Jani Hirsmäki

# Lokinhallintatyökalun evaluointi

Insinööri (AMK)
Tieto- ja viestintätekniikka
Kevät 2022

## Tiivistelmä

**Tekijä(t)**: Hirsmäki Jani

**Työn nimi:** Lokienhallintatyökalun evaluointi

**Tutkintonimike:** Insinööri (AMK), tieto- ja viestintätekniikka

**Asiasanat:** Lokinhallinta, SIEM, tietoturva

Tämän opinnäytetyön tavoitteena on selvittää, kuinka järjestelmien ylläpitoa toteuttavaan yritykseen evaluoidaan keskitetty lokienhallintatyökalu ja millä toimenpiteillä hankintaprosessi voidaan toteuttaa onnistuneesti. Opinnäytetyöprosessi aloitettiin alkukeväästä 2021 ja sitä jatkettiin vuoden 2021 syksyyn asti. Toimeksiantajana opinnäytetyölle toimi Herman IT Oy, joka tarjoaa asiakkaille mm. konesali- ja pilvipalveluita, IT-asiantuntijapalveluita sekä resursseja sovelluskehityksen ja ohjelmoinnin tehtäviin.

Evaluointiprosessissa selvitettiin, mitä lokienhallintaa toteuttavia järjestelmiä markkinoilta löytyy ja miten yrityksen teknisiin vaatimuksiin ja tarpeisiin löydetään soveltuva lokityökalu. Aineiston osalta turvauduttiin muihin vastaaviin projekteihin ja lokityökalujen valmistajien verkkosivuilta löytyvään informaatioon.

Testauksen avulla selvitettiin, kuinka lokitietoja saadaan kerättyä analysoitavaksi lokijärjestelmälle ja kuinka sillä saadaan toteutettua sille tyypillisiä tietoturvaominaisuuksia, kuten raportointi ja tietoturvailmoitukset. Evaluoinnin tuloksena saatiin kartoitettua yrityksen tarpeet lokijärjestelmältä ja projektista tuotettua aineistoa pystytään käyttämään jatkossa pohjana vastaavissa hankkeissa.

Lopullista päätöstä työkalun hankkimisesta ei päättötyön toiminnallisen suorituksen aikana saatu muodostettua, mutta ominaisuuksiltaan käyttökelpoisimmaksi todettu FortiSIEM-työkalu jäi toiseen vaiheeseen jatkotestattavaksi organisaation tuotantoympäristöön.

KAMK • University of Applied Sciences

## Abstract

**Author(s):** Hirsmäki Jani

**Title of the Publication:** Evaluation of a Log Management Tool

**Degree Title:** Bachelor of Engineering, Information and Communication Technology

**Keywords:** Log management, SIEM, security

The aim of this Bachelor's thesis is to determine how a centralized log management tool is evaluated for a company that maintains systems and what measures can be taken to successfully implement the procurement process. The thesis process started in the early spring of 2021 and continued until the autumn of 2021. The thesis was commissioned by Herman IT Oy, which offers customers e.g. data center and cloud services, IT expert services, and resources for application development and programming tasks.

In the evaluation process, it was found out which systems implementing log management can be found on the market and how a log tool suitable for the company's technical requirements and needs can be found. For the material, recourse was made to other similar projects and to the information found on the log tool manufacturers' websites.

The testing was used to find out how log data can be collected for analysis by the log system and how it can implement its typical security features, such as reporting and security notifications. As a result of the evaluation, the company's needs were mapped from the log system, and the material produced from the project can be used as a basis for similar projects in the future.

The final decision to acquire the tool could not be formed during the functional execution of the thesis, but the FortiSIEM tool, which was found to have the most useful features, remained in the second phase for further testing in the organization's production environment.

Sisällys

ASIASANASTO

Lokipolitiikka

Tietoturvapoliittinen liite, jossa otetaan kantaa organisaation lokien käsittelyyn liittyvissä asioissa.

Aggregointi

Yhdistetään samankaltaiset kirjaukset koherentiksi tietojoukoksi.

Korrelointi

Etsitään samoista tai eri lokikirjauksista yhteneväisyyksiä, joista voidaan hahmottaa uutta tietoa.

Normalisointi

Lokitietojen muuttaminen eri sisällöistä ja formaateista yhtenäiseen luettavaan muotoon.

Rotaatio

Lokitietojen sijoittaminen säilytykseen ilman, että tietoa päällekirjoitetaan.

Multitenantti

Ratkaisu jossa toisen asiakkaan ohjelmiston tiedot eivät näy muille asiakkaille eikä käyttö vaikuta muihin asiakkaisiin.

EPS

Kuinka monta tapahtumaa jokin järjestelmä tuottaa sekunnin aikana.

Indeksointi

Lokien lajittelumenetelmä, jossa lokit järjestellään avaimina.

Virtualisointi

Ohjelmien erotteleminen tietokoneen fyysisestä kerroksesta, että koneella voidaan ajaa useampia virtuaalikoneita.

On-premise

Paikallisesti yrityksen sisäisesti, eikä pilvessä toimiva ohjelmisto.

# 1 Johdanto

Tässä työssä perehdytään lokitiedon käsittelyn taustoihin ja kartoitetaan vaadittavat toimenpiteet edistyksellisen lokienhallinnan toteuttamiselle konesalipalveluita tarjoavalle yritykselle sekä valitaan markkinoilla olevista kaupallisista lokienhallintajärjestelmistä yksi tuote kokeiluun. Valittua työkalua testataan muutamien toimintojen osalta sekä tutkitaan, kuinka työkalulla voi toteuttaa tietoturvaan keskittynyttä lokinhallintaa.

Opinnäytetyö on jaettu kuuteen pääosaan: ensimmäisessä osassa selvitetään, mitä loki on ja tarkastellaan toimia liittyen sen keräämiseen ja käsittelyyn, toisessa osassa tutustutaan erilaisiin lokinhallintatyökalutyyppeihin, kolmannessa osassa tutkitaan tietoturvallisen lokinkäsittelyn eri skenaarioita, neljännessä osassa selvitetään, mitä ominaisuuksia lokityökalulta halutaan toimeksiantajayrityksessä ja valitaan testattavaksi sopiva työkalu, viidennessä osassa tehdään valitun työkalun pystytys ja kuudennessa osassa kokeillaan joitakin toimintoja testauksen kohteeksi valitulta työkalulta.

Työ on tehty toimeksiantona Herman IT Oy:lle ja aihe valikoitui työharjoittelujakson aikana keväällä 2021. Työ toteutettiin osana organisaation projektia, jossa varsinainen evaluointi lokijärjestelmälle toteutettaisiin. Lokijärjestelmää lähdettiin evaluoimaan yrityksen tarpeesta keskittää lokinkeräys ja automatisoida tietoturvatapahtumien käsittely lokinhallintatyökalun avulla. Kiinnostavaa aiheessa oli lokinhallintatyökalujen toimintaperiaatteisiin perehtyminen ja lokinkäsittelyn tutkiminen ilmiönä.

# 2 Loki

Loki on tallenne, joka koostuu kirjauksista, tietojärjestelmien muutoksista ja muista laitteiden sisäisistä tapahtumista. Pääsääntöisesti kaikki laitteet ja ohjelmistot maailmassa synnyttävät lokitietoa toimintansa aikana. Lokitieto pyritään luokittelemaan sen luonteesta riippuen ja se voi olla esimerkiksi käyttölokia, tapahtumalokia, viestintälokia tai virhelokia. [1.]

Lokeja on tietotekniikan historiassa käytetty alunperin vikadiagnostiikan tukemisessa, mutta niiden käyttö on laajentunut myöhemmin mm. järjestelmien ja verkkojen suorituskyvyn optimointiin, laitteiden käyttäjien tekemien toimenpiteiden seurantaan ja tiedon keräykseen tietoturvatapahtumien selvittämiseksi. Lokit ovat tätä nykyä myös kehittyneet sisältämään informaatiota enemmän eri järjestelmätapahtumista. Usein yrityksten laitteiden tallentamat lokikirjaukset liittyvät tietoturvatapahtumiin, kuten pääsylokeihin, jotka kirjaavat käyttäjien autentikaatioyritykset sekä järjestelmän turvallisuuslokeihin, jotka kirjaavat mahdolliset hyökkäystapahtumat.

Lokin hallinnan tarpeen on synnyttänyt räjähdysmäinen tietojärjestelmien, verkko- ja muiden laitteiden määrällinen kasvu ja niihin kohdistuvat tietoturvauhat. Myös lokien suuret volyymit ja monimuotoisuudet ovat vaikuttaneet lokinhallinnan tarpeen kasvuun. Lokikirjausten lukemiseen suurissa it-ympäristöissä ja useampien lähdelaitteiden kokonaisuuksissa on suotavaa valjastaa käyttöön hallintajärjestelmä lokitiedoille, jotta jokaista lokia tuottavaa järjestelmää ei tarvitse seurata erikseen. Tätä kutsutaan keskitetyksi lokinhallintajärjestelmäksi.

Lokinhallintaa toteuttavan yrityksen on viisasta huomioida jokaisen mahdollisen lokitiedon lähteen painoarvon toteuttaessaan ja suunnitellessaan lokinhallintaratkaisua. Suurin osa lokilähteistä, esimerkiksi palvelimet työskentelevät kellon ympäri, joten ne luovat aina uutta lokitietoa jatkuvasti. Jotkut laitteet ovat kuitenkin käytössä vain tilapäisesti, joten ne luovat merkintöjä erissä usein säännöllisin väliajoin. Käsiteltävän lokin määrä kannattaakin arvioida etenkin järjestelmän laajuutta skaalatessa. [2.]

