Anssi Mustonen

KESKITETTY LOKIENHALLINTA HP ARCSIGHTILLA

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikka ja liikenne
Tietoturvateknologia
Kevät 2014

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikan ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Anssi Mustonen	
Työn nimi Keskitetty lokienhallinta HP ArcSightilla	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Toimeksiantaja Ymon Oy / Riku Lokka
Aika Kevät 2014	Sivumäärä ja liitteet 52+2

Tämän työn tavoitteena oli tutkia työn tilaajalle Ymon Oy:lle sitä, kuinka Hewlett-Packardin ArcSight-tuoteperheen avulla rakennetaan keskitetty lokienhallintajärjestelmä ja miten hyvän lokienhallinnan tavoitteet toteutuvat.

Tietoturvan osa-alueita ovat luottamuksellisuus, eheys, kiistämättömyys ja saatavuus. Lokienhallinta liittyy olennaisena osana kaikkiin näihin neljään osa-alueeseen ja parantaa niiden toteutumista valitussa ympäristössä. Lähes poikkeuksetta kaikki tietoliikenneverkossa toimivat laitteet tuottavat lokia. Lokitiedon avulla saadaan tarkka käsitys tapahtumasta, ajanhetkestä ja autentikointia käytettäessä tekijästä. Keräämällä lokitiedot keskitettyyn lokienhallintajärjestelmään ja normalisoimalla eri lokit yhtenäiseen lokimuotoon saadaan kokonaiskuva koko järjestelmän tapahtumiin. Keskitetystä järjestelmästä voidaan vaivattomasti nähdä tarvittavat tiedot helposti verrattuna hajallaan oleviin eri lokiformaatteja sisältäviin järjestelmiin. Nämä vaatimukset ovat erityisen tärkeitä luottamuksellisia tietoja käsittelevillä organisaatioilla, kuten luottokorttiyhtiöillä.

Tämän työn tuloksena syntyi tutkielma, jossa arvioidaan, miten ohjeistukset ja säännökset erityisesti VAHTI-lokiohjeessa vaikuttavat lokienhallinnan toteutukseen. Lopputuloksena syntyi myös pelkistetty malli miten yksinkertainen ja vikasietoinen keskitetty lokienhallintajärjestelmä voidaan toteuttaa HP ArcSightin lokienhallintatuotteilla.

Kieli	Suomi
Asiasanat	Tietoturva, lokienhallinta, ArcSight
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS
ABSTRACT

School Engineering	Degree Programme Information Technology
Author(s) Anssi Mustonen	
Title Centralized Log Management by HP ArcSight	
Optional Professional Studies Information Security	Commissioned by Ymon Oy / Riku Lokka
Date Spring 2014	Total Number of Pages and Appendices 52+2

The purpose of this Bachelor's thesis was to study a centralized log management system for Ymon Oy. This study concentrates on examining the centralized log management system, how it is implemented with Hewlett Packard ArcSight and how well the log management objectives are met.

The aspects of information security include confidentiality, integrity, non-repudiation and availability. Log management is an essential component of each of these four areas and significantly improves their implementation. Almost without exception all the communication network devices produce log information. Log information tells the exact nature and time of the event and also of its author, if authentication is used. Gathering log information into a centralized log management system and normalizing it to one log format gives an overview of the events of the whole system. Without this kind of system log information must be collected from various scattered devices and systems. Managing log information efficiently and securely is often a necessary requirement for organizations that handle confidential information.

This thesis resulted in a study which assesses how the guidelines and regulations, regarding the VAHTI log-guide in particular, affect the implementation of the log management system. This work also includes the basics of planning, designing and implementation that need to be considered when creating a simple and fault-tolerant centralized log management system with HP ArcSight products. The thesis is especially helpful for those who are looking for information about what kinds of problems may appear at various stages of the development when building a log management system.

Language of Thesis	Finnish
Keywords	Information Security, HP ArcSight, Log Management
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

ALKUSANAT

Haluan kiittää päättötyön aiheesta ja mahdollisuudesta perehtyä lokienhallintaan Ymon Oy:tä. Haluan myös kiittää työn ohjaajaa Raili Simanaista ja suomen kielen opettajaani Eero Soinista Kajaanin ammattikorkeakoululta. Lisäksi kiitokset kuuluvat läheisilleni ja ystäville, jotka jaksoivat minua tämän työprosessin aikana. Erityiskiitokset ansaitsee koulukaverini, joka jaksoi motivoida minua tekemään opinnäytetyötä päätoimisen työn ohessa.

SISÄLLYS

LYHENTEET JA MÄÄRITELMÄT

Big Data	Nimitys tietomäärille joiden hallinnassa ei voida soveltaa perinteisiä tiedon hallintatapoja.
CEF	Common Event Format
Connector Appliance	Itsenäinen lokienkeräin alusta
Epoch-aika	Unix-käyttöjärjestelmässä käytettävä ajan tallennustapa
EPS	Event Per Second, käytetään tapahtumien vastaanottokyvyn ilmaisuun
ESM	Enterprise Security Management
FlexConnector	Lokisovitin
GPS	Global Positioning System
IDS	Intrusion Detection System
ISO27001	Standardi
ISP	Internet Service Provider
NAS	Network Attached Storage
NTP	Network Time Protocol
PCI DSS	Standardi
RegEx	Regular Expression, säännöllisiä lausekkeita noudattava kieli

SAN	Storage Area Network
SANS	SysAdmin, Audit, Networking, and Security, Yksityinen yhdysvaltalainen yritys
SAS	Serial Attached SCSI
SATA	Serial ATA
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
SLA	Service Level Agreement
SmartConnector	Lokisovitin
SNMP trap	SNMP-agentin lähettämä viesti
SQL	Structured Query Language

1 JOHDANTO

Ymon Oy on perustettu vuonna 2003. Yhtiön toimipisteet sijaitsevat Vantaalla ja Kajaanissa. Ymon on erikoistunut tietoverkkoihin ja tietoturvaan, tarjoten palveluja aina vaativista vian selvitystehtävistä organisaatioiden infrastruktuurin arkkitehtuurisuunnitteluun ja lokienhallintaan. Tavoitteena on, että asiakas voi keskittyä liiketoimintaansa ja jättää tietoverkkoon liittyvät asiat Ymonin hoidettavaksi. Asiakkaina ovat pääasiassa suuret ja keskisuuret yritykset.

Lokienhallinta ja sen merkitys on kasvanut viime vuosina maailmalla yritysten käsitellessä yhä enemmän säilytettävää ja liiketoiminnan kannalta tärkeää tietoa. Tämä tarkoittaa myös tietojen suojaamistarvetta erilaisin ratkaisuin. Keskitetyn lokienhallinnan avulla saavutetaan parempi näkemys siitä, mitä tietoliikenneverkoissa, laitteissa ja ohjelmistoissa tapahtuu. Lisäksi tietoja voidaan säilyttää myöhempää tarkoitusta varten, kuten todistamaan väärinkäytökset.

Työssä tutkittiin keskitetyn lokienhallintajärjestelmän toteuttamiseen liittyvää teoriaa ja vaatimuksia. Teoriatietojen perusteella tarkasteltiin, kuinka lokienhallinta on toteutettavissa HP Arcsight -tuotteiden avulla. Tutkittiin, millaista lisäarvoa keskitetty lokienhallinta tuottaa sitä käyttävälle tai sen hankkivalle yritykselle. HP Arcsightin osalta perehdyttiin sen toiminnallisuuteen, keskeisiin ominaisuuksiin ja miten tuote toimii perusperiaatteiltaan. Tämän perusteella lukija kykenee hahmottamaan tuotteen toiminnallisen idean ja vertailemaan sitä kilpaileviin tuotteisiin. Työstä käy selville, millainen lokienhallintajärjestelmän täytyy minimissään olla, että siitä saadaan vikasietoinen ja toteutuskelpoinen.

2 TIETOTURVA

Tietoturvallisuus on osa yritysturvallisuutta, joka käsittää useita yrityksen turvallisuusosa-alueita. Kaikilla yritysturvallisuutta suojaavilla toimenpiteitä pyritään suojaamaan yritykselle tärkeitä ja keskeisiä osa-alueita: henkilöt, maine, tiedot, omaisuus ja ympäristö. Näiden osa-alueiden tietoturvallisuuden laiminlyönti voi pahimmillaan lamauttaa organisaation toiminnan. Kokonaisuutena tietoturvan tulee tukea organisaation liiketoimintaa. [1.]

2.1 Organisaation tietoturvallisuus

Tietoturvallisuudessa keskitytään sananmukaisesti yrityksen tietojen suojaamisen osa-alueeseen. Jotta tietoturvalliset toimintatavat ovat tarkoituksenmukaisia ja osana koko organisaation tekemistä, vaatii se ohjaamista. VAHTI-ohjeistuksen mukaan tietoturvallisuus voidaan jakaa kuvassa 1 esitettyihin kahdeksaan osaan. Hallinnollinen tietoturvallisuus toimii pohjana ja ohjaa kaikkia muita tietoturvan osa-alueita ja varmistaa niiden toteutumisen. Yksinkertaisesti selitettynä hallinnollinen tietoturvallisuus on kuvaus tietoturvallisuuden periaatteista organisaatiossa. [2.]

Kuva 1. Tietoturvallisuuden kahdeksan osa-aluetta VAHTI-ohjeistuksen mukaan.

Kahdeksan kuvassa esitettyä osa-aluetta muodostavat organisaation tietoturvallisuuden. Näiden tietoturvan osa-alueiden toteutumista ohjaa organisaation ydinliiketoiminnasta riippuen kolme pääosiota. Kuvassa 2 nämä osa-alueet voidaan jakaa VAHTI-ohjeistuksen mukaan kolmeen kokonaisuuteen: lainsäädäntöön, sopimuksiin sekä muihin velvoitteisiin, suosituksiin ja ohjeisiin. Organisaation toimialasta riippuu, mitä näihin kokonaisuuksiin kuuluu ja mitkä rajoittavat ja velvoittavat toimintaa. [3.]

Kuva 2. Organisaation tietoturvallisuutta ohjaavat ja siihen vaikuttavat useat eri asiat.

Lainsäädännöstä tulevat tekijät velvoittavat organisaatiota huolehtimaan tietoturvasta ja asettavat minimivaatimukset tietoturvalle. Sopimukset voivat velvoittaa organisaatiota noudattamaan sopimuksessa esitettyjä tietoturvaa parantavia toimia. Tällaisia sopimuksia voi olla muun muassa organisaation ja sen alihankkijana toimivan yrityksen kanssa. Organisaatio voi vahvistaa kilpailukykyään ja luotettavuuttaan hankkimalla liiketoiminnalleen puolueettoman auditoinnin avulla tietoturvastandardin [4]. [3.]

Organisaation tietoturvan toimintaa ohjaavien asioiden lisäksi tietoa ja tietojärjestelmiä pitää suojata. Saatavuus vaatii, että järjestelmiin tallennetut tiedot ovat siihen oikeutettujen henkilöiden saatavilla silloin, kun he niitä tarvitsevat. Eheyden vaatimus on, että vastaavat tiedot ovat oikeita ja niihin voidaan luottaa. Luottamuksellisuuden vaatimuksena on varmistaa, että

tietoja voivat käsitellä vain oikeutetut henkilöt. Todennus, jota joissakin yhteyksissä kutsutaan autentikoinniksi, takaa tietoja tarkastelevan henkilön luotettavan tunnistautumisen. Kiistämättömyydellä varmistetaan, ettei käyttäjä voi kieltää tapahtunutta. Tapahtuma voidaan myös luotettavasti todistaa jälkikäteen, jolloin se toimii todisteena. Ohjelmistoissa, tietoliikenteessä ja tietojärjestelmissä tapahtuneen todistaminen tietyllä ajan hetkellä vaatii lokin tapahtumasta. Tapahtumista kertovien lokien kerääminen tehokkaasti siten, että niitä voidaan hyödyntää, vaatii lokienhallintajärjestelmän. [5.]

2.2 Suojattava tieto

Tieto on yrityksen arvokkain osa ja tekee siitä yksilöllisen ja erottaa sen muista saman alantoimijoista. Tieto voi olla monessa muodossa, aina asiakirjoista ääni- tai videotallenteisiin ja tietokantoihin, jotka monesti ovat yrityksen kaikista arvokkaimman tiedon säilytyspaikka. Tietotekniikan aikakaudella se on yhä useammin sähköisessä muodossa ja sitä siirrellään tietoliikenneverkkoja pitkin. Yrityksen menestyksen kannalta sen tulee suojata tietonsa selviytyäkseen niin normaaleissa kuin poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Teollisuusvakoilu ja tietomurrot ovat muodostuneet pysyväksi ja tekniikoiltaan kehittyväksi uhkaksi tietotekniikan saralla. Suojelupoliisin [6 s. 7] vuosina 2009–2011 tehdyn selvityksen mukaan laiton tiedonhankinta ja sen yritykset ovat pysyneet samalla tasolla aikaisempien vuosien tutkimusten kanssa. Lievemmät, sekä tahalliset että tahattomat tietoturvaloukkaukset ovat arkipäivää. [7.]

3 LOKIENHALLINTA

Tässä luvussa keskitytään lokienhallintajärjestelmän rakentamisen syihin ja lähtökohtiin, joista lokienhallintajärjestelmää on hyvä lähteä rakentamaan. Tarkasteltavana on asioita, jotka huomioimalla järjestelmän suunnittelussa vältytään pahimmilta virheiltä ja yllättäviltä kustannuksilta. Järjestelmän toteutuksen osalta käsitellään asioita, joita minimissään vaaditaan toimivaan järjestelmään. Käsittelyssä on teknisiä ja muita huomionarvoisia seikkoja. Lokienhallintajärjestelmän ylläpitämisen osalta on nostettu esiin järjestelmän ylläpitämisen vaatimuksia. Lokitietojen käsittelyssä käydään läpi kaikki lokien käsittelyyn liittyvät vaiheet ja kerrotaan niiden merkitys.

3.1 Lokienhallinnan tarve

Yrityksen sijoittaessa tietoturvansa kehittämiseen ja lokienhallintaan vaatii se perusteluita vastaavalla tavalla kuin muutkin investoinnit. Yhdistystoiminta, jonka ei välttämättä tarvitse tuottaa voittoa, on eri asia. Suorien hyötyjen näkeminen tietoturvan kehittämisessä ja lokienhallinnan onnistuneessa toteutuksessa voi olla vaikeaa näyttää toteen. Tietoturvan kehittäminen ja lokienhallinnasta huolehtiminen on parhaimmillaan ennakoimista ennen kuin riskit toteutuvat.

Tietoturvassa samoin kuin lokienhallinnassa säästöt voidaan laskea vertaamalla siihen, kuinka paljon kustannuksia ja aikaa joudutaan käyttämään, kun keskitettyä lokienhallintaa ei ole käytössä. Toteutettaessa lokienhallinta keskitetysti voidaan sillä saavuttaa kustannussäästöjä, vaikka järjestelmän hankinta voi olla kerralla iso investointi. Organisaation riskienhallinnassa tulee arvioida, voiko lokienhallinnan laiminlyömisestä seurata rahallisia sanktioita, kun lailliisuusvelvoitteet tai sopimuksissa vaaditut kohdat eivät täyty. Seurauksena voi olla muun muassa maineen menetys huonosti hoidetun tietoturvallisuuden takia. Tietoturvan ja siihen kuuluvan keskitetyn lokienhallinnan laiminlyömisestä selkeän tarpeen edessä voi olla yritykselle ja sen asiakkaille pitkälle tulevaisuuteen haitallisesti vaikuttavia seurauksia.

Yrityksen suunnitellessa keskitetyn lokienhallintajärjestelmän hankkimista on järjestelmä hyvä rakentaa mahdollisimman standardeja mukailevaksi. Näin meneteltynä järjestelmä on myöhemmin mahdollista päivittää ja auditoida esimerkiksi PCI DSS -standardin vaatimuksia vastaavaksi. Jälkeenpäin järjestelmän muokkaaminen standardeja vastaavaksi aiheuttaa ylimääräisiä kustannuksia ja voi haitata järjestelmän normaalia käyttöä. Lokien tutkiminen keskitetystä järjestelmästä on helpompaa kaikkien lokien ollessa saatavilla yhdestä paikasta. Lokienhallinta tarjoaa usein kokonaisvaltaisen näkymän yrityksen sisäiseen tietoverkkoon, niihin kytkettyihin laitteisiin ja järjestelmiin. Havaittuihin uhkiin tai ongelmiin kyetään puuttumaan nopeammin ja ajoissa. Lokien keräämisestä on parantuneen tietoturvan lisäksi kohdejärjestelmän kuormituksen seuraaminen. Löytämällä mahdollinen tietoliikenneverkon yli- tai alikapasiteetti voidaan käytössä olevia resursseja ohjata oikein. Lisäksi voidaan löytää ongelmia aiheuttavat laitteet, jotka vaikuttavat verkon toimivuuteen, tietoturvaan tai laitteiden ja järjestelmien toimintaan. [8.],[9.]

Ilman verkon seurannan tuottamaa lokitietoa on vaikeaa arvioida, mikä on verkon normaalitila ja miten ja millä tavalla se on muuttunut. Onko joidenkin verkon osien rasitus noussut tilapäisesti ja vaatiiko se muutoksia verkkoon, jotta se palvelee käyttäjiä tehokkaasti jatkossa. Kyseessä voi olla epätavallinen kuormitus, johon tulee kiinnittää huomiota ja joka vaatii välittömiä jatkotoimia. Lokienhallinnalla voidaan löytää esimerkiksi vikatilanteissa verkon laitteisiin tehdyt muutokset, jotka ovat aiheuttaneet vikatilanteen. Organisaation tietoturvasta vastuussa olevia henkilöitä kiinnostaa tietoturvan taso, toteutuminen ja havainnointi organisaation sisällä. Kriittisissä ja vaativissa ympäristöissä voi olla erillinen tietoturvaryhmä, joka seuraa reaaliaikaisesti lokitietoja ja tietoliikennettä, havaitsee mahdolliset uhkat ja suorittaa tarvittavat toimenpiteet. Tämä ryhmä seuraa reaaliajassa tunkeilijan havaitsemisjärjestelmän (Intrusion Detection System, IDS) tietoja hyökkäysten torjumiseksi ja kohdejärjestelmän suojaamiseksi. Tämä asettaa vaatimuksia lokienvalvontajärjestelmän rakentamiseksi sillä tavoin, että se kykenee tuottamaan reaaliaikaista analyysia lokitiedoista ja korrelaatiota lokitietojen niiden välille. Käytännössä tämä vaatii Security Event Management (SEM) -pohjaisen tuotteen. Tätä varten HP ArcSight tarjoaa Enterprise Security Manager tuotetta (ESM). [9.]

