

KARELIA-AMMATTIKORKEAKOULU  
Tietotekniikan koulutusohjelma

Perttu Ryynänen  
Markus Tuupanen

SECURITY INFORMATION AND EVENT  
MANAGEMENT -JÄRJESTELMÄT

Opinnäytetyö  
Huhtikuu 2015



**OPINNÄYTETYÖ**  
**Huhtikuu 2015**  
**Tietotekniikan koulutusohjelma**

Karjalankatu 3  
80200 JOENSUU  
013 260 600

**Tekijät**  
Perttu Ryyänen ja Markus Tuupanen

**Nimeke**  
Security information and event management -järjestelmät

**Toimeksiantaja**  
Itä-Suomen yliopisto / Tietotekniikkapalvelut

**Tiivistelmä**

Opinnäytetyö tehtiin Itä-Suomen yliopistolle, jolla on tarve keskitettyyn lokienhallintaan ja tietoturvan monitorointiin. Työn päätavoitteena on toimia apuvälineenä Security Information and Event Management -järjestelmiin perehtymiseen. Tästä aiheesta on tehty aiemmin vain vähän suomenkielisiä julkaisuja.

Teoriaosuudessa esitellään liiketoiminnallista näkökulmaa ja projektin läpivientiä. Osuudessa käsitellään myös SIEMin keskeiset käsitteet ja teknologiat. Esitetyt laskukaavat auttavat järjestelmän mitoittamista IT-ympäristöön sopivaksi. Yhtenä opinnäytetyön tehtävänä oli esitellä eri valmistajien SIEM-ratkaisuja. Käsiteltäväksi valittiin tuotteita kahdeksalta eri valmistajalta, joista avoimen lähdekoodin AlienVault OSSIM kuvataan tarkemmin.

Opinnäytetyötä varten tehty demoympäristö esittelee AlienVault OSSIMin käyttöönottoa pienessä ympäristössä. Teknisen dokumentaation tarkoituksena ei ole toimia asennusohjeena, vaan esitellä SIEMin toiminnallisuutta käytännön esimerkkien avulla. Tiedonkulku on kuvattu datan keräämisestä korreloidun tapahtuman analysointiin.

**Kieli**  
suomi

**Sivuja 74**  
**Liitteet 20**

**Asiasanat**  
SIEM, AlienVault, OSSIM, tietoturva



**THESIS**  
**April 2015**  
**Degree Program in Information Technology**

Karjalankatu 3  
80200 JOENSUU  
FINLAND  
+358 13 260 600

**Authors**  
Perttu Rynänen and Markus Tuupanen

**Title**  
Security Information and Event Management Systems

**Commissioned by**  
University of Eastern Finland / IT Services

**Abstract**

This thesis was commissioned by the University of Eastern Finland. There is a demand for a centralized log management and information security monitoring. The main goal was to provide aid for familiarization with Security Information and Event Management systems. There are not many Finnish publications about this topic yet.

The theory section describes the business perspective and the completion of the project. SIEM concept and its technologies are also explained. The introduced formulas help the scaling system to fit for an IT environment. One objective of the thesis was to demonstrate various SIEM solutions from different vendors. Products from eight different vendors are introduced. An open source SIEM system AlienVault OSSIM is described in more detail.

The test environment was made to demonstrate AlienVault OSSIM's deployment in a small network. The technical documentation is not a deployment guide for SIEM. It presents the functionality of SIEM with practical examples. The information flow is described from data collection to analysis of correlated events.

**Language**

Finnish

Pages 74

Appendices 20

**Keywords**

SIEM, AlienVault, OSSIM, information security

# Sisältö

|       |  |    |
|-------|--|----|
| 1     | Johdanto.....                                  | 11 |
| 1.1   | Opinnäytetyön lähtökohdat .....                | 12 |
| 1.2   | Lähdekriittisyys.....                          | 12 |
| 2     | Yritysten tietoturvavahkat.....                | 13 |
| 3     | Security information and event management..... | 15 |
| 3.1   | SIEM liiketoiminnan näkökulmasta.....          | 16 |
| 3.2   | SIEM-projekti .....                            | 18 |
| 3.3   | SIEM-tekniikat.....                            | 21 |
| 3.3.1 | Tiedon kerääminen.....                         | 22 |
| 3.3.2 | Normalisointi.....                             | 23 |
| 3.3.3 | Tiedon korrelointi.....                        | 24 |
| 3.3.4 | Monitorointi .....                             | 25 |
| 3.3.5 | Hälytykset .....                               | 25 |
| 3.4   | SIEM:n laskennalliset vaatimukset.....         | 25 |
| 4     | Erilaiset SIEM-ratkaisut .....                 | 28 |
| 4.1   | HP ArcSight .....                              | 29 |
| 4.2   | McAfee Enterprise Security Manager.....        | 31 |
| 4.3   | Trustwave SIEM .....                           | 32 |
| 4.4   | IBM Security QRadar .....                      | 34 |
| 4.5   | LogRhythm .....                                | 35 |
| 4.6   | NetIQ.....                                     | 36 |
| 4.7   | Splunk .....                                   | 37 |
| 4.8   | AlienVault OSSIM.....                          | 39 |
| 4.8.1 | OSSIMin keskeisimmät komponentit .....         | 40 |
| 4.8.2 | Ongelmien havaitseminen .....                  | 40 |
| 4.8.3 | Tiedon kerääminen.....                         | 41 |
| 4.8.4 | Korrelointi .....                              | 42 |
| 4.8.5 | Erot OSSIM- ja USM-järjestelmän välillä.....   | 42 |
| 4.9   | Splunkin ja AlienVaultin vertailu .....        | 43 |
| 5     | Demoympäristö .....                            | 43 |
| 5.1   | AlienVault OSSIM.....                          | 44 |
| 5.1.1 | Asennus .....                                  | 45 |
| 5.1.2 | Laitteiden lisäys ja tiedon kerääminen.....    | 50 |
| 5.1.3 | Threat intelligence.....                       | 56 |
| 5.1.4 | Monitorointi .....                             | 58 |
| 5.1.5 | Tiedon analysointi .....                       | 59 |
| 5.2   | Hyökkäyksen havaitseminen.....                 | 60 |
| 5.2.1 | Brute-force-hyökkäys.....                      | 60 |
| 5.2.2 | DoS-hyökkäys .....                             | 63 |
| 6     | Pohdinta.....                                  | 66 |
|       | Lähteet.....                                   | 68 |

## Liitteet

- Liite 1 15 yleisintä tietoturvavaukkaa
- Liite 2 Tietoturvatiedonkulku SIEM-järjestelmässä
- Liite 3 Laitteiden EPS-keskiarvoja
- Liite 4 HP ArcSight -lisenssivaihtoehdot
- Liite 5 SIEM Solution Portfolio from McAfee
- Liite 6 McAfee ESM -tuotteiden tekniset tiedot
- Liite 7 QRadar virtual appliances -laitteistovaatimukset
- Liite 8 LogRhythmin käyttöönottovaihtoehdot
- Liite 9 NetIQ-ohjelmistovaatimukset
- Liite 10 NetIQ-laitteistovaatimukset
- Liite 11 Klusteroitu Splunk-järjestelmä
- Liite 12 Splunk-järjestelmävaatimukset
- Liite 13 AlienVault OSSIMin toiminnallisuus
- Liite 14 Verkkokuva
- Liite 15 OSSEC-agentin asentaminen Ubuntu-palvelimeen
- Liite 16 Autentikointiavaimen lisääminen OSSEC-agenttiin Ubuntussa
- Liite 17 Cisco 2960 Catalyst -kytkimen konfiguraatio
- Liite 18 Toimintamalli SSH-brute-force-hyökkäyksen havaitsemiseen
- Liite 19 OSSIM-tiketti
- Liite 20 Cisco ASA 5505 -palomuurin konfiguraatio

## Lyhenteet

|             |  |
|-------------|--|
| ACK         | Acknowledgement, TCP-protokollan kolmivaiheisen kättelyn viimeinen paketti, jolla lähelaite ilmoittaa kohdelaitteelle onnistuneesta tiedonsiirrosta.                 |
| Agentti     | Seurattavalle järjestelmälle asennettava ohjelma, joka lähettää tietoa hallintapalvelimelle [1].   |
| APT         | Advanced persistent threats, yritykseen tai organisaatioon kohdistuva kehittynyt ja huomaamaton hyökkäys [2].  |
| Brute-force | Hyökkäysmenetelmä, joka perustuu käyttäjätunnuksen tai salasanan arvaamiseen koneellisesti yrittämällä [3].  |
| Bwm-ng      | Bandwidth Monitor NG, työkalu, jolla seurataan eri verkkokorttien kaistankäyttöä ja kovalevyjen tiedonsiirron määrää [4].  |
| BYOD        | Bring Your Own Device, käytäntö, jonka mukaan yrityksen työntekijä voi tuoda työpaikalle omia laitteita ja käyttää niitä työskentelyyn.                              |
| CEF         | Common Event Format, HP:n kehittämä tallennusstandardi lokitiedolle.   |
| DC          | Domain Controller, toimialueen hallintapalvelin.   |
| DNS         | Domain Name System, IP-verkoissa käytettävä nimipalvelujärjestelmä.  |
| DoS         | Denial of Service, palvelunestohyökkäys, jonka avulla hyökkääjä pyrkii estämään oikeiden käyttäjien pääsyn palveluun. Hyökkääjä tukkii verkon turhalla datalla. [5.] |
| EPS         | Events Per Second, tapahtumaa sekunnissa.  |
| ESM         | Enterprise Security Management, HP:n ja McAfeen SIEM-ohjelmiston nimi.   |
| FTP         | File Transfer Protocol, TCP-yhteyttä käyttävä tiedonsiirtoprotokolla [6].  |
| HIDS        | Host-based Intrusion Detection System, IDS-sovellus, joka tarkkailee poikkeamia yksittäiseltä laitteelta. Asennetaan yleensä paikallisesti tietokoneelle. [7.]       |

|           |   |
|-----------|---|
| HR        | Human Resources, henkilöstöosasto, jonka tehtäviin kuuluu työvoiman palkkaaminen, kouluttaminen ja hallinnointi sekä työsuhteisiin liittyvät sopimusasiat [8].                          |
| Htop      | Järjestelmän prosessorikuorman, muistinkäytön ja prosessien seurantaan tarkoitettu tekstipohjainen työkalu [9].   |
| HTTP      | Hyper Text Transfer Protocol, protokolla, jota käytetään selainten ja WWW-palvelinten väliseen tiedonsiirtoon.  |
| HTTPS     | Hyper Text Transfer Protocol Secure, protokolla, jossa yhdistyy HTTP-protokolla ja SSL/TLS-salaus.  |
| ICT       | Information and communications technology, tieto- ja viestintäteknologia.   |
| IDS       | Intrusion Detection System, tunkeutumisen havaitsemisjärjestelmä. Tunnistaa luvaton, laitonta ja poikkeavaa käytöstä ympäristössä. Toiminta perustuu verkkoliikenteen tarkkailuun. [7.] |
| Incident  | Tapahtuma, joka poikkeaa normaalista IT-palvelun toiminnasta. Aiheuttaa häiriöitä tai palvelutason laskemista. Vaikuttaa myös asiakkaan tuottavuuteen.                                  |
| IP        | Internet Protocol, tietoliikenneprotokolla, jossa verkkoliikenne jaetaan paketteihin. Eri laitteet tunnistetaan IP-osoitteen perusteella. [10.]   |
| IPS       | Intrusion Prevention System, järjestelmä, joka havaitsee ja estää haitallisen toiminnan tietoverkossa [11, 2. luku, 1].   |
| ISO 27001 | Standardi, joka määrittelee vaatimuksia tietoturvan hallintajärjestelmille [12].  |
| IT        | Information technology, tietotekniikka.   |
| LDAP      | Lightweight Directory Access Protocol, protokolla, jota käytetään käyttäjätunnistuksessa.   |
| LME       | Log Management Enterprise, Trustwave-yrityksen tarjoama laitteistopohjainen SIEM-tuoteperhe.  |
| MPS       | Messages Per Second, viestiä sekunnissa [13].   |

|         |  |
|---------|--|
| NetFlow | Cisco Systemsin kehittämä protokolla tietoliikenteen seuraamiseen ja keräämiseen verkkolaitteilta [14].  |
| Netstat | Komentorivipohjainen työkalu reititystaulujen ja verkkoliikenteen listaukseksi [15].   |
| Ntop    | Ohjelma, jolla seurataan verkonkäyttöä. Toimii verkkokerroksilla 2 ja 3. [16.]   |
| OE      | Operations Edition, yksi Trustwaven tarjoama SIEM-ratkaisu.  |
| OSI     | Open Systems Interconnection, malli, jossa laitteiden välinen tiedonsiirto jaetaan seitsemään kerrokseen [17].   |
| OSSEC   | Open Source Host-based Intrusion Detection System, avoimen lähdekoodin HIDS-ohjelma.   |
| OSSIM   | Open Source Security information and event management, avoimen lähdekoodin ohjelmisto tietoturvatiedon ja tapahtumien hallintaan.  |
| PCI DSS | The Payment Card Industry Security Standard, maksukorttialan turvallisuusstandardi. Laajasti käytössä oleva standardi, jonka tavoitteena on optimoida maksukorttien käytön turvallisuus. [18.] |
| RAID    | Redundant array of independent disks, tekniikka, jolla saadaan suurempi kapasiteetti, parempi vikasietoisuus tai parempi suorituskyky käyttämällä useita kovalevyjä [19].                      |
| RHEL    | Red Hat Enterprise Linux, yrityskäyttöön tarkoitettu avoimen lähdekoodin Linux-jakelu.   |
| ROI     | Return on Investment, sijoitetun pääoman tuotto. ”Tunnusluku, joka mittaa yrityksen sitomilleen varoille ansaitseman tuoton.” [20.]  |
| Rsyslog | Rocket-fast system for log processing, ohjelmisto nopeaan lokitiedon käsittelyyn. Kykenee välittämään paikallisesti jopa miljoona viestiä sekunnissa. [21.]                                    |
| Samba   | Avoimen lähdekoodin ohjelmisto, jota käytetään tiedosto- tai tulostinjako- palvelimena tai asiakasohjelmana, jolla otetaan yhteyttä näihin verkkojakoihin [22].                                |



|            |  |
|------------|--|
| SELinux    | Security-Enhanced Linux, Linux-ytimen laajennos, jolla järjestelmän ja käyttäjien oikeuksia hallitaan tarkemmin.   |
| SEM        | Security Event Management, yksi osa SIEM-järjestelmästä, johon kuuluu tietoturvatiedon seuranta ja korrelointi.  |
| SIEM       | Security Information and Event Management, tietoturvatiedon ja tapahtumien hallinta.   |
| SIM        | Security Information Management, yksi osa SIEM-järjestelmästä, johon kuuluu aiemman tiedon analysointia ja raportointia.   |
| SLES       | SUSE Linux Enterprise Server, Linux-pohjainen palvelinkäyttöjärjestelmä [23].  |
| SMB        | Server Message Block, Microsoftin verkkoprotokolla tiedostojen jakoon [24].  |
| SNMP       | Simple Network Management Protocol, laajasti käytetty protokolla verkkolaitteiden ja tietokoneiden tarkkailuun [25].   |
| Snmpttrapd | Eräs SNMP-sovellus, joka vastaanottaa SNMP-ilmoituksia ja välittää niitä SNMP-hallintajärjestelmään tai ulkoiselle sovellukselle [25].   |
| SSH        | Secure Shell, salattu protokolla komentorivipohjaista etähallintaa varten.   |
| SYN        | Synchronize, TCP-yhteyden ensimmäinen paketti, jota käytetään yhteyden avaamiseen.   |
| SYN-ACK    | Synchronize Acknowledge, TCP-protokollan kolmivaiheisen kättelyn toinen paketti, joka ilmoittaa lähdelaitteelle SYN-paketin saapumisen.  |
| Syslog     | Protokolla lokitiedon tallentamiseen ja lähettämiseen tietoverkossa [26].  |
| TCO        | Total Cost of Ownership, omistuksen kokonaiskustannus. Sisältää kaikki järjestelmän ylläpidosta ja hankinnasta aiheutuvat suorat ja välilliset kulut. [27.]  |
| TCP        | Transmission Control Protocol, protokolla, joka määrittelee kuinka isäntäkoneiden välinen tiedonsiirto tehdään. Protokolla tekee virheentarkistusta ja varmistaa pakettien välittymisen kolmisuuntaisella kättelymenetelmällä. |

|         |   |
|---------|---|
| Tiketti | Kirjaus huomiota vaativasta palvelupyynnöstä. Tiketille määritetään muun muassa yhteyshenkilö, kiireys, ajankohta ja kuvaus viasta. |
| UDP     | User Datagram Protocol, tiedonsiirtoprotokolla, joka ei varmista tiedon perillepääsyä [28].   |
| USM     | Unified Security Management, AlienVaultin maksullinen SIEM-ohjelmisto.  |

## 1 Johdanto

Tietoturvaan liittyvät ongelmat ja uhat lisääntyvät maailmalla päivittäin. Samalla käsiteltävän tiedon määrä on kasvussa. Tietoturva on nykyään tärkeämmässä asemassa kuin koskaan ennen ja sen merkitys korostuu tulevaisuudessa entisestään. Tämän opinnäytetyön toimeksiantajalla on hallittavana laajamittainen tietojärjestelmä, jota kehitetään jatkuvasti. Tietojärjestelmä tuottaa koko ajan tietoturvaan liittyvää erimuotoista dataa.

Opinnäytetyön toimeksiantaja oli Itä-Suomen yliopisto, joka on yksi Suomen suurimmista yliopistoista. Siellä opiskelee noin 15 000 opiskelijaa ja se toimii työpaikkana 2800 henkilölle. Yliopistolla on kampukset kolmessa kaupungissa, joita ovat Joensuu, Kuopio ja Savonlinna. Yliopistossa opetetaan yli sataa eri pääainetta. Tiedekuntia ovat filosofinen tiedekunta, luonnontieteiden ja metsätieteiden tiedekunta, terveystieteiden tiedekunta sekä yhteiskuntatieteiden ja kauppatieteiden tiedekunta. [29.]

Yliopiston tietotekniikkapalveluilla on käytössä laaja tietojärjestelmä tukemassa nykyaikaista opiskeluympäristöä. Kampusten välillä on useita runkolinkkejä. Verkon aktiivilaitteita yliopistolla on useita satoja ja palvelinympäristössä on yli 250 virtuaalista palvelinta. Yliopiston IT-ympäristössä on noin 32 000 käyttäjätiliä ja noin 6 000 työasemaa. Järjestelmän laajuudesta johtuen laitteilta tulee päivittäin erilaisia tietoturvaan liittyviä raportteja ja lokitietoja, joiden hallinta on työlästä. Laajamittaisen tietoturvatiedon hallinta on haasteellista perinteisin menetelmin, joten toimeksiantaja on kiinnostunut Security Information and Event Management -järjestelmän (SIEM) käyttöönotosta lähitulevaisuudessa. Lokitietoa tulisi kerätä siten, että tapahtuneet tietomurrot voidaan todeta aukottomalla todistusketjulla.

## 1.1 Opinnäytetyön lähtökohdat

Syksyllä 2014 toimeksiantajan kanssa toteutettiin erillisenä kouluprojektina Cactin käyttöönotto verkkoliikenteen valvontaan. Projektin loppuvaiheessa kysyimme toimeksiantajalta opinnäytetyölle aihetta ja SIEM nousi esille keskustelussa. Ennen toimeksiannon vastaanottamista perehdyimme aiheeseen yleisellä tasolla ja tulimme siihen tulokseen, että tästä aiheesta tehtyjä opinnäytetöitä ja tutkimuksia on vähän.

Opinnäytetyön tavoitteena oli tuottaa dokumentaatio, joka auttaa mahdollisen SIEM-järjestelmän valinnassa myöhemmin. Teoriaosuudessa käsiteltiin keskeisimmät käsitteet ja esiteltiin eri valmistajien ratkaisuja. Yksi mukana oleva järjestelmä otettiin tarkempaan tutkintaan, minkä käyttöönotto ja konfigurointi dokumentoitiin teknisellä tasolla. Koko tekninen toteutus tehtiin testiympäristössä eikä sitä opinnäytetyössä viety tuotantokäyttöön.

SIEM on selvästi kasvava trendi ICT-alalla uhkien yleistyessä ja datamäärien kasvaessa. Järjestelmien laajentuessa ja monimutkaistuessa syntyy tietoturvatietoa koko ajan enemmän. Yrityksillä on ydintoiminnan kannalta tärkeää tietoa, jonka tulee säilyttää luottamuksellisuus, eheys ja saatavuus. Tietoturvatiedon käsittelyssä SIEM voi olla hyvinkin ratkaisu toimeksiantajan tapauksessa tai muissa suuremmissa IT-ympäristöissä.

## 1.2 Lähdekriittisyys

Opinnäytetyössä käytettiin useita lähteitä mahdollisimman laajan näkökulman saamiseksi. ICT-ala on nopeasti kehittyvä, joten opinnäytetyössä pyrittiin pääsääntöisesti käyttämään enintään muutaman vuoden vanhoja lähteitä. Vanhemmat lähteet eivät usein kuvasta asioiden nykytilaa.

Ohjelmistojen esittelyä tehtäessä Gartnerin tekemä Magic Quadrant for SIEM -tutkimus oli yksi tärkeimmistä lähteistä. Siinä oli haastateltu yli 500:aa järjestelmien loppukäyttäjää ja tutkittu 24:ää eri toimittajaa [30]. Tutkimuksessa oli arvioitu yrityksiä useista eri näkökulmista.

Opinnäytetyössä käytettyjä SANS-instituutin julkaisuja pidettiin riippumattomina lähteinä. SIEM-järjestelmiä tuottavien yritysten julkaisuja ja teknisiä dokumentteja käytettiin opinnäytetyössä kertomaan ohjelmistojen ominaisuuksista. Tämän tyyppisiin lähteisiin tulee suhtautua kriittisesti. Näiden yritysten julkaisemissa teksteissä pyritään markkinoimaan heidän tuotteitaan kertomalla ainoastaan hyvistä puolista.

Talous- ja ICT-lehtien artikkeleihin viitataan useasti opinnäytetyössä. Lähteiksi valittiin tunnettuja ja laajalevikkisiä lehtiä. Esimerkiksi SC Magazine on tietoturvan liiketoimintaan ja tekniseen tietoon erikoistunut lehti ja yhdysvaltalainen talouslehti The Wall Street Journal toimii kansainvälisesti.

Lähteinä on käytetty useita tietoturva-asiantuntijoiden blogi-kirjoituksia ja esityksiä. Kirjallisuutta aiheesta on saatavilla todella rajatusti. Opinnäytetyön tueksi saatiin tietoturva-asiantuntijoiden kirjoittama Security Information and Event Management (SIEM) Implementation -kirja, jota pidetään opinnäytetyössä luotettavana lähdemateriaalina.

## **2 Yritysten tietoturvaaukat**

Nykyisin yritykset ovat riippuvaisia tietojärjestelmien toiminnasta. Lyhyetkin katkokset tuotantojärjestelmissä voivat aiheuttaa alasta riippuen suuria kustannuksia joko tuotannon pysähtymisenä, tärkeän tiedon menetyksenä tai tietovarkautena. Tietosuojatason täytyy olla erittäin korkea käsiteltäessä henkilö- tai pankkitietoja tai yrityssalaisuuksia. Tietoturvaaukien määrä kasvaa maailmalla jatkuvasti ja uusia hyökkäystapoja kehitetään koko ajan lisää. [31, 20–21.]

Yrityksen työntekijät ovat usein suuri tietoturvaauka. Verizonin tekemässä tutkimuksessa käy ilmi, että 98 prosentissa tapauksista ulkoinen tekijä vaikuttaa murtoon [32, 3]. Työntekijän tahallinen tai tahaton virhe mahdollistaa usein murron varsinaiselle ulkoiselle hyökkääjälle.

Tutkimuksessa todetaan kolmannen osapuolen havaitsevan 92 % onnistuneista murroista viikkojen tai kuukausien jälkeen tapahtuneesta. Tyypilliset hyökkäykset ovat yksinkertaisia ja helposti vältettävissä pienillä toimenpiteillä. [32, 3.]

Ulkoverkosta hyökätään jatkuvasti yrityksiin. Hyökkäysten taso vaihtelee yksittäisistä porttiskannauksista ammattilaisten suorittamiin verkkohyökkäyksiin. Automatisoituja hyökkäyksiä on paljon helpompi havaita suuren verkkoliikennemäärän takia kuin ihmisten suorittamia kohdistettuja hyökkäyksiä. Ulkoisia uhkia on helpompi estää kuin sisäverkosta tapahtuva väärinkäytöksiä. Yleisellä tasolla yrityksen sisäisiä ongelmia vähennetään rajaamalla työntekijöiden pääsyoikeuksia vain heidän tarvitsemiinsa resursseihin, kouluttamalla tietoturvatietoutta ja seuraamalla lokitietoja, joista ongelmat voidaan havaita. [31, 23–25.]

Uusi yrityksiä kohtaan tuleva advanced persistent threats -tietoturvauhka (APT) on erittäin hankala havaita. Tavallisissa verkkohyökkäyksissä yritetään murtaa mahdollisimman monia yrityksiä työkaluilla, jotka luovat paljon liikennettä. APT-hyökkäyksen erona on se, että kohteena on yleensä tietty yritys, johon on tavoitteena saada pitkäaikainen ja huomaamaton yhteys. Tämäntasoiset hyökkäykset ovat monimutkaisia ja vaativat kuukausien suunnittelun. Vähäisen verkkoliikennemäärän takia haitallisen liikenteen huomaaminen on haastavaa. [2.]

Hyökkäykset alkavat tiedonkeruulla, jolloin esimerkiksi kohteen yhteistyökumppaneilta voidaan saada hyödyllistä tietoa. Erilaisilla tiedonkalastelutekniikoilla saadaan selville käyttäjätunnuksia ja salasanoja tai ujutetaan haittaohjelma yrityksen verkkoon haitallisen liitetiedoston mukana. Tämän jälkeen hyökkäystä jatketaan hitaasti syvemmälle yritykseen. Kerättyä tietoa lähetetään ulos yrityksestä esimerkiksi piilottamalla se muuhun verkkoliikenteeseen. Hyökkäyksen havaitsemiseksi on tärkeä seurata ympäristön lokitietoja, mihin SIEM-järjestelmän lokienkeräys- ja korrelointiominaisuudet soveltuvat hyvin. [2.]

ENISAn selvityksen mukaan suurimman tietoturvauhan vuonna 2014 muodostivat madot ja troijalaiset. Haittaohjelmien dynaamisuuden ja monimuotoisuuden takia 50 % niistä jää huomaamatta virustorjuntaohjelmilta. [33, 14] Liitteessä 1 on listattu ENISAn selvityksen 15 merkittävintä tietoturvauhkaa.