Lokienhallinnalla tarkoitetaan siis lokidatan generointia, siirtoa, tallennusta, analysointia ja arkistointia. Lokitietoa tarvitaan, jotta voidaan selvittää lähdelaitteelta mitä, miksi ja milloin jotakin on tapahtunut. Loki kattaa lisäksi myös kaikki tapahtumat ja muutokset tietojärjestelmissä ja siitä vastuussa olevan henkilön on päätettävä, mitä tietoa kirjataan, miten kerätyt tiedot kuljetetaan, mihin ne tallennetaan ja kuinka pitkäksi aikaa. [1.]

## 2.1 Lokitiedon keräys, käsittely ja analysointi

Lokienhallintaan räätälöidyt työkalut mahdollistavat lokitietona kerättyjen tapahtumien ja niiden yksityiskohtien poimimisen siten, että ainoastaan asiaankuuluva tieto voidaan raportoida suoraan lokienhallitsijalle analysoitavaksi. On kuitenkin huomioitava, että lokiin tallentuva tiedon tyyppi on tunnistettavissa ja tarpeellisia tietoja kerätään riittävästi lokitiedon analysoinnin mahdollistamiseksi. Lokit käsitellään analysoimalla automatisoidusti tai manuaalisesti. Lisäksi lokinkäsittely tulee tehdä optimoidusti, että resursseja ei tuhlata turhan tiedon keräämisessä ja analysoinnissa.

Lokien analysoinnin avulla päästään tunnistamaan uhkaavat tietoturvatapaukset, käytäntörikkomukset, mahdollinen vilpillinen toiminta sekä järjestelmän sisäiset ongelmat. Suuremmassa mittakaavassa lokienhallinta mahdollistaa operationaalisten trendien tunnistamisen sekä tukee ongelmien analysointia pitkällä kantamalla. [3.]

Lokihallinta käsittää myös tietosuojan, tiedon yhtenäisyyden ja lokien saatavuuden. Keskitetyn lokienhallintajärjestelmän ansiosta lokihallitsija kykenee tekemään tehokkaita analyysejä lokidatasta ja nopeuttamaan toimia vianselvitystilanteissa. Lokitietojen säilömisen osalta oleellisia tekijöitä ovat tiedon todennettavuus ja eheys, jonka vuoksi lokit tulevat olla luettavissa lokijärjestelmästä muuttumattomina, kuten alkuperäinen järjestelmä on ne kirjannut. [1.]

## 2.2 Lokinkäsittelyn kustannukset

Lokinkeräykseen, tallentamiseen ja analysointiin suunnatut työkalut tai järjestelmät ovat yrityksille perusteltuja investointeja siinä missä muutkin rahallista panostusta vaativat hankkeet, ja ne tulisi ottaa käyttöön kustannustehokkaasti ja vaatimukset täyttäen. Kustannustehokkuutta voi edistää pyrkimällä määrittelemään järjestelmän toiminta etukäteen, mutta lokien analysoinnin ja käytön tulisi noudattaa samaa linjaa lokien keräämistarkoituksen kanssa.

Lokijärjestelmän kustannuksista vain osa kertyy itse työkalun ominaisuuksien toteuttamisesta, ja kuluja kertyy yleisemmin järjestelmän käytönaikaisista kustannuksista ja henkilöstökuluista. Vaikka kehittyneet lokijärjestelmät ovat pitkälle automatisoituja, ihminen silti tekee viime kädessä lopullisen tulkinnan koneen käsittelemästä lokista.

Lokianalysoinnilla voidaan kuitenkin mahdollistaa kustannuksellisia säästöjä esimerkiksi monitoroimalla tietojärjestelmän käyttökapasiteettia tai optimoimalla kuluja aiheuttavia järjestelmäresursseja. Nämä toimenpiteet mahdollistavat kapasiteetin mitoittamisen riittävän kokoiseksi ja auttavat ennakoimaan kuormituksellisten pullonkaulojen syntymisen. [3.]

## 2.3 Lokinhallinan haasteet

Lokihallinnassa haastava tekijä on usein lokilähteiden suuri määrä, epäjärjestelmällinen lokisisältö, formaatti, epäyhtenäiset aikaleimat lokilähteiden kesken sekä lokidatan suuret volyymit. IT-ympäristössä lokeja syntyy useista lähteistä ja yksittäinen lähdelaite, järjestelmä tai palvelu voi kerätä usean tyyppistä lokitietoa, kuten autentikaatio- ja verkkotapahtumia eri lokitiedostoihin ja vaihtelevassa formaatissa. Jokainen lähdelaite tallettaa lokitietoonsa IP-osoitteita ja käyttäjätunnuksia ja laitteet ovat tämän avulla tunnistettavissa.

Lokien analysoinnin helpottamiseksi organisaatioiden täytyy kuitenkin usein ottaa käyttöön automaattisia menettelytapoja lokitietojen kääntämiseksi eri sisällöistä ja formaateista tiedon muuttamiseksi yhtenäiseen standardiin. Vaikeuksia yleensä kuitenkin ilmenee, kun yritetään yhdistää talletetut lokitiedot eri lähteistä, jotka käyttävät erilaista formaattia, jossa tietyt järjestelmät kerävät saman tiedon eri muodossa. Esimerkiksi aikaleima voi olla MM–DD–YYYY tai MMDDYYYY. Toisena esimerkkinä file transfer protocol voi tallentua yhtenä lokina ("FTP") ja toisessa lokissa portin numerona "(21)". Tämä vaikeuttaa yhtenäisen lokin ylläpitoa, kun järjestelmässä on useita eri lokilähteitä. Useimmiten jokainen lokilähde tallettaa tietoja järjestelmän kaikista toiminnoista, täytyy lokijärjestelmän kerätä vain tärkeimmät ja oleellisimmat tiedot lokien hallitsijalle, tehokkuuden vuoksi. [1.]

## 2.4 Lokijärjestelmän hankinnan vaiheet

Kun aloitetaan hankkimaan keskitettyä lokienhallintajärjestelmää, tulisi ensimmäisessä vaiheessa kartoittaa yrityksen nykyinen lokienkäsittelyn tila ja selvittää vaatimukset lokienhallinnan toteuttamiselle. Alkuvaiheessa tulisi myös selvittää, mihin yritys lokienhallintaa tarvitsee ja mistä lähtötilanteesta prosessia lähdetään toteuttamaan. Esiselvityksessä on kyettävä tekemään listaus ongelmista, joihin ratkaisu voidaan saada lokienhallinnan avulla. Sunnittelemalla prosessin etenemismalli voidaan selvittää, kuinka haluttuihin tavoitteisiin päästään. [3.]

Lokijärjestelmän hankinnalle tulee asettaa lähtökohdaksi organisaation varsinaiset tarpeet ja järjestelmä kannattaa valita tarvekartoitukseen perustuen. Myös suunnitteluun ja järjestelmän määrittelyyn kannattaa panostaa, koska aiemman vaiheen satsaukset voivat näkyä lokijärjestelmän käyttöönottovaiheessa. Alkuvaiheen toteutus tulee kuitenkin rajata tarkasti, jotta päästään mahdollisimman onnistuneeseen lopputulokseen. Huolellisen pohjatyön ansiosta voi jatkossa laajentaa ratkaisua mahdollisesti muihinkin käyttökohteisiin. [4.]

Jos yrityksessä ei olla valjastettu käyttöön aikaisemmin keskitettyä lokienhallintajärjestelmää, on tärkeää muodostaa järjestelmään liitettäville laitteille lähtötilanne, jotta voidaan selvittää, mikä on kunkin laitteen normaalitila. Jos yrityksessä on toteutettu aikaisemmin lokinkäsittelyä, saattaa siellä olla jo aikaisemmin määritelty lokipolitiikka. Puuttellinen tai vanhentunut lokipoliitiikka tulee päivittää, sillä se määrittelee yleisellä tasolla kaikki lokien käsittelyyn ja säilytykseen liittyvät asiat. Jotta lokienhallintajärjestelmän hankintaprosessia voidaan helpottaa, täytyy organisaation tehdä perusteellinen ja ajan tasalla oleva tietoliikenteen arkkitehtuuridokumentaatio. Arkkitehtuuridokumentaation puuttuminen vaikeuttaa lokienhallintajärjestelmän pystyttämistä, sillä lokia tuottavat laitteet eivät välttämättä ole kartoitettuna järjestelmästä ja verkkojen välisestä liikennöinnistä ei aina saada haluttua kokonaiskuvaa.

Lokijärjestelmän budjetoinnissa tulee ottaa huomioon, kuinka paljon kustannuksia järjestelmän ylläpitämisestä syntyy sekä kuinka paljon siihen varataan henkilöresursseja. Ylläpitämisessä kustannuksia syntyy lokijärjestelmän sovellusten ja mahdollisten oheislaitteiden päivittämisestä. Lokijärjestelmän päivitykset koostuvat usein uusista ominaisuuksista sekä toimintojen muutoksista ja näiden käyttöön ottaminen tarvitsee toimenpiteitä henkilöstöltä. Usein lokijärjestelmästä hankittuun maksulliseen lisenssiin kuuluu tekninen tuki ja se kannattaa huomioida järjestelmän vikatilanteita ratkoessa budjetin säästämiseksi. [3.]

