. Kirjautumistietoja voidaan puolestaan käyttää hyödyksi muun muassa palomuureissa, joissa voidaan määrittää käyttäjän oikeuksia päästä verkkoresursseihin. Lokeista kerätyn datan ja informaation perusteella tulisi ilmetä kuka on kirjautunut järjestelmään ja mitä hän on tehnyt. [4, s. 1 – 2][6, s. 1250 – 1251]

3.1 Lokin sisältö

Lokiviestin tulisi yleensä vastata kysymyksiin:

- Mitä on tapahtunut?
- Milloin tapahtunut?
- Missä tapahtunut?
- Kuka on osallisena?
- Mistä hän tai se saapui?

Lokien muodot vaihtelevat riippuen järjestelmästä ja valmistajasta. Tästä syystä on hyvä tulla tutuksi lokien kanssa ja määrittää tarpeelliset lokiviestit, jotta välttyy toisaalta hukkumisesta lokien määrään ja toisaalta, että lokeja voidaan hyödyntää organisaation toiminnassa. [4, s. 2]

Loki koostuu aikaleimasta, lähteestä ja datasta riippuen siitä, mikä järjestelmä tai laite on sen generoinut. Aikaleimassa on päivämäärä, kellonaika ja mahdollisesti aikavyöhyke. Aikaleima kertoo, milloin lokiviesti on generoitu, lähde voi olla esimerkiksi laitteen isäntänimi ja data kertoo mitä on tapahtunut, esimerkiksi jokin palvelu voi olla sammu-

nut. [4, s. 6 – 7, 13] Kuvassa 2 on esimerkki lähiverkon kytkimen lokista, joka kertoo, että NTP-palvelimeen ei saada yhteyttä.

```
I 06/19/17 18:34:34 00414 SNTP: Unable to reach configured SNTP servers
I 06/19/17 18:35:04 02631 SNTP: Server not found at 172.16.10.13.
```

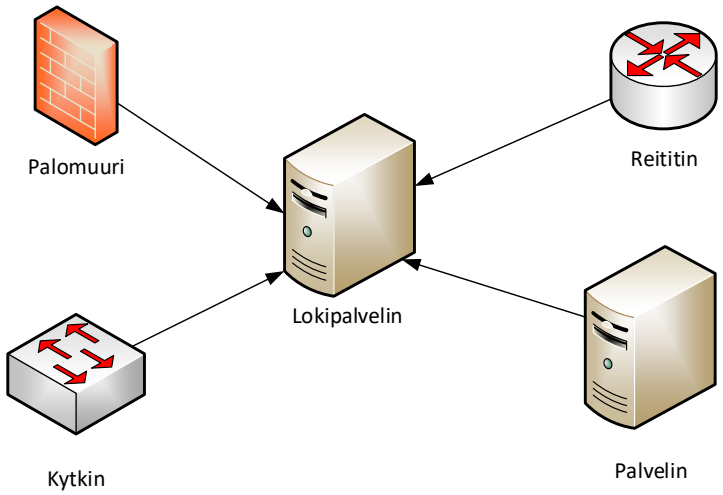
Kuva 2. *Kuvakaappaus lähiverkon kytkimen lokista.*

Lokit voidaan jakaa eritasoisiin kategorioihin: informatiivisiin, debug-viesteihin, varoituksiin, virheisiin ja hälytyksiin. Informatiiviset viestit ovat niin sanottuja hyvänlaatuisia, jotka kertovat ylläpitäjälle informaatiota jostakin operaatiosta, esimerkiksi verkkolaitteen hallitusta uudelleenkäynnistyksestä. Debug-viestit kertovat ohjelmiston ongelmasta, jonka pohjalta ohjelmistokehittäjät voivat tehdä vianpaikannusta ohjelmiston koodista. Varoitukset kertovat, jos järjestelmästä puuttuu jotakin, mutta se ei kuitenkaan vaikuta toimintaan. Virhelokit voivat generoitua usealta eri tasolta järjestelmästä, ja yleensä ne vain avustavat vian selvityksen alkuun, mutta eivät kerro ongelman pääsyytä. Hälytykset puolestaan liittyvät johonkin turvallisuuslaitteeseen tai turvallisuuteen liittyvään järjestelmään, jotka kertovat jotakin mielenkiintoista, mistä on haluttu saatavan tietoa, esimerkiksi IDS (*eng. Intrusion Detection System*) tai IPS (*eng. Intrusion Prevention System*) järjestelmä.

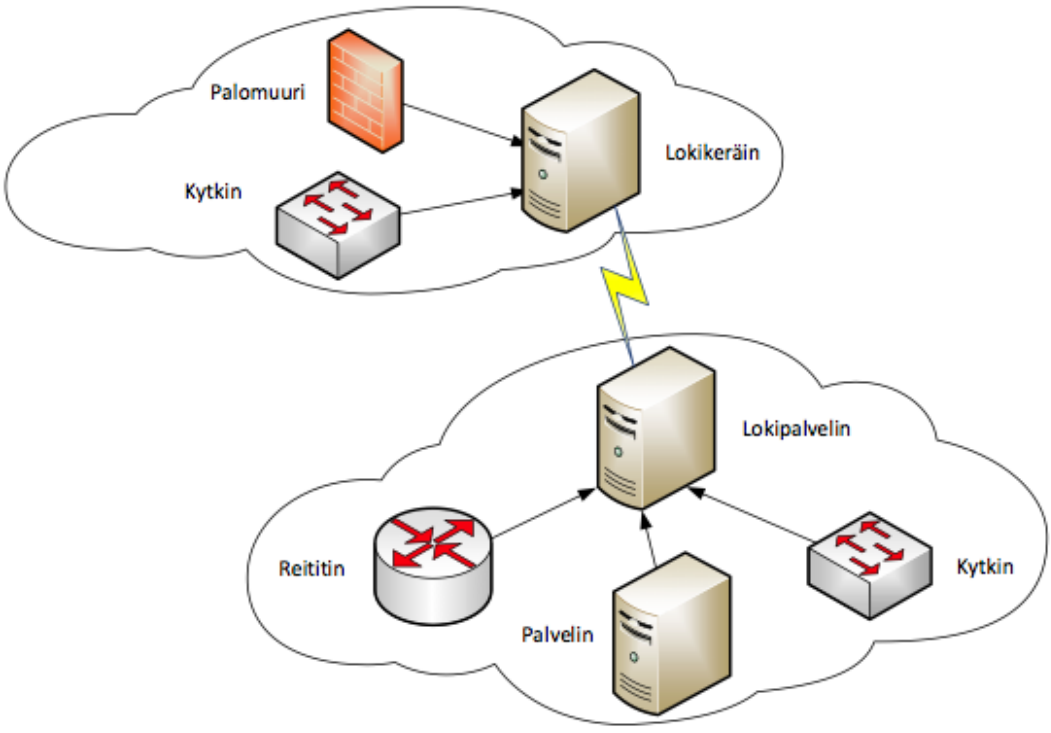
VAHTI Lokiohje 03/2009 määrittelee lokit ylläpito-, käyttö-, muutos- ja virhelokeihin. Lokit voivat kuitenkin kuulua useampaan luokkaan, joten niitä ei välttämättä voida sijoittaa pelkästään yhteen luokkaan. Ylläpitolokista selviää muun muassa käyttöoikeuksiin liittyvät muutokset, rekistereiden käytöstä aiheutuvat virhetilanteet ja järjestelmiin tehdyt muutokset. Käyttölokissa puolestaan selviää sisään- ja uloskirjautumiset, epäonnistuneet kirjautumiset, tietokantojen kyselyt. Muutoslokin tarkoituksena on kertoa tietosisältöjen muutoksista, järjestelmän parametrien ja konfiguraatiotiedostojen muutoksista. Virhelokiin jää järjestelmästä tai tapahtumasta havaitut virheet sekä rekisterissä havaituista epäjatkuvuuksista ja virheistä. [3, s. 3 – 4][23, s. 14, 29 – 30]

3.2 Lokin keräys ja kuljetus

Eri järjestelmät ja laitteet pystyvät lähettämään lokinsa eteenpäin, ja lokia voidaankin kerätä yhteen pisteeseen tai hajautetulla järjestelmällä. Valittava keräystapa riippuu paljolti organisaation koosta ja toimipisteiden sijainnista. Eri laitteiden ja järjestelmien tuottaessa eri muotoista lokia keskitetyn lokienhallinnan etuna on lokiviestien normalisointi ja indeksointi, joiden avulla lokimassasta hakeminen ja lokiviestien analysointi helpottuvat [6, s. 1257]. Esimerkiksi pienelle organisaatiolle sopii yksi keskitetty lokipiste, jossa organisaation verkossa on yksi palvelin keräämään lokiviestejä keskitetysti, kuten kuvassa 3. Puolestaan geologisesti eri paikoista koostuvan organisaation olisi hyvä toteuttaa hajautettu lokien keräys, joka ei ole riippuvainen WAN-yhteyksien toimivuudesta, kuten kuvassa 4. [4, s. 11]



Kuva 3. *Keskitetty lokinkeräys. (mukaillen [4])*

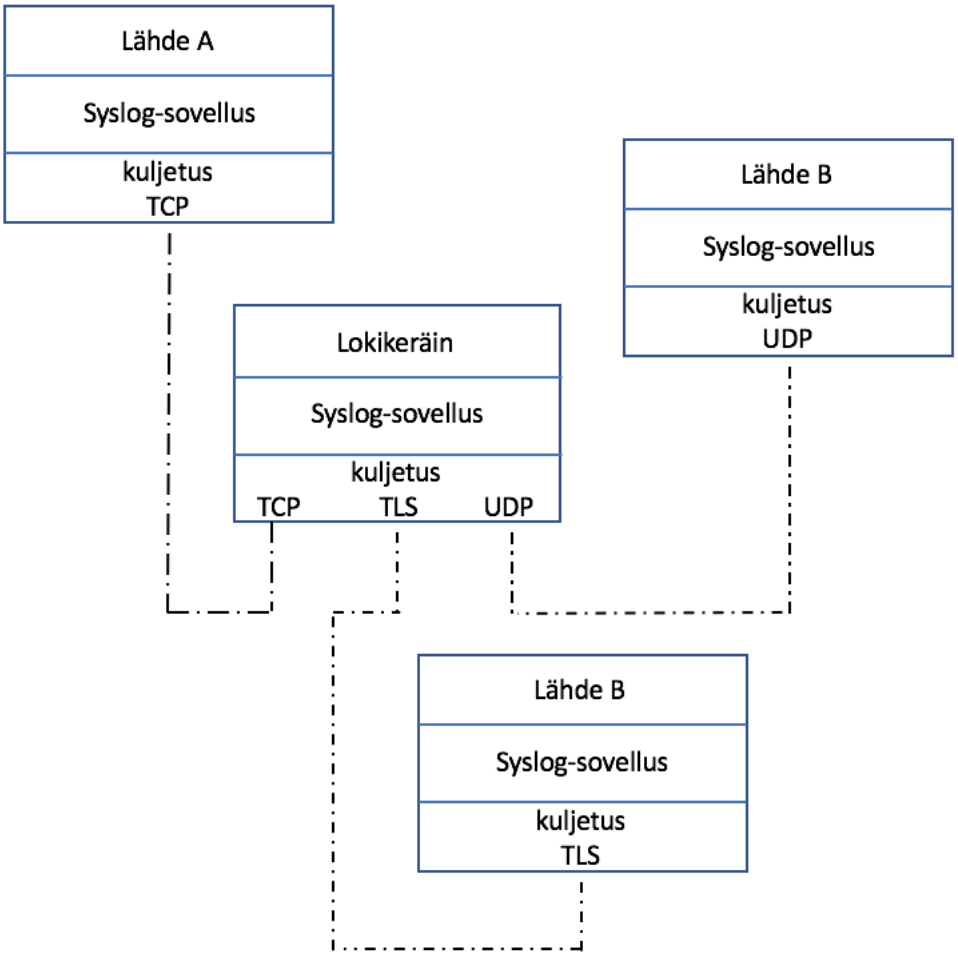


Kuva 4. *Hajautettu lokinkeräys. (mukaillen [4])*

Kerättävien laitteiden ja keräysjärjestelmien kellonaikojen tulisi olla samassa tahdissa, jotta mahdolliset tapahtumaketjut pystyttäisiin selvittämään. Kellonajan tahdistukseen voidaan käyttää keskitettyä aikapalvelinta, jolloin laitteet synkronoivat kellonajan palvelimelta. Aikapalvelimesta käytetään lyhennettä NTP (*eng. Network Time Protocol*). Organisaatiolla voi olla oma aikapalvelin tai vaihtoehtoisesti se voi käyttää julkisesti saatavilla olevia palveluita, kuten esimerkiksi VTT:n tarjoamaa mikes.fi – palvelua. Luottokorttiyhtiöiden PCI-DSS standardi velvoittaa synkronoimaan järjestelmien kellot. [23, s. 23, 26]

Lokien kuljetukseen paikasta toiseen on olemassa eri mekanismeja riippuen käyttötarkoituksesta ja tuotteesta. Kuten tietoturvassa yleensäkin, myös lokeissa ja niiden kuljetuksessa on tärkeää, että eheys, saatavuus ja luottamuksellisuus ovat kunnossa. Eheys ennen kaikkea, jotta voidaan varmistua, ettei lokia ole peukaloitu. [4, s. 35][23, s. 57]

Syslog UDP on yleisesti käytetyin mekanismi Unix-järjestelmissä ja verkkolaitteissa vaikkakin siinä on useita puutteita. Syslog UDP:n puute on UDP-prokollan ominaisuus, jossa ei varmistuta onko tieto kulkenut perille. Lisäksi Syslog UDP:n käyttämä liikenne ei kulje salattuna. Syslog-viestejä voidaan kuljettaa myös TCP-prokollan kanssa sekä TLS-suojauksen kanssa, joista puhutaan termeillä Syslog TCP ja Secure Syslog. Kuvassa 5 havainnollistetaan Syslog-protokollan eri versioita, jossa katkoviivoilla kuvaillaan kuljetukseen käytettävissä olevia versioita. VAHTI 03/2009 lokiohje suosittelee käyttämään Secure Syslogia lokiviestien kuljettamiseen. [23, s. 62] [24, s. 4, 6]

