OULUN AMMATTIKORKEAKOULU

Aleksi Ylitalo

Lokienhallintajärjestelmän soveltuvuusselvitys

SIEM-järjestelmät

Lokienhallintajärjestelmän soveltuvuusselvitys

SIEM-järjestelmät

Aleksi Ylitalo
Opinnäytetyö
Syksy 2018
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tutkinto-ohjelma, Suuntautumisvaihtoehto

Tekijä(t): Aleksi Ylitalo
Opinnäytetyön nimi: SIEM ja soveltuvuusselvitys
Työn ohjaaja: Jukka Kaisto
Työn valmistumislukukausi ja -vuosi: Syksy 2018 Sivumäärä: 38 + 3

Lokitietojen hallinta on ollut esillä Euroopan tietosuoja-asetuksen vuoksi, joka tuli voimaan keväällä 2018. SIEM-järjestelmät nähdään hyvänä vaihtoehtona lokitietojen hallinnan osalta. SIEM-järjestelmällä on mahdollista parantaa organisaation tietoturvaa ja tehostaa IT-ympäristön valvontaa, koska SIEM-järjestelmän avulla voidaan toteuttaa tehokasta lokitietojen analysointia.

Tein opinnäytetyöni keskisuurelle yritykselle. SIEM-järjestelmällä halutaan täyttää Euroopan tietosuoja-asetuksen vaatimukset ja siirtää tärkeät lokitiedot keskitettyyn säilytyspaikkaan, jotta tietojenkäsittelyä voidaan valvoa tehokkaammin.

Opinnäytetyön tavoitteena oli kertoa SIEM-järjestelmistä ja lisätä tietoisuutta niiden toiminnasta. Opinnäytetyössä käsiteltiin myös mitä kaikkea SIEM-järjestelmällä kannattaa seurata. Tämän lisäksi tarkastelin kolmea SIEM-järjestelmää, jotka olivat vaihtoehtoina soveltuvuusselvityksen tekoon ja lopuksi tein soveltuvuusselvityksen yhdestä järjestelmästä. Soveltuvuusselvitykseen annettiin tietyt tavoitteet ja näihin tavoitteisiin päästiin valitun SIEM-järjestelmän kanssa. Tavoitteet soveltuvuusselvityksessä olivat lokitietojen haku tietokannasta ja näkyvyyden lisääminen. Soveltuvuusselvityksessä kerron myös oman näkökulman SIEM-järjestelmän käytöstä organisaation IT-ympäristössä.

Avainsanat: lokitieto, tietoturva, testaus

ABSTRACT

Oulu University of Applied Sciences
Degree programme, option

Author(s): Aleksi Ylitalo
Title of thesis: SIEM and proof of concept
Supervisor(s): Jukka Kaisto
Term and year when the thesis was submitted: autumn 2018 Number of pages: 38 + 3

Log management has been on the carpet last few years because of the European Union General Data Protection Regulation. SIEM system is a good option for log management because SIEM system offers many capalities to log analysis.

This thesis has been made to mid-sized organisation. Organisation wants to fulfill GDPR requirements in regards of log data. Log data needs to be transfered from distributed locations to centralized location. When log data is in centralized location organisation can supervise data processing more effectively.

Purpose of this thesis is to reveal how SIEM systems work and what to monitor with SIEM. After that I reviewed few SIEM system alternatives and made proof of concept with selected SIEM system. Proof of concept objectives were to transfer log data from database and to increase visibility of the IT enviroment. Those objectives were fulfilled in this thesis. Lastly I talk about my own experience about selected SIEM system and how it worked in the organisation's IT enviroment.

Keywords: log, proof of concept, security

SISÄLLYS

KÄSITTEET 7
1 JOHDANTO 11
2 SIEM 13
2.1 Prosessit 14
2.2 Koostaminen 14
2.3 Suodatus 16
2.4 Normalisointi 17
2.5 Yhdistely 18
2.6 Säilytys 20
2.7 Toimenpide 20
2.8 Raportit 21
2.9 Näkymät 23
2.9.1 Autentikointi 23
2.9.2 Muutokset 24
2.9.3 Tietoliikenne 25
2.9.4 Resurssit 26
2.9.5 Haittaohjelmat 28
2.9.6 Kriittiset virheet 28
3 KÄYTTÖÖNOTTO 30
3.1 Suunnitteluvaihe 30
3.2 Testausvaihe 30
3.3 Hallittu käyttöönotto 31
3.4 Jatkuvan kehityksen vaihe 31
3.5 Ohjeita käyttöönottoon 31
4 SOVELTUVUUSSELVITYS 33
4.1 Logpoint 33
4.2 ELK 35
4.3 RSA 37
4.4 Järjestelmän valinta 38
4.5 SIEM-järjestelmän soveltuvuus 38

5 POHDINTA 42
6 LÄHTEET 44
7 LIITTEET 48

KÄSITTEET

Active Directory	Windows-toimialueen hakemistopalvelin
Avoin lähdekoodi	Ohjelmiston kehitysmenetelmä, jonka periaate on, että käyttäjillä on mahdollisuus muokata ohjelmiston lähdekoodia
EPS	Events per second. Tämä tarkoittaa sitä, kuinka montaa lokitietoa SIEM-järjestelmään tulee sekunnissa.
Haittaohjelma	Ohjelmisto, jonka tarkoituksena on aiheuttaa haittaa järjestelmälle.
Haittaohjelmien torjuntaohjelmisto	Ohjelma, jonka tarkoitus on huomata ja estää haittaohjelmat.
IDS	Intrusion detection system. Tarkoittaa tunkeilijan havaitsemisjärjestelmää.
IP-osoite	Tunniste, jonka avulla verkkosovittimia yksilöidään
IPS	Intrusion prevention system. Tarkoittaa murron estämisjärjestelmää.
JSON	JavaScript Object Notation. standartoitu tiedostomuoto.
Koostaminen	Tarkoittaa lokitietojen viemistä yhteiseen yhtenäiseen järjestelmään.
Lisp	Ohjelmointikieli, jonka datarakenne koostuu linkitetyistä listoista.
Lokitieto	Tapahtumarekisteri johon kerätään tapahtumahistoriat.

Lokiagentti	Ohjelma, jonka avulla lokitiedot lähetetään.
Normalisointi	Tarkoittaa lokien muuttamista samankaltaiseen muotoon.
NoSql	Tietokantamalli, joka poikkeaa perinteisestä relaatiomallista.
ODBC-yhteys	Tietokanta yhteys, jonka avulla sovellukset hakevat tietokannasta tietoa.
Ohjelmistorajapinta	Määrittää, kuinka ohjelmisto tarjoaa tietoa tai palveluita muille tietojärjestelmille.
Portti	Tarkoittaa tietoliikenteessä palvelupistettä.
Soveltuvuusselvitys	Vaihe, jossa testataan järjestelmän toimivuutta ja perustellaan sen arvo.
Prosessi	Tarkoittaa ajossa olevaa ohjelmaa.
Rekisteri	Microsoft Windowsissa sijaitseva tietokanta, jossa on tietoja joita Windows sekä sovellukset käyttävät.
Restful ohjelmistorajapinta	Rajapinta, joka käyttää http-prokollan käskyjä tiedon hakemiseen.
Rogue access point	Langaton tukiasema, joka toimii lähiverkossa ilman ylläpitäjän lupaa tai oikeutetusta.
SEM	Security event manager. Järjestelmä, jonka avulla lokeja voidaan seurata reaaliajassa sekä yhdistellä tapahtumia.
SIEM	Security information and event management.Yhdistää SIM ja SEM-järjestelmien toiminnallisuudet.

SIM	Security information management. Järjestelmä, jonka avulla lokeja kerätään keskitettyyn paikkaan pitkä aikaiseen säilytykseen ja mahdollistaa analysoinnin sekä raportit.
Skriptit	Sarja komentoja, jotka ajetaan. Skriptin avulla on mahdollista automatisoida prosesseja.
SNMP	Protokolla, jonka avulla verkossa olevalta laitteelta haetaan tilatietoja.
Suodattaminen	Tarkoittaa tiedon erittelyä, että mitä lokitietoa halutaan lähettää SIEM-järjestelmään.
Syslog	Protokolla, jonka avulla laitteet lähettävät lokeja keskitettyyn palvelimeen. Syslog on myös standardi, joka määrittää tapahtumalokien mallin.
Tapahtuma	On normalisoitu lokitieto.
TCP	Transmission Control Protocol tarkoittaa yhteyksellistä tietoliikenneprotokollaa.
Tietokanta	Tietovarasto, jossa on kokoelma tietoja ja niillä voi olla yhteys. Yleisin tietokanta malli on relaatiotietokanta. Siinä tiedot tallennettaan tauluihin.
UDP	User Datagram Protocol. Tietoliikenneprotokolla, joka on yhteydetön.
UEBA	Järjestelmä, joka analysoi koneoppimisen avulla käyttäjien ja laitteiden toimintaa.
WAF	Web application firewall. Suomeksi se tarkoittaa Verkkosovellus palomuuria.

WMI	Windows management instrumentation on osa Windowsia ja se mahdollistaa hallintatietojen käsittelemisen IT-ympäristössä paikallisesti ja etänä.
VPN-yhteys	virtual private network. Tarkoittaa suomeksi virtuaalinen erillisverkko.
Väsytyshyökkäys	Toiselta nimeltään brute force hyökkäys. Tällä hyökkäyksellä yritetään järjestelmällisesti arvata salasana.
XML	Extensible Markup Language. Merkintä kieli, jonka avulla voidaan varastoida sekä siirtää tietoa.
Yhdistely	Tarkoittaa tapahtumien yhdistämistä. Voidaan käyttää myös termiä korrelaatio.

1 JOHDANTO

SIEM-järjestelmä mahdollistaa lokitietojen keräämisen keskitettyyn paikkaan ja niiden tehokkaan analysoimisen. SIEM-järjestelmä on lisännyt suosiota viime vuosina erilaisten määräysten ja standardien vuoksi. Euroopan unionin tietosuoja-asetus lisäsi järjestelmän suosiota, koska sen avulla voidaan varmistaa oikeaoppinen tietojenkäsittely. SIEM-järjestelmän avulla on mahdollista parantaa organisaation tietoturvaa ja tietosuojaa. Nämä ovat asioita, joiden merkitys on ollut kasvussa IT-alalla sekä muutenkin organisaatioissa. Hyökkäyksen sattuessa infrastruktuuri voi lamaantua ja ihmisten tietoja joutua vääriin käsiin. Yleisiä ovat niin kutsutut palvelunestohyökkäykset. Hyökkäykset aiheuttavat pahimmillaan sen, että organisaation tarjoamat palvelut eivät ole saatavilla. Toinen vakava trendi on ollut kiristyshaittaohjelmien yleistyminen. Ne salaavat tietokoneen tai palvelimen kovalevyn ja tämän vuoksi tiedot eivät ole saatavilla. SIEM-järjestelmän avulla tällaiset hyökkäykset voi huomata ajoissa, jolloin tietoturvahenkilöstö voi aloittaa tarvittavat toimenpiteet. Myös yritykset ovat huomanneet SIEM-järjestelmien hyödyn. Tutkimuksen mukaan SIEM-markkinat tulevat kasvamaan noin 10,1 prosenttia vuoteen 2023 mennessä (PRnewswire 2017, viitattu 30.9.2018).

Opinnäytetyön aiheen sain toimeksiantajalta, joka toimii finanssialalla ja siellä työskentelee satoja työntekijöitä ympäri Suomea. IT-ympäristö koostuu noin 200 palvelimesta sekä kymmenistä verkkolaitteista. SIEM-järjestelmällä haetaan apua Euroopan unionin uuden tietosuoja-asetuksen vaatimiin edellytyksiin. Tämä tarkoittaa organisaation näkökulmasta sitä, että lokitietojen täytyy olla hyvässä tallessa. Tärkeimmät lokitiedot halutaan tallettaa yhteen paikkaan talteen. Tällöin lokitietojen hallinta on helpompaa ja niitä voidaan analysoida tehokkaammin. SIEM-järjestelmällä kehitetään yrityksen tietoturvaa sekä saadaan enemmän näkyvyyttä siihen, mitä organisaation järjestelmissä sekä tietoliikenneverkoissa tapahtuu. Tietoturvallinen ympäristö on lähempänä tavoitettaan, kun järjestelmä on saatu siihen vaiheeseen, että lokitietoja tulee monista eri järjestelmistä ja niitä analysoidaan. SIEM-järjestelmällä voisi myös helpottaa IT-infrastruktuurin valvontaa, koska SIEM-järjestelmän avulla tapahtumalokeja voidaan yhdistellä ja näkymien avulla nähdään jatkuvasti ympäristön tilanne.

Opinnäytetyössäni esitellään SIEM-järjestelmien perusteita, jotta niiden toimintaa voidaan ymmärtää. Tämän lisäksi käytännön työ koostuu SIEM-järjestelmän soveltuvuusselvityksestä organisaatiolle. Tutkin myös, mitä asioita SIEM-järjestelmällä kannattaa tehdä organisaation näkökulmasta

sekä tarjoan mahdollisia vinkkejä käyttöönottoon liittyen. Opinnäytetyöhön liittyy myös SIEM-järjestelmien keskeisten ominaisuuksien vertailu sekä valitun järjestelmän laajempi esittely. Arvioinnin kohteiksi valikoituivat sellaiset järjestelmät, jotka olivat organisaatiossa vaihtoehtoina. Tämän vertailun avulla voidaan nähdä mikä SIEM-järjestelmä olisi paras organisaatiolle.

2 SIEM

SIEM-järjestelmä määritellään usein kahden eri järjestelmän sulautumisena, koska SIEM-järjestelmä yhdistää SIM- ja SEM-järjestelmän toiminnallisuudet. SIM-järjestelmä pitää sisällään toiminallisuudet kuten lokitietojen kerääminen, analysointi ja raportointi. SEM-järjestelmä koostuu lokitietojen reaaliaikaisesta seurannasta ja yhdistelystä. Näin ollen SIEM-järjestelmä on tehokas työkalu lokitietojen analysointiin, koska nämä ominaisuudet tulevat yhdessä paketissa. SIEM-järjestelmä kerää lokitietonsa IT-ympäristöstä. Lähteitä ovat esimerkiksi sovellukset, työasemat, palvelimet ja verkkolaitteet. Lokitietojen keräämisen jälkeen SIEM-järjestelmä tunnistaa ja kategorisoi tapahtumat sekä analysoi ne (Csonline, 2017, Mary K. Pratt, viitattu 29.9.2018.)