Ohjelmistovalmistajat korjaavat haavoittuvuuksia julkaisemalla päivityksiä käyttöjärjestelmille ja ohjelmistoille. Virustorjuntaohjelmistojen toiminta perustuu tietokantoihin, jotka on päivitettävä säännöllisesti uusien haittaohjelmien löytämiseksi. Estämällä edellä mainitut päivitykset hyökkääjä voi edelleen hyväksikäyttää samoja haavoittuvuuksia. Usein hyökkääjä asentaa haitallisia palveluja tai ohjelmistoja kohdejärjestelmille ja ottaa palomuurin pois käytöstä. Näillä toimenpiteillä hyökkääjä mahdollistaa pääsyn sisäverkkoon myös jatkossa ja pystyy vähitellen murtautumaan syvemmälle järjestelmään. [31, 29–32.]

SIEM-järjestelmällä on mahdollista havaita saastuneet koneet verkosta. Hyökkääjä on kuitenkin voinut estää näiden koneiden yhteyden SIEM-palvelimeen, jolloin tieto hyväksikäytöstä ei välity eteenpäin. Tätä varten on määriteltävä hälytykset, mikäli se ei vastaanota lokitietoja seurattavilta laitteilta tietyn aikavälin sisällä. [31, 30.]

### 3 Security information and event management

Eri verkkolaitteilta sekä palvelimilta saatavat lokitiedot auttavat mahdollisten hyökkäysten tai muiden järjestelmäongelmien etsimisessä. Kuitenkin laitemäärien kasvaessa hyödyllisen tiedon löytäminen valtavasta tietomäärästä on ongelmallista. Nopeasti kasvavan tietoturvatiedon ja tapahtumien hallintaan on ratkaisuna security information and event management. Ensimmäiset SIEM-toimittajat aloittivat vuonna 1996 [34].

Vaikka SIEM-markkinat ovat kasvaneet jo jonkin aikaa, on standardointi hyvin vähäistä. Yritysten julkaisuista on pääteltävissä, että ne pitävät menetelmänsä salaisina menestyäkseen markkinoilla. Ohjeistukset ja julkaisut on usein kerrottu yleisellä tasolla tai epämääräisesti. Tekniset dokumentaatiot sisältävät todella vähän johdonmukaista luotettavaa tietoa ja tekniset yksityiskohdat ovat niukkoja. [35, 9.]

SIEM-järjestelmät soveltuvat hyvin tietoturvan raportointiin ja ohjeistuksen mukaiseen toimintamalliin. Teknologian avulla on mahdollista tarkkailla yrityksen sisäisiä ja ulkoisia tietoturvauhkia joustavasti. Hyvin toteutetut ratkaisut parantavat tietohallinnon toimintatehokkuutta ja vähentävät hallinnollisia kuluja. [36.]

SIEM-järjestelmän implementointi on haasteellista. Teknologia on monimutkaista ja markkinasegmentti on jatkuvassa muutostilassa, jonka takia yhteistyö toimittajien välillä ei ole välttämättä pysyvää. Haasteita eri ratkaisujen tuottajille aiheuttavat monimutkaisen teknologian vaatima korkeatasoinen tekninen osaaminen, yhteistyökumppaneiden kouluttaminen ja sertifiointit. [36.]

### 3.1 SIEM liiketoiminnan näkökulmasta

SIEM-markkinat kokonaisuudessaan olivat vuonna 2014 arvoltaan noin 2,57 miljardia dollaria ja sen odotetaan kasvavan 4,54 miljardiin dollariin vuoteen 2019 mennessä. [37] SIEM on ICT-alalla selvästi kasvava trendi ja tulee yleistymään lähitulevaisuudessa.

Ennen järjestelmän hankkimista on hyvä arvioida saatavia hyötyjä liiketoiminnallisesta näkökulmasta. Hyvin toteutetulla järjestelmällä on mahdollisuus tehdä suuria taloudellisia säästöjä parantamalla tehokkuutta automatisoinnilla. Tietomurrot ja petokset aiheuttavat yrityksille mittavia kuluja, joiden estäminen on yrityksen talouden ja maineen puolesta erityisen tärkeää. Henkilöstökuluissa on mahdollista tehdä säästöä tietoturvatiedon käsittelyn yksinkertaistuksessa. [38] Toisaalta järjestelmän käyttöönotto vaatii monihenkisen työryhmän ja aiheuttaa samalla merkittäviä henkilöstökuluja projektin aikana.

Sijoitetun pääoman tuoton (ROI) sijaan SIEM:issa kannattaa arvioida hyödyllisyyttä kulojen välttämisen näkökulmasta. Järjestelmän avulla on mahdollista välttää tietomurrosta aiheutuvia suuria kuluja, mikä kompensoi järjestelmän kallista hintaa. [31, XXXI.]

Tietoturvasta aiheutuvista kustannuksista voidaan tehdä kahtiajako. Kuluja aiheuttavat uhkilta suojautuminen ja toisen puolen tekevät toteutuneiden uhkien aiheuttamat kustannukset. Ihannetilanne saavutetaan optimoimalla tietoturvan taso suhteessa tiedon arvoon. [39.]

Tietomurrosta johtuva järjestelmän alhaallaoloaika aiheuttaa välittömiä ja välillisiä kuluja yritykselle. Hyvin toimivan SIEM-järjestelmän avulla on mahdollista ennakoivasti estää tietomurroista johtuvia katkoksia yrityksen tietojärjestelmissä. Itä-Suomen yliopiston tapauksessa ICT-palveluissa aiheutuvat katkokset rajoittaisivat laajasti opettamisen ja tutkimustyön järjestämistä. Nykymuotoinen opetus vaatii lähtökotaisesti taustalle aina toimivan IT-järjestelmän ja verkkoyhteydet. Alla on lainaus aiheesta Digitoday-verkkolehdestä.

Gartner Dataquestin tutkimuksen mukaan 12 prosenttia yrityksistä laskee tunnin katkoksen maksavan yritykselle alle 25 000 dollaria. Toisaalta viisi prosenttia yrityksistä ilmoittaa katkoksen kustannusarvioiksi yli 2,5 miljoonaa dollaria jokaista tuntia kohden. Yritykset eivät välttämättä edes hahmota kaikkia tietoturvauhkien toteutuessaan aiheuttamia potentiaalisia kustannuksia. Yritys saattaa menettää jopa asiakkaitaan tietomurron aiheuttaman negatiivisen imagon myötä. Asiakkaan tai yhteistyökumppaneiden luottamuksellisten tietojen vuotaminen tietoturvamurron seurauksena saattaa johtaa mittaviin vahingonkorvauksiin. [39.]



Taloudellisten hyötyjen ohella SIEM tuottaa myös muita hyötyjä. Tietojärjestelmän yleistä tilaa on helpompi tarkkailla raporttien avulla. Huomiota vaativien tapausten korjaaminen on helpompaa priorisoida ja tietoturvaan liittyvistä prosesseista tulee johdonmukaisempia sekä hallittavampia. [38.]

Kustannuksia SIEM-järjestelmässä tulee muustakin kuin sen hankinnasta. Liimatainen ja Sarjakivi Nixu-yrityksestä jaottelevat sen omistamisen kokonaiskustannukset (TCO) neljään osaan, jotka ovat järjestelmä, projekti, ylläpito ja reagointi (kuva 1). [40.]



Kuva 1. SIEM-ratkaisun TCO [40]

SIEM:n määritelmä ja toiminnot eivät ole yksiselitteisiä. Jokaisella valmistajalla on omanlaisensa kokoelma toimintoja heidän ratkaisuissaan. Järjestelmän hankinta vaatii asiakkaalta hyvää tietoteknistä koulutusta ja osaamista määrittääkseen yhteensopivuuden ja skaalautuvuuden omaan ympäristöön. Näiden ratkaisujen yleistymistä hidastaa vaikeus arvioida sijoitetun pääoman tuottoa. SIEM-järjestelmät ovat pienille ja keskisuurille yrityksille usein liian monimutkaisia ja kalliita. [41.]

SIEM-järjestelmän hankinta ja käyttöönotto eivät automaattisesti tuo hyötyjä ja tehosta yrityksen IT-toimintoja. Huonosti toteutettu SIEM aiheuttaa yritykselle mittavia kustan-

nuksia. Useiden kaupallisten ratkaisujen hinnat vaihtelevat kymmenien- ja satojentuhansien eurojen välillä. Toisaalta itsetoteutettu käyttöönotto vie huomattavan määrän työaikaa ja vaatii erityisosaamista. Mikäli ratkaisusta ei saada ymmärrettävää tietoturvatietoa ulos huonosti toteutetun käyttöönoton vuoksi, investoitu raha ja työaika menevät hukkaan.

### **3.2 SIEM-projekti**

SIEM on mahdollista toteuttaa ohjelmisto-, laite- tai palvelupohjaisena ratkaisuna. Käyttöönottoa suunniteltaessa kannattaa tarkasti miettiä, mikä ratkaisu sopii parhaiten omiin tarpeisiin. Projektin toteutuksessa ei pysty täysin soveltamaan perinteisiä projektimalleja, joissa toteutus viedään kerralla alusta loppuun. Ennen projektin aloittamista on hyvä tiedostaa vaadittu työmäärä. Projektin läpivienti ja järjestelmän ylläpito vaatii monen työntekijän täyden työpanoksen.

Käyttöönotot epäonnistuvat monesti organisaatioiden aliarvioidessa ylläpitoon vaadittavia resursseja. Vaikka resursseja olisi tarpeeksi saatavilla, ongelmia ilmenee huonon suunnittelun seurauksena. Organisaatiot pyrkivät yleensä lähettämään kaiken mahdollisen lokitiedon kerralla SIEM-järjestelmään. Tästä seuraa kuitenkin usein valtava määrä virheellisiä havaintoja (false positive). [42.]

Yrityksessä SIEM ei ainoastaan kosketa IT-osastoa. Yhteistyötä vaaditaan yrityksen korkeamman johdon, talousosaston, HR:n sekä riskienhallinnasta ja sääntelystä vastaavien tahojen kanssa. Kaikkien osapuolten täytyy hyväksyä SIEM:n käyttöönotto. Projektille täytyy määrittää ohjausryhmä, joka koostuu eri osastojen edustajista. [43.]

Projekti on hyvä viedä läpi pienissä osissa. Perinteisellä suunnittelulla koko järjestelmä rakennetaan alusta loppuun kerralla, jolloin projekti viivästyy ja jämähtää helposti lokien keräilyyn. Tällöin budjetti venyy ja organisaation luottamus SIEM-järjestelmää kohtaan hiipuu heti alussa projektin laajuuden takia. [44] Ei ole merkityksellistä kerätä heti kaikista mahdollisista lähteistä lokitietoa ja miettiä vasta sitten kuinka niitä analysoidaan. Tärkeämpää on saada merkityksellistä dataa käsiteltäväksi pienissä osissa ja tehdä niille oikeat analysointimääritykset.

Käyttöönotossa tulisi keskittyä enintään viidestä seitsemään käyttökohteeseen ensimmäisen kuuden kuukauden aikana. Projektille tulee määrittää selkeä rajausta ja monitoroitavat

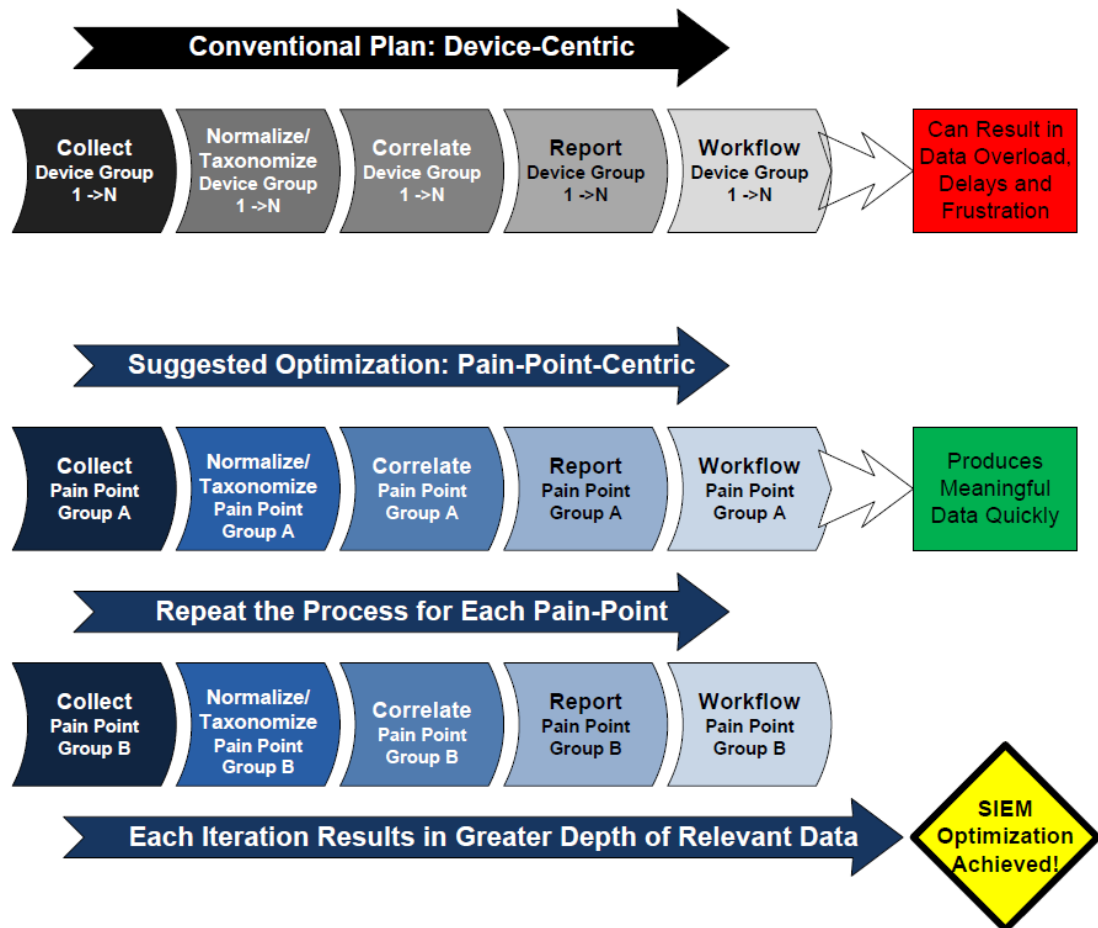
tietolähteet tulee määrittää tarkasti. Hallintapaneelin ja raporttien määrittäminen tulee kiinnittää huomiota. [42] Onnistumisen myötä projektin laajuutta voi varovasti kasvattaa.

Projekti aloitetaan arvioimalla IT-järjestelmän ja tietoturvan nykytila. Tiedossa olevat tietoturvaongelmat tulee korjata ennen varsinaisen toteutuksen aloittamista. Eri järjestelmien kriittisyys tulee määrittää ja priorisoida tärkeimpien järjestelmien kytkeminen SIEM-järjestelmään ensimmäiseksi. [43.]

Seuraavaksi tulee yksinkertaistaa IT-ympäristöä mahdollisimman paljon tietoturvan näkökulmasta. Ylimääräiset monimutkaisuudet tuottavat turhaa tietoa SIEM-järjestelmässä ja aiheuttavat vääriä hälytyksiä. Panostamalla tähän vaiheeseen säästyy varsinaisessa konfiguroinnissa turhalta vaivalta. [43.]

Kolmannessa vaiheessa hienosäädetään IT-ympäristössä olevia IPS- ja IDS-laitteita tuottamaan mahdollisimman vähän tarpeettomia hälytyksiä. Nämä laitteet tuottavat valtaosan kaikista hälytyksistä ja kustannuksista suuri osuus riippuu käsiteltyjen tapahtumien määrästä. [43.]

Neljännessä eli käyttöönottovaiheen alussa tulee tarkastella SIEM:n soveltuvuutta vastaamaan yrityksen liiketoimintamalleja. Varsinainen toteutus viedään läpi pienissä osissa. [43] Tarkkailtavat ongelmat (Pain Point) tulee ryhmitellä. Jokaisen kohdan osalta käydään järjestelmällisesti läpi normalisointi, korrelointi, raportointi ja työnkulun määrittely. Tällä menetelmällä saadaan nopeasti merkityksellistä tietoa SIEM-järjestelmään pienissä paloissa ja projekti etenee sujuvammin. Vastaavanlainen prosessi toistetaan kuvan 2 mukaisesti kaikille kohdille, minkä jälkeen järjestelmä paranee jokaisella kerralla. [44.]



Kuva 2. SIEM:n käyttöönoton optimointi [44]

Pivot Point Security -yrityksen mukaan projektin työ jakautuu karkeasti neljään kategoriaan. Vaatimusmäärittelylle ja järjestelmäarkkitehtuurin yksityiskohtaiselle suunnittelulle varataan 25 % työmäärästä, järjestelmän rakentamiselle ja testaukselle 40 % sekä järjestelmän rasiustestaukselle ja integroinnille 20 %. Loput 15 % varataan raportoinnille. [44.]

Laaja SIEM-järjestelmä, jossa on noin 400 miljoonaa tapahtumaa päivässä, vaatii optimaaliseen käyttöön ylläpidolta noin 12 henkilötyöpäivää kuukaudessa. Työ jakautuu Taulukko 1 mukaisesti. [44.]

Taulukko 1. Työmäärän jakautuminen SIEM-järjestelmän ylläpidossa [44]

| Työn osa-alueet ylläpidossa   | Työmäärä, % |
|-------------------------------|-------------|
| Tietokannan hallinta          | 15          |
| Järjestelmän hallinta         | 10          |
| Erilliset tutkimukset         | 20          |
| Raporttien luonti ja muuntelu | 25          |
| Agenttien kehittäminen        | 15          |
| Tuki muutoksille              | 15          |

IT-ympäristöt elävät koko ajan ja muutoksia tulee jatkuvasti. Jokainen ympäristöön tehty muutos vaikuttaa potentiaalisesti SIEM-järjestelmään ja vaatii siihen tehtäväksi tarvittavat muutokset. Esimerkiksi päivitykset laitteissa, joista lokitietoa kerätään, voivat vaikuttaa tapaan, jolla SIEM keskustelee laitteiden kanssa. [44] Järjestelmä ei ole koskaan täysin valmis, vaan sen tulee muuttua koko ajan IT-ympäristön mukana.

### 3.3 SIEM-tekniikat

SIEM-ohjelmistojen tarkoituksena on keskittää lokitietojen hallinta sekä mahdollistaa eri laitteilta saatavien tietojen korrelointi keskenään. Tällöin työajasta käytetään vähemmän aikaa lokien seurantaan ja pystytään keskittymään ongelmien ratkomiseen. Hyökkäys voi jäädä havaitsematta seurattaessa yksittäisen verkkolaitteen toimintaa. Ristiinkorreloidessa esimerkiksi palomureja, palvelimia ja LDAP-protokollaa saadaan tarkempi kuva hyökkäyksestä. [45, 8] Tietoturvatiedonkulku SIEM-järjestelmässä on kuvattu kaaviolla liitteessä 2.

SIEM-järjestelmässä yhdistyy SIM- ja SEM-ohjelmistojen ominaisuudet. SIM-osa kerää lokitietoja eri verkkolaitteilta, minkä pohjalta se luo raportteja. SEM ristiinkorreloi kerättyä tietoa ja analysoi sitä. Tämä voidaan myös määrittää ilmoittamaan automaattisesti, mikäli määritetty tapahtuma ilmenee. Ohjelmistoissa yleensä on valmiiksi määritettyjä sääntöjä, joiden perusteella tietoa analysoidaan. Kuitenkaan nämä eivät välttämättä toimi eri ympäristöissä. Tämän takia eri tilanteita varten luodaan omia sääntöjä, joita kehitetään jatkuvasti. [46.]

### 3.3.1 Tiedon kerääminen

SIEM-ohjelmiston pääasiallinen tarkoitus on kerätä lokitietoja, mutta tämän lisäksi ohjelma voi seurata esimerkiksi SQL-kyselyjä tai verkkoliikennettä. Tietoa kerätään useilta erilaisilta laitteilta kuten palomureilta, kytkimiltä, ohjelmistoilta, palvelimilta sekä reitittimiltä. [47.]

Lokitiedon keräämiseen on kaksi päätapaa. Yksi vaihtoehto on asentaa seurattavalle laitteelle agenttiohjelma. Tämä seuraa laitteen tietoja ja lähettää ne SIEM-ohjelmistolle. Agentit pystyvät hyödyntämään kerättyä tietoa kattavasti, mutta niissä on suuri ylläpityö. Suurissa järjestelmissä asennukseen kuluu paljon aikaa, koska jokaiselle laitteelle agenttiohjelma asennetaan erikseen. Nämä ohjelmistot lisäävät myös tietoturvariskejä, koska ne tarvitsevat järjestelmävalvojan oikeudet kohdelaitteella. [47.]

Toinen vaihtoehto on käyttää valmiita verkkoprotokollia lokitiedon siirtämiseen. Käytettäviä tiedonsiirtoprotokollia ovat esimerkiksi syslog, NetFlow ja SNMP. Tässä tapauksessa kohdejärjestelmään ei tarvitse asentaa agenttiohjelmistoa, joka tuo lisäkuormaa ja tietoturvariskejä laitteelle. Myös järjestelmän ylläpitykuorma vähenee. [47] Protokollien välillä on eroja tietoturvan ja tiedon todentamisen suhteen, mikä on otettava huomioon suunniteltaessa käyttöönottoa.

Syslog-protokolla on yleisesti käytössä oleva standardi lokitiedon tallentamiseen ja sen lähettämiseen keskitettyyn lokivarastoon [31, s.56]. Oletuksena syslog käyttää UDP-yhteyttä, joka ei varmenna tiedon saapumista kohdepalvelimeen. Uusissa syslog-palvelimissa on mahdollista ottaa myös TCP-yhteys käyttöön. [31, s.73]. Tämä on suositeltavaa, koska UDP-protokollan käyttäminen aiheuttaa ongelmia esimerkiksi verkkohyökkäyksen aikana, jolloin verkkoa kuormitetaan paljon. Tällöin tärkeää hyökkäykseen liittyvää tietoa voi jäädä matkalle.

Kerätty tieto yhdistetään keskitettyyn järjestelmään, jossa sitä analysoidaan. Järjestelmän hajauttaminen useampaan osaan vähentää yksittäisen laitteen kuormaa. Agenttiohjelmit voivat kerätä tietoa laitteilta ja siirtää sitä vähitellen SIEM-järjestelmään. Keskitetty järjestelmä vaatii kokonaisuudessaan paljon laskentatehoa, koska nykyaikaisen tietojärjestelmän lokimäärät ovat valtavia. Tämä rasittaa myös tietoverkkoja. [48.]

Lokitiedon keräyksen syynä on tietoturvan parantaminen, kuten hyökkäysten havaitseminen ja yleinen tietoverkon tapahtuminen seuranta. Lisäksi säännökset voivat määrätä lokitiedon keräämisen tietyltä aikaväliltä. Turhien kohteiden seuraaminen lisää vain SIEM-

järjestelmän kuormitusta ja hallintaan menevää aikaa. Samalla tärkeää tietoa ei välttämättä huomata turhan informaatiovirran seasta. [31, 81.]

Aluksi tulee suunnitella tarkasti tärkeimmät kohteet, joista tieto kerätään. Laitteet on hyvä luokitella tärkeyden perusteella, jolloin voidaan jättää turhat kohteet kokonaan pois. Seuraamalla laitteiden lokitietojen kokoa voidaan laskea tarvittavan levytilan määrä. Lopuksi on päätettävä tarvitaanko reaaliaikaista tapahtumatietoa vai riittääkö jälkeinpäin suoritettava analysointi. Nämä tiedot eivät kuitenkaan anna todellisia laitteistovaatimuksia SIEM-järjestelmälle, koska kokonaisuuteen vaikuttaa moni muukin asia. Esimerkiksi tietomurtojen aikana lokitietoa tulee valtava määrä, joten laitteiston täytyy kestää laskettua arvoa suurempi kuorma. [31, 80–81.]

### 3.3.2 Normalisointi

Normalisoinnin tarkoitus on yhdenmukaistaa eri lähteistä saatava tieto. Ylimääräinen data voidaan tallentaa omaan tietovarastoon mahdollista myöhempää analysointia varten [48]. Ongelmana normalisoinnissa on se, että kaikki laitteet tai ohjelmistot eivät ole yhteensopivia, koska eri valmistajilla on erilainen tapa tuottaa lokitietoa. On myös mahdollista, että aikaisemmin yhteensopivalta tuotteelta ei päivityksen jälkeen saada enää tietoja tai osa tiedoista jää keräämättä. [49.]

Constantine esittää normalisoinnista esimerkkinä onnistuneen kirjautumisen. Lokitieto jakautuu tapahtumaan, lähteen IP-osoitteeseen ja käyttäjätunnukseen. [50, 5] Alkuperäisen lokitieto on alla olevassa muodossa.

```
Successful Login from 192.168.100.2 to account "Admin"
```

Normalisoinnin jälkeen eri tapahtumat jaoteltiin omiin kenttiin yhden tekstirivin sijaan. Nyt tieto on helposti etsittävässä ja lajiteltavissa eri kenttien perusteella. Korrelointi ei ole mahdollista ilman tätä toimenpidettä. [50, 5] Normalisoitu tapahtuma on alla olevassa muodossa.

```
Event: Successful Login  
SrcIP: 192.168.100.2  
User: Admin
```

Seurattavilla laitteilla tulee olla oikeat aika- ja päivämääräasetukset. Väärät ajat laitteissa vähentävät tiedon luotettavuutta merkittävästi. Väärällä aikaleimalla olevia tapahtumia ei voida myöhemmin jäljittää ja tiedosta tulee täten merkityksetöntä.

Lokitietoa tuottavia sovelluksia on olemassa valtava määrä eikä lokitiedon keräämiseen ole käytössä yleistä standardia. Kuitenkin HP:n kehittämä Common Event Format on useiden valmistajien käyttämä tapa tuottaa lokitietoa, mutta se on edelleen melko marginaaliasemassa. [49.]

### 3.3.3 Tiedon korrelointi

Verkkohyökkäyksiä on hankala havaita seuraamalla yksittäisen kohteen lokitietoja, mutta yhdistämällä tietoa useista eri lähteistä pystytään havaitsemaan melko huomaamattomia-kin hyökkäyksiä. Tämän takia SIEM-järjestelmän tärkeä ominaisuus on useiden eri lähteiden välisen tiedon korrelointi. [51.]

Ristiinkorreloinnissa tapahtumatietoa yhdistetään eri laitteilta ja tulkitaan sitä määriteltujen sääntöjen perusteella. Ohjelmistossa on valmiita sääntöjä, joita käytetään verkkohyökkäysten tai väärinkäytösten havaitsemiseen, mutta monesti ne eivät riitä kaikkiin yrityksen tarpeisiin. Sääntöjä voi luoda itse, mutta niiden ymmärtäminen vaatii paljon asiantuntemusta tietoturvasta. Korrelointisääntöjen kanssa kannattaa olla tarkkana, koska mitä yleispätevämpiä säännöt ovat, sitä enemmän ilmenee vääriä hälytyksiä. Taas liian yksityiskohtaiset säännöt eivät havaitse hyökkäyksiä kunnolla. Sääntölistojen kasvaessa lisääntyy prosessointikuorma. [51.]