Yrityksissä tai organisaatioissa, joissa ei ole keskitettyä lokien valvontaa tai laista tulevaa pakotetta sille, on tietoturvaloukkausten ja murtojen selvittäminen huomattavasti vaikeampaa. Pahimmissa tapauksissa tietomurrosta tiedetään vasta siinä vaiheessa, kun hyökkääjä ilmoittaa tehneensä murron yrityksen verkkoon. Tällöin ei pystytä selvittämään, että mistä hyök-

kääjä on tullut ja mitä tietoja yrityksen verkosta on varastettu tai vaarantunut. Syntyneiden vahinkojen arviointi on vaikeaa ja uusien estäminen haastavaa tai mahdotonta. Lisäksi hyökkääjä on saattanut jättää järjestelmään takaportteja. [8.]

3.2 Lokienhallintajärjestelmän kehittämisvaiheet

Lokienhallinnan kehittäminen ja rakentaminen voidaan jakaa erilaisiin vaiheisiin. Lokienhallinnan kehittämistyö noudattaa pitkälti tietojärjestelmien kehittämisen vaiheita, ottaen lisäksi huomioon lokienhallinnan näkökulman. Tässä työssä kehitystyötä tarkastellaan ulkoisen yrityksen tekemänä projektina työn tilaavalle asiakkaalle. Kehitystyön ulkoistamisen perusteita tarkastellaan ensin. Tämän jälkeen tulevat esiselvityksen tekeminen, etenemismalli ja tavoitetila. Käytännön osuudessa tulevat toteutus ja ylläpito. Toteutuksen osioon kuuluvat muun muassa testaus ja käyttöönottovaiheet, joita ei ole käsitelty laajemmin. Näiden osuuksien sisältö riippuu hyvin pitkälti lokienhallintajärjestelmälle asetetuista vaatimuksista, ja ne voivat vaihdella voimakkaasti. Viimeisenä vaiheena on ylläpito, johon on koottu huomioitavat asiat lokienhallintajärjestelmän ylläpitämisessä.

3.2.1 Lokienhallintajärjestelmän ulkoistaminen

Onnistuneen lokienhallinnan toteutumisessa on tärkeää lähteä etenemään suunnitelmallisesti. Lokienhallintajärjestelmät voidaan toteuttaa ulkoisen, liiketoiminnaltaan lokienhallintaan perehtyneen yrityksen toimesta kuin myös sisäisenä projektina. Toteutettaessa lokienhallinnan käyttöönotto sisäisenä projektina ostaa yritys lokienhallintalaitteet ja tarvittaessa konsultaatioapua järjestelmän käyttöönottoon. Syitä lokienhallintajärjestelmän toteuttamiseen ulkoisella yrityksellä voi olla useita. Tilaajayrityksellä voi puuttua riittävä tietotaito lokienhallinnan alueesta. Keskitettyä lokienhallintaratkaisua hakeva asiakas saattaa olla kiinnostunut keskittymään enemmän omaan ydinliiketoimintaan.

Tilaajayritys valitsee kilpailutuksen kautta ulkopuolisen yrityksen toteuttamaan lokienhallintajärjestelmän rakentaminen. Ulkopuolisen yrityksen toteuttama lokienhallintajärjestelmä voi olla kustannuksiltaan pienempi kuin yrityksen sisäisesti toteuttama. Pitkään alalla toiminut ja useita lokienhallintajärjestelmiä rakentanut yritys tuntee käyttöönottamisen prosessin ja tietää

kuinka se toteutetaan onnistuneesti. Järjestelmän pystytykseen liittyvät tyypilliset virheet ja ongelmatilanteet osataan välttää. Lokienhallintapalveluita tuottava ja markkinoiva yritys voi myös rakentaa järjestelmän tilaavalle asiakkaalle tai tuottaa sitä vaihtoehtoisesti palveluna. Lokienhallinnan palveluna ostavalle asiakkaalle taataan tietty palvelutaso ja huolehditaan lokienhallintajärjestelmän kunnossapidosta aina sovelluksista laitteistoihin. Ostettaessa lokienhallintajärjestelmä palveluna tulee tässä tapauksessa huomata, ettei lokien omistussuhde muutu, vaikka ne tallennettaisiin palveluntarjoajan tallennustilaan. Lokit ovat edelleen lokeja tuottavan järjestelmän omistajan omaisuutta. [8.]

3.2.2 Esiselvitys

Esiselvityksen tarkoituksena on saada selville yrityksen lokienhallinnan nykytila ja edellytykset lokienhallinnan toteuttamiselle. Esiselvitysvaiheessa selvitetään, miksi lokienhallintaa tarvitaan ja mistä lähtökohdista työtä lähdetään tekemään. Esiselvitykseen voidaan kirjata ongelmakohdat, joihin lähdetään hakemaan ratkaisua lokienhallinnalla. Ongelmien ratkaisemiseksi tarvitaan myös etenemismalli, kuinka asetettuihin tavoitteisiin päästään ja missä järjestyksessä. Organisaatiossa, jossa lokienhallintajärjestelmää ei ole aiemmin ollut, on tärkeää muodostaa lähtötilanne sille, millainen on lokivalvonnan kohteena olevan laitteiden ja järjestelmien normaalitila. Yrityksillä, joilla on olemassa entuudestaan lokienhallintajärjestelmä, on usein määritelty lokipolitiikka. Mikäli lokipolitiikkaa ei ole tai se ei ole ajantasainen, tulee se päivittää. Lokipolitiikka määrittelee lokien säilytykseen, käsittelyyn ja käsittelyn tarpeeseen liittyvät asiat yleisellä tasolla. [8.]

3.2.3 Tavoitetila

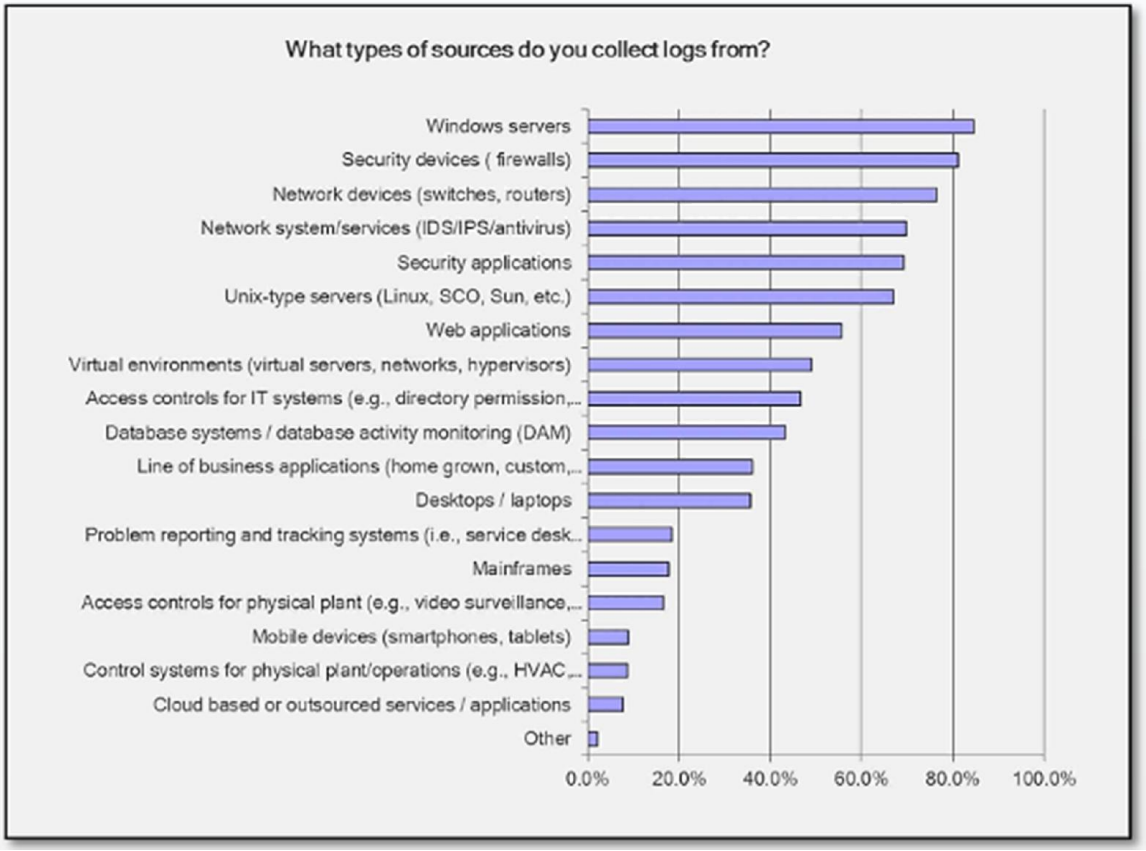
Esiselvityksen osana on selostus tavoitetilasta johon pyritään. Tavoitetilaan kirjataan selkeästi etenemismalli, kuinka tavoitteisiin päästään. Jotta lokienhallintajärjestelmä pystytään rakentamaan onnistuneesti, täytyy yrityksellä olla tarkka ja ajantasainen dokumentaatio tietoliikenneverkon arkkitehtuurista. Ilman tietoliikenneverkon arkkitehtuurin dokumentaatiota on vaikeaa suunnitella toimiva lokienhallintajärjestelmä. Joissakin tapauksissa yrityksen tietoliikenneverkon dokumentaatio on jäänyt tekemättä. Näissä tapauksissa joudutaan ensin selvittämään yrityksen verkon arkkitehtuuri, ennen kuin lokienhallintajärjestelmää voidaan lähteä

suunnittelemaan tai rakentamaan. Ajantasainen dokumentaatio helpottaa suunnittelun lisäksi toteutusvaiheessa käytännön työn tekemistä ja ongelmatilanteiden selvittämistä, kun lokia tuottavia järjestelmiä liitetään lokienhallintajärjestelmään.

Esiselvitykseen kuuluu edellä mainittujen tietojen lisäksi kokonaiskustannusarvio ja työmäärä. Työmäärän perusteella lokienhallintajärjestelmän pystytys voidaan aikatauluttaa ja varata siihen tarvittavat henkilöresurssit. Lokienhallintajärjestelmän budjettia arvioidessa on muistettava ottaa huomioon järjestelmän ylläpitämisestä aiheutuvat kustannukset. Tällaisia ylläpitotoimia ovat esimerkiksi laitteiden ja sovelluksien päivittäminen. Päivitykset sisältävät usein virheiden korjauksia, parannuksia ja uusia ominaisuuksia. Näiden käyttöönottaminen vaatii rahallista panostusta. Lokienhallintajärjestelmän tukilisenssien pituudet ja valmistajan ylläpidon kattavuus on huomioitava vikatilanteita ajatellen. Järjestelmän ylläpidon laiminlyönti voi nopeuttaa lokienhallintajärjestelmän vanhentumista. [8.]

Lokien kerääminen

Lokijärjestelmän suunnittelussa tulee tunnistaa alkuvaiheessa, millaista tietoa lokien keräysjärjestelmään halutaan kerätä. Lokienhallintajärjestelmää ei voida lähteä rakentamaan ilman tietoa lähdejärjestelmän laitteista, koska ei tiedetä, kuinka ne konfiguroidaan lähettämään loki uuteen järjestelmään. VAHTI-ohjeistuksessa [8, s. 23] on annettu kuvaus, millaisten järjestelmien tulee tuottaa lokia: ”Tietojärjestelmien ja ympäristön turvallisuutta tukevien järjestelmien tulee kerätä lokitietoja.” Lokitietoa voidaan kerätä tyypillisesti yrityksessä eri käyttöjärjestelmistä tietoliikenneverkon laitteista, kuten kytkimistä ja reitittimistä. Kuvassa 3 on SANS-yhtiön tuottamasta dokumentista otettu kuva lokien keräyskohteista vuodelta 2013. Kuvasta nähdään, että Windowsin suosio yleisimpänä käyttöjärjestelmänä aiheuttaa sen, että se on myös yleisin lähde, josta lokia kerätään. Seuraavana tulevat tietoliikenneverkon laitteet, joita löytyy lähes poikkeuksetta kaikkien yritysten verkosta, kuten palomuurit, kytkimet ja reitittimet



Kuva 3. Lokeja kerätään eniten Windows palvelimista, palomuureista ja tietoliikenneverkon laitteista [10, s. 6].

Käyttäjät yksilöiviä lokitietoja kerätessä on huomattava, että niistä muodostuu henkilörekisteri. Näiden tietojen tallentamisesta henkilötietolaki määrää, ettei tarpeetonta tietoa saa kerätä. Jos henkilötietoja on tarpeen kerätä, täytyy keräämiselle löytyä peruste. Henkilötietoja sisältävät lokitiedot ovat usein arkaluonteista ja luottamuksellista tietoa, ja niiden keräämisestä on säädetty laissa. Tarpeettoman lokitiedon keräämisen voi mieltää helposti sivuseikaksi, jos kerättävät lokimäärät ovat kokonaisuudessaan vähäisiä. Suuria lokimääriä kerätessä tarpeettoman lokitiedon kerääminen vie tallennustilaa, varsinkin jos lokeja arkistoidaan pitkäksi aikaa. Ylimääräinen lokitieto hidastaa myös analysointia. [8.]

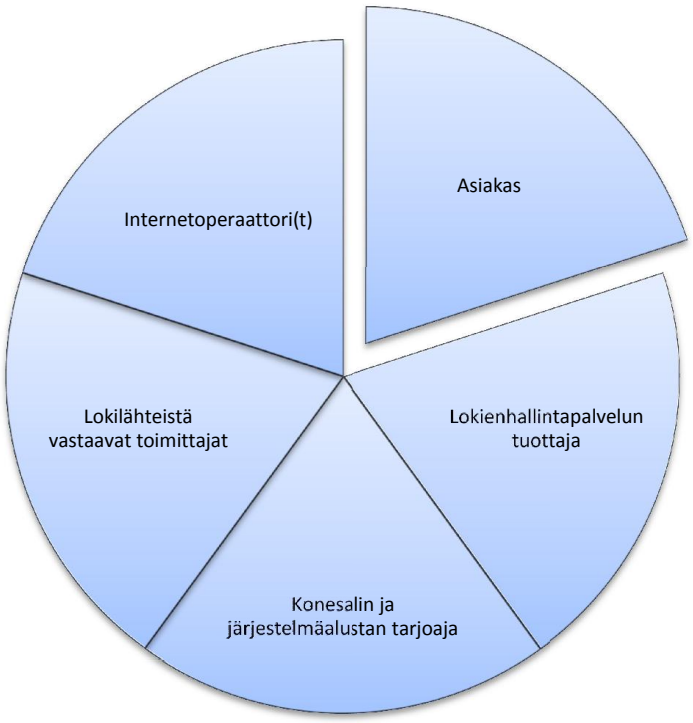
Säilyttäminen

Järjestelmää suunniteltaessa on selvitettävä, millaisia lokeja järjestelmään aiotaan tallentaa. Lokitiedon määrään vaikuttaa, kuinka paljon lokia tuottavia lähteitä on ja paljonko lokia kertyy tietyssä ajassa. Lokien säilytysaikojen pituudet ja arkistointi tulee olla suunniteltu. Kustannussyistä lokitietoja ei ole järkevää säilyttää jatkuvasti sekä nopeasti saatavilla. Lokit, joita

ei tarkastella päivittäin, kannattaa tietyn ajan jälkeen pakata ja arkistoida. Pitkäaikaislokeja säilytetään usein lainsäädännöllisistä tai muista standardeista tulevista määräyksistä johtuen, vaikka niille ei ole muuten käyttöä.

3.2.4 Osapuolet

Ennen lokienhallintajärjestelmän rakentamista on hyvä sopia lokijärjestelmän vastuualueet ongelmien välttämiseksi projektin aikana. Lokienhallintajärjestelmän rakentamisessa voi olla mukana useita eri osapuolia ostavan asiakkaan ja myyjän lisäksi. Kuvassa 4 on kuvattu ympyrämallin avulla kokonaisuus, josta järjestelmän rakentaminen koostuu kokonaisuudessaan. Lokienhallintajärjestelmää ei koskaan voida rakentaa ulkopuolisen toimittajan puolesta ilman tiivistä yhteistyötä asiakkaan kanssa.



Kuva 4. Lokienhallintaprojektin rakentamisen osapuolet.

Yksi osapuoli voi olla palveluntarjoaja, joka tarjoaa konesalitilat asiakkaan laitteille tai mahdollisesti virtuaalialustan. Verkkoyhteydet saattavat olla yhteyksien varmuuden maksimoimiseksi kahden eri Internet-operaattorin eli ISP:n tarjoamana. Tyypillisesti toisen operaattorin yhteys toimii varayhteytenä. Mikäli asiakkaan lokilähteet ovat monimutkaisia laitteita, joiden

hallinnointi ja huoltaminen eivät ole asiakkaan vastuulla, on laitteiden lokiin liittyvät kysymykset ohjattava näistä vastaaville tahoille. Lokienhallintajärjestelmän osa-alueiden vastuu on tärkeää olla kaikille osapuolille selvillä. Vastuun lisäksi on huomioitava, missä ajassa viat on kyettävä selvittämään ennen mahdollisia sanktioita. Vikatilanteessa vastuualueiden selvittäminen hidastaa vian korjaamista ja paikallistamista. Osapuolten velvollisuudet ja säännökset on usein kirjattu Service Level Agreement (SLA) -sopimuksiin. [8.]