# 3 Lokinhallintatyökalutyyppejä

Tietoturvamarkkinoiden kehityksen myötä markkinoille on syntynyt laaja valikoima eri tietoturvaohjelmistoja. Lokinkeräykseen suunnatut ohjelmistot jaetaan usein lyhenteisiin SIM, SEM, SIEM ja näiden määritelmät ovat usein herättänyt hämmennystä sekä vaikeuttanut määrittää työkaluille vaatimuksia.

SEM (Security event management) mahdollistaa tietoturvatapahtumien seurannan ja hallinnan reaaliajassa, sekä se sisältää sille ominaisia toimintoja, kuten reaaliakaisen tapahtumien ja tietojen aggregoinnin ja korreloinnin lokikeräyksen yhteydessä. Lokitapahtumien hallinta ja tarkastelu onnistuvat ohjauspaneelista ja automaattiset hälytykset ovat määriteltävissä tietoturvatapahtumille.

SIMin eli security information managementin avulla päästään puolestaan tarkkailemaan historiallisia analyyseja ja raportteja tietoturvatapahtumista. Nämä toiminnot vaativat runsaasti kerättyä dataa ja sen korrelointia, jota ei kuitenkaan voi tehdä reaaliajassa vaan tapahtumien ajallisessa kontekstissa. Korreloinnin avulla lokitietojen välille voidaan luoda suhteita, joilla lokitapahtumista voidaan löytää yhteisiä ominaispiirteitä ja täten karsia epäoleellista tietoa. SIM-tyyppiset työkalut usein sisältävät joustavia kysely- ja raportointiominaisuuksia indeksoiduista lokiarkistosta.

Yhteisiksi ominaisuuksiksi SIMin ja SEMin välille voidaan luetella mm. työnkulku, resurssien painotus ja raportointi. Kun yhdistetään molemmat työkalutyypit, niin saadaan security information and event management eli SIEM. Tämä toteuttaa molempien työkalutyyppien välisen keskitetyn, kattavan ratkaisun. SIEM-työkalun tärkeimmiksi ominaisuudeksi voidaan luokitella tietoturvatapahtumien analysointi ja järjestelmähaavoittuvuuksien jäljittäminen. SIEM kykenee lisäksi suodattamaan suuria lokimääriä ja näin ollen vastaustoimintojen hallintaan ja priorisointiin tarvitaan vähemmän työtä. Lisäksi SIEM toteuttaa joustavia analyysejä, jotka mahdollistavat totuudenmukaisia kyselytuloksia ja näkymiä, jotka ovat tarpeellisia tietoturvatutkimusten suorittamisessa.

Usein lokienhallintajärjestelmät luonnehtivat itseään SIEM-tyyppiseksi, vaikka todellisuudessa ne ovat kuuluneet joko SEM tai SIM-kategorian alle. Tästä syystä tuotteen arvioimiseksi on kerättävä käsitys siitä, millaiselta SIEM-toteutus näyttää todellisuudessa. [5.]

# 4 SIEMin käyttöskenaariot

Lokienhallinta ja SIEM voidaan jakaa kolmeen eri käyttötapaus päätyyppiin ja niistä ensimmäinen on ”etsivä ja tutkiva tietoturva”. Tässä käyttötapauksessa keskitytään hyökkäyksiin, haittaohjelmiin, tietovarkauksiin ja muihin turvallisuustapahtumiin. Skenaariota, jossa hyödynnetään SIEM:iä vastaavassa käyttötapauksessa, kutsutaan SOC:iksi eli security operations centeriksi. Tavanomaisesti SIEMillä toteutetaan SOC:issa reaaliaikaisia yleiskatsauksia ja tapahtumien korrelaatiota ja tietoturva-analyysin suorittajan on oltava tällöin käytettävissä kellon ympäri tekemässä tietoturvan hallintaa.

Toinen käyttötapaustyyppi on nimeltään ”globaali sääntely- ja paikallisten käytäntöjen vaatimuksenmukaisuus”. Tämä käyttötapaus keskittyy erilaisten lakien, mandaattien, kehysten sekä paikallisen yrityspolitiikan vaatimusten toteuttamiseen. Mini-SOC:iksikin kutsuttavassa skenaariossa tietoturvaa toteuttavat henkilöt tarkkailevat SIEM:in luomia hälytyksiä ja raportteja reaaliajattomasti. Aikariippumattomuudesta johtuen työajan ulkopuolella tapahtuneisiin tietoturvatapauksiin päästään usein vastaamaan vasta seuraavana päivänä.

Kolmatta käyttötapausta kutsutaan ”käyttö-, järjestelmä- ja verkkovianmääritys ja normaali toiminta” -nimellä. Tähän skenaarioon lukeutuvat yritykset, jotka konfiguroivat SIEM:insä tekemään lokianalysointiin pohjautuvia ilmoituksia ja raportteja, mutta tietoturvahenkilö ei koskaan seuraa tapahtumia reaaliajassa vaan pyrkii suorittamaan pelkästään pakolliset toimenpiteet. Näihin tyypillisesti kuuluuvat raporttien tarkastelu ja tietoturvahälytyksiin reagoiminen. Tämä käyttötapaus on pienempien yritysten suosiossa ja kutsutaan nimellä ”Automated SOC”.

Näistä kaikista yleisimpänä SIEM-asiakkaana pidetään automated SOCia toteuttavia yrityksiä. Automated SOCissa lokin käsittelijät usein keskittyvät raportoinnin avulla toteuttamaan määräysten mukaista ylläpidon hallintaa, jossa ei välttämättä ole aina tietoturvafokusta. [6.] Toimeksiantajayrityksen voisi mahdollisesti sijoittaa tähän viimeisenä mainittuun kategoriaan, sillä siellä lokien hallinta pyrittäisiin tekemään mahdollisimman automatisoidusti, että se ei vaatisi paljoa henkilöstön työtä.

# 5 Vaatimusmäärittely ja evaluointi

Vaatimusmäärittelyn avulla voidaan määritellä, millainen hankkeen kohteena olevan järjestelmän tulisi olla ja mitä ominaisuuksia siltä halutaan. Vaatimusmäärittely on merkityksellinen järjestelmän teknisen ominaisuuksien kannalta ja vaikuttaa suuresti järjestelmähankkeen onnistumiseen ja menestykselliseen lopputulokseen. Ohjelmiston vaatimusmäärittelyn taustalla ovat usein ne tahot, joihin järjestelmä vaikuttaa. [7.]

## 5.1 Herman IT:n vaatimukset lokijärjestelmälle

Ennen kun työn toimeksiantajaorganisaatiossa haluttiin räätälöidä evaluoitaville lokijärjestelmille vaatimusmäärittely, kerättiin ennakkoon mahdollisimman paljon arkipäiväisiä teknisiä vaatimuksia. Alustavaan listaukseen kirjattiin useita toimintoja, joihin lukeutuu esimerkiksi lokitietojen lähetys ja vastaanotto ilman tiedon peukaloinnin mahdollisuutta. Haluttiin myös, että lokin lähettäjä- ja vastaanottajalaite tunnistaisi toisensa jollain mekanismilla ja ne hylkäisivät muualta kuin hyväksytyiltä vastaanottajilta tulevat kirjaukset. Lokitieto haluttiin pitää mahdollisimman muuttumattomana, jotta lokijärjestelmässä olevia lokitietoja ei voitaisi muokata tai poistaa ennenaikaisesti. Etenkin tietoturvallisen lokitiedon käsittelyn edellyttämiseksi kaiken datan haluttiin olevan luettavissa yhtenäisessä formaatissa ja vain luku -oikeuksilla. Lokitiedossa täytyi olla lisäksi eri tasoiset lukuoikeudet ja ennakkoon erilaisille lokikirjauksille määriteltävissä olevat säilytysajat.

Yrityksen eri järjestelmät tuottavat omat lokikirjauksensa erilaisin teknisin ratkaisuin ja siksi lokijärjestelmän toivottiin mahdollisimman vähin ylläpitotoimin ja asennuksin kyetä vastaanottamaan lähettäjä sekä tunnistamaan tiedon eheys säilyttäen lokikirjaukset käytössä olevista järjestelmistä. Lokitiedon analysointia ajallisessa kontekstissa toteuttavan lokijärjestelmän haluttiin kykenevän synkronoitumaan samaan aikalähteeseen kuin lokia tuottavien järjestelmien. Lokijärjestelmän toivottiin olevan kevyesti ylläpidettävä ja sen käyttöönotto tulisi onnistua nopeasti. Järjestelmältä toivottiin lisäksi helppokäyttöisyyttä ja analysoinnin tehokkuutta. Tarpeellisena vaatimuksena pidettiin myös sitä, että järjestelmän ohjelmistoa kehitettiin aktiivisesti ja siihen oli mahdollista saada riittävästi teknistä tukea. Yrityksellä ei ollut tarkkaa lukumäärää siitä, kuinka paljon kaikista laitteista lokia syntyy kokonaisuudessan, joten järjestelmän haluttiin skaalautuvan tarvittaessa riittävästi yrityksen lokinkeräystarpeisiin ja järjestelmän täytyisi olla organisaation omassa ympäristössä toteutettava on-premise -ratkaisu.