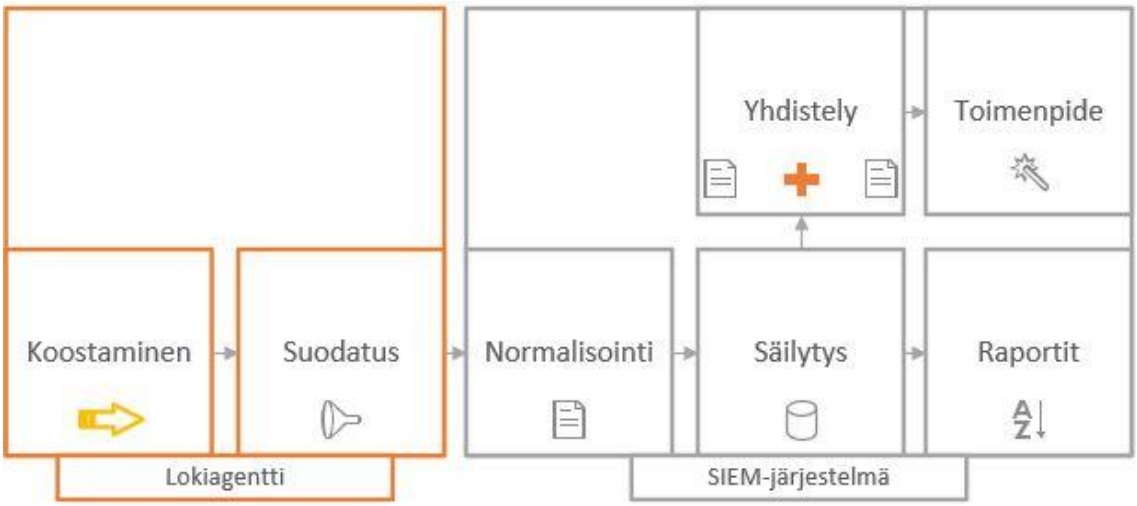
SIEM-järjestelmä auttaa IT-henkilöstöä valvomaan, mitä heidän järjestelmissään ja tietoliikenneverkoissaan tapahtuu. SIEM-järjestelmä antaa näkyvyyttä tietoliikenneverkkojen ja järjestelmien tilasta sekä tapahtumista. (Sama lähde, kuin edellisessä kappaleessa.) Tämä lisää IT-henkilöstön luottamusta. Luottamuksella tässä asiassa tarkoitetaan sitä, että järjestelmät ja tietoliikenneverkot täytyy tuntea hyvin, jotta voidaan sanoa, milloin poikkeavuuksia tapahtuu. (Chuvakin, Schmidt, Phillips kappale 7, 2013.) Petri Vesamäen mukaan SIEM-järjestelmä auttaa organisaatiota reagoimaan ja löytämään ongelmat sekä tietomurrot. Näin ollen vikoihin ja tietomurtoihin voidaan reagoida nopeammin ja tuotanto katkot voidaan selvittää pikaisemmin. (Viestintävirasto, 2016, Petri Vesamäki, viitattu 3.7.2018.)

Tänä päivänä SIEM-järjestelmä integroituu moniin eri järjestelmiin. Tämä on tärkeää, että SIEM-järjestelmä tukee mahdollisimman monia järjestelmiä, koska tällöin datan määrä on suurempi. Mitä suurempi lokitietojen määrä sen paremmin SIEM-järjestelmällä saadaan tuloksia aikaan. (Sama lähde, kuin edellisessä kappaleessa.)

SIEM-järjestelmien kehittäjiä on monia. Tunnetuimpia ovat Solarwinds, ArchSight ja Splunk (Comparitech, 2018, Tim Keary, viitattu 5.9.2018). On myös muita pienempiä toimijoita kuten Logpoint. Avoimeen lähdekoodiinkin perustuvia SIEM-järjestelmiä on markkinoilla. Tällaisia ovat esimerkiksi Alien Vaultin kehittämä OSSIM ja Elasticsearch pohjainen ELK-stack.

2.1 Prosessit

SIEM-järjestelmän toiminnasta täytyy tietää tietyt prosessit, jotka liittyvät oleellisesti järjestelmän toimintaan. Nämä prosessit ovat suodatus, normalisointi, yhdistäminen, toimenpide ja raportit (Chuvakin, Schmidt, Phillips, kappale 9, 2013). Lisäksi prosesseihin kuuluu aggregointi eli koostaminen ja säilytys (Stackify, 2017, viitattu 30.9.2018). Näistä kyseisistä prosesseista rakentuu koko SIEM-järjestelmän perusta.



Kaavio lokitiedon vaiheista

2.2 Koostaminen

Koostaminen tarkoittaa lokitietojen siirtämistä SIEM-järjestelmään. Lokitiedot tallennettaan yleensä tietokantaan ja tämän avulla tapahtuu raportointi, analysointi ja yhdistely. Lokitietoja voi tulla lähteistä reaaliajassa tai järjestelmät on voitu konfiguroida niin, että lokitietoja lähetetään tietyn ajan välein. (Securosis, 2010, Adrian Lane, viitattu 30.7.2018.)

SIEM-järjestelmä saa lokitietoja lokiagenttien ja kerääjien avustuksella. Lokitietojen lähetys voidaan konfiguroida myös ilman lokiagenttia tietyissä tapauksissa. Lokiagentti on ohjelmisto, joka lähettää lokitietoja tietoliikenneverkon kautta SIEM-palvelimelle. Yleisesti lokiagentti on parempi vaihtoehto, kuin ilman lokiagenttia tapahtuva lokitietojen siirto (Eventsentry, 2017, Ingmar Koecher, viitattu 30.9.2018.)

Lokiagentit ovat turvallisempia, koska agentti lähettää lokitiedot eteenpäin. Ilman agenttia toimivassa ympäristössä palvelimet on konfiguroitu, niin että lokitiedot haetaan etäyhteyksien avulla. Tämä aiheuttaa tietoturvauhkan, koska järjestelmään tulee lisää keinoja, kuinka tietoa voidaan hakea etäyhteyden avulla. Lisäksi tunnukset täytyy olla yhdessä tallessa, josta ne haetaan, kun etäyhteys otetaan. Tämän vuoksi tunnukset ovat vaarassa, koska ne haetaan verkon välityksellä toiselta palvelimelta. Toisen palvelimen joutuessa murretuksi, tunnukset ovat vaarassa. (Sama lähde, kuin edellisessä kappaleessa.)

Luotettavuus lokiagenteissa tulee siitä, jos tietoliikenneverkossa ilmenee jokin ongelma, niin yleensä agentit pystyvät tallentamaan lokitiedot. Agentit tallentavat lokitiedot välimuistiinsa ja lähettää ne eteenpäin, kun vika on korjattu. Näin SIEM-järjestelmä saa lokitietonsa, kun ongelmat on korjattu. (Sama lähde, kuin edellisessä kappaleessa.)

Lähettämisen yhteydessä voidaan suodattaa, mitä lokitietoja halutaan lähettää eteenpäin. Tämä on hyvä, koska sen avulla säästetään tietoliikenneverkon resursseja. Ilman lokiagenttia toimiva lokitietojen haku ei mahdollista tehokasta suodatusta. (Sama lähde, kuin edellisessä kappaleessa.)

Lokiagenteilla voidaan siirtää paljon eri tyyppisiä lokitietoja, koska lokiagentti on asennettu paikallisesti palvelimille ja niillä on pääsy palvelimien resursseihin. Ilman lokiagenttia toimivassa ympäristössä eri tyyppisten lokitietojen kerääminen on hyvin rajattua. Tämä johtuu siitä, että yleensä lokiagentit voivat käyttää tietojen hakemiseen monia eri keinoja kuten ohjelmistorajapintaa, WMI-rajapintaa tai rekisteriä. Ilman lokiagenttia toimivissa ympäristöissä käytetään vain WMI-rajapintaa. (Sama lähde, kuin edellisessä kappaleessa). WMI-rajapinnalla tarkoitetaan Windowsin työkalua, joka mahdollistaa palvelimien ja työasemien ylläpidon etänä. Esimerkiksi skriptejä voi ajaa sen kautta etänä. (Techopedia, viitattu 5.9.2018.)

Verkkolaitteet kuten kytkimet ja reitittimet eivät käytä lokiagentteja (Eventsentry, 2017, Ingmar Koecher, viitattu 30.9.2018). Verkkolaitteissa lokitiedot liikkuvat SNMP-protokollan ja syslog-protokollan avulla. Näillä molemmilla on omat käyttötarkoituksensa. SNMP-protokollan avulla saadaan tietoa reaaliajassa ja sen avulla voidaan seurata laitteen tilannetta. Syslog-protokollan lokitiedoilla on hyvä tarkastella tapahtumia jälkikäteen. SNMP-protokolla käyttää hyödyksi UDP-porttia 161 ja 162. Syslog-protokolla käyttää TCP/UDP-porttia 514. (Ipwithease, 2015, viitattu 30.9.2018.) SNMP-protokollaa ja Syslog-protokollaa voidaan käyttää myös niin, että SNMP-protokollan avulla

lähetetään Syslog lokitietoja eteenpäin. Tämä on kätevä ominaisuus tietoliikenneverkoissa, joissa on sallittu vain SNMP-protokollan liikenne. (Dooley, Brown, kappale 17.14, viitattu 1.10.2018.)

Kaikkiin palvelimiin tai työasemiin ei kuitenkaan asennetta lokiagentteja. Tällaisessa tilanteessa kerääminen voidaan toteuttaa esimerkiksi Windows ympäristössä niin, että palvelin, jossa on lokiagentti, hakisi lokitietoja palvelimelta. Tämä onnistuu yksinkertaisimmillaan, niin että tapahtumavalvonnan kautta konfiguroidaan tilaus kyseiselle palvelimelle sekä määritetään, millaisia lokitietoja sieltä haetaan. Tällöin palvelin, jossa lokiagentti on hakisi lokitiedot ja sen jälkeen lähettää lokitiedot eteenpäin. Kannattaa kuitenkin muistaa, että tässä on omat riskinsä. Lokitietojen hakeminen tapahtuu WMI-rajapintaa käyttäen. Tällöin avataan aina etäyhteys, jonka kautta lokitiedot haetaan. (Logpoint, Agentless, WMI-Less Collection of Endpoint Logs, 2015, Christian Have, viitattu 4.8.18.)

Tärkeissä palvelimissa on parasta käyttää lokiagenttia, koska silloin lokitietojen toimitus on luotettavaa. Ilman lokiagenttia toimiva lokitietojen hakeminen toimii hyvin, jos kyseessä on monia työasemia, joista niitä halutaan kerätä, koska lokiagenttien pitäminen ajan tasalla on haastavaa sekä niiden konfiguroiminen eri työasemille on hidasta. (Sama lähde, kuin edellisessä kappaleessa.)

Joissain SIEM-järjestelmissä koostaminen toimii niin, että lokiagentti lähettää lokitiedot ensin kerääjälle ja kerääjä lähettää lokitiedon eteenpäin SIEM-järjestelmälle (Pratum, 2016, Colton Bachman viitattu 9.9.2018).

2.3 Suodatus

Lokienhallintajärjestelmissä ja SIEM-järjestelmissä suodatuksella otetaan alkuperäinen lokitieto ja päätetään mitä lokitietoja halutaan siirtää eteenpäin. Näin saadaan säästettyä tilaa ja siirrettyä vain sellaisia lokitietoja, joita halutaan. Suodatuksen tekee yleensä lokiagentti, joka huolehtii lokitietojen siirrosta. Suodatuksen jälkeen alkuperäiset lokitiedot normalisoidaan. (Chuvakin,Schmidt, Phillips kappale 9, 2013.)

2.4 Normalisointi

Normalisoimalla lokitietoja kaikki saapuvat lokitiedot muutetaan samanlaiseen muotoon, koska eri valmistajien järjestelmät tuottavat lokitietoja, joiden rakenteessa on paljon eroavaisuuksia. Tärkeimmät tiedot, joita alkuperäisistä lokitiedoista otetaan ovat: lähde ja kohde IP-osoitteet, lähde- ja kohdeporttinumerot, määritellään niin kutsuttu taksonomia, aikatiedot, käyttäjäinformaatio, prioriteetti, tapahtuma ja alkuperäiset lokitiedot. (Chuvakin, Schmidt, Phillips, kappale 9, 2013.)

IP-osoitteet on hyvä ottaa mukaan, koska ne ovat tärkeitä yhdistelyprosessissa ja niiden avulla tiedetään mistä lokitieto on tai mikä sen on aiheuttanut. IP-osoitteiden avulla on helppo etsiä tapahtumia, jotka koskevat vain tiettyä palvelinta. IP-osoitteiden lisäksi, kun otetaan lähde- ja kohdeporttitiedot, niin tällöin tiedetään, että mihin palveluun yritetään päästä kohde järjestelmässä. (Sama lähde, kuin edellisessä kappaleessa.)

Taksonomia tarkoittaa tiedon luokittelua. Lokitiedot luokitellaan tässä tapauksessa yleensä sen mukaan mitä on tapahtunut. Esimerkiksi eri laitteet tuottavat kirjautumislokeja. Taksonomia voidaan toteuttaa niin, että jaetaan onnistuneet ja epäonnistuneet kirjautumiset erikseen. Analytiikan kannalta tämä on hyödyllistä, sillä kaikki samaa tarkoittavat kirjautumislokitiedot menevät samaan kategoriaan, vaikka järjestelmän toimittajat ovat eriä. (Sama lähde, kuin edellisessä kappaleessa.)

Aikatiedoilla tiedetään, milloin jotain on tapahtunut. Hyvin toteutuksessa normalisoinnissa on kaksi aikatietoa. Milloin lokitieto on luotu järjestelmään ja milloin lokitietojärjestelmä on saanut lokitiedon. (Sama lähde, kuin edellisessä kappaleessa.)