3.2.5 Etenemismalli

Etenemismalliin kirjataan kuinka selvityksestä päästään haluttuun tavoitetilaan. Tavoitetilaksi voidaan määritellä lokienhallintajärjestelmän toiminta esitettyjen vaatimusten mukaisesti. Etenemismalliin kuuluu myös havaittujen ongelmien priorisointi lokienhallintajärjestelmän kehitystyössä. Käytännössä lokienhallintajärjestelmän rakentaminen vaiheistetaan ja aikataulutetaan. Lisäksi selvitetään myös mahdolliset riippuvuudet toisiinsa, jolloin tiedetään mitä osia projektista voidaan edistää samaan aikaan. Tällä saavutetaan kustannustehokkuutta.

3.3 Toteutus

Toteuttaminen tarkoittaa projektin alussa määriteltyjen asioiden toteuttamista vaatimusten mukaiseksi järjestelmäksi suunnitellussa aikataulussa.

3.3.1 Aikapalvelimet ja NTP-protokolla

Järjestelmän rakennusvaiheessa ensimmäisenä tulee ottaa huomioon, että kohde- ja lähdejärjestelmän laitteet ovat samassa ajassa. Käytännössä tämä vaatii UDP-pohjaista protokollaa (Network Time Protocol, NTP) käyttävän aikapalvelimen käyttöönottamista yrityksen verkossa. Tämä on toimivan lokienhallinnan yksi keskeisin vaatimus. Tämä vaatimus esitetään muun muassa PCI DSS -standardissa VAHTI-lokiohjeessa. Standardissa ei määritellä, että NTP-teknologiaa tulee käyttää, mutta se esitellään yhtenä ratkaisuna. [8],[11.]

3.3.2 Aikapalvelinten merkitys

Tarkalla ajalla voidaan lokienhallintajärjestelmässä tehdä aikajana tapahtumien kulusta, jonka avulla voidaan selvittää kohdejärjestelmän tapahtumia. Usein tätä tarvitaan viimeistään siinä vaiheessa, kun selvitetään tietomurtoa. Parhaimmillaan lokeista nähdään kaikki laitteet, joihin murtautuja on päässyt sisälle, sekä yhteydet ja reitit, joita on käytetty. Tämän perusteella voidaan tehdä arvio, kuinka paljon mitäkin tietoa on vaarantunut tai varastettu. Tämän takia aikapalvelimet ja NTP-protokolla ovat tärkeässä asemassa lokienhallintajärjestelmässä.

3.3.3 Aikapalvelinten määrä

Pienessä ympäristössä kaikki verkon laitteet voidaan asettaa synkronoimaan aikansa aikapalvelimelta. Suosituksena on käyttää vähintään neljää, mutta korkeintaan viittä NTP-aikapalvelinta. Neljältä palvelimelta ajan hakeva laite pystyy päättelemään, onko jokin ajan tarjoavista palvelimista väärässä ajassa. On myös mahdollista, että aikapalvelin on sillä hetkellä saavuttamattomissa. Tässä tilanteessa loput kolme palvelinta tarjoavat ajan, ja niistä voidaan päätellä kaksi tarkimmassa ajassa olevaa palvelinta. Kuusi aikapalvelinta aiheuttaa turhaa aikapalvelimen vaihtumista laitteissa. Suositeltavaa ei ole käyttää aikapooleja. Näissä yhden aikapalvelinosoitteen takana on usein useita satoja aikapalvelimia. Vaihtuvuus on tällöin suurta, ja on mahdollista, että jokaisella ajan synkronointikerralla aika saadaan eri palvelimilta. Tässä tapauksessa aikaa hakevat laitteet eivät opi arvioimaan, missä suhteessa niiden kello edistää tai jätättää. [12.],[13.]

Mikäli verkon laitteet sijaitsevat eri verkoissa, fyysisesti eri sijainneissa tai eri aikavyöhykkeillä, on aikapalvelinten sijoittaminen mietittävä tarkkaan. Tällaiset tapaukset tulevat esille tilanteissa, joissa yrityksellä on toimipisteitä ympäri maailman ja lokitiedot halutaan kerätä keskitetysti yhteen järjestelmään. Tämä vaatii usein kullekin aikavyöhykkeelle aikapalvelimen sijoittamisen, joka tarjoaa ajan lokia tuottaville lähdejärjestelmille tai laitteille ajan.

3.3.4 Stratum-tasot

Palvelimet eivät pysty päättelemään pelkän saadun ajan perusteella, mikä käytettävissä olevista NTP-palvelimista on tarkin mahdollinen. Tämän takia mukaan lisätään aikapalvelimen Stratum-taso. Stratum-tasot on määritelty taulukon 1 mukaisesti ja tasojen numerointi jatkuu kronologisesti eteenpäin. Mitä suurempi Stratum-tason numero on, sitä epätarkempi sen aika on verrattuna alkuperäiseen lähteeseen. [12.]

Taulukko 1. Stratum-tasot 0–3.

Stratum 0	Atomikellot ja ajan mittaukseen tarkoitetut GPS-vastaanottimet. Näitä ei voida suoraan liittää verkkoon, vaan ne vaativat esimerkiksi palvelimen.
Stratum 1	Palvelin, joka hankkii ajan atomikellolta. Kaikista tarkin mahdollinen lähde, josta aika voidaan jakaa käytettäväksi verkon laitteille.
Stratum 2	Laitteet, jotka ottavat ajan Stratum 1 -tasoiselta palvelimelta
Stratum 3	Laitteet, jotka synkronoivat ajan Stratum 2 -tasoiselta palvelimelta.

Jos yrityksessä tai verkossa halutaan saavuttaa korkeatasoinen NTP-aikapalvelin, saadaan se parhaiten hankkimalla verkkoon oma palvelin tai laitteisto, jonka tehtävänä on poimia aikasignaali suoraan satelliitin GPS-signaalista. Aikapalvelimen tärkeydestä kertoo muun muassa se, että PCI DSS -standardissa vaaditaan verkon laitteille tietty Stratum-taso. Yrityksen omassa verkossa olevasta NTP-aikapalvelimesta on etua. Kriittisen järjestelmän, muutoin erityisesti suojattavan verkon tai suljetun verkon ei tarvitse olla kytkettynä Internetiin tarkan ajan saamiseksi, jos NTP-palvelin on toteutettu GPS-signaalista ajan ottavalla laitteella. Tietomurtojen riskejä voidaan tällä tavoin pienentää. [11.],[12.]

3.4 Testaus

Ennen kuin järjestelmä voidaan ottaa tuotantokäyttöön, täytyy sen toimivuus testata. Testauksessa selvitetään, toimiiko lokienhallintajärjestelmä esitettyjen vaatimusten mukaisesti. Lisäksi testauksella voidaan muun muassa selvittää, esiintyykö järjestelmässä tai sen osassa ongelmia, joita ei ole huomioitu suunnittelussa tai rakennusvaiheessa. Yhtenä tärkeänä asiana on hyvä selvittää, miten järjestelmä toimii yleisimmissä vikatilanteissa ja kuinka niistä toivutaan. Lokienhallintajärjestelmä, jonka täytyy toimia ympäri vuorokauden kaikkina viikonpäi-

vinä lukuun ottamatta huoltokatkoja, vaatii valvonnan toimivuuden varmistamiseksi. Testauksessa on tällöin hyvä selvittää, toimiiko valvontajärjestelmä toivotulla tavalla ja osaako se ilmoittaa lokienhallintajärjestelmän laitteiden vikatilanteista. Testauksen aikana voidaan lisäksi tehdä opas yleisimpien lokienhallintajärjestelmän vikatilanteiden toteamiseksi ja selvittämiseksi. Testauksen osalta tulee muistaa, että testauksesta ei voida tehdä täydellistä, koska muuttuvien tekijöiden määrä on liian suuri.

3.5 Lokienhallintajärjestelmän ylläpito

Järjestelmän ylläpitämisessä on hyvä huomioida, että yrityksen muuttuva tietoliikenneverkko vaatii myös muutoksia lokienhallintajärjestelmään. Yrityksen verkkoon lisätyt uudet laitteet on konfiguroitava lähettämään lokit lokienhallintajärjestelmään. Laitteet, joihin löytyy suora tuki lokienhallintajärjestelmästä, voidaan konfiguroida lähettämään lokitietoa. Vaihtoehtoisesti tuotteesta voidaan kerätä lokitietoa. Tuotteen ollessa uusi tai jos sitä ei ole tuettu HP ArgSightin puolelta, joudutaan tuotteelle tekemään tätä varten kustomoitu lokienkeräin. Lokienhallinnanjärjestelmän laitteet voivat sijaita fyysisesti asiakkaan tiloissa, järjestelmän toimittajan tiloissa tai näiden yhdistelmänä tuotettavassa muodossa.

Luottokorttidataa käsittelevässä lokienhallintajärjestelmässä täytyy tietoturvaan kiinnittää erityistä huomiota. Monet rahaliikennettä käsittelevät yhtiöt noudattavat PCI DSS-standardia. Standardi määrittelee, millaisia keinoja ja tapoja voidaan käyttää kortinhaltijoiden tietojen suojaamiseen. Näiden keinojen noudattamista vaaditaan PCI DSS -luokituksen saamiseksi. Näistä voi ottaa mallia lokienhallintajärjestelmän käytäntöihin, vaikka standardia ei otettaisi käyttöön. [11.]

PCI DSS -standardissa on määritelty kulunvalvonnan ja vierailijalokin käyttäminen tiloissa, joissa lokienhallinnan laitteet sijaitsevat. Vierailijalokin ylläpitämistä helpottaa kulunvalvontajärjestelmä, josta saadaan automaattisesti ja vaivattomasti kulkuaika henkilöille, jotka pääsevät tilaan, jossa lokienhallinnan palvelimia säilytetään. Vierailijoista, joille ei anneta vierailijakorttia, tulee pitää käsin vierailijakirjaa. Vierailijoilla tulee olla kaikissa tilanteissa saattaja mukanaan kaikkiin niihin tiloihin, joissa korttitietoa sisältävää tietoa käsitellään tai säilytetään. Tiloihin pyrkivällä henkilöillä tulee lisäksi olla mukanaan asianmukainen henkilöllisyystodistus. [11.]

Lokienhallintajärjestelmän laitteiden ja ohjelmien päivitys tulee suunnitella tarkoituksenmukaisesti. Järjestelmää ei ole kannattavaa päivittää jokaiseen uuteen versioon, ellei se ole saatuun hyötyyn nähden tarpeeksi kannattavaa. Ennen kaikkea päivityksiä olisi hyvä koeajaa testiympäristössä, jossa voidaan havaita mahdolliset ongelmat. Aina uudet versiot eivät pelkästään korjaa olemassa olevia ongelmia. Ne saattavat samalla luoda uusia entuudestaan tuntemattomia ongelmia. Avainasemassa tällaisissa tilanteissa on regressiotestaus, jossa aiemmin suoritettuja testejä ajetaan uudessa versiossa ja etsitään mahdollisia virheitä. Suositeltavaa on laatia testaussuunnitelma, joka suoritetaan päivitettäessä järjestelmää tai sen komponentteja.

3.6 Lokitiedot

Lokien kerääminen kohdeympäristöstä ja laitteilta tulee suorittaa riittävällä tarkkuudella. Tähän tulee sisältyä vähintään seuraavat asiat:

Mikä tapahtuma on kyseessä: Onko tapahtuma onnistunut vai epäonnistunut. Kerättävästä tiedosta tulee poimia onnistuneet tapahtumat ja epäonnistuneet sisäänkirjautumiset. Pelkästään onnistuneiden kirjautumisten kerääminen antaa virheellisen kuvan järjestelmän toiminnasta, tietoturvan tasosta ja murtautumisyrityksistä kohdejärjestelmään. [8],[14.]

Tapahtuman tekijä: Riippuen autentikoinnin tasosta ja kerättävistä tiedoista voidaan selvittää tarkasti tapahtuman suorittaja. [8],[14.]

Ajankohta: Milloin tapahtuma on tapahtunut. [8],[14.]

Tarpeettoman tiedon keräämistä tulee kuitenkin välttää. Se vie pitkällä aikavälillä tilaa olennaiselta lokitiedolta, hidastaa analyysien tekemistä ja tärkeiden epäkohtien havaitsemista. Lokien keräysjärjestelmä tulee suunnitella siten, että se estää kerättyjen lokien muuttamisen, ja jos mahdollista, lokienkeräysjärjestelmään lähetettävien lokien muuttamisen. Tämä tulee erityisen tärkeäksi silloin, kun järjestelmään, sovellukseen tai laitteeseen murtaudutaan. Valvontajärjestelmä ei välttämättä tällöin estä murtautujaa toimimasta, mutta estää hyökkääjää peit-

tämästä tietomurron jälkiä. Mikäli lokeja muutetaan, tulee siitä aiheutua automaattisesti hälytys järjestelmää valvoville ylläpitäjille. Myös ylläpidon toimet lokienvalvontajärjestelmässä tulee kirjata. Tämä antaa selkeän kuvan muutoksista tai päivityksistä, joita järjestelmään on tehty. [8.]

3.6.1 Lokitiedon merkitys

Monissa organisaatioissa keskitetyn lokienhallinnan tärkeimpänä vaatimuksena on lokien eheyden turvaaminen. Ulkopuoliset tai lokia tuottavien järjestelmien käyttäjät eivät saa päästä muuttamaan lokitietoja tai edes tarkastamaan niitä. Lokien avulla täytyy pystyä kiistämättömästi osoittamaan tapahtuma ja tarvittaessa todistusaineistona. Esimerkiksi sairaanhoidossa lokien avulla varmistetaan potilaiden oikeusturvan toteutuminen ja pystytään selvittämään väärinkäytökset. [8.]

Lokienhallinnan merkitys korostuu väärinkäyttötapauksissa, joissa hyökkääjä murtautuu kohdejärjestelmään toisen käyttäjän tunnuksilla. Näissä tapauksissa lokienhallintajärjestelmällä on ensin luotu malli lokin keräyksen kohteena olevasta järjestelmästä ja sen normaalista toiminnasta. Valvontajärjestelmä tunnistaa käyttäjän poikkeavan toiminnan, ja se voidaan tällöin asettaa hälyttämään poikkeavasta tapahtumasta. Osassa ohjelmistoja, jotka on rakennettu tiukasti Security and Event Management -järjestelmän (SIEM) yhteyteen, on mahdollista estää käyttäjätilin toiminta muun muassa lukitsemalla se kohdejärjestelmän suojaamiseksi. Tämä tulee toteuttaa asettamalla valvontajärjestelmään auditointijärjestelmä, joka valvoo kaikkea kirjautumista lokienhallintajärjestelmään ja kerää siihen liittyvät lokit. Näin kaikki muutokset kirjautuvat automaattisesti ja tarvittaessa muutoksista, jotka vaativat välitöntä reagointia, voidaan saada hälytykset. Tämä myös tuo turvaa tietomurtotilanteissa, jos lokienhallintajärjestelmään päästään murtautumaan ei murtautumisen jälkiä pystytä peittämään. [8.]

3.6.2 Lokien analysointi

Kaikkien lokimerkintöjen läpi käyminen ja tarkasteleminen käsin ja yksitellen olennaisen tiedon löytämiseksi on mahdotonta. Tästä syytä kerätystä lokitiedoista on tehtävä analyyseja, joiden pohjalta havaitaan poikkeamat, jotka vaativat tarkempaa tarkastelua. Lokitietoa on

myös kategorisoitava sopivalla tavalla. Kunkin organisaation tarpeet vaihtelevat, ja yhtä oikeaa mallia jaotteluun ei ole olemassa. Jaottelun pohjana voidaan käyttää VAHTI-lokiohjetta, jossa lokit on jaettu neljään tyypillisimpään luokkaan: ylläpitoloki, käyttöloki, muutosloki ja virheloki [8.]

Lokitietojen luokittelussa on huomattava, että lokitietoa tarkastelevat usein eri henkilöt, eikä kaikilla ole tarve päästä kaikkiin lokitietoihin käsiksi. Tässä myös lainsäädäntö (sähköisen viestinnän tietosuojalaki, henkilötietolaki ja työelämän tietosuojalaki) asettaa rajoitteita, jos lokitiedot sisältävät henkilötietoja. Jos lokienhallintajärjestelmässä on mahdollisuus suojata henkilötiedot tai muutoin arkaluonteiset tiedot, tulee tätä ominaisuutta hyödyntää. Erityisesti kannattaa tutkia, onko lokitietoa mahdollista suojata lähdelaitteesta lokitietoa kerätessä. Kerätty loki päätyy keskitettyyn lokienhallintajärjestelmään suojattuna koko sen matkan ajan. Yksi mahdollisuus suojata arkaluonteista tietoa on käyttää korvikenumeroita, jolloin riski väärinkäytöksistä on huomattavasti pienempi järjestelmään tarkastelevien henkilöiden väärinkäytöksien osalta. Tiedon suojaamisella matkalla saavutetaan lokitiedon luottamuksellisuuden pysyminen. Tiedot ovat vain niihin oikeutettujen henkilöiden tarkasteltavissa. Mikäli lokitietoja ei suojata matkan aikana, on mahdollista, että joku luvaton henkilö pääsee kaappaamaan lokiliikennettä. [8.]

Lokitiedon analysointia tehtäessä on otettava huomioon useita erilaisia näkökulmia. Organisaatiossa saattaa olla useita henkilöitä, jotka tarkastelevat lokitietoja eri syistä. Tavallisesti tarve tarkastella lokeja tulee vianselvityksen yhteydessä. Tällöin tietoliikenneverkkoa ylläpitävälle henkilölle on ensiarvoisen tärkeää, että hän pääsee tutkimaan verkon lokitiedostoja pitkältä aikaväliltä, jolloin vian paikallistaminen nopeutuu. Yritysten tietoliikenneverkot pysyvät harvoin muuttumattomina monia vuosia. Ennen kuin analyyseja lähdetään tekemään lokitietojen pohjalta, täytyisi kohderyhmille poimia lokitiedoista ne asiat, jotka vaativat tarkempaa tarkastelua. Analyysin ulkopuolelle voidaan jättää tarkasteltavien lokitietojen ulkopuolelle järjestelmän normaalista toiminnasta kertovat tapahtumat. Täytyy kuitenkin muistaa, että lokitietoa voidaan käyttää hyväksi normaalin tilan kartoittamiseksi ja tilastotiedon keräämiseksi. [8.]