Korrelaatio-sääntöjen suunnittelussa tulee ottaa huomioon se, että tapahtumasarja vaihtelee eri hyökkäysten välillä. Pelkkä tapahtumasarjan kuvaaminen ei riitä verkkohyökkäysten havaitsemiseen, vaan peräkkäisille tapahtumille on määriteltävä aikaikkuna, jonka välillä ne tapahtuvat. Sääntöjen suunnittelu on aikaavievää ja sääntöjä täytyy jatkuvasti kehittää tietoturvan edistämiseksi. [51.]

Lane esittää yhtenä hyökkäysesimerkkinä tapauksen, jossa hyökkääjä aluksi etsii julkisia palvelimia esimerkiksi porttiskannerilla. Mikäli palvelimia havaitaan, niitä vastaan hyökätään tunnetuilla haavoittuvuuksilla. Jos hyökkäyksen avulla murtaudutaan palvelimelle, sinne luodaan uusi käyttäjä, jonka avulla voidaan päästä sisälle yritysverkkoon. [51.]

Yksittäisten lokien seuraamisella hyökkäys olisi jäänyt havaitsematta. Palomuurin huomaa porttiskannaukset, mutta näitä tapahtuu internetissä jatkuvasti eikä sen perusteella voi todeta tietomurtoa. IDS- ja IPS-laitteet havaitisivat haavoittuvuuksien hyväksikäytön ja palvelimen lokitiedoissa näkyvä uuden käyttäjän lisääminen. Vasta yhdistämällä kaikki



tämä tieto saadaan todellisempi kokonaiskuva onnistuneesta hyökkäyksestä ja se voidaan estää. [51.]

### **3.3.4 Monitorointi**

SIEM-järjestelmää hallitaan joko web-pohjaisesti tai ohjelmalla, joka on asennettu tietokoneelle. Tämä on käyttöliittymä, jonka kautta suurin osa järjestelmän hallinnasta tapahtuu. Samaa sovellusta käytetään myös kerätyn tiedon tutkimiseen. [31, 91] Monien valmistajien tuotteissa on mukautettava yleisnäkymä, josta nähdään kerralla kokonaiskuva IT-ympäristön tietoturvatilasta.

Kerätty data on tarkasteltavissa selkeinä kuvaajina, normalisoituna tekstinä tai raakalokina. Normalisoinnin ansiosta tietoa on mahdollista suodattaa eri hakuheitojen perusteella. Järjestelmässä olevasta tiedosta on mahdollista luoda valmiita raportteja. Eri SIEM-tuotteilla on vaihtelevat raportointivalmiudet. Osassa järjestelmistä on valmiina eri standardien mukaiset raporttimallit. Näitä ovat esimerkiksi ISO 27001 ja PCI DSS.

### **3.3.5 Hälytykset**

Pelkkä tiedon analysoiminen ei auta parantamaan tietoturvan tasoa eikä estämään hyökkäyksiä. Ilman hyvää hälytysjärjestelmää tietoturvasta vastaava henkilöstö ei saa ajoissa ilmoituksia hyökkäyksistä, jolloin tietoturvahukat voivat jäädä havaitsematta. Hyökkääjä voi varastaa yrityssalaisuuksia tai tehdä tuhoja järjestelmän sisällä. Hyökkäyksiä on hankala, ellei mahdoton havaita ilman hyvää lokien seuranta.

Eri SIEM-ohjelmistojen ilmoitusasetukset vaihtelevat. Kriittiset hälytykset, kuten tietoturvahyökkäykset, ilmoitetaan suoraan sähköpostilla tai tekstiviestillä, mikä nopeuttaa IT-henkilöstön reagoimista ongelmiin. Vähemmän tärkeitä ilmoituksia tarkkaillaan suoraan hallintakäyttöliittymästä tai lähetetään ilmoitus tiketointijärjestelmään. [51.]

## **3.4 SIEM:n laskennalliset vaatimukset**

SIEM-järjestelmän suorituskykyä on mahdollista arvioida numeerisesti. Mittareiden käyttäminen on hyödyllistä valittaessa järjestelmää ja arvioitaessa sen toimintaa. Esimerkiksi tuotetuille lokeille varattua kokonaistilaa mitataan gigatavuina. [52.]

Käytettyjä resursseja mitataan suorittimen käyttöasteella, muistin- ja levytilankäytöllä. Kohteiden seuraaminen tuottaa myös verkkoliikennettä, jota voidaan mitata esimerkiksi avoimena olevien TCP-yhteyksien lukumäärän ja käytetyn kaistan mukaan. [52.]

SIEM-järjestelmän tuottamien hälytysten määrää mitataan ajan, kohteen, tyyppin tai säännön mukaan. Hälytysten käsittelymäärä lasketaan analysoijan, säännön ja kohteen mukaisesti. [52.]

Tietoturvatapahtumien muodostamien tapausten (incident) määrää mitataan aikayksikön, analysoijan tai kohteen mukaan. Yksi tärkeimmistä mittareista on reagointiaika tapauksille. Tällä tarkoitetaan aikaa, joka kuluu hälytyksestä tapaukseen reagointiin ja reagoinnista tapauksen ratkaisemiseen tai eskalointiin jatkotutkimusta varten. [52.]

Useat SIEM-järjestelmät sisältävät tiketöintityökalun. Tikettien muodostumista ja ratkaisuaikoja seuraamalla saa käsityksen järjestelmän toiminnan tehokkuudesta. Tämä edellyttää, että tiketöinti hoidetaan asianmukaisesti.

EPS-arvolla viitataan ohjelmiston kykyyn käsitellä tietty määrä tietoturvaan liittyviä tapahtumia sekunnin aikana. Yksittäinen tietoturvaan liittyvä tapahtuma voi olla esimerkiksi tieto käyttäjän kirjautumisesta järjestelmään. Arvosta on mahdollista laskea keski- ja maksimiarvo. [52.]

Eri valmistajat laskevat EPS-arvon eri tavalla, joten valmistajien ilmoittamat arvot eivät välttämättä ole vertailukelpoisia keskenään. Yhdellä valmistajalla EPS-arvon tapahtumilla viitataan havaittuihin, toisella vastaanotettuihin ja kolmannella prosessoituihin tapahtumiin. Myös tapahtumien koko vaihtelee. Yleensä EPS-arvossa valmistajat käyttävät pienikokoisia tapahtumia laskemiseen. Valmistajien ilmoittamia arvoja tulee tutkia kriittisesti, sillä valmistajat ilmoittavat sen arvon, jolla heidän tuotteensa suoriutuvat parhaiten. [53.]

EPS-arvon lisäksi valmistajat käyttävät myös EPD-arvoa (Events Per Day). EPD-arvo lasketaan EPS-arvon pohjalta kaavan 1 mukaisesti. [54.]

$$\frac{E}{s} = EPS \quad (1)$$

$$EPS * 86400 = EPD$$

missä  $E$  = Tapahtumien lukumäärä

$s$  = Aika sekunteina

EPS = Tapahtumaa sekunnissa

EPD = Tapahtumaa vuorokaudessa

Tuotantojärjestelmän yhteenlasketun hetkellisen maksimitapahtumamäärän (Peak number of security events) laskentaa helpotetaan käyttämällä  $PE_x$ -arvoa, joka kuvastaa identtisten laitteiden tuottamaa yhteenlaskettua tapahtumamäärää.  $PE_x$  saadaan laskettua kaavan 2 avulla. Liitteessä 3 on mainittu tyypillisiä EPS-keskiarvoja eri laitteille. [55.]

$$n_{laitteet} * EPS_{laitetyyppi\ x} = PE_x \quad (2)$$

missä  $n_{laitteet}$  = Tietyn tyyppisten laitteiden lukumäärä  
 $EPS_{laitetyyppi\ x}$  = Tietyn laitetyypin EPS-arvo

Kaikkien laiteryhmiä PE-arvot lasketaan yhteen kaavalla 3 [55].

$$(PE_1 + PE_2 + \dots + PE_n) = Summa_1 \quad (3)$$

missä  $PE_1$  = Ensimmäisen laitetyyppiryhmän EPS-arvo  
 $PE_2$  = Toisen laitetyyppiryhmän EPS-arvo  
 $PE_n$  = Viimeisen laitetyyppiryhmän EPS-arvo  
 $Summa_1$  = Kaikkien laitteiden EPS-summa

Laskettuun summaan tulee lisätä kymmenen prosenttia, että arvio laitteen tuottamasta tapahtumamäärästä ei varmasti ole alimitoitettu. Järjestelmän kasvuvaralle lasketaan lisäksi vielä toiset 10 % (kaava 4). [55.]

$$\begin{aligned} Summa_1 + (Summa_1 * 10\%) &= Summa_2 \\ Summa_2 + (Summa_2 * 10\%) &= PE_{yhteensä} \end{aligned} \quad (4)$$

missä  $Summa_1$  = Kaikkien laitteiden EPS-summa  
 $Summa_2$  = Varmuuskertoimella kasvatettu EPS-summa  
 $PE_{yhteensä}$  = Kasvu- ja varmuuskertoimella kasvatettu EPS-summa

Tiedon varastointiin vaadittava vuotuinen tilantarve on hyvä laskea SIEM-järjestelmän suunnitteluvaiheessa. Tällöin pystytään suunnittelemaan järjestelmävaatimukset yrityksen tarpeiden mukaan.

Tilantarpeen laskemiseen käytetään EPD-arvoa. Saatu tulos jaetaan pakkauksen määrällä (kaava 5). Normalisoidut tiedot tarvitsevat yli kaksi kertaa enemmän levytilaa. [54] Compress-muuttujalle määritetään pakkaussuhde. Esimerkiksi, jos pakattu tieto vie kymmenesosan alkuperäisestä, sijoitetaan muuttujaan 10.

$$\frac{EPD * RAW}{COMPRESS} * 365 = \text{tilantarve} \quad (5)$$

missä  $RAW$  = yksittäisen tapahtuman koko

$EPD$  = tapahtumaa vuorokaudessa

$COMPRESS$  = pakkaussuhde

Ennen projektin toteuttamista on hyvä tehdä laskelmia kapasiteettitarpeista. Huolellisesti tehdyillä laskelmilla pystytään mitoittamaan SIEM-järjestelmä ympäristöön sopivaksi.

#### 4 Erilaiset SIEM-ratkaisut

Jokaisella valmistajalla on oma tapansa toteuttaa SIEM-ratkaisuja. Valmistajien ratkaisuja esitellään eri lähteiden näkökulmista. Osa esittelyistä on tehty valmistajien kertomien tietojen pohjalta. Näihin lähteisiin tulee suhtautua kriittisesti.

Tärkeänä lähteenä esittelyssä pidetään Gartnerin-tutkimusta. Tutkimus jaottelee SIEM-ohjelmistot neljään kenttään suoriutumiskyvyn ja liiketoiminnallisten valmiuksien mukaan. Nelikentässä pystyakselilla (ability to execute) arvioidaan yrityksen tuotteiden ja tuen suorituskykyä sekä asiakastyytyvääsiisyyttä. Vaaka-akselilla (completeness of vision) arvioidaan yrityksen innovatiivisuutta ja liiketoiminnallista toimintatapaa. [30.]

Kuvassa 3 Leaders-kenttään sijoittuvat valmistajat, jotka menestyvät tällä hetkellä hyvin ja joilla on hyvät edellytykset pärjätä hyvin myös tulevaisuudessa. Challengers-kentässä olevat yritykset pärjäävät tällä hetkellä, mutta ymmärrys markkinoiden kehityssuunnasta on heikko. Visionaries-kentässä olevat yritykset ymmärtävät markkinoita, mutta suoriutuvat keskiarvoa heikommin. Niche Players -kentässä olevat yritykset keskittyvät pieneen markkinasegmenttiin ja eivät pärjää innovaatioiden ja suorituskyvyn puolesta muille. [56] Esiteltäviksi ohjelmistoiksi valittiin kaikki Leaders-kenttään sijoittuneet valmistajat ja lisäksi muista kentistä yksi valmistaja (kuva 3).



Kuva 3. SIEM-ohjelmistojen nelikenttä [30]

#### 4.1 HP ArcSight

Kansainvälisesti toimiva Hewlett-Packard osti ArcSight Inc. -yrityksen vuonna 2010 1,5 miljardilla dollarilla. HP sai laajennettua liiketoimintaansa kaupan myötä tietoturvamarkkinoille. [57.]

Gartnerin tekemän tutkimuksen mukaan Leaders-kenttään sijoittuva HP ArcSight -ohjelmisto tarjoaa hyvät SEM-valmiudet. Express versio tarjoaa yksinkertaistetun vaihtoehdon SIEM-järjestelmän käyttöönotolle. ArcSight Logger on edullinen vaihtoehto pitkäaikaiseen lokitiedon varastointiin. [30.]

Tutkimuksessa huomautetaan ArcSightin kykenevän reaaliaikaiseen tilastolliseen korrelointiin, mutta profilointiin ja poikkeusten havaitseminen on mahdollista ainoastaan his-

toriatietojen pohjalta. ArcSightin nykyään käyttämä CORR-Engine on poistanut valtaosan käyttöönnoton ja ylläpidon monimutkaisuudesta, mutta asiakkaat pitävät HP ESM -ohjelmistoa monimutkaisempana kuin muita johtavia kilpailijoita SIEM-markkinoilla. [30.]

HP ArcSight -ohjelmistosta on saatavilla useita lisenssivaihtoehtoja. Lisensointi perustuu vuorokausittain käsiteltävän datan määrään. Eri vaihtoehdot ovat esillä liitteessä 4 olevassa taulukossa. ArcSight ESM:n lisenssi on mahdollista laajentaa yli 250 GB/vrk laajuuteen. Todellisen päivärajoituksen asettavat viimekädessä laitteistovaatimukset. Liitteen 4 taulukossa mainittu EPS-arvo on suuntaa antava eikä sitä käytetä lisensoinnin pohjana. [58.]

HP ArcSight vaatii toimiakseen Red Hat Enterprise Linux -käyttöjärjestelmän, jonka versio on 6.4 tai 6.5 (64 bit) sekä SUSE 11 SP3 (64bit). ArcSight toimii myös RHEL-käyttöjärjestelmään perustuvalla CentOS 6.5 -käyttöjärjestelmällä. Konsolikäyttöliittymä toimii edellä mainittujen käyttöjärjestelmien lisäksi Windows-versioilla 7 (SP1), 8, 8.1, Server 2008 R2 ja Applen MacOS 10.7 -käyttöjärjestelmällä. Web-käyttöliittymää hallitaan Internet Explorer-, Firefox-, Chrome-, ja Safari-selaimilla. [58.]

HP esittelee sivuillaan kolme erilaista asennusskenaariota laitteistovaatimusten osalta (Taulukko 2).

Taulukko 2. HP ArcSight -laitteistovaatimukset [58]

| Laitteistoresurssit | Ympäristön koko             |                               |                                 |
|---------------------|-----------------------------|-------------------------------|---------------------------------|
|                     | Pieni                       | Keskisuuri                    | Suuri                           |
| Suoritinytimet, kpl | 8                           | 16                            | 32                              |
| Muisti, GB          | 36                          | 64                            | 128                             |
| Tallennustila, GB   | 250 (RAID 10<br>15 000 RPM) | 1 500 (RAID 10<br>15 000 RPM) | <=8 000 (RAID 10<br>15 000 RPM) |

## 4.2 McAfee Enterprise Security Manager

Yhdysvaltalainen Intel osti kaikki tietoturvayhtiö McAfeen osakkeet elokuussa 2010. Kaupan kokonaishinta oli noin 7,68 miljardia dollaria. McAfee toimii Intelin omistamana erillisenä tytäryhtiönä. [59] Toukokuussa 2013 McAfee osti suomalaisen tietoturvayhtiön Stonesoft Oyj:n 389 miljoonalla dollarilla [60]. Ennen yrityskauppoja Stonesoftilla oli tarjolla oma SIEM-käyttöön soveltuva Stonesoft Management Center -ratkaisu [61].

McAfee Enterprise Security Managerissa on SIM- ja SEM-ominaisuudet. Tätä voidaan laajentaa lisäosilla, jolla esimerkiksi seurataan tarkemmin ohjelmistoja sekä tietokantatapahtumia. Gartnerin mukaan ESM pystyy tehokkaasti käsittelemään myös erittäin suuria tietomääriä nopeasti ja soveltuu hyvin esimerkiksi tietokantojen sekä teollisten hallintajärjestelmien valvontaan. Tutkimuksen nelikentässä (kuva 3) McAfee sijoittuu Leaderskenttään. [30.]

Gartnerin tutkimuksessa McAfee saa kritiikkiä rajoittuneista NetFlow:n suodatus- ja hälytysvalmiuksista. McAfee mahdollistaa SIEM-ominaisuuksien parantamisen esimerkiksi päätelaitteiden tiedusteluominaisuuksilla. Tämä vaatii kuitenkin integrointeja ja lisäinvestointeja McAfeen tuotteisiin. Käyttäjät pitävät McAfeen tarjoamaa tukea hyvänä, mutta oikean asiantuntijan tavoittaminen on vaikeaa. [30.]

McAfee ESM -järjestelmässä on useita käyttöönottovaihtoehtoja. Järjestelmä voidaan ostaa kuukausimaksullisena palveluna (Security-as-a-Service), valmiina laitteena, jossa on kaikki tarvittava ohjelmisto tai hajautettuna ratkaisuna usealle palvelimelle. Jokaisessa vaihtoehdossa on monipuoliset työkalut järjestelmän hallintaan web-pohjaisen käyttöliittymän kautta. Myös etähallinta on mahdollista. Kun järjestelmä tilataan valmiina palveluna, on tätä helppo skaalata käyttöasteen mukaan ilman uusia laitehankintoja. Silloin järjestelmästä maksetaan käytön mukaan. [62, 1–2.]

ESM-ohjelmisto seuraa tietoturvatietoa reaaliaikaisesti, jolloin ongelmat voidaan havaita heti. Myös aikaisempia historiatietoja voidaan käyttää pidempikestoisten hyökkäysten selvitykseen. Yrityksen koon mukaan on valittavissa sopiva vaihtoehto järjestelmästä. Pienille yrityksille soveltuu yksi laite, jossa on kaikki tarvittavat komponentit. Suuremmat yritykset voivat hajauttaa järjestelmän useille eri palvelimille, jolloin yksittäisen laitteen kuorma vähenee. Liitteessä 5 on McAfeen eri SIEM-ratkaisut. [63.]

Laitteet eroavat tiedonkeräysnopeudessa sekä kiintolevykapasiteetissa. Edullisin vaihtoehto pystyy keräämään 1 200 tapahtumaa sekunnissa, kun taas paras 360 000 tapahtumaa yhden sekunnin aikana. Lisätietoa on liitteessä 6. [64.]

Järjestelmän käyttöönotto on yksinkertaista. Aluksi ESM-palvelimeen kytketään näppäimistö ja näyttö. Tämän jälkeen asetetaan IP-osoite laitteen hallintaa varten. Jatkossa konfigurointi tapahtuu ottamalla yhteys selaimella laitteen web-pohjaiseen käyttöliittymään, josta laitetta hallitaan. Käyttöliittymä on toteutettu Flash-pohjaisesti, mikä on helpokäyttöinen ja selkeä. [65.]

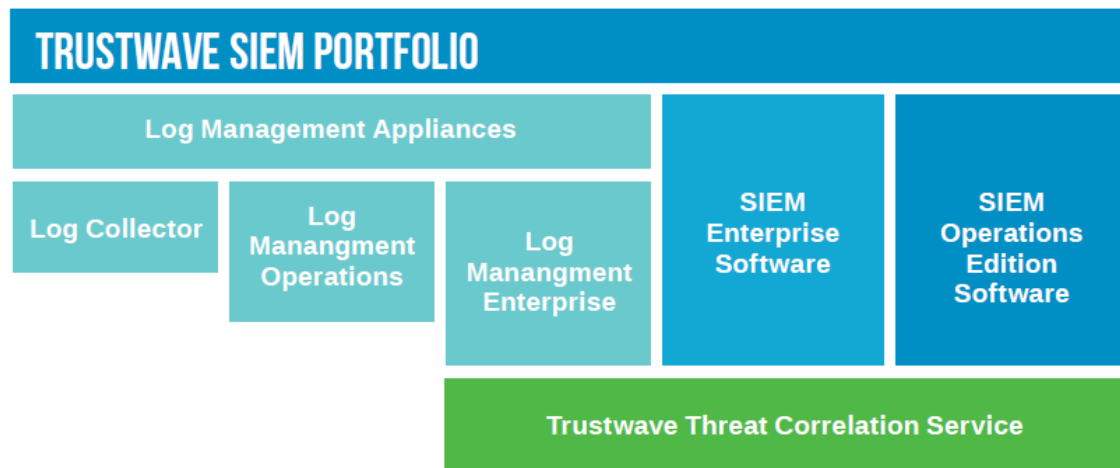
Järjestelmän käyttöliittymä on muokattavissa eri käyttäjien tarpeiden mukaan, mikä tehostaa työtä pitkällä aikavälillä. Arvion mukaan ohjelmisto on yksi markkinoiden selkeimmistä ja helpokäyttöisimmistä. ESM-ohjelmistossa tietoja haetaan ja rajataan eri aktiiviteettien perusteella. Haut ovat nopeita, vaikka järjestelmässä on paljon seurattavia kohteita. Ohjelmistossa on monipuoliset raportointityökalut, joilla raporteista voi tehdä omaan käyttöön sopivia. [66, 2.]

SIEM-ohjelmistossa korrelointi eri tietojen välillä on tärkeä ominaisuus. ESM-ohjelmistossa on valmiita korrelointisääntöjä sekä uusia sääntöjä voi luoda käsin graafisessa käyttöliittymässä. [66, 11.]

### **4.3 Trustwave SIEM**

Trustwave tarjoaa tietoturvan hallintaan useita lähestymistapoja. SIEM-käyttöä varten saatavilla on lokienhallintalaitteita (Log Management Appliances). Lokienhallintaratkaisut Trustwave jaottelee kolmeen tuotteeseen, joita ovat Log Collector, Log Management Operations ja Log Management Enterprise (kuva 4). Näitä ratkaisuja on mahdollista yhdistää toimimaan Trustwaven muiden SIEM-tuotteiden ja palveluiden kanssa, joita ovat SIEM Enterprise, SIEM Operations Edition sekä Managed SIEM. [67.]





Kuva 4. Trustwaven SIEM-ratkaisut [67]

Lokienhallintaratkaisusta Log Management Enterprise on laitepohjainen, mistä valmistaja tarjoaa kuutta eri mallia taulukon 3 mukaisesti. Trustwaven LME-tuoteperheellä päästään valmistajan mukaan mallista riippuen EPS-arvoihin 115–3 400. LME tarjoaa yli 70 eri korrelointipohjaa, joita on mahdollista määrittää uudelleen.

Taulukko 3. Trustwave LME -tuoteperhe. [68]

| TRUSTWAVE LOG MANAGEMENT APPLIANCE MODELS |            |            |            |            |             |             |
|---|------------|------------|------------|------------|-------------|-------------|
|   | LME 2-10   | LME 2-20   | LME 2      | LME 3      | LME 4       | LME 5       |
| EPS*                                      | 115        | 230        | 460        | 925        | 1,735       | 3,400       |
| EPD*                                      | 10 million | 20 million | 40 million | 80 million | 150 million | 300 million |
| RAM                                       | 12 GB      | 12 GB      | 12 GB      | 16 GB      | 24 GB       | 48 GB       |
| Effective Storage**                       | 9 TB       | 9 TB       | 9 TB       | 18 TB      | 29 TB       | 44 TB       |
| Online Retention***                       | 5 years    | 4 years    | 3 years    | 3 years    | 2 years     | 1 year      |
| Redundant Power                           | Yes        | Yes        | Yes        | Yes        | Yes         | Yes         |
| Interfaces                                | 4 GIG Eth  | 4 GIG Eth  | 4 GIG Eth  | 4 GIG Eth  | 4 GIG Eth   | 4 GIG Eth   |

\* Events Per Second and Events Per Day rates are calculated based on full functionality and normalization of average data types and sizes. Rates will vary by location based on the data types and sizes being processed. Rates for acquisition go up to 100,000 EPS or 8.6 billion EPD.  
 \*\* Effective storage rates are local storage online all the time. Storage is included with the appliances and is configured with redundancy (RAID) to protect data in the case of drive failure.  
 \*\*\* Online retention is based on average data types and sizes. Retention times will vary depending on the data types and sizes processed. Purchasing a larger appliance and processing less data will increase data retention.

Trustwave SIEM Operations Edition (OE) on ohjelmistopohjainen lokienhallintaratkaisu, joka on valmistajan mukaan helppo käyttöönottaa yhdellä palvelimella tai hajautettuna usealle palvelimelle. OE soveltuu erityisesti mobiili- ja BYOD-ympäristöihin ja analysoi tietoturvatapahtumia automaattisesti ja visualisoi ne. [69.]

Gartnerin tutkimuksen nelikentässä Trustwave sijoittuu Niche Players -kenttään, joka kertoo yrityksen ratkaisujen olevan keskitasoa heikommin suorituvia ja liiketoimintamallien olevan myös keskitason alapuolella. Trustwaven tuotteiden vahvuuksia ovat laaja palveluvalikoima ja sen tarjoamat useat käyttöönottovaihtoehdot. Asiakkaille, joilla on laajamittaisia tapahtumien seurantavaatimuksia, Trustwaven SIEM OE kykenee tarjoa-

maan tarvittavan analytiikkaan, kapasiteetin ja räätälöintimahdollisuudet. Hyvänä ominaisuutena pidetään myös Trustwaven tuotteiden kykyä reagoida tapahtumiin automaattisesti karanteeni- ja estolistatoiminnoilla. [30.]

Trustwave SIEM OE -ratkaisun käyttäjät ovat ilmaisseet mukautettujen raporttien tekemisen ohjatulla työkalulla hankalaksi ja käsin tehtävien raporttien teko vaatii osaamista SQL- ja XML-kielistä. Kilpailijoiden uusiutuvan tietoturvateknologian ja Trustwaven tuotteiden yhteensopivuutta pidetään kyseenalaisena. SIEM-järjestelmän ylläpitäjän tulee tarkkailla tarjoavatko muut toimittajat tukea Trustwaven tuotteiden kanssa. [30.]

SC Magazine -lehden tekemässä arviossa Trustwave SIEM:n vahvuuksina pidetään hyviä ominaisuuksia ja laajaa valmista mallipohjakokoelmaa. Trustwaven heikkous on konfiguroinnin vaikeus. Saadakseen siitä kaiken irti, Trustwaven käyttö edellyttää läpikotaista tuntemista käytössä olevasta IT-ympäristöstä. Hyvin konfiguroituna Trustwaven SIEM on hyvä työkalu. Käyttöönotto suoritetaan ohjatussa web-pohjaisessa näkymässä. Käytönnoton jälkeen laitetta hallinnoidaan web-konsolilla. Trustwaven toimittama asennusdokumentaatio on selkeää ja johdonmukaista luettavaa. Trustwave tarjoaa tuotteilleen vuosisopimuksella teknistä tukea puhelimitse, sähköpostilla ja internetissä olevassa tietolähteessä. [107.]