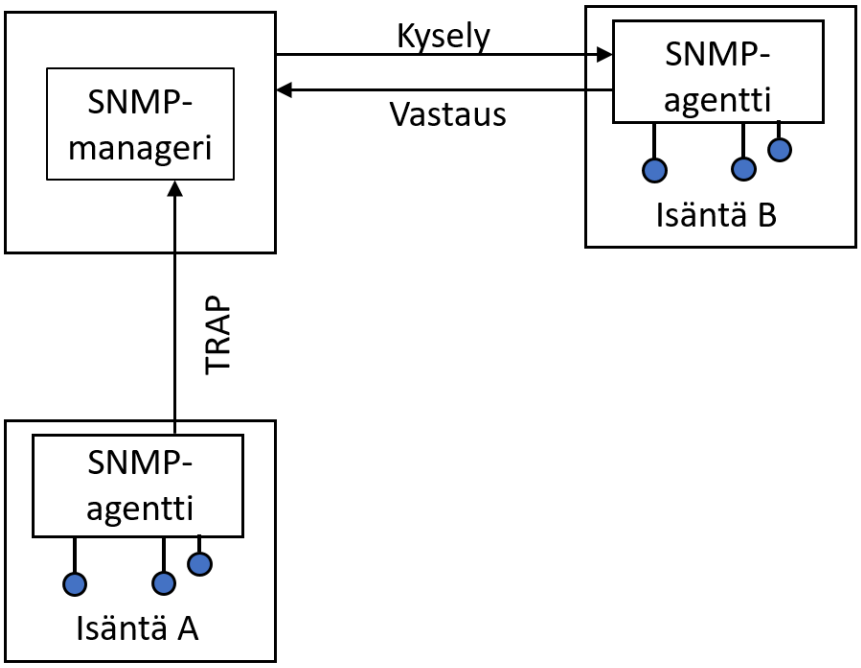


Kuva 5. *Syslog-kuljetukset (mukaillen [24, s. 4])*

Lokiviestejä voidaan kuljettaa Syslog-mekanismin lisäksi muun muassa SOAP over HTTP -konseptin, SNMP-protokollan, FTP- tai SCP-protokollien ja RELP-protokollan

avulla. SOAP-protokolla (*eng. Simple Object Access Protocol*) käyttää XML-merkkauskieltä, joka kuljetetaan HTTP- tai SMTP-protokollan avulla, jolloin puhutaan termistä “SOAP over HTTP”. [4, s. 35]

SNMP (*eng. Simple Network Management Protocol*) on verkon hallintaan käytettävä protokolla. SNMP perustuu manageriin ja agenttiin, jossa agentin tilaa voidaan kysyä tai vaihtoehtoisesti agentti voi tiedottaa tilasta tai muutoksesta lähettämällä managerille trap-viestejä. SNMP:n perustoimintaa kuvaillaan kuvassa 6. SNMP:stä on olemassa kolme eri versiota ja ne ovat versioitu SNMPv1, SNMPv2 ja SNMPv3. Versioiden kehittämisessä on pyritty turvallisuuden parantamiseen, ja SNMPv3 tukee autentikointia ja salausta. [25][26, s. 4 – 5]



Kuva 6. *SNMP:n toimintaa havainnollistava kuva. (mukaillen[25])*

RSYSLOG- (*eng. rocket-fast system for log processing*) ja RELP-protokolla (*eng. Reliable Event Logging Protocol*) ovat Syslog-protokollasta laajennettuja versiota, joita voidaan kuljettaa TCP-prokollan kanssa. RSYSLOG tarjoaa parempaa suorituskykyä ja parempia tietoturvallisuus-ominaisuuksia verrattuna perinteisiin Syslog-protokollaan. [27][28]

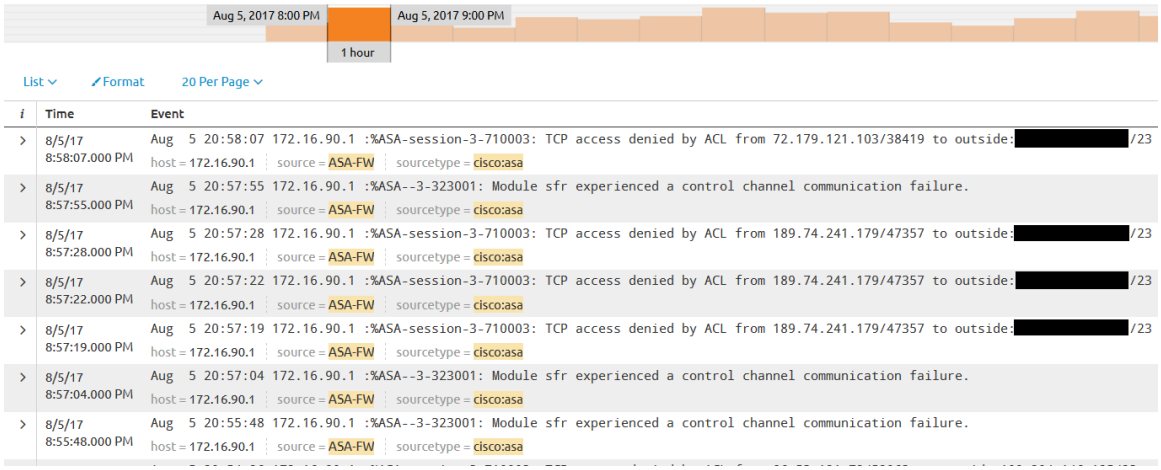
Keskitetyn lokienkeräys-järjestelmän kanssa saattaa tulla tilanne, jossa lokienkeräin ei ole saatavilla ja silloin lokiviestit menetetään. RSYSLOG tarjoaa mahdollisuuden konfiguroida kahdennetun syslog-viestien toimittamisen, josta puhutaan englanniksi termillä ”Failover Syslog Server”. Jotta kahdesta Syslog-palvelimen määrityksestä päästäisiin hyötymään, tarvitsisi lokiviestit kuljettaa TCP-protokollan kanssa, jolloin mahdollinen käyttökatko havaittaisiin ja sekundaarinen Syslog-palvelin otettaisiin käyttöön. [28]

3.3 Lokien visualisointi

Tässä aliluvussa käsitellään lokien visualisointia ja sen avulla poikkeavuuksien havainnointia lokidatasta. Yksinkertainen esimerkki lokien visualisoinnista on tail-komento Linux-järjestelmässä. Kuvassa 7 on kuvakaappaus tail-komennon tuottamasta tuloksesta. Lokidatan ja laitteiden lisääntyessä visualisointi monimutkaistuu ja niin se sopiikin pienelle lokimäärälle. Lokimäärän kasvaessa visualisointi voi kuitenkin vaatia lokien keräämisen yhteen pisteeseen, jossa tulevia tapahtumia voidaan tarkastella. Lokien visualisointia voi tehdä jälkikäteen kerätystä lokimassasta tai reaaliajassa tietyin rajoituksin, tapahtumien kokonaiskuvan hahmottaminen voi vaatia palaamisen reaaliajassa taaksepäin. Myös SIEM-järjestelmät voivat tarjota lokien visualisointiin omia työkalujaan, kuten esimerkiksi kuvassa 8 on havainnollistettu. [4, s. 219 – 220]

```
root@PRODSRV01:~# tail -f /var/log/syslog
Aug  6 12:44:58 PRODSRV01 /etc/mysql/debian-start[1170]: /usr/bin/mysql_upgrade:
 the '--basedir' option is always ignored
Aug  6 12:44:58 PRODSRV01 /etc/mysql/debian-start[1170]: Looking for 'mysql' as:
 /usr/bin/mysql
Aug  6 12:44:58 PRODSRV01 /etc/mysql/debian-start[1170]: Looking for 'mysqlcheck
' as: /usr/bin/mysqlcheck
Aug  6 12:44:58 PRODSRV01 /etc/mysql/debian-start[1170]: This installation of My
SQL is already upgraded to 5.5.46, use --force if you still need to run mysql_up
grade
```

Kuva 7. *Lokien visualisointi tail-komennolla.*



Kuva 8. *Lokien visualisointi Splunk-järjestelmässä.*

3.4 Lokijärjestelmään kohdistuvat uhat

Lokiviestien käsittelyssä nojataan lokidatan eheyteen, jonka toteutumisessa on erityisen tärkeässä roolissa pääsynhallinta lokidataan. Lokidata ei saa muuttua eikä sitä saa päästää tuhoutumaan. Uhka voi olla ulkopuolinen hakkeri tai sisäpuolelta esimerkiksi järjestelmän ylläpitäjä. Hakkerin tärkein motiivi lokitietojen peukaloinnin suhteen on hänen jälkiensä peittäminen ja todisteiden hävittäminen. Toisaalta hakkeri voi hyötyä lokidatan sisällöstä hyökätessään toisiin järjestelmiin. [4, s. 305 – 306]

Hyökkäys voi kohdistua lokidatan lähteeseen, lokidatan siirtoon verkossa tai lokidatan kerääjään. Hyökkäyksen kohteena voi myös olla tietokanta, jossa lokitietoja keskitetysti säilytetään tai lokidatan analysointiprosessi. Tietoturvallisuuden tiedon kolme ominaisuutta pätee lokidatankin suhteen, luottamuksellisuudella hakkerin mahdollisuutta lukea lokiviestejä, eheydellä peukaloida sisältöä ja toisaalta saatavuudella estää lokiviestin poistaminen. Hyökkäys voi yksinkertaisimmillaan olla esimerkiksi tietoverkon kuormittaminen niin, että lokiviestin saapuminen perille estyy. [4, s. 306 – 307]

3.5 Lokipolitiikka

Lokiviestit auttavat järjestelmien ylläpitäjiä seuraamaan järjestelmän toimintaa ja niiden avulla voidaan keventää vianselvitystä. Lokiviestit avustavat myös käyttäjien oikeusturvan toteutumista. Lokien kerääminen, säilytys ja seuranta tulee olla suunnitelmallista, toteuttaa tietoturvallisuus ja tietosuoja huomioiden, ja hyvien käytännön mukaisesti lokien käsittelystä tulisi määrittää lokipolitiikka. [23, s. 13, 45]

Lokien käsittelyssä tulee ottaa huomioon lokiviestin sisältö, koska ne saattavat sisältää henkilö- tai tunnistamistietoja, jolloin niiden käsittelyä on rajattu laeissa. Lokitietojen käsittelyn säätelyyn kohdistuvat muun muassa henkilötietolaki, sähköisen viestinnän tietosuojalaki ja työelämän tietosuojalain velvoitteet. [23, s. 31, 33]

Lokien käsittelyllä tarkoitetaan eri lokien liittyviä toimenpiteitä, joita ovat lokien kerääminen, analysointi, säilyttäminen, luovuttaminen ja poistaminen tai arkistointi. Lokien käsittelyn tulisi perustua määritettyyn tarpeeseen ja analysointien pohjalta tehtävien toimenpiteiden pitäisi olla ennalta määritettyjä. Lokien analysointijärjestelmät tukevat lokiviestin analysointia, mutta analysointi ei saisi pohjautua pelkästään järjestelmän toimintaan. [23, s. 19]

Kuten tietoturvapolitiikassa, myös lokipolitiikassa tulee määritellä roolit, vastuut, toimintatavat ja prosessit lokien käsittelyyn. Lokipolitiikka pitää sisällään teknisten asioiden ja ratkaisuiden määrittelyn lisäksi vastuut ja velvollisuudet. VAHTI Lokiohje 03/2009 tuo esille asioita joita kunkin organisaation tason tulisi ottaa huomioon. Organisaation ylimmälle johdolle, tietohallinnolle, tietoturvavastaavalle, henkilöstöhallinnolle on listattu asioita, joiden mukaan lokipolitiikkaa olisi hyvä määrittää ottaen huomioon lainsäädännöt ja muut vaatimusympäristöjen käsittelyssä olevat hyvät käytännöt. [23, s. 43 – 45]

Esimerkiksi ylimmälle johdolle on listattuna muun muassa ”vaatimuksien tunnistus”, ”suojaustarpeet ja tavat”, ”käsittelytavat ja vastuut”. Tietohallinnon tulisi seurata järjestelmien toimintaan ja kapasiteettiin liittyviä lokeja sekä seurata määritettyjen lokiviestien syntyä ja säilöntää. Tietoturvavastaava tai tietoturvaorganisaation tulisi seurata ylläpitäjien toimintaa sekä seurata lokeja tietoturvallisuuden huolehtimiseksi. Lisäksi tietoturvarikkomuksien selvitys, auditointien teettäminen lokitietojen suojauksen todenta-

miseksi ja ylimmän johdon avustaminen kuuluvat tietoturvavastaavan tai tietoturvaorganisaation toimenkuvaan. Lokitietojen suojaamiseen liittyy myös käyttöoikeuksien määritys, toisin sanoen kuka saa nähdä ja käsitellä lokitietoja. Henkilöstöhallinto voi olla vastuussa käyttöoikeuksien hallinnasta, mutta käyttöoikeuksien hyväksynnät voivat tulla järjestelmän omistajan tai sovelluksen pääkäyttäjän kautta. Myös ulkoistuksiin liittyvät oleellisena osana lokitietojen vaatimukset ja määrittelyt. [23, s. 43 – 46]

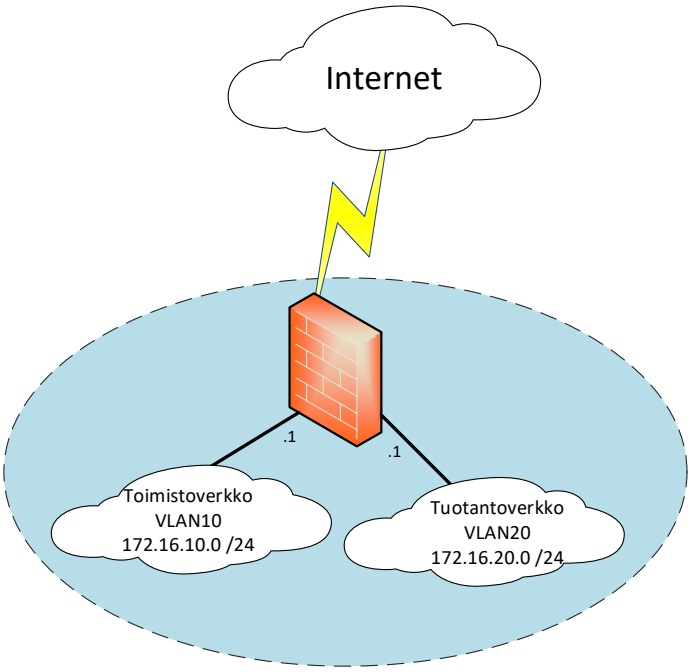
4. LÄHTÖTILANTEEN KARTOITUS JA HALLINTAVERKON ERIYTYS

Diplomityön käytännön toteutusvaiheen alussa tehtiin kartoitus, jossa hyödynnettiin testejä, kuten avoimien TCP- porttien skannausta ja liikenteen kaappausta sekä tutkittiin järjestelmästä valmiina olevia dokumentaatioita ja järjestelmäkuvauksia. Lisäksi toteutusvaiheen pohjalta tavoitteena oli pyrkiä luomaan havainnollistavia ja hyödynnettäviä dokumentteja muun muassa verkkotopologista ja kytkennöistä.