Noudattamalla lokien analysoinnissa säännöllisyyttä saavutetaan vertailupohja sille, mikä on järjestelmän normaalia toimintaa, mitkä muutokset ovat uusia ja onko niiden alkuperään tarvetta perehtyä. Tämä mahdollistaa poikkeamien havaitsemisen ja niihin reagoimisen ajoissa ja riittävällä vakavuudella. Lokeihin pätevät samat säännöt kuin muuhunkin onnistuneeseen

tiedon käsittelyyn: lokitiedon saatavuus, suojaus, eheys ja laatu tulee olla kunnossa. Lokien analysointi vaatii usein ihmisen silmää tunnistamaan poikkeustapaukset ja tilanteet, jotka vaativat toimenpiteitä riippumatta siitä, kohdistuvatko ne käyttäjiin tai laitteisiin. [5.]

3.6.3 Jäsentely ja lokimuunnos

HP ArcSightin tuotteilla ja yleisesti ottaen lokienhallinnassa lokien jäsentely, lokimuunnokset ja lokien muuntaminen ihmiselle helposti luettavaan muotoon kuuluu kaikki tiukasti yhteen. Lokien jäsentelyssä tarkoitetaan lähdelokissa olevien tietojen lukemista siten, että ne voidaan siirtää toiseen formaattiin halutulla tavalla. Toiseen formaattiin siirtämistä nimitetään lokimuunnokseksi, jossa koko loki muunnetaan lähdelokimuodosta lokienhallintajärjestelmä formaattiin. HP ArcSightin tuotteilla lokimuunnos tehdään lähdelokimuodosta Common Event Format (CEF)-muotoon. Alkuperäinen loki voidaan kuitenkin säilyttää RAW Event -muodossa CEF-muotoisessa lokissa. Tämä on erityisen tärkeää silloin, jos lokia joudutaan tarkastelemaan jälkeenpäin erityisen suurella tarkkuudella. Tällöin alkuperäisestä lokista on selkeää hyötyä tarkastelua tehdessä. Lokitiedon sisällyttämisessä tulee kuitenkin huomioida lokin koon kasvaminen. Tällä on erityisen paljon merkitystä silloin, kun kerättävää lokitietoa on paljon. [8.]

Lokimuunnoksessa tehdään samalla myös lähdejärjestelmästä tulevan turhan lokitiedon suodatusta, yhdistämistä ja normalisointia. Suodatuksessa ylimääräinen loki, jonka katsotaan olevan tarpeetonta, suodatetaan pois. Tätä lokia ei välitetä ollenkaan lokienhallintajärjestelmään. Yhdistämisellä tarkoitetaan samankaltaisten lokitietojen yhdistämistä yhdeksi tiedoksi, joka välitetään lokienhallintajärjestelmään. Tyypillinen esimerkki tästä on usean samanlaisen lokitiedon tuleminen samalta laitteelta, joiden sisältö on sama, ainoastaan lokin tapahtuma-ajalla eroa muutama millisekunti. Nämä lokit yhdistetään yhdeksi lokitiedoksi, joka välitetään lokienhallintajärjestelmään. Yhdistämisellä poistetaan samankaltaisten lokitietojen kerääminen lokienhallintajärjestelmään sekä sen kuormittuminen ja tallennuskapasiteetin kuluminen. [8.],[15.]

3.6.4 Normalisointi

Lokien normalisoinnilla tarkoitetaan lokitiedossa olevien tietojen muuttamista yhtenäiseen esitysmuotoon. Tähän sisältyy myös lokitiedon luokittelu vastaavalla tavalla. Hyvin tyypillinen esimerkki normalisoinnista on lähdelokin ajan yhtenäistäminen. Pelkästään Unix- ja Windows käyttöjärjestelmät käyttävät periaatteeltaan erilaista tekniikkaa ajan mittaamiseen. Unixissa käyttöjärjestelmässä käytetään ajan mittaamiseen Unix-aikaa, josta käytetään myös nimitystä Epoch-aika. Epoch-aikaa käytettäessä aloitetaan ajan laskeminen siitä, kuinka monta sekuntia on kulunut 1. tammikuuta 1970 tähän hetkeen. Suomalaisissa tietojärjestelmissä ja käyttöjärjestelmissä käytössä on harvemmin 12 tunnin aikaformaatti 24 tunnin sijaan, mutta tämäkin on mahdollista. Tällöin lähdeaika on muunnettava yhteen muotoon, joka on yleensä 24 tunnin esitysmuoto. Lisähaasteita tuottaa, jos lokia tuottavat laitteet sijaitsevat eri aikavyöhykkeillä. Näissä tapauksissa eri muodossa oleva aika pitää lisäksi muuttaa lokientallennusjärjestelmässä sovittuun paikalliseen aikaan. [8.],[15.]

3.6.5 Arkistointi

Arkistointi on lokitiedon pitkäaikaissäilyttämistä. Lokin arkistointiajan pituus riippuu kerättävän lokin tarkoituksesta. Arkistoinnin yhteydessä tehdään yleensä lokien tiivistämistä ja supistamista. Tiivistämisessä loki pakataan säilytystä varten niin tiiviisti kuin mahdollista kuitenkaan muuttamatta lokin sisältöä. Lokien supistamisessa lokista poistetaan tarpeettomia tietokenttiä, jotta lokin viemä tila saadaan minimoitua. Tiivistäminen ja supistaminen vaikuttavat merkittävästi siihen, kuinka paljon tallennustilaa arkistoitavalle lokitiedolle tarvitaan. Lokien arkistointiajan pituutta säätelee laki, jossa on määritelty vaatimuksia lokitiedon säilytykselle. Loki kertoo usein jostakin tapahtumasta tai tiedon tallentamisesta ja käsittelystä, kuten on aiemmin mainittu. Täten lokitiedon tulee olla saatavilla samaan tapaan kuin tieto, jota loki koskee. Joissakin tapauksissa pidempään kuin itse tieto, josta loki on muodostunut. Lokitieto toimii luotettavana todisteena, kun tarkastellaan, että onko lokin kohteena oleva tieto tuhottu tai hävitetty asianmukaisesti. Tästä johtuen lokia säilytetään pidempään kuin itse tietoa. [8.],[15.]

Lokitieto, jonka säilytysaika umpeutunut, on tuhottava asianmukaisesti. Lisäksi on huolehdittava, että tieto tuhotaan myös varmuuskopioista. Käytännössä tietojen tuhoaminen varmuuskopioista kuten varmistusnauhoilta voi olla hankalaa. Lokitiedon tuhoamista voi kuitenkin helpottaa esimerkiksi suunnittelemalla lokitietojen varmuuskopioinnin siten, että eri säilytysajat vaativat lokitiedot ovat eri varmuuskopioilla. Tällöin ne hävitetään esimerkiksi varmistusnauhalle kopioitaessa normaalin kierron mukana. Tietoturvan takaamiseksi varmuuskopioiden suojaaminen salauksella on suositeltavaa. [8.]

3.6.6 Lokien suojaaminen

Jotta lokitieto on luotettava todiste jostakin tapahtumasta, on tärkeää, ettei lokeja voi tuhota tai muuttaa oikeudettomasti. Pääperiaatteena voidaan pitää, että lokitietoja ei saa päästä muokkaamaan niiden syntymisen jälkeen missään vaiheessa. Jos lokin tietoa joudutaan muuttamaan jostain syystä, voidaan yleisenä hyvänä periaatteena pitää seuraavaa: Muutoksen kohteena olevasta lokista kirjataan uusi arvo ja säilytetään kuitenkin vanha. Tästä muutoksesta muodostuu ”Audit Trail” -loki, josta näkee selvästi tapahtuneen. Lokien suojaamiseen kuuluu myös lokien katseluoikeuksien rajoittaminen. Lokien tarkastelusta ja niiden yrityksistä tulee pitää myös kirjaa. Tämä on tärkeää varsinkin niissä tapauksissa, kun lokitiedot sisältävät henkilötietoja tai muutoin arkaluonteista lokitietoa. [8.]

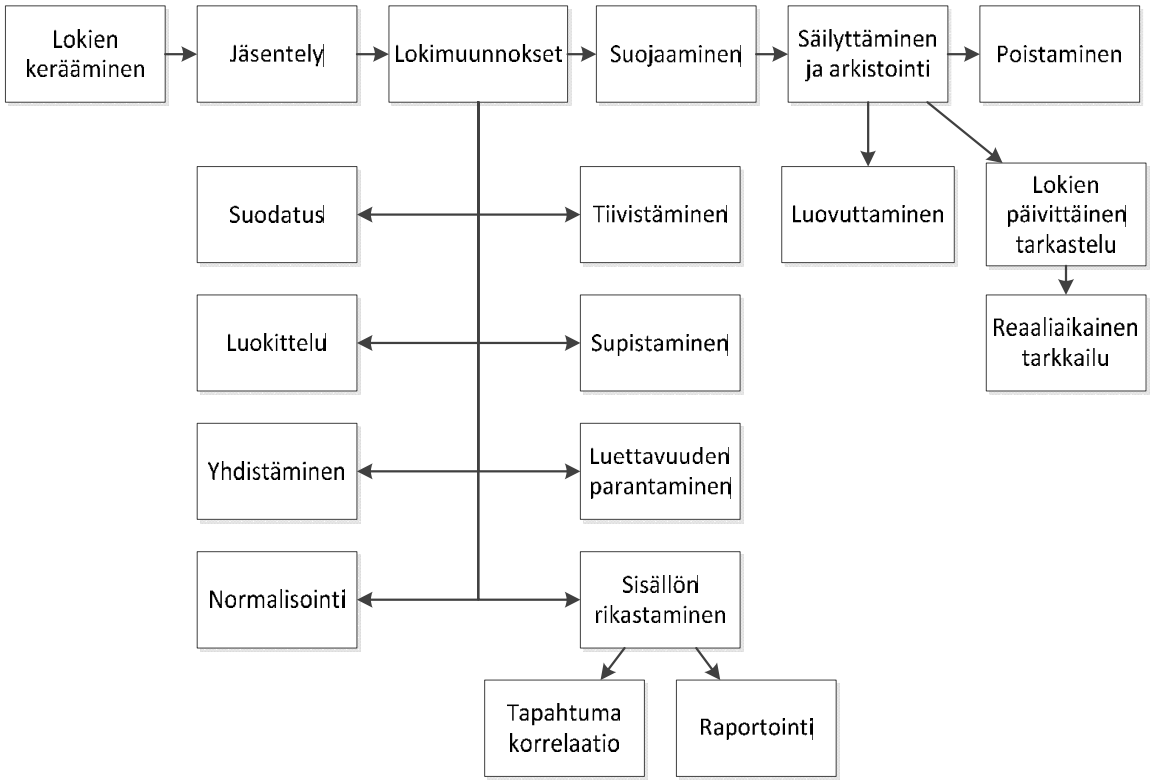
3.6.7 Lokien raportointi ja tarkkaileminen

Lokitietojen keräämistä ja tallentamista tulee seurata säännöllisesti jo pelkästään sen takia, että tiedetään mitä tietoa tallennetaan järjestelmään ja kuinka paljon. Lisäksi tilanteet, joissa lokia tuottava laite tai järjestelmä päivitetään, voivat merkitä muutoksia lähdelokin muotoon. Ellei tätä ei ole huomioitu ennen päivittämistä, voi lokimuunnos CEF-formaattiin epäonnistua. Lokitiedoista voidaan myös havaita mahdolliset poikkeamat, jotka vaativat toimenpiteitä. Kaikkien lokitietojen läpikäyminen ei ole ajallisesti järkevää tai tehokasta. Tämän takia raportit lokitapahtumista ovat tärkeitä. Raportit ovat usein yhteenveto sovitulta aikaväliltä, jolloin lokitapahtumia on kerätty. [8.],[15.]

3.6.8 Tapahtumakorrelaatio

Tapahtumakorrelaatiossa lokienhallinta menee raportointia pidemmälle. Lokienhallinnassa tapahtumakorrelaatiolla tarkoitetaan lokien perusteella tehtävien sääntöjen, sekvenssien ja kuvioiden yhdistämistä tapahtumaketjuksi, jonka avulla voidaan päätellä yhteneväisyyksiä. Korrelaatiotekniikka on useimmissa järjestelmissä samalla sisällön rikastamista, tosin edistyneemmin kuin raportoinnissa. Lokitapahtumien näkeminen tapahtumaketjuina, jotka liittyvät toisiinsa, on helppoa käyttäjälle. Tietojärjestelmälle se on kuitenkin opetettava, ja useimmat järjestelmät ovat entistä tarkempia, mitä pidempään niitä käytetään. [8],[15],[16]

Lokien korreloinnissa lokienkeräysjärjestelmä valvoo saapuvia lokeja ja etsii edellä mainittuja loogisia sekvenssejä, kuvioita ja arvoja, jotka ovat muutoin näkymättömiä erillisten järjestelmien avulla. Sen perusteella pystytään suorittamaan nopeita toistuvia analyyseja saapuvista lokeista ja havaitsemaan normaalista poikkeavia tapahtumaketjuja. Tietoturvatapahtumien valvonta automatisoituu näin merkittävästi. Käyttäjälle jää tehtäväksi tutkia lokienvalvontajärjestelmän tuottamat analyysit ja ryhtyä niiden perusteella tarvittaviin toimenpiteisiin. Järjestelmät, jotka sisältävät edistynyttä lokien korrelaation havaitsemistekniikkaa, ovat usein SIEM-järjestelmiä. Kuvassa 5 on esitetty kaikki aiemmin selitetyt lokitiedon käsittelyyn liittyvät vaiheet aina lokin elinkaaren loppuun, jolloin se poistetaan. [15],[16]



Kuva 5. Lokitiedon elinkaari ja sen vaiheet.

3.7 SIEM ja lokienhallinta

Hyvin toteutettu lokienhallinta mahdollistaa aukottoman tapahtumaketjun, jonka seuraamisella voidaan todentaa tapahtuneita. Suurimmassa osassa tapauksista lokienhallintajärjestelmä on rakennettu tavallisesti SIEM:n kaltaiseksi järjestelmäksi. HP ArcSightin on ratkaissut asian jakamalla lokienhallinnan kahteen osaan. Security Information Management (SIM), jota tässä työssä käsitellään tarkoittaa jälkeenpäin tehtävää lokien tutkimista. Security Event Management (SEM) tarkoittaa reaaliaikaista lokien korreloimista ja hälytysten tekemistä. Tätä varten HP ArcSight tarjoaa Enterprise Security Manager tuotetta (ESM). Ottamalla käyttöön HP ArcSightin SIM ja SEM tuotteet saadaan SIEM kokonaisuus.

Vaihtoehtoisesti Loggeri voidaan liittää olemassa olevan SIEM-järjestelmän yhteyteen. Kokonaisuus voi olla myös rakennettu eri valmistajien järjestelmistä, joilla saavutetaan SIEM:n kaltainen kokonaisuus. Hajautetuista järjestelmistä rakennetut SIEM-kokonaisuudet ovat tyypillisiä ratkaisuja yrityksillä, jotka hakevat kustannussäästöjä täydentämällä tietoturvaansa

päivittämällä sitä pienissä osissa. Yrityksellä voi olla olemassa tietoturvasta huolehtivia järjestelmiä, joissa on havaittu puutteita. Ne voivat olla esimerkiksi vanhentuneita tai jääneet jälkeen uusilla ominaisuuksilla varustettujen tuotteiden tultua markkinoille. Puutteita havaituissa tietoturvajärjestelmissä täydennetään tuotteilla, jotka täydentävät yrityksen tietoturvan kokonaisuutta, kuten keskitetty lokienhallinta.

3.8 Standardit ja lokienhallinta

ISO27001- ja PCI-standardit velvoittavat niitä organisaatiota lokienhallinnassa ja auditointikriteereissä, jotka ovat ottaneet ne käyttöön. Erityisesti tämä koskee rahoitussektoria, jossa toimivat luottokorttiyhtiöt ja muut toimijat, jotka käsittelevät järjestelmissään luottokorttitietoja. Näitä sitoo useissa maissa laki ja ohjaa PCI DSS:n kaltaiset standardit. Standardeilla pyritään siihen, että kaikki luottokorttitietoja käsittelevät tahot toimivat samalla turvalliseksi havaitulla tavalla tietojen käsittelyssä ja säilytyksessä. Tiedot, joiden varastamisesta voi potentiaalisesti aiheutua vahinkoa tai haittaa, on suojattava huomattavasti muita vastaavia tietoja paremmin. PCI DSS -standardin kuten muidenkaan vastaavien tietoturvaa ohjaavien standardien tarkoituksena ei ole syrjäyttää paikallisia tai alueellisia lakeja, viranomaismääräyksiä tai muita lakisääteisiä vaatimuksia. PCI DSS -standardia voi käyttää hyvänä ohjenuorana, jonka pohjalta voidaan luoda yrityksen tai organisaation tieturvaohjeistusta. Yrityksen suunnitellessa keskitetyn lokienhallintajärjestelmän hankkimista on järjestelmä hyvä suunnitella standardeja mukailevaksi. Näin meneteltynä järjestelmä on myöhemmin mahdollista päivittää ja auditoida PCI DSS -standardin vaatimuksia vastaavaksi. [8.],[11]

4 HP ARCSIGHT

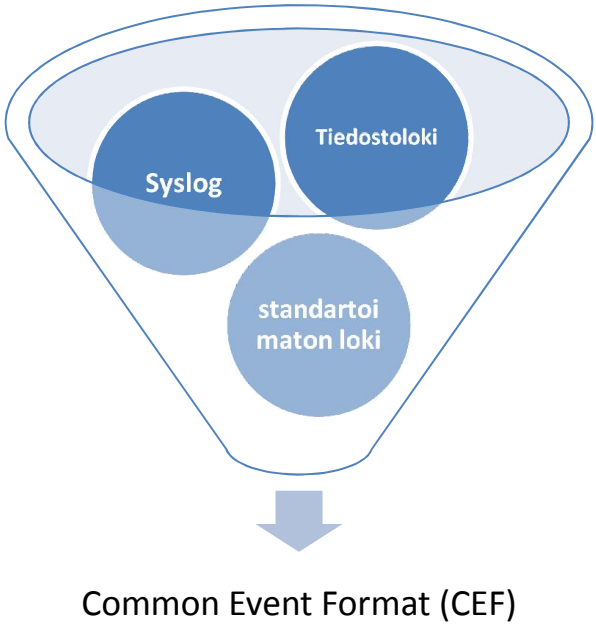
Tässä luvussa perehdytään HP Arcsightin tuotteisiin ja sen toiminnallisuuteen SIM-näkökulmasta eli jälkikäteen tehtävästä lokien tutkinnasta. Käsiteltävänä on myös muutamien esimerkkien avulla nähtävät havainnollistukset tuotteiden käyttämisestä, erityisesti CEF-formaatista, johon koko tuote pohjautuu.