Käyttäjätiedoilla yksilöidään käyttäjä (Sama lähde, kuin edellisessä kappaleessa). Lokitiedossa käyttäjänimen kohdalla voi olla prosessin nimi. Käyttäjätieto on tärkeä silloin, kun seurataan käyttäjien toimintaa IT-ympäristössä.

Tapahtuma kertoo, että mitä on tapahtunut tiettynä ajan hetkenä (Securosis, 2010, Adrian Lane, viitattu 30.7.2018). Tämän lisäksi monet järjestelmän toimittajat antavat prioriteettiarvon tapahtumalle. Se kertoo, kuinka tärkeä tapahtuma on kyseessä (Chuvakin, Schmidt, Phillips, kappale 9, 2013).

Alkuperäiset lokitiedot halutaan säilyttää, koska niitä tarvitaan siihen, että varmistetaan normalisoidun tapahtuman kelpoisuus. Tämä tapahtuu vertaamalla alkuperäistä lokitietoa normalisoituun tapahtumaan. Tämän lisäksi voi olla vaatimuksia, että alkuperäinenkin lokitieto täytyy säilyttää. (Chuvakin, Schmidt, Phillips, kappale 9, 2013.) Alkuperäiset lokitiedot yleensä tallennettaan SIEM-järjestelmissä erillisiin hakemistoihin. Lisäksi SIEM-järjestelmissä voi olla ominaisuus, että alkuperäiset lokitiedot on yhdistetty normalisoituun tapahtumaan. (Securosis, 2010, Adrian Lane, viitattu 30.7.2018.)

Normalisoimalla lokitietoja niiden tutkiminen ja analysointi onnistuu helpommin sekä tehokkaammin, koska ei tarvitse tietää jokaisen valmistajan lokimallia vaan riittää, että osaa lokihallintajärjestelmän lokimallin. Normalisoinnin jälkeen lokitietoja kutsutaan tapahtumiksi. (Sama lähde, kuin edellisessä kappaleessa.)

2.5 Yhdistely

SIEM-järjestelmien yhdistelyn mahdollistaa niin kutsuttu korrelaatiomoottori. Hyvästä moottorista löytää ominaisuuksia kuten tilallinen toiminta, laskenta, aikakatkaisu, sääntöjen uudelleen käyttäminen, prioriteetti ja kieli. (Chuvakin, Schmidt, Phillips kappale 9, 2013.)

Tilallisella toiminnalla tarkoitetaan sitä, että yhdellä säännöllä on monta eri tilaa. Esimerkiksi voidaan seurata tapahtumia joiden kohdeportti olisi 80, jos tällainen tapahtuma löytyy, niin seuraava tila voisi tarkastella kaikkia tapahtumia, joissa on tämän http tapahtuman kanssa sama lähde IP-osoite. Tällä kyseisellä esimerkillä voitaisiin selvittää luvatonta webpalvelimen käyttöä. (Sama lähde, kuin edellisessä kappaleessa.)

Laskenta on yksinkertainen ominaisuus, mutta hyödyllinen. Sen avulla voidaan tehdä sääntöjä, jotka laskevat montako kertaa jokin tapahtuma esiintyy. Käytännön esimerkki tästä on, jos tiettyä porttia skannataan monta kertaa, niin silloin voidaan laskea samojen tapahtumien määrä. Tästä voidaan huomata, että joku pyrkii ahkerasti löytämään tämän tietyn portin avonaisena. (Sama lähde, kuin edellisissä kappaleissa.)

Aikakatkaisu liittyy korrelaatiomoottorin ominaisuuksiin. Kun yhdistelyä tehdään, niin korrelaatiomoottori käyttää välimuistia siihen, että se toimisi mahdollisimman sulavasti. Välimuistin täyttyessä

hidastuu isäntäkone sekä itse SIEM-järjestelmä. Tämän vuoksi välimuistia pitää tyhjentää tietyn ajan välein sen mukaan, onko tapahtuma vastannut muihin kriteereihin. Jos välimuistin tyhjennystä on mahdollista konfiguroida, niin sen tyhjennys kannattaa ajastaa noin viiteen minuuttiin. (Sama lähde, kuin edellisissä kappaleissa.)

Sääntöjen uudelleen käyttämisellä helpotetaan ylläpitäjien työtä, koska sääntöjä voi olla monia ja niillä voi olla monenlaisia tiloja. Sääntöjen osia on hyvä pystyä uudelleen käyttämään, koska näin sääntöjen tekemisessä säästetään aikaa. (Sama lähde, kuin edellisissä kappaleissa.)

Prioriteetti tarkoittaa sitä, että säännöille määritellään prioriteettiarvo. Tämä määrittää sen mikä sääntö on tärkeämpi, kuin toinen. Korkeammalla prioriteetti arvolla olevat säännöt ajetaan ensin. (Sama lähde, kuin edellisissä kappaleissa.)

Jokaisessa korrelointimoottorissa on oma kieli, jonka avulla sääntöjä tehdään. Tässä tärkein asia on se, että kieli olisi mahdollisimman helppo oppia ja käyttää. Yleisimmät kielet, joita käytetään ovat XML ja Lisp. (Sama lähde, kuin edellisissä kappaleissa.)

Yhdistelyn kanssa täytyy pitää mielessä se, että ne voivat tuottaa myös vääriä hälytyksiä. Esimerkiksi, jos organisaatio itse tekee aktiivisesti porttiskannausta ja SIEM-järjestelmä huomaa tämän, niin se luulee sitä oikeaksi vakoilu yritykseksi. Onkin tyypillistä, että alussa SIEM-järjestelmä tuottaa paljon vääriä hälytyksiä, mutta tämä voidaan välttää hienosäätämällä järjestelmää. Kannattavaa on tarkastella yhdistelysäännöt läpi, joita kaikissa SIEM-järjestelmissä on käytössä jo valmiina. Näistä yleensä noin 60% joudutaan poistamaan, mutta riippuu tietenkin ympäristöstä. (Scnsoft, 2017, Dmitry Nikolaenya, viitattu 31.7.2018.)

Yhdistelyllä voidaan yhdistellä tapahtumia keskenään. Tämä on tehokas keino, sillä sen avulla voidaan huomata suhteita eri tapahtumien välillä ja luoda näin kuva tapahtumaketjuista. Yhdistely on tärkeää, koska sen avulla tarkastellaan tietoturvaa ympäristön tasolla eikä pelkästään yksittäisten laitteiden tasolla. Yhdistelemällä voidaan parantaa vikojen huomaamista, koska yhdistelemällä tapahtumia voidaan huomata tapahtumaketjuja. Jos tietomurto tapahtuisi, niin yhdistelyn avulla voidaan huomata kokonaiskuva siitä, miten hyökkäys on tehty. Tämä kokonaiskuva luo tukevan pohjan tietomurto tutkimuksille. (Manageengine, 2018, Nivathi Bhat, viitattu 7.9.2018.)

SIEM-järjestelmät tekevät yhdistelyn sääntöpohjaisesti. Käytännössä se tarkoittaa sitä, että järjestelmän ylläpitäjä tekee säännöt. Näiden sääntöjen avulla järjestelmä yhdistelee tiettyjä tapahtumia ja ilmoittaa, jos nämä toteutuvat. (Alienvault, 2018, Kim Crawley, viitattu 31.7.2018.) SIEM-järjestelmissä on yleensä valmiiksi tehtyjä sääntöjä heti käyttöönotossa. Näihin ei kuitenkaan kannatta luottaa, koska ympäristöissä on paljon eroja ja jokainen on omanlainen. (Scnsoft, 2017, Dmitry Nikolaenya, viitattu 31.7.2018.)

2.6 Säilytys

Lokien säilytys on tärkeä osa, koska sieltä voidaan tarkastella jälkikäteen, jos historiassa on tapahtunut jotain poikkeavaa. SIEM-järjestelmä on tähän käyttötarkoitukseen hyvä, koska nämä järjestelmät tallentavat lokitiedot tietokantaan. Järjestelmässä voidaan säätää, kuinka kauan lokitiedot säilötään. Järjestelmissä lokitiedot on mahdollista jakaa eri kansioihin sen mukaan, minkälainen lokitieto on kyseessä. Eri standardit voivat määrittää sääntöjä sen suhteen, miten kauan lokitietoja pidetään säilössä (tästä esimerkkinä on ISO-27001). Lisäksi lokien säilytyksessä täytyy määrittää se, kuka lokitietoja pääsee lukemaan ja kuinka ne on suojattu, koska lokitietojen luottamuksellisuus sekä eheys täytyy taataa. Luottamuksellisuus tarkoittaa sitä, että vain sellaiset henkilöt pääsevät lukemaan lokitietoja keillä on siihen oikeus. Eheys tarkoittaa sitä, että tieto ei saa muuttua ja se on oikeaa (Advisera, 2015, Antonio Segovia, viitattu 18.11.2018.)

Säilytyksessä täytyy ottaa huomioon se, että miten paljon massamuistia tarvitaan tietokantaa varten, jota SIEM-järjestelmät käyttävät. Arvion voi laskea tällaisella kaavalla: palvelinten lukumäärä * (lokitiedon koko * lokien määrä päivässä) * säilytettävä aika. (Auvik, 2014, Rod Lewis, viitattu 25.9.2018.)

2.7 Toimenpide

SIEM-järjestelmissä toimenpide tarkoittaa tiettyihin tapahtumiin tai yhdistettyihin tapahtumiin vastaamista. Toimenpiteitä voi olla monenlaisia SIEM-järjestelmästä riippuen. Yleisimmät ovat sähköpostin, tekstiviestin tai työpyynnön aukaisu, joka kertoo ylläpitäjälle mitä on tapahtunut ja toimii näin ollen hälytyksenä. Tähän sitten ylläpitäjä vastaa parhaaksi näkemällään tavalla. Kehittyneimmissä järjestelmissä voi olla toimenpiteenä jonkin prosessin ajo vastauksena tapahtumalle. Tällainen

yleensä toteutetaan ajamalla skripti tapahtuman yhteydessä. Tällainen toimenpide voisi olla esimerkiksi jonkin palvelun sulkeminen, jos hyökkäys tulee tiettyä palvelua vastaan. (McAfee, 2014, viitattu 2.8.18.)

2.8 Raportit

Raportilla on tarkoitus dokumentoida tapahtumia ja kertoa tilanteesta kohteelle (Kajaanin ammattikorkeakoulu, viitattu 30.9.2018). Näin raporttia kuvataan yleensä ja SIEM-järjestelmän raportit tekevät tätä samaa. Ne kertovat mitä ympäristössä tapahtuu yleensä graafisten kaavioiden ja tietojen avulla. Henkilöstö muodostaa itse tästä tiedosta mielipiteensä.

SIEM-järjestelmän seurannan kattavuutta voidaan kasvattaa yleisten raporttien avulla. Niissä on paljon vaihtoehtoja eri raporteille. Päätettäessä millaisia raportteja seurataan, niin yleensä seurataan sellaisia raportteja kuten kuka, milloin ja mistä. Hyödylliset SIEM-järjestelmän raportit koostuvat yleensä seuraavista asioista: Autentikoinnit, muutokset, tietoliikenne, resurssien valvonta, haittaohjelmat ja kriittiset virheet raportit (Chuvakin, Schmidt, Phillips, kappale 12, 2013). Näitä raportteja täytyy seurata säännöllisesti ja sen vuoksi pitääkin sopia, kuinka useasti raportteja katsotaan ja kuka tai ketkä ovat siitä vastuussa. Näiden lisäksi täytyy miettiä toimia, jos on tapahtumia, jotka ovat normaalista poikkeavia. (Searchdatacenter, 2018, Jessica Lulka, viitattu 18.8.2018.)

Autentikointiraportit koostuvat onnistuneista sekä epäonnistuneista autentikoinneista järjestelmiin. Tähän raporttiin kuuluu myös käyttöoikeustasojen seuranta. Esimerkiksi sellaisten käyttäjien, joilla on järjestelmänvalvojan oikeudet. Autentikointiraportit ovat tärkeitä, koska autentikointi määrittelee pääsyn nykypäivän järjestelmiin. Näiden raporttien tarkastelun täytyy olla yksi organisaation pääasiallinen tietoturvan seurantakeino. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Muutosraportit pitävät sisällään tiedot muutoksista, joita järjestelmiin ja laitteisiin on tehty. Nämä raportit ovat tärkeitä, koska niiden avulla saadaan selville, milloin muutoksia on tehty. Näin nähdään helposti, jos on tapahtunut muutos, joka on tehty luvatta. Luvatta tehdyt muutokset voivat aiheuttaa järjestelmien kaatumisia, tietohävikkiä ja turvallisuuteen liittyviä selkkauksia. Lisäksi hyökkääjät useasti muokkaavat järjestelmien asetuksia, jotta he pääsisivät tulevaisuudessa järjestelmiin helpommin. Schmidtin mukaan myös huolellinen muutoksien seuranta parantaa IT-henkilöstön toimintaa. (Sama lähde, kuin edellisessä kappaleessa.)

Tietoliikenteen raportit paljastavat mahdolliset vaaralliset aktiviteetit tietoliikenneverkossa. Nämä raportit ovat tärkeitä, koska tietoliikenneverkko on pääasiallinen keino, kuinka uhat saapuvat järjestelmiin. Tämän lisäksi tietoliikenneverkkoja käytetään hyödyksi tietovarkauksissa ja tietovuodoissa. (Sama lähde, kuin edellisissä kappaleissa.)