#### **4.4 IBM Security QRadar**

IBM osti vuonna 2011 Q1 Labs -ohjelmistoyrityksen, joka kehitti tietoturvatapahtumien seurantaan ja korrelointiin tarkoitettua QRadar-ohjelmistoa. Tämän jälkeen IBM muodosti tietoturvayksikön, johon kuului useita IBM:n aikaisemmin ostamia yrityksiä. [70]. Tällä IBM kilpailee Hewlett-Packardin ostamaa ArcSight-ohjelmistoa vastaan [71]. Gartnerin tutkimuksen mukaan IBM Security on yksi SIEM-ohjelmistojen markkinajohtajista [30].

QRadar pystyy lähes reaaliaikaisesti seuraamaan, normalisoimaan ja korreloimaan tietoa tuhansilta kohteilta, joita ovat esimerkiksi sovellukset, tietokannat, käyttöjärjestelmät ja verkkolaitteet [72]. VFlow-ominaisuudella seurataan jokaista OSI-mallin kerrosta jo fyysiseltä kerrokselta sovelluskerrokseen asti. Ohjelmisto tukee heti asennuksen jälkeen yli tuhatta seurattavaa sovellusta. Ominaisuus tarkkailee erilaisia verkkoprotokollia ja niiden käyttöä. Se mahdollistaa hyökkäysten havaitsemisen esimerkiksi silloin, jos liikennemäärissä on omituisia muutoksia tai tietyillä palvelimilla on käynnissä haitallisia palveluita.

Tähän yhdistetään lokien ja verkkoliikenteen välinen korrelointi, jolloin pystytään havaitsemaan uhkia, joita ei muuten löydettäisi. [73.]

QRadarin voidaan asentaa ohjelmana RHEL-käyttöjärjestelmään, erillisinä prosessointi-, keräys- ja hallintalaitteina tai pienempään järjestelmään yhtenä laitteena, jossa on kaikki edellä luetellut toiminnot [30]. InfoSec Nirvanan arvion mukaan QRadar on yksinkertainen ottaa käyttöön ja asentaa. Ohjelmisto on suoraan käyttövalmis ja siinä on valmiina yli 1500 raporttipohjaa. Kuitenkaan QRadaria ei ole mahdollista mukauttaa yhtä hyvin, kuin esimerkiksi sen kanssa kilpailevaa ArcSight-ohjelmistoa. [71.]

Järjestelmävaatimuksena asennettaessa QRadar Security Intelligence Platform RHEL-järjestelmän päälle on vähintään 8 gigatavua keskusmuistia, 256 gigatavua vapaata levytilaa konsolijärjestelmää varten ja 70 gigatavua vapaata tilaa QRadar Qflow Collector -ohjelman käyttämälle levyllä. Palomuurista sallitaan HTTP-, HTTPS- ja SSH-yhteydet sekä otetaan SELinux pois käytöstä. [74.]

QRadar Virtual Appliances on tarkoitettu asennettavaksi VMware-virtualisointialustalle. Mukana ovat kaikki ohjelmistot, jotka kuuluvat myös valmiisiin IBM:n laitteistopohjaisiin ratkaisuihin. Näiden laitteistovaatimukset ovat mainittu liitteessä 7. Kaikkia IBM:n ohjelmisto- ja laitepohjaisia SIEM- ja lokiratkaisuja voi käyttää keskenään. [75, 9.]

Järjestelmävaatimuksena virtualisointialustalle on VMware ESXi Version 5.0 tai 5.1. Kovalevytilaa vaaditaan vähintään 256 gigatavua, jonka lisäksi QRadar QFlow Collector tarvitsee vähintään 70 gigatavua levytilaa. Muistivaatimukset vaihtelevat käytettävästä ohjelmistosta riippuen liitteen 7 mukaan. [76.]

## **4.5 LogRhythm**

Gartnerin tutkimuksen mukaan LogRhythm tarjoaa SIEM-ratkaisuja laite- ja ohjelmistopohjaisesti. LogRhythm sijoittuu Gartnerin nelikentässä Leaders-osioon. Kohderyhmänä ovat keskisuuret ja suuret yhtiöt. LogRhythm skaalautuu hyvin pienten ympäristöjen lokihallinnasta monimutkaisempaan keskitettyyn tapahtumien hallintaan. LogRhythm sisältää valmiit agentit yleisimmille käyttöjärjestelmille. System Monitor Agent -ohjelmilla on mahdollista seurata prosesseja ja tiedostojen eheyttä Windows- ja Unix-alustoilla. LogRhythm:n SIEM-tuote toimii hyvin myös verkkoliikenteen seurannassa. [31.]

LogRhythm soveltuu hyvin yrityksille, jotka kaipaavat yhtä aikaa verkonvalvontaan, SIEMiin ja tiedostojen eheyteen liittyviä ominaisuuksia. LogRhythm saa kehuja käyttöönoton helppoudesta. Esimääritellyt korrelointisäännöt ja raporttipohjat ovat laadukkaita. [31] LogRhythm tuottamat dokumentaatiot ovat laadukkaita ja kuvaavat selkeästi kaikki toiminnot. Hinnat alkavat 27 500 dollarista ja saatavilla on eritasoisia tukisopimuksia perustason tuesta ympärivuorokautiseen tukeen. [77.]

Moitteita LogRhythm saa heikosti muunneltavista sähköpostihälytyksistä. Ohjelmistosta löytyy tuki vanhojen laitteiden lokienkäsittelyyn, joka tekee käytöstä monimutkaisempaa. [30.]

Liitteessä 8 on esitetty LogRhythm erilaiset SIEM-ratkaisut. Valmistaja käyttää EPS-arvon sijaan omaa MPS-arvoa. Eri ratkaisut kykenevät käsittelemään 1 000 - 75 000 viestiä sekunnissa [13].

Ohjelmistopohjaiset tuotteet toimivat virtualisoina VMware-, Citrix XenServer- ja Windows Server Hyper-V -alustoilla. LogRhythm tarjoaa SIEM-järjestelmiin liittyviä tukipalveluita erikokoisille organisaatioille. [13.]

## **4.6 NetIQ**

NetIQ sijoittuu Gartnerin nelikentässä Challengers-osioon. Se ei yllä parhaiden SIEM-valmistajien tasolle, mutta se on kehittynyt paljon viimeisten vuosien aikana. Sen Sentinel-ohjelmistopakettiin kuuluu Sentinel, Sentinel Log Manager ja Change Guardian. Gartnerin arvion mukaan järjestelmä toimii suurissakin ympäristössä erityisesti tietoturvaauhkien seuraamisessa ja SEM-järjestelmänä. Arviointihetkellä Sentinelissa ei ollut threat intelligence feeds -ominaisuutta, joka esimerkiksi analysoi IP-osoitteiden luotettavuutta. Tämä ominaisuus sisältyy useiden muiden valmistajien tuotteisiin. Sentineliin voidaan integroida myös muita NetIQ-ohjelmistoja kuten AppManager tai Access Manager. [30.]

NetIQ Sentinel -ohjelmistossa on perinteisen SIEM-ratkaisun tarvitsemat ominaisuudet. Sentinel-ohjelmistolla on mahdollista kerätä lokitietoa useilta eri kohteilta, jonka jälkeen tieto analysoidaan ja korreloidaan. Ohjelmasta on saatavilla 90 päivän testiversio, jolloin yrityksessä voidaan testata ohjelman toimivuus omassa ympäristössä. SANSin arviossa suurena ongelmana pidettiin huonoa dokumentaatiota ohjelmasta. [78, 1.]

Asennuksessa on kolme eri tapaa. NetIQ voidaan asentaa ohjelmana käyttöjärjestelmän päälle. Toinen vaihtoehto on käyttää valmiista levykuvaa (virtual appliance), joka asennetaan ESX- tai XEN-virtualisointialustan päälle. Lisäksi saatavilla on DVD ISO -tiedosto, jota käytetään asennettaessa Microsoft Hyper-V -alustalle tai laitteeseen, jossa ei ole asennettua käyttöjärjestelmää. Tarkemmat ohjelmistovaatimukset ovat liitteessä 9. [79.]

Sentinel-palvelinohjelmisto koostuu kolmesta komponentista. Collection Manager kerää tietoa kohteilta, Correlation Engine on kerätyn tiedon korrelointia varten ja NetFlow Collector Manager -komponentti on verkkoliikenteen keräystä varten. Sillä esimerkiksi kerätään tietoa Ciscon reitittimiltä NetFlow-protokollalla. Jokainen komponentti on hajautettavissa useammalle palvelimelle. [80.]

Sentinel-järjestelmän suunnittelussa on huomioitava järjestelmävaatimukset. NetIQ tarjoaa konsultointipalvelua laitteistovaatimusten määrittämiseksi erilaisiin tarpeisiin ja listaa Sentinel-dokumentaatioissa laitteistosuositukset erikokoisille ympäristöille EPS-arvon perusteella. Järjestelmävaatimukset on listattu tarkemmin liitteessä 10. [81.]

#### **4.7 Splunk**

Splunk sijoittuu Gartnerin nelikentässä Leaders-osioon, jossa Splunk on yksi viidestä SIEM-markkinajohtajasta. Gartnerin arviossa sen loki- ja analytiikkaominaisuudet ovat monipuoliset ja muokattavat eri tarpeisiin sopiviksi. Valmiit raportointitoiminnot ovat rajoittuneemmat kuin kilpailijoilla. Splunkin käyttöönottoa pidettiin huomattavasti kalliimpana kuin sen kanssa kilpailevien yritysten tuotteita. [30.]

Splunk Enterprise on tiedonkeruuseen, -analysointiin sekä sen visualisointiin tarkoitettu ohjelmisto. Tietoa voidaan kerätä useita erilaisista lähteistä kuten verkkolaitteilta, palvelimilta sekä verkkosivuilta. [82] Tarjolla on myös Splunk Cloud -pilvipalvelu, joka voidaan yhdistää Splunk Enterprise -ohjelmistoon ja hallita molempia samasta käyttöliittymästä. [83.]

Splunk Enterprisessä on mahdollista luoda omia reaaliaikaisia korrelointisääntöjä ja tehdä raportteja, jolloin se toimii SIEM-ohjelmiston tapaan. Splunkiin voidaan asentaa Splunk App for Enterprise Security -sovellus, joka tuo siihen SIEM-ominaisuuksia. Siinä on valmiina esimerkiksi hälytystoiminnot, korrelaatisääntöjä ja käyttöliittymä tietoturvatiedon hallintaan. [84.]

Järjestelmä koostuu palvelinohjelmistosta ja data forwarder -ohjelmista. Molemmat ohjelmistot asennetaan käyttöjärjestelmän päälle. Splunkia hallitaan web-käyttöliittymässä. Suurissa järjestelmissä Splunk voidaan hajauttaa useille palvelimille ja tasata kuormaa. Toiminta on laajennettavissa sovelluksilla (apps), joissa on valmiita raporttipohjia ja hakutoimintoja. [85, 3–4, 9.]

Data forwarderit, joita on kolme vaihtoehtoa, vastaavat Splunk-terminologiassa agentteja, jotka asennetaan seurattaville kohteille. Light forwarder on poistumassa käytöstä ja Splunk suosittelee käytettäväksi universal forwarderia. Se on näistä kevyin vaihtoehto ja korvaa light forwarderin. Kuitenkin rajoituksena universal forwarderissa on se, ettei se indeksoi tai hae tietoa eikä lähetä hälytyksiä. [86.]

Heavy forwarderit ovat raskaampia, koska ne pohjautuvat Splunk Enterpriseen, josta on otettu ominaisuuksia pois käytöstä. Kuitenkin heavy forwarder pystyy jäsentämään ja indeksoimaan tietoa ennen sen lähettämistä eteenpäin. Light forwarderia ei enää suositella käytettäväksi muualla kuin vanhoissa järjestelmissä, joihin ei ole mahdollista asentaa muuta vaihtoehtoa. [86.]

Splunk-ohjelmistosta on myös ilmainen Splunk Free -versio. Tämä toimii rajoittamattoman ajan, mutta päiväkohtainen indeksointimäärä on rajattu 500 megatavuun. Hakutoiminto estetään, mikäli päiväkohtainen rajoitus ylitetään yli kolmena päivänä 30 päivän sisällä. Splunk Free -ohjelmistossa on myös muita rajoituksia, joiden takia se ei sovellu suuremmille yrityksille. Ilmaisessa versiossa ei ole mahdollista asettaa hälytyksiä, jolloin tietoturvaongelmat voivat jäädä huomaamatta. Se ei tue ollenkaan käyttäjätunnistusta, joten järjestelmää hallitaan selain- tai komentoriviyhteydellä ilman käyttäjätunnusta ja salasanaa järjestelmävalvojan oikeuksilla. Myös klusterointimahdollisuus puuttuu ilmaisesta versiosta. [87.]

Pienissä järjestelmissä tai testikäytössä Splunk Enterprise -asennus on mahdollista tehdä yhdelle palvelimelle. Suuremmissa ympäristöissä Splunk-järjestelmä kannattaa hajauttaa useille palvelimille, jolloin suurien tietomäärien kerääminen ja analysointi on mahdollista. Splunkin tietovirta koostuu tiedon keräämisestä, kerätyn tiedon indeksoinnista ja hakujen suorittamisesta tästä tiedosta. [88.]

Forwardereilla seurattavien laitteiden määrän kasvaessa järjestelmään täytyy lisätä useita indeksoijia, koska muuten kapasiteetti ei riitä. Forwarder voidaan määritellä tasaamaan

kuorma useiden indeksoijien kesken, jolloin yksittäisen indeksoijan raskaus vähenee. Tällöin vikatilanteessa forwarder osaa myös automaattisesti valita toimivan indeksoijan, mikäli jokin indeksoija on alhaalla. Haku tapahtuu kuitenkin jokaisen indeksoijan sisällä. Suuremmassa järjestelmässä indeksoijien välillä voidaan hakea tietoa käyttämällä search head -komponenttia, joka on mahdollista klusteroida useille palvelimille. [88] Liitteessä 11 on esimerkki klusteroidusta Splunk-järjestelmästä.

Splunk tukee useita eri Windows- ja Unix-pohjaisia käyttöjärjestelmiä. Kuitenkin arkkitehtuurituki vaihtelee eri käyttöjärjestelmien välillä. Tuetut järjestelmät on tarkemmin listattuna liitteessä 12. Laitteistosuosituksena Splunk Enterprise -ohjelmistolla on kaksi kuusiytimistä prosessoria, 12 gigatavua keskusmuistia, 64-bittinen käyttöjärjestelmä ja RAID 0 tai 0+1. [89.]

#### **4.8 AlienVault OSSIM**

AlienVault OSSIM -ohjelmistoon tutustuttiin opinnäytetyössä tarkemmin toimeksiantajan pyynnöstä. AlienVault OSSIM SIEM-järjestelmänä tuo potentiaalisesti säästöä kustannuksissa, koska ohjelmisto perustuu avoimeen lähdekoodiin ja on täten ilmainen.

AlienVault kehittää kahta SIEM-ohjelmistoa. OSSIM on ainoa ilmainen avoimen lähdekoodin SIEM-ohjelmisto. Se julkaistiin vuonna 2003. AlienVault-sivuston perusteella OSSIM-ohjelmistoja on otettu käyttöön noin 18 000 ympäri maailmaa. [90] AlienVaultin tarjoama maksullinen vaihtoehto on nimeltään Unified Security Management (USM).

AlienVault OSSIM -ohjelmisto yhdistää useita avoimen lähdekoodin ohjelmistoja yhdeksi monipuoliseksi kokonaisuudeksi. AlienVaultin kehittämässä OSSIM-järjestelmässä on tehokkaat korrelointi-, raportointi- ja hallintaominaisuudet, joilla voidaan helposti hallita suuriakin lokitietomääriä. [31, 140] AlienVault OSSIM:n toiminnallisuus on kuvattu kaaviolla liitteessä 13.

AlienVault OSSIM ja USM -ohjelmistojen järjestelmävaatimuksena on vähintään 8-ytiminen prosessori, 16 gigatavua keskusmuistia, 250 gigatavua kiintolevytilaa ja VMware 4.0 -versio tai uudempi. [91] Järjestelmävaatimukset kasvavat suhteessa käsiteltävän datan määrään.

#### 4.8.1 OSSIMin keskeisimmät komponentit

Järjestelmä voidaan toteuttaa yhdellä palvelimella, jossa kaikki komponentit ovat tai hajauttaa nämä usealle palvelimelle. Komponentteja ovat hallintapalvelin, sensorit, tietokanta ja käyttöliittymä. Ennen käyttöönottoa on suunniteltava sopiva topologia omaan järjestelmään. [31, 147–149.] Monitasoinen, usealle palvelimelle asennettu järjestelmä vaatii maksullisen USM-järjestelmän käyttämisen [92].

Sensorien avulla OSSIM kerää tietoa agenteilta tai suoraan laitteilta käyttämällä eri verkoprotokollia. Lisäksi sensoreilla on mahdollista tehdä haavoittuvuuskannauksia verkossa ja se voi toimia IDS-sovelluksena. Se on asennettavissa omalle palvelimelle tai se voi olla samalla palvelimella muiden komponenttien kanssa. Sensorit ovat yhteydessä hallintapalvelimeen, jonne kerätty data lähetetään. [31, 147–149.]

Hallintapalvelin jakautuu Frameworkd-prosessiin, joka ohjaa muita komponentteja sekä OSSIM-palvelimeen, joka vastaanottaa tietoa sensoreilta. Palvelimella kerätty tieto normalisoidaan ja korreloidaan. Normalisoitu data tallennetaan tietokantaan. [31, 147–149.] Ilmainen OSSIM ei sovellu pidempiaikaisen lokitiedon keräämiseen, vaan silloin tarvitaan maksullista USM-tuotetta [92].

#### 4.8.2 Ongelmien havaitseminen

OSSIM-ohjelmistossa on kahdentyyppisiä tapoja havaita verkko-ongelmia tai -hyökkäyksiä. Yleisesti käytössä oleva tapa on valmiisiin malleihin perustuva tunnistus (pattern-based). Kun ohjelma havaitsee tietyn mallin mukaista käyttäytymistä verkossa, se lähettää siitä hälytyksen. OSSIM sisältää IDS- ja HIDS-ominaisuudet, joilla malleihin perustuvia hyökkäyksiä havaitaan. Lisäosilla OSSIM voidaan määrittää seuraamaan myös muiden valmistajien IDS-tuotteita. [31, 142–143.]

Toinen tapa havaita hyökkäyksiä on seurata verkossa tapahtuvia poikkeavuuksia. Aluksi määritellään milloin verkkotapahtumat ovat normaalin vertailuarvon sisällä. Kun tietoverkossa tapahtuu jotain, joka ei kuulu tähän normaaliin vertailukohtaan, lähettää ohjelmisto ilmoituksen asiasta. Näin havaitaan myös nollapäivähaavoittuvuuksia sekä ongelmia, joita malleihin perustuvat ohjelmistot eivät havaitse. [31, 143.]

Verkkoseuranta varten OSSIM-järjestelmään on integroitu useita ohjelmistoja. Ntop-ohjelmalla seurataan tiedonsiirtokapasiteetin ja eri verkkoprotokollien käyttöä sekä kerättyä tietoa suoraan muiden valmistajien verkkolaitteilta esimerkiksi NetFlow-protokollalla



Ciscon tuotteista. DoS-hyökkäysten havaitsemiseen käytetään Nagios-työkalua, joka tunnistaa, mikäli jokin verkkolaite on alhaalla. OSSIM-järjestelmään sisältyy useita työkaluja verkon haavoittuvuuksien etsimiseen. Kaikkia työkaluja on mahdollista mukauttaa eri järjestelmiin sopiviksi. [31, 143.]

OSSIM käsittelee tietoturvatietoa lokitietojen, hälytysten, tapahtumien ja tikettien perusteella. Eri tapahtumien riskeistä ohjelma tekee riskiarvion kaavan 6 perusteella. [90.]

$$\frac{AV * P * R}{25} = ROE \quad (6)$$

missä  $AV$  = Asset value, kohteen arvo. Arvo määritetään väliltä 0 – 5

$P$  = Priority, prioriteetti. Arvo määritetään väliltä 0 – 5

$R$  = Reliability, luotettavuus. Arvo määritetään väliltä 0 – 10

$ROE$  = Risk of event, tapahtuman riski. Arvo on väliltä 0 – 10

### 4.8.3 Tiedon kerääminen

AlienVault OSSIM -järjestelmässä tietoa kerätään suoraan verkkolaitteilta SNMP- tai syslog-protokollalla tai palvelimilta agenttiohjelmistoilla. Keräämisen jälkeen tieto normalisoidaan eri laitteilta yleiseen muotoon. Datamäärien kasvaessa on suositeltavaa määrittellä tietoa kerääviltä sensoreilta eri laitteille tärkeysaste, jonka mukaan tieto lähetetään palvelimelle. Priorisoinnin ansiosta tärkeä tieto ei jää keräämättä verkon kuormitustilanteessa. [31, 144.]

Palvelimille ja työasemille voidaan asentaa agenttiohjelmisto. Agenttivaihtoehtoja on esimerkiksi Snare, OSSEC, rsyslog tai snmptrapd. [90.] Oletuksena OSSIM käyttää OSSEC-agenttia.

OSSIM vaatii tiedonkeräykseen lisäosia, joita OSSIM-ohjelmiston mukana tulee yli 2000. Lisäosia on saatavilla laajasti yleisimpiä laitteita ja ohjelmistoja varten. Laajasta lisäosavalikoimasta huolimatta kaikkien valmistajien tuotteet eivät toimi välttämättä suoraan, koska osa lisäosista on vanhentuneita. Tarkkailtavien laitteiden ja ohjelmistojen lokimuotoilut muuttuvat ajan myötä ja tämä aiheuttaa yhteensopivuusongelmia [90.]

#### 4.8.4 Korrelointi

OSSIM suorittaa kolmea erityyppistä korrelointia. Looginen korrelointi pohjautuu sääntöihin. Sääntölistoja on jo valmiina ohjelmistossa ja uusia voi luoda käsin. Laitteisiin perustuvassa korreloinnissa seurattavien laitteiden ominaisuuksia verrataan tiettyihin toimintamalleihin. Tällöin mikäli laitetta vastaan hyökätään, mutta hyökkäys on tarkoitettu toiselle laitetypille, voidaan uhka jättää huomioimatta. Ristiinkorreloinnissa OSSIM yhdistää useiden lähteiden tiedot, jolloin uhkien löytyminen helpottuu ja virheelliset havainnot (false positive) vähenevät. [31, 145.]

Automatisointi nopeuttaa ongelmatilanteiden tai hyökkäysten ratkomista. Ilmoitusten lisäksi OSSIM pystyy muokkaamaan esimerkiksi palomuurien asetuksia tapahtumasarjan tai yksittäisen tapahtuman jälkeen. [31, 145] Esimerkkinä tästä on DoS-hyökkäys palvelimelle, jolloin palvelinta vastaan hyökätään useista osoitteista. OSSIM-ohjelmiston havaitessa hyökkäyksen, se pystyy lisäämään palomuurin pääsyyloihin automaattisesti estosäännöt, jolloin hyökkääjien liikenne pysähtyy palomuurille. Automaattinen toiminto tekee konfiguraatiomuutokset huomattavasti nopeammin verrattuna siihen, että työntekijä saisi ilmoituksen tapahtumasta, jonka jälkeen pääsyyloita muokattaisiin käsin. Näiden sääntöjen kanssa täytyy kuitenkin olla tarkkana, koska muuten estetään helposti yrityksen omaa liikennettä ja palveluita.

#### 4.8.5 Erot OSSIM- ja USM-järjestelmän välillä

OSSIM-ohjelmistossa lokien kerääminen on rajoittuneempaa kuin maksulisessä Unified Security Management -ohjelmistossa. Raportoimistoiminnot on rajoitettu kolmeen pohjaan. OSSIM asennetaan yhdelle palvelimelle eikä se ole hajautettavissa useammalle. Käyttäjähallinta on rajoittuneempi ja jokaista komponenttia hallitaan erikseen. Ongelmatilanteissa joudutaan turvautumaan yhteisön tukeen, koska ammattitasoista teknistä tukea ei ole saatavilla. [92.]

Unified Security Management -ohjelmistossa on valmiina yli 150 muokattavaa raporttipohjaa. Järjestelmä on mahdollista hajauttaa useammalle palvelimelle, jolloin se toimii suurilla kuormilla paremmin. Käyttäjille on määritettävissä eritasoisia rooleja pääsynhallintaa varten. Myös hallinta on keskitetty, jolloin eri komponentteja ei tarvitse muokata erikseen. Järjestelmän hinnat alkavat 3600 dollarista. Ohjelmistolla on täysi ammattilaisten ylläpitämä tekninen tuki. [92.]

#### **4.9 Splunkin ja AlienVaultin vertailu**

Splunk ei ole varsinainen SIEM-tuote vaan se on tarkoitettu ensisijaisesti tehokkaaseen lokitiedon keräämiseen. Lisensoinnissa Splunk eroaa AlienVaultista merkittävästi. AlienVault OSSIM on ilmainen ja paremmilla ominaisuuksilla varustetusta USM-lisenssistä täytyy maksaa vain kerran. Tuesta ja ylläpidosta USM-lisenssissä maksetaan erikseen. USM-lisenssin hinnoittelu on helposti ennustettavissa. Splunk käyttää puolestaan hinnoitteluperusteena lokidatan määrää. Suurilla lokimäärillä Splunk on todella kallis. Splunkin käyttämä hinnoittelumalli on tästä syystä myös ennalta-arvaamaton. Vaihtelevat lokimäärät aiheuttavat vaihtelua kustannuksissa. [93.]

Splunkin SIEM-ominaisuuksia pidettiin InfoSec Nirvanan arviossa heikompana kuin vertailtujen tuotteiden. Sen käyttöönottoa oli helppoa, mutta SIEM-toimintojen muokkaaminen ja käyttäminen oli hankalaa. [94.] Suuremmassa järjestelmässä ilmaisen Splunk Free-version 500 megatavun päivärajoitus [87] tulee nopeasti vastaan, kun taas OSSIM-ohjelmistossa ei ole päiväkohtaisia rajoituksia kerätylle tiedolle. Demojärjestelmässä AlienVaultin käyttöönotto oli yksinkertaista ja lokienkeräys alkoi heti. Myös agenttien asennus ja tiedonkerääminen SNMP-protokollalla oli helppoa ja valmiit korrelointisäännöt olivat asennuksen jälkeen toiminnassa.

AlienVaultin mukaan OSSIM on mahdollista saada toimimaan yhdessä Splunkin kanssa. Tämän tyyppisessä kokoonpanossa Splunk hoitaa tehokkaasti ja skaalautuvasti tiedonkeruun. AlienVault korreloi kerätyn tiedon ja havaitsee uhkat. [95.]

### **5 Demoympäristö**

Demoympäristön tarkoituksena on kuvata käytännön tasolla SIEM-järjestelmän toimintaa. Demojärjestelmä on pienikokoinen ja sisältää ainoastaan pakolliset komponentit, joilla kuvataan SIEMin toimintaa. Ohjelmistoksi asennettiin AlienVault OSSIM, jolla kerättiin lokitietoa laitteilta ja seurattiin järjestelmään kohdistuneita hyökkäyksiä. Liitteessä 14 on demoympäristön verkkokuva.