4.1 Yleistä HP ArcSightista

Alun perin HP ArcSight on ollut itsenäinen yhtiö. Vasta yrityskauppojen kautta se siirtyi Hewlett Packardin omistukseen. HP ilmoitti syyskuussa 2010 ostavansa ArcSightin vajaalla 1,2 miljardilla eurolla [17]. Tästä seurasi ArcSightin sulauttaminen osaksi HP:n muita tuotteita ja nimeäminen HP Arcsightiksi. Vastaavalla tavalla ArcSightin kilpailija Q1Labs siirtyi lokakuussa 2011 IBM:n haltuun. [18.] Tuotteen laadukkuudesta kertoo arvostetun SC Magazinen antama palkinto toukokuussa 2014 markkinoiden parhaana SIEM ratkaisuna. Luotettavuudesta vastaavasti vakuuttaa se, että sitä käyttää muun muassa sotilasliitto NATO. Muita vastaavia isoja yhtiöitä, jotka käyttävät ArcSightin tuotteita, ovat BMW, Vodafone ja AirTran Airways. [19.]

4.2 Lokitiedon käsitteleminen

Riippumatta siitä, käsitelläänkö syslogia, tiedostolokia tai standardoimatonta lokia, käsitellään kaikki lokitiedot saman prosessin läpi. Kuvassa 6 havainnollistetaan suppilomallin avulla eri lokiformaattien saattamista CEF-formaatin mukaiseen lokiin, riippumatta siitä, ovatko ne standardoituja tai standardoimattomia.



Kuva 6. Eri lokien muuntaminen CEF-muotoiseksi lokiksi.

Lokitiedon kerääminen laitteesta voidaan tehdä joko vastaanottamalla lokitietoa tai hakemalla se tiedostosta, jos laite ei kykene sitä lähettämään. Kerätty tieto jäsennellään, joissa tapauksissa käytetään myös nimitystä parsiminen (Parsing), lokisovittimessa kuten SmartConnectorissa, FlexConnectorissa tai Connector Appliancessa. Lisäksi lokitietoa normalisoidaan ja kategorisoidaan. Jos kyseessä on lokienhallinnan edistyneempiä tuotteita, kuten HP ArcSight Express, sen sisältöä myös rikastetaan lokikorrelaatiolla. Lokitiedoista kerätään vain hyödylliset osat ja ne sijoitetaan CEF-formaatissa vastaaviin kenttiin. Jossain tapauksissa alkuperäisessä lokiformaatissa on tieto, jolle ei ole suoraa kenttää CEF-formaatissa. Näissä tapauksissa voidaan ottaa käyttöön oma kenttänsä, johon kyseinen tieto määritellään CEF-formaatissa. [20.]

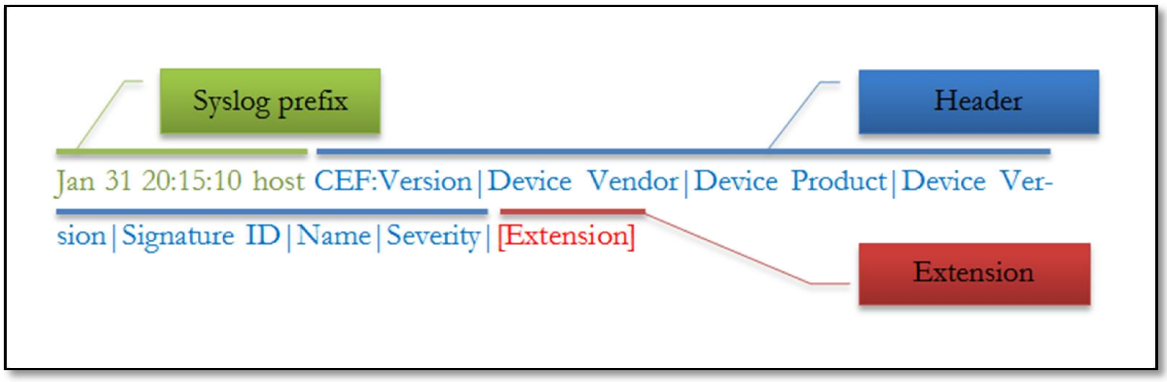
4.3 Common Event Format

Common Event Format (CEF) on Arcsightin luoma avoin lokistandardi, joka mahdollistaa useiden eri lokiformaattien kokoamisen yhteen muotoon. Avoin lokistandardi mahdollistaa, että muut yhtiöt voivat sertifioida tuotteitaan käyttämään CEF-formaattia. Tästä on etuna se, että niiden lähettämille CEF-formaatin lokitiedoille ei tarvitse tehdä enää lokimuunnosta. Tämä helpottaa järjestelmien välisten tietojen jakamista. Kaikki HP Arcsightin laitteet käyttävät CEF-formaattia lokitietojen tallennuksessa. [21.]

CEF-lokitietojen välityksessä HP Arcsightin laitteille käytetään syslog-formaattia. Jokainen syslog-viesti sisältää päivämäärän, lähdelaitteen nimen ja viestin: [21.]

Jan 31 20:15:10 host message

Tietoja välitetään syslogin avulla, mutta CEF-formaatissa viesti sisällytetään syslogiin, jolloin viesti rakentuu syslogin etuliitteestä (Syslog prefix), otsikosta (Header) ja laajennuksesta (Extension). CEF-formaatin kentät on eroteltu pystymerkillä, josta voidaan käyttää myös nimitystä putkimerkki (Pipe). Kuvassa 7 on havainnollistettu miten CEF-loki sisältyy syslogin sisään. [21.]



Kuva 7. CEF-loki sisältyy Message-kentän sisään, jolloin siihen kuuluvat kuvassa olevat Header- ja Extension kentät.

Version: CEF-versiotieto on pakollinen osuus viestissä. Tällä on tärkeä merkitys viestin loppuosan tulkitsemisessa. Väärä versionumero voi aiheuttaa viestin väärin tulkitsemisen. Kaikkien loppuosan kenttien tulisi olla määriteltyjä ja mukana viestissä. [21.]

Device Vendor, Device Product ja Device Version ovat tekstimuotoisia kenttiä, joiden perusteella pystytään yksilöimään laitteen valmistaja, laitteen malli ja versio. Signature ID on

yksilöllinen tunniste kullekin tapahtumalle. Tämä voi olla teksti tai numeerinen tieto. Signature ID kertoo, minkä tyyppinen tapahtuma on kyseessä. Name eli nimikenttä on tekstimuotoinen, käyttäjille helposti luettava tieto mistä tapahtumasta on kyse. Tähän kenttään ei pidä sisällyttää mitään sellaista tietoa, joka on kerrottu muissa kentissä. Severity-kenttä on numeerinen tieto ja kertoo tärkeysarvon. Tässä kentässä vain luvut nollasta kymmeneen ovat sallittuja, ja numero kymmenen edustaa kaikista tärkeintä tapahtumaa. Extension-osuus viestistä on varattu lisäinformaatiolle, mutta sitä ei ole pakollista käyttää, vaikka se on suositeltavaa. Kuvassa 8 tapahtuma on määritelty Common Event Formatin mukaisiin kohtiin. Extension-kentän sisältö vaihtelee suuresti. Siinä voidaan esittää olennaisia tietoja tapahtumaan liittyen. Tämän kentän sisällön esittämiseen on laaja määrä sääntöjä ja ohjeita, joihin joutuu perehtymään, jos lokimuotoa ei ole suoraan tuettu HP ArcSightin toimesta. [21.]

Kuvassa 8 on esimerkki lokista, jonka tiedot on sijoitettu kuvassa 7 nähtäviin kenttiin pystyviivoilla erotettuna. Kuvan 8 perusteella nähdään, että syslogin viestikenttä (Message) on varattu kokonaan CEF-viestille. [21.]

Kuva 8. Esimerkkinä CEF-muotoinen loki.

4.4 HP ArcSight-lokienhallintalaitteet ja komponentit

HP Arcsightin lokienhallintaan liittyviä tuotteita on useita eritasoisia. Tuotteiden käyttötarkoitus ja soveltuvuus tietylle kohderyhmälle riippuu pitkälti yritysten koosta, toimialasta ja tarpeesta.

4.4.1 SmartConnector

SmartConnectorista voidaan käyttää nimitystä lokisovitin. Lokisovitin on keskeisessä asemassa HP ArcSightin tuotteissa. Niiden tehtävänä on kerätä tai vastaanottaa valituilta laitteilta lokitietoa. Lokisovittimen käsittelemät lokitiedostot normalisoidaan. Normalisointi käsittää lokin tärkeyden, prioriteetin ja aikavyöhykkeen muuttamisen yhtenäiseen muotoon. Samalla lokista poistetaan tarpeettomat tiedot ja lokitieto välitetään eteenpäin. [22.]

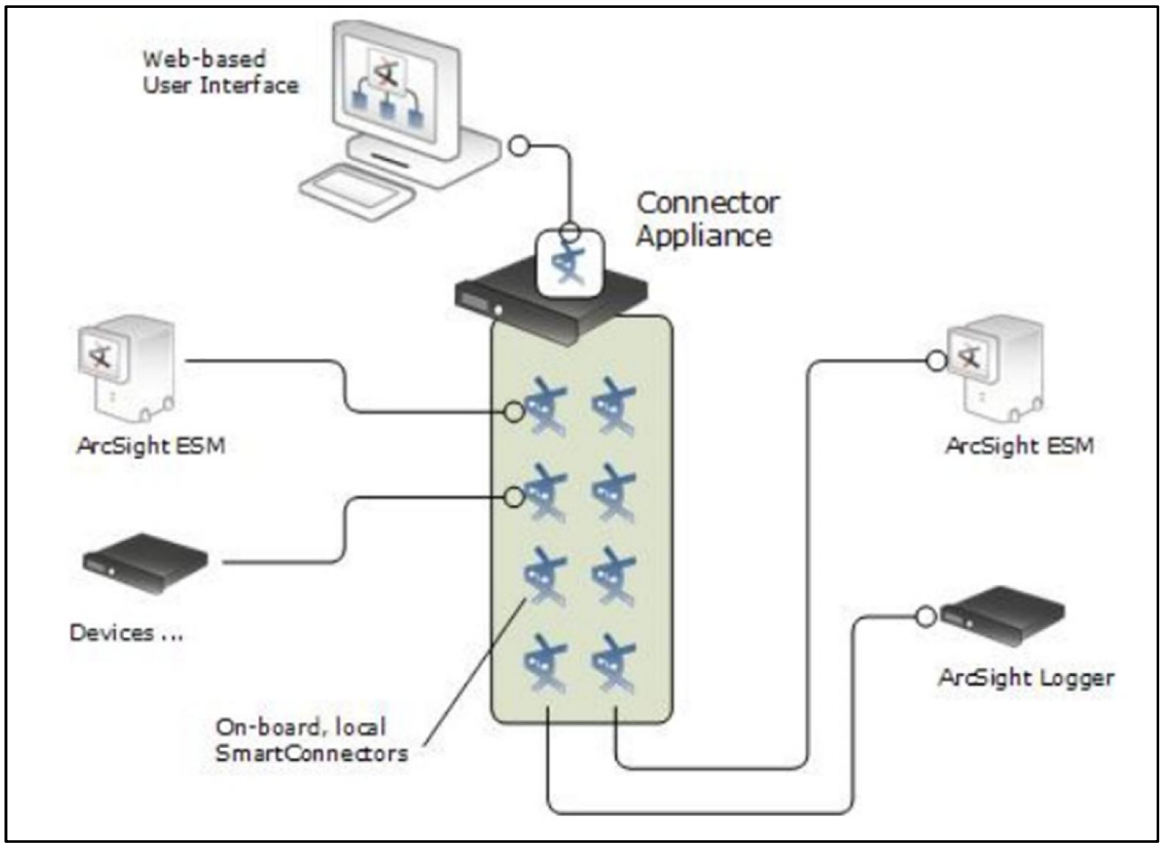
Lokisovittimen tärkein ominaisuus on sen joustavuus. Riippuen käsiteltävästä lokitiedosta, kyetään sitä keräämään monista eri lähteistä ja monessa eri muodossa. Näin voidaan kaikki lokitiedot normalisoida yhteen formaattiin. Tarvittaessa SmartConnector voidaan määrittää myös tekemään lokien tiivistämistä. Tämä voi olla tarpeen käsiteltäessä palomuurilta tulevaa lokitietoa. Tiivistämisessä määritellään loki, joka tulee tietystä lähteestä ja sisältää lähes samanmuotoista tietoa yhdistetään samaksi. Loki lähetetään vasta tämän jälkeen eteenpäin. Tarvittaessa voidaan myös tehdä suodatusta. Tämä voi olla tarpeen, jos tiettyjä lokitietoja ei haluta lähettää eteenpäin tai jos ne koetaan olevan tarpeettomia. [22.]

4.4.2 Connector Appliance

Connector Appliance/Conn App/Appliance on itsenäinen SmartConnector-alusta, jonka päällä SmartConnectorit toimivat. Appliancea on saatavilla sekä virtuaaliympäristöihin, kuten VMwaren virtuaalikoneiksi, että omalla palvelimella toimivana Appliancena. Toiminnoiltaan Appliance ja levykuvasta toimiva virtuaalikone ovat pääperiaatteiltaan samanlaisia. SmartConnectoreita on Conn App:lla C3500-mallissa 16 kpl ja C5500-mallissa 32 kpl. Oletuksena voidaan lisäksi hallita laitteille asennettuja SmartConnectoreita tai FlexConnectoreita pienemmässä mallissa 50 ja suuremmassa 150. Appliancen hallinta on keskitetty kokonaisuudessaan webkäyttöliittymän kautta. Appliancea ja sen asetuksia hallitaan webkäyttöliittymän kautta. Kirjautuminen tapahtuu webselaimella https-yhteyttä käyttäen. [23.],[24.]

Websivulta voidaan hallita keskitetysti kaikkia SmartConnectoreita ja niiden asetuksia, mukaan lukien palvelimilla sijaitsevat SmartConnectorit tai FlexConnectorit. Conn App:n mallista riippuen se kykenee vastaanottamaan lokitietoa tietyn määrän minuutissa. Tätä vastaanottokykyä kuvataan Event Per Second –arvolla (EPS). Kuvassa 9 on havainnollistettu

ConnApp:n ominaisuuksien kokonaisuus. SmartConnectorit voidaan konfiguroida lähettämään vastaanottamaansa lokitietoa eteenpäin. Kuvan esimerkissä lokitietoa lähetetään ArcSight Loggerille ja ArcSight Enterprise Security Managerille (ESM). Vaihtoehtoisesti sitä voidaan vastaanottaa samoilta laitteilta. ArcSight ESM:ltä. ESM toimii hyvänä esimerkkinä siitä, että lokitietoa voidaan vastaanottaa siltä ja lähettää sille, riippuen millaiseksi lokienhallintajärjestelmä on rakennettu. [23.]



Kuva 9. Connector Appliancen rakenne [20].

Connector Appliance on hyödyllinen alusta varsinkin silloin, jos yritys hankkii HP Arcsightin tuotteista esimerkiksi HP Arcsight Loggerin ja omaa useita toimipisteitä. Jokaiselle toimipisteelle voidaan sijoittaa Connector Appliance, joka kerää lokitiedot ja välittää ne Loggerille. Connector Appliancen palvelinalusta on optimoitu lokien käsittelyä varten. Täten Appliance on tehokkaampi kuin tavalliselle palvelimelle asennettavat SmartConnectorit lokien keräämisessä.

Connector Appliance kykenee vastaanottamaan pienimmillä malleilla (C3400) maksimissaan 2500 tapahtumaa sekunnissa (EPS). SmartConnectorin, joka on asennettu tavalliselle palvelimelle, lokien käsittelykyky riippuu palvelimen suorituskyvystä. [23.],[24.]