Resurssienvalvonta raporttien avulla seurataan tiettyjen järjestelmien, sovelluksien sekä tietokantojen käyttöä organisaatiossa. Näiden avulla voidaan toteuttaa aktiviteetti-, trendi ja tapahtumaseurantaa. Resurssien seurannan avulla voidaan paljastaa, jos organisaation sisältä joku väärinkäyttää tietoja. Nämä raportit ovat myös hyvin arvokkaita, kun vastataan tapahtumiin. Esimerkiksi, jos halutaan tietää mihin tietoihin hyökkääjä on päässyt käsiksi ja onko hän muokannut tietoja. Resurssiraportteja voidaan myös käyttää muutenkin hyödyksi, esimerkiksi, jos suunnitellaan tallennustilan käyttöä. (Sama lähde, kuin edellisissä kappaleissa)

Haittaohjelma raportit tiivistävät erilaisten epäilyttävien sovelluksien toimintaa, jotka mahdollisesti liittyvät haittaohjelmaan. Haittaohjelmaraportit ovat tärkeitä, koska haittaohjelmat ovat yksi suurimmista tietoturvauhkista yritykselle. Pelkkä haittaohjelmien torjuntaohjelmisto ei riitä, vaan sen lisäksi tarvitaan lokitietojen tai tapahtumien analysointia, koska haittaohjelma voi päästä läpi tietoturva ohjelmistosta. SIEM-järjestelmällä on mahdollista huomata haittaohjelma, jos palvelin alkaa esimerkiksi oireilemaan ja siitä saadaan lokitietoja SIEM-järjestelmään. Lisäksi SIEM-järjestelmä saa haittaohjelma torjuntaohjelmiston lokitietoja. Varsinkin nykyaikana, koska haittaohjelmien torjunta tehokkuus on ollut laskussa. (Sama lähde, kuin edellisissä kappaleissa.) Vuonna 2017 tehdyn raportin mukaan tämä pitää paikkansa. Haittaohjelmien tunnistusprosentti laski vuodesta 2015-2016 noin kaksi prosenttiyksikköä. Huomion arvoisin oli kuitenkin, niin kutsuttujen nollapäivähyökkäyksien huomaaminen. Näiden tunnistaminen tippui jopa 10 prosenttia. Vuosina 2015-2016 tunnistamisen prosentti oli 80 ja 2017 se on tippunut 70 prosenttiin. (Csonline, 2017, Is antivirus getting worse, Maria Korolov, viitattu 22.8.2018.)

Kriittisten virheiden raporttien avulla tiivistetään merkittävät virheet ja kaatumiset. Näillä voi olla myös tietoturvaan kohdistuva yhteys. Nämä raportit antavat tärkeää ja arvokasta tietoa turvallisuusuhkista. Tähän lukeutuu kehittyneet uhat, joita tietoturvaan omistetut laitteetkaan eivät huomaa. Tällaisia laitteita ovat IDS- sekä IPS-järjestelmät. On hyvä keino tarkastella epätavalliset virheet, koska ne voivat olla merkki haittaohjelmasta, joka on päässyt organisaation ympäristöön ja aiheuttaa haittaa. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

2.9 Näkymät

SIEM-järjestelmässä näkymät ovat tärkeitä. Tässä yhteydessä näkymät tarkoittavat visuaalisesti esitettyä tietoa tapahtumista. Ne ovat kuin raportteja, mutta ne päivittyvät tietyn ajan välein ja muuttuvat parhaimmillaan reaaliajassa. Näkymät ovat tämän vuoksi hyödyllisiä. Raportin ja näkymän erona on siis se, että raportit ovat kuvaus tietystä ajan hetkestä, kun taas näkymä seuraa asioita jatkuvasti. (Sisense, 2018 Shelby Blitz, viitattu 26.9.2018.)
Tässä kappaleessa kerrottaan tarkemmin mitä näillä näkymillä voidaan ja kannattaa seurata.

2.9.1 Autentikointi

Näkymä kaikista epäonnistuneista ja onnistuneista kirjautumisista työaikojen aikana sekä niiden ulkopuolella, kuten viikonloppuisin. Nämä voivat koostua monista erilaisista näkymistä. Ne voidaan jakaa sen mukaan, mille laitteelle kirjautumiset ovat tapahtuneet. Lisäksi voidaan laskea yhdistelyn avulla epäonnistuneet kirjautumiset käyttäjäkohtaisesti ja erotella mihin järjestelmiin yritykset ovat suuntautuneet. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Kirjautumisyritykset käyttäjätileihin, jotka on otettu pois käytöstä ja oletus käyttäjätileihin. Tällaisiin käyttäjätileihin ei pitäisi tulla kirjautumisyrityksiä, eikä varsinkaan onnistuneita sellaisia. Onnistuneet sekä epäonnistuneet kirjautumiset näihin käyttäjätileihin täytyy tutkia tarkasti tietoturva asiantuntijoiden toimesta. (Sama lähde, kuin edellisessä kappaleessa.)

VPN-autentikoinnit ja etäyhteyksien onnistuneet ja epäonnistuneet kirjautumiset. Vaikka kaikki kirjautumiset ovat tärkeitä, niin näitä etäyhteyksien kirjautumisia tulee seurata tarkasti. (Sama lähde, kuin edellisissä kappaleissa.)

Kaikki käyttäjät, jotka kirjautuvat järjestelmänvalvojan tunnuksilla, koska järjestelmänvalvojilla on laajemmat oikeudet, kuin normaalikäyttäjillä. Näillä käyttäjätunnuksilla on mahdollista aiheuttaa vahinkoa. (Sama lähde, kuin edellisissä kappaleissa.)

Kannattavaa on seurata, jos käyttäjällä on monta epäonnistunutta kirjautumista ja sen jälkeen onnistunut. Tämä voi kertoa siitä, että käyttäjätiliin on päästy käsiksi väsytyshyökkäyksen tai arvatun

salasanan kautta. Tätä voidaan valvoa yhdistelyn avulla laittamalla ehdoksi tietyn määrän epäonnistuneita kirjautumisia ja sen jälkeen onnistunut kirjautuminen. (Sama lähde, kuin edellisissä kappaleissa.) Mielenkiintoisen lisän tähän saa myös, jos tarkastelee sitä, mistä maasta kyseiset yritykset ovat tulleet. Näin huomataan, jos tunnuksilla yritetään kirjautua maasta mistä ei pitäisi tulla kirjautumisyrityksiä. (Linkedin, 2018, SIEM use cases , Rajivarnan R, viitattu 1.10.2018.)

2.9.2 Muutokset

Näkymä, jossa kerrottaan muutoksista käyttäjätunnuksiin ja ryhmiin. Tähän lukeutuu lisäykset, muutokset ja poistot. Tämä on siksi tärkeä, koska hyökkääjän päästyään järjestelmin he yleensä lisäävät käyttäjän ja joskus poistavat sen, kun ovat ensin päässeet sisälle järjestelmiin. Tärkeintä on seurata sellaisia ryhmiä, jotka antavat laajoja oikeuksia järjestelmiin. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Salasanan muutokset käyttäjien toimesta ja järjestelmänvalvojien tekemät salasanan muutokset käyttäjille. Tämä näkymä on yhtä tärkeä, kuin uusien käyttäjätunnuksien luomisen seuranta. Tämän avulla seurataan sitä, että henkilöstö noudattaa organisaation tietoturvapolitiikkaa salasanan muutoksien osalta. (Sama lähde, kuin edellisessä kappaleessa.)

Palveluiden lisääminen ja poistaminen järjestelmistä. Varsinkin sellaisten palveluiden, jotka käyttävät tietoliikenneverkkoa, koska hyökkääjät usein kohdistavat hyökkäyksensä tällaisia palveluita vastaan. (Sama lähde, kuin edellisissä kappaleissa.)

Näkymä, joka kertoo, jos järjestelmälle tärkeitä tiedostoja on muutettu. Tällaisia ovat esimerkiksi verkkolaitteiden konfiguraatiotiedostot. Ei ole väliä onko muutos ollut vahinko, tahallinen vai suunniteltu. Kaikkia näitä täytyy seurata. Järjestelmät voivat käyttää myös muita tärkeitä tiedostoja toimiakseen. Myös näiden tiedostojen muutoksia on kannattavaa seurata. (Sama lähde, kuin edellisissä kappaleissa.)

Näkymä, joka kertoo muutoksista tiedostojen käyttöoikeuksiin. Tämä on tärkeä, koska käyttöoikeuksia muuttamalla tiedostoihin voidaan päästä huomaamatta käsiksi. Tällaiset luvattomat käyt-

töoikeuksien lisäämiset voivat johtaa tiedostojen varastamiseen. Suositeltavaa on seurata tiedostojen ja kansioiden käyttöoikeuksien muutoksia erillisillä näkymillä. (Sama lähde, kuin edellisissä kappaleissa.)

Sovelluksien latauksia ja päivityksiä tulisi seurata, jotta nähdään järjestelmiin asennetut sovellukset, joita ei ole lupa asentaa. Tätä voidaan seurata käyttäjän, järjestelmän tai sovelluksen tasolla. (Sama lähde, kuin edellisissä kappaleissa.) Windows maailmassa näiden seuranta on haastavampaa, koska Windows-käyttöjärjestelmässä luodaan lokitieto vain sovelluksista, jotka asennettaan Windows asennuspaketilla eli MSI-paketilla (Addictivetips, 2016, Fatima Wahab, viitattu 25.8.2018).

2.9.3 Tietoliikenne

Kaikkea liikennettä, joka suuntautuu sisäverkosta ulkoverkkoon ja demilitarisoidulta alueelta tulisi seurata. Tämän avulla voidaan huomata tunkeutumiset sekä mahdolliset haittaohjelmat. Lisäksi huomataan, jos on käyttäjiä, jotka väärinkäyttävät organisaation tietoliikenneverkkoa. Näitä kyseisiä asioita kannattaa seurata myös silloin, kun organisaatio on suljettuna. Erittäin tarkka näkymä saadaan, kun yhdistetään välityspalvelimen sekä palomuurin lokitietoja. Käyttämällä välityspalvelimen sekä palomuurin lokitietoja saadaan tarkempi kuva ajallisesti. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Isoimmat tiedostojen siirrot tai sessiot sen mukaan montako tavua on siirretty. Nämä molemmat näkymät auttavat selvittämään, jos epäillään tietoliikenneverkon väärinkäyttöä tai räikeää tiedon varastamista. (Sama lähde, kuin edellisessä kappaleessa.)

Kaikki lataukset ulkoverkosta tiedostopäätteen mukaan. Esimerkiksi voidaan listata exe tai dll tiedostojen lataamisia. On tärkeää seurata, millaisia tiedostoja saapuu ulkoverkosta sisäverkkoon. (Sama lähde, kuin edellisissä kappaleissa.)

Sisäisiä järjestelmiä sekä niiden portteja tulisi seurata. Ei ole luotettavaa keinoa tietää onko kyseessä haittaohjelma, mutta on epäilyttävää, jos sisäinen järjestelmä alkaa käyttämään yllättäen monia portteja keskustellakseen ulospäin. (Sama lähde, kuin edellisissä kappaleissa.)

Järjestelmät, jotka tuottavat suurimmat määrät erilaisia IDS, IPS ja WAF-hälytyksiä. Tällaiset näkymät ovat hyödyllisiä, koska ne kertovat järjestelmästä, josta tulee suuri määrä hälytyksiä. Tällöin tiedetään, että kyseisellä järjestelmällä ei ole kaikki hyvin. (Sama lähde, kuin edellisissä kappaleissa.)

VPN-yhteyden käytöstä kertova näkymä. Tähän tuodaan tietoa VPN-yhteydestä kuten käyttäjätunnus, sessiossa käytetty tavu määrä, laskettu sessioiden määrä ja sisäisten resurssien käyttö. Tätä seurataan siksi, että tarkastellaan VPN-yhteyden käyttöä ja tietoliikenteen poikkeavuuksia. (Sama lähde, kuin edellisissä kappaleissa.)

Näkymä, joka kertoo langattomien verkkojen käytöstä. Tässä seurataan käyttäjiä ketkä yhdistävät langattomaan verkkoon. Kannattaa myös seurata, jos ilmestyy, niin kutsuttu rogue access point. (Sama lähde, kuin edellisissä kappaleissa.)

Jotta tietoliikenneverkoista huomataan isompi kuva, täytyy seurata, kuinka paljon verkkolaitteilta tulee lokitietoja päivässä (Sama lähde, kuin edellisissä kappaleissa). Kannattavaa on luoda näkymä missä näkyy verkkolaitteilta tuleva tapahtumien määrä. Ne voidaan jakaa, niin että nähdään lokitietojen määrä laitetyypin mukaan. Kytkimet, reitittimet ja palomuurit voidaan jakaa eri näkymiin.

2.9.4 Resurssit

Kriittisten resurssien käyttöä tulisi seurata silloin, kun organisaatio on kiinni. Samalla tavalla, kuin kirjautumisia ja tietoliikenneverkon käyttöä seurataan. Näin voidaan seurata, jos on epäilyttävää resurssien käyttöä esimerkiksi yöllä. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.) Kriittisillä resursseilla tarkoitetaan esimerkiksi organisaatiolle tärkeitä tiedostoja ja niiden käyttöä.

Tulisi seurata sellaisia käyttäjiä, joilta on eniten evätty pääsyjä kielletyille sivustoille. Eväykset ovat voineet tulla välityspalvelimelta tai palomuurista. Tämän näkymän avulla voidaan seurata, jos järjestelmä on vaarantunut. Sen avulla on myös mahdollista parantaa tuottavuutta. (Sama lähde, kuin edellisessä kappaleessa).

Tiedostojen ja kansioiden käyttöä voidaan valvoa, kuten kuka on päässyt lukemaan tiedoston, kuka ei ole ja mahdolliset muutokset, joita tiedostoihin on tehty. Tämän seurannan avulla saadaan selville, milloin tiedosto on poistettu ja kenen toimesta. Kiristyshaittaohjelma voidaan havaita tämän näkymän avulla. (Netfort, 2015, Darrag Delaney, viitattu 29.9.2018).

Tietokantaan liittyvien näkymien seuranta on hyödyllistä, koska ne ovat kriittisiä järjestelmiä organisaatiolle. Kannattaa seurata käyttäjiä, joilla on tietokannan hallintajärjestelmään laajempia oikeuksia. Toinen käyttäjiin liittyvä seuranta on se, että seurataan ketkä käyttävät ahkerimmin tietokantaa. Tästä voidaan kuitenkin rajata pois tunnetut sovellukset. Kyselyiden seuranta on hyödyllistä, koska sen avulla saadaan näkyville mitä tietokannassa tapahtuu. Kannattaa seurata mitkä kyselyt ovat yleisimpiä, koska näiden näkymien avulla voidaan huomata epäsäännöllinen tapahtuma. Lisäksi kriittisiä kyselyitä kuten insert, delete, create ja grant kyselyitä kannattaa seurata, koska näillä kyselyillä on mahdollista saada vahinkoa aikaan tietokannassa. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Tiivistelmät tietokantojen varmuuskopioista. Tietokantojen varmuuskopiot siirtävät suuren määrän dataan toiseen paikkaan ja tätä voidaan pahimmillaan käyttää rikollisiin tarkoituksiin. Tämän avulla voidaan seurata mitkä varmuuskopioista ovat oikeita ja mitkä ovat luvattomia, jos sellaisia on. (Sama lähde, kuin edellisessä kappaleessa.)