## 5.2 Tarvekartoituksen ja vaatimusmäärittelyn kirjaaminen

Tarvekartoituksen avulla saatiin selkeytettyä, kuinka lokienhallintaa voitaisiin organisaatiossa toteuttaa lokinkäsittelyyn suunnatulla ohjelmistolla. Tämän jälkeen tehtiin kysely ja haastateltiin organisaation sisäisiä lokitietojen parissa työskenteleviä työntekijöitä, eli lokijärjestelmän sidosryhmää. Kyselyn ja haastattelujen tuloksista saatiin kerättyä lista kohdekäyttäjien tarpeista sekä halutuista ominaisuuksista.

Lokienhallinnan nykytila määriteltiin seuraavasti: koska yrityksessä ei oltu hyödynnetty keskitettyä lokienhallintajärjestelmää laajamittaisessa käytössä, jouduttiin kaikki lokitieto kaivamaan laitekohtaisesti ja tämä oli hankaloittanut että hidastanut vianselvitystilanteita. Lokitietoja yrityksessä haluttiin kerätä tuotantoalueen eri järjestelmstä eli verkkolaitteista, palvelimista, sovelluksista ja virtualisoiduista käyttöjärjestelmistä. Koko lokinhallintajärjestelmäprojektin keskinäiseksi tavoitteeksi työkalulle asetettiin se, että sen täytyy helpottaa palvelimienhallintatyöprosesseja ja sillä tulisi saada edistyksellisempi kokonaiskuva yrityksen järjestelmien tilasta. Myöhemmin tarkemmaksi vaatimukseksi muodostui tietoturvatapahtumien analysointi, joka käytännössä karsi pois kaikki tuotteet, jotka eivät olleet SIEMejä.

Kyselyn ja tarvekartoituksen pohjalta pystyttiin nyt kokoamaan vaadittavat ominaisuudet vaatimusmäärittelyyn ja halutuille ominaisuuksille voitiin määritellä tärkeysprioriteetit. Prioriteetit jaettiin kolmeen eri tasoon ja niiden avulla voitiin pisteyttää työkalut, jotka toteuttivat parhaiten haluttuja ominaisuuksia.

### 5.3 Mahdollisia lokiyökaluja

Vertailuun koottiin lista saatavilla olevista lokityökaluista ja tarkoituksena oli ottaa vertailuun mukaan kymmenen lokityökalua, joista tultaisiin vertailemaan ominaisuudet ja valittaisiin parhaiten pisteytyksessä suoriutuneet myöhempään kokeiluvaiheeseen. Markkinoilla olevia lokityökaluja haettiin pikaisella Google-katsauksella ja valittiin kymmenen potentiaalisinta työkalua ominaisuusvertailuun. Osa tarjolla olevista järjestelmistä olivat tavallisia keskitettyjä lokienhallintaratkaisuja ja osa taas tietoturvaan kohdistuvia SIEM-järjestelmiä. Valmistajien lupaamat ominaisuudet eivät huomattavasti eronneet eri työkalujen kohdalla ja lupauksiin suhtauduttiin näin ollen varauksellisesti. Lokityökalujen ominaisuusvertailuun valittiin ArcSight, Nagios Log Server, OpManager, Graylog, Opsview, Op5, Splunk, FortiSIEM, AlienVault USM ja ELK stack.

ArcSight on Micro Focuksen kehittämä kattava lokinhallintaratkaisu, joka toteuttaa mm. tehokkaita hakutoimintoja ja turvallisen säilytyksen. Työkalussa on myös toimintoja, jotka toteuttavat keskittämisen ja raportoinnin. [8.] Nagios Log Server on puolestaan helppokäyttöinen ja rajattomasti skaalautuva lokiohjelmisto, joka mahdollistaa käyttöliittymän muokkaamisen, verkkoturvatoimintoja sekä edistyksellisen käyttäjänhallinnan. Nagios sopeutuu helposti kolmannen osapuolen ratkaisuihin, jotka on otettu käyttöön samassa ympäristössä. [9.] OpManager luokitellaan luotettavaksi, mutta kohdistuu pääasiassa reaaliaikaista verkkomonitorointia toteuttavaksi ohjelmistoksi. Työkalun valmistaja on ManageEngine ja käyttöliittymään pääsee käsiksi myös puhelinsovelluksella. [10.] Graylog on samannimisen valmistajan kehittämä lokiohjelma, joka kerää lokit keskitettyyn paikkaan ja mahdollistaa siitä reaaliaikaiset hakuoperaatiot. Graylog-ohjelmiston lokinsäilytys toteutetaan pilviympäristössä. [11.] Opsview on jäljitelmä Nagiosista ja se on suunnattu liiketoimintapalvelun ja it-infrastruktuurin monitorointiin. OpsView mahdollistaa Nagios liitännäisten käyttämisen järjestelmässä ja tarjoaa niitä kattavasti. [12.] Op5 tai nykyisin Op5 monitor on ITRS:n valmistama lokitapahtumien seurantatyökalu, jolla tehdään pääosin liiketoimintaan kohdistettua raportointia. Op5 tukee OpsViewin tavoin myös Nagios-liitännäiset. [13.] Splunk on markkinajohtaja lokityökalujen saralla ja sillä voi tavanomaisesti luoda lokidatasta raportteja, hälytyksiä ja eri visualisaatioita. Splunkista löytyy myös suuri määrä eri maksullisia ja maksuttomia liitännäisiä. [14.] FortiSIEM on Fortinetin kehittämä lokienhallintatyökalu, joka keskittyy lokinkeräyksen lisäksi myös tietoturva-analysointiin ja automatisoituun ympäristön tarkkailuun. FortiSIEMissä ominaisuudet on pyritty räätälöimään tietoturva edellä. [15.] AlienVault USM on AT&T:n tuottama SIEM-järjestelmä, joka toteuttaa verkkojen monitorointa ja erilaisten tietotur-

vatapahtumien analysointia. USM on tietoturvaominaisuuksien osalta kattava työkalu, jos lokitiedot halutaan säilyttää pilvessä. [16.] ELK Stack koostuu kolmesta erillisestä avoimeen lähdekoodiin perustuvasta komponentista: Elasticsearch, joka toteuttaa hakutoiminnot, Logstash, joka toteuttaa lokin käsittelyn ja Kibana, joka toteuttaa lokidatasta muodostettujen visualisoinnin ja raportoinnin. ELK Stack ei kuitenkaan siltään tarjoa käyttövalmiita tietoturvatapahtumien analysointiratkaisuja. [17].

### 5.4 Testattavien työkalujen ominaisuusvertailu

Lokityökalujen ominaisuuksia selvitettiin kunkin tuotteen valmistajan verkkosivuilta, dokumentaatiosta ja muualta verkosta löydettävällä materiaalilla. Ominaisuusvertailun avulla pystyttiin kartoittamaan jokaiselta työkalulta vaadittujen ominaisuuksien toteutuminen suuntaa-antavasti. Jokaisen erillisen ominaisuuden selvittäminen verkkohakumenetelmän avulla ei kuitenkaan aina tuottanut vahvistettua tulosta ja se otettiin huomioon vertailun pisteytyksessä. Pintapuolisella selvityksellä pystyttiin kuitenkin pisteyttämään taulukkoon jokaisen lokityökalun ominaisuuksien vastaavuus yrityksen vaatimuksiin. Pisteytyksessä jaettiin ominaisuuksien täyttyvyys viiteen eri tasoon, jotka olivat ”täyttyy”, ”täyttymisessä huomioitava kohta”,”täyttyy osittain”,”ei täyty” ja ”täyttyminen ei selvinnyt”. Lopulta ominaisuusvertailun avulla laskettiin taulukkoon, kuinka monta ominaisuutta kukin työkalu toteuttaa ja millä tasolla. Ominaisuusvertailun tulokset ovat nähtävissä taulukosta 1.

| | ArcSight | Nagios Log server | OpManager | Graylog | Opsview | OP5 | Splunk | FortiSiem | AlienVault | ELK stack |
|---|---|---|---|---|---|---|---|---|---|---|
| Ominaisuus täyttyy | 30 | 31 | 29 | 22 | 20 | 23 | 35 | 31 | 30 | 23 |
| Ominaisuus täyttyy osittain | 0 | 0 | 5 | 3 | 6 | 3 | 0 | 0 | 2 | 3 |
| Ominaisuus täyttyy osittain | 1 | 1 | 0 | 4 | 2 | 5 | 0 | 2 | 2 | 5 |
| Ominaisuus ei täyty | 1 | 0 | 0 | 1 | 2 | 1 | 0 | 0 | 0 | 1 |
| Ominaisuuden täyttyminen ei selvinnyt | 4 | 4 | 2 | 5 | 6 | 4 | 1 | 3 | 2 | 4 |

Taulukko 1 ominaisuusvertailun tulokset.

Ominaisuusvertailun pisteytyksen pohjalta korkeimman tuloksen sai Splunk ja toiseksi parhaan pistetuloksen FortiSIEM lokityökalu. Tässä opinnäytetyössä tutustutaan FortiSIEM-lokityökaluun ja sen toimintaan, sillä se oli myöhemmin ilmenneiden tietoturvavaatimuksien kannalta yritykselle sopivampi SIEM-ratkaisu.

## 5.5 Testauksen suunnittelu

Testauksen kohteeksi valittiin FortiSIEM-lokityökalu ja kyseisen järjestelmän testaus kohdistui ominaisuusvertailussa listattuihin ominaisuuksiin ja niiden täyttyvyyden todentamiseen. Testauksen tavoitteena oli ensisijaisesti todentaa järjestelmän yleinen toimivuus vaatimusmäärittelyssä eriteltyjen vaatimusten perusteella. Järjestelmätasolla testaus suoritettiin ohjelmiston tarjoajan järjestelmädokumentaation ja testaussuunnitelmassa eriteltyjen testausmenetelmien avulla.