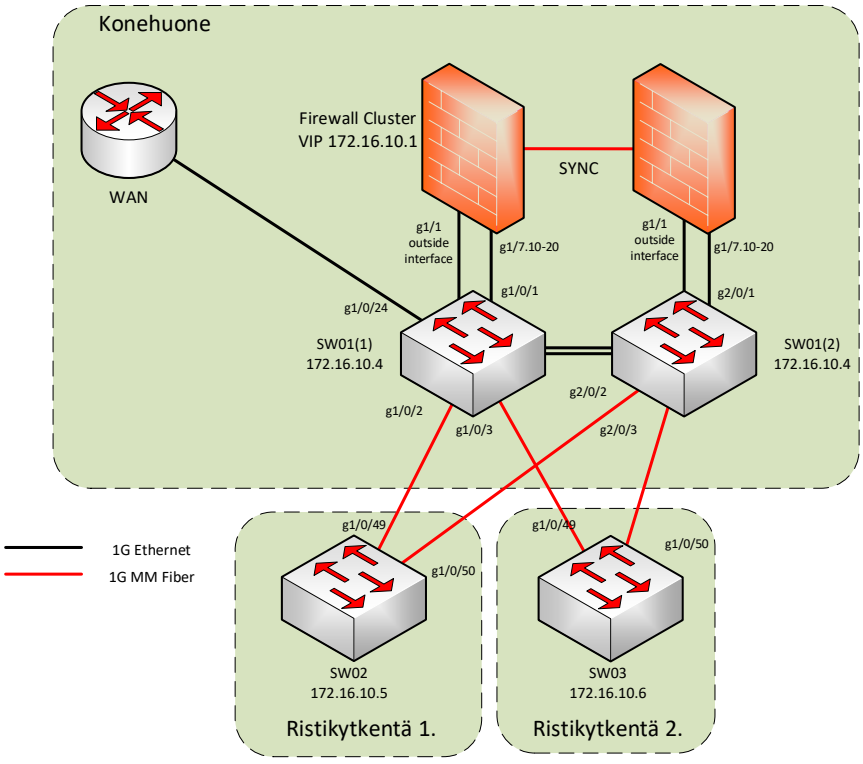
Tietoturvan tilannetietoisuuden kannalta tärkeässä roolissa on ympäristön tunteminen, jotta mahdollisiin ongelmiin ja poikkeavuuksiin pystyttäisiin reagoimaan. Määrittely kohdistettiin teknologioihin ja siinä pyrittiin käymään läpi tietoverkon aktiivilaitteet, palvelimet, kriittiset tuotannolliset työasemat sekä mahdolliset muut laitteet, jotka ovat verkkoon kytkettyinä. Tässä luvussa käydään lisäksi kartoituksessa hyväksi käytettyjen menetelmien teoriaa.

4.1 Verkko

Diplomityössä tutkittava verkko koostuu yhdestä toimipisteestä, jonka sisäverkko on jaettu toimisto- ja tuotantoverkkoon, jotka ovat erotettuina Internetistä palomuurilla. Liikenne näiden verkkojen välillä reititetään palomuurissa. Kuvassa 9 kuvaillaan organisaation verkon L3-topologiaa. Toimipisteen lähiverkko koostuu kahdesta runkokytkimestä, jotka ovat pinossa ja näkyvät loogisesti yhtenä laitteena. Lisäksi ristikytkentäkaappeja on kaksi kappaletta ja niissä on molemmissa yhdet kytkimet, joista on kahdennetut monimuotovalokuitu yhteydet runkokytkimiin. Kuvassa 10 havainnollistetaan organisaation verkon L2-topologiaa.



Kuva 9. *Havainnollistava L3-topologia kuva.*

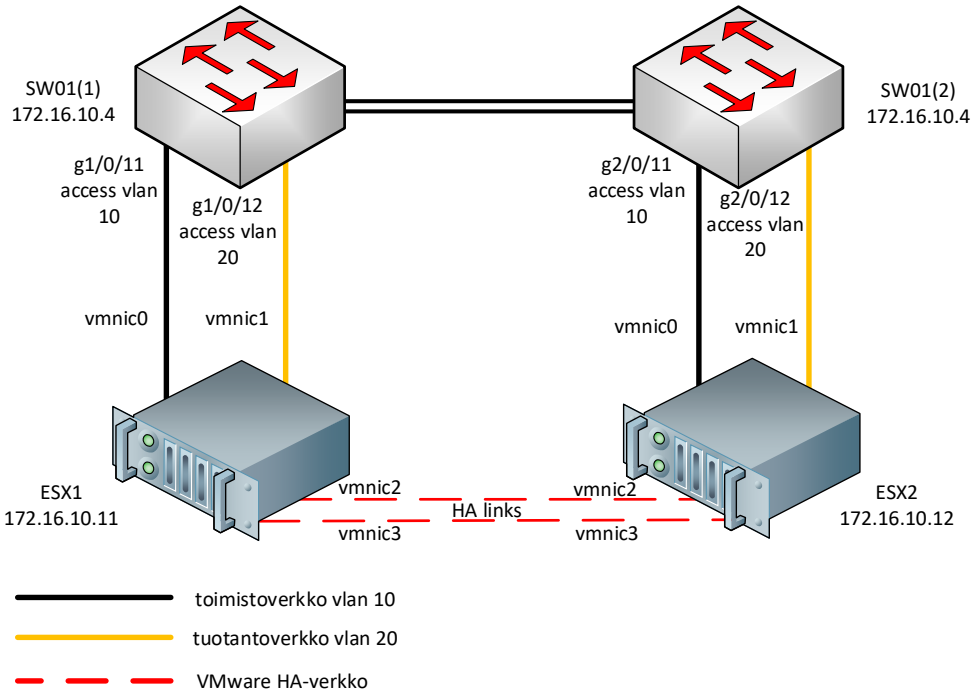


Kuva 10. *Toimipisteen L2-topologian havainnollistava kuva.*

4.2 Palvelimet

Toimipisteen sovellus- ja tukipalvelimet ovat virtuaalisina kahdennetussa VMware-virtualisointialustassa. Virtuaalipalvelimet ovat pääasiassa Windows Server -käyttöjärjestelmillä, joiden lisäksi on muutamia Linux-palvelimia. Tässä diplomityössä tehtiin kaksi uutta virtuaalipalvelinta, jotka sijoitettiin samaan virtualisointialustaan.

Virtualisointialustaan on kytkettynä molemmat toimipisteen verkon runkokytkimet access-portteina. VMwaren käyttämä High Availability -liikenne kuljetetaan fyysisesti myös runkokytkimien kautta, mutta kuvaan ne ovat piirrettynä kuin ne loogisesti toimivat, toisin sanoen ne näkevät vain toisensa.



Kuva 11. *VMware-palvelinympäristön verkkokytkennät.*

4.3 Verkkoon kytkettyjen laitteiden selvittäminen

Kartoituksen tarkoituksena on selvittää, mitä kaikkea halutaan valvoa ja havaita mahdolliset poikkeavuudet heti alussa. Kartoituksessa käytetään hyväksi penetraatiotestauksen alkupään vaiheita, koska niiden avulla päästään selville verkkoon kytketyistä laitteista ja niiden palveluista. Seuraavaksi käsitellään penetraatiotestauksen tiedustelun ja skannauksen periaatteita, koska niitä voidaan hyödyntää organisaation ympäristön kartoituksessa. Tässä diplomityössä ei kuitenkaan toteuteta penetraatiotestausta kokonaisuudessa, johon kuuluisi tiedustelun ja skannauksien lisäksi järjestelmän kaappaaminen ja kaappauksen ylläpitäminen.

Tietoturvan teknillisestä testauksesta on käytössä monenlaisia termejä esimerkkeinä eettinen hakkerointi, penetraatiotestaus ja haavoittuvuustestaus. Penetraatiotestauksessa selvitetään, kuinka testattavana oleva kohde on huolehtinut ennaltaehkäisystä ja havaitsemisesta. Sen avulla voidaan selvittää, löytyykö järjestelmistä hyödynnettävissä olevia haavoittuvuuksia. [18, s. 91 – 92, 116]

Penetraatiotestauksen ensimmäinen vaihe on tiedustelu (*eng. Reconnaissance)*, jossa penetraatiotestaukseen valmistaudutaan keräämällä mahdollisimman paljon erilaista tietoa testattavasta kohteesta. Tiedustelua voidaan toteuttaa esimerkiksi erilaisilla ilmaisilla työkaluilla, joiden avulla voidaan saada selville isäntänimiä, IP-osoitteita ja niin edelleen. Tallaista tiedostelua kutsutaan passiiviseksi tiedusteluksi ja siinä käytettävissä olevia työkaluja ovat esimerkiksi nslookup ja dig. Passiivista tiedustelua voidaan tukea aktiivisella tiedustelulla, jossa otetaan yhteyttä suoraan testattavaan kohteeseen, yksi tehokkaimmista keinoista on ”Social Engineering”. [29, s. 151 – 158, 172]

Tässä diplomityössä ei suoranaisesti käytetä penetraatiotestauksen tiedusteluvaiheen menetelmiä. Tiedustelu perustuu tässä tapauksessa toimeksiantajan olemassa olevien dokumentaatioiden tutkimiseen ja perehtymiseen, jotka edesauttavat tietoturvan tilannetietoisuuteen tähtäävien järjestelmien määrittelyä ja käyttöönottoa.

Tiedustelun jälkeen seuraa skannausvaihe (*eng. Scanning*), jossa penetraatiotestaaja selvittää lisää testattavasta kohteesta esimerkiksi löytämiensä IP-osoitteiden avulla. Vaiheesta käytetään myös nimitystä haavoittuvuustunnistus (*eng. Vulnerability Identification*). Skannausvaiheessa selvitetään, onko kohdejärjestelmä vielä olemassa ja saatavilla, onko se kykeneväinen kommunikoimaan penetraatiotestaajan kanssa.

Skannausvaiheen avulla saadaan selville avoimet portit ja palvelut porttiskannauksella. Lisäksi voidaan hyödyntää olemassa olevia haavoittuvuusskannauksia, jos haluttaisiin saada palveluista selville, löytyykö niistä haavoittuvuuksia. Valmiiden haavoittuvuusskannausohjelmien ongelmana on satojen sivujen listat haavoittuvuuksista, joita ei kuitenkaan pystyisi todellisuudessa käyttämään hyväksi. [18, s. 101] [30, s. 53 – 55]

Skannauksia varten on olemassa ilmaisia työkaluja, joista avoimeen lähdekoodiin perustava Nmap on tehokas tietoverkon havainnointiin ja tietoturva-auditointiin käytettävä työkalu. Komentorivipohjaisen Nmap-version lisäksi on myös saatavilla graafisella käyttöliittmällä varustellu versio Zenmap.

Tässä diplomityössä hyödynnettiin Zenmap-työkalua, jonka skannausominaisuuksia käytettiin hyväksi havaitsemaan verkkoon kytkettyjä laitteita. Skannauksien avulla saatiin mahdollisimman laaja otanta. Skannausta tulisi tehdä myös jatkossa tietyin väliajoin ja päivittää sekä vertailla asennettujen palveluiden versioita ja näin ollen saada korjattua mahdollisimman hyvin löydetyt haavoittuvuudet. Käytettyjen ohjelmaversioiden perusteella voi hakea olemassa olevia haavoittuvuuksia esimerkiksi Exploit DB:stä. Kuvassa

12 esimerkkinä tuotantoverkon palvelimesta avoimet portit, jotka Zenmap työkalulla pystyy jäljittämään komennolla *nmap –A <target ip>*.

```
Nmap scan report for 172.16.20.5
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
```

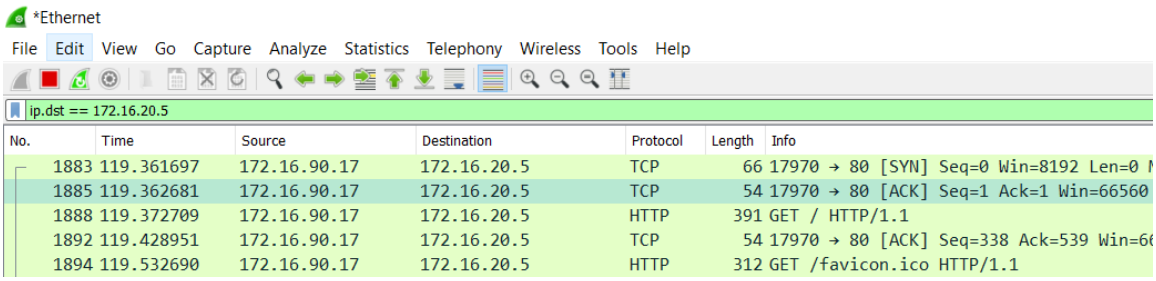
Kuva 12. *Zenmap-työkalulla havaitut Linux-palvelimen portit*

4.4 Verkkoliikenteen analysointi

Wireshark on verkkoliikenteen analysointiin tarkoitettu avoimen lähdekoodin työkalu, jonka avulla pystytään tarkastelemaan IP-pakettien sisältöä. Wiresharkin avustuksella voi esimerkiksi selvittää järjestelmien välisiä liityntöjä. Tässä diplomityössä päädyttiin tekemään yksi Wireshark pakettikaappaus, toisin sanoen tietyn hetken ajan kaikki liikenne otettiin talteen, ja sitä pystyttiin tutkimaan jälkeenpäin. Tcpdump toteutettiin runkokytkimen aktiiviseen porttiin, joka on kytkettynä palomuuriin. Liikenne monitoroitiin molempiin suuntiin. Monitorointia varten kytkimeen konfigurointiin väliaikaisesti portti, jota halutaan monitoroida ja tämän lisäksi portti, johon liikenne kopioidaan ja Wireshark-ohjelmiston omaava tietokone kytketään.

```
SW01(config)# monitor session 1 source interface gigabitethernet 1/0/1
SW01(config)# monitor session 1 destination interface gigabitethernet 1/0/18
encapsulation dot1q
```

Wireshark tcpdumpista voidaan rajata osumia esimerkiksi kohde IP-osoitteen mukaan. Seuraavassa kuvassa 13 on esimerkki Wireshark tcpdumpista ja kohde IP-osoitteen perusteella tehdystä rajauksesta.