Lista käyttäjätileistä, jotka lähettävät eniten liitteitä sähköpostilla. Tämän näkymän avulla voidaan huomata mahdollinen tietojen varastaminen. Jos tällainen tietojen varastaminen on tapahtunut, voidaan tämän näkymän avulla tutkia sitä. Tämän näkymän lisäksi voidaan tehdä näkymä, josta selviää lähetettyjen liitteiden tiedostopääte, tiedostokoko ja tiedostonimi. (Sama lähde, kuin edellisissä kappaleissa.)

Kaikki sisäiset järjestelmät, jotka lähettävät sähköpostia, pois lukien tiedettyihin sähköpostipalvelimiin. Näin huomataan, jos jokin järjestelmä on saastunut ja sitä kautta haittaohjelma lähettää roskapostia maailmalle. (Sama lähde, kuin edellisissä kappaleissa.)

Seurata lokitietojen pääsynvalvontaa sekä kuka niitä on käynyt lukemassa. Tämä on tärkeää, koska tietyt säännökset vaativat, että tätä seurataan (Sama lähde, kuin edellisissä kappaleissa).

2.9.5 Haittaohjelmat

Huomattujen haittaohjelmien trendit ja lopputulokset. Tämä on näkymä, jossa on tiivistelmä huomatuista haittaohjelmista. Lisäksi näkymässä pitäisi näkyä lopputulos siitä, onko haittaohjelma hoidettu tai jätetty hoitamatta. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Haittaohjelmien torjuntaohjelmiston huomatut tapahtumat, joille ei ole tehty mitään. Kaikki haittaohjelmien torjuntaohjelmistot kirjoittavat lokitietoja tapahtumista, joissa haittaohjelmalle ei ole tehty mitään. Tämän näkymän avulla on mahdollista huomata sellaiset haittaohjelmat joille ei ole tehty mitään ja ryhtyä tarvittaviin toimenpiteisiin, jotta haittaohjelma ei pääsisi tekemään tuhoja. (Sama lähde, kuin edellisessä kappaleessa.)

Kaikki haittaohjelmien torjuntaohjelmiston kaatumiset ja muut virheet. Nykypäivänä haittaohjelmat osaavat vastata haittaohjelmien torjuntaohjelmistoihin. Haittaohjelmat voivat olla syy siihen miksi torjuntaohjelmisto on kaatunut. (Sama lähde, kuin edellisissä kappaleissa.)

Sisäiset yhteydet tiedettyihin haitallisiin IP-osoitteisiin. Tämä näkymä toteutetaan vertaamalla palomuurin lokeja julkisiin listoihin, joissa on määritelty haitallisia IP-osoitteita. (Sama lähde, kuin edellisissä kappaleissa.)

Haittaohjelma tyypit, joita on löytynyt vähiten. Tämä antaa hyvää sisäpiiri tietoa epätavallisiin haittaohjelmiin. Tämä on tärkeä, koska haittaohjelmissa epätavalliset sellaiset voivat olla hyvin vahingoittavia organisaatiolle ja päästä läpi torjuntaohjelmistosta. (Sama lähde, kuin edellisissä kappaleissa.)

2.9.6 Kriittiset virheet

Järjestelmissä sekä sovelluksissa tapahtuneet kriittiset virheet. Näitä kannattaa seurata ainakin, jos virhe esiintyy ensimmäisen kerran, koska ne voivat olla ensimmäisiä viitteitä haittaohjelmista. Virheisiin kuuluu seurata järjestelmien ja sovelluksien kaatumiset, sammumiset ja uudelleen käynnistymiset. Jos järjestelmä tai sovellus kaatuu hyökkäyksen vuoksi, sillä on vaikutusta organisaation toimintaan. Näitä ei kannatta seurata pelkästään saatavuuden vuoksi, vaan sen lisäksi myös tietoturvan kannalta. (Chuvakin, Schmidt, Phillips, kappale 12, 2013.)

Epäonnistuneet varmuuskopiot ovat kriittisiä tapahtumia, jotka vaikuttavat organisaation jatkuvuuteen ja mahdollisesti myös määräykset vaativat niiden seurantaa. Lisäksi luvattomat varmuuskopioiden ajamiset voivat olla merkki siitä, että joku yrittää varastaa tietoa (Sama lähde, kuin edellisessä kappaleessa.)

Näkymät komponenttien tilasta kuten välimuistin, prosessorin sekä muistin käyttö. Tällaiset tapahtumat voivat kertoa mahdollisesta palvelunestohyökkäyksestä tai muista hyökkäyksistä järjestelmiä kohtaan. Järjestelmien resurssien käyttö on myös kriittistä organisaation kannalta, koska järjestelmät toimivat hitaasti, jos resurssien käyttö on maksimissa. (Sama lähde, kuin edellisissä kappaleissa.)

3 KÄYTTÖÖNOTTO

SIEM-järjestelmän käyttöönotto voidaan jakaa neljään eri vaiheeseen, jotka ovat: suunnittelu, testaus, kontrolloitu käyttöönotto ja jatkuvan kehityksen vaihe (Stackify, 2017, viitattu 30.9.2018).

3.1 Suunnitteluvaihe

Suunnitteluvaiheessa ensimmäinen ja tärkein asia on tarkastella omia tavoitteita, kuten mitä SIEM-järjestelmällä halutaan saavuttaa. Kannattaa tutkia tarkasti organisaation tietoturvapolitiikka ja miettiä mitkä seikat ovat tärkeitä organisaatiolle. Mitkä politiikat ovat sellaisia, jotka ovat määräyksien mukaisia ja mitkä ovat niin kutsuttuja parhaita käytäntöjä. (Stackify, 2017. viitattu 30.9.2018.)

Tässä vaiheessa kannattaa tunnistaa myös nykyiset valvontatoimet ja kuinka ne toimivat käytännössä. Ideaali tilanne olisi se, että toimenpiteet toimisivat politiikan mukaisesti, mutta valitettavasti näin ei usein ole ja SIEM-järjestelmän käyttöönotto tuo nämä puutteet ilmi. Nämä olisi hyvä laittaa kuntoon, jotta SIEM-järjestelmän hyödyt voidaan integroida jokapäiväiseen käyttöön ongelmitta. (Ingram Micro, viitattu 9.8.2018.)

Tunnista pieni joukko kohtia nykyisestä tietoturvapolitiikasta, joiden avuksi SIEM-järjestelmä voidaan ottaa käyttöön. Tunnista myös pieni joukko lokilähteitä, joista lokitietoja halutaan tuoda SIEM-järjestelmään (Sama lähde, kuin edellisessä kappaleessa).

3.2 Testausvaihe

Testausvaiheen tavoitteena on selvittää, mitä SIEM-järjestelmällä on mahdollista saavuttaa. Tässä vaiheessa testataan päästäänkö kyseisen järjestelmän avulla suunnitteluvaiheen tavoitteisiin. Näiden pohjalta perustellaan, miksi SIEM-järjestelmä on sijoittamisen arvoinen. (Stackify, 2017. viitattu 30.9.2018.)
Testausvaiheessa on myös tarkoitus kehittää toimintamalli SIEM-järjestelmästä, eli kuinka SIEM-järjestelmää voidaan käyttää päivittäisessä käytössä (Ingram Micro, viitattu 25.9.2018).

3.3 Hallittu käyttöönotto

Tässä vaiheessa SIEM-järjestelmään aletaan vähitellen tuomaan lisää lokitietoa erilaisista lähteistä. Tämän lisäksi tässä vaiheessa kehitetään käyttöönottotyötä ja järjestelmää testataan todellisessa tuotantoympäristössä. Kaikki prosessit, menettelyt ja toiminnot tulisi dokumentoida tässä vaiheessa tarkasti (Stackify, 2017. viitattu 30.9.2018.)

3.4 Jatkuvan kehityksen vaihe

Tämä vaihe ei SIEM-järjestelmän osalta lopu koskaan, koska sitä täytyy koko ajan kehittää. Uusia hyökkäyksiä kehitetään jatkuvasti ja SIEM-järjestelmän kanssa täytyy olla askeleen edellä hyökkääjiä. (Stackify, 2017. viitattu 30.9.2018.)

Ajan kanssa saa selville, miten ympäristö käyttäytyy ja sen tiedon avulla voidaan hienosäätää SIEM-järjestelmää. Järjestelmän avulla on myös hyvä kehittää organisaation tietoturvapolitiikkaa ja prosesseja. (Sama lähde, kuin edellisessä kappaleessa.)

3.5 Ohjeita käyttöönottoon

Paras tapa ottaa SIEM-järjestelmä käyttöön on edetä rauhallisesti askel askeleelta, koska silloin oppii paljon enemmän ympäristöstä ja pystyy hienosäätämään strategiaa matkan varrella. Kun etenee rauhallisesti, on helpompaa huomata mahdolliset käyttöönotossa tulleet virheet ja korjata ne (Stackify, 2017. viitattu 30.9.2018). Ei kannata kerätä sellaisia lokeja mistä ei ole hyötyä ja joita ei voi käyttää yhdistelyssä hyödyksi. Jos tällaisia kerää, niin ne vievät turhaan resursseja sekä haittaavat SIEM-järjestelmän käyttöä. (Tripwire, 2018, Tyler Wall, viitattu 16.8.2018.)

Tarkastellessa internetistä tulevaa liikennettä kannattaa käyttää hyödyksi IP-osoite mainelistauksia. Näiden avulla voidaan huomata, jos liikennettä tulee IP-osoitteista, jotka ovat huono maineisia. Tämä auttaa myös pitämään huolta omien IP-osoitteiden maineesta. (Stackify, 2017. viitattu 30.9.2018.)

Tutki mitkä laitteet ovat tärkeimpiä liiketoiminnan kannalta. Ota mahdollisimman paljon selvää näistä laitteista. Mitä portteja on auki, mitä palveluita niillä on käynnissä ja mitkä muut palvelimet kommunikoivat niiden kanssa. (Iansresearch, Raffy Marty, viitattu 10.8.2018.)

SIEM-järjestelmässä täytyy pitää huolta siitä, että lokitietoja saapuu kaikista kohteista, joista niitä kerätään (Sama lähde, kuin edellisessä kappaleessa).

Ennen, kuin aletaan tekemään yhdistelysääntöjä, niin täytyy määritellä säännöille logiikka. Esimerkiksi, jos seurataan monia lukittuja käyttäjätunnuksia, niin silloin täytyy määritellä, monennestako lukittautumisesta tulee hälytys. (Tripwire, 2018, Tyler Wall, viitattu 16.8.2018.)

Yleistä on, että sääntöjen kynnys on alussa liian matalalla. Ei siis kannatta säikähtää, jos uuden yhdistelysäännön kanssa tulee heti hälytyksiä, vaan kannattaa rauhallisesti seurata ja hieno säätä yhdistelysääntöjä. Yleensä yhdistelysääntöjä seurataan viikon verran ja niitä hienosäädetään samalla. Joissain SIEM-järjestelmissä löytyy mahdollisuus, että säännöt otetaan käyttöön, mutta ne eivät hälytä. Tämä auttaa siinä mielessä, että tällöin turhista yhdistetyistä tapahtumista ei tule hälytyksiä. Turhat hälytykset taas aiheuttavat sen, että SIEM-järjestelmää seuraava henkilöstö menettää motivaatiota turhien hälytyksien vuoksi (Sama lähde, kuin edellisessä kappaleessa.)

Yhdistelysääntöjä kannattaa seurata kvartaali perusteellisesti. Tällöin tarkastetaan, mistä yhdistelysäännöistä on ollut hyötyä ja mitkä eivät ole tuottaneet odotettua hyötyä. Tällöin sääntöjä mahdollisesti lisätään, poistetaan tai muokataan, jotta niistä saataisiin enemmän hyötyä (Sama lähde, kuin edellisissä kappaleissa.)

Tärkeä asia SIEM-järjestelmän käyttöönotossa on, että IT-ympäristön ja SIEM-järjestelmän kellonajat ovat synkronoituja, koska kellonaika on yksi kriittisimmistä tiedoista lokitiedoissa ja tapahtumissa. (Eventtracker, 2010, viitattu 21.9.2018.) Esimerkkinä siitä mitä väärä kellonaika voi tehdä on se, että yhdistely ei toimi, niin kuin pitäisi. Hälytystä ei tällöin tule välttämättä ollenkaan tai se tulee väärään aikaan. (McAfee, 2015, viitattu 21.9.2018.)

4 SOVELTUVUUSSELVITYS

Soveltuvuusselvityksessä on tarkoitus vertailla SIEM-järjestelmiä ja valita testiin sellainen, joka soveltuu parhaiten organisaation ympäristöön. Soveltuvuusselvityksessä tarkastellaan SIEM-järjestelmän käytettävyyttä ja soveltuvuutta organisaation IT-ympäristöön. Tärkeintä on kokeilla, pystyykö tällä SIEM-järjestelmällä toteuttamaan asioita, joita sillä halutaan tehdä. SIEM-järjestelmästä halutaan tehdä säilytyspaikka lokitiedoille ja parantaa tietoturvaa analysoimalla näitä tehokkaammin. Tärkeimmät lokitiedot ovat peräisin organisaation omista sovelluksista. Nämä sovellukset kirjoittavat lokitietojaan tietokantaan ja nämä pitäisi saada siirrettyä SIEM-järjestelmään. Tämän lisäksi näkyvyyttä halutaan lisätä tuomalla autentikointeihin liittyviä lokitietoja. Arvioitavat järjestelmät ovat ELK, Logpoint ja RSA.

4.1 Logpoint

Logpointin mukaan heidän järjestelmä on suunniteltu alusta asti niin, että se on yksinkertainen, joustava ja skaalautuva. Tätä tukevat heidän mukaansa virtaviivainen käyttöliittymä sekä käyttöönotto ja integraatio työkalut, joiden ansiosta SIEM-järjestelmä saataisiin monissa organisaatioissa tehokkaasti käyttöön. Nämä käytännössä tarkoittavat sitä, että arkkitehtuuria ja toiminnallisuuksia voidaan laajentaa jatkuvasti ilman, että julkaistaan uusi versio järjestelmästä (Logpoint, How it works 30.9.2018.)