Testaus suunniteltiin toteutettavaksi VMware-virtualisointiympäristössä. Pohjana testauksessa käytettiin aikaisemmin määriteltyä vaatimuslistaa. Järjestelmälle asetettujen vaatimuksien täyttyvyys testattiin ja dokumentoitiin erilliseen testaus- ja vertailudokumenttiin, josta voitiin pisteyttämällä löytää työkalu, joka vastaa kaikista eniten haluttuihin vaatimuksiin. Osa testattavista vaatimuksista jäi väistämättä testauksen ulkopuolelle, sillä niiden vaatimat tekniset toiminnot olivat testiympäristössä mahdottomia toteuttaa. Toteuttamattomat testit jätettiin projektin toiselle kierrokselle, jossa testausympäristönä voitiin käyttää yrityksen tuotantoympäristöä ja näin ollen testitulokset saatiin luotua mahdollisimman todenmukaisessa ylläpitoskenaariossa.

Testauksen eri vaiheet suunniteltiin toteutettavaksi testaussuunnitelmassa määriteltyjen vaiheiden mukaisesti ja ensimmäisessä vaiheessa tehtäisiin varsinainen ympäristön pystytys. Toisessa vaiheessa pystytettävä työkalu konfiguroitaisiin testiympäristöön ajettavaksi ja kolmannessa vaiheessa tehtäisiin varsinainen toimintojentestaus ja siinä todennettaisiin vaatimusmäärittelyyn kirjattujen ominaisuuksien toteutuminen. Lopuksi testitulosten perusteella valittaisiin parhaiten suoriutunut järjestelmä hankittavaksi.

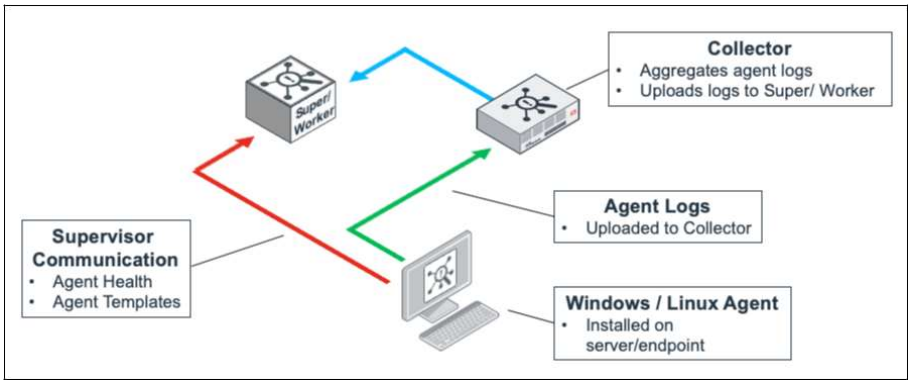
# 6 Testityökalun pystytys

Testityökaluksi valitun FortiSIEM-lokienhallintajärjestelmän asennus toteutettiin VMware Vcenter -virtualisointitympäristössä, joka toimii virtuaalikoneille hallintapaneelina. Ennen varsinaista lokijärjestelmän pystytystä jouduttin hankkimaan Fortinet-ohjelmistontarjoajalta loki-työkalun testilisenssi ja tekemään esikartoitus vaadittavista toimenpiteistä ja vaadittavista arkkitehtuurista. FortiSIEM-järjestelmä koostuu useammista nodeista eli solmuista ja kahdesta eri ympäristötyypistä. Nämä ympäristötyypit ovat enterprise ja service provider. Vaatimuksena olevien toimintojen perusteella valittiin FortiSIEM-ympäristöksi service provider.

Service provider -tila mahdollistaa useampien organisaatioiden luomisen lokijärjestelmään ja toimii edellytyksenä multitenantille hallintajärjetelmälle, jossa mm. yrityksen asiakkaille voidaan luoda omia näkymiä ja rajata sisältö pelkästään asiakkaan tarpeisiin. Ympäristötilaa valitessa Service provider tai enterprisen välillä tulee olla tarkkana, sillä sitä ei voi jälkeenpäin enää vaihtaa muuten kuin hankkimalla uusi lisenssi lokityökalulle.

FortiSIEMin klusterointiarkkitehtuuri (kuva 1.) koostuu worker-, collector- ja supervisor-solmuista, jotka toteuttavat lokitiedon keräyksen, analysoinnin ja säilytystoimintojen hajauttamisen omina laitteinaan ja mahdollistavat täten joustavasti skaalautuvan järjestelmäkokonaisuuden kohdeorgansiaation IT-alueen koosta riippumatta. Collectorit kommunikoivat lokia keräävien laitteiden kanssa ja toteuttavat keräyksen, jäsentelyn ja pakkaamisen lokitiedon jatkokäsittelyä varten. Worker puolestaan analysoi collectorilla käsitellyn lokitiedon ja vähentävät kuormaa supervisorilta. Supervisor on FortiSIEM-klusterin tärkein komponentti ja se on minimivaatimus yksinkertaisinta lokinhallintajärjetelmää pystyttäessä. Supervisor-solmu sisältää graafisen käyttöliittymän ja liiketoimintalogiikkan sovelluspalvelimen sekä sovellustilan ylläpidossa käytettävän relaatiotietokannan. [18.]

Testiympäristöön suunniteltiin pystytettäväksi yksi supervisor ja kaksi collectoria. Supervisor pystyi toteuttamaan lokianalysointia eli ns. raakaa työtä, joten workeria ei klusteriin tarvinnut liittää. Rajallisesta laitelisenssimäärästä johtuen järjestelmään ei haluttu liittää turhia laitteita.




Kuva 1. Esimerkki FortiSIEM-klusterista [19.]

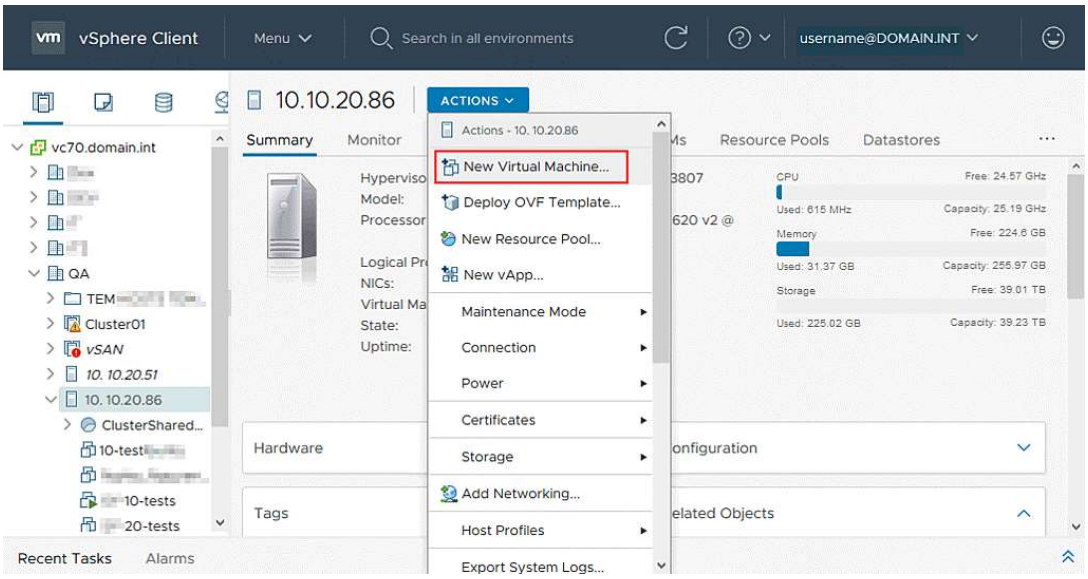
## 6.1 Pystytystoimenpiteet

Vmware-testilaboratorioon luotiin useita virtuaalikoneita, joissa oli vastaavia käyttöjärjestelmiä kuin yrityksen tuotantoympäristössä, jotta niiden ja lokijärjestelmän välinen yhteensopivuus voitiin testata. Laboratorioon luotiin myös erillisiä verkkoja, jotta voitiin testata lokienhallintajärjestelmän toiminta, kun sen komponentit ovat hajautettuna eri verkkoihin.

Lokityökalun pystytystä alettiin toteutettaa tuotteen valmistajan ohjeisiin tukeutuen ja ensimmäisessä vaiheessa sijoitettiin Fortinetiltä ladattu Supervisor-levykuva Vmware-virtualisointiympäristöön. Levykuvan sijoittaminen Vmware-hallintapaneeliin oli suoraviivainen toimenpide, jossa virtuaalikoneelle määriteltiin nimi, isäntälaite, verkko ja tallennustila. Lokityökalulta otettiin huomioon myös vaatimukset järjestelmäresurssien osalta ja niiden mitoittamisessa käytettiin kyseiselle toimenpiteelle tarkoitettua valmistajan opasta (kuva 2.). Tässä vaiheessa testityökalulle asetettiin resurssit minimivaatimusten mukaan, sillä testiympäristön lokia tuottavien virtuaalikoneiden määrä oli pieni ja näin ollen EPS arvioitiin myös vähäiseksi. VMware Vcenter hallintapaneeli, jota käytettiin, näkyy kuvassa 3.

| Node | vCPU | RAM | Local Disks |
|---|---|---|---|
| Supervisor (Cluster) | Minimum – 16<br>Recommended - 32 | Minimum<br>• without UEBA – 24GB<br>• with UEBA - 64GB<br>Recommended<br>• without UEBA – 32GB<br>• with UEBA - 64GB | OS – 25GB<br>OPT – 100GB<br>CMDB – 60GB<br>SVN – 60GB |
| Collector | Minimum – 4<br>Recommended – 8 ( based on load) | Minimum – 4GB<br>Recommended – 8GB | OS – 25GB<br>OPT – 100GB |

Kuva 2. Valmistajan suosittelemat järjestelmäresurssit kullekin asennetavalle solmulle [20.]