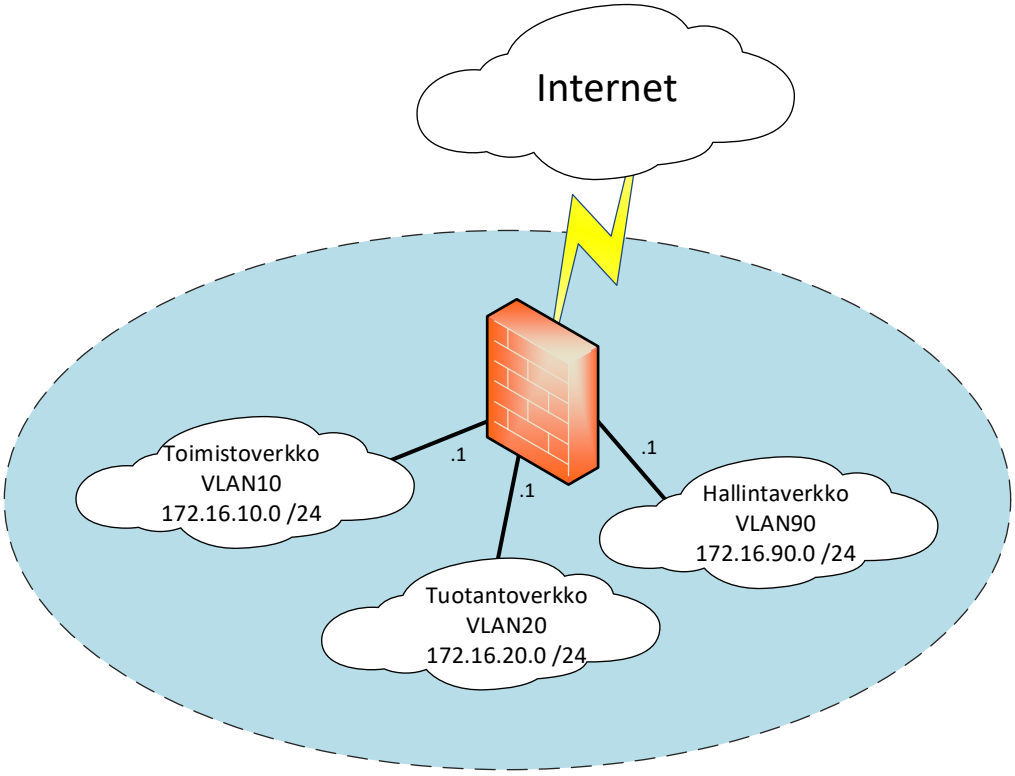


Kuva 13. *Wireshark kuvakaappaus.*

Valvottavia ja tutkittavia kohteita päätettiin rajata, jotta diplomityön laajuus pysyisi hallittavassa laajuudessa. Näin ollen päätettiin, että keskitytään verkon aktiivilaitteisiin, VMware virtualisointialustaan sekä kahteen virtuaalipalvelimeen. Tulevaisuudessa toimeksiantaja voi halutessaan lisätä valvonnan piiriin lisää kohteita, kuten varmistusratkaisut, sovelluksien tapahtumat ja identiteetin hallintajärjestelmän.

4.5 Hallintaverkon eriyttäminen

Diplomityössä toteutettavia järjestelmien käyttöönottoa varten toteutettiin erillinen hallintaverkko, jonka avulla pystytään rajaamaan liikennettä ja turvaamaan käyttöönotettavia järjestelmiä sekä muun muassa verkkolaitteiden hallintayhteyksiä. Hallintaverkkoa varten tarvittiin uusi osoitealue, VLAN ID ja palomuuriin uusi liityntäportti. Hallintaverkon osoitealueeksi valittiin 172.16.90.0 /24 ja VLAN ID:ksi 90.



Kuva 14. *L3-topologia uuden hallintaverkon myötä.*

4.5.1 Kytkimien ja palomuurin muutokset

Lähiverkon kytkimiin konfigurointiin uusi hallinta-VLAN, lisättiin uudet hallintaosoitteet, määritettiin uusi oletusyhdyskäytävä sekä poistettiin vanha hallintaosoite toimisto-VLANista. Alla konfigurointikäskyt esimerkkinä runkokytkimestä:

```
SW01(config)# vlan 90
SW01(config-vlan)# name Hallintaverkko
SW01(config-vlan)# ip address 172.16.90.11 255.255.255.0
SW01(config-vlan)# exit
SW01(config)# no ip default-gateway 172.16.10.1
SW01(config)# ip default-gateway 172.16.90.1
SW01(config)# vlan 10
SW01(config-vlan)# no ip address 172.16.10.11 255.255.255.0
SW01(config-vlan)# exit
```

Ciscon ASA-palomuuriklusteriin lisättiin uusi aliliityntäportti. Muutoksesta ei aiheutunut käyttökatkoa ja se pystyttiin tekemään tuotantokäytössä. Konfiguraatiot uuden aliliityntäportin käyttöönotosta:

```
ASA(config)# interface GigabitEthernet1/7.90
ASA(config-subif)# vlan 90
ASA(config-subif)#  nameif Hallintaverkko
ASA(config-subif)#  security-level 95
ASA(config-subif)#  ip address 172.16.90.1 255.255.255.0
```

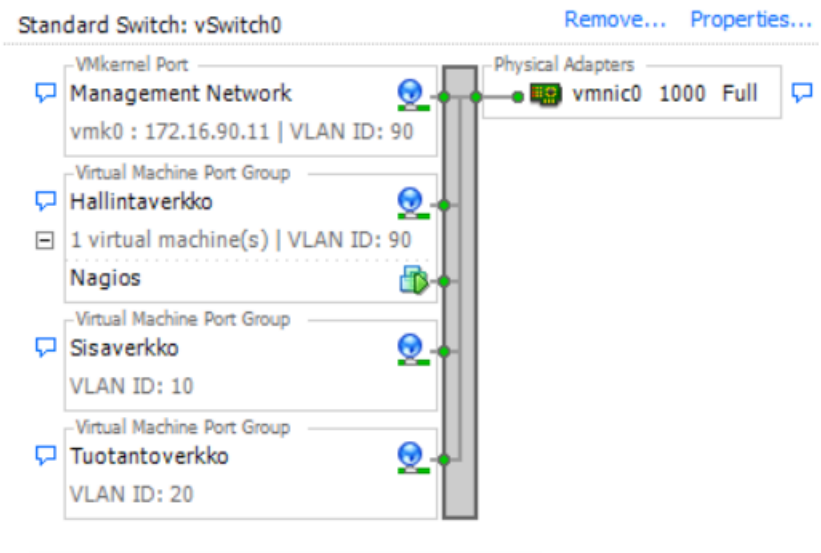
4.5.2 VMware vCenter hallintaverkon lisäys ja hallintaosoitteiden muutokset

Virtualisointialustan host-koneiden liityntäportteja muutettiin niin, että niissä kuljetetaan VLAN-tagit. Standard vSwitchein lisättiin VLAN-tagit, jolloin eri virtuaaliset verkot kuljetetaan samaa fyysistä kaapelia pitkin. Samassa yhteydessä haluttiin lisätä redundanttisuutta, joten host-koneiden toiset fyysiset liityntäportit siirrettiin niin, että host-koneiden yhteydet tulevat molempien runkokytkimien kautta. Näin ollen toisen runkokytkimen vikaantuessa molemmat host-koneet olisivat toiminnassa edelleen. Muutoksia varten virtuaalipalvelimet siirrettiin ajoon toiselle host-koneelle, jotta muutokset päästiin tekemään huoletta tuotantoon vaikuttamatta.

Runkokytkimiin tehtiin myös VLANien kuljetusta varten tarvittavat määritykset:

```
SW01(config)# interface g1/0/11
SW01(config-if)# switchport trunk encapsulation dot1q
SW01(config-if)# switchport mode trunk
SW01(config-if)# switchport trunk allowed vlan 10,20,90
```

VMwaren hostien ja vCenterin hallintaosoitteet muutettiin uuteen hallintaverkkoon. Sitä varten osoitteet muutettiin konsolin kautta ja vCenterin Clusteriin jouduttiin määrittämään hostit uudelleen.



Kuva 15. *VLAN tagit ja uusi hallintaverkko lisättynä VMware ESXi hostin verkkomäärityksiin.*

4.5.3 Palomuurisäännöt

Uuden osoite-alueen käyttöönoton, muuttuneiden hallintaosoitteiden ja uusille palvelimille varattavien osoitteiden seurauksena dokumentaatioita tarvitsi päivittää ja tarvittavia palomuurisääntöjä suunnitella. Alla olevassa kuvassa on listattuna uudet osoitteet, jotka otettiin tämän diplomityön aikana käyttöön:

VLAN 90 - Hallintaverkko 172.16.90.0 / 24

IP-osoite	Nimi	Käyttöjärjestelmä
172.16.90.0	Verkon osoite	
172.16.90.1	ASA	
172.16.90.2		
172.16.90.3		
172.16.90.4	SW01	
172.16.90.5	SW02	
172.16.90.6	SW03	
172.16.90.7		
172.16.90.8		
172.16.90.9		
172.16.90.10	VCENTER	Windows Server 2012 R2
172.16.90.11	ESX1	VMware ESXi 6.0
172.16.90.12	ESX2	VMware ESXi 6.0
172.16.90.13	NAGIOS	CentOS 7
172.16.90.14	SPLUNK	CentOS 7
…		
…		
172.16.90.255	Broadcast	

Uutta hallintaverkkoa varten luotiin palomuurisääntöjä, joilla sallittiin vain tarpeellinen liikenne hallintaverkon ja toimisto- sekä tuotantoverkkojen välillä. Muihin palomuurisääntöihin ei perehdytty tässä diplomityössä. Kuvassa 16 on listattuna palomuurisäännöistä esimerkkejä, jotka diplomityön aikana otettiin käyttöön.

Palomuurisäännöt (SIEM käyttöönotto)			
Hallintaverkko			
Lähde	Kohde	Palvelu	Kuvaus
172.16.90.0/24	172.16.10.0/24 172.16.20.0/24	ICMP	ICMP:t hallintaverkosta toimisto- ja tuotantoverkkoon.
172.16.90.0/24	172.16.10.15 172.16.10.16	53	DNS-kyselyt nimipalvelimiin.
NAGIOS	172.16.10.0/24 172.16.20.0/24	12489	NSClient kyselyt palvelimien Agenteilta.
VCENTER	172.16.10.15 172.16.10.16	any	vCenter-palvelimelta domain controllereille.
Toimistoverkko			
172.16.10.0/24	VCENTER	3389	Sallitaan toimistoverkosta RDP hallintapalvelimelle.
172.16.10.13	SPLUNK	8089, 9998	Sallitaan SRV01-palvelimelta lokien toimitus.
Tuotantoverkko			
172.16.20.5	SPLUNK	8089, 9997	Sallitaan PRODSRV1-palvelimelta lokien toimitus.

Kuva 16. *Listaus palomuurisäännöistä.*

5. JÄRJESTELMIEN KÄYTTÖÖNOTTO

Tässä kappaleessa käsitellään käyttöönotettuja järjestelmiä sekä syvennytään, kuinka niiden käyttöönotto ja konfigurointi tapahtuivat. Tässä diplomityössä päädyttiin toteuttamaan Nagios-tuotteella verkkolaitteiden ja palvelimien kapasiteettien valvonta ja hälytykset sekä Splunk-tuotteella keskitetty lokien keräys, hallinta ja analysointi. Yksi perustelu Nagios- ja Splunk-tuotteiden valintaan oli saatavilla oleva yhteisö- ja valmistajatuki. Aiempi positiivinen kokemus työelämässäni Nagioksesta vaikutti myös sen valintaan. Splunkiin olen tutustunut opiskeluideni aikana aiemmin yhdellä kurssilla, jonka perusteella jäi halu perehtyä tuotteeseen lisää, joten siihen tuli hyvä mahdollisuus tässä diplomityössä.

5.1 Nagios

Nagios on Linux-pohjainen tuote, josta on saatavilla ilmainen avoimen lähdekoodin versio sekä maksullinen Nagios XI. Tämän diplomityön tavoitteisiin riitti mainiosti ilmainen Nagios Core, jossa on oleellisimmat monitorointi ja hälytys –ominaisuudet. Coren ominaisuuksia pystyy täydentämään ilmaisilla Nagios Plugineilla, joita on Nagioksen virallisia sekä yhteisön tekemiä.

Nagios Coressa on www-pohjainen käyttöliittymä, josta tapahtuu monitorointi ja isäntäkoneiden selaus. Nagiosta varten asennettiin uusi virtuaalipalvelin, johon valittiin käyttöjärjestelmäksi CentOS 7. Virtuaalipalvelimelle annettiin resursseiksi 1 CPU, 1 GB keskusmuistia, kiintolevyksi 20 GB ja verkkokortti uuteen hallintaverkkoon.

Nagios-valvontaan lisättiin verkosta tärkeimmät kytkimet ja niiden portit, toimistoverkon yksi kriittinen palvelin ja tuotannon kriittinen palvelin. Kohteet jaoteltiin ryhmiin (Firewalls, Switches, Windows-Servers ja Linux-Servers). Valvottavista laitteista ja niiden palveluista toteutettiin hälytykset sähköposti-ilmoituksina. Hälytyksiä olisi myös mahdollista laajentaa esimerkiksi testiviesteiksi, joita varten tarvittaisiin erillinen GSM-modeemi ja SIM-kortti.

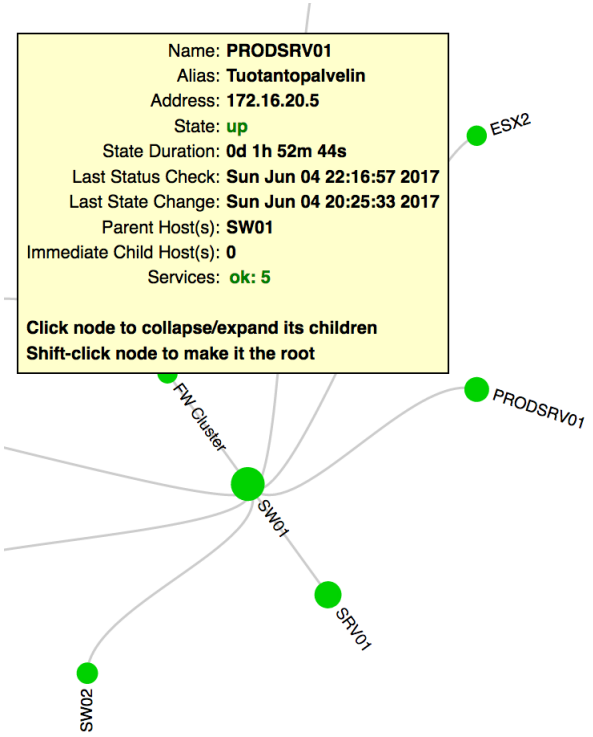
5.1.1 Verkkolaitteiden valvonta

Runkokytkimien porteista valvontaan lisättiin nousuyhteydet access-kytkimiin, yhteydet VMware ESXi -palvelimiin sekä Internet-liittymän WAN-reitittimelle kulkeva linkki. Kuvassa 17 on kuvakaappaus Nagioksen porttivalvonnan näkymästä.