Logpointin mukaan heidän järjestelmä jaetaan arkkitehtuurisesti kolmeen eri osaan. Nämä ovat Logpoint kerääjät, tausta ja haku. Nämä kyseiset toiminnot voidaan toimittaa samassa paketissa. Jos asiakas kuitenkin haluaa asentaa nämä kolme toimintoa eri palvelimille, niin sekin on mahdollista. Tämän vuoksi asiakkailla on joustavuutta sen suhteen, kuinka Logpointin SIEM-järjestelmä otetaan käyttöön. (Sama lähde, kuin edellisessä kappaleissa.)

Kerääjä vaiheessa lokiagentit sekä kerääjät toimivat yhteistyössä. Agentteja hallittaan Logpointin palvelimelta ja tämä helpottaa niiden hallintaa. Logpointissa agentit lähettävät salattuna lokitietoja eteenpäin kerääjille ja nämä kerääjät vastaavat lokitietojen normalisoinnista sekä tiedon rikastamisesta. Koska tiedon normalisointi tapahtuu kerääjällä, niin tämän ansiosta yhdistämisprosessi sekä

haku toimivat nopeammin. Normalisoinnin ja rikastamisprosessin jälkeen kerääjä lähettää tapahtumat SIEM-järjestelmään. (Sama lähde, kuin edellisissä kappaleissa.)

Kuten muissakin SIEM-järjestelmissä, niin myös Logpointissa on mahdollista kasvattaa lokilähteiden määrää liitännäisten avulla. Logpoint tukee asennus vaiheessa satoja järjestelmiä. Jos asiakkaalla on tarve saada jonkin sellaisen järjestelmän lokitiedot joita Logpoint ei tue, niin Logpoint tekee liitännäisen asiakkaan puolesta. Järjestelmän täytyy olla sellainen, että sen saa ostettua toimittajalta. (Sama lähde, kuin edellisissä kappaleissa.)

Logpoint käyttää tapahtumien ja alkuperäisten lokitietojen säilytykseen tietokantaa. Logpointin tietokanta on nosql pohjainen ratkaisu. Tämä NoSQL on hyödyllinen tällaisessa järjestelmässä, koska tietoja kertyy paljon ja nosql mahdollistaa nopeamman haun. Asiakas sitten itse jakaa tämän arkkitehtuurin kansioiden avulla. Tämä on hyödyllistä, koska kansioiden tasolla määritellään se, kuinka kauan mitäkin lokitietoja ja tapahtumia säilytetään. Kansioiden tasolla voidaan myös määrittää käyttöoikeuksia, kuten kuka voi tarkastella minkäkin kansion lokitietoja ja tapahtumia. (Sama lähde, kuin edellisissä kappaleissa.)

Haku on järjestelmän se osa, jonka avulla asiakas kehittää mukautettuja hakuja, jotka hakevat tietoja alkuperäisistä lokitiedoista tai normalisoiduista tapahtumista. Järjestelmän käyttäjä määrittää järjestelmässä raportit ja hälytykset käyttäen haku funktioita hyödyksi. Kaikki hakeminen tapahtuu käyttäen samoja arvo tunnisteita. Tämän ansiosta, jos uusi päivitys tulee, niin nykyiset toiminnot eivät lakkaa toimimasta. (Sama lähde, kuin edellisissä kappaleissa.)

Logpoint-järjestelmässä tapahtumat voivat laukaista hälytyksiä, mutta ne voidaan konfiguroida myös niin, että ne laukaisevat tapauksen. Tapaus Logpointissa tarkoittaa sitä, että tapaukselle määritellään riskiarvo ja sen jälkeen se voidaan kohdistaa tietylle henkilölle ratkaistavaksi. Käyttäjä kenelle tapaus on kohdistettu voi käyttöliittymän kautta siirtyä suoraan tapahtumaan. Kun tämä tapaus on selvitetty, henkilö voi kommentoida siihen ja sulkea tapauksen. (Sama lähde, kuin edellisissä kappaleissa.)

Logpoint-järjestelmässä tietoja voidaan myös sensuroida tietosuojatilassa. Jokainen alue, joissa on sellaisia tietoja, joiden avulla käyttäjä voidaan tunnistaa, voidaan salata. Jos henkilöllä on tarve nähdä tämä tieto, hän voi pyytää pääsyä siihen tietyksi ajaksi. Tietosuojatilassa käyttäjä voi käyttää kyselyitä normaalisti ja tarkastella raportteja. (Sama lähde, kuin edellisissä kappaleissa.)

Gartnerin käyttäjä arvosteluiden perusteella Logpoint-järjestelmällä on paljon hyviä ominaisuuksia, mutta myös kehitettävää. Käyttäjät ovat kehuneet Logpoint-järjestelmän käytettävyyttä, joustavuutta, hakujen tehokkuutta, asiakaspalvelua ja lisenssointia. Käytettävyyden positiiviset asiat tulevat yksinkertaisesta käyttöliittymästä ja siitä, että järjestelmä on helppo ottaa käyttöön. Joustavuutta kehutaan, koska lokitietoja voidaan tuoda monista lähteistä. Lokitietojen haku toimii nopeasti ja tämä on Logpoint-järjestelmän oman kyselykielen ansiota. Asiakaspalvelu on käyttäjien mielestä nopeaa ja he kuuntelevat asiakkaita heidän toiveista järjestelmään liittyen. Lisensointi Logpoint-järjestelmässä on sen mukaan, kuinka monta lokilähdettä on. Tämä on helppo lisensointimalli ja se helpottaa pitämään SIEM-järjestelmän kustannukset halutulla tasolla.

Käyttäjien mielestä Logpoint-järjestelmässä pitäisi kehittää dokumentaatio, joka koskee järjestelmän ominaisuuksia ja hallintaa. Tämän lisäksi käyttäjien mielestä yhdistelyä pitäisi kehittää tehokkaammaksi. Se ei käyttäjien mukaan ole sillä tasolla, kuin markkinajohtajien SIEM-järjestelmissä.

Gartnerin arvosteluissa Logpointin arvosana on 4,5/5. Arvosteluja on kirjoittamisen aikana 174 kappaletta (Gartner, viitattu 20.10.18).

Liite 1 on taulukko Logpointin vahvuuksista sekä heikkouksista

4.2 ELK

ELK eli Elastic stack. ELK on lyhenne sanoista Elasticsearch, Logstash ja Kibana. Nämä ovat erillisiä avoimen lähdekoodin projekteja, jotka sulautuvat tehokkaasti keskenään. (Elastic, ELK-stack, viitattu 19.9.2018.)

Elasticsearch on hajautettu restful ja JSON-pohjainen hakukone sekä analytiikkamoottori. Elasticin mukaan se integroituu ja skaalautuu hyvin sekä on helppokäyttöinen. Elasticsearch on nosql pohjainen tietokanta ratkaisu. Se käyttää tallennus paikkana JSON-pohjaisia tiedostoja, joista se hakee tietoja Apache Lucene hakumoottorin avulla. Nämä mahdollistavat sen, että tiedonhaku toimii todella nopeasti ja se etsii tapahtumia nopeammin, kuin monet muut SIEM-järjestelmät. (Elastic, Elasticsearch, viitattu 19.9.2018.)

Elasticin mukaan Logstash on palvelin puolen prosessointi putki, joka vastaa lokitiedon tuomisesta, suodatuksesta, normalisoinnista ja viemisestä. Lokitieto saapuu Logstash putkeen ja sieltä suodatuksen sekä normalisoinnin jälkeen tapahtuma menee Elasticsearchin tietokantaan. (Elastic, Logstash, viitattu 19.9.2018.)

Kibana vastaa Elasticsearchin tiedon visualisoinnista. Tämän avulla voidaan tehdä erilaisia diagrammeja ja analysoida niiden pohjalta lokitietoja (Elastic, Kibana, Viitattu 19.9.2018.). Tämä toimii samalla tavalla, kuin SIEM-järjestelmien näkymät. Kibanaan on mahdollista tuoda myös monitorointi tietoa kuten prosessorin ja keskusmuistin käyttöä.

ELK-pakettiin liittyy myös Beats. Se on lokiagentti, joka lähettää salattuna tietoja Logstashiin tai Elasticsearchiin. Beats-agentteja on monenlaisia. Esimerkiksi Auditbeat tuo auditointitietoa ja winlogbeat tuo Windowsin lokitietoja. (Elastic, Beats, viitattu 19.9.2018.) Tämä on siis sama asia, kuin aiemmin läpikäydyt lokiagentit.

Kokonaisuudessaan ELK toimii, niin että Beats-agentti lähettää lokitietoja Logstashiin. Logstash ottaa vastaan lokitiedot ja käsittelee ne. Logstash lähettää tämän jälkeen lokitiedot/tapahtumat Elasticsearchin tietokantaan. Kibana sitten käyttää Elasticsearchin hakua hyödyksi ja hakee tietoja sekä visualisoi ne. (Logz.io, 2018, Complete guide to elk-stack, Daniel Berman viitattu 19.9.2018.)

Organisaation näkökulmasta ELK-järjestelmän hyvä puoli on siinä, että se on avoimenlähdekoodin järjestelmä. Tämän vuoksi itse järjestelmä on periaatteessa ilmainen. Tässä on huonona puolena se, että ELK voi olla hyvin työläs ottaa käyttöön ja vaatii paljon henkilöstöresursseja ylläpitoon. Esimerkkinä tästä on se, että Logstashiin täytyy tehdä config-tiedostoja, joissa määritellään suodatus ja normalisointisääntöjä. Kun lokitietoja tuodaan monista järjestelmistä työmäärä kasvaa valtavasti. Jotta ELK-järjestelmä saadaan integroitua mahdollisimman laajasti organisaation järjestelmiin, se vaati ulkopuolista apua. Lisäksi pelkkä ELK-paketti ei riitä määrittelemään tätä järjestelmää SIEM-järjestelmäksi. ELK-järjestelmästä puuttuu monia ominaisuuksia, joita esimerkiksi kaupallisista järjestelmistä löytyy. Näitä puuttuvia ominaisuuksia ovat esimerkiksi raportit sekä hälytys toiminallisuudet. Hälytys ominaisuudet voidaan lisätä lisäosien avulla kuten Elasticin oman X-packin avulla, joka on kuitenkin maksullinen. Avoimen lähdekoodin lisäosia löytyy myös, jonka avulla järjestelmä saadaan hälyttämään. (Logz.io, 2018, Open source SIEM-tools, Daniel Berman, viitattu 20.9.2018.)

ELK-järjestelmän hyviä ominaisuuksia ovat ne, että tällä järjestelmällä voidaan suorittaa myös valvontaa, koska järjestelmään voidaan tuoda tietoja komponenttien käyttöasteista. Lisäksi järjestelmään voidaan tuoda periaatteessa mitä tahansa tietoa, koska se on joustava järjestelmä. REST API:n ansiosta tämä järjestelmä voidaan integroida hyvin ja jakaa sen avulla tietoja myös muille järjestelmille.

Käyttäjien mielestä yhdistely toimii tässä SIEM-järjestelmässä heikommin, kuin muissa SIEM-järjestelmissä. Lisäksi mielipiteissä nousi esille se, että ELK on työläs ottaa käyttöön ja vaatii ulkopuolista konsultaatio apua.

ELK-järjestelmän arvosana Gartnerin käyttäjien arvosteluissa on 4,3/5 ja arvosteluja on kirjoittamisen aikana 75 kappaletta (Gartner, ELK-stack, viitattu 20.10.18).

Liite 2 on taulukko ELK-stackin vahvuuksista ja heikkouksista.

4.3 RSA

RSA:n SIEM-järjestelmä on tehokas ja se on tarkoitettu suurille organisaatioille. Tämä SIEM-järjestelmä on modulaarinen ja se onkin jaettu erilaisiin paketteihin. Lokitietojen käsittely ja tietoliikenneverkon seuranta kuuluu ensimmäiseen pakettiin. Lisäksi siihen saa toisen paketin, joka mahdollistaa palvelinten seurannan. Lisensointi menee tässä SIEM-järjestelmässä eri portaiden avulla. Ensimmäinen porras pitää sisällään 50GB käsiteltyä lokitietoa päivässä sekä 1 teratavu päivässä käsiteltyjä tietoliikennepaketteja.

Gartnerin käyttäjä arvostelujen mukaan tämän SIEM-järjestelmän vahvuudet ovat tietoliikenteen seuranta ja tehokkaat SIEM ominaisuudet kuten yhdistäminen. Lisäksi lokitietojen arkistointi toimii tässä SIEM-järjestelmässä hyvin, koska vanhat lokitiedot voidaan arkistoida erilleen aktiivisista lokitiedoista. RSA:ssa on myös monipuoliset UEBA-ominaisuudet.

Heikkouksia käyttäjien mielestä ovat huono käyttöliittymä ja muutenkin monimutkainen järjestelmä käyttää päivittäin. Normalisointi pakettien tekeminen esimerkiksi omille sovelluksille on arvostelujen mukaan todella haastavaa.

Tämän järjestelmän arvosana Gartnerin arvosteluissa on 4,2/5. Arvosteluja on 63 kappaletta kirjoittamisen ajankohtana (Gartner, RSA, viitattu 20.10.18).

Liite 3 on taulukko RSA:n vahvuuksista sekä heikkouksista.