Kuva 3. VMware Vcenter -hallintapaneeli [21.]

Minimijärjestelmävaatimuksiin perustuen, supervisorille oli määriteltävä 16 CPU:ta, 24 gigatavua välimuistia sekä 245 gigatavua levytilaa. Molemmille collectorille määriteltiin 4 CPU:ta, 4 gigatavua välimuistia ja 125 gigatavua levytilaa. Workeria ei asennettu, koska arvioitiin että EPS ei saavuta siihen vaadittua lukumäärää.

Lokitietojen pitkäaikaista säilytystä eli arkistointia varten täytyi arvioida verkkolevyn käyttöaste ja siinä voitiin käyttää hyödyksi laskukaavoja. Kaavojen avulla voitiin selvittää, kuinka paljon levytilaa järjestelmä saattaa kuluttaa teraatavauina, normaalissa ja pahimmassa tapauksessa. Käytännössä kaavoihin tarvitsee vain sijoittaa EPS:n huippupiste ja tallennusaika kuukausina. [20.]

Lokitietojen arkistointia ei kuitenkaan päästy testaamaan ollenkaan, sillä arkistointia toteuttava tallennusjärjestelmä oli laboratorioympäristön ulottumattomissa.

$$Average\ case = \frac{0.5 \times Peak\ EPS \times 100 \times 86400 \times 30 \times Storage\ Months}{10^{12}}$$

Kaava 1. Levytilan keskiverto kulutus teratavuissa [20].

$$Worst\ case = \frac{Peak\ EPS \times 150 \times 86400 \times 30 \times Storage\ Months}{10^{12}}$$

Kaava 2. Levytilan kulutus pahimmassa tapauksessa [20].

Kun asennustoimenpiteet oli supervisorin osalta tehty, voitiin FortiSIEMin hallintapaneeliin kirjautua verkkoselaimen kautta ja rekisteröidä demolisenssi annetuilla tunnuksilla. Tässä vaiheessa valittiin ympäristötilaksi alussa vahingossa enterprise eikä service provider, minkä vuoksi jouduttiin tilaamaan uusi testilisenssi sekä järjestelmä oli asennettava kokonaan uudestaan. Uuden yrityksen jälkeen supervisorille valittiin kuitenkin oikea ympäristötila. Supervisorilla oli luotava hallintapaneelin kautta uusi organisaatio sekä käyttäjä asennuksen jälkeen, jotta järjestelmää päästiin käyttämään. Hallintapaneelin etusivu näkyy kuvassa 4.


Kuva 4 FortiSIEMin hallintapaneeli [22.]

Suunnitelman mukaisesti pystytystä jatkettiin collectoreiden osalta ja niiden sijoittaminen laboratorioympäristöön toteutettiin samalla levykuvalla kuin supervisorilla. Tässä tapauksessa collectorille lisättiin vain sille suunnatut järjestelmäresurssit ja asennuskonfiguraatiota tehdessä valittiin asennettavaksi collector. Collectorin asennuksen jälkeen se täytyi rekisteröidä lokijärjestelmään supervisorilta ja rekisteröinnin jälkeen collector pystyi muodostamaan yhteyden supervisoriin. [23.]

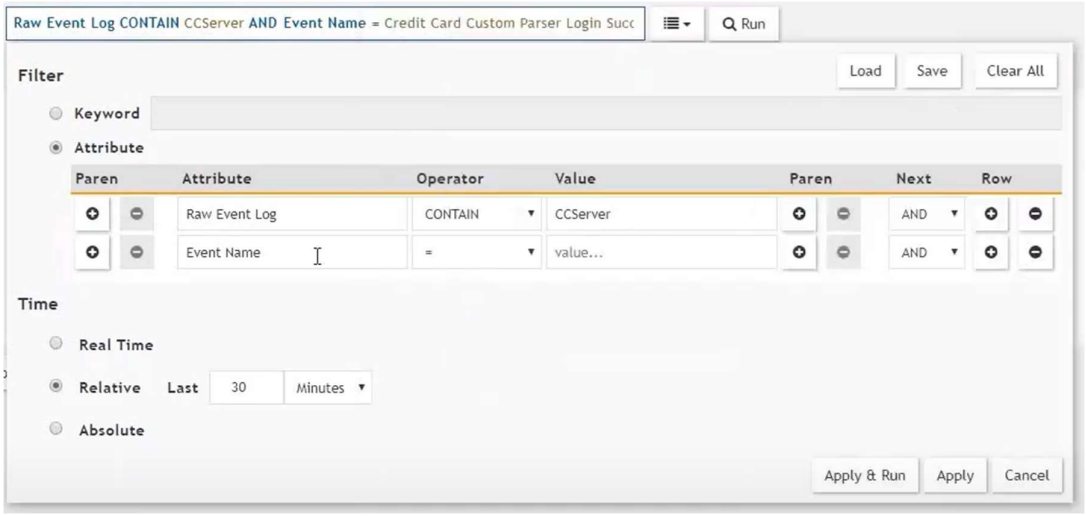
Lokin keräämisen edellyttämiseksi laboratorioympäristön testilaitteet oli vielä liitettävä lokijärjestelmään ja FortiSIEMin kohdalla liitos toteutettiin lähdelaitteille asennettavien agenttien avulla. Windows-käyttöjärjestelmiin agentti asennettiin FortiNETin omalla asennustiedostolla ja Linuxissa tai muissa Unix- pohjaisissa järjestelmissä asennus toteutui asennusskriptillä. Asennuksen yhteydessä täytyi agentille määritellä parametrit ja Windowsissa se oli toteutettu erillisellä konfigurointitiedostolla. Konfiguroinnin esimerkki löytyy kuvasta 5. Lopuksi agentit vielä rekisteröitiin oikealle organisaatiolle käytettäväksi supervisorissa.

Agentin tehtävä on kerätä järjestelmästä määritellyt lokitiedot ja lähettää ne toiseen kohteeseen. Agentteja pidetään yleisesti tarpeellisena siitä syystä, että ne mahdollistavat kaikkien lokien keräämisen samalta laitteelta kerralla. [23.] Järjestelmissä, joissa lokin rotaatiota ei olla otettu käyttöön, voi syntyä skenaario, missä lokitietoa päällekirjoitetaan. Näissä tapauksissa agentista on hyötyä, sillä lokit saadaan kerättyä reaaliajassa ennen lokitietojen häviämistä. [24.]

```
<InstallConfig Version="1">
    <Org>
        <ID>ORG_ID</ID> <!-- Organisaation id ESIM 2000 -->
        <Name>ORG_NAME</Name> <!-- Organisaation nimi ESIM Lokilabra -->
    </Org>
    <Super>
        <Name>SUPER_IP</Name> <!-- Supervisorin ip tai FQDN-->
        <Port>443</Port> <!-- Supervisorin portti -->
    </Super>
    <HostName>AGENT_HOST_NAME</HostName> <!-- Agentin host name -->
    <Registration>
        <Username>ORG_NAME/AGENT_USER</Username> <!-- organisaation nimi ja agentin käyttäjänimi -->
        <Password><![CDATA[AGENT_PASSWORD]]></Password> <!-- Agentin salasana -->
    </Registration>
    <Proxy>
        <Server />
        <Port />
    </Proxy>
    <SSLCertificate>check</SSLCertificate>
</InstallConfig>
```

Kuva 5. Windows-agentin konfigurointi.

Kun halutut lokia tuottavat laitteet saatiin kytkettyä lokijärjestelmään, pystyttiin nyt kerätylle lokille suorittamaan hakutoimintoja käyttöliittymästä. FortiSIEMissä hakutoiminnot suoritetaan hakukenttään syötettävillä avainsanoilla tai suodattimella, johon voi erikseen määrittää haetulle lokille ehdot. Haussa voidaan myös erikseen määritellä tapahtuman aikaikkuna, josta tiedot haetaan. Hakuikkuna näkyy kuvassa 6. [25.]




Kuva 6. FortiSIEM -hakutoimintojen ruutu kohdassa 6:36 [26.]

# 7 Lokityökalun toimintojen testaus

## 7.1 Hälytykset

Kaikki monitoroidut tapahtumat, jotka viittaavat tietoturva-, laite- tai sovellusongelmaan kuuluisi jollakin menetelmällä jäljittää niiden alkupisteeseen. Organisaation lokinkeräysvaatimuksista riippuen tulisi lokipolitiikkaan kirjata menettelytapa yhtäjaksoiselle lokien monitoroinnille. Tämän menetelmän täytyy perustua siihen, kuinka usein vaadittavat tapahtumat ovat tarkistettava reaaliajassa ja lokienhallintajärjestelmän täytyy kyetä tuottamaan ilmoitus sen perusteella. [27.]