SW01	PING	OK	06-04-2017 22:11:38	27d 2h 5m 19s	1/3
	Port g1/0/1 FW Cluster node1 uplink Link Status	OK	06-04-2017 22:09:07	0d 2h 45m 47s	1/3
	Port g1/0/1 SW03 uplink1 Link Status	OK	06-04-2017 22:11:13	0d 2h 43m 41s	1/3
	Port g1/0/11 ESX1 vmnic0 Link Status	OK	06-04-2017 22:14:00	0d 2h 50m 54s	1/3
	Port g1/0/12 ESX2 vnnic0 Link Status	OK	06-04-2017 22:09:53	0d 1h 35m 1s	1/3
	Port g1/0/2 SW02 uplink1 Link Status	OK	06-04-2017 22:13:19	0d 2h 41m 35s	1/3
	Port g1/0/24 WAN Link Status	OK	06-04-2017 22:07:45	0d 2h 47m 9s	1/3
	Port g2/0/1 FW Cluster node2 uplink Link Status	OK	06-04-2017 22:05:25	0d 2h 39m 29s	1/3
	Port g2/0/11 ESX1 vmnic1 Link Status	OK	06-04-2017 22:09:38	0d 2h 45m 16s	1/3
	Port g2/0/12 ESX2 vmnic0 Link Status	CRITICAL	06-04-2017 22:08:16	0d 2h 50m 38s	3/3
	Port g2/0/2 SW02 uplink2 Link Status	OK	06-04-2017 22:09:21	0d 2h 45m 33s	1/3
	Port g2/0/3 SW03 uplink2 Link Status	OK	06-04-2017 22:11:27	0d 2h 43m 27s	1/3
	Uptime	OK	06-04-2017 22:06:36	27d 2h 3m 35s	1/3

Kuva 17. *SW01 kytkimen porttien valvonta.*

Nagios-objekteihin pyrittiin määrittämään ”parents”–määritys, jonka avulla verkon rakenteesta tulee todellisen rakenteen mukainen. Todellisen rakenteen avulla havaitaan millä verkon tasolla ongelma on ja todellisen rakenteen avulla myös mahdolliset hälytykset tulevat sen mukaan. Lisäksi Nagioksessa sisäänrakennettuna oleva kartta isäntäkoneista muodostuu todellisen loogisen kytkennän mukaisesti, kuten kuva 18 esittää.



Kuva 18. *Parents-määritys*

5.1.2 Windows-palvelimen valvonta

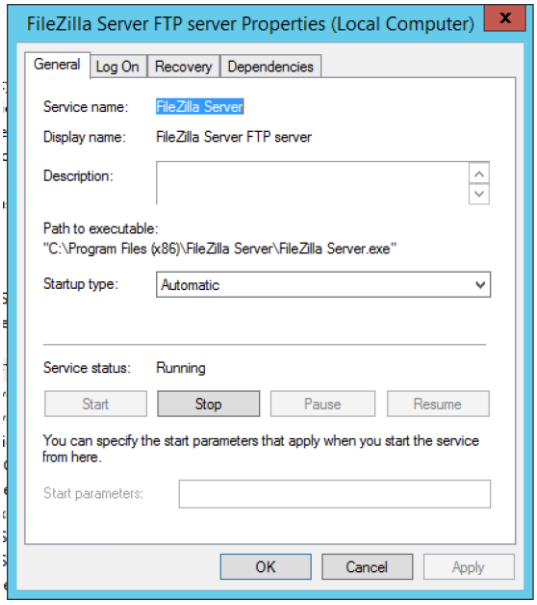
Windows-palvelimesta pystytään valvomaan mm. prosessorin käyttöä, muistin käyttöä, levytilojen määriä ja palvelimen palveluita. Tässä työssä päädyttiin valvomaan yhtä

Windows-palvelinta. Toiminnan kannalta yksi kriittisimmistä on palvelimen vapaa levytila sekä FTP Server –palvelu. Levytilan valvonnassa määritettiin varoitustasoksi 80% ja kriittiseksi tasoksi 90%. Nagioksessa levytilan valvonta konfiguroitiin tässä tapauksessa windows.cfg –tiedostossa, jonne luotiin uusi ”Define Service” alla listattujen parametrien mukaisesti:

 # SRV01-palvelimen C-levyn valvonta

```
defice service {
      use                     generic-service
      hostname                SRV01
      service_description     C:\ Drive Space
      check_command           check_nt!USEDDISKSPACE | -l c –w 80 – c 90
}
```

SRV01-palvelimessa on FTP Server -palvelu, jonka toimintaa haluttiin valvoa. Windows-palvelun valvontaa varten tarvitsee tietää palvelun nimi, jota Nagioksen konfiguraatiossa käytetään. Kuvassa 19 on kuvakaappaus esimerkiksi FileZillan FTP Server –palvelusta. Kuvan 19 alapuolella on tarvittavat parametrit listattuna, joiden avulla Windows-palvelimen palvelua voidaan valvoa.



Kuva 19. *Filezilla FTP Server -palvelu.*

 # SRV01-palvelimen FileZillan valvonta

```
defice service {
      use                     generic-service
      hostname                SRV01
      service_description     FTP Server -palvelu
      check_command           check_nt!SERVICESTATE! -d SHOWALL -l Filezilla
                              Server
}
```

Kuvassa 20 on kuvakaappaus Windows-palvelimen valvottavista kohteista, joissa näkyy valvottavan kohteen tila ja informaatiota. Etenkin levytilan valvonta koettiin hyödylliseksi ja informatiiviseksi. Isäntien listaus antaa rajapinnan laajemmalle havainnoinnille, ja sen hyödynnettävyys korostuu valvottavien palvelimien lisääntyessä. Rajapinta mahdollistaa proaktiivisen työskentelyn nopeutumisen, esimerkiksi levytilan alkaessa vähentyä.

OK	08-28-2017 22:22:30	85d 0h 13m 19s	1/3	c: - total: 59.66 Gb - used: 24.37 Gb (41%) - free 35.29 Gb (59%)
OK	08-28-2017 22:14:28	5d 5h 0m 35s	1/3	CPU Load 73% (5 min average)
OK	08-28-2017 22:26:26	5d 6h 18m 37s	1/3	D: - total: 120.00 Gb - used: 27.89 Gb (23%) - free 92.10 Gb (77%)
OK	08-28-2017 22:22:25	0d 0h 6m 46s	1/3	FileZilla Server: Started
OK	08-28-2017 22:22:41	85d 0h 39m 46s	1/3	Memory usage: total:4799.46 MB - used: 1998.94 MB (42%) - free: 2800.52 MB (58%)
OK	08-28-2017 22:14:40	85d 0h 13m 26s	1/3	NSClient++ 0.5.0.62 2016-09-14
OK	08-28-2017 22:26:38	85d 0h 21m 6s	1/3	System Uptime - 0 day(s) 0 hour(s) 7 minute(s)

Kuva 20. *SRV01-palvelimen valvottavat kohteet.*

5.1.3 Linux-palvelimen valvonta

Tuotantopalvelimesta haluttiin valvoa muun muassa levytilan käyttöä ja Apache-palvelun käynnissä oloa. Lisäksi päätettiin valvoa kokonaisprosessien määrää, jotka olivat tässä tapauksessa vakioituneet. Kokonaisprosessien määrän valvonnalla haluttiin havaitanormaalista poikkeavaa prosessien määrää. Hälytysrajat määritettiin prosessimäärien mukaan niin, että normaalista poikkeavasta määrästä yhden kasvu aiheuttaa varoituksen ja kahden prosessimäärän kasvu kriittisen hälytyksen. Tarvittavat määritykset ovat listattuna alla ja kuvassa 21 kuvakaappaus Nagioksen PRODSRV01-palvelimen näkymästä.

 # PRODSRV01-palvelimen prossien maara

```
defice service {
      use                     generic-service
      hostname                PRODSRV01
      service_description     Total Processes
      check_command           check_local_procs!38!39RSZDT
}
```

OK	08-28-2017 20:25:54	85d 0h 4m 35s	1/4	OK - load average: 0.07, 0.22, 0.15
OK	08-28-2017 20:27:18	43d 6h 35m 1s	1/4	DISK OK - free space: / 15707 MB (90.30% inode=99%):
OK	08-28-2017 20:29:15	5d 5h 7m 40s	1/4	HTTP OK: HTTP/1.1 200 OK - 568 bytes in 0.006 second response time
OK	08-28-2017 20:26:11	5d 5h 7m 23s	1/4	PING OK - Packet loss = 0%, RTA = 1.13 ms
OK	08-28-2017 20:27:34	0d 0h 2m 30s	1/4	PROCS OK: 38 processes with STATE = RSZDT

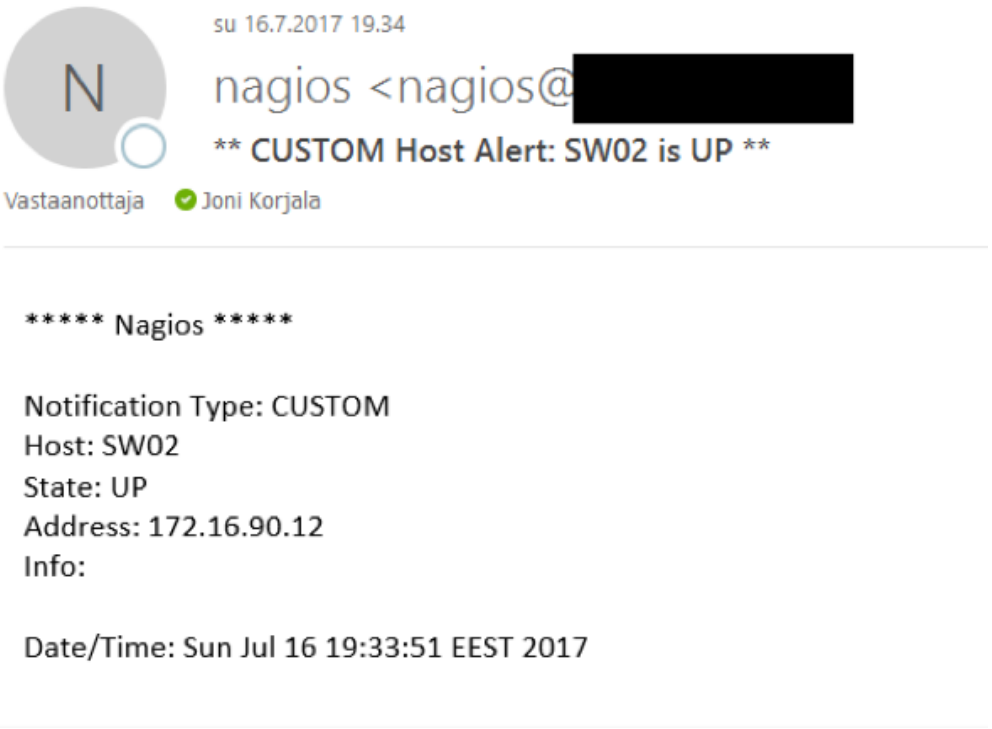
Kuva 21. *Tuotannon Linux-palvelimen valvottavat kohteet.*

5.1.4 Hälytykset

Hälytyksiä varten määritettiin kontaktit, joille hälytykset välitetään eteenpäin. Konfiguraatioissa on mahdollista määrittää muun muassa eri aikataulut ja vastaanottoja esimerkiksi toimistoaikoina tietyille vastaanottajille ja muina aikoina esimerkiksi päivystysryhmälle. Sähköpostihälytyksiä varten jouduttiin tekemään määrityksiä sähköpostipalvelimeen, jossa sallittiin Nagioksen lähettää sähköpostia ulkopuolisiin osoitteisiin. Alapuolella on esimerkki konfiguraatioista, jota käytin hälytyksien testauksessa.

```
defice contact {
      contact_name                  nagiosadmin
      alias                         Nagios Admin Joni
      service_notification_period   24x7
      host_notification_period      24x7
      service_notification_commands notify-service-by-email
      host_notification_commands    notify-host-by-email
      email                         etunimi.sukunimi@domainisi.fi
}
```

Sähköpostihälytyksen muotoa ja sen sisältöä pystyy muokkaamaan haluamakseen, tässä diplomityössä päädyttiin käyttämään Nagioksen oletuksena tarjoamaa muotoilua ja informaation sisältöä, jossa mielestäni tärkeimpinä isäntäkoneen nimi, IP-osoite ja tapahtuman kuvaus. Kuvassa 22 on esimerkki testihälytyksestä yhdestä lähiverkon kytkimestä:


su 16.7.2017 19.34

N

nagios <nagios@[redacted]

** CUSTOM Host Alert: SW02 is UP **

Vastaanottaja Joni Korjala

***** Nagios *****

Notification Type: CUSTOM
Host: SW02
State: UP
Address: 172.16.90.12
Info:

Date/Time: Sun Jul 16 19:33:51 EEST 2017

Kuva 22. *Nagioksen testihälytys.*

Nagiosta parannettiin vielä sen verran, että selaimen istunnot tapahtuvat ainoastaan HTTPS-yhteydellä, joten näin sen paikalliset tunnukset kulkevat salattuna käyttäjän päätelaitteelta palvelimelle. HTTPS-kirjautuminen toteutettiin itseallekirjoitetulla sertifikaatilla ja määritykset tehtiin Apachen konfiguraatioihin.

5.2 Splunk

Splunk on ohjelmisto, joka mahdollistaa lokien keräyksen eri laitteista ja järjestelmistä. Lokien keräyksen lisäksi Splunkissa on muitakin toiminnollisuuksia. Tässä diplomityössä perehdyttiin lokien visualisointiin ja analysointiin. Splunk-ohjelmistoon on saatavilla yleisimpien laitavalmistajien tuotteisiin räätälöityjä laajennuksia, kuten esimerkiksi Ciscon ja Paloalton palomuureihin tarkoitettuja.

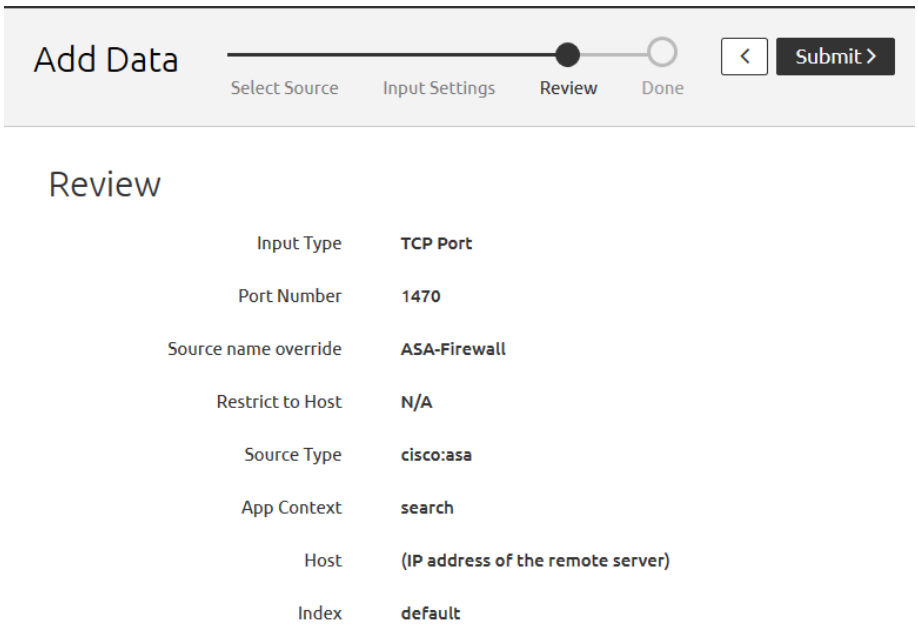
Splunk voidaan asentaa joko Windows- tai Linux-pohjaiselle alustalle. Tässä diplomityössä päädyttiin asentamaan Splunk CentOS 7 -käyttöjärjestelmälle. Asennusta varten tarvittiin uusi virtuaalipalvelin, jolle annettiin resursseiksi 1 CPU, 2 GB keskusmuistia ja 40 GB kiintolevyä. Nagios-palvelimen mukaisesti tämäkin virtuaalipalvelin liitettiin hallintaverkkoon.