Ympäristölle oli varattu C-luokan sisäverkko 192.168.65.0/24, mitä varten käytössä oli virtuaalilähiverkko VLAN 305. Tällöin järjestelmämme oli erillään laboratorion muista verkoista. HP ProLiant -palvelimella oli VMware ESXi -virtualisointialusta, jolle asennettiin kaikki käytetyt virtuaalipalvelimet.

Asiakaskoneita varten määritettiin Cisco 2960 Catalyst -kytkimelle VLAN-asetukset. Verkkohyökkäyksiä testattiin Kali Linux -käyttöjärjestelmällä, joka asennettiin Virtual-box-virtualisointiohjelmaan yhdelle asiakaskoneelle.

Demojärjestelmässä oli käytössä toimialuepalvelin, jonka käyttöjärjestelmänä oli Windows Server 2012 R2. Käytettävän toimialueen nimi oli siemdemo.ad. DC:lle lisättiin DNS-tietue, joka viittaa nimellä ossim.siemdemo.ad IP-osoitteeseen 192.168.65.30. Ubuntu 14.04 palvelimella, jonka nimi oli uef-demo2, ylläpidettiin web-, DNS- ja Samba-palveluita. Molemmille palvelimille asennettiin OSSEC-agentit, joilla kerättiin tietoa SIEM-järjestelmään.

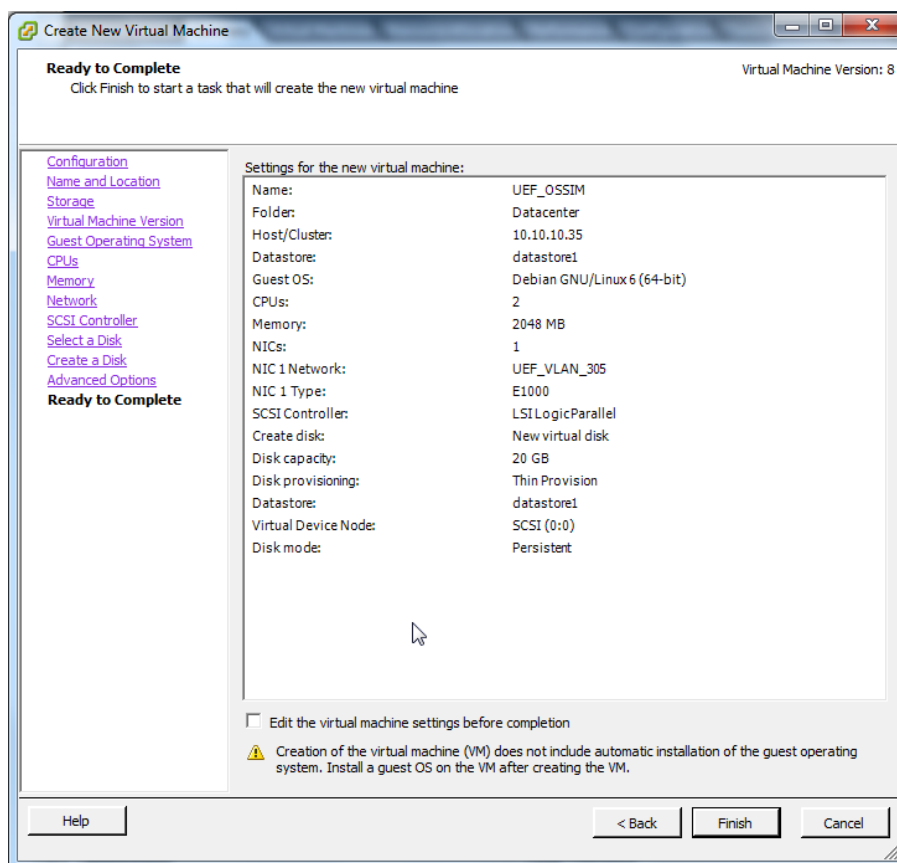
## **5.1 AlienVault OSSIM**

Tässä osiossa käsiteltiin AlienVault OSSIM -järjestelmän asennus, käyttöönotto ja testaus. Dokumentaation tarkoituksena oli kuvata SIEM-järjestelmän toimintaa käytännön tasolla eikä toimia käyttöönotto-ohjeena tuotantoympäristöä varten.

Osiossa kuvattiin käytännön esimerkkien avulla tiedonkulku datan keräämisestä eri kohteilta sen monitorointiin asti. Myös OSSIMin käyttöliittymän tärkeimmät osat ja järjestelmän erilaiset työkalut esiteltiin.

### 5.1.1 Asennus

AlienVault OSSIM asennettiin VMware ESXi -virtualisointialustalle käyttäen vSphere-hallintaohjelmaa. Virtuaalikoneelle määritettiin kuvan 5 mukaiset konfiguraatiot.



Kuva 5. AlienVault OSSIM -virtuaalikone

OSSIM:n asennus aloitettiin asettamalla levykuva virtuaalikoneeseen. Vaihtoehtoina asennukselle olivat AlienVault OSSIM 4.14 ja Sensor 4.14. Asennusta jatkettiin valitsemalla OSSIM (kuva 6).



Kuva 6. Asennuksen aloittaminen

Asennuksen seuraavassa vaiheessa määritettiin kieli- ja sijaintiasetukset. Näihin valittiin taulukon 4 mukaiset tiedot. Seuraavaksi asennusohjelma latsi asennuskomponentit levyltä, minkä jälkeen määritettiin verkkoasetukset taulukon 5 mukaisesti.

Taulukko 4. Kielivalinnat

| Asetus                       | Valinta     |
|------------------------------|-------------|
| Kieli (Language)             | English     |
| Sijainti (Location)          | Finland     |
| Kielimäärittys (Locales)     | en_US.UTF-8 |
| Näppäimistöasettelu (Keymap) | Finnish     |

Taulukko 5. Verkkoasetukset

| Verkkoasetus                           | Asetettu arvo |
|--|---------------|
| IP-osoite (IP address)                 | 192.168.65.30 |
| Aliverkonpeite (Netmask)               | 255.255.255.0 |
| Oletusyhdyskäytävä (Gateway)           | 192.168.65.1  |
| Nimipalvelimet (Name server addresses) | 172.16.32.20  |

Tämän kohdan jälkeen varsinainen asennus alkoi. Se oli ajallisesti pisin vaihe asennuksessa. Asennuksen jälkeen OSSIMin paikalliseen hallintakonsoliin kirjaututtiin syöttämällä root-tunnus ja salasana (kuva 7).

```

=====
===== http://www.alienvault.com =====
=====
==== Access the AlienVault web interface using the following URL: ====
                        https://192.168.65.30/
=====

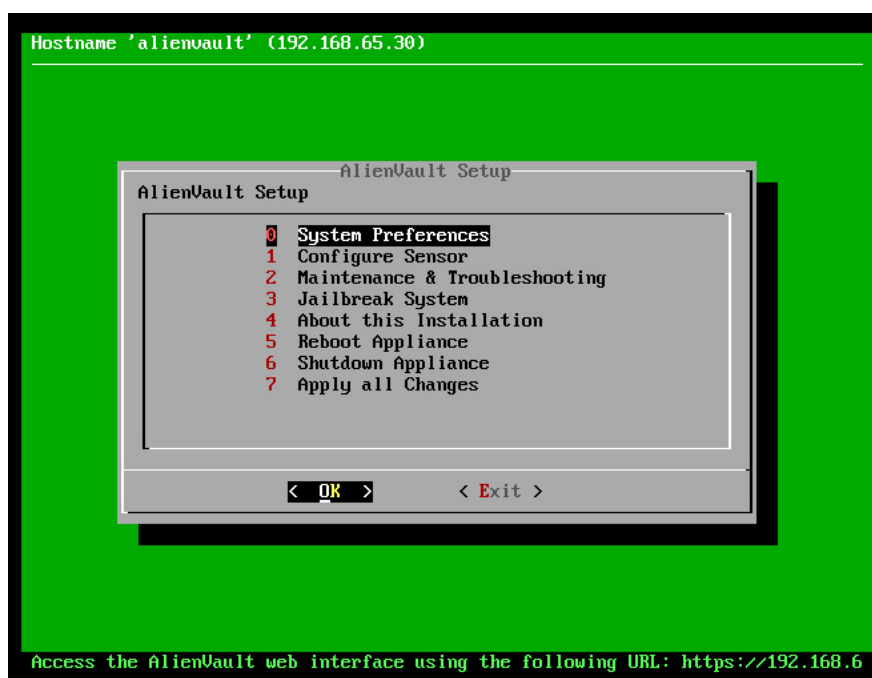
AlienVault USM 4.14 - x86_64 - tty1

alienvault login: root
Password: _

```

Kuva 7. Kirjautuminen paikalliseen hallintakonsoliin

Hallintakonsolinäkymä avautui kirjautumisen jälkeen (kuva 8). Asennuksen jälkeen konsoliin pystyi kirjautumaan myös SSH-yhteydellä. Asetuksia oli helppo muokata valikkopohjaisen käyttöliittymän kautta, missä oli yleisimmät perustoimenpiteet kuten järjestelmän sammuttaminen ja uudelleenkäynnistäminen.



Kuva 8. Paikallinen hallintakonsoli

System Preferences -kohdan alla pystyi muokkaamaan yleisiä asetuksia kuten käytössä olevia verkkokortteja, asettamaan DNS-palvelimen osoitteen, vaihtamaan hallintasalasanaa ja päivittämään järjestelmän. Sensoriasetukset määritettiin Configure Sensor -kohdasta. Tässä esimerkiksi muokataan seurattavia verkkoja, asetetaan hallintakäyttöön tarkoitetun IP-osoitteen sekä otetaan lisäosia käyttöön tai poistetaan niitä käytöstä.

Maintenance & Troubleshooting on järjestelmäongelmien selvittelyä varten. Alavalikoissa on työkaluja tietokantaongelmien korjaamiseen sekä lokien tyhjentämiseen tai tarkasteluun. Tarkasteltavia lokitietoja oli sekä AlienVault-komponenteilta että paikalliselta käyttöjärjestelmästä. Näitä olivat kern.log, dmesg, syslog, auth.log ja daemon.log. Järjestelmän toiminnan seurantaan oli valmiina htop-, netstat- ja bwm-ng-työkalut.

Mikäli web-käyttöliittymästä tai konsolin valikoista ei pystynyt tekemään jotain tehtävää, on valittavissa Jailbreak System -kohta. Tällöin palvelinta hallittiin suoraan komentorivipohjaisesta käyttöliittymästä, jossa voitiin muokata kaikkia palvelimen asetuksia. Pääasiallisesti OSSIM-järjestelmän hallinta tulisi kuitenkin tehdä web-pohjaisesta käyttöliittymästä [96].

Web-käyttöliittymään kirjauduttiin osoitteesta <https://ossim.siemdemo.ad> tai käyttäen IP-osoitetta <https://192.168.65.30>. Ensimmäisellä kerralla luotiin pääkäyttäjätili. Tiedot täytettiin kuvan 9 mukaisesti. Määritys päätettiin valitsemalla Start using AlienVault. Järjestelmä kysyi tämän jälkeen juuri luodut pääkäyttäjätunnukset kirjautuessa.

**Welcome**

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

If you need more information about AlienVault, please visit [AlienVault.com](https://www.alienvault.com).

### Administrator Account Creation

Create an account to access your AlienVault product.

*\* Asterisks indicate required fields*

FULL NAME \*

USERNAME \*


PASSWORD \*   
strong

CONFIRM PASSWORD \*   
strong

E-MAIL \*

COMPANY NAME

LOCATION  → [View Map](#)



[START USING ALIENVAULT](#)

Kuva 9. Pääkäyttäjätilin luonti

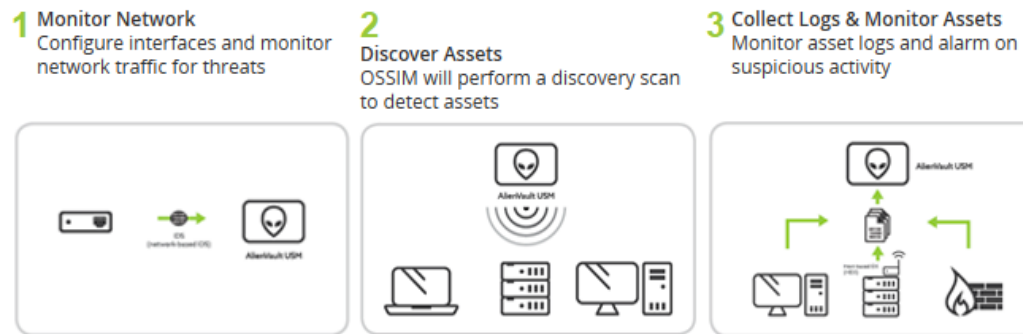
Ensimmäisen kirjautumisen jälkeen käyttöönoton voi suorittaa ohjatulla toiminnolla tai siirtymällä varsinaiseen web-näkymään suoraan valitsemalla Skip AlienVault Wizard. Tässä vaiheessa valittiin Skip-toiminto (kuva 10).





## Welcome to the AlienVault OSSIM Getting Started Wizard

You are about to use this wizard to configure the critical security capabilities provided by AlienVault OSSIM.



Once done you'll be ready to use AlienVault OSSIM. Now, go forth!

[Skip AlienVault Wizard](#)

**START**

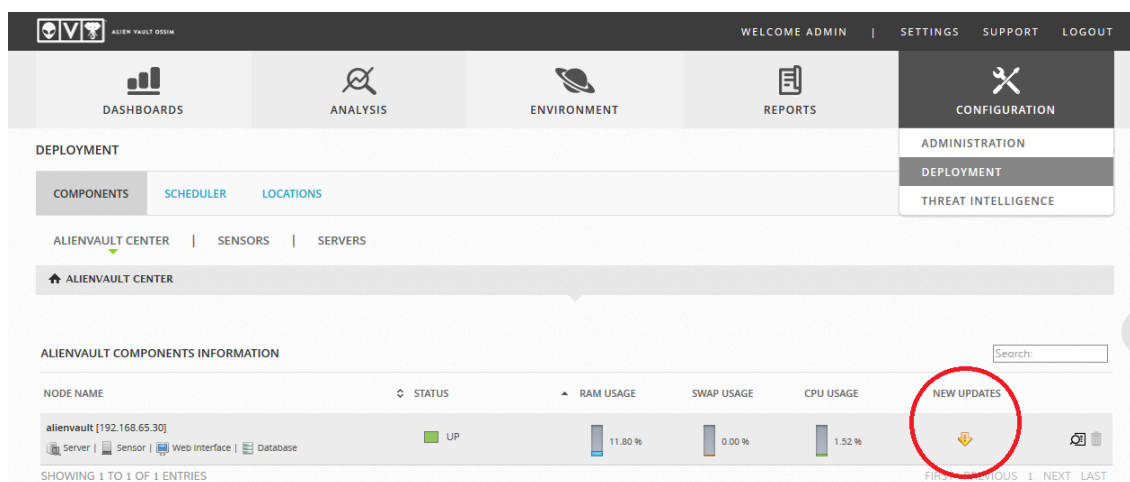
Kuva 10. Ohjattu käyttöönotto

Alkuperäiset virtuaalikoneen resurssit olivat liian vähäiset OSSIMin käyttöön. Asennuksen jälkeen OSSIM-palvelin saatiin siirrettyä vähemmän kuormitetulle Blade-palvelimelle, joten resursseja saatiin kasvatettua (kuva 11). Palvelimelle määritettiin käyttöön 16 GB keskusmuistia ja 6 prosessoriydintä.

| Hardware          | Summary   |
|-------------------|---|
| Memory            | 16384 MB  |
| CPUs              | 6   |
| Video card        | Video card                                      |
| VMCI device       | Restricted                                      |
| SCSI controller 0 | LSI Logic Parallel                              |
| Hard disk 1       | Virtual Disk                                    |
| CD/DVD drive 1    | [datastore1] AlienVault_OSSIM_64bits_4.14.0.iso |
| Network adapter 1 | UEF_VLAN305                                     |
| Floppy drive 1    | Client Device                                   |

Kuva 11. SIEM-palvelimen tiedot

Järjestelmälle oli saatavilla päivitys versioon 4.15. Päivitys asennettiin Configuration-välilehden alla olevasta Components-kohdasta (kuva 12). Samalla sivulla näkee järjestelmän käyttämän muistin määrän ja suorittimen käyttöasteen.



Kuva 12. Järjestelmän päivitys

Seuraavalla sivulla on nähtävissä päivityksen muutokset. Päivitys aloitettiin valitsemalla alareunasta Upgrade. Päivitys asentui muutamassa minuutissa. Opinnäytetyön aikana järjestelmään tuli useita pienempiä päivityksiä.

### 5.1.2 Laitteiden lisäys ja tiedon kerääminen

SIEM vaatii toimiakseen laitteilta tietoa, jota kerätään useilla tavoilla. Yrityksillä on tärkeää olla ajantasainen tieto järjestelmän laitekannasta, jolloin havaitaan tietoturvan osalta puutteellisia laitteita. OSSIM-järjestelmässä Environment-valikon alla olevasta Assets-kohdasta hallitaan laitelistaa. Laitteita on mahdollista lisätä käsin tai käyttää Asset Discovery -toimintoa.

Asset Discovery -toiminto tarkistaa automaattisesti yksittäisen laitteen, laiteryhmän, verkon tai verkkoryhmän tiedot (kuva 13). Mikäli kohteen tiedot ovat muuttuneet, tallennetaan muutokset uuden skannauksen jälkeen tietokantaan. Sensor Selection -kohdan alta määritetään sensori, jota käytetään verkkoskannauksessa. Valittavana on paikallinen sensori, automaattinen valinta, jossa käytetään ensimmäisen saatavilla olevaa sensoria tai tietyn sensorin valitseminen käsin. Lisäasetuksina on skannaustyyppi, joka vaikuttaa tarkistettavien porttien määrään. Timing Template -asetus vaikuttaa skannauksen nopeuteen, mutta käytettäessä liian suurta nopeutta voi osa tiedosta jäädä keräämättä. Lisäksi käyttöönotettavia ominaisuuksia ovat käyttöjärjestelmätunnistus ja käänteisnimipalvelu.

ASSETS

ASSETS ASSET DISCOVERY

NEW SCAN

TARGET SELECTION

Please, select the assets you want to scan:

siemverkko (192.168.65.0/24)

Type here to search assets

- All Assets
- Assets
- Asset Groups
- Networks
- 10.0.0.0/24
- 172.16.0.0/16
- 192.168.0.0/16
- 192.168.65.0/24
- siemverkko (192.168.65.0/24)
- Network Groups

DELETED ALL

SENSOR SELECTION

Local sensor Launch scan from the framework machine

Automatic sensor Launch scan from the first available sensor

SELECT AN SPECIFIC SENSOR

ADVANCED OPTIONS

Scan type: Normal

Timing template: Normal

Autodetect services and Operating System

Enable reverse DNS Resolution

START SCAN

Kuva 13. Asset Discovery

Uusia kohteita lisättiin käsin Add Assets -painikkeesta. Tärkeimmät määriteltävät kohdat olivat laitteen nimi, IP-osoite ja laitetyyppi (kuva 14). Tallentamisen jälkeen uusi laite oli Assets-listalla.

NEW HOST

Values marked with (\*) are mandatory

Name \* SW1

IP Address \* 192.168.65.2

FQDN/Aliases

Asset Value \* 2

External Asset \*  Yes  No

Sensors \*  192.168.65.30 (alienvault)

Description Cisco 2960 -kytkin

Thresholds \* C: 30 A: 30

Scan options  Availability Monitoring

Icon Allowed format: 16x16 png | jpg | gif image

Choose file ...

Location 80100 Joensuu, Finland

Latitude/Longitude 62.6011 29.7635

Devices Types Network Device Switch

ADD

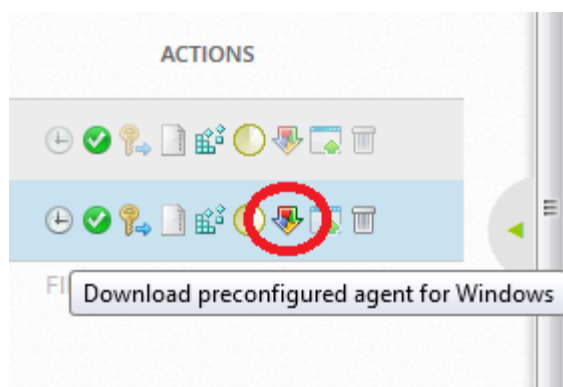
Network Device:Switch

CANCEL SAVE

Kuva 14. Uuden kohteen lisäys

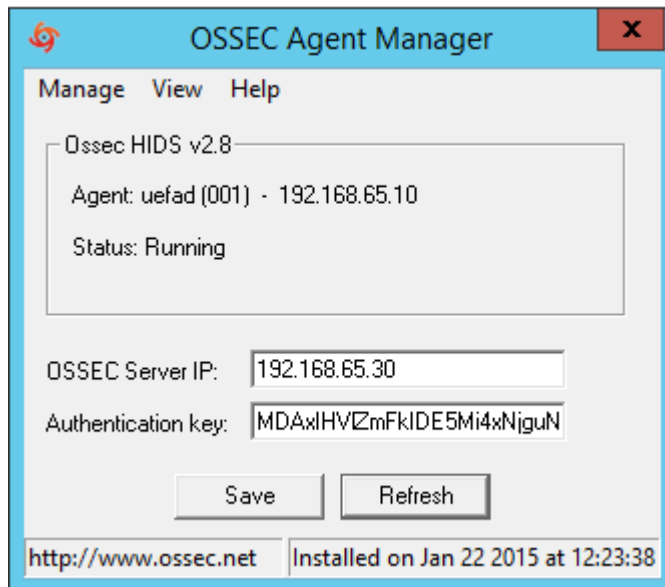
Listassa olevia kohteita voi lajitella näyttämään esimerkiksi vain ne, joilla on hälytyksiä, tapahtumia, haavoittuvuuksia tai määritetty value-arvo eli kohteen tärkeys. Laitteita etsitään listalta hakutoiminnolla, johon on määritettävissä useita suodattimia. Laitteen kohdalta Details-painikkeella saadaan tarkempi kuva laitteen tiedoista. Tämä näkymä jaetaan General-, Activity-, Location ja Notes-kohtaan. General-välilehdessä näkyy avoimena olevat portit, joiden saatavuutta OSSIM voidaan määrittää seuraamaan. Mikäli esimerkiksi www-palvelimen HTTP-portti ei vastaa, antaa ohjelmisto siitä hälytyksen. Activity-välilehti on laitteen hälytysten, tapahtumien ja verkkoliikenteen seuraamiseen. Location-välilehdellä esitetään laitteen sijainnin kartalla ja Notes-välilehti on muistiinpanoja varten.

Agenteilla tarkkailtavia laitteita sai lisättyä Environment-välilehden alta olevasta Detection-kohdasta välilehdeltä Agents. Uusi laite lisättiin valitsemalla alareunasta Add Agent. Laitteelle määritettiin nimi ja IP-osoite. Laite tuli näkyviin sivulla olevaan listaan. Sivulta ladattiin vielä kuvan 15 mukaisesta painikkeesta valmiiksi määritetty OSSEC-agentin asennustiedosto ja se siirrettiin DC-palvelimelle.



Kuva 15. Agentin lataaminen

OSSEC-agentti asentui asennusohjelman käynnistämisen jälkeen suoraan loppuun asti. Ohjelma asentui hakemistoon C:\Program Files (x86)\ossec-agent. Agentin toiminnan voi varmistaa OSSIM:in ja tarkkailtavan tietokoneen puolelta. Kun yhteys toimi, näkyi OSSIMin agents-sivun status-kohdassa Active. Jos yhteyttä ei saatu muodostettua, luki teksti Never Connected. Tarkkailtavalla tietokoneella toimivan yhteyden merkiksi OSSEC-agentin päänäkymässä oli OSSIM:ssa käytetty laitenimi uefad.



Kuva 16. OSSEC-agentti

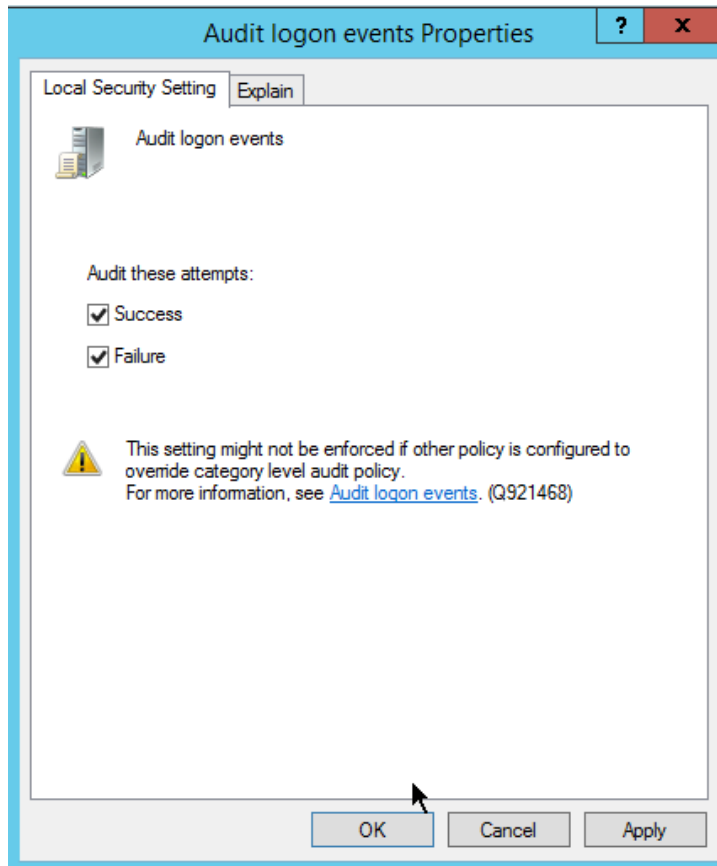
Mikäli yhteys ei toiminut, apua ongelman ratkaisemiseen sai valitsemalla View ja View Logs. OSSEC-agentti oli määritettävissä myös vianselvitystilaan (debug mode) muuttamalla agentin kansiossa olevasta internal\_options-conf-tiedostosta windows.debug-arvoksi 1 tai 2. Vianselvitystilassa agentin lokiin saatiin yksityiskohtaisempaa tietoa. Debug-tilan sai pois kokonaan asettamalla arvon 0. OSSEC-agentille oli mahdollista määrittää tarkkailtavia kohteita valitsemalla ohjelmasta View ja View Config.

Autentikointiavaimen sai tarvittaessa OSSIMista agents-sivulta valitsemalla Extract Key (kuva 17). OSSEC-agentissa avaimen sai syötettyä päänäkymään kohtaan Authentication key (kuva 16).