4.4 Järjestelmän valinta

Logpoint valittiin siksi, koska se integroituu hyvin ja se tukee valmiiksi järjestelmiä, joita organisaatiossa on käytössä. Merkittävä tekijä valinnassa oli myös Logpoint-järjestelmän selkeä lisensointimalli. Heillä lisensointi menee lokilähteiden määrän mukaan. Yleensä muilla SIEM-järjestelmillä lisensointi määräytyy sen mukaan, kuinka monta lokitietoa tulee tietyssä ajassa. Useimmiten se on lokitietoja sekunnissa eli EPS-lisensointimalli. Tällainen EPS-lisensointimalli on huono, koska helposti voi käydä niin, että lokitietojen keräämisessä aletaan säästämään. Toinen huono asia on, että helposti saattaa tulla yllätyksiä maksuissa, jos lokitietoja on tullut odotettua enemmän. Tällaisella selkeällä lisensointimallilla kuten Logpoint-järjestelmällä tiedetään tarkkaan kustannukset ilman yllätyksiä. Logpoint on hinnaltaan edullisempi heidän lisensoinnin ansioista. Yksi ominaisuus oli myös, joka nousi Logpoint-järjestelmästä esille. Logpoint-järjestelmään on tulossa tulevaisuudessa UEBA-ominaisuudet, joka tarkoittaa sitä, että järjestelmä käyttää koneoppimista hyödyksi. Se pystyy oppimaan, kuinka käyttäjät käyttäytyvät normaalisti. Jos joku käyttäjä käyttäytyy normaalista poikkeavalla tavalla, niin UEBA ilmoittaa tästä. (Logpoint, UEBA-solution, viitattu 9.9.2018). SIEM ja UEBA-järjestelmät ovat yhdessä tehokas kombinaatio.

Logpoint-järjestelmän edustajien kanssa keskusteltaessa tuli ilmi myös tärkeä ominaisuus. Logpoint-järjestelmällä voi tehdä itse normalisointisääntöjä. Tämä mahdollistaa sen, että lokitietoa voi tuoda monenlaisista järjestelmistä, vaikka Logpoint-järjestelmässä ei olisi valmiina normalisointipakettia.

4.5 SIEM-järjestelmän soveltuvuus

Logpoint-järjestelmän soveltuvuutta testattiin organisaation tuotantoympäristössä. Tarkoituksena oli ensin kokeilla järjestelmää tuomalla lokitietoja sellaisista lähteistä, joille on jo valmiiksi normalisointisäännöt. Ensimmäisenä kokeillaan Windows palvelimella, jossa ei ollut monia palveluita. Lokiagentin asennuksen jälkeen järjestelmä konfiguroitiin vastaanottamaan lokitietoja. Järjestelmään

täytyi konfiguroida lokitietojen säilytykseen liittyvät asiat ja valita oikea normalisointisääntö. Tämän vaiheen jälkeen lisättiin laite, jolta lokitiedot tulevat ja lokiagentti konfiguroitiin tätä kautta etänä SIEM-järjestelmästä käsin. Huomion arvoisimmat asetukset, joita lokiagenttiin konfiguroitiin, olivat lokiagentin sekä Logpoint-järjestelmän välisen tietoliikenteen salaaminen. Toinen asetus liittyi lokitietojen toimitukseen. Jos lokitietojen toimitus ei onnistuisi jostain syystä, niin lokiagentti osaa tallentaa nämä tiettyyn hakemistoon ja lähettää ne, kun se on mahdollista. Lokiagentissa voidaan myös suodattaa sitä, millaisia lokitietoja lähetetään. SIEM-järjestelmään tuodaan testin vuoksi kaikki mahdolliset lokitiedot. Konfiguroinnin jälkeen tarkistetaan, että lokitiedot tulevat SIEM-järjestelmään. Tapahtumia saapui SIEM-järjestelmään tasaiseen tahtiin.

Seuraavassa vaiheessa asennetaan lokiagentti sellaiselle palvelimelle, joka on tärkeä organisaation ja tietoturvan näkökulmasta. Tältä palvelimelta saadaan sellaisia lokitietoja, joilla saadaan merkityksellisiä näkymiä SIEM-järjestelmään. Tämä kyseinen palvelin, jolta lokitietoja tuodaan, on Active Directory palvelin ja sieltä saadaan autentikointitietoja. Active Directorylle tehdään oma kansio SIEM-järjestelmään, vaikka sen olisi voinut yhdistää valmiiksi olevaan Windows-kansioon. Tämä tehtiin siksi, koska tämän ansiosta Active Directorystä tulevia lokitietoja voidaan analysoida mahdollisimman tehokkaasti. Toistetaan siis ensimmäisen kappaleen kohdat konfiguroinnin osalta. Konfiguroinnin jälkeen voitiin huomata, että lokitietoja tulee paljon Active Directorystä. Tämän ansiosta voitiin tehdä näkymiä, joista olisi apua organisaatiolle.

Autentikointi osiosta tehtiin kaikki sellaiset kohdat, jotka voidaan toteuttaa Active Directoryn avulla. Ensimmäiseksi tehtiin näkymä onnistuneista kirjautumisista. Tässä oli kuitenkin sellainen ongelma, että Windows kirjoittaa lokitietoja kirjautumisista niin, että kirjautumistapahtuma tulee aina, kun käyttäjä yhdistää ja avaa jaetun verkkokansion. Tämän vuoksi käyttäjän tapahtumia tuli kymmeniä yhtä kirjautumista kohti. Tämä näkymä jätettiin, mutta se ei ole hyvä analysoinnin kannalta. Tähän liittyen tehtiin vielä näkymä, joka kertoo epäonnistuneista kirjautumisista. Tämä näkymä toimi oikein, koska siitä tuli yksi tapahtuma jokaista epäonnistunutta kirjautumista kohti. Tästä tapahtumasta tehtiin yhdistelyn avulla vielä sellainen näkymä, joka näyttää tapahtumat, joissa salasana on laitettu kolme kertaa väärin ja tämän jälkeen tulee onnistunut kirjautuminen.

Käyttäjiin liittyen tehtiin vielä sellaisia näkymiä kuten lukitut käyttäjätilit, avatut käyttäjätilit, käytöstä pois otettujen käyttäjätilien kirjautumiset ja näkymä, joka seuraa järjestelmänvalvojien kirjautumisia. Lukittujen ja avattujen käyttäjätilien näkymät ovat samanlaisia. Molemmat on toteutettu ympyrädiagrammin avulla, koska silloin voidaan helposti vertailla niitä ja katsoa, onko jokin käyttäjätili

avattu. Käytöstä pois otettujen käyttäjien kirjautumisyritykset toivat esille mielenkiintoisia asioita. Selvisi esimerkiksi, että eräs skripti oli käynnissä eräällä palvelimella turhaan. Tämän lisäksi oli monia kirjautumisyrityksiä tileihin, jotka oli otettu pois käytöstä. Näille kirjautumisille ei löytynyt selitystä. Järjestelmänvalvojien kirjautumisia valvova näkymä toimi kuten pitääkin ja tämä toteutettiin käyttäen sankey-diagrammia. Sen avulla tällaisia tapahtumia on helppo seurata, koska sankey-diagrammin avulla voidaan hyvin seurata tapahtumien suhteita. Katso liite 4

Autentikointien lisäksi tehtiin sivu muutoksista. Tällä sivulla ovat näkymät käyttöoikeuksien lisäyksistä sekä poistoista. Tämän ansiosta jää jälki kaikista oikeuksien lisäämisistä, jotka tehdään Active Directory ryhmien kautta ja nähdään, kuka oikeudet on lisännyt tai poistanut. Tilastojen osalta tehtiin näkymä, joka näyttää suosituimmat ryhmät. Tämän avulla saadaan tilastoja siitä mitä käyttöoikeuksia käyttäjät tarvitsevat eniten ja osataan käyttää tätä tilastoa hyödyksi esimerkiksi käyttäjätilien luomisessa. Muutokset sivulla on näkymä lisätyistä sekä poistetuista käyttäjistä ja näiden avulla nähdään, jos tulee epäilyttäviä käyttäjälisäyksiä tai poistoja. Tästä on myös se hyöty, että käyttäjäluonneista ja poistoista jää jälki. Viimeinen näkymä tällä sivulla näyttää, jos käyttäjätili on otettu pois käytöstä tai aktivoitu uudestaan sekä kuka tämän on tehnyt. Katso liite 5

Näiden näkymien jälkeen kokeillaan, että soveltuuko tämä SIEM-järjestelmä organisaation näkökulmasta tärkeimpään asiaan eli lokitietojen hakuun tietokannasta. Tässä SIEM-järjestelmässä on tuki ODBC-yhteydelle, jonka avulla lokitietoja voidaan hakea tietokannasta.

Ensin SIEM-järjestelmään konfiguroidaan oma säilytyspaikka tietokannasta tuleville lokitiedoille. Tämän jälkeen lisättiin tietokanta palvelin laite listaan ja konfiguroidaan ODBC-yhteys SIEM-järjestelmästä. Tämän jälkeen tarkistetaan, että lokitiedot saapuvat järjestelmään. Lokitiedot tulivat SIEM-järjestelmään, mutta ongelmaa oli siinä, että näitä ei ole normalisoitu ja näin ollen näkymien teko on mahdotonta ja analysointi erittäin haastavaa. Tässä SIEM-järjestelmässä voidaan tehdä itse normalisointisääntöjä. Normalisointisääntö tehdään ja se otetaan käyttöön ODBC-yhteydellä tuleviin lokitietoihin. Tarkastelemalla lokitietoja huomataan, että normalisointi toimii kuten pitääkin ja tuloksista voidaan muodostaa näkymiä. Tapahtumille tehtiin kuitenkin vielä yksi asia, jonka avulla lokitiedoista saadaan selvempiä. Lokitietoja rikastettiin toisen tietokanta taulun tiedoilla, jotta tapahtumille saatiin nimet. Tämän ansiosta oli helpompi analysoida näitä tapahtumia.

Lopuksi tehtiin vielä kaksi näkymää etusivulle. Ensimmäisessä näkyvät lokitietojen määrä yhteensä viikon aikana, joita on tullut SIEM-järjestelmään. Toisessa näkymässä on sama ajatus, mutta siinä on eroteltu eri palvelimilta tulevat lokitiedot. Katso liite 6

Näiden kokeilujen pohjalta Logpoint toimi odotusten mukaisesti ja ylitti odotukset esimerkiksi järjestelmän selkeyden osalta. Merkittävin asia tässä SIEM-järjestelmässä on se, että normalisointisääntöjä voi tehdä helposti itse. Näin ollen tähän SIEM-järjestelmään voidaan tuoda lokitietoa todella monipuolisesti eri lähteistä ja se integroituu hyvin organisaation ympäristöön.

Gartnerissa esiintyvät palautteet ovat sellaisia, jotka pitävät paikkansa. Lokitietojen yhdistelyä pitäisi kehittää tehokkaammaksi. Dokumentointi on kehittynyt, sillä tämän uusimman version dokumentaatio oli selkeää ja vertailtuani vanhoihin dokumentteihin, niin tämän osalta kehitystä on tapahtunut. Dokumentaatiota voisi kuitenkin vielä kehittää kertomalla syvällisemmin esimerkiksi hausta ja hakukielen syntaksista. Huomasin myös, että näkymien sijoittelua pitäisi kehittää. Sijoittelu tuntui hyvin rajatulta.

SIEM-järjestelmän merkittävyyttä ei voi yli korostaa, sillä sen avulla saatiin paljon näkyvyyttä organisaation ympäristöstä, vaikka tämä kokeilu oli lyhyt ja sen avulla toteutettiin vain vähän mahdollisia seurattavia asioita. Tällä kyseisellä SIEM-järjestelmällä voidaan seurata monia muitakin järjestelmiä, joita organisaatiolla on käytössä. Mahdollisuuksia on paljon sen osalta, kuinka voidaan kehittää organisaation tietoturvaa SIEM-järjestelmän kanssa.

Voidaan todeta, että tämän kokeilun tavoite täyttyi, koska lokitietoja saatiin tuotua tietokannasta ja niistä saatiin muodostettua järkeviä näkymiä. Tämän lisäksi näkyvyys nousi ympäristössä autentikoinneista sekä muutoksista kertovien näkymien ansiosta. Logpoint soveltuisi organisaation käyttöön tämän kokeilun perusteella. Varsinkin, jos SIEM-järjestelmä halutaan ottaa käyttöön organisaatiossa ilman ulkopuolista apua.

5 POHDINTA

Opinnäytetyö tuntui aluksi vaikealta, koska aihe oli minulle uusi ja en ollut aiemmin kuullut SIEM-järjestelmistä. Aloitettuani etsimään tietoa ja materiaalia huomasin, että ihmiset olivat suositelleet Chuvahkinin kirjaa. Ostettuani tämän kirjan ja luettuani sen, aloin ymmärtämään paremmin SIEM-järjestelmistä sekä lokitietojen hallinnasta. Luettuani kirjan päätin kirjoittaa SIEM-järjestelmien prosessit auki, koska henkilöt, joille SIEM-järjestelmät ovat uusia ymmärtäisivät näiden järjestelmien toiminnasta. Lisäksi itselläni ymmärrys kasvoi, kun kirjoitin prosessit opinnäytetyöhön.

Organisaation näkökulmasta katsottuna kiinnostavia asioita olivat SIEM-järjestelmän käyttöönotto ja käyttökohteet. Halusin kertoa nämä teoria osuudessa, jotta ymmärrys kasvaisi sen osalta, kuinka tällaista järjestelmää kannattaisi ottaa käyttöön ja mitä sillä voisi käytännössä tehdä.

Opinnäytetyössäni piti vertailla kolmea SIEM-järjestelmää, mutta vertailu oli haastavaa, koska en itse voinut kokeilla näitä kolmea SIEM-järjestelmää, vaan minun piti etsiä ihmisten mielipiteitä näistä järjestelmistä. SIEM-järjestelmistä arvosteluita oli niukasti saatavilla. Järjestelmäntoimittajilta mielipidettä olisi voinut kysyä, mutta se tieto olisi ollut puolueellista ja siksi en vertaillut niiden perusteella. Kerroin arvostelu osiossa, kuinka järjestelmäntoimittajat kuvailevat heidän SIEM-järjestelmää ja sen lisäksi katsoin Gartnerista käyttäjien arvosteluita. Gartnerin mukaan he seuraavat arvosteluita ja varmistavat kirjoittajat oikeiksi. Kerroin soveltuvuusselvityksen lopussa vielä siitä, että oliko kokemukseni samanlainen, kuin Gartnerin käyttäjillä ja osuiko järjestelmätoimittajan kuvaus oikeaan.