Connector Appliancen etuna on sen sijoittaminen esimerkiksi toiselle toimipisteelle, jos lokia tulee paljon. Logger voi samalla sijaita esimerkiksi yhtiön pääkonttorilla, jonne ConnApp lähettää prosessoidut lokit. Toimipisteen yhteyden katketessa pääkonttoriin tai Loggerille voidaan lokeja puskuroida muistiin. Puskurimuistin täyttymisnopeus riippuu siitä, kuinka paljon lokeja lähetetään Connector Appliancelle. Yhteyden palauduttua lähetetään varastoidut lokit Loggerille. Tämä varmistaa sen, ettei lokeja katoa eri toimipisteiden välillä olevien yhteysongelmien vuoksi. Pienemmällä ConnApp-mallilla lokia voidaan varastoida 500 GB:n edestä. Vertailun vuoksi erilliselle palvelimelle asennettava SmartConnector kykenee parhaimmillaan varastoimaan 50 GB:n edestä lokitietoa. Jos lokitietoa tulee Appliancen ja Loggerin välisen yhteyskatkoksen aikana enemmän kuin sitä pystytään puskuroimaan muistiin, ylikirjoitetaan vanhimpia lokitietoja uusilla lokitiedoilla. Lokien puskuroinnin etuna voi olla myös toimipisteen Internet-liittymän liikenteen priorisointi yrityksen tarvitsemalle tietoliikenteelle, jolloin lokiliikenteen määrää voidaan rajoittaa. Lokiliikenteelle voidaan antaa lupa käyttää Internet-liittymän kaistaa enemmän sellaisena aikana, jolloin toimipisteellä ei ole muuta sellaista tietoliikennettä, jonka prioriteetti on lokiliikennettä korkeampi. [23],[24]

4.4.3 Logger

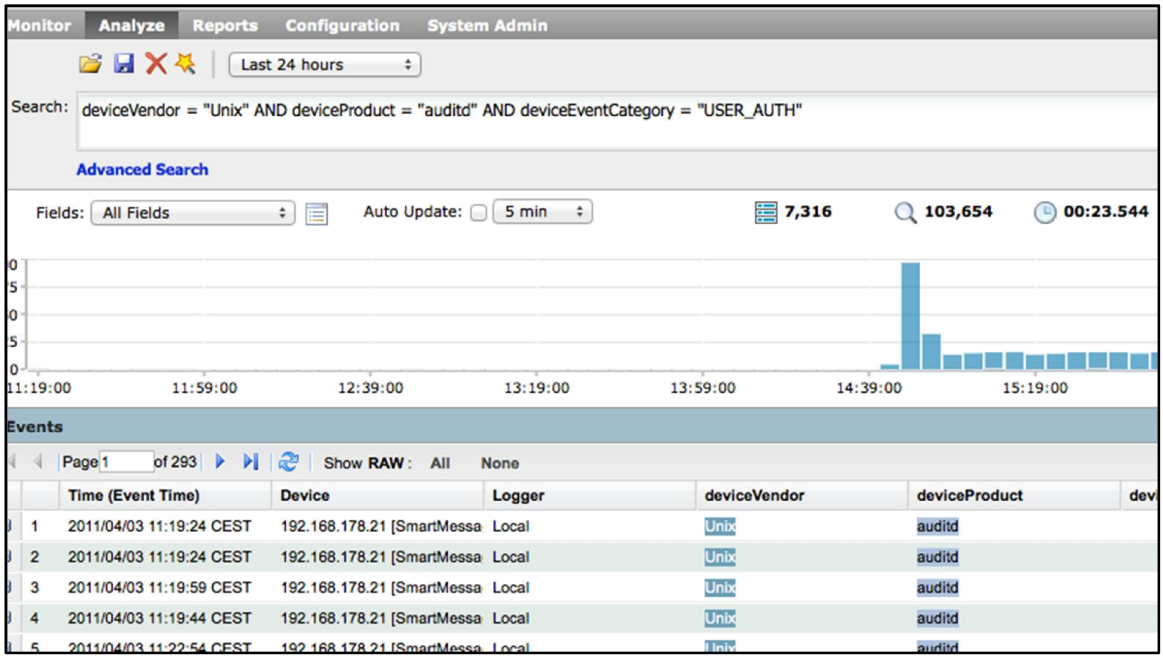
HP ArcSight Loggerin etuna muiden valmistajien lokilaitteisiin nähden on sen kyky analysoida lokidataa vaarantamatta Loggerin lokien keräysnopeutta ja tallennustehokkuutta. Logger on saatavilla omassa palvelimessa tai virtuaalisena levykuvatiedostona virtuaaliympäristöjä kuten VMwarea varten. Toiminnoiltaan virtuaalisena levykuvana ja omalla palvelimella toimiva Logger ovat samanlaiset. Appliance-alusta on kuitenkin optimoitu ottamaan suurempia lokimääriä kerralla oman palvelinlaitteiston takia. [25.]

Loggeria ja sen asetuksia hallitaan webkäyttöliittymän kautta. Kirjautuminen Loggerille tapahtuu webselaimella käyttäen suojattua https-yhteyttä. Kirjauduttaessa sisään avautuu ensimmäisenä Loggerin etusivu (Dashboard), johon voidaan liittää erilaisia lokienhallintaan liit-

tyviä näkymiä. Yläreunassa on nähtävissä kolme mittaria: EPS (Event Per Second) sisäänpäin, EPS ulospäin ja prosessorin kuormitus. [25.]

Lokitietojen tutkiminen Loggerilla

Lokien hakeminen Loggerilta tapahtuu hakukonemaiselta Analyze-välilehdeltä. Hakutulosten rajaaminen haluttuihin lokeihin tehdään käyttämällä Boolean-operaattoreita. Aikaväli, jolta lokeja haetaan, voidaan valita valmiina olevista vaihtoehdoista tai määritellä halutuksi. Kuvassa 10 lokeja on haettu viimeisen 24 tunnin ajalta. Haun tulokset ovat helposti ymmärrettäviä, ja ne voidaan esittää tarvittaessa erilaisina kaavioina ymmärtämisen helpottamiseksi. Tämä onnistuu lisäämällä hakulausekkeeseen määrittely, joka muuntaa hakutulokset esimerkiksi pylväsdiagrammiksi. Kuvan 10 Search-kohdassa näkyy käytetty hakulause. Hakukentän alapuolella oleva diagrammi näyttää lokien vastaanottamisen esiintymismäärät haetulla aikavälillä. Alimpana sijaitsevassa Events-kohdassa näkyvät haetut lokit. [25.], [26]



Kuva 10. Analyze välilehden hakukenttä ja esimerkki hausta [27].

Peer Logger

Loggereita voi olla HP ArcSight -tuotteisiin perustuvassa lokienhallintajärjestelmässä useita. Tiettyjen lokitietojen hakeminen Loggerilta voi olla työlästä ja hankalaa, jos käyttäjä ei tiedä tai muista, millä Loggerilla lokitiedot ovat nähtävillä. Tämän takia Loggereissa on Peer Logger -ominaisuus. Tämä tarkoittaa, että Loggereille on otettu käyttöön Peering-ominaisuus,

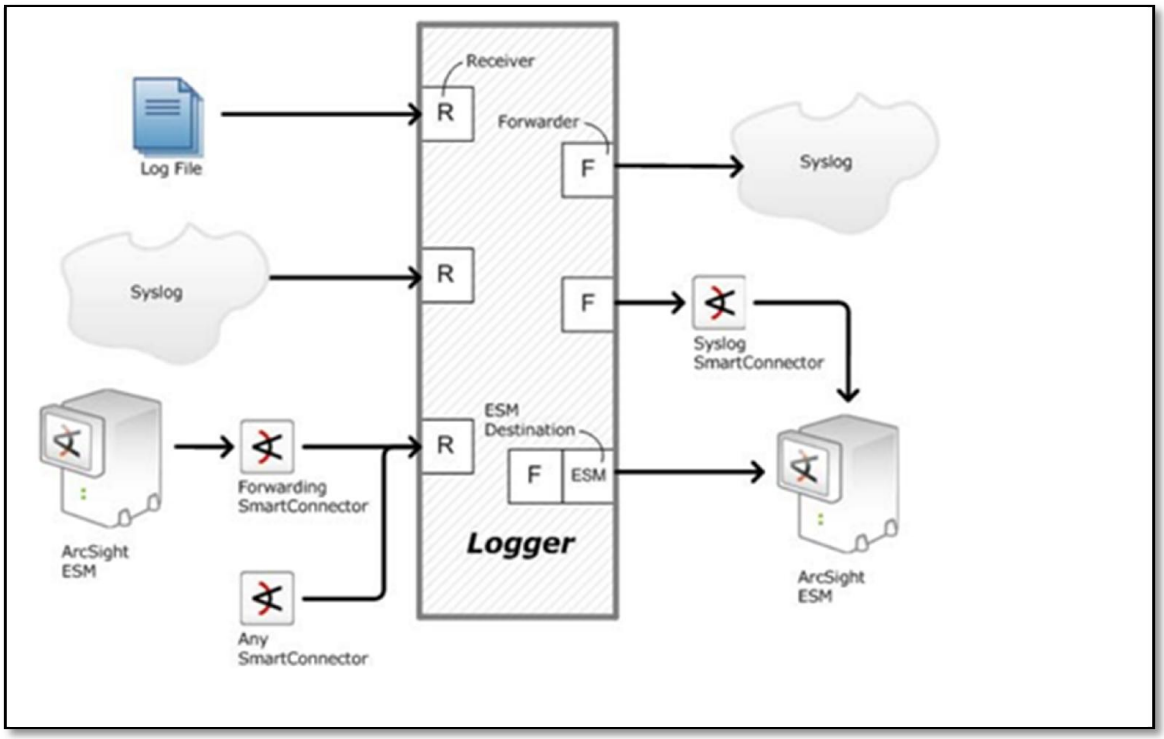
joka mahdollistaa hajautettujen hakujen tekemisen. Käyttäjä, joka tekee hakua yhdellä Loggerilla, voi määritellä haun tehtäväksi kaikista Loggereista. Haun tulokset esitellään vastaavalla tavalla kuin ne olisi haettu kyseiseltä Loggerilta. [25.],[26.]

Lokitietojen tallentaminen

Loggerilla lokitietojen tallentaminen tapahtuu tallennusryhmiin. Vastaanvanlaisia tallennusryhmiä on käytettävissä myös Connector Appliancelle. Näitä tallennusryhmiä Loggerilla voi olla maksimissaan kuusi. Kahdelle näistä on oletuksena määritelty sisäinen tallennusryhmä ja oletustallennusryhmä. Käyttäjä voi määritellä kokonaisuudessaan neljä tallennusryhmää. Kokonaisuudessaan viisi ryhmää voidaan määritellä tapahtumien eli lokientallentamiseen ja yksi Loggerin sisäisten tapahtumien tallentamiseen. Tallennusryhmillä voidaan asettaa lokien säilytysaika. Arkistoitavia lokeja voidaan tallentaa ryhmään, jossa niitä säilytetään pidempään. Loggerin keräämät lokit voidaan varastoida pakkaamalla ne parhaimmillaan suhteella 10:1. Vastaavasti lyhytaikaiseen säilytykseen tarkoitetut lokit voidaan sijoittaa toiseen ryhmään. Ulkoisten tallennusjärjestelmien, kuten Storage Area Network (SAN), liittämistä suositellaan heti alkuvaiheessa. Ulkoisista järjestelmistä on suositeltavaa allokoida tilaa lokien tallentamista varten, koska se vie aikaa. Myöhemmässä vaiheessa tehtävä allokointi syö Loggerin suorityskykyä varsinkin, kun Loggerille kerätään samanaikaisesti lokia. [25.],[26.]

Forwarder ja Receiver

Connector tai Connector Appliancet on tarkoitettu pääasiassa lokien vastaanottamiseen, voidaan lokeja vastaanottaa myös Loggerilla, kuten kuvassa 11 on esitetty. Lähetettäessä lokeja suoraan lähdelaitteilta Loggerille tulee huomioida, että Loggeri ei tee lokeille normalisointia, kuten Appliance tai SmartConnector. Jos Loggeri määritellään vastaanottamaan lokia, määritellään sille Receiver. Se sisältää tarkan määritelmän, millaista lokia halutaan vastaanottaa. Vastaavasti lokeja voidaan lähettää eteenpäin esimerkiksi yrityksen käyttämälle SIEM:lle, HP ArcSight ESM:lle tai muulle tuotteelle, joka voi hyödyntää lokitietoa. Lokien eteenpäin lähettäminen tehdään Forwarderin avulla. Forwarder on vastaavanlainen kuin Receiver, mutta lähettää lokia vastaanottamisen sijaan. [25.],[26.]



Kuva 11. Loggeri voi vastaanottaa ja lähettää lokia eteenpäin erimuodoissa. [25.]

Hälytykset

Loggerille voidaan määritellä hälytyksiä, jotka aktivoituvat, kun saapunut loki tai lokien määrä täyttää ennalta asetetun kyselyn (query) ehdot. Hälytykset voidaan määritellä lähetettäväksi sähköpostina, SNMP trap-muodossa tai syslogina. Kyselyitä voidaan hyödyntää esimerkiksi tilanteissa, joissa halutaan tietää, milloin tiettyä lokia tulee Loggerille. Tämä voi koskea laitteita, jotka lähettävät vain harvoin ja ainoastaan kriittistä lokitietoa Loggerille. [25.]

4.4.4 FlexConnector

HP Arcsightin vahvuutena kilpailijoihin nähden on sen laaja valmis pohja erilaisia Connectoreita. Connectoreiden avulla pystytään liittämään yli 100:lle tietylle laitetyypille/sovellukselle tehtyä Connectoria, joka muuntaa lokitiedon CEF-formaattiin ja välittää HP Arcsightin keskitettyyn lokienhallintaan. Nämä Connectorit tarvitsee vain asentaa ja määritellä asetukset asennusvaiheessa. Jos järjestelmää tai laitetta ei ole tuettu täytyy, sille tehdä FlexConnector.

FlexConnectorit on vapaasti muokattava SmartConnector, joka voidaan muokata keräämään laitteesta valittuja lokitietoja ja muuttaa ne CEF-formaattiin. FlexConnetorin määritykset tehdään tiedostoon, johon määritellään, mitä tietoja valituista lokeista muutetaan eli parsitaan CEF-formaattiin. Määrittely aloitetaan valitsemalla FlexConnector-tyyppi, jonka ominaisuudet soveltuvat halutun järjestelmän lokitiedon keräämiseen. Liitteenä 1 olevaan taulukkoon on listattu eri vaihtoehdot ja lyhyt selostus kunkin käyttötarkoituksesta. [28.]

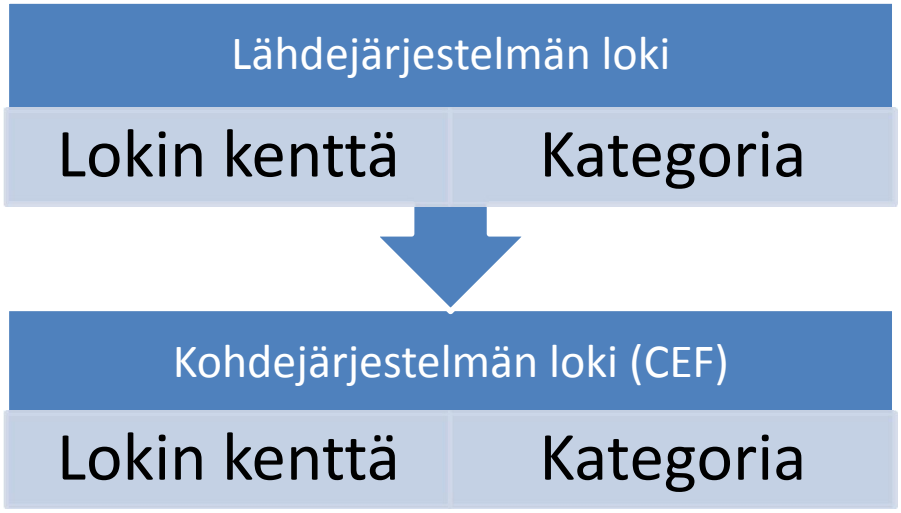
FlexConnectorin valinnan jälkeen aloitetaan lokisovittimen tekeminen. Sovitin on konfiguraatiotiedosto, joka kertoo FlexConnectorille, miten lähdejärjestelmän loki muunnetaan CEF-formaatin mukaiseksi lokitiedoksi. Sovitinta on suositeltavaa testata testiympäristössä ennen sen siirtämistä tuotantoympäristöön. Testiympäristön tulisi mallintaa tuotantoympäristöä mahdollisimman tarkasti siinä laajuudessa kuin se on tarpeellista. Usein tällaisessa testiympäristössä on lokienkeräyslaitteistona pelkästään Logger ja Connector Appliance. Nämä ovat riittäviä testaukseen, mutta laajamittaista testausta varten molempia on suositeltavaa olla kaksi kappaletta. Tällöin voidaan testata muun muassa erikoistilanteita, joissa lokia lähetetään lähdelokia keräävältä SmartConnectorilta kahdelle eri Loggerille, jotka eivät ole yhteydessä toisiinsa.

Lokien lähdejärjestelmän omistava yritys ei välttämättä tunne lokia tuottavia laitteita niin hyvin, että osaisi antaa lokista riittävän tarkan kuvauksen sovittimen tekemistä varten. Pelkästään tämän takia tarvitaan mallilokia lähdejärjestelmästä, jonka perusteella lokisovitin tehdään. Lähdelokista on kerrottava riittävällä tarkkuudella kaikki lokin osat. Joissakin tapauksissa näytelokista joudutaan poistamaan arkaluonteista tietoa, joka ei saa päätyä sovittimen tekijälle. Tämä tulee korvata vastaavankaltaisella tiedolla, kuitenkin siten, ettei lokin kentän merkitys muutu ratkaisevasti. Lähdelokista tarvitaan lisäksi selostus lokikentistä, jonka perusteella lähdelokin kentät ohjataan kohdelokin kenttiin, kuten kuvassa 12 on esitetty.

Selostuksessa voidaan jättää kertomatta lokin merkitys, jos sen katsotaan aiheuttavan tietoturvariskejä. Tärkeämpää on kertoa, millaista tietoa lokin kentissä esiintyy. Sovittimen suunnittelemiseksi on jokaisen lokinäytteessä esiintyvän merkin tai välilyönnin merkitys selostettava lähdelokin kuvauksessa. Näiden perusteella voidaan valita kohdelokista oikea kenttä. Lisäksi tämä mahdollistaa merkityksettömien tietojen poistamista CEF-formaattiin muunnettavasta lokista. Hyvällä lokikuvauksella voidaan välttää tilanteet, joissa lokisovitin toimii väärin. Nämä tilanteet ovat mahdollisia, jos lähdejärjestelmän lokinäytteestä puuttuu harvinainen lokitapahtuma, jonka toistuvuus on esimerkiksi kerran kuukaudessa.

Sovittimen tekeminen vaatii tarkan dokumentoinnin siitä, miten lähdejärjestelmän kentät on muutettu kohdejärjestelmän lokiksi. Dokumentista on käytävä ilmi, mitä tarkoittaa uudessa CEF-muotoisessa lokissa oleva kenttä ja mikä on alkuperäinen kenttä lähdejärjestelmän lokissa.

Tehdyn sovittimen testaamista voidaan suorittaa kahdessa osassa. Ensimmäisenä testataan lähdejärjestelmästä saadun näytelokin avulla sovittimen toimintaa. Kohdeloki ohjataan kansioon ja tarkastellaan, onnistuuko muunnos CEF-formaattiin haetulla tavalla. Testaus voidaan tehdä suoraan sovittimen kehitysalustalla. Tämä vaatii sen, että alustalle on mahdollista asentaa kyseinen FlexConnector, koska muussa tapauksessa testaus täytyy tehdä eri ympäristössä. Tämä testauksen tavoitteena on ainoastaan selvittää, tapahtuuko lokimuunnos oikein. Toisessa vaiheessa testataan lokisovitinta tuotantoympäristöä mallintavassa testiympäristössä. Tässä testissä lähdejärjestelmästä ohjataan reaaliaikaista lokia testijärjestelmään. Sovittimen testauksella varmistetaan sovittimen toiminta. Lisäksi saadaan selville, jos sovittimen tavassa käsitellä lokia on virheitä. Virheet vaativat testausprosessin uudelleen läpikäynnin, kunnes sovitin toimii oikein.