Kuva 17. Autentikointiavaimen haku OSSIM:sta

DC-palvelimen paikallisiin ryhmäkäytäntöihin määritettiin onnistuneiden ja epäonnistuneiden kirjautumisten merkintä tapahtumalokiin. Tapahtumalokin tiedot välittyvät OSSEC-agentilla SIEM-järjestelmään. Ryhmäkäytäntö määritettiin Group Policy Editor -työkalulla. Audit logon events -käytäntö oli puussa kohdassa Computer Configuration - Windows Settings - Security Settings - Local Policies - Audit Policy. Asetukset käytännölle määritettiin kuvan 18 mukaisesti.



Kuva 18. Kirjautumisten seuranta

Asetusten määrittämisen jälkeen DC-palvelimelle kirjaututtiin uudelleen. Kirjautumistieto siirtyi nyt OSSEC-agentin välityksellä SIEM-järjestelmään. Tapahtuma näkyi OSSIM:n Analysis-välilehden Security Events (SIEM) -kohdassa. Tapahtumia on mahdollista suodattaa esimerkiksi ajankohdan, sisällön ja osoitteiden perusteella. OSSIM normalisoi tapahtuman tiedot automaattisesti yhtenäiseen muotoon (kuva 19).

|                  |                                      |                            |                                 |                        |           |           |
|------------------|--------------------------------------|----------------------------|---------------------------------|------------------------|-----------|-----------|
| NORMALIZED EVENT | DATE                                 | ALIENVAULT SENSOR          | INTERFACE                       |                        |           |           |
|                  | 2015-01-29 08:28:55 GMT+2:00         | alienvault [192.168.65.30] | eth0                            |                        |           |           |
|                  | TRIGGERED SIGNATURE                  | EVENT TYPE ID              | CATEGORY                        | SUB-CATEGORY           |           |           |
|                  | ossec: Windows Logon Success.        | 18107                      | Authentication                  | Login                  |           |           |
|                  | DATA SOURCE NAME                     | PRODUCT TYPE               | DATA SOURCE ID                  |                        |           |           |
|                  | ossec-authentication_success         | Authentication and DHCP    | 7009                            |                        |           |           |
| SOURCE ADDRESS   | SOURCE PORT                          | DESTINATION ADDRESS        | DESTINATION PORT                | PROTOCOL               |           |           |
| 192.168.65.10    | 0                                    | 192.168.65.10              | 0                               | TCP                    |           |           |
| SIEM             | UNIQUE EVENT ID#                     | ASSET S → D                | PRIORITY                        | RELIABILITY            | RISK      |           |
|                  | a78011e4-903b-0050-56bf-477e19778770 | 2 → 2                      | 3                               | 1                      | 0         |           |
|                  | USERNAME                             | USERDATA1                  | USERDATA2                       | USERDATA3              | USERDATA4 | USERDATA5 |
|                  | Administrator                        | 3                          | windows.authentication_success. | Windows Logon Success. | 4624      | 3         |
|                  | USERDATA6                            | USERDATA7                  | USERDATA8                       | USERDATA9              |           |           |
| SIEMDEMO         | 0x2e98f7                             | -                          | L30                             |                        |           |           |

Kuva 19. Kirjautumistapahtuma näkyi OSSIMissa

OSSEC-agentti asennettiin myös Ubuntu-palvelimelle. Ennen OSSEC-agentin lataamista Ubuntu 14.04 -palvelimelle asennettiin build-essential-paketti, joka on vaadittu, agentin kääntämiseksi lähdekoodista. Agentti ladattiin wget-työkalulla tmp-hakemistoon. Ladatakset paketti purettiin tar-komennolla. Ubuntu käyttää oletuksena Dash-komentotulkkiä, mutta tällä asennus epäonnistuu. Tämän takia asennuksessa käytettiin Bash-komentotulkkiä. [97] Käytetyt komennot on lueteltu alla.

```
sudo apt-get install build-essential
cd /tmp
wget http://www.ossec.net/files/ossec-hids-2.8.1.tar.gz
tar -xvzf ossec-hids-2.8.1.tar.gz
cd ossec-hids-2.8.1/
sudo /bin/bash ./install.sh
```

Asennusohjelma oli interaktiivinen ja kysyi käyttäjältä halutut asennusvaihtoehdot. Alussa valittiin käytettäväksi kieleksi englanti, joka on myös oletuskielenä. Asennustyyppiä valittiin agentti, koska tältä palvelimelta oli tarkoitus kerätä ja lähettää tietoa OSSIM-palvelimelle. OSSEC Agent asennettiin /var/ossec-kansioon, joka oli myös oletusasennushakemistona. OSSEC HDS server -kohtaan asetettiin OSSIM-palvelimen IP-osoite 192.168.65.30. Loput asetukset annettiin olla oletusarvoina. Asetukset ovat liitteessä 15.

Asennuksen jälkeen uusi agentti lisättiin OSSIM-hallintakäyttöliittymästä kuten aiemmin tässä osiossa Windows-palvelimen osalta. Komennolla `sudo /var/ossec/bin/manage_agents` avautui työkalu, johon autentikointiavain kopioitiin (liite 16). Lopuksi palvelu käynnistettiin uudelleen komennolla `sudo /etc/init.d/ossec restart`.

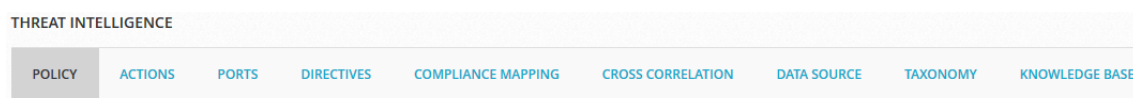
OSSIM-ohjelmistossa testattiin kohteiden seuranta ilman agenttia SNMP-protokollalla. Tätä varten Cisco 2960 -kytkimeen määriteltiin IP-osoite 192.168.65.2 VLAN 305 -virtuaalilähiverkolle. Tämän jälkeen kytkin asetettiin lähettämään SNMP Trap -ilmoituksia OSSIM-palvelimen IP-osoitteeseen. NTP-palvelu asetettiin käyttöön, jotta kellonaika oli oikea. Muuten kytkimen lokitiedot olisivat väärässä ajassa. Lisäksi kytkimeen määritettiin salasanojen salaus, SSH-yhteys sekä Privileged EXEC -tilan salasana. Kytkimen konfiguraatio on kokonaisuudessaan liitteessä 17. SNMP-toiminnon käyttöönottoon tarvittavat asetukset tehtiin alla olevilla komennoilla.

```
SW1(config)#interface vlan305
SW1(config-if)#ip address 192.168.65.2 255.255.255.0
SW1(config)#logging trap notifications
SW1(config)#logging 192.168.65.30
```

OSSIM-palvelimella kytkin lisättiin Assets-kohtaan. Tämän jälkeen kytkimelle määritettiin Details-välilehden alta Plugins-kohdasta käytettävä lisäosa. Cisco 2960 -kytkimelle ei löytynyt suoraan sopivaa, joten tässä käytettiin 300-sarjalle tarkoitettua lisäosaa.

### 5.1.3 Threat intelligence

Järjestelmän toimintakykyä saa paranneltua Configuration-välilehden Threat Intelligence -osiossa (kuva 20). Policy-kohdassa voidaan määrittää käytäntöjä tapahtumien käsitteilyyn. Käytännöille määritetään, minkä tapahtuman perusteella suoritetaan toimintoja (Actions). Näille tapahtumille määritetään seuraukset (Policy Consequences). Esimerkiksi tietyn tyyppisestä tietoturvatapahtumasta lähetetään sähköpostivaroitus, avataan tiketti tai käynnistetään erillinen sovellus. Actions-kohdassa on mahdollista määrittää uusia toimintoja.



Kuva 20. Threat Intelligence -valikot

OSSIM sisältää oletuksena yleisimmät käytetyt portit. Portteja voi lisätä ja ryhmitellä Ports-kohdasta. Jokaiselle portille määritetään numero, protokolla, palvelu ja kuvaus. Porttilistaan kannattaa lisätä oman ympäristön käyttämät portit, joita ei listalla vielä ole.

Directives-kohdassa on mahdollista muokata ja lisätä toimintamalleja eri tapahtumasarjoille. Liitteessä 18 on esimerkkinä toimintamalli SSH-brute-force-hyökkäyksen havaitsemiseen. Tässä mallissa tarkastetaan epäonnistuneiden SSH-tunnistautumisten lukumäärää. Mitä useammin tapahtuma toistuu, sitä suuremmaksi luotettavuus kasvaa. Directive Info -kohdassa määritetään, minkä tyyppisiä hälytyksiä toimintamalli laukaisee. Knowledge DB -kohdassa on määritettävissä tapahtumalle kuvaus ja suositeltavat toimenpiteet.

AlienVault OSSIM tukee standardeja ISO 27001, PCI DSS 2.0 ja PCI DSS 3.0. Näiden pohjalta on mahdollista tehdä määrittämiä Compliance Mapping -kohdassa. Kuvassa 21 on esimerkkinä kohta PCI DSS 3.0 -vaatimuksesta. Vaatimusta vastaavia tietoturvatapahtumia saa määritettyä Data Sources -kohdasta sivun oikeasta laidasta.



R.8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

```
directive_event: AV-FREE-FEED Bruteforce attack, login authentication attack against DST_IP  
directive_event: AV-FREE-FEED Bruteforce attack, Windows authentication attack against DST_IP  
directive_event: AV-FREE-FEED Bruteforce attack, NetBIOS/Samba authentication attack against SRC_IP  
directive_event: AV-FREE-FEED Bruteforce attack, SIP authentication attack against SRC_IP  
directive_event: AV-FREE-FEED Bruteforce attack, HTTP authentication attack against SRC_IP  
directive_event: AV-FREE-FEED Bruteforce attack, Telnet authentication attack against SRC_IP
```

Kuva 21. PCI DSS 3.0 -standardin 8.1.6-vaatimukseen liitetyt tapahtumatyytit

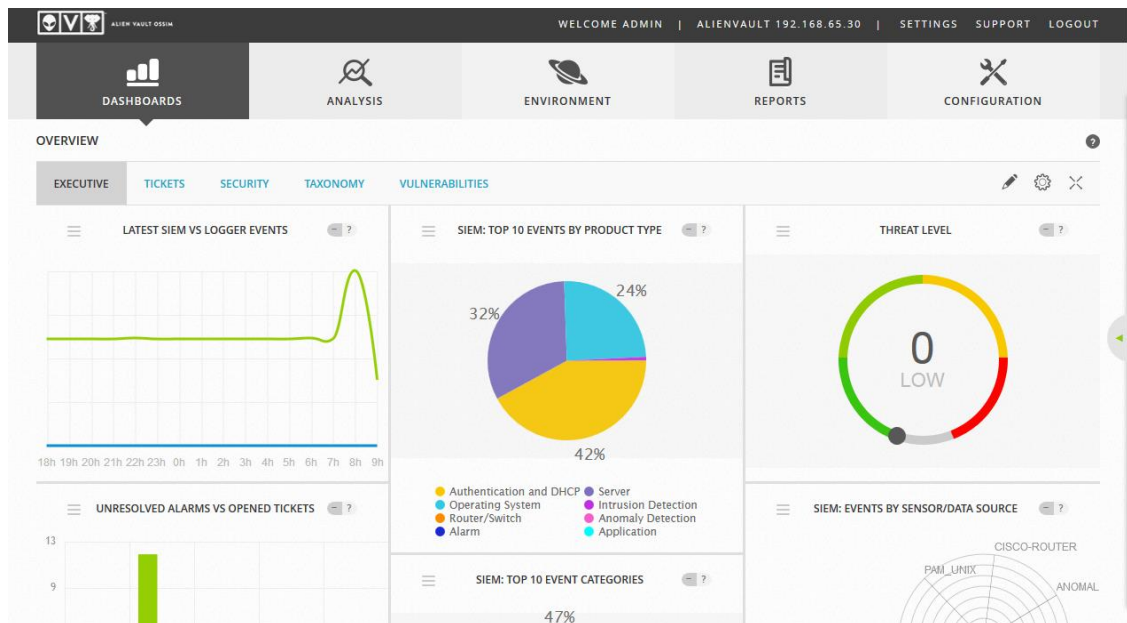
Tiedon korrelointiin AlienVaultissa on laaja kokoelma valmiita korrelointisääntöjä. Sääntöjä saa muokattua ja lisättyä vastaamaan omia tarpeita. Ristiinkorrelointisääntöjen muokkaus on mahdollista Cross Correlation -kohdassa.

Taxonomy-kohdassa luokitellaan tietolähteitä erilaisten kategorioiden alle. Kategorioita voi muokata ja lisätä vapaasti. OSSIM tukee taksonomiapohjaista korrelointia [98].

Knowledge Base -osiossa on mahdollista muokata ja määrittää uusia kuvauksia tapahtumille. Tapahtumien kuvauksiin voidaan koostaa tekstiä, joka sisältää muuttujina esimerkiksi laitteiden tietoja. Kuvaukset sisältävät toimintaohjeita ongelman ratkaisemiseen.

## 5.1.4 Monitorointi

OSSIM-päänäkymä avattiin Dashboards-välilehdeltä valitsemalla Overview. Kuvan 22 näkymässä oli yleiskuva järjestelmän nykytilasta. Tämä jakautui viiteen eri välilehteen, joista jokainen oli mukautettavissa. Välilehtien oikealla puolella olevista painikkeista sai muokattua ulkoasua, asetettua käyttäjille oikeuksia eri välilehtiin sekä avattua näkymän uuteen ikkunaan koko näytöllä tapahtuvaa tarkastelua varten.



Kuva 22. OSSIM-päänäkymä

Korkeantason näkymässä (Executive) on tilastotietoa tietoturvaan liittyvistä tapahtumista erilaisina kuvaajina, joissa on järjestelmän ympäristön tapahtumien yleistiedot. Tässä on esitetty esimerkiksi tapahtumien määrä eri aikoina, eri tapahtumatyyppien jakautuminen, tikketitilanne sekä ympäristön uhkataso.

Tikettien tilastotiedot ovat nähtävissä Tickets-välilehdellä. Kohdassa voi esimerkiksi tarkkailla avonaisia tikettejä ja tikkettien ratkaisuaikoja. OSSIM tilastoi tikketit myös eri tyyppien mukaan.

Security-välilehdellä on esitetty tietoturvan yhteenveto. Kymmenen epäilyttävintä kohdetta on listattu tapahtumamäärien perusteella. Tämän avulla on mahdollista havaita, mikäli joillakin kohteilla on haitallista toimintaa. Tietoturvatapahtumien kehittymisen seuraamiseen tässä näkymässä on kuvaajat, joissa on niiden lukumäärä kuluneen päivän ja viikon ajalta. Lisäksi erilaiset tietoturvahälytykset- ja tapahtumat on listattu tyyppin perusteella. Valitsemalla jokin tyyppi tai ajankohta päästään tarkastelemaan siihen liittyviä lo-kitapahtumia.

Taxonomy-välilehdellä tapahtumatyypit on luokiteltuna eri ryhmiin. Välilehdellä tapahtumat on jaettu virus- ja haittaohjelmahavaintoihin, autentikoinnin onnistumiseen ja epäonnistumiseen, palomuurisääntöjen jakautumiseen estettyihin ja sallittuihin yhteyksiin, järjestelmätapahtumiin sekä hyväksikäyttötyyppeihin. Vulnerabilities-välilehdellä haavoittuvuudet voidaan listata vakavuuden, palveluiden, kohteiden tai verkkojen mukaan.

### **5.1.5 Tiedon analysointi**

Lokitiedon analysointi ja tikettien hallinta tapahtuu päävalikossa olevassa Analysis-välilehdessä. Sen alla olevassa Alarms-kohdassa seurattavaan ympäristöön kohdistuneet tietoturvaohjelmat esitetään aikajanalla. Tämän alapuolella hyökkäykset on listattu erikseen. Eri kohdista saa lisätietoa valitsemalla sen.

Security Events (SIEM) -kohta on lokitiedon tarkastelua varten. Tässä valittavana on kaiken tapahtumatiedon tai reaaliaikaisen tiedon seuraaminen. Monipuolisella hakutoiminnolla suuresta tietomäärästä on mahdollista löytää tärkeät tapahtumat. Ehtoina käytettävissä on esimerkiksi riskitaso, tapahtumatyyppi, kohteen tyyppi, nimi, IP-osoite tai aika-väli.

Uusi ikkuna avautuu valitessa tietyn tapahtuman. Yläreunassa on kuvattu normalisoidut tiedot, jotka ovat kaikissa tapahtumissa samassa järjestyksessä. Tämä helpottaa eri loki-muotoilustandardeja käyttävien kohteiden välistä vertailua. Alapuolella on OSSIMin Taxonomy-tiedoista saatu kuvaus tapahtumaan liittyen, mikä voi auttaa vianselvityksessä. Alimpana on lokitieto raakamuodossa, jossa se on ennen normalisointia.

AlienVault USM -ohjelmistossa on mahdollisuus luoda lokitiedosta digitaaliset allekirjoitukset ja aikaleimat, jolloin lain vaatima tiedon luotettavuus ja eheys on mahdollista varmistaa. Myös pakkaus on mahdollista ottaa käyttöön tallennustilan säästämiseksi. [99] OSSIM-järjestelmässä Raw Logs -kohdassa on pelkästään mainos maksullisen USM-version ominaisuuksista.

## 5.2 Hyökkäyksen havaitseminen

AlienVault OSSIM pystyi havaitsemaan erilaisia verkkohyökkäystyyppejä. Ominaisuu- den testaamiseksi virtuaalikoneeseen asennettiin ilmainen avoimen lähdekoodin Kali Li- nux -käyttöjärjestelmä, jossa on valmiina satoja työkaluja eri haavoittuvuuksien testaa- miseen [100].

Esimerkkeinä teimme kaksi erilaista hyökkäystä. Ensimmäinen hyökkäys oli brute-force- tyyppinen ja toinen DoS-tyyppinen.

### 5.2.1 Brute-force-hyökkäys

Hydra on salasanojen murtamiseen tarkoitettu työkalu. Se tukee esimerkiksi SSH-, FTP-, SMB- sekä HTTP-protokollia. Salasanoja ja käyttäjätunnuksia voi yrittää murtaa brute- force-hyökkäyksillä tai valmiilla salasanalistailla. [101]. Salasanahyökkäystä testattiin OSSIM-palvelimen IP-osoitteeseen. Hyökkäyksessä käytettiin brute-force-tekniikkaa, jolloin murtoyrityksiä oli helppo luoda paljon.

SSH-hyökkäykseen käytettiin Hydra-työkalua. Kuvassa 23 näkyy käytetty komento pa- rametreineen sekä salasanoja, joilla ohjelma yritti kirjautua järjestelmään. Käytettyjen pa- rametrien kuvaukset on listattu alla.

-t (tasks), määrittää kuinka monta yhteyttä otetaan yhtä aikaa kohteeseen [102].

-V (verbose mode), näyttää salasanat, joilla kohdejärjestelmään yritetään kirjautua tällä hetkellä. [102]

-f, lopettaa brute-force-hyökkäyksen, kun oikea salasana löytyy [102].

-l (login), käyttäjätunnus, jonka salasanaa yritetään murtaa. Voidaan myös käyttää val- miita käyttäjätunnuslistoja. [102].

-x, käytetään brute-force-hyökkäyksissä. Tämän parametrin jälkeen määritetään käytettä- vien merkkien määrä muodossa x:y:z, joista x on murrettavan salasanan minimipituus, y on maksimipituus arvattavalle salasanalle ja z on käytettävä merkistö. [101.]

```

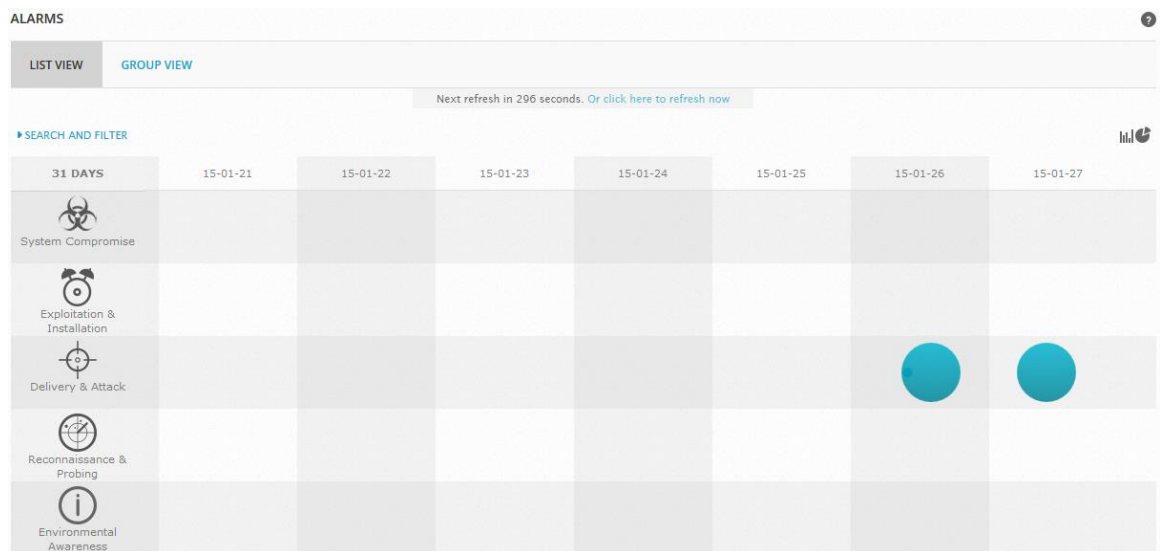
root@kali:~# hydra -t 4 -V -f -l user -x 12:14:a ssh://192.168.65.30
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-01-27 11:48:55
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] 4 tasks, 1 server, 2576581829865418752 login tries (l:1/p:2576581829865418752), ~644145457466354688 tries per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaa" - 1 of 2576581829865418752 [child 0]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaab" - 2 of 2576581829865418752 [child 1]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaac" - 3 of 2576581829865418752 [child 2]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaad" - 4 of 2576581829865418752 [child 3]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaee" - 5 of 2576581829865418752 [child 0]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaaf" - 6 of 2576581829865418752 [child 2]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaag" - 7 of 2576581829865418752 [child 1]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaah" - 8 of 2576581829865418752 [child 3]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaai" - 9 of 2576581829865418752 [child 0]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaaj" - 10 of 2576581829865418752 [child 2]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaak" - 11 of 2576581829865418752 [child 1]
[ATTEMPT] target 192.168.65.30 - login "user" - pass "aaaaaaaaaaaal" - 12 of 2576581829865418752 [child 3]
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@kali:~#

```

Kuva 23. Brute-force-hyökkäys Hydra-työkalulla

Brute-force-hyökkäys näkyi Alarms-välilehdellä. Hyökkäyksestä OSSIM piirsi listanäkymään hyökkäyksen laajuutta kuvaavan pallon (kuva 24).



Kuva 24. Hälytys hyökkäyksestä graafisesti

Tapahtuneesta sai tarkemman kuvan valitsemalla kyseisen hälytyksen. Brute-force-hyökkäyksestä OSSIM listasi yksittäiset yrityskerrat erikseen. Tapahtumalle järjestelmä määritteli risikitason automaattisesti. Hälytystapahtumasta avattiin tiketti valitsemalla alareunasta Open Ticket (kuva 25).

ALARMS

LIST VIEW GROUP VIEW

Alarms > AV-FREE-FEED Bruteforce attack, SSH service authentication attack against

Bruteforce Authentication — SSH

Open >1116 Events 2 Risk > 5 mins

| SOURCE  | DESTINATION  | KNOWLEDGE BASE  |
|---|--|---|
| <p>192.168.65.122</p> <p>Location: Unknown</p> <p>OTX: No</p> <p>Ports: 51940 51941 51942 51943 51944 52082 52083 52084 52089 52189</p> | <p>192.168.65.30</p> <p>Location: Unknown</p> <p>OTX: No</p> <p>Ports: SSH</p> | <p>AlienVault Incident Response: Alarm / Bruteforce</p> <p>A possible BruteForce has been detected via correlating events seen on the network. Brute Force attempts are one of the few things in security that are identifiable by their volume, not their type; while a system can be exploited with as little as a single packet of data, brute-force intrusion requires greater numbers to achieve. This presents a problem in determining the validity of a brute-force attempt, as opposed to just a broken system. One system repeatedly trying to log into the same account (and failing), over and over again, is visibility different from a single system trying thousands of different accounts and passwords. Not all brute-force attempts will be about account credentials, any attempt to gain access to something through trial-and-error repetition is a brute force</p> |

EVENT DETAIL SOURCE (1) DESTINATION (1)

| # | ALARM                 | RISK | DATE                | SOURCE               | DESTINATION       | CORRELATION LEVEL |
|---|-----------------------|------|---------------------|----------------------|-------------------|-------------------|
| 1 | SShd: Failed password | 0    | 2015-01-27 11:44:27 | 192.168.65.122-52413 | 192.168.65.30:ssh | 6                 |
| 2 | SShd: Failed password | 0    | 2015-01-27 11:44:27 | 192.168.65.122-52409 | 192.168.65.30:ssh | 6                 |
| 3 | SShd: Failed password | 0    | 2015-01-27 11:44:27 | 192.168.65.122-52392 | 192.168.65.30:ssh | 6                 |
| 4 | SShd: Failed password | 0    | 2015-01-27 11:44:27 | 192.168.65.122-52410 | 192.168.65.30:ssh | 6                 |

FEEDBACK TO OTX OPEN TICKET CLOSE ALARM

Kuva 25. Tarkemmat tiedot hyökkäyksestä

Valinnan jälkeen avautui ikkuna, jossa määrättiin tiketti administrator-tilille. OSSIM täytti tapahtuman perustiedot automaattisesti. Prioriteetin ja tyypin voi halutessaan muuttaa (kuva 26).

Values marked with (\*) are mandatory

NEW TICKET

|                         |   |
|-------------------------|---|
| TITLE *                 | AV-FREE-FEED Bruteforce attack, SSH service authentication attack against D |
| ASSIGN TO *             | User: administrator   |
| PRIORITY *              | 2   |
| TYPE *                  | Anomalies   |
| SOURCE IPS              | 192.168.65.122  |
| DEST IPS                | 192.168.65.30   |
| SOURCE PORTS            | 52266   |
| DEST PORTS              | 22  |
| START OF RELATED EVENTS | 2015-01-27 09:39:27   |
| END OF RELATED EVENTS   | 2015-01-27 09:49:06   |

SAVE

Kuva 26. Tikeinluonti hälytystapahtumasta

Tikeit mahdollistavat tapahtumien paremman hallinnan ja varmistavat, että vastuhenkilö hoitaa tapauksen loppuun. Analysis-välilehden alla olevalta Tickets-sivulta on mah-

dollista määrittellä tiketeille tarkempia kuvauksia ja liittää tapahtumaan liittyviä liitetiedostoja. Tiketti on suljettavissa vastuuhenkilön ratkaistua tapauksen. Ratkaistulle tiketille voi kirjoittaa tehdyt toimenpiteet ja tapahtuma on määritettävissä toisen henkilön tutkitavaksi. Liitteessä 19 on esimerkki yhdestä tiketistä.