Splunk tarjoaa eri laajuisia versioita ja tämän diplomityön tarpeiden pohjalta valittiin versio Splunk Light. Ohjelmiston valmistaja tarjosi ohjeet ohjelmiston asennukseen, joiden pohjalta Splunk saatiin asennettua CentOS 7 -käyttöjärjestelmälle. Oletuksena Splunkin web-pohjainen hallinta tapahtuu HTTP-protokollan kautta ja tämä päädyttiin heti muuttamaan HTTPS-protokollaksi käyttäen itseallekirjoitettua sertifikaattia. Cen-

toksen omasta palomuurista tarvitsi avata HTTPS liikenne, jotta web-pohjaiseen hallintaliittymään päästiin käsiksi.

5.2.1 Palomuurin määritys

Ciscon ASA-palomuureille on saatavilla oma lisäosa, ja sitä päädyttiinkin kokeilemaan ensimmäiseksi. Lisäosan asennuksen jälkeen Splunkiin asetettiin avoin TCP-portti, joka kuuntelee ja kerää lokiviestien virtaa palomuurilta. Määrittelyissä valitaan lähteen tyyppi, tässä tapauksessa ”cisco:asa” sekä voidaan määrittää kuinka lähettävä isäntä indeksoidaan järjestelmään, toisin sanoen IP-osoitteella, DNS-nimellä tai vaihtoehtoisesti mukautetulla, kuten kuvassa 23.



Kuva 23. *Lokivirran avaus Splunkissa palomuurille.*

Ciscon ASA tukee myös Secure Syslogia, mutta sen tuomille eduille ei tässä diplomityössä nähty niin suurta arvoa, että sitä olisi otettu käyttöön. Palomuurille tarvitsi vielä konfiguroida, mistä liityntäportista, mihin kohdeosoitteeseen ja mitä porttia viestien lokiviestin välittämiseen eteenpäin käytetään. TCP-portin eteen määritetään, minkä vakavuustason viestit toimitetaan eteenpäin. Cisco jaottelee viestit kahdeksaan eri luokkaan, ja luokat ovat listattuna taulukossa 1.

Hätätilanne	0	Järjestelmä epävakaa
Hälytys	1	Toimenpiteitä tarvitaan välittömästi
Kriittinen	2	Kriittinen tila
Virhe	3	Virhetila
Varoitus	4	Varoitustila
Ilmoitus	5	Normaali mutta merkittävä tila
Informatiivinen	6	Vain informatiiviset viestit
Debug	7	Debug-viestit

Taulukko 1. *Ciscon Syslog-viestien luokittelu*

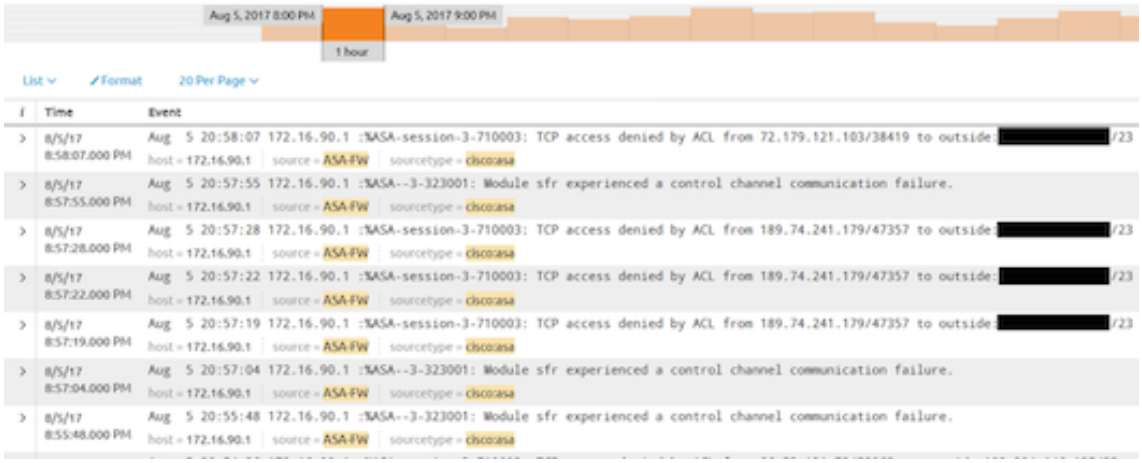
Tässä diplomityössä päädyttiin valitsemaan vakavuudet varoituksista alkaen, alla on tarvittavat komennot, jotka palomuuriin tarvitsi määrittää:

```
ASA(config)# logging host Hallintaverkko 172.16.90.14 4/1470
ASA(config)# logging permit-hostdown
ASA(config)# flow-export destination Hallintaverkko 172.16.90.15 518
```

Lokivirtaa alkoi kerääntyä määrityksien jälkeen ja lokimassasta päästiin testaamaan erilaisten hakulauseiden ja hakukriteereiden toteutusta. Splunkin ensimmäisten lokiviestin tarkastelun perusteella pystyi toteamaan, että tuotteesta on hyötyä ainakin tämän diplomityön tavoitteille. Tässä tapauksessa palomuurin sisäinen tallennustila oli rajallinen ja Splunkin avulla lokiviestit pystytään säilömään pidemmän aikaa.

Splunk mahdollistaa pidemmän ajan keräämisen ja säilömisen, mikä parantaa mahdollisuuksia selvittää ongelmatilanteita lokiviesteistä. Esimerkiksi virheviesteistä havaittiin palomuurin SFR-moduulin yhteydessä olevan ongelmia, kuten kuva 24 osoittaa. SFR-moduuli tarjoaa ASA:n palomuurissa ”next-generation” palomuuripalveluita, esimerkiksi kehittyneiden haittaohjelmien suojauksen (*eng. Advanced Malware Protection*). SFR-moduulin täyden toiminnallisuuden kannalta löydetty lokiviesti oli hyödyllinen ja sen pohjalta pystyttiin jatkamaan toiminnallisuuden ja ongelman aiheellisuuden selvitystä. Virheviestit saatiin esille hakulauseella:

source=”ASA-FW” sourcetype=”cisco:asa” severity_level=error



Kuva 24. *Kuvakaappaus virheviestin hakutuloksista.*

5.2.2 Linux-palvelimen määritys

Ubuntu-palvelimen konfigurointia varten asennettiin erillinen Splunk Forwarder, joka on mahdollista saada eri Linux-jakeluille. Asennus tapahtui Debian-paketin asennusrutiinien mukaisesti. Lisäksi splunkforwarder on hyvä määrittää käynnistymään automaattisesti palvelimen käynnistyksen yhteydessä:

```
# /opt/splunkforwarder/bin/splunk enable boot-start
```

Kun splunkforwarder on saatu asennettuna, tarvitsee siihen vielä asettaa määritykset Splunk-palvelimelle sekä Splunk-palvelimella määrittää uusi lokivirran vastaanotto:

```
# /opt/splunkforwarder/bin/splunk add forward-server 172.16.90.14:9997
```

Kun palvelinyhteyden määritys on saatu tehtyä, voidaan yhteyttä testata. Testaus tapahtuu valvottavan palvelimen konsolilta komennolla:

```
/opt/splunkforwarder/bin/splunk list forward-server
```

```
[root@PRODSRV01:/opt# /opt/splunkforwarder/bin/splunk list forward-server
[Splunk username: admin
[Password:
Active forwards:
        172.16.90.14:9997
Configured but inactive forwards:
        None
```

Kuva 25. *Yhteyden testaus Splunk-palvelimeen.*

Linux-palvelimelle tarvitsee vielä kertoa, mistä polusta lokiviestit lähetetään eteenpäin Splunk-palvelimelle. Määritys tapahtuu alla olevalla komennolla. Määrityksen lisäksi Splunk Forwarder-palvelu tarvitsee vielä käynnistää uudelleen.

```
# /opt/splunkforwarder/bin/splunk add monitor /path/ -index main -sourcetype
name
```

```
# /opt/splunkforwarder/bin/splunk restart
```

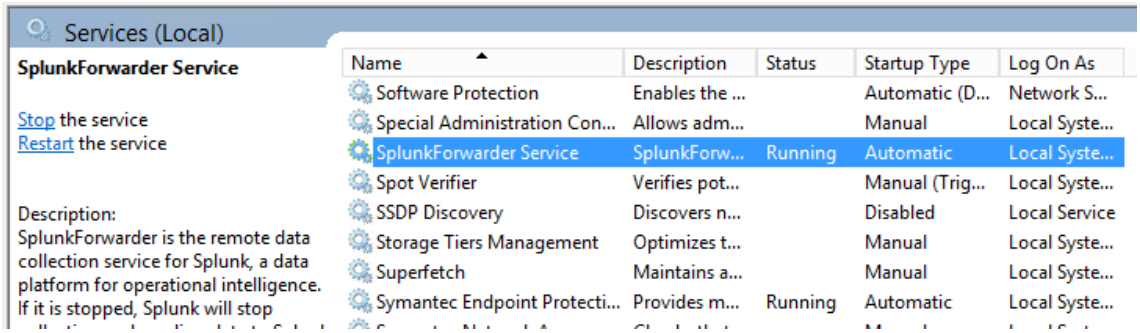
Tämän jälkeen Splunk-palvelimelle alkaa kulkea Linux-palvelimelta lokiviestit. Tässä diplomityössä päädyttiin seuraamaan muun muassa kirjautumisyrityksiä kyseiselle palvelimelle. Kuvassa 26 on kuvakaappaus havainnollistamaan lokiviestit liittyen kirjautumisyrityksiin.

Time	Event
8/6/17 3:51:56.000 PM	Aug 6 15:51:56 PRODSRV01 sshd[2273]: PAM service(sshd) ignoring max retries; 6 > 3 host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog
8/6/17 3:51:56.000 PM	Aug 6 15:51:56 PRODSRV01 sshd[2273]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.90.151 host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog
8/6/17 3:51:56.000 PM	Aug 6 15:51:56 PRODSRV01 sshd[2273]: Disconnecting: Too many authentication failures for toor [preauth] host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog
8/6/17 3:51:56.000 PM	Aug 6 15:51:56 PRODSRV01 sshd[2273]: Failed password for invalid user toor from 172.16.90.151 port 30881 ssh2 host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog
8/6/17 3:51:54.000 PM	Aug 6 15:51:54 PRODSRV01 sshd[2273]: pam_unix(sshd:auth): check pass; user unknown host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog
8/6/17 3:51:52.000 PM	Aug 6 15:51:52 PRODSRV01 sshd[2273]: Failed password for invalid user toor from 172.16.90.151 port 30881 ssh2 host = PRODSRV01 source = /var/log/auth.log sourcetype = syslog

Kuva 26. *Epäonnistuneet autentikoitumisyritykset.*

5.2.3 Windows-palvelimen määritys

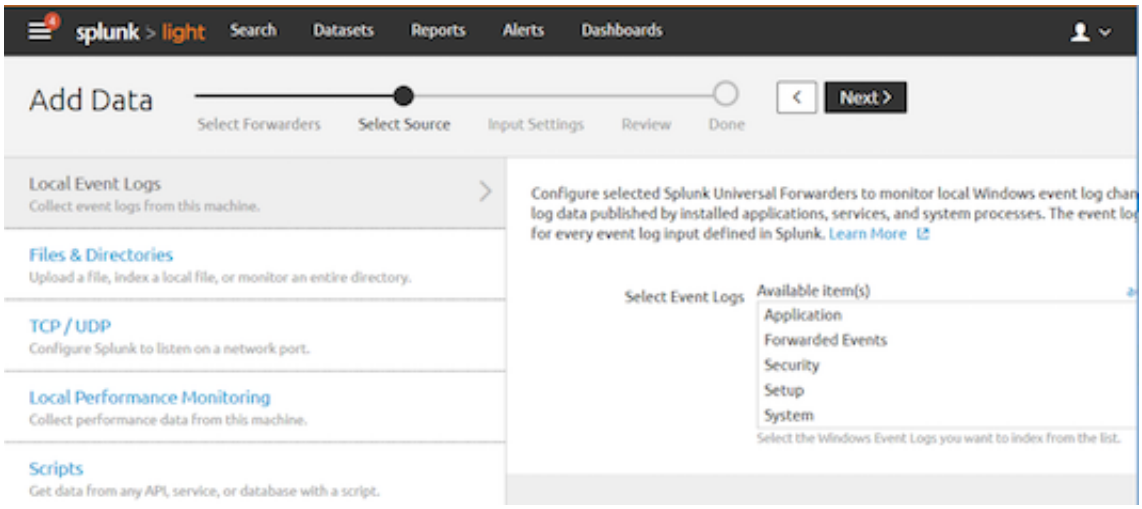
Windows-palvelimen käyttöönotto aloitettiin lataamalla ja asentamalla Universal Splunk Forwarder -paketti Windows-koneille. Asennuksen aikana kysytään käytettävän Splunk palvelimen IP-osoite ja portti. Splunk-palvelimen päähän lisättiin uusi Forwarder porttiin 9998, joka varattiin SRV01-palvelimelle. Asennuksen jälkeen Splunk Forwarder näkyy Windowssissa palveluna, kuten kuva 27 osoittaa.



Kuva 27. *Splunk Forwarder –palvelu.*

SRV01-palvelin tuli näkyviin Splunk-palvelimen Forwarder Management -näkymässä, mutta mitään dataa ei kuitenkaan tullut. Syyksi paljastui Symantec Endpoint Protection –tuote, joka esti Splunk-palvelimen 8089-portin, jota käytetään kontrollidatan kuljettamiseen. Yhteyden Splunk-palvelimeen voi varmistaa esimerkiksi netstat-komennolla, joka kertoo yhteyden tilan Splunk-palvelimeen. Netstat-komennon tulisi listata kaksi eri ”ESTABLISHED”-yhteyttä Splunk-palvelimeen. Symantec Endpoint Protection –tuotteeseen asetuksiin tehtyjen muutoksien jälkeen myös kontrolliyhteys alkoi toimia.

Kunnossa olevien yhteyksien jälkeen voidaan alkaa määrittämään, mitä tietoja Windows-palvelimesta halutaan tietää. Tämä tapahtuu Splunk-palvelimen hallinnassa kohdassa ”Add Data”, josta voidaan valita esimerkiksi ”Windows Event Logs”. Määrityksessä löytyy listattuna yhteensopivat laitteet, tässä tapauksessa SRV01-palvelin. Alla olevassa kuvassa 28 on kuvakaappaus Windowsin lokienkeräysvalikosta.