Kuva 12. Lähdelokissa kukin lokissa olevan kohta ja kategoria tulee määritellä kohdejärjestelmän lokiin eli CEF-lokiin.

Sovittimen tekeminen ei pääty sovittimen dokumentaation tekemiseen. Sovitin on asennettava lokia tuottavaan lähdejärjestelmään tai konfiguroitava uudelleen lähettämään lokin tuotantojärjestelmään testijärjestelmän sijaan. Sovittimen tehnyt henkilö ei tee välttämättä asennusta lähdejärjestelmään. Tämä tarkoittaa, että kohdejärjestelmään tehtävää asennusta varten

voidaan joutua tekemään ohjeet henkilölle, joka tekee FlexConnectorin asentamisen. Sen voi tehdä henkilö, joka tuntee järjestelmän ja hänellä on riittävät oikeudet siihen.

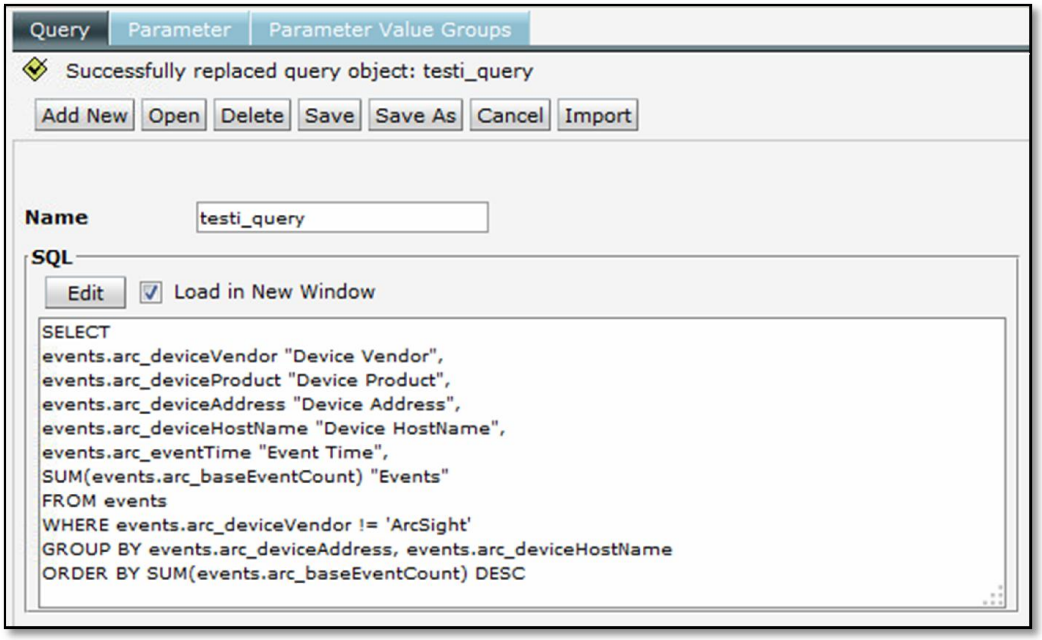
4.5 FlexConnectorin tekeminen

FlexConnectoreita ohjaava konfiguraatio tehdään lähdelokin perusteella. Lokit, joita muunnetaan CEF-formaattiin voivat olla vaihtelevissa muodoissa. Monessa tapauksessa sovitin tehdään käyttäen säännöllisiä lausekkeita Regular Expression (RegEx). Näiden lausekkeiden avulla haetaan lähdelokista halutut kohdat ja jäsentelyä varten.

4.6 Raporttien suunnittelu

Lokien keräämisestä ja kerätystä lokitiedoista on usein välttämätöntä tuottaa raportteja, joista voidaan nähdä kerättyihin lokeihin liittyvää tietoa. Raportit luodaan Loggerissa, ja ne rakentuvat kahdesta keskeisestä osasta: SQL-kyselyistä ja raportin ulkoasusta. SQL-kyselyiden avulla määritellään, millaisia tietoja lokeista halutaan kerätä ja esittää. Useimmissa tapauksissa vähimmäisvaatimuksena raportoinnin määrittelyssä on rajata raporttiin analysoitavien lokien laajuus esimerkiksi lokia tuottavien lähdelaitteiden perusteella. Tarvittaessa voidaan määritellä tarkasti ne kentät, joiden perusteella raportti luodaan ja joista raportin tilaaja on kiinnostunut. Raportti voidaan tuottaa eri muodoissa. Tyypillisiä vaihtoehtoja ovat Microsoft Excel ja Portable Document Format (PDF). Raporttiin voidaan luoda kuvaajia kuten pylväs- tai sektoridiagrammeja hahmottamaan raportin tuloksia. [25.]

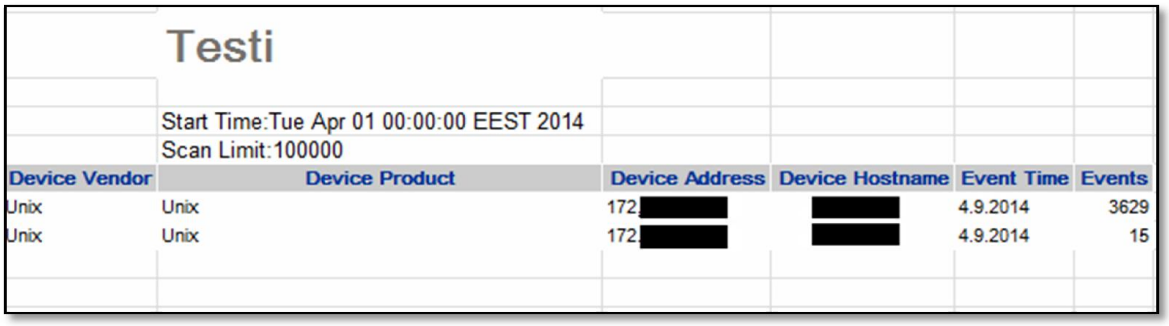
Kuvassa 13 on näkyvillä SQL-kyselyn ikkuna, jossa kysely laaditaan. Samassa ikkunassa on myös nähtävillä yksinkertainen kysely, jossa valitaan SELECT-komennolla raporttiin tulevat kentät lokitiedoista, sekä millä nimellä ne esiintyvät raportissa. SUM-komennolla lasketaan yhteen tapahtumat. FROM-komennolla tiedot haetaan tapahtumista. WHERE-komento valitsee lokit, joissa laitteen toimittaja on ”Arcsight”. GROUP BY ja ORDER BY komentojen avulla tiedot ryhmitellään ja järjestellään raportille valittuun muotoon.



Kuva 13. SQL-kyselyn suunnitteluikkuna.

Raportin suunnittelu tehdään Report Designer -työkalulla. Raporttiin valitaan SQL-kysely, jota käytetään haluttujen tietojen hakemiseen. Raporttiin valitaan vielä kyselystä halutut kentät, jotka raportissa esitetään. Suodatusta ja ryhmittelyä voidaan tehdä myös suunnitteluvaiheessa, jos sitä ei tehdä SQL-kyselyssä.

Raporttien ajamisvaiheessa valitaan erilaisia ehtoja, joista olennaisin on haluttu aikaväli, jolta tietoa haetaan. Aikaväli voidaan asettaa kiinteäksi tai dynaamiseksi, kuten viimeiset kaksi tuntia. Tällöin aikaväli muuttuu automaattisesti riippuen raportin ajamiskohdasta. Raportteja voidaan suorittaa myös tietyin väliajoin, tai ne voidaan määritellä toimitettavaksi sähköpostitse. Tämä vaatii, että kyseinen ominaisuus on määritelty ja otettu käyttöön Loggerilla. Kuvassa 14 nähdään kuvan 13 SQL-kyselyn perusteella luotu Microsoft Excel -muodossa oleva raportti. Raporttiin on rajattu nähtäville keskeisimmät tiedot.



Testi

Start Time:Tue Apr 01 00:00:00 EEST 2014
Scan Limit:100000

Device Vendor	Device Product	Device Address	Device Hostname	Event Time	Events
Unix	Unix	172.[redacted]	[redacted]	4.9.2014	3629
Unix	Unix	172.[redacted]	[redacted]	4.9.2014	15

Kuva 14. SQL-kyselyn perusteella luotu raportti.

4.7 HP ArcSight -lokienhallintajärjestelmä

Työssä on aiemmin esitelty lokienhallinnan teoreettiset perusteet sekä HP ArcSightin tuotteet ja niiden omaisuudet. Tässä luvussa esitellään esimerkki siitä miten toimiva järjestelmäkokonaisuus muodostuu. Tässä työssä kuvattu esimerkki on yksi tapa toteuttaa perusmuotoinen lokienhallintajärjestelmä. Toteutusmallissa ei kerrota kaikkia teknisiä yksityiskohtia, vain periaatteellinen malli. Tarkoituksena on tarjota yleiskuva laitteiden toimimisesta kokonaisuutena. Järjestelmä voidaan jakaa kerroksiin, joissa kullakin kerrokselle on oma tehtävänsä. Kerrokset jakavat lokienhallintajärjestelmän helposti ymmärrettäviin kokonaisuuksiin. Tämä helpottaa ymmärtämään laitteiden merkityksen lokienhallintajärjestelmän toiminnassa. Seuraavissa kappaleissa on selostettu liitteessä 2 olevan kuvan segmentit.

4.7.1 Lähteet-segmentti

Mallissa ylimmäisenä lähtötasona ovat lokilähteet. Suurin osa lähteistä tuottaa lokinsa suoraan Syslog-formaatissa. Vaihtoehtoisesti lähdelaitteeseen asennetaan SmartConnector, joka suorittaa lokienkeräyksen ja välittää ne suoraan salatussa muodossa Connector Appliancelle jatkokäsiteltäväksi. Lähes kaikissa lokienhallintajärjestelmissä osaan lokia tuottavista järjestelmistä joudutaan tekemään FlexConnector.

4.7.2 Keräys-segmentti

Seuraavalla lokikeräimet-kerroksella ovat Connector Appliancet, jotka on nimetty seuraavasti: Aarne, Bertta, Celsius ja Daavid. Näitä on sijoitettu kerrokselle neljä kappaletta. Connector Appliancet toimivat pareittain, Aarne ja Bertta, jotka muodostavat Tuotantokeräin-ryhmän. Vastaavasti Celsius ja Daavid muodostavat Auditointikeräin-ryhmän. Molemmat Connector Appliancet on konfiguroitu identtisiksi, mutta vain toinen näistä keräimistä on aktiivinen ja ottaa vastaan kuormanjakajalta tulevaa lokitietoa. Kuormanjakaja on tässä oleellisessa osassa, koska Connector Appliancessa itsessään ei ole suoraan tukea High Availability (HA) tyyppiselle ratkaisulle. HA-ratkaisuissa, laitteet toimivat pareittain, toisen laitteen vikaantuminen aiheuttaa varalaitteen välittömän vaihtumisen tilalle. Tässä tapauksessa kuormanjakajat ohjaavat lähdejärjestelmien lokit tilanteen mukaan käytettävissä olevalle keräimelle. Lokitietoja ei tällöin katoa järjestelmästä missään vaiheessa. Tällä saavutetaan vikasietoisuus keräyskerrokselle ja voidaan tehdä tarvittavia huoltotoimia ilman, että lokien kerääminen vaarantuu. Ulkoisten uhkien takia keräimet on suositeltava sijoittaa asianmukaiseen konesaliin, jossa muun muassa sähkösyöttö on varmennettu. Mahdollisuuksien mukaan laitteet on suositeltavaa sijoittaa konesalissa eri telineisiin eli ”räkkeihin”.

4.7.3 Tallennus & Arkistointi -segmentti

Tässä kerroksessa lokit tulevat tallennettavaksi ja tarkasteltavaksi lokijärjestelmän käyttäjille. Tässä kerroksessa Loggereita on vastaavat neljä kappaletta ja ne toimivat pareissa. Tuotantolokiparin muodostaa Loggerit Eemeli ja Faarao. Auditointilokiparin vastaavasti Loggerit Gideon ja Heikki. Loggereita on kaksi kappaletta vikasietoisuuden saavuttamiseksi ja huoltotoimenpiteiden mahdollistamiseksi. Molemmista pareista vain toinen Loggeri käsittelee tietoa. Loggerit on lisäksi virtualisoitu VMwaren alustalle, joka on klusteroitu kahdelle palvelimelle. Tämä varmistaa virtualisointialustan vikasietoisuuden tilanteessa, jossa toinen klusteripalvelimista vikaantuu.

Lokijärjestelmän suunnittelussa on otettu huomioon lokienhallintajärjestelmän tapahtumien auditointi. Kaikista lokien tarkasteluista, kirjautumisista ja lokien hauista jää jälki, joka tallentuu Auditointi-ryhmän Loggerille. Tällä varmistetaan, ettei lokienhallintajärjestelmän tapahtumia päästä muuttamaan ja kaikki tapahtumat järjestelmässä saadaan talteen. Lokitieto tal-

lennetaan erilliseen levyjärjestelmään. SAS-levyt on tarkoitettu alle 30 päivää vanhojen lokitietojen tallentamiseen. SATA-levyt toimivat arkistona pitkään säilytettäville lokitiedoille.

4.7.4 Analyysi & Raportointi -segmentti

Viimeinen kerros on Analyysi & Raportointi -segmentti, jossa Loggerin lokitiedoista voidaan tuottaa raportteja ja hälytyksiä. Auditointikerroksen Loggerilla pystytään tarkkailemaan lokien tarkastelua. Auditointi-Loggeri on erillinen Loggeri, joka kerää lokitiedot ainoastaan Loggereihin liittyvistä lokitapahtumista. Tämän avulla Loggerille tallentuu kaikki lokien tarkastelut sekä niiden yritykset muuttaa lokitietoja. Lisäksi lokienhallintajärjestelmän Loggerille tehdyistä asetusten muutoksista tallentuu lokitieto Auditointi-Loggerille.

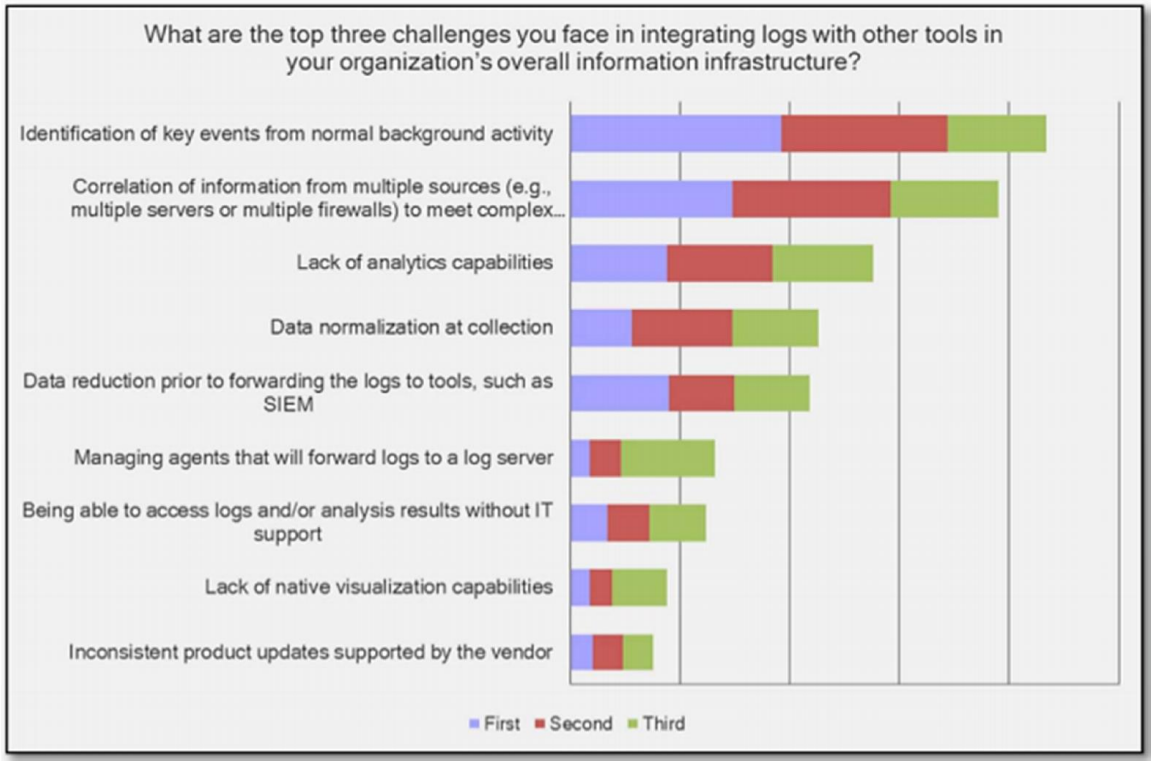
4.7.5 Järjestelmän looginen kuvaus

PCI DSS -standardi määrittelee tiukan ohjeistuksen ketkä saavat tarkastella lokeja ja miten lokienhallintajärjestelmään pääsee kirjautumaan. Lokienkeräyslaitteet kuten Appliance ja Logger voidaan eristää muusta verkosta palomuurilla, jota vasten suoritetaan vahva autentikointi, ennen kuin käyttäjät pääsevät kirjautumaan Loggerille tai Appliancelle ja tarkastelemaan lokitietoja. Laitteiden toimintaa ja kuntoa on hyvä valvoa erillisellä verkon ja laitteiden valvontaohjelmistolla. Näin havaitaan mahdolliset ongelmat lokienhallintalaitteistoissa tai laitteiden toiminnassa.