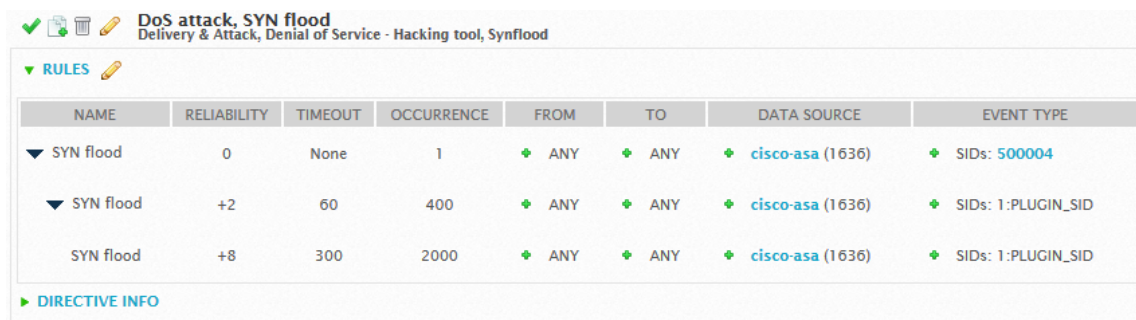
Tiketit säilyvät järjestelmässä myöhempää käyttöä varten ja ongelmien toistuessa vanhoista tiketeistä voi löytyä apua ongelmien ratkaisuun, joten ratkaisut on hyvä kuvata mahdollisimman tarkasti.

## 5.2.2 DoS-hyökkäys

Toisessa hyökkäysesimerkissä käsittelemme omien korrelointisääntöjen määrittämistä ja näiden aiheuttamia hälytyksiä. Hyökkäysmenetelmänä tässä osiossa käytämme SYN flood -tyyppistä DoS-hyökkäystä.

Demoympäristöön asennettiin tätä esimerkkiä varten Cisco ASA 5505 -palomuurilaite. Tähän asetettiin peruskonfiguraatiot, jossa määritettiin sisä- ja ulkoverkko. Lokitiedon keräämistä varten palomuri asetettiin lähettämään syslog-tietoja OSSIMiin. Laitteen konfiguraatiot ovat liitteessä 20.

OSSIMiin määritettiin Correlation Directive -sääntö hyökkäyksen havaitsemiseksi (kuva 27). Säännölle määritettiin nimeksi DoS attack, SYN flood. Korrelointisääntö kasvattaa tapahtuman luotettavuutta (Reliability) tietyn aikavälin sisällä ilmenneiden tapahtumien määrään. Priority-arvoksi säännölle asetettiin 3. Sääntöjä oli mahdollista luoda ja muokata myös XML-muodossa tiedostossa `/etc/ossim/server/a54e392b-9b0f-11e4-88ca-005056bf477e/user.xml` (kuva 28).

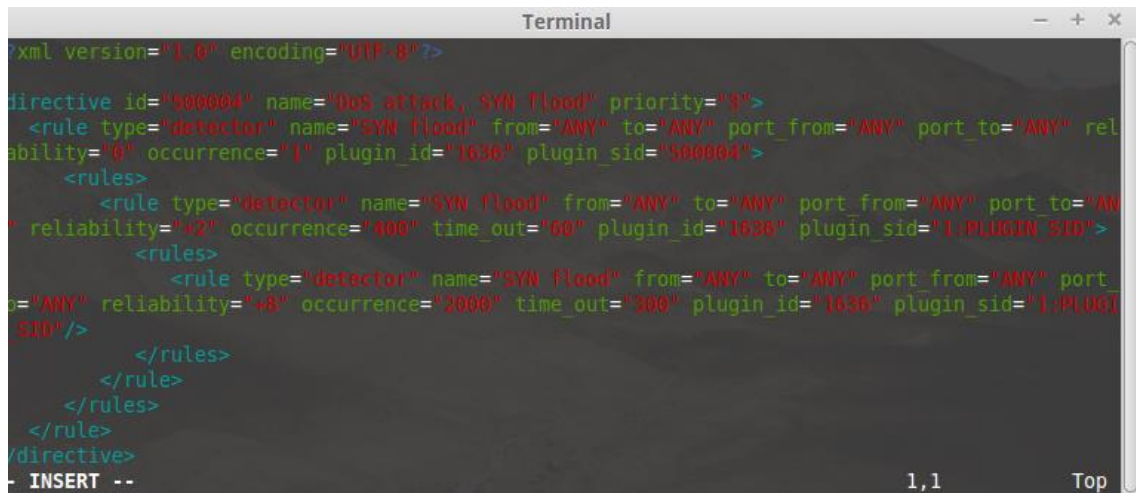


The screenshot shows the OSSIM interface for configuring a rule. The rule is named 'DoS attack, SYN flood' and is categorized as 'Delivery & Attack, Denial of Service - Hacking tool, Synflood'. The 'RULES' section is expanded to show a table of rules.

| NAME      | RELIABILITY | TIMEOUT | OCCURRENCE | FROM | TO  | DATA SOURCE      | EVENT TYPE         |
|-----------|-------------|---------|------------|------|-----|------------------|--------------------|
| SYN flood | 0           | None    | 1          | ANY  | ANY | cisco-asa (1636) | SIDs: 500004       |
| SYN flood | +2          | 60      | 400        | ANY  | ANY | cisco-asa (1636) | SIDs: 1:PLUGIN_SID |
| SYN flood | +8          | 300     | 2000       | ANY  | ANY | cisco-asa (1636) | SIDs: 1:PLUGIN_SID |

Below the table, there is a section for 'DIRECTIVE INFO'.

Kuva 27. Korrelointisääntö web-käyttöliittymässä



```

Terminal
'xml version="1.0" encoding="UTF-8"?>
directive id="500004" name="DoS attack, SYN Flood" priority="3">
  <rule type="detector" name="SYN flood" from="ANY" to="ANY" port_from="ANY" port_to="ANY" reliability="0" occurrence="1" plugin_id="1636" plugin_sid="500004">
    <rules>
      <rule type="detector" name="SYN Flood" from="ANY" to="ANY" port_from="ANY" port_to="ANY" reliability="+2" occurrence="400" time_out="60" plugin_id="1636" plugin_sid="1.PLUGIN_SID">
        <rules>
          <rule type="detector" name="SYN flood" from="ANY" to="ANY" port_from="ANY" port_to="ANY" reliability="+8" occurrence="2000" time_out="300" plugin_id="1636" plugin_sid="1.PLUGIN_SID"/>
        </rules>
      </rule>
    </rules>
  </rule>
</directive>
- INSERT --
1,1 Top

```

Kuva 28. Korrelointisääntö XML-muodossa

Hping3 on komentorivipohjainen työkalu, jolla voidaan luoda ja analysoida verkkoliikennettä. Työkalua käytetään myös DoS-hyökkäysten tekemiseen tai niiden testaamiseen. [103.]

SYN flood -hyökkäyksessä kohteeseen lähetetään TCP-protokollan kolmivaiheisen käsittelyn SYN-paketteja. Kuitenkaan hyökkääjä ei vastaa kohteen lähettämään SYN-ACK-pakettiin, jota kohde jää odottamaan. Liikennettä lähetetään niin paljon, ettei kohde pysty vastaamaan sallittuihin yhteyksiin. Usein hyökkäyksissä myös huijataan lähteen IP-osoite. [104.]

Esimerkissä käytettiin DoS-hyökkäystä, jossa hping3-työkalulla (kuva 29) lähetettiin SYN-paketteja jatkuvasti palomuriin. Tässä tarkoituksena oli luoda palomuurille liikennettä, joka loi tapahtumatietoa sen lokiin ja lähetettiin SIEMiin. Käytettyjen parametrien kuvaukset on listattu alla.

-S(syn), lähetetään SYN-paketteja [103].