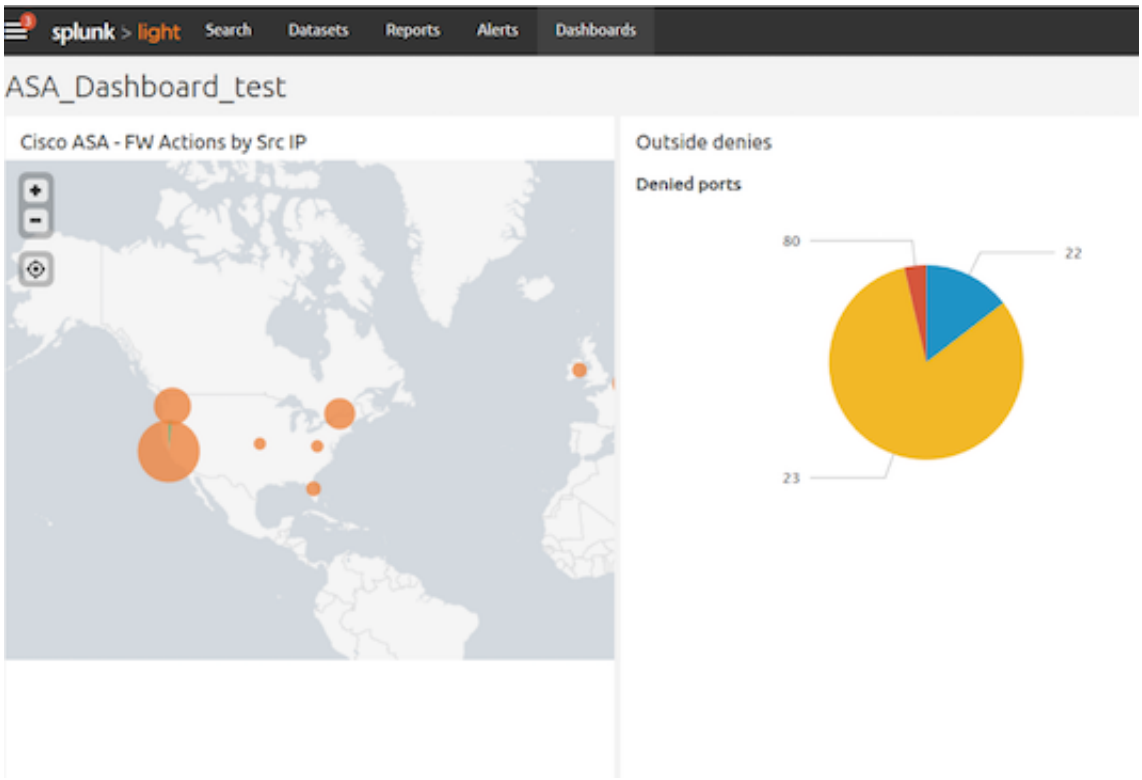


Kuva 28. *Kuvakaappaus Windowsin lokien valinnasta.*

5.2.4 Valvontanäkymät

Splunk mahdollistaa useiden valvontanäkymien (*eng. Dashboard*) luomisen. Tässä diplomityössä päädyttiin aloittamaan valvontanäkymien luonti palomuurin internetyhteyden liityntäportin tarkastelusta. Tarkastelussa hakulauseet tehtiin niin, että etsittiin estetty liikenne internetin suunnasta ja kahteen erillisen paneeliin määritettiin karttanäkymä lähdeosoitteen perusteella ja toiseen piirakkadiagrammi kohdeportin mukaan. Kuvassa 29 on tunnin ajalta kerättyä liikennettä. Esimerkiksi piirakkadiagrammin hakulause toteutettiin:

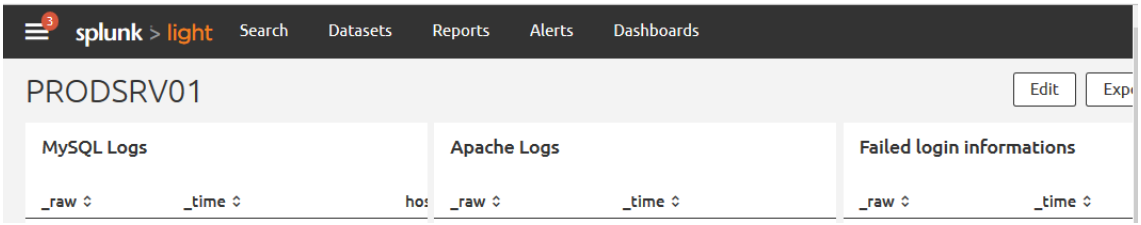
Sourcetype=”cisco:asa” Cisco_ASA_vendor_action=”access denied” | stats count by dest_port



Kuva 29. *Kuvakaappaus palomuurin valvontanäkymästä.*

Kiinnostavaksi lokien tutkimiseksi valittiin myös palomuurin otetut etäyhteydet ja niiden kirjautumisyritykset ASDM:llä, SSH:lla ja HTTPS:llä. Palomuurin hallintayhteydet olivat rajoitettuna niin, että se oli mahdollista vain hallinta- ja sisäverkosta sekä ylläpitäjien VPN-yhteyden kautta ja diplomityön teon aikana saatiin ainoastaan lokimerkintöjä onnistuneista kirjautumisista, jotka olivat aiheellisia. Yhteysyrityksien hälytyksiä voisi tehdä siinä tapauksessa, että määritettäisiin tarkemmin lähdeosoitteet, joista yhteyksien otot olisivat normaaleja, ja kaikista muista aiheutettaisiin esimerkiksi sähköpostihälytys. Valvontanäkymistä voi myös generoida tiedot PDF-muotoon sekä ajastaa PDF-tiedoston luonnin. Näin pystyttäisiin esimerkiksi organisaation johdolle näyttämään tilastoja.

PRODSRV01-palvelimelle räätälöitiin oma valvontanäkymä, johon määritettiin muun muassa MySQL- ja Apache2-palveluiden lokiviestit sekä epäonnistuneet kirjautumisyritykset. Valvontanäkymä helpottaa kriittisiin palveluihin liittyvien lokiviestien havaitsemisen yhden näkymän kautta, kuvassa 30 kuvakaappaus hallintanäkymästä. Valvontanäkymään voitaisiin myös lisätä esimerkiksi statistiikkaa tietokantaa kirjoittamisesta tai esimerkiksi PHP:n hylkäämät lomaketiedot.



Kuva 30. *PRODSRV01 Splunk-hallintanäkymä.*

Windowsin-palvelimien toimintaa voitaisiin valvoa graafisella näkymällä, jossa voitaisiin hyödyntää kirjautumisdataa, verkkojakojen käyttö sekä esimerkiksi tulostuksia. Splunk mahdollistaa myös Windowsin rekisterin ja prosessien valvomisen, jonka avulla voitaisiin määrittää erilaisia ehtoja ja mahdollisuuksien mukaan havaita poikkeavuuksia. Tässä diplomityössä keskityttiin lokiviestin keräykseen ja analysointiin Windows-palvelimen suhteen.

6. POHDINTA

Nagioksen käyttöönotto oli onnistunut ja se tarjoaa hyödyllisiä ominaisuuksia ilmaisversiossakin, kuten levytilojen ja palveluiden valvonnan ja hälytykset. Nagioksen käyttö ja muutoksien tekeminen sujuivat ongelmitta, mikä helpottaa jatkossa järjestelmän ylläpitämistä ja valvottavien kohteiden laajentamista. Nagios lisää huomattavasti nopeutta reagoida ongelmiin, ja se helpottaa proaktiivista työskentelyä. Nagioksen ominaisuuksista analysointiin muutamia tässä diplomityössä ja siinä löytyy jäljellä olevaa potentiaalia mahdollisille jatkotutkimuksille.

Nagioksen sähköpostihälytyksien lisäksi Nagioksessa on mahdollista toteuttaa SMS-tekstiviestihälytykset. Tämän toteuttaminen ei vaatisi kovin suuria ponnisteluja ja käyttöönotosta voisi saada lisäarvoa, jos valvottavan ympäristön valvontaa haluttaisiin tehdä tehokkaasti muulloinkin kuin toimistotyöaikoina.

Splunkin avulla lokien luettavuus helpottui ja Splunk lisää lokien seuraamista. Keskitetyn lokien hallinnan merkitys korostuu mitä isommasta ympäristöstä on kysymys. Lisäksi lokiviestejä pystytään Splunkin avulla säilyttämään kauemmin. Diplomityössä käyttöönotettujen järjestelmien ansiosta ongelmiin reagoiminen helpottui ja ennalta ehkäisevään työhön saatiin rajapinta toteutettujen järjestelmien avulla. Käyttöönotettu järjestelmät tukevat myös toimintaa, jolla pyritään minimoimaan tietoteknisistä johtuvien ongelmien vaikutuksia liiketoiminnan jatkuvuuteen.

Valvontajärjestelmien lisäksi tärkeässä roolissa on määritellä, kuinka toivutaan mahdollisista ongelmatilanteista. Esimerkiksi kuinka on varauduttu tarpeellisilla varalaitteilla, kuuluvatko laitteet ylläpito- ja takuusopimuksien piiriin, onko varalaitteissa kuinka pitkä toimitusaika tai viive. Lisäksi konfiguraatioista tulisi olla ajantasaiset varmuuskopiot ja muutoksien versionhallinta. Palvelimien toipumissuunnitelmassa tulisi olla otettuna huomioon varmistukset, ja onko varmistukset olemassa niin, että niillä pystytään palautumaan totaalisesta katastrofista.

Lokiviesti kertoo yleensä mitä on tapahtunut, milloin on tapahtunut, missä on tapahtunut, kuka on liittynyt tähän ja mistä hän tai se saapui. Pelkkä lokiviesti ei kuitenkaan kerro mitä tulee tapahtumaan seuraavaksi tai mitä muuta on tapahtunut, josta pitäisi tietää. Lokiviestit ja mielestäni etenkin Windowsin lokiviestit saattavat olla kriittisyysmääritykseltä korkealla, mutta niiden merkitys on kuitenkin matala. Tämä asettaa haasteita pohtiessa millaisia lokiviestejä halutaan seurata ja mitä sellaisista halutaan generoituvan, esimerkiksi hälytyksien muodossa. Toisin sanoen, kuinka erotella hyödynnettävä loki suuresta lokimäärästä.

Diplomityön aikana järjestelmät pyrittiin käyttöönottomaan tietoturvallisuus huomioiden. Vaikka diplomityössä ei tehty erillistä lokipolitiikkaa, toteutuksessa huomioitiin kuitenkin lokien käsittelyn hyviä menetelmiä, joita VAHTI 03/2009 Lokiohjeessa suositellaan, kuten esimerkiksi aikapalvelimien käyttö laitteiden aikojen synkronoinnissa, lokiviestien keräys perustuu tarpeeseen ja lokitietoja käsitellään yksityisyydensuoja huomioiden.

Splunk lisää lokiviesteihin tiedon siitä, milloin lokiviesti on indeksoitu. Indeksointiajan ja lokiviestin aikaleiman avulla voidaan analysoida mahdollisia viiveitä lokien toimittamisessa ja havaita jos lokilähteen ajassa tai aikavyöhyke ei ole kunnossa. Splunkin kahdentamisella pystyttäisiin lisäämään lokien keräyksen saatavuutta, esimerkiksi päivitys ja huoltotöissä.

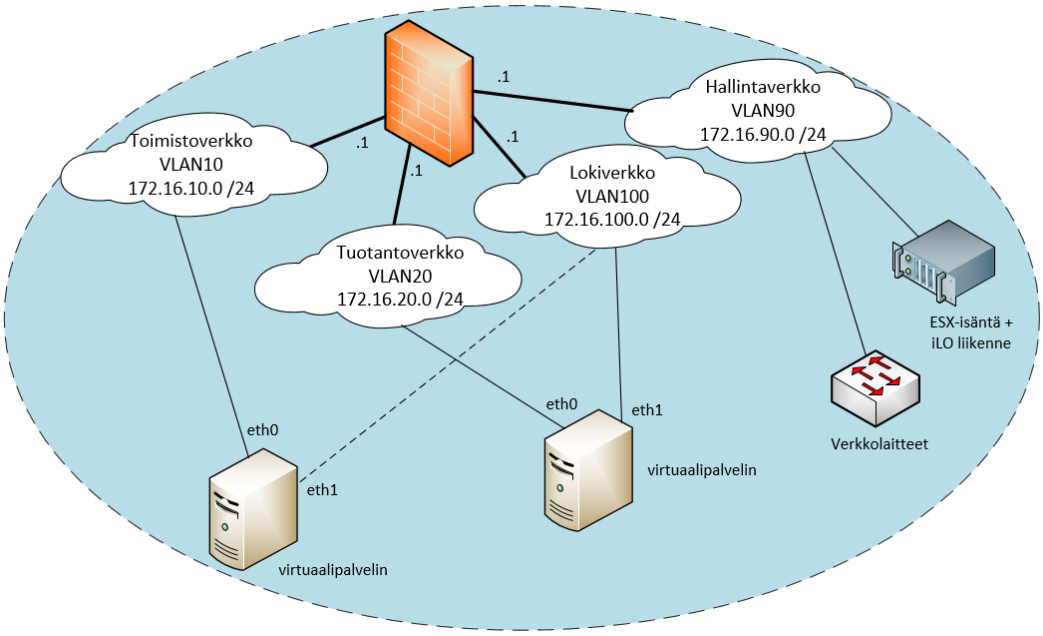
Diplomityössä ympäristön kartoituksessa käytettyjen testien avulla voidaan havaita järjestelmissä käytössä olevia versioita ja versiotietojen perusteella tutkia mahdollisia haavoittuvuuksia. Haavoittuvuuksien hallinta ja seuraaminen kuuluvat tietoturvatyöhön ja tietoturvallisuuden tilannekuvaan. Manuaalista analysointia helpottamaan on olemassa automatisoituja työkaluja, jotka voidaan mahdollisuuksien mukaan integroida SIEM-järjestelmään yhdeksi osaksi luomaan tietotuvallisuuden tilannekuvaa.

Kehittämistä Nagioksen osalta jäi Windows-palvelimen valvontaan käytettävän NSClientin liikenne, jolla tarkoitan sitä millä protokollilla valvonta tapahtuu. Nagios kommunikoi oletuksena NSClient-ohjelmien kanssa selkokielellä, toisin sanoen liikennettä ei ole salattu Nagioksen ja valvottavan kohteen välillä. Windows-palvelimen päässä pystytään rajoittamaan, mistä osoitteista NSClienttiin otetaan yhteyttä, joten suoraan Windows-palvelintakaan ei pysty NSClientin salasanalla kaappaamaan. Nagios ja NSClient tukevat nykyään sertifikaattipohjaista autentikointia, jonka avulla liikenne niiden välillä pystyttäisiin kuljettamaan salattuna TLS-yhteyttä pitkin.