Lokien keräyslaitteiden ollessa eristetyssä verkkosegmentissä, lokienhallinnan laitteille voidaan joutua siirtämään esimerkiksi tiedostoja tai ohjelmistopäivityksiä. Tätä varten eristetyn verkkosegmentin sisällä on hyvä olla niin sanottu hyppykone, jolle päivitykset voidaan siirtää eristetyn verkkosegmentin ulkopuolelta ennen kuin ne siirretään niitä tarvitsevalle laitteelle.

5 LOKIENHALLINNAN KEHITYSSUUNNAT

Yhtenä haasteena lokienhallinnassa on noussut niin sanotun Big Datan määrä. Googlen toimitusjohtajan Eric Schmidt mukaan tuotamme tällä hetkellä enemmän tietoa kahdessa päivässä, kuin olemme tuottaneet sivilisaation alusta vuoteen 2003 asti [29]. Tiedon määrän kasvu tarkoittaa samalla lokien määrän kasvua ja haasteita lokienhallinnalle. Kuvassa 15 on pylväsdiagrammi, jossa on käyttäjät ovat pisteyttäneet haastavimmat osa-alueet lokienhallinnassa. Tietomäärän kasvu aiheuttaa haasteita erottaa keskeiset ja tärkeät lokit normaaleista lokeista, jotka eivät vaadi toimenpiteitä. Toiseksi haasteeksi on noussut lokien tapahtumien korreloiminen, kun niitä tulee useasta eri lähteestä. Kolmas pylväs osoittaa, että tietomäärän kasvu aiheuttaa haasteita myös lokienhallintalaitteiden kykyyn käsitellä lokitietoa.



Kuva 15. Lokienhallinnan haasteet. [10.]

Lokienhallinta kehittyy, automatisoituu ja paranee entisestään samalla kun käsin tehtävän työn määrä vähenee. Useissa terveydenhuollonjärjestelmissä lokiraporttien tulkitsemiseksi tarvitaan henkilökuntaa, joka osaa selostaa asiakkaalle lokiraportin sisällön. Lokienhallintajärjestelmien kehittyessä voi tulevaisuudessa olla mahdollisuus tarkastella itseään koskevia lokitietoja esimerkiksi verkkosivun kautta. Tulevaisuuden näkymissä on myös pilvipohjaisen lokienhallinnan yleistyminen. Tämä kuitenkin vaatii normaalia lokienhallintaan enemmän tieto-

turvasta huolehtimista ja se voi olla riskialttiimpi ratkaisu, varsinkin jos pilvipohjaista lokienhallintaa tarjoava yritys on ulkomainen.

6 YHTEENVETO

Tämän työn tavoitteena oli tutkia työn tilaajalle Ymon Oy:lle, kuinka Hewlett-Packardin ArcSight-tuoteperheen avulla rakennetaan keskitetty lokienhallintajärjestelmä ja miten hyvän lokienhallinnan tavoitteet toteutuvat. Työhön kuului myös perustasoisen lokienhallintakokonaisuuden suunnittelu, joka vaaditaan lokienhallinnan toteutukseen.

Työssä käsiteltiin aluksi projektina toteutettavan lokienhallintajärjestelmän kehitysvaiheet, aloittaen lokienhallintajärjestelmän tarpeesta ja syistä. Lisäksi kehitysvaiheista käytiin esiselvityksen keskeisimmät asiat, tavoitteet, osapuolet ja etenemismalli. Toteutuksen osuudesta käsiteltiin tarkasti läpi aikapalvelimet ja niiden merkitys. Lisäksi käsiteltiin järjestelmän ylläpitämiseen liittyviä asioita, jotka on hyvä huomioida. Lokitiedoista selostettiin lokien käsittelyyn liittyvät vaiheet ja niiden merkitys, sekä HP Arcsightin tuotteet ja niiden tapa käsitellä lokitietoa. Common Event Format (CEF) -lokiformaatin keskeinen merkitys ArcSightin tuotteilla toteutetussa lokienhallinnassa selostettiin. Lopputuloksena oli lokienhallinnan yksinkertaistettu toteutusjärjestelmäpohja ja perusteet sille. Työtä on mahdollista jatkaa tutkimalla HP ArcSightin tuotteita, kuten HP ArcSight Express ja Enterprise Security Management (ESM). Lisäksi lokienhallinnan vaativiin osuuksiin ja erikoistilanteisiin voisi perehtyä syvällisemmin.

Työn tekeminen oli pitkä ja haastava prosessin, jonka aika selvisi, että lokienhallintajärjestelmän käyttöönottaminen on haastava ja monivaiheinen projekti. Samalla ymmärrettiin mistä syystä on suositeltavaa toteuttaa lokienhallinta siihen erikoistuneen yrityksen avulla. Tässä työssä käsitellyistä HP ArcSight -tuotteista selvisi, että ne ovat perustoiminnoiltaan yksinkertaisia, mutta vaativat asiantuntemusta erikoistilanteissa. Työssä selvisi myös, että varsinkin VAHTI-dokumentissa esitettyihin asioihin verrattuna lokienhallinnan periaatteet toteutuvat hyvin HP ArcSightilla. Työn aikatauluttaminen ei onnistunut täydellisesti muun muassa työn haastavuuden takia. Toisaalta se mahdollisti aineiston kokoamisen ja perehtymisen työhön pitkällä aikavälillä.

LÄHTEET

1 Elinkeinoelämän keskusliitto. Yritysturvallisuus. Luettu 18.4.2014. [WWW-sivusto]. <http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/>

2 Valtionvarainministeriö. Vahti ohjeiden ryhmittely. Luettu 19.4.2014. [WWW-sivusto]. <https://www.vahtiohje.fi/web/guest/vahti-ohjeet-by-caterogy>

3 Valtionvarainministeriö. Vahti teknisen ICT-ympäristön tietoturvataso-ohje 3/2012. Luettu 18.4.2014. [PDF-dokumentti]. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/ICT_taitto.pdf>

4 Tietokone.fi. Auditointi tarkastaa tietoturvan tason. viimeksi muutettu 30.11.2004. [WWW-sivusto]. <http://www.tietokone.fi/artikkelit/auditointi_tarkastaa_tietoturvan_tason>

5 Järvinen, P. Tietoturva ja yksityisyys, 1. painos. Porvoo: Docendo Finland Oy, 2002. 22-28, 44, 79-80 s. ISBN 951-846-152-X

6 Poliisi.fi. Suojelupoliisi Vuosikertomus 2012. Luettu 23.1.2014. [PDF-dokumentti]. <http://www.poliisi.fi/poliisi/supo60/home.nsf/files/CBC606E685686634C2257B1D0047E7CD/$file/2012_Supo-FIN_web.pdf >

7 Valtionvarainministeriö. Käyttäjän tietoturvaohje 5/2003. Luettu 23.1.2014. [PDF-dokumentti]. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf>

8 Valtiovarainministeriö. Vahti lokiohje 3/2009. Luettu 5.1.2014. [PDF-dokumentti]. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf>

9 SearchSecurity. Log management best practices: Five tips for success. Luettu 2.2.2014. [WWW-sivusto]. <http://searchsecurity.techtarget.com/tip/Log-management-best-practices-Five-tips-for-success>

10 SANS.org. Analyst Program, Sorting Through the Noise. Luettu 22.2.2014. [PDF-dokumentti]. <https://www.sans.org/reading-room/analysts-program/SortingThruNoise>

11 Pcisecuritystandards.org. Payment Card Industry (PCI). Data Security Standard, Requirements and Security Assessment Procedures, Version 3.0 November 2013. Luettu 1.2.2014. [PDF-dokumentti]. <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf>

12 Support.ntp.org. The NTP Public Services Project. Selecting Offsite NTP Servers. Luettu 17.1.2014. [WWW-sivusto]. <http://support.ntp.org/bin/view/Support/SelectingOffsiteNTPServers>

13 Stanislav Shalunov. Network Time Protocol (NTP): Overview and Configuration. Luettu 17.1.2014. [PDF-dokumentti]. <http://e2epi.internet2.edu/npw/a2/ntp.pdf>

14 Owasp.org. Logging Cheat Sheet The Open Web Application Security Project (OWASP). Luettu 28.12.2013. [WWW-sivusto]. <https://www.owasp.org/index.php/Logging_Cheat_Sheet >

15 CastleForce IT Security. What is Log management. Luettu 3.5.2014. [WWW-sivusto]. <http://www.castleforce.co.uk/Solutions/LogManagement.aspx>

16 Alien Vault. What Is Log Correlation? Luettu 4.5.2014. [PDF-dokumentti]. <https://alienvault.bloomfire.com/posts/531844-what-is-log-correlation/public>

17 Helsingin Sanomat.fi. Hewlett-Packard ilmoitti uudesta jättikaupasta. Viimeksi muutettu 14.9.2010. [WWW-sivusto]. <http://www.hs.fi/talous/artikkeli/HewlettPackard+ilmoitti+uudesta+j%C3%A4ttikaupasta/1135260124748>

18 Techcrunch. IBM Buys Network Security Intelligence Company Q1 Labs. Luettu 6.5.2014. [WWW-sivusto]. <http://techcrunch.com/2011/10/04/ibm-buys-network-security-intelligence-company-q1-labs/ >

19 HP.com. SC Magazine Europe awards HP ArcSight as the best SIEM Solution. Luettu 15.5.2014. [WWW-sivusto]. <http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/SC-Magazine-Europe-awards-HP-ArcSight-as-the-best-SIEM-Solution/ba-p/6469816#.U4OnaChZizN>

20 User's Guide ArcSight SmartConnectors, September 30 2013. Luettu 5.2.2014. [Sisäinen PDF-dokumentti]

21 ArcSight Common Event Format CEF Guide V18, January 2012 Revision 18. Luettu 3.2.2014. [Sisäinen PDF-dokumentti]

22 User's Guide, ArcSight SmartConnectors, September 30, 2013. Luettu 15.2.2014. [Sisäinen PDF-dokumentti]

23 Administrator's Guide , ArcSight™ Connector Appliance v6.4, November 9, 2012. Luettu 28.4.2014. [Sisäinen PDF-dokumentti]

24 HP.com. HP ArcSight Connectors Datasheet Get scalable log collection today. Luettu 5.2.2014. [PDF-dokumentti]. <http://www.hp.com/hpinfo/newsroom/press_kits/2013/HPDiscover2013/Datasheet_ArcSight_Connectors.pdf>

25 Administrator's Guide ArcSight Logger™ v5.1, May 14, 2011. Luettu 28.4.2014. [Sisäinen PDF-dokumentti]

26 ArcSight Logger 5.1 Administration and Operations Book 1 – Course Presentations LOGR510i, 2011. Luettu 17.5.2014. [Kurssimateriaali]

27 Eromangzataz.com. Eric Romang Blog Unix Auditd Authentication Events Analysis and Visualisations with ArcSight Logger. Luettu 24.5.2014. [WWW-sivusto]. <http://eromang.zataz.com/2011/09/18/unix-auditd-authentication-events-analysis-and-visualisations-with-arcsight-logger/>

28 FlexConnector Developer's Guide, November 15 2010. Luettu 6.2.2014. [Sisäinen PDF-dokumentti]

29 TechCruch. Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003. Luettu 22.2.2014. [WWW-sivusto]. <http://techcrunch.com/2010/08/04/schmidt-data/>

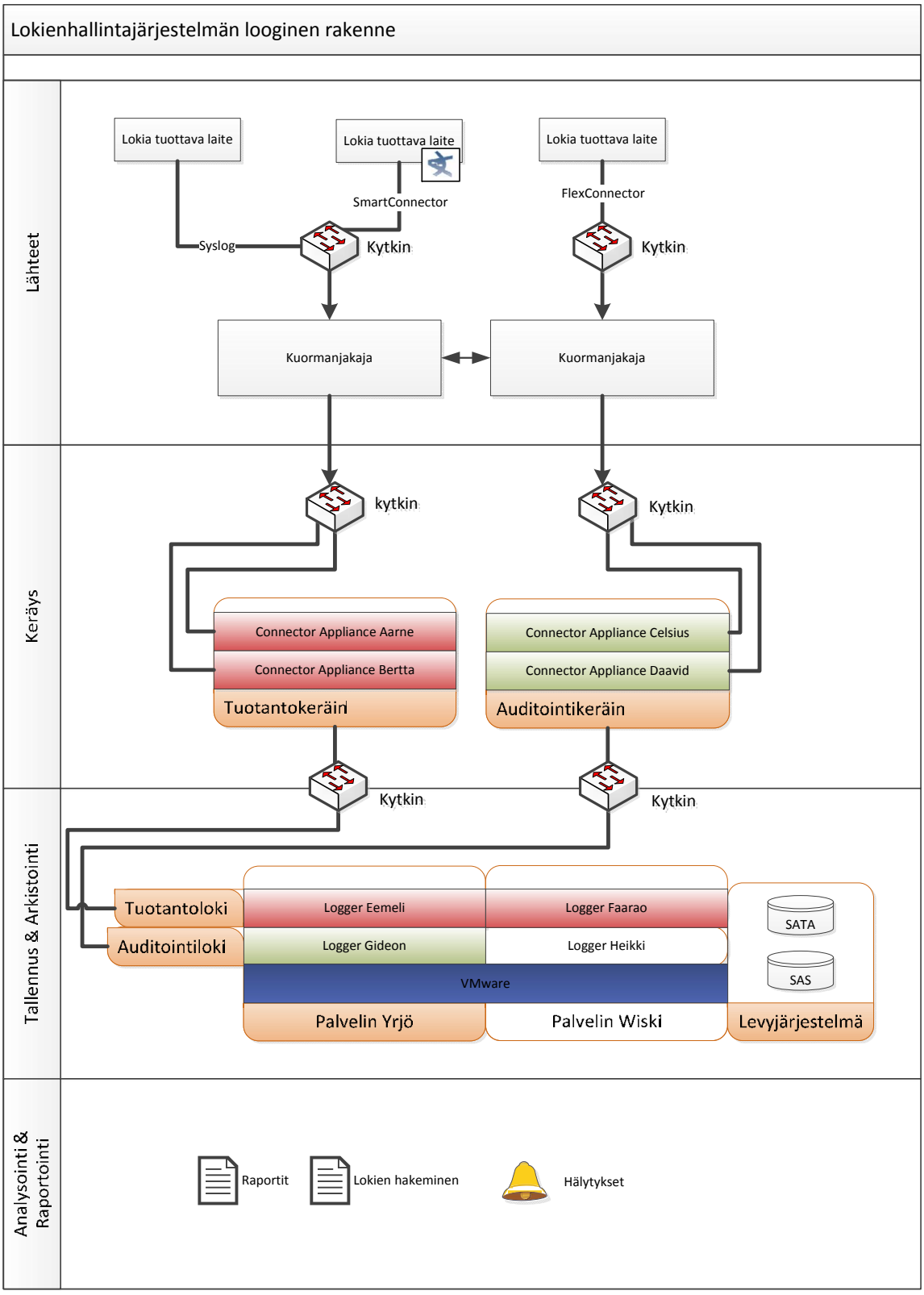
LIITTEET

LIITE 1: Listattu FlexConnector tyypit ja mihin tarkoitukseen kukin Connector on tarkoitettu.

LIITE 2: Kuva lokienhallintajärjestelmän loogisesta rakenteesta.

Log File FlexConnector	Sopii käytettäväksi silloin, kun jokaisella rivillä on sama vakiomäärä kenttiä samassa järjestyksessä. Lokitiedot tiedot voidaan erotella pilkuilla tai muilla erottimilla. [19.]
Regex Log File FlexConnector	Jokaisessa lokitiedostossa on yksitapahtuma rivillään, mutta muoto saattaa vaihdella kullakin rivillä riippuen tapahtumasta. Jokaisella rivillä on yhtenäisenä tekijänä esimerkiksi päivämäärä tai lähdelaitteen nimi. [19.]
Regex Folder Follower FlexConnector	Kaksi aiempaa FlexConnectoria lukee tapahtumia reaaliajassa. Tämä soveltuu niille laitteille, jotka eivät tee näin. Tällä saadaan luettua kaikki lokit lokilähdekansiosta. [19.]
Multiple Folder Follower FlexConnectors	Soveltuu tilanteisiin, joissa lokitietoa kirjoitetaan useaan kansioon. [19.]
Time-Based Database FlexConnector	Jotkin laitteet kirjoittavat tietoturva tapahtumatiedot tietokantaan. Tämän avulla voidaan lukea tapahtumia tietokannasta taulukkoriveittäin.
ID-based Database FlexConnector	Sopii käytettäväksi, kun käytetään yksilöllisiä tunnuksia tapahtumien lukemiseksi tietokannasta. [19.]
Multi-Database FlexConnector	Tietojen hakeminen useista eri tietokannoista käyttäen samaa kyselyä (query) tai jos haetaan tietoa eri tapahtumia käyttäen erilaisia kyselyjä samasta tietokannasta. [19.]
SNMP FlexConnector	Vastaanottaa tietoturvatapahtuma tietoja Simple Network Management Protocol

	(SNMP) traps -muodossa. [19.]
Syslog Daemon SmartConnector	Kuuntelee tietoturvatapahtumia syslog-paketeista. Käyttää ArcSight Syslog Daemon SmartConnectoria ja määrittelee Syslog FlexConnector sub-connectoria jäsentämään kiinnostavat syslog-paketit. [19.]
XML FlexConnector	Sopii niille laitteille, jotka kirjoittavat lokitapahtumat XML-tiedostoiksi. Tapahtumatiedot näissä tiedostoista on esitetty XML-standardin mukaisesti. [19.]


Lokienhallintajärjestelmän looginen rakenne
Lähteet
Keräys
Tallennus & Arkistointi
Analysointi & Raportointi
Lokia tuottava laite
Lokia tuottava laite
Lokia tuottava laite
SmartConnector
FlexConnector
Syslog
Kytkin
Kytkin
Kuormanjakaja
Kuormanjakaja
kytkin
Kytkin
Connector Appliance Aarne
Connector Appliance Bertta
Tuotantokeräin
Connector Appliance Celsius
Connector Appliance Daavid
Auditointikeräin
Kytkin
Kytkin
Tuotantoloki
Auditointiloki
Logger Eemeli
Logger Faarao
Logger Gideon
Logger Heikki
VMware
Palvelin Yrjö
Palvelin Wiski
SATA
SAS
Levyjärjestelmä
Raportit
Lokien hakeminen
Hälytykset