FortiSIEM-lokityökalun sääntöjen luomisessa täytyy määrittää kyseiselle säännölle attribuutit, joihin kirjataan laukaisuehdot ja mahdolliset poikkeukset ja niiden perusteella säännöstä laukaistaan ilmoitus lokijärjestelmässä [28]. Testauksessa toteutettiin lokityökalulle mm. esimerkkisääntö, jossa järjestelmä nostaa ilmoituksen kun 5 epäonnistunutta kirjautumisyritystä tapahtuu peräkkäin. Tämä toteutettiiin valmistajan tekemällä esimerkillä, joka konfiguroidaan taulukon 2 mukaisesti.

| Filter | Attribute | Constraints |
|---|---|---|
| Event type = Login Failure | Source IP, Destination IP | COUNT (Matched Event) >= 5 |

Taulukko 2.

Säännön konfiguroinnin yhteydessä voi säännön toteutumisesta luoda insidentin eli tapahtuman ja tähän voidaan kirjata esimerkiksi hälytyksen vakavuus, kategoria ja notifikaatio [28]. Hälytyksen ilmoitukset ilmaantuivat Incidents-sivulle, joka näkyy kuvasta 7.

Hälytyksiä lähdettiin toteuttamaan sillä ajatuksella, että vakavimmissa tapahtumissa hälytykset tulisivat tekstiviesti-ilmoituksena ja matalamman riskiluokan tapahtumahälytykset tulisivat sähköpostiin tai lokijärjestelmän hallintapaneeliin nähtäville. Laboratoriossa kuitenkin pystyttiin testaamaan pelkästään viimeistä vaihtoehtoa.

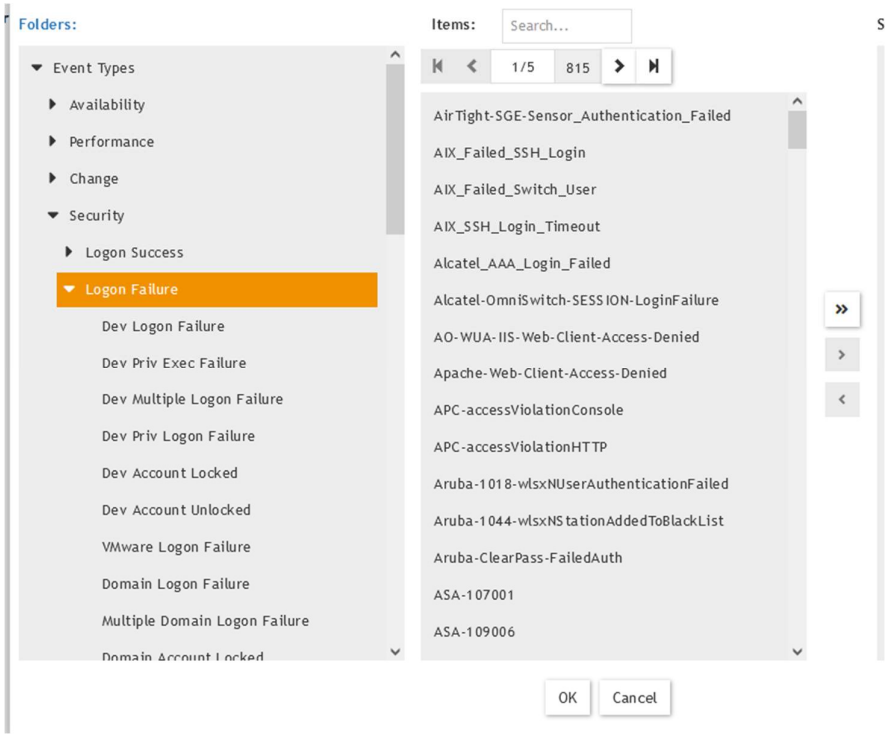

Kuva 7. Nostettujen hälytyksien näkymä kohdassa 0:30 [29.].

## 7.2 Raportit

Raporttina voidaan pitää raakalokista tuotettua aineistoa, joka pohjautuu olemassa oleviin lokimerkintöihin. Esimerkkinä voidaan pitää esimerkiksi erilaisilla analysointimenetelmillä luotuja poikkeavien lokitapahtumien listoja ja muita verkkoliikenteen tai palomuurien tapahtumien yhteenvetoja. Lokidatasta luotujen raporttien tehtävä on mm. etsiä tietoturvauhkiin viittaavia ennalta tunnistettuja syy-seuraus -suhteellisia tapahtumaketjuja. [30.]

Toimeksiantajan yksi tavoitteista lokityökalun raportoinnille oli mahdollistaa lokitiedostojen sisältämän datan tarkastelu säännöllisin väliajoin. Raportoinnin kohteeksi haluttiin ottaa ainakin onnistuneet ja epäonnistuneet kirjautumiset, laitekohtaisten käyttäjätunnusten käyttö järjestelmissä, pääkäyttäjätunnuksen käyttö (sudo-komennot), erityisvalvottuihin tiedostoihin kohdistuneet toimenpiteet ja konfiguraation muutokset sekä lokijärjestelmän EPS-käyttöaste.

Raportin luominen onnistui FortiSIEM-työkalun käyttöliittymästä “resources and reports” -osiossa. Malliraportiksi luotiin raportti epäonnistuneista kirjautumisista ja sen luomiseen käytettiin apuna CMDB eli configuration management databasesta löytyvää tietoturvatapahtuma -tyyppiä. CMDB-tietokannasta löytyy runsaasti raportoitavia järjestelmätapahtumia ja varsin tavanomaiseen kirjautumisyritysten seurantaan löytyy useita sääntöihin määriteltäviä tapahtumia (kuva 8).




Kuva 8. CMDB-tapahtumatietokanta.

Dev Logon Failure -mallisääntöä hyödyntäen raporttiin saatiin kerättäväksi kaikilta laitteilta poimitut tapahtumat, jotka ovat toteuttaneet kyseisessä säännössä määritellyt ehdot eli epäonnistuneet kirjautumiset. Raportin sisällön ulkomuotoa pystyttiin räätälöimään halutun näköiseksi kirjaamalla sarakkeille tulevien tietojen attribuutit, “define display column“-osiossa.

Raporttiin lisättiin myös ajastin ja siihen määriteltiin, miltä ajalta kerätään tapahtumat sekä kuinka usein raportti tallentuu. Raportin luonnin viimeisessä osiossa on määriteltävä raportin tallennusmuoto, säilytysaika ja tallennussijainti. Laboratorioympäristöön ei pystytetty sähköpostipalvelua, joten raportti asetettiin tallennettavaksi PDF-muotoon yhdelle lähdelaitteista. Raportoinnin kohteeksi kerättävät tapahtumat olivat helposti simuloitavissa, kun koeympäristön laitteisiin kirjattiin tahallisesti virheellisiä autentikaatioyrityksiä. Esimerkkiraportin tulokset näemme kuvasta 9.

Found Records 4

| Rank | Source IP | User | Server | COUNT(Matched Events) |
|---|---|---|---|---|
| 1 | 192.168.1.11 | lokittaja | koopa | 10 |
| 2 | 192.168.1.11 | lokittaja | goomba | 5 |
| 3 | 192.168.1.11 | lokittaja | toad | 4 |
| 4 | 10.10.140.121 | lokipomo | LUIGI.lokilabra.local | 1 |

Kuva 9. Esimerkkiraportin tulos.

## 7.3 Windows defender ja Powershell lokien keräys

Windows defender on Microsoftin kehittämä virustentorjuntaohjelma, joka pystyy tekemään reaaliaikaista suojausta sekä haittaohjelmatarkistuksia [31]. Windows Event Viewer on Windows-käyttöjärjestelmälle kehitetty lokien tarkastelutyökalu, joka jakaa lokit kolmeen eri kategoriaan: sovelluslokit, järjestelmälokit ja turvallisuuslokit [32].

Windows defenderin lokikeräys pystyttiin toteuttamaan lisäämällä Windows event viewerin -lokitapahtumien hakemisto FortiSIEMiin. Defender-lokien lisäyksen avulla saatiin kerättyä mm. virustarkastusten tulokset ja tapahtumat, joissa Windows defender havaitsi laitteella haittaohjelman. Lisäämällä defender-lokien keräys kaikille lokikerääjään liitetyille Windows-laitteille saatiin valvottua ne haittaohjelmien varalta ja nostamaan ilmoitukset tietoturvatapahtumien ilmetessä.

Lokienhallintajärjestelmän haluttiin keräävän PowerShell-komentokehotteella suoritetut toimenpiteet valvotuilta laitteilta. PowerShellin lokikeräyksellä pystyttiin seuraamaan powershellissä luotujen prosessien toimintaa ja niiden suorittamia komentoja. Suosittu tapa tunkeutujille on hyväksikäyttää kohdejärjestelmien omia työkaluja ja etenkin PowerShell-komentorivityökalua [33]. PowerShell-lokien keräys saatiin totettua kytkemällä ensin Windowsin ryhmäkäytännöistä ”PowerShell module logging” päälle ja lopuksi FortiSIEMiltä muutettiin Windowsin lokikeräyssääntöön kerättäväksi Event Viewer -polku ”Microsoft-Windows-PowerShell/Operational”. PowerShell lokien pohjalta pystyttiin nyt lokijärjestelmässä luomaan sääntöjä lokitiedossa olevista virhekoodeista ja ajettavista komennoista saatiin tarvittavat hälytykset.