Valittuani Logpointin soveltuvuusselvitykseen aloitin järjestelmän asentamisen ja konfiguraation. Logpointtia käyttäessä huomasin, että SIEM-järjestelmien prosessien kirjoittaminen tähän opinnäytetyöhön auttoi paljon. Ymmärsin SIEM-järjestelmän eri toiminnallisuuksia hyvin. Lisäksi käyttökohteiden tutkiminen auttoi, koska tiesin, mitä asioita voidaan seurata SIEM-järjestelmällä, jotta näkyvyyttä saadaan lisättyä. Järjestelmän käyttö sujui jouhevasti ja olin tyytyväinen järjestelmään. Mielipiteeni varmistui siitä, että Logpoint on oikea järjestelmä organisaatiolle, koska tärkein tavoite eli tietokannasta lokitietojen haku toimi hyvin.

Opinnäytetyössä opin paljon asioita SIEM-järjestelmistä sekä lokitiedoista. Lisäksi tutustuin järjestelmiin, joista lokitietoja haettiin. Koen, että ymmärrykseni kasvoi merkittävästi tämän opinnäytetyön myötä.

Jouduin opinnäytetyössäni rajaamaan kuvia ja jättämään osan niistä kokonaan pois, koska niissä olisi näkynyt kriittisiä tietoja. Lisäksi alun perin olisin laittanut opinnäytetyöhöni tarkan dokumentaation SIEM-järjestelmän asennuksesta ja konfiguroinnista, mutta sopimustekniset asiat eivät salli näiden laittamista.

6 LÄHTEET

Addictivetips, 2016. Fatima Wahab. viitattu 25.8.2018, https://www.addictivetips.com/windows-tips/how-to-tell-which-user-installed-or-removed-an-app-in-windows/

Advisera, 2015. Antonio Segovia. viitattu 18.11.2018, https://advisera.com/27001academy/blog/2015/11/23/logging-and-monitoring-according-to-iso-27001-a-12-4/

Alienvault, 2018. Kim Crawley. viitattu 31.7.2018, https://www.alienvault.com/blogs/security-essentials/how-siem-correlation-rules-work

Auvik, 2014. Rod Lewis. viitattu 25.9.2018, https://www.auvik.com/media/blog/centralized-logging-checklist/

Comparitech, 2018. Tim Keary. viitattu 5.9.2018, https://www.comparitech.com/net-admin/siem-tools/#gref

Csonline, 2017, Is antivirus getting worse. Maria Korolov, viitattu 22.8.2018, https://www.csoonline.com/article/3159073/computers/is-antivirus-getting-worse.html

Csonline, 2017. Mary K. Pratt. viitattu 29.9.2018, https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

Dooley, Brown, 2017. viitattu 1.10.2018, Cisco IOS Cookbook 2nd edition

Elastic, Beats, viitattu 19.9.2018, https://www.elastic.co/products/beats

Elastic, Elasticsearch. viitattu 19.9.2018, https://www.elastic.co/products/elasticsearch

Elastic, Kibana, Viitattu 19.9.2018, https://www.elastic.co/products/kibana

Elastic, Logstash, viitattu 19.9.2018, https://www.elastic.co/products/logstash

Elastic. ELK-stack. viitattu 19.9.2018, https://www.elastic.co/elk-stack

Eventsentry, 2017. Ingmar Koecher. viitattu 30.9.2018, https://www.event-sentry.com/blog/2017/03/agent-vs-agentless-why-you-should-monitor-event-logs-with-an-agent-based-log-monitoring-solution.html

Eventtracker 2010. viitattu 21.9.2018, https://www.eventtracker.com/tech-articles/5-cyber-security-myths-the-importance-of-time-synchronization/

Gartner, ELK-stack, viitattu 20.10.18, https://www.gartner.com/reviews/market/security-information-event-management/vendor/elasticsearch/?pid=8643

Gartner, Logpoint. viitattu 20.10.2018, https://www.gartner.com/reviews/market/security-information-event-management/vendor/logpoint/?pid=27392

Gartner, RSA. viitattu 20.10.18, https://www.gartner.com/reviews/market/security-information-event-management/vendor/dell-technologies-rsa/product/rsa-security-analytics?pid=14628%7C14628

Iansresearch, Raffy Marty, viitattu 10.8.2018, https://www.iansresearch.com/insights/reports/best-practices-for-managing-a-siem

Ingram Micro. viitattu 9.8.2018, http://www.ingrammicroadvisor.com/security/a-step-by-step-guide-to-a-successful-siem-deployment

IPwithease, 2015. viitattu 30.9.2018, https://ipwithease.com/snmp-vs-syslog/

Kajaanin ammattikorkeakoulu, viitattu 30.9.2018, https://www.kamk.fi/oppiminen/Oppimisen-tyokalupakki/Kirjoittamisen-tyokalut/Asiakirjoittaminen/Raportti

Linkedin, 2018. SIEM use cases, Rajivarnan R. viitattu 1.10.2018, https://www.linkedin.com/pulse/siem-use-cases-rajivarnan-r

Logging and log management (Chuvakin, Schmidt, Phillips, 2013)

Logpoint, Agentless, WMI-Less Collection of Endpoint Logs, 2015. Christian Have, viitattu 4.8.18, https://www.logpoint.com/en/blog/agentless-wmi-less-collection-of-endpoint-logs/

Logpoint, How it works, Logpoint 30.9.2018, https://www.logpoint.com/en/product/how-it-works/

Logpoint, UEBA-solution. viitattu 9.9.2018, https://www.logpoint.com/en/product/ueba-solution/

Logz.io, 2018, Open source SIEM-tools. Daniel Berman, viitattu 20.9.2018, https://logz.io/blog/open-source-siem-tools/

Logz.io, 2018. Complete guide elk-stack. Daniel Berman. viitattu 19.9.2018, https://logz.io/learn/complete-guide-elk-stack/#intro

Manageengine, 2018. Nivathi Bhat, viitattu 7.9.2018, https://blogs.manageengine.com/it-security/eventloganalyzer/2018/04/24/connecting-logs-event-correlation.html

McAfee, 2014. viitattu 2.8.18, https://community.mcafee.com/t5/Documents/McAfee-SIEM-FAQ/ta-p/550598

McAfee, 2015. viitattu 21.9.2018, https://kc.mcafee.com/corporate/index?page=content&id=KB85600&actp=null&viewlocale=en_US&locale=en_US

Netfort, 2015. Darrag Delaney. viitattu 29.9.2018, https://www.netfort.com/blog/auditing-file-access-on-file-servers/

Pratum, Colton Bachman, 2016. viitattu 9.9.2018, https://pratum.com/blog/313-how-does-siem-work

PRnewswire, 2017. viitattu 30.9.2018, https://www.prnewswire.com/news-releases/security-information-and-event-management-market-2014-2022-key-players-are-dell-hp-ibm-logrhythm-mcafee-solarwinds-splunk-symantec-trend-micro--trustwave-holdings-300499766.html

Scnsoft, 2017. Dmitry Nikolaenya. viitattu 31.7.2018, https://www.scnsoft.com/blog/what-can-go-wrong-with-siem-correlation-rules

Searchdatacenter, 2018. Jessica Lulka. viitattu 18.8.2018, https://searchdatacenter.techtarget.com/feature/14-SIEM-reports-and-alerts-to-boost-security

Securosis, 2010. Adrian Lane, viitattu 30.7.2018, https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen

Sisense, 2018. Shelby Blitz. viitattu 26.9.2018, https://www.sisense.com/blog/dashboards-vs-reports-need/

Stackify, 2017. viitattu 30.9.2018, https://stackify.com/siem-implementation-strategy-and-plan/

Techopedia, viitattu 5.9.2018. https://www.techopedia.com/definition/3455/windows-management-instrumentation-wmi

Tripwire, 2018. Tyler Wall. viitattu 16.8.2018, https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/siem-implementation-strategies/

Viestintävirasto 2016, Petri Vesamäki, viitattu 3.7.2018, https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603151527.html

7 LIITTEET

Vahvuudet	Heikkoudet
▪ Selkeä käyttöliittymä ▪ Hyvä tiedon visualisointi ▪ Lokitietojen hakeminen tehokasta ▪ Laajat muokkaus mahdollisuudet ▪ Tiedon rikastaminen ▪ Euroopassa kehitetty järjestelmä ▪ Lisenssointimalli ▪ Hinta/laatusuhde ▪ Kehuttu asiakaspalvelu	▪ Korrelointi rajattua ▪ Korrelointi hidasta ▪ Näkymien sijoittelu haastavaa ▪ Dokumentaatio voisi olla parempaa

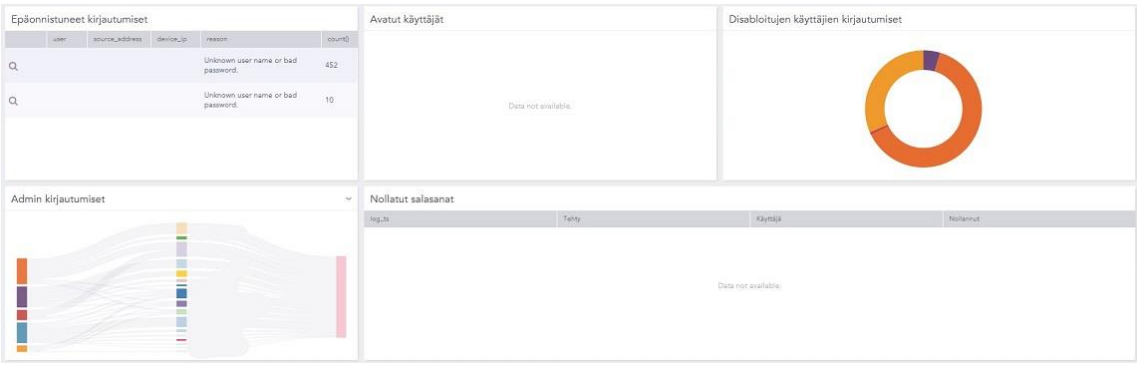
Liite 1 Logpoint vahvuudet/heikkoudet

Vahvuudet	Heikkoudet
▪ Avoin lähdekoodi ▪ Laajasti muokattava ▪ Nopea lokitietojen haku ▪ Samassa infrastruktuurin valvonta ▪ Periaatteessa tietoa voi tuoda mistä vain ▪ Euroopassa kehitetty järjestelmä ▪ REST API	▪ Työläs ottaa käyttöön ▪ Vaatii ulkopuolista apua ▪ Alkuperäisestä ELK-paketista puuttuu toiminnallisuuksia ▪ Mukautettujen normalisointien teko haastavaa

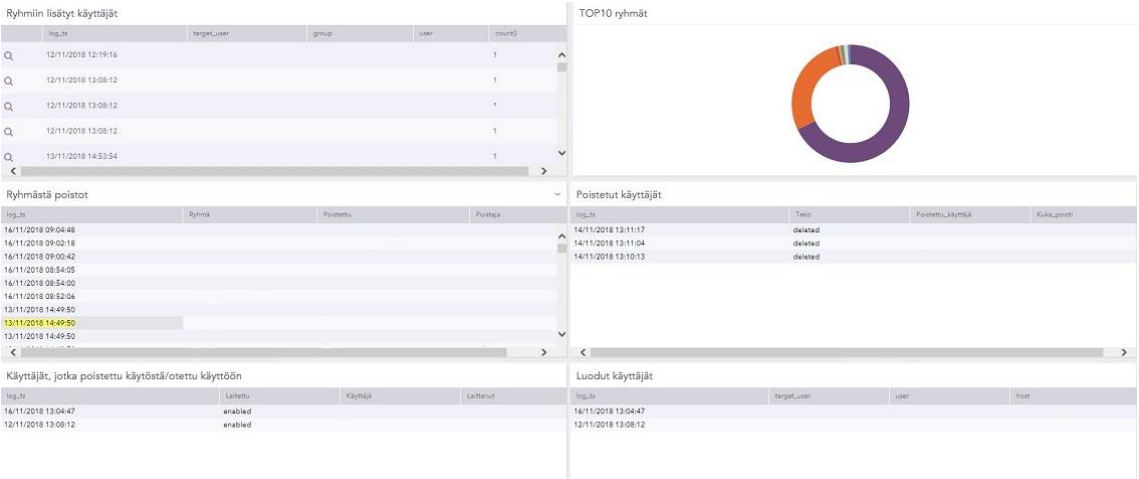
Liite 2 ELK vahvuudet/heikkoudet

Vahvuudet	Heikkoudet
▪ Hyvä tietoliikenteen seuranta ▪ UEBA ▪ Arkistointi ▪ Tehokas korrelointi ▪ Soveltuu suuriin lokitieto määriin	▪ Huono käyttöliittymä ▪ Monimutkainen käyttää ▪ Vaatii ulkopuolista apua käyttöönotossa ▪ Mukautettujen normalisointien tekeminen haastavaa ▪ Lisensointimalli perustuu lokitietojen määrään

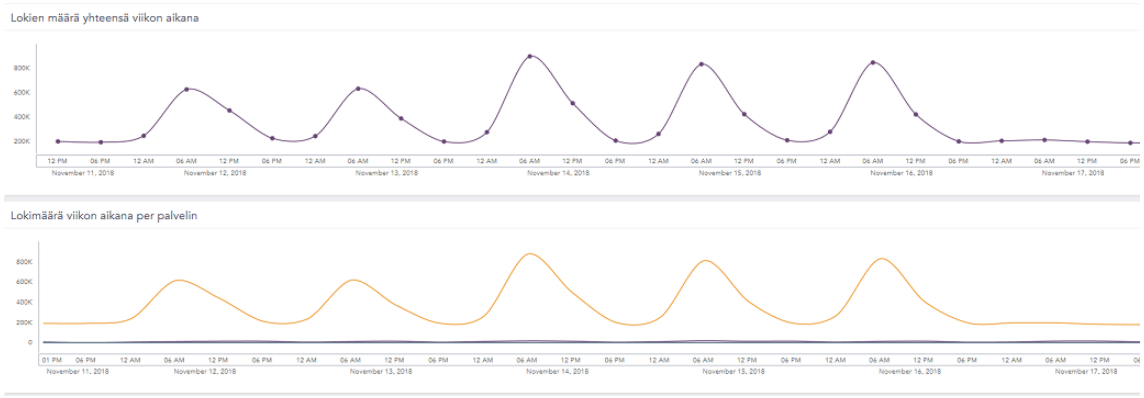
Liite 3 RSA vahvuudet/heikkoudet



Liite 4 autentikoinnit



Liite 5 muutokset



Liite 6 lokitietojen määrä