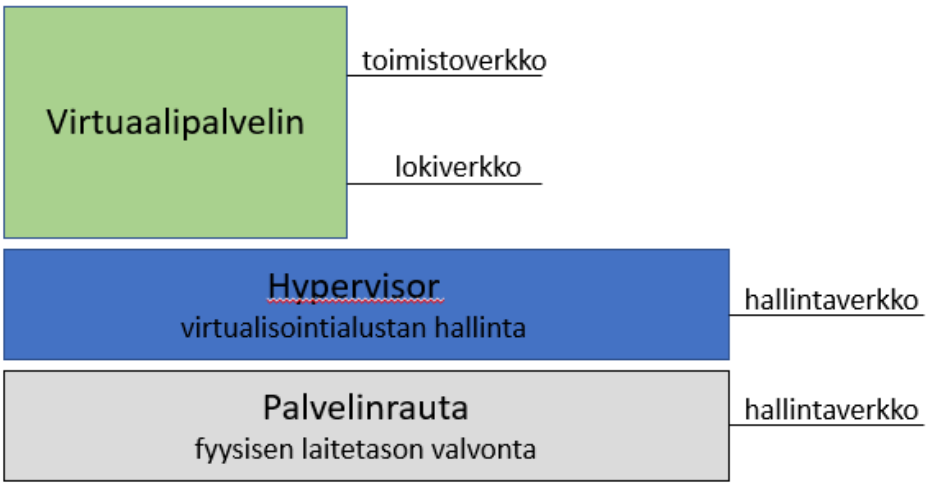
Myös perinteisen Syslog-lokivirran voisi pyrkiä korvaamaan Secure-Syslogia käyttämällä. Splunk tukee Unix- ja Windows-palvelimien valvonnassa TLS-salattua liikennettä käytettäessä Universal Splunk Forwardereja. Yhtenä osana tätä diplomityötä olisi voitu rakentaa oma juurivarmentajan, jonka avulla olisi myönnetty tarvittavat sertifikaatit niin Nagios- ja Splunk-järjestelmille. Tällöin myös Secure-Syslogin käytön laajentamisesta tulisi hallitumpaa, kun sertifikaattien hallinta olisi keskitettyä.

Verkkoteknisestä näkökulmasta virtuaalipalvelimien lokiviestit voitaisiin kuljettaa omaa yhteyttä pitkin, jolloin palvelimen yhteyksistä voitaisiin puhua ”kaksikätisyydestä”, jossa sovelluksien ja muiden hyötyliikenne kulkisi varsinaista liityntää pitkin ja lokiviestit kuljetettaisiin suoraan hallinta-liityntää pitkin. Näin ollen lokiviestit eivät kulkisi tässä tapauksessa ”toimisto-” tai ”tuotantoverkon” kautta. Vaihtoehto olisi luoda erikseen hallintaverkon lisäksi myös erillinen lokiverkko, jolloin virtuaalipalvelimen lokivirta kerättäisiinkin lokiverkosta ja hallintaverkko jätettäisiin ainoastaan verkkolaittei-

den ja palvelinalustojen hallintaa varten. Tällöin verkkoja olisi segmentoitu vielä niin, että tilanteessa jossa virtuaalipalvelin joutuisikin kaappauksen kohteeksi, ei lokiverkosta olisi pääsyä suoraan hallintaverkkoon. Tämänkaltainen toteutus vaatisi enemmän suunnittelua ja päätöksiä sekä toisaalta ylläpitäminenkin monimutkaistuisi. Kuvassa 31 on havainnollistettu lokiverkon ja hallintaverkon eriyttämistä omiksi verkoiksi. Lisäksi kuvassa 32 on pyritty havainnollistamaan virtuaalipalvelinalustan näkökulmasta verkkojen määritystä.



Kuva 31. *Hallinta- ja lokiverkon eriyttäminen.*



Kuva 32. *Virtuaalipalvelinalustan verkot.*

Liikenteestä tehtyjen analysointien perusteella voitaisiin määrittää hyödyllisiä hälytyksiä. Analysoinnissa voitaisiin seurata palomuurin kautta kulkevan liikenteen määriä eri

porttien välillä ja sen pohjalta tehdä päätelmät sopivista hälytysrajoista. Hälytysrajojen ylittyessä ylläpito voisi tehdä tarkempia analyysejä mahdollisesta väärinkäytöstä, esimerkiksi onko organisaatiosta kulkemassa dataa ulos.

Organisaatiosta lähteviä yhteyksiä Internettiin voitaisiin tarkkailla siltä osin, onko useammassa laitteessa yhteydet auki samoihin kohdeosoitteisiin, jolloin mahdollisesti voisi olla käynnissä jotakin normaalista poikkeavaa toimintaa, esimerkiksi laitteiden kaappauksia. Verkkoliikenteen analysointia ja statistiikan keräystä voitaisiin tehdä NetFlown avulla.

Diplomityön määrittely ja rajaaminen onnistuivat mielestäni hyvin diplomityön laajuuden ja asettamieni tavoitteiden suhteen. Lokiviestien laajemmalle analysoinnille olisi ollut tarvetta ja sen toteuttaminen olisi ollut mielekästä, mutta diplomityön laajuuden ja siihen käytettävän ajan ollessa rajallinen, ei se ollut mahdollista. Analysointivaiheeseen olisi voinut päästä nopeammin, jos tutkittavan ympäristön kuvaus, hallintaverkon eriyttäminen ja Nagios-valvonta eivät olisi vieneet aikaa diplomityön tekemisestä. Toisaalta minulle jäi tästä diplomityöstä paljon kokemusta ja osaamista vastaavan järjestelmän käyttöönottoon, joka mahdollistaa tulevaisuudessa taitojeni kehittämistä lokiviestien analysoinnin suhteenkin.

7. YHTEENVETO

Diplomityössä tutkittiin lokiviestejä ja niiden keskitettyä hallintaa sekä tietoturvallisuuden tilannekuvan mahdollistavia menetelmiä. Tietoturvallisuuden hallintaan liittyy tietoturvapolitiikka, joka ohjaa ja tukee organisaation tietoturvallisuuden toteutumista. Diplomityössä esiteltiin yleisellä tasolla tietoturvallisuuden hallintaan liittyviä osa-alueita, koska lokiviestien käsittelyn tulee perustua tarpeeseen ja niiden käsittelyssä tulee huomioida tietoturvallisuuden ja tietosuojan näkökulmat.

Lokiviestien käsittelyä ja järjestelmien valvontaa varten diplomityön alussa toteutettiin erillinen hallintaverkko, joka mahdollisti diplomityössä otettujen järjestelmien ja verkkolaitteiden hallintayhteyksien kerrospuolustuksen. Palomuurauksen avulla saavutettiin myös näkyvyyttä verkkojen välille. Segmentoidun hallintaverkon lisäksi diplomityössä hyödynnettiin testejä, joiden avulla parannettiin käsitystä tutkittavasta ympäristöstä. Verkon skannaus ja liikenteen analysointi yhdessä dokumentaation tutkimisen kanssa avustivat kriittisten kohteiden määrittämisen. Riskien arviointia käytetään tukemaan suunnitellessa toimenpiteitä ja riittäviä resursseja, jotta saavutetaan sopivassa suhteessa riittävä taso tietoturvallisuuden toteutumiseen järjestelmäkohtaisesti.

Diplomityössä saavutettiin sille asetettuja tavoitteita, kuten esimerkiksi lokiviestien keskitetyn keräyksen toteuttaminen, sen avulla helpomman luettavuuden ja mahdollisuuden lokiviestien analysointiin. Nagios-valvonnan avulla saavutettiin rajapinta, josta voidaan tarkastaa valvottavien kohteiden tiloja ja valvonta generoi hälytyksiä, jotka parantavat ongelmatilanteisiin reagoimisen vasteaikoja. Toteutetut järjestelmät tukevat toimintaa, jossa pyritään minimoimaan tietotekniikasta aiheutuvien ongelmien vaikutus liiketoiminnan jatkuvuuteen.

Vastaavan kaltainen kokoonpano olisi mahdollista toistaa ja sen uudelleenkäytettävyys voitaisiin automatisoida, esimerkiksi erilaisten template-pohjien myötä. Perehtyminen aihepiirin teoreettisen näkökulmaan antoi minulle uusia näkökulmia ja ulottuvuuksia lokiviestien käsittelyyn, joka kattaa kuljettamisen, säilyttäminen, analysoinnin ja niin edelleen. Tietoturvallisuuteen liittyvät standardit ja ohjeistukset ovat hyvä ottaa huomioon ja niitä pystyy käyttämään tukena luotaessa organisaatiolle esimerkiksi tietoturvapolitiikkaa ja lokipolitiikkaa. Seuraavien vuosien aikana lokiviestien käsittelyyn tullaan paneutumaan tarkemmin, kun EU:n tietosuojauudistus astuu voimaan ensi vuoden aikana.

LÄHTEET

[1] S. Garfinkel, The Cybersecurity Risk, Communications of the ACM, 2012, s. 29. Saatavissa: http://dl.acm.org.libproxy.tut.fi/citation.cfm?id=2184330

[2] A. Kakareka, Detecting System Intrusions. Network and System Security, 2013, s. 20. Saatavissa: http://www.sciencedirect.com/science/article/pii/B9780124166899000010

[3] R. Montesino, S. Fenz, W. Baluja, SIEM-based framework for security controls automation, Information Management & Computer Security, Vol. 20, 2012, s. 3-4, 249-250, 253, 256-260. Saatavissa: http://dx.doi.org/10.1108/09685221211267639%5Cnhttp://dx.doi.org/10.1108/IMCS-07-2013-0053%5Cnhttp://dx.doi.org/10.1108/IMCS-05-2013-0041%5Cnhttp://

[4] A. Chuvakin, K. Schmidt, C. Philips, Logging and Log Management, Elsevier, 2013, s. 1-3, 6-7, 11-13, 35, 219-220, 305-307. Saatavissa: http://linkinghub.elsevier.com/retrieve/pii/B9781597496353000014

[5] A. Talus, E. Autio, A. Hänninen, H. Pihamaa, S. Kantonen, Miten valmistautua EU:n tietosuoja-asetukseen?, Oikeusministeriön julkaisu 4/2017, s. 9, 13. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

[6] O. Söderström, E. Moradian, Secure Audit Log Management, Procedia Computer Science 22, 2013, s. 1249-1258. Saatavissa: http://dx.doi.org/10.1016/j.procs.2013.09.212

[7] V. Bumgarner, Implementing Splunk: Big Data Reporting and Development for Operational Intelligence, Packt Publishing, 2013. Saatavissa: http://library.books24x7.com.libproxy.tut.fi/assetviewer.aspx?bookid=93170&chunkid=440586223

[8] B. Sigman, Splunk Essentials, Packt Publishing, 2015. Saatavissa: https://ebookcentral.proquest.com/lib/tut/reader.action?docID=1968969

[9] B. Peterson, Secure Network Design : Micro Segmentation, SANS Institute, 2016, s. 18-19 . Saatavissa: https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775

[10] J. Harmening, Managing Information Security, Computer and Information Security Handbook, Elsevier, 2013, s. 48-49. Saatavissa: http://www.sciencedirect.com.libproxy.tut.fi/science/book/9780123943972#ancp2

[11] C. Laybats, L. Tredinnick, Information security, Business Information Review VOL 33(2), 2016, s. 78-79. Saatavissa: http://journals.sagepub.com/doi/10.1177/0266382116653061

[12] D. Landoll, Information Security Policies, Procedures, and Standards: A Practioner´s Reference, Auerbach Publ. 2016. Saatavissa: http://library.books24x7.com.libproxy.tut.fi/assetviewer.aspx?bookid=117417&chunkid=392892637&noteMenuToggle=0&leftMenuState=1

[13] LIITE 4: Esimerkki Tietoturvapolitiikka (VAHTI 3/2007), 2007. Saatavissa: https://www.vahtiohje.fi/web/guest/602

[14] Information Security Policy Templates. Saatavissa: https://www.sans.org/security-resources/policies. [Haettu 22.08.2017].

[15] J. Engblom, Liikeriskit – luonne, lajit ja riskikentän mallintaminen, Turun kauppakorkeakoulun julkaisu, 2003, s. 23-24. Saatavissa: https://www.doria.fi/bitstream/handle/10024/96678/Ae2_2003.pdf?sequence=2

[16] Riskienhallintaprosessi, Suomen Riskienhallintayhdistys. Saatavissa: http://www.pk-rh.fi/index.php?page=riskienhallintaprosessi%0D. [Haettu 16.06.2017].

[17] A. Andersson, J. Koivisto, Tietoturvaa toteuttamassa, Tallinna: Tietosanoma Oy, 2013, s. 51.

[18] C. Jackson, Network Security Auditing. Indianapolis: Cisco Press, 2010, s. 20-22, 68, 76, 91-92, 101, 106.

[19] Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto, 2017. Saatavissa: https://www.vahtiohje.fi/web/guest;jsessionid=6A28CA86239EFE3D177BDB25CAC384539EB58CC6318D9DEB9A74EB1379B725299E16A9547FEDB1E077A4CE

[20] R. Miani, B. Zarpelao, B. Sobesto, M. Cukier, A Practical Experience on Evaluating Intrusion Prevention System Event Data as Indicators of Security Issues, 2015 IEEE 34th Symposium on Reliable Distibuted Systems, 2015, s. 296. Saatavissa: http://ieeexplore.ieee.org/document/7371594/

[21] Best Security Information and Event Management (SIEM) Software of 2017 as Reviewed by Customers, 2017 Saatavissa: https://www.gartner.com/reviews/customer-choice-awards/security-information-event-management. [Haettu 26.08.2017]

[22] E. Knapp, J. Langill, Exception, Anomaly, and Threat Detection. Industrial Network Security, Syngress, 2015, s. 190, 192. Saatavissa: http://www.sciencedirect.com/science/article/pii/B9780124201149000113%5Cn http://linkinghub.elsevier.com/retrieve/pii/B9780124201149000113

[23] Lokiohje 3/2009, Valtionhallinnon tietoturvallisuuden johtoryhmä, 2009, s. 13-14, 19, 23-26, 29-33, 43-46, 57, 62. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=775179cb-6c54-4dfb-b65d-e925d47c61d2&groupId=10229

[24] R. Gerhards, C. Lonvick, Transmission of Syslog Messages over TCP, 2012, s. 4, 6. Saatavissa: https://tools.ietf.org/pdf/rfc6587.pdf

[25] Chapter 1. Agent Integrator Overview, Docs Oracle. Saatavissa: https://docs.oracle.com/cd/E13192_01/manager/mgr20/intref/overview.htm

[26] U. Blumenthal, B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), 2002, s. 4-6. Saatavissa: https://tools.ietf.org/html/rfc3414

[27] RSYSLOG. Saatavissa: http://www.rsyslog.com/. [Haettu 23.08.2017].

[28] Failover Syslog Server. Saatavissa: http://www.rsyslog.com/doc/v8-stable/tutorials/failover_syslog_server.html. [Haettu 23.08.2017]

[29] T. Wilhelm, Professional Penetration Testing, Waltham: Syngress, 2013, s. 151-158, 172.

[30] P. Engebretson, The basics of hacking and penetration testing. Waltham: Syngress, 2013, s. 53-55.