# 8 Tulokset

SIEM-tuotteet myydään niillä odotuksilla, että ne sisältäisivät automatisoituja toimintoja, mutta useinkaan nämä odotukset eivät vastaa todellisuutta [6]. Opinnäytetyössä tarkasteluun kohdistuneet FortiSIEM-lokiohjelmiston toiminnot kuitenkin osoittivat, että työkalulla voidaan toteuttaa edistynyttä lokienhallintaa yrityksessä, jossa lokikeräyksen kohteeksi otetaan joukko virtualisoituja järjestelmiä, laitteita tai muita teknisiä ratkaisuja.

FortiSIEMin hyvinä puolina koettiin sen massiivinen tietokanta, josta valmiita lokianalysoinnin sääntöjä voitiin hyödyntää. Valmiiden sääntöjen ansiosta säästyy suurelta vaivalta, kun ei tarvitse käyttää paljoa työaikaa raporttien ja hälytyksien räätälöimiseen. Työkalussa huonoksi koettiin kuitenkin valmistajan dokumentaatio, kun se ei ollut ajan tasalla ja sieltä oli vaikea hakea haluttu tieto. Myös järjestelmän käytettävyydessä koettiin heikkouksia, sillä aina päivityksen myötä lokijärjestelmän osa toiminnoista lakkasi toimimasta ja korjaustoimenpiteet hukkasivat henkilöresursseja.

Lokityökalujen vertailusta opittiin, että kannattaa tehdä perinpohjainen tutustuminen aihepiiriin, jotta kaikki tuotteen vaatimukset saadaan kerättyä projektin mahdollisimman varhaisessa vaiheessa. Työkalun evaluointia ei pystytty toteuttamaan sen alkuperäisen projektisuunnitelman mukaisesti, sillä jokaisen työkalun testauksen aikana saatiin paljon tarkempi kuva siitä, millaista lokityökalua todellisuudessa ollaan hakemassa ja FortiSIEMin kohdalla päästiin lähimmäksi toivejärjestelmää. Vaatimukset, jotka vertailuvaiheessa karsivat eniten lokijärjestelmän valintaa olivat SIEM-toiminnot, ohjelmiston multitenattisuus ja on-premise -vaatimus.

Testauksessa havaittiin se, että perusteellisten testausten suorittaminen laboratorio- ja tuotantoympäristössä vaativat runsaasti aikaa, varovaisuutta ja teknistä tuntemusta järjestelmistä, joita lokijärjestelmään aiotaan liittää. Lokijärjestelmä jäi jatkotestattavaksi ja sen kokeilusta tuotantoympäristössä luotiin jatkossa uusi projekti.

# 9 Lähteet


1. Kyberturvallisuuskeskus: Näin keräät ja käytät lokitietoja, 2020. [Viitattu 22.12.2021]. Saatavilla osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

2. Karen K. & Murugiah S. Guide to Computer Security Log Management, 2006, [Viitattu 22.12.2021]. Saatavilla osoitteesta: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

3. Valtiovarainministeriö, Lokiohje, 2009, [Viitattu 05.01.2022]. Saatavilla osoitteesta: https://www.suomidigi.fi/sites/default/files/2020-06/pdf_3_2009.pdf

4. Yrjö K. SIEM-järjestelmä on organisaation kyberturvallisuuden hermokeskus, 2017. [Viitattu 22.12.2021]. Saatavilla osoitteesta: https://www.insta.fi/ajankohtaista/siem-j%C3%A4rjestelm%C3%A4-on-organisaation-kyberturvallisuuden-hermokeskus

5. Amir Jamil. The difference between SEM, SIM and SIEM, 2010, [Viitattu 16.01.2022]. Saatavilla osoitteesta: https://www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew=

6. Dr. Anton C. The Complete Guide to Log and Event Management. [Viitattu 19.12.2021]. Saatavilla osoitteesta: https://www.netiq.com/en-gb/docrep/documents/m47h82fbmy/the_complete_guide_to_log_and_event_management_wp_ee.pdf

7. Johanna K. Vaatimusmäärittely käyttäjäkeskeisessä tuotekehityksessä, 2005. [Viitattu 18.1.2022]. Saatavilla osoitteesta: https://www.researchgate.net/publication/242738874_Vaatimusmaarittely_kayttajakeskeisessa_tuotekehityksessa

8. MicroFocus, ArcSight Logger, [Viitattu 16.01.2022]. Saatavilla osoitteesta: https://www.microfocus.com/en-us/products/siem-log-management/overview

9. Nagios. What can nagios help you do? [Viitattu 27.01.2022]. Saatavilla osoitteesta: https://www.nagios.com/

10. ManageEngine, ArcSight Logger, [Viitattu 16.01.2022]. Saatavilla osoitteesta: https://www.manageengine.com/network-monitoring/?pos=All-prod&cat=NS&loc=links&prev=AB2

11. Graylog, Security and log data done right, [Viitattu 29.01.2022]. Saatavilla osoitteesta: https://www.graylog.org/

12. OpsView, Cloud & infrastructure monitoring for your business, [Viitattu 16.01.2022]. Saatavilla osoitteesta: https://www.opsview.com/

13. ITRS Group. ITRS OP5 Monitor, [Viitattu 18.01.2022]. Saatavilla osoitteesta: https://www.itrsgroup.com/products/network-monitoring-op5-monitor

14. Splunk. The Data Platform for the Hybrid World, [Viitattu 04.02.2022]. Saatavilla osoitteesta: https://www.splunk.com/

15. Fortinet. FortiSIEM Solutions, [Viitattu 02.02.2022]. Saatavilla osoitteesta: https://www.fortinet.com/products/siem/fortisiem

16. AT&T Cybersecurity.USM Appliance Documentation, [Viitattu 16.03.2022]. Saatavilla osoitteesta: https://cybersecurity.att.com/documentation/usm-appliance.htm

17. Elastic. What is the ELK Stack? [Viitattu 16.03.2022]. Saatavilla osoitteesta: https://www.elastic.co/what-is/elk-stack

18. Fortinet, Key Concepts, [Viitattu 18.03.2022]. Saatavilla osoitteesta: https://help.fortinet.com/fsiem/5-1-2/Online-Help/HTML5_Help/Key_concepts.htm

19. Fortinet. Disaster Recovery Procedures, [Viitattu 18.03.2022]. Saatavilla osoitteesta: https://docs.fortinet.com/document/fortisiem/5.4.0/disaster-recovery-procedures-elasticsearch/565771/disaster-recovery

20. Fortinet, Sizing Guide, [Viitattu 20.03.2022]. Saatavilla osoitteesta: https://docs.fortinet.com/document/fortisiem/6.2.1/sizing-guide/965243/fortisiem-sizing-guide

21. Michael B. How to Create a Virtual Machine Using vSphere Client 7.0, 2020, [Viitattu 30.04.2022]. Saatavilla osoitteesta: https://www.nakivo.com/blog/how-to-create-a-virtual-machine-using-vsphere-client-7/

22. Stephen C. FortiSIEM Review & Alternatives, [Viitattu 30.04.2022]. Saatavilla osoitteesta: https://www.comparitech.com/net-admin/fortisiem-review-alternatives/

23. Thu N. Logging Agents VS. Logging Libraries: Which should you use? 2019, [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://www.mezmo.com/blog/logging-agents-vs-logging-libraries-which-should-you-use

24. Solarwinds loggly. Managing Linux Logs, [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://www.loggly.com/ultimate-guide/managing-linux-logs/

25. Fortinet.Undestanding Search Components, [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://help.fortinet.com/fsiem/5-1-0/Online-Help/HTML5_Help/Understanding_search_components.htm

26. We-Learns. Fortinet | FortiSIEM |Adding Events to the CMDB, [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://www.youtube.com/watch?v=3Ttp6P3F7CA&ab_channel=WE-Learns

27. Olga B. Event Log Management and Monitoring, 2020. [Viitattu 18.05.2022]. Saatavilla osoitteesta: https://www.virtualmetric.com/blog/log-management-monitoring

28. Fortinet, Creating Rules, [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://help.fortinet.com/fsiem/6-1-0/Online-Help/HTML5_Help/Creating-rules.html

29. Fortinet Video Library. Incident Investigation and Visibility, [Viitattu 20.05.2022]. Saatavilla osoitteesta: https://www.youtube.com/watch?v=OTv3Fh8Qsk8&t=676s&ab_channel=FortinetVideoLibrary

30. Fortinet, FortiSIEM Deployment Scenarios, [Viitattu 22.05.2022]. Saatavilla osoitteesta: https://help.fortinet.com/fsiem/5-2-1/Online-Help/HTML5_Help/FortiSIEM_deployment_scenarios.htm#Enterpri

31. Microsoft. Suojaa koneesi Windowsin suojauksella, [Viitattu 26.05.2022]. Saatavilla osoitteesta: https://support.microsoft.com/fi-fi/windows/suojaa-koneesi-windowsin-suojauksella-2ae0363d-0ada-c064-8b56-6a39afb6a963

32. Donald B. Windows Event Viewer, 2015, [Viitattu 25.05.2022]. Saatavilla osoitteesta: http://www.dba-oracle.com/t_windows_event_viewer.htm

33. Traficom, Opas tietomurtojen havaitsemiseen, 2020 [Viitattu 16.05.2022]. Saatavilla osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Opas-tietomurtojen-havaitsemiseen.pdf