--flood, pakettien lähettäminen mahdollisimman nopeasti näyttämättä vastauspaketteja [103].



```

root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali:~# hping3 -S --flood 10.0.0.1
HPING 10.0.0.1 (eth0 10.0.0.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Kuva 29. SYN-flood-hyökkäys

OSSIM laskee tapahtumalle riskiarvon (ROE) kappaleessa 6.8.2 esitetyn laskukaavan mukaisesti. Riskiarvon ollessa yhtä suurempi tapahtumasta tulee hälytys Alarms-välilehdelle (kuva 30). Lopuksi hälytyksestä oli mahdollista avata tiketti samalla tavalla kuin luvussa 7.2.1 on esitetty.

Alarms > DoS attack, SYN flood

Denial of Service - Hacking tool — Synflood Open >2401 Events 2 Risk

| SOURCE   | DESTINATION  |
|--|--|
| <p>10.0.0.3</p> <p>Location: Unknown</p> <p>OTX: No</p> <p>Ports 39940 39944 39945 39946<br/>39947 44030 44031 44032<br/>44033 44034</p> | <p>10.0.0.1</p> <p>Location: Unknown</p> <p>OTX: No</p> <p>Ports Unknown</p> |

Kuva 30. Hyökkäyksen aiheuttama hälytys

## 6 Pohdinta

Opinnäytetyö tehtiin parityönä. Jaoin molemmille päiväkohtaisia kirjoittamistavoitteita ja jokaisen päivän päätteeksi yhdistimme valmiit tekstit. Tämän jälkeen tarkastimme yhdessä molempien tuotokset ja teimme korjauksia. Työn aikana pidimme päiviä, jolloin tarkastimme kaiken siihen asti kirjoitetun tekstin ja korjasimme sekä asiasisältöä että kieliasua. Pidimme päiväkirjaa tehdystä työstä ja suunnittelimme tulevien päivien ohjelmaa noin viikoksi eteenpäin.

Opinnäytetyön aihe oli molemmille täysin uusi. Aluksi keskityimme tiedon hankkimiseen ja teorian käsittelyyn. Ongelmallista oli kirjoittaa valmistajien tuotteista, koska tietoa oli niukasti saatavilla ja se ei ollut aina neutraalia. Eri valmistajista oli saatavilla hyvin eritasoisia lähdemateriaalia, joten niistä kertominen yhdenmukaisesti oli haastavaa. Osa tästä materiaalista oli pelkkää mainostekstiä, jossa keuhuttiin omia tuotteita kilpailijoita paremmiksi. Haastavinta opinnäytetyössä oli laadukkaan lähdemateriaalin löytäminen ja sen soveltaminen.

SIEM-aiheiset artikkelit olivat usein melko yleisluontoisia eikä niissä selitetty asioita tarpeeksi syvällisesti. Suurin osa lähteistä oli verkkosivuja, mutta käytössä oli myös ainoa aiheesta löytämämme kirja Security Information and Event Management (SIEM) Implementation. Siinä oli esitelty yrityksen tietoturvatiedon hallinnan ja SIEMin perusteet. Kirjan SIEM-ohjelmistojen esittely- ja käyttöönotto-osiota emme käyttäneet lähteenä, koska sen tieto oli osittain vanhentunutta.

Opinnäytetyö aloitettiin tammikuussa 2015 ja suunnitelman mukaan sen tuli olla valmis huhtikuussa. Loppuvaiheessa kävimme toimeksiantajan kanssa keskustelemassa työstä ja heidän mukaansa se saavutti asetetut tavoitteet hyvin. Palaverin aikana löytyi hyviä parannusehdotuksia ja lisäyksiä, joita teimme opinnäytetyöhön. Työ palautettiin tarkistettavaksi maaliskuussa.

Pääsimme omasta mielestämme toimeksiannossa annettuihin tavoitteisiin ja opimme työn aikana paljon tietoturvasta ja lokitiedon hallinnasta. Aihe on laaja ja välillä olennaisen tiedon valitseminen asiakokonaisuuteen oli haastavaa. Jälkeenpäin ajatellen OSSIM-järjestelmään olisi voinut lisätä useampia seurattavia kohteita ja tehdä testejä niiden välisistä ristiinkorrelloinneista.

Toimeksiantajan toiveesta työn pääpainona oli teorian sekä eri ratkaisujen esittely, joten demojärjestelmällä esitellään ainoastaan SIEMin perustoiminnallisuudet. Ympäristön käyttöönotto ja konfigurointi toi käytännön näkökulmaa aiheeseen. Koska opinnäytetyö käsittelee aihetta eri näkökulmista, voi sitä käyttää tietopakettina SIEMiin perehtymisessä ja mahdollisen käyttöönottoprojektin aikana.

## Lähteet

1. Mitchell, B. How It Works. Ossec. 2015. [Viitattu 29.1.2015]. Saatavissa: [http://www.ossec.net/?page\\_id=169](http://www.ossec.net/?page_id=169).
2. Karthik. Advanced Persistent Threats – Attack and Defense. InfoSec Institute. 2013. [Viitattu 25.2.2015]. Saatavilla: <http://resources.infosecinstitute.com/advanced-persistent-threats-attack-and-defense/>.
3. Janssen, C. Brute Force Attack. Technopedia. 2015. [Viitattu 27.1.2015]. Saatavissa: <http://www.techopedia.com/definition/18091/brute-force-attack>.
4. Volker Gropp. bwm-ng (Bandwidth Monitor NG). Volker Gropp. 2013. [Viitattu 10.2.2015]. Saatavilla: <http://www.gropp.org/?id=projects&sub=bwm-ng>.
5. McDowell, M. Security TIP (ST04-015) Understanding Denial-of-Service Attacks. 2009. Päivitetty 6.2.2013. [Viitattu 23.1.2015]. Saatavissa: <https://www.us-cert.gov/ncas/tips/ST04-015>.
6. Rouse, M. File Transfer Protocol (FTP). TechTarget. 2007. [Viitattu 29.1.2015]. Saatavissa: <http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol>.
7. Berge, M. & Ernst, Y. Intrusion Detection FAQ: What is Intrusion Detection?. SANS. 2015. [Viitattu 23.1.2015]. Saatavissa: [http://www.sans.org/security-resources/idfaq/what\\_is\\_id.php](http://www.sans.org/security-resources/idfaq/what_is_id.php).
8. Entrepreneur. Human Resources. Entrepreneur. 2014 [Viitattu 25.2.2015]. Saatavissa: <http://www.entrepreneur.com/encyclopedia/human-resources>.
9. Heddings, L. Using htop to Monitor System Processes on Linux. How-To Geek. 2007. [Viitattu 10.2.2015]. Saatavilla: <http://www.howto-geek.com/howto/ubuntu/using-htop-to-monitor-system-processes-on-linux/>.
10. Mitchell, B. IP - Internet Protocol. About.com. 2015. [Viitattu 29.1.2015]. Saatavissa: [http://compnetworking.about.com/od/networkprotocolsip/g/ip\\_protocol.htm](http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm).
11. Scarfone, K. & Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). 2007. [Viitattu 29.1.2015]. Saatavissa: <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>.
12. ISO. ISO/IEC 27001 - Information security management. ISO. 2015 [Viitattu 11.2.2015]. Saatavissa: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.
13. LogRhythm. Log Rhythm's Security Intelligence Platform. LogRhythm. 2015. [Viitattu 9.2.2015]. Saatavissa: [https://www.logrhythm.com/Portals/0/resources/LR\\_Security\\_Intelligence\\_Platform.pdf](https://www.logrhythm.com/Portals/0/resources/LR_Security_Intelligence_Platform.pdf).
14. Rouse, M. NetFlow. TechTarget. 2014. [Viitattu 29.1.2015]. Saatavissa: <http://whatis.techtarget.com/definition/NetFlow-Cisco>.
15. Rouse, M. What is netstat?. TechTarget. 2007. [Viitattu 10.2.2015]. Saatavilla: <http://searchnetworking.techtarget.com/definition/netstat>.
16. Deri, L. NTOP. Ntop.org. 2005. [Viitattu 23.1.2015]. Saatavissa: <http://www.ntop.org/wp-content/uploads/2011/09/ntop-man.html>.
17. Rouse, M. OSI reference model (Open Systems Interconnection). TechTarget. 2014. [Viitattu 25.2.2015]. Saatavilla: <http://searchnetworking.techtarget.com/definition/OSI>.
18. Rouse, M. PCI DSS (Payment Card Industry Data Security Standard). TechTarget. 2015. [Viitattu 11.2.2015]. Saatavissa: <http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>.

19. Webopedia Staff. RAID - redundant array of independent disks. Webopedia. 2015. [Viitattu 25.2.2015]. Saatavilla: <http://www.webopedia.com/TERM/R/RAID.html>.
20. Taloussanomat. Taloussanakirja: sijoitetun pääoman tuotto prosentti. Taloussanomat. 2015. [Viitattu 23.1.2015]. Saatavissa: <http://www.taloussanomat.fi/porssi/sanakirja/termi/sijoitetun%20p%E4%E4oman%20tuotto prosentti/>.
21. RSYSLOG. Home. RSYSLOG. 2013. [Viitattu 23.1.2015]. Saatavissa: <http://www.rsyslog.com/>.
22. FreeBSD. File and Print Services for Microsoft® Windows® Clients (Samba). FreeBSD. 2014. [Viitattu 25.2.2015]. Saatavilla: <https://www.freebsd.org/doc/en/books/handbook/network-samba.html>.
23. SUSE. FAQ. SUSE. 2015. [Viitattu 25.2.2015]. Saatavilla: <https://www.suse.com/products/server/frequently-asked-questions/#q1.html>.
24. Microsoft, Microsoft SMB Protocol and CIFS Protocol Overview. Microsoft. 2015. [Viitattu 29.1.2015]. Saatavissa: <https://msdn.microsoft.com/en-us/library/windows/desktop/aa365233%28v=vs.85%29.aspx>.
25. Net-SNMP, SNMP. Net-SNMP. 2013. [Viitattu 27.1.2015]. Saatavissa: <http://www.net-snmp.org/>.
26. Leskiw, A. Understanding Syslog: Servers, Messages & Security. 2015. [Viitattu 29.1.2015]. Saatavissa: <http://www.networkmanagementsoftware.com/what-is-syslog>
27. Computer Hope, TCO, Computer Hope. 2015 [Viitattu 4.2.2015]. Saatavissa: <http://www.computerhope.com/jargon/t/tco.htm>.
28. Rouse, M. UDP (User Datagram Protocol). TechTarget. 2005. [Viitattu 29.1.2015]. Saatavissa: <http://whatis.techtarget.com/definition/NetFlow-Cisco>
29. Itä-Suomen yliopisto. Tutustu yliopistoon. Itä-Suomen yliopisto. 2014. [Viitattu 12.1.2015]. Saatavissa: <http://www.uef.fi/fi/tutustu>.
30. Kavanagh, K., Nicolett M. & Rochford, O. Magic Quadrant for Security Information and Event Management. Gartner, Inc. 2014. [Viitattu 13.1.2015]. Saatavissa: <http://www.gartner.com/technology/reprints.do?id=1-1VW8N7D&ct=140625&st=sb>.
31. Miller, D., Harris, S., Harper, A., Vandyke, S. & Blask, C. 2011 Security Information and Event Management (SIEM) Implementation. New York City: The McGraw-Hill Companies
32. Verizon. 2012 Data breach investigations. Verizon. 2012. [Viitattu 26.2.2015]. Saatavissa: [http://www.wired.com/images\\_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf](http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf).
33. ENISA. ENISA Threat Landscape 2014. ENISA. 2014. [Viitattu 25.2.2015]. Saatavissa: [https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at\\_download/fullReport](https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport).
34. Chuvakin, A. SIEM: Is It What Is SIEMs?. Security Warrior Consulting. 2008. [Viitattu 14.1.2015]. Saatavissa: [http://www.slideshare.net/anton\\_chuvakin/siem-is-it-what-is-siems-security-information-and-event-management-summit-at-csi-35th-conference-presentation](http://www.slideshare.net/anton_chuvakin/siem-is-it-what-is-siems-security-information-and-event-management-summit-at-csi-35th-conference-presentation).
35. Dorigo, S. Security Information and Event Management. Master Thesis. Radboud University Nijmegen. Nijmegen. 2012.
36. Dr.Dobb's. SIEM: A Market Snapshot. Dr.Dobb's. 2007. [Viitattu 14.1.2015]. Saatavissa: <http://www.drdoobs.com/siem-a-market-snapshot/197002909>.
37. Rohan. Security Information and Event Management (SIEM) Market worth \$ 4.54 Billion by 2019. Markets and Markets. 2015. [Viitattu 15.1.2015.] Saatavissa:

- <http://www.marketsandmarkets.com/PressReleases/security-information-event-management.asp>.
38. Hewlett-Packard. Demonstrating the ROI for SIEM. Hewlett-Packard. 2011. [Viitattu 14.1.2015]. Saatavissa: <http://h71028.www7.hp.com/enterprise/downloads/software/Demonstrating%20the%20ROI%20for%20SIEM.pdf>.
  39. Kuivalainen, J. Kehittyvän tietoturvan hinta. Digitoday. 2002. [Viitattu 14.1.2015]. Saatavissa: <http://www.digitoday.fi/tietoturva/2002/11/06/kehittyvauml-n-tietoturvan-hinta/20025462/66>.
  40. Sarjakivi, P. & Liimatainen J-P. Tekninen näkökulma: Lokienhallinta vai SIEM? Nixu Corporation. 2014. [Viitattu 3.2.2015]. Saatavissa: <http://www.sli-deshare.net/NixuOy/tekninen-nkkulma-lokienhallinta-vai-siem>.
  41. Espinoza, M. Frost & Sullivan: Greater Sophistication of Cyber Crimes Encourages Adoption of Security Information and Event Management. Market Wired. 2011. Päivitetty 14.3.2011. [Viitattu 15.1.2015]. Saatavissa: <http://www.marketwired.com/press-release/Frost-Sullivan-Greater-Sophistication-Cyber-Crimes-Encourages-Adoption-Security-Information-1410638.htm>.
  42. Blevins, B. Plan ahead to avoid SIEM deployment pitfalls. TechTarget. 2014. [Viitattu 4.2.2015]. Saatavissa: <http://searchsecurity.techtarget.com/news/2240227732/Plan-ahead-to-avoid-SIEM-deployment-pitfalls>.
  43. Holloway, J. How To Prepare For a Security Information and Event Management Deployment. Help net security. 2007. [Viitattu 4.2.2015]. Saatavissa: <http://www.net-security.org/article.php?id=1008&p=1>.
  44. Pivot Point Security. SIEM Whitepaper. Pivot Point Security. 2013. [Viitattu 19.1.2015]. Saatavissa: <http://www.pivotpointsecurity.com/siem-whitepaper>.
  45. Swift, D. A Practical Application of SIM/SEM/SIEM Automating Threat Identification. SANS Institute. 2006. [Viitattu 12.1.2015]. Saatavissa: <http://taylorandfrancis.metapress.com/openurl.asp?genre=article>.
  46. Barreiro, A. How to choose a SIEM solution: An overview. TechRepublic. 2011. [Viitattu 12.1.2015]. Saatavissa: <http://www.techrepublic.com/blog/it-security/how-to-choose-a-siem-solution-an-overview/>.
  47. Lane, A. Understanding and Selecting SIEM/LM: Data Collection. Securosis. 2010. [Viitattu 20.1.2015]. Saatavissa: <https://securosis.com/blog/understanding-and-selecting-siem-lm-data-collection>.
  48. Lane, A. Understanding and Selecting SIEM/LM: Aggregation, Normalization, and Enrichment. Securosis. 2010. [Viitattu 16.1.2015]. Saatavissa: <https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen>.
  49. Goncharov, A. Who Needs Event Normalization?. AlienVault. 2014. [Viitattu 16.1.2015]. Saatavissa: <http://www.metanetivs.com/event-normalization/>.
  50. Constantine, C. Plugins, SID's and Log Normalization. Securosis. 2013. Päivitetty 19.7.2014 [Viitattu 19.1.2015]. Saatavissa: <https://alienvault.bloomfire.com/posts/520572-plugins-sid-s-and-log-normalization/public>.
  51. Lane, A. Understanding and Selecting a SIEM/LM: Correlation and Alerting. Securosis. 2010. [Viitattu 16.1.2015]. Saatavissa: <https://www.securosis.com/blog/understanding-and-selecting-a-siem-lm-correlation-and-alerting>.
  52. Chuvakin, A. On SIEM Tool and Operation Metrics. Gartner. 2014 [Viitattu 19.1.2015]. Saatavissa: <http://blogs.gartner.com/anton-chuvakin/2014/06/17/on-siem-tool-and-operation-metrics/>.
  53. Lafferty, S. Cutting through SIEM vendor hype. SC Magazine. 2008 [Viitattu 20.1.2015] Saatavissa: <http://www.scmagazine.com/cutting-through-siem-vendor-hype/article/119440/>.

54. Netcerebral. Basic Log Storage Calculations. Buzz Circuit. 2012. [Viitattu 20.1.2015] Saatavissa: <http://www.buzzcircuit.com/208/>.
55. Butler, J. Benchmarking Security Information Event Management (SIEM). SANS Analyst program. 2009. [Viitattu 16.1.2015]. Saatavissa: <http://www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755>.
56. Lehman, J. Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market. Gartner. 2008. [Viitattu 26.2.2015]. Saatavissa: <https://www.gartner.com/doc/486094/magic-quadrants-marketscopes-gartner-evaluates>.
57. Worthen, B & Anupreeta, D. H-P Buys ArcSight for \$1.5 Billion. The Wall Street Journal. 2010. [Viitattu 15.1.2015]. Saatavissa: <http://www.wsj.com/articles/SB10001424052748703897204575488013169090950>
58. Hewlett-Packard, L.P. ARCSIGHT ESM TECHNICAL SPECIFICATIONS. Hewlett-Packard, L.P. 2015. [Viitattu 13.1.2015]. Saatavissa: <http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/tech-specs.html>.
59. Intel Corporation. Intel to Acquire McAfee. Intel Corporation. 2010. [Viitattu 16.1.2015]. Saatavissa: <http://www.sec.gov/Archives/edgar/data/50863/000119312510192748/dex991.htm>.
60. Ashford, W. What McAfee's acquisition of Stonesoft means for the companies and their customers. ComputerWeekly. 2013. [Viitattu 25.2.2015]. Saatavissa: <http://www.computerweekly.com/news/2240187944/What-McAfees-acquisition-of-Stonesoft-means-for-the-companies-and-their-customers>.
61. Stonesoft Corporation. Stonesoft™ SIEM Solution. 2013. [Viitattu 25.2.2015]. Saatavissa: <http://webcache.googleusercontent.com/search?q=cache:mWjodnSBCMsJ:213.28.200.138/opencms/export/system/galleries/download/datasheets/siem.pdf+&cd=6&hl=en&ct=clnk&gl=fi>.
62. McAfee, Inc., McAfee Enterprise Security Manager Services solutions for Managed Service Providers (MSPs). McAfee, Inc. 2014. [Viitattu 14.1.2015]. Saatavissa: [www.mcafee.com/hk/resources/solution-briefs/sb-enterprise-security-manager.pdf](http://www.mcafee.com/hk/resources/solution-briefs/sb-enterprise-security-manager.pdf).
63. McAfee, Inc. McAfee Enterprise Security Manager Discover. Respond. Comply. McAfee, Inc. 2014. [Viitattu 14.1.2015]. Saatavissa: <http://www.mcafee.com/ca/resources/data-sheets/ds-enterprise-security-manager.pdf>.
64. McAfee, Inc. McAfee Enterprise Security Manager. McAfee, Inc. 2015. [Viitattu 14.1.2015]. Saatavissa: <http://www.mcafee.com/ca/products/enterprise-security-manager.aspx#vt=vtab-SystemRequirements>.
65. Stephenson, P. McAfee Enterprise Security Manager product review. SC Magazine. 2013. [Viitattu 14.1.2015]. Saatavissa: <http://www.scmagazine.com/mcafee-enterprise-security-manager/review/3851/>.
66. Shackelford, D. Security Intelligence in Action: SANS Review of McAfee Enterprise Security Manager (ESM) 9.2. SC Magazine. 2013. [Viitattu 14.1.2015]. Saatavissa: <https://www.sans.org/reading-room/whitepapers/analyst/security-intelligence-action-review-mcafee-enterprise-security-manager-esm-92-35095>.
67. Trustwave, SIEM Portfolio overview. Trustwave. 2014. [Viitattu 15.1.2015]. Saatavissa: <https://www.trustwave.com/Resources/Library/Documents/Trustwave-SIEM/?dl=1>.
68. Trustwave, Log management enterprise. Trustwave. 2014. [Viitattu 15.1.2015]. Saatavissa: <https://www.trustwave.com/Resources/Library/Documents/Trustwave-Log-Management-Enterprise/?dl=1>.

69. Trustwave, SIEM Operations edition. Trustwave. 2014. [Viitattu 15.1.2015]. Saatavissa: <https://www.trustwave.com/Resources/Library/Documents/Trustwave-SIEM-Operations-Edition/?dl=1>.
70. Dignan, L. IBM acquires Q1 Labs, creates security division. ZDNet. 2011. [Viitattu 15.1.2015]. Saatavissa: <http://www.zdnet.com/article/ibm-acquires-q1-labs-creates-security-division/>.
71. InfoSec Nirvana. Punching Hard – QRadar Security Intelligence Platform. InfoSec Nirvana. 2013. [Viitattu 15.1.2015]. Saatavissa: <http://infosecnirvana.com/qradar-security-intelligence-platform/>.
72. IBM. IBM Security QRadar SIEM. IBM. 2015. [Viitattu 15.1.2015]. Saatavissa: <http://www-03.ibm.com/software/products/en/qradar-siem>.
73. Q1Labs. The Value of QRadar QFlow and QRadar VFlow for Security Intelligence. Q1Labs. 2011. [Viitattu 15.1.2015]. Saatavissa: <https://www.ndm.net/siem/pdf/q1labs/The-Value-of-QRadar-QFlow-and-QRadar-VFlow-for-Security-Intelligence.pdf>.
74. IBM. Prerequisites for installing RHEL on your own appliance. IBM. 2015. [Viitattu 15.1.2015]. Saatavissa: [https://www-304.ibm.com/support/knowledgecenter/SS42VS\\_7.2.1/com.ibm.qradar.doc\\_7.2.1/c\\_siem\\_rhat\\_inx\\_os.html](https://www-304.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_siem_rhat_inx_os.html).
75. Q1Labs. QRadar Security Intelligence Platform Appliances. Q1Labs. 2015. [Viitattu 15.1.2015]. Saatavissa: <http://www.securelink.nl/wp-content/uploads/2013/04/QRadar-Appliance-Family-Data-Sheet-.pdf>.
76. IBM. QRadar Security Intelligence Platform Appliances. IBM. 2015. [Viitattu 15.1.2015]. Saatavissa: [https://www-304.ibm.com/support/knowledgecenter/SS42VS\\_7.2.1/com.ibm.qradar.doc\\_7.2.1/c\\_siem\\_vrt\\_ap\\_reqs.html](https://www-304.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_siem_vrt_ap_reqs.html).
77. Stephenson, P. LogRhythm v6.2. SC Magazine. 2014. [Viitattu 6.2.2015]. Saatavissa: <http://www.scmagazine.com/logrhythm-v62/review/4149/>.
78. Shenk, J. NetIQ Sentinel 7 Review. SANS Institute. 2012. [Viitattu 6.2.2015]. Saatavilla: <https://www.sans.org/reading-room/whitepapers/analyst/netiq-sentinel-7-review-35165>.
79. NetIQ Corporation. Supported Operating Systems and Platforms. NetIQ Corporation. 2014. [Viitattu 6.2.2015]. Saatavilla: [https://www.netiq.com/documentation/sentinel72/s721\\_install/data/bwwvoij.html](https://www.netiq.com/documentation/sentinel72/s721_install/data/bwwvoij.html).
80. NetIQ Corporation. Advantages of Distributed Deployments. NetIQ Corporation. 2014. [Viitattu 6.2.2015]. Saatavilla: [https://www.netiq.com/documentation/sentinel72/s721\\_install/data/b19meos5.html](https://www.netiq.com/documentation/sentinel72/s721_install/data/b19meos5.html).
81. NetIQ Corporation. Advantages of Distributed Deployments. NetIQ Corporation. 2014. [Viitattu 6.2.2015]. Saatavilla: [https://www.netiq.com/documentation/sentinel72/s721\\_install/data/bwwvoik.html](https://www.netiq.com/documentation/sentinel72/s721_install/data/bwwvoik.html).
82. Splunk Inc. About Splunk Enterprise. Splunk Inc. 2015. [Viitattu 4.2.2015]. Saatavissa: <http://docs.splunk.com/Documentation/Splunk/latest/Overview/AboutSplunkEnterprise>.
83. Splunk Inc. Splunk Cloud. Splunk Inc. 2015. [Viitattu 4.2.2015]. Saatavissa: [https://www.splunk.com/en\\_us/products/splunk-cloud.html](https://www.splunk.com/en_us/products/splunk-cloud.html).
84. Splunk Inc. Using Splunk Software as a SIEM. Splunk Inc. 2013. [Viitattu 4.2.2015]. Saatavissa: [http://www.splunk.com/web\\_assets/pdfs/secure/Splunk\\_as\\_a\\_SIEM\\_Tech\\_Brief.pdf](http://www.splunk.com/web_assets/pdfs/secure/Splunk_as_a_SIEM_Tech_Brief.pdf).
85. Roberts, C. Discovering Security Events of Interest Using Splunk. SANS Institute. 2013. [Viitattu 3.2.2015]. Saatavissa: <https://www.sans.org/reading-room/whitepapers/logging/discovering-security-events-interest-splunk-34272>.



86. Splunk Inc. Types of forwarders. Splunk Inc. 2015. [Viitattu 3.2.2015]. Saatavissa: <http://docs.splunk.com/Documentation/Splunk/6.2.1/Forwarding/Typesofforwarders>.
87. Splunk Inc. About Splunk Free. Splunk Inc. 2015. [Viitattu 3.2.2015]. Saatavissa: <http://docs.splunk.com/Documentation/Splunk/6.2.1/Admin/MoreaboutSplunkFree>.
88. Splunk Inc. Distributed Splunk Enterprise overview. Splunk Inc. 2015. [Viitattu 4.2.2015]. Saatavissa: <http://docs.splunk.com/Documentation/Splunk/latest/Deploy/Distributedoverview>.
89. Splunk Inc. System requirements. Splunk Inc. 2015. [Viitattu 3.2.2015]. Saatavissa: <http://docs.splunk.com/Documentation/Splunk/6.2.1/Installation/Systemrequirements>.
90. Lkhamsuren, T. AlienVault OSSIM Review – Open Source SIEM. InfoSec Institute. 2012. [Viitattu 13.1.2015]. Saatavissa: <http://resources.infosecinstitute.com/alienvault-ossim-review-open-source-siem/>.
91. Barraco, L. AlienVault Getting Started Guide v4.14. AlienVault Repository of Knowledge. 2014. Päivitetty 28.12.2014. [Viitattu 13.1.2015]. Saatavissa: <https://alienvault.bloomfire.com/posts/891226-alienvault-getting-started-guide-v4-14/public>.
92. AlienVault. Compare AlienVault Products. AlienVault. 2015. [Viitattu 13.1.2015]. Saatavissa: <https://www.alienvault.com/products/compare-ossim-to-alienvault-usm>.
93. Terra Verde, AlienVault & Splunk: Which should I be purchasing? Terra Verde. 2015. [Viitattu 3.2.2015] Saatavissa: [http://info.terraverdeservices.com/alienvault-vs-splunk?portalId=319268&hsFormKey=29c63602904a7cd61af922536460ee0a&submissionGuid=8f3554e5-b79f-48b6-af20-0fe4522cc59c#module\\_1390846220226394](http://info.terraverdeservices.com/alienvault-vs-splunk?portalId=319268&hsFormKey=29c63602904a7cd61af922536460ee0a&submissionGuid=8f3554e5-b79f-48b6-af20-0fe4522cc59c#module_1390846220226394).
94. Misnomer. SIEM Product Comparison – 101. InfoSec Nirvana. 2014. [Viitattu 10.2.2015]. Saatavilla: <http://infosecnirvana.com/siem-product-comparison-101/>.
95. AlienVault, AlienVault + Splunk®: Bringing the power of threat detection & incident response to Big Data. AlienVault. 2015. [Viitattu 3.2.2015]. Saatavissa: <https://www.alienvault.com/solutions/alienvault-for-splunk>
96. Russ. Commandline Access. AlienVault, Inc. 2014. [Viitattu 10.2.2015]. Saatavilla: <https://www.alienvault.com/forums/discussion/1087/commandline-access>.
97. Constantine, C. OSSEC Client Installation for Linux Clients. AlienVault. 2013. [Viitattu 29.1.2015]. Saatavissa: [https://bloomfire-production.s3.amazonaws.com/crocodoc\\_documents/328538/original/OSSEC\\_Client\\_Deployment\\_on\\_Linux.pdf?AWSAccessKeyId=AKIAIKMPP7FRDWCQ22UA&Expires=2147385600&Signature=%2BTXeyQdD5syp1KLpzLyHDeIBzxA%3D&response-content-disposition=attachment](https://bloomfire-production.s3.amazonaws.com/crocodoc_documents/328538/original/OSSEC_Client_Deployment_on_Linux.pdf?AWSAccessKeyId=AKIAIKMPP7FRDWCQ22UA&Expires=2147385600&Signature=%2BTXeyQdD5syp1KLpzLyHDeIBzxA%3D&response-content-disposition=attachment).
98. Blasco, J. New AlienVault OSSIM v4.0 is out: New correlation capabilities. AlienVault. 2012. [Viitattu 11.2.2015]. Saatavissa: <https://www.alienvault.com/open-threat-exchange/blog/new-alienvault-ossim-v40-is-out-new-correlation-capabilities>.
99. AlienVault. The AlienVault Logger. AlienVault. 2015. [Viitattu 26.2.2015]. Saatavilla: <https://www.alienvault.com/docs/data-sheets/AlienVault-Logger.pdf>.
100. Offensive Security. What is Kali Linux. Offensive Security. 2013. [Viitattu 27.1.2015]. Saatavissa: <http://docs.kali.org/introduction/what-is-kali-linux>.
101. Hauser, V. HYDRA README. THC. 2014. [Viitattu 27.1.2015]. Saatavissa: <https://www.thc.org/thc-hydra/README>.

102. Echeverry, D. Ubuntu Manpage: hydra - A very fast network logon cracker which support many different. Canonical Ltd. 2011. [Viitattu 27.1.2015]. Saatavissa: <http://manpages.ubuntu.com/manpages/oneiric/man1/hydra.1.html>.
103. DarkMORE Ops. Denial-of-service Attack – DOS using hping3 with spoofed IP in Kali Linux. DarkMORE Ops. 2014. [Viitattu 4.3.2015]. Saatavilla: <http://www.darkmoreops.com/2014/08/21/dos-using-hping3-spoofed-ip-kali-linux/>.
104. Incapsula, Inc. SYN Flood. Incapsula, Inc. 2015. [Viitattu 4.3.2015]. Saatavilla: <http://www.incapsula.com/ddos/attack-glossary/syn-flood>
105. McAfee, SIEM Solutions from McAfee. McAfee. 2014. [Viitattu 28.1.2015]. Saatavissa: <http://www.mcafee.com/ca/resources/data-sheets/ds-siem-solutions-from-mcafee.pdf>.
106. IBM, System requirements for virtual appliances. IBM. 2015. [Viitattu 28.1.2015]. Saatavissa: [https://www-304.ibm.com/support/knowledgecenter/SS42VS\\_7.2.1/com.ibm.qradar.doc\\_7.2.1/c\\_siem\\_vrt\\_ap\\_reqs.html](https://www-304.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_siem_vrt_ap_reqs.html).
107. Stephenson, P. Trustwave SIEM. SC Magazine. 2011. Päivitetty 2.4.2011. [Viitattu 15.1.2015]. Saatavissa: <http://www.scmagazine.com/trustwave-siem/review/3483/>.

## 15 yleisintä tietoturvauuhkaa


**ENISA Threat Landscape 2014**  
*Overview of current and emerging cyber-threats*

December 2014

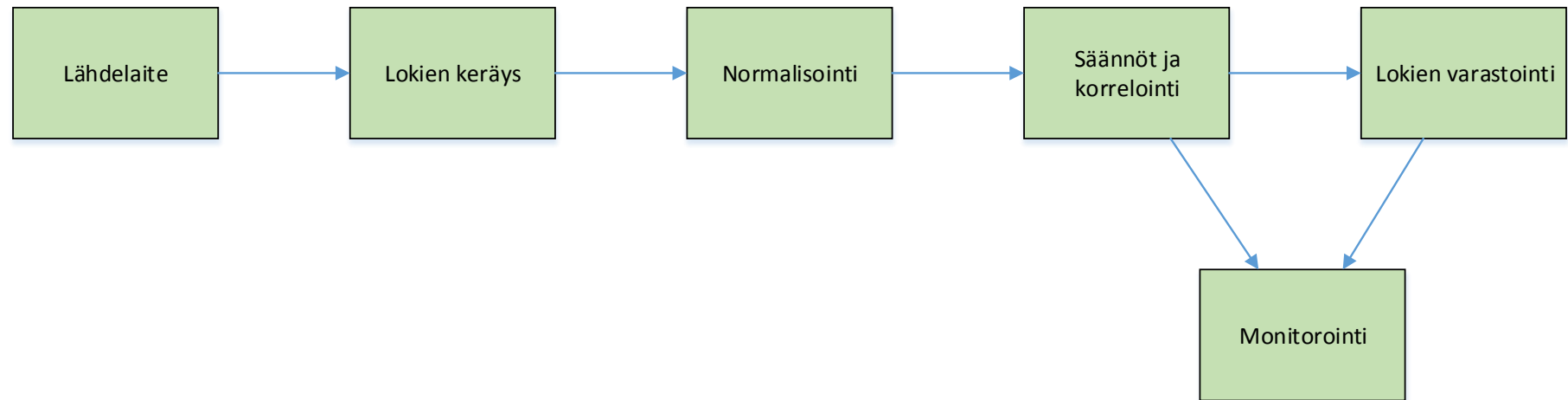
| Top Threats                                   | Current Trends | Top 10 Threat Trends in Emerging Areas |                  |                 |                 |          |                    |                      |
|---|----------------|--|------------------|-----------------|-----------------|----------|--------------------|----------------------|
|   |                | Cyber-Physical Systems and CIP         | Mobile Computing | Cloud Computing | Trust Infrastr. | Big Data | Internet of Things | Netw. Virtualisation |
| 1. Malicious code: Worms/Trojans              | ↑              | ↑                                      | ↑                | ↑               | ↑               |          | ↑                  | ↑                    |
| 2. Web-based attacks                          | ↑              | ↑                                      | ↑                | ↑               | ↔               |          | ↑                  |                      |
| 3. Web application attacks /Injection attacks | ↑              | ↑                                      | ↑                | ↑               | ↑               |          | ↑                  | ↑                    |
| 4. Botnets                                    | ↓              |  | ↑                | ↑               |                 |          |                    |                      |
| 5. Denial of service                          | ↑              | ↑                                      |                  | ↔               | ↔               |          | ↑                  | ↑                    |
| 6. Spam                                       | ↓              | ↑                                      |                  |                 |                 |          |                    |                      |
| 7. Phishing                                   | ↑              |  | ↑                |                 | ↑               | ↑        | ↑                  | ↑                    |
| 8. Exploit kits                               | ↓              |  | ↑                |                 | ↑               |          | ↑                  |                      |
| 9. Data breaches                              | ↑              |  |                  | ↑               |                 | ↑        |                    | ↑                    |
| 10. Physical damage/theft /loss               | ↑              | ↑                                      | ↑                |                 | ↑               | ↑        | ↑                  | ↑                    |
| 11. Insider threat                            | ↔              | ↑                                      |                  | ↑               |                 | ↑        | ↑                  | ↑                    |
| 12. Information leakage                       | ↑              | ↑                                      | ↑                | ↑               | ↑               | ↑        | ↑                  | ↑                    |
| 13. Identity theft/fraud                      | ↑              | ↑                                      | ↑                | ↑               | ↑               | ↑        | ↑                  | ↑                    |
| 14. Cyber espionage                           | ↑              | ↑                                      |                  | ↑               | ↑               | ↑        |                    | ↑                    |
| 15. Ransomware/Rogueware/Scareware            | ↓              |  | ↑                |                 |                 |          |                    |                      |

Legend: Trends: ↓ Declining, ↔ Stable, ↑ Increasing

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014<sup>1</sup>

<sup>1</sup> Please note that the ranking of threats in the emerging landscape is different than the one in the current landscape. The rankings of emerging threat trends can be found in the corresponding section (see chapter 6). Arrows that show a stability

### Tietoturvatiedonkulku SIEM-järjestelmässä



## Laitteiden EPS-keskiarvoja

**Table 1: Baseline Network Device EPS Averages**

| Qty            | Type   | Description  | Avg EPS                    | Total Peak EPS             | Average Peak EPS           |
|----------------|--|--|----------------------------|----------------------------|----------------------------|
| 750            | Employees/Endpoints (Windows XP)                       | Desktops & laptops at 5 locations  | Included at domain servers | Included at domain servers | Included at domain servers |
| 7              | Cisco Catalyst Switches                                | One at each location, one in DMZ and one in the Trusted network  | 5.09                       | 51.88                      | 26.35                      |
| 7              | Cisco Gateway/Routers                                  | One at each location   | 0.60                       | 380.50                     | 154.20                     |
| 5              | Windows 2003 Domain Servers                            | One at each location   | 40.00                      | 404.38                     | 121.75                     |
| 3              | Windows 2003 Application Servers                       | In high availability cluster at data center  | 1.38                       | 460.14                     | 230.07                     |
| 3              | MS SQL Database Servers running on Windows 2003 Server | High availability cluster at data center   | 1.83                       | 654.90                     | 327.45                     |
| 6              | Microsoft Exchange Servers                             | One at each location with two (cluster) at the data center   | 3.24                       | 1,121.50                   | 448.60                     |
| 3              | MS IIS Web Servers on Windows 2003                     | High availability cluster at data center   | 1.17                       | 2,235.10                   | 1,117.55                   |
| 2              | Windows DNS Servers                                    | At data center – failover  | 0.72                       | 110.80                     | 110.80                     |
| 2              | Linux Legacy Application Servers                       | At data center   | 0.12                       | 43.60                      | 21.80                      |
| 1              | Linux MySQL Database Server                            | One in Trusted network for legacy application  | 0.12                       | 21.80                      | 21.80                      |
| 7              | NitroGuard IPS   | One at each location, one in DMZ and one in the Trusted network  | 40.53                      | 5,627.82                   | 1,607.95                   |
| 1              | Netscreen Firewall                                     | Netscreen facing the Internet  | 0.58                       | 2,414.00                   | 2,414.00                   |
| 3              | Cisco Pix Firewalls                                    | Between the data center and the other four sites, in front of Trusted network, between Trusted and the DMZ | 39.00                      | 1,734.00                   | 1,178.00                   |
| 1              | Cisco VPN Concentrator                                 | Located at data center Facing the Internet   | 0.83                       | 69.45                      | 69.45                      |
| 1              | Squid Proxy  | Located at data center   | 14.58                      | 269.03                     | 269.03                     |
| <b>Totals:</b> |  |  | <b>149.79</b>              | <b>15,598.90</b>           | <b>8,118.80</b>            |

[55]

## HP ArcSight -lisenssivaihtoehdot

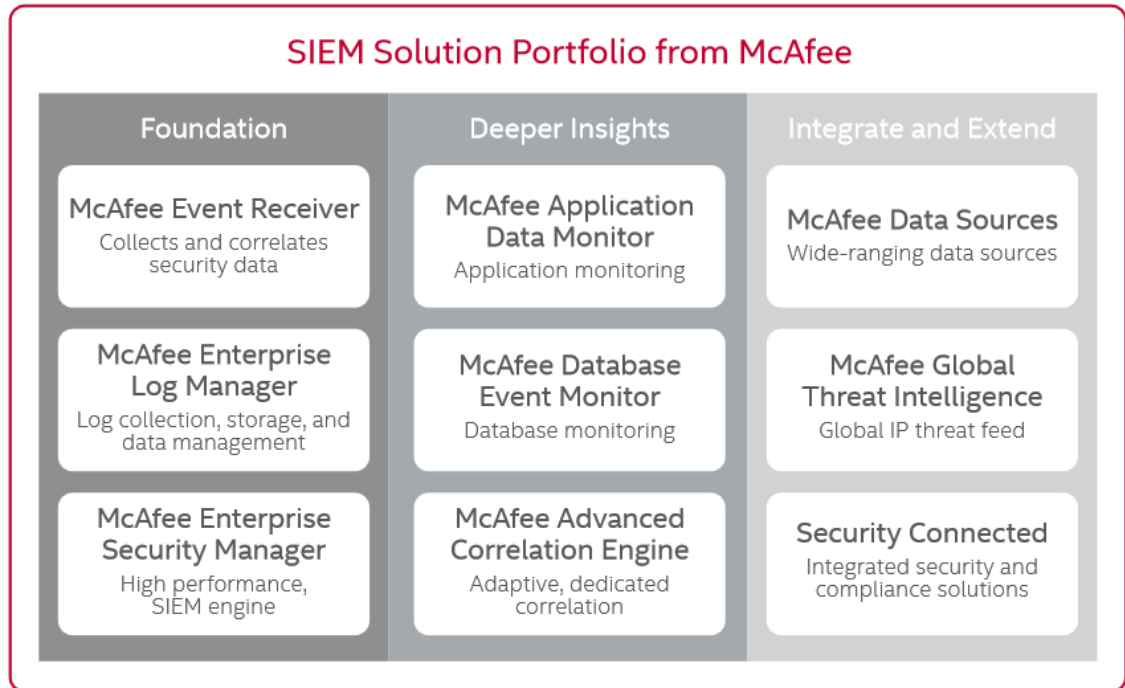
## ArcSight ESM Suite with CORR-Engine Software Specifications

| Software Model                                | ESM 20 GB/d | ESM 50 GB/d | ESM 100 GB/d | ESM 150 GB/d | ESM 250 GB/d     |
|---|-------------|-------------|--------------|--------------|------------------|
| <b>Total Gigabytes Per Day (GB/Day)</b>       | 20          | 50          | 100          | 150          | 250 <sup>1</sup> |
| <b>Average Events Per Second<sup>2</sup></b>  | 1,000       | 2,500       | 5,000        | 7,500        | 12,500           |
| <b>Network Devices</b>                        | 100         | 250         | 500          | 500          | 500              |
| <b>Named Web interface users</b>              | 10          | 25          | 25           | 25           | 25               |
| <b>Named Console users</b>                    | 2           | 3           | 3            | 3            | 3                |
| <b>Vulnerability assets</b>                   | 10,000      | 10,000      | 10,000       | 10,000       | 10,000           |
| <b>IdentityView actors</b>                    | 50          | 50          | 50           | 50           | 50               |
| <b>Connector Management licenses included</b> | 4           | 4           | 4            | 4            | 4                |

1 - ESM can be expanded beyond 250 GB/d via licensing upgrades. GB/d is only limited by hardware capability.

2 - Event per second (EPS) value is to be used as a guideline only. ESM is not licensed based on EPS.

**SIEM Solution Portfolio from McAfee**



[105, 2]

## McAfee ESM -tuotteiden tekniset tiedot

Scalable deployment options — Hybrid delivery choices include physical and virtual appliances. For McAfee Enterprise Security Manager integration information, see the [ESM Integration](#) data sheet.

|   |   |   |  |   |  |  |  |
|---|---|---|--|---|--|--|--|
| <b>McAfee Enterprise Security Manager</b><br>Hardware Appliance Specifications* | McAfee Enterprise Security Manager X6         | McAfee Enterprise Security Manager X4         | McAfee Enterprise Security Manager 6000      | McAfee Enterprise Security Manager 5600   | McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 4600 Combination       | McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 5600 Combination | McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 6000 Combination |
| Collection Rates  | 360,000 events per second <sup>1</sup>        | 180,000 events per second <sup>1</sup>        | 84,000 events per second <sup>1</sup>        | 60,000 events per second <sup>1</sup>   | 1,200 events per second <sup>1</sup>   | 3,000 events per second <sup>1</sup>   | 6,000 events per second <sup>1</sup>   |
| Local Storage   | 14 TB <sup>2</sup> + 3.2 TB SSD <sup>3</sup>  | 14 TB <sup>2</sup> + 800 GB SSD <sup>3</sup>  | 14 TB <sup>2</sup> + 480 GB SSD <sup>3</sup> | 8 TB <sup>2</sup> + 480 GB SSD <sup>3</sup>   | 3 TB <sup>2</sup> + 480 GB SSD <sup>3</sup>  | 8 TB <sup>2</sup> + 480 GB SSD <sup>3</sup>  | 14 TB <sup>2</sup> + 480 GB SSD <sup>3</sup>   |
| <b>McAfee Enterprise Security Manager</b><br>Virtual Appliance Specifications*  | McAfee Enterprise Security Manager 32 Core VM | McAfee Enterprise Security Manager 12 Core VM | McAfee Enterprise Security Manager 8 Core VM | McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 8 Core VM Combination | McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 12 Core VM Combination |  |  |
| Collection Rates  | 85,000 events per second <sup>1</sup>         | 40,000 events per second <sup>1</sup>         | 1,500 events per second <sup>1</sup>         | 1,000 events per second <sup>1</sup>  | 5,000 events per second <sup>1</sup>   |  |  |
| Recommended Storage   | 2 TB <sup>2</sup> + 800 GB SSD <sup>3</sup>   | 500 GB <sup>2</sup> + 480 GB SSD <sup>3</sup> | 250 GB <sup>2</sup>                          | 250 GB <sup>2</sup>   | 500 GB <sup>2</sup> + 480 GB SSD <sup>3</sup>  |  |  |

1. Based on typical network environments using average event and flow aggregation.

2. Represents usable event and flow storage, after RAID configuration.

3. Minimum 50K IOPS for SSD; additional storage should be a minimum of 100 IOPS.

\*The product specifications and descriptions herein are provided for information only, are subject to change without notice, and are provided without warranty of any kind, expressed or implied.



**QRadar virtual appliances -laitteistovaatimukset**

| <b>Appliance</b>                         | <b>Minimum memory requirement</b> | <b>Suggested memory requirement</b> |
|--|-----------------------------------|-------------------------------------|
| QRadar VFlow Collector 1290              | 6 GB                              | 6 GB                                |
| QRadar Event Collector Virtual 1590      | 12 GB                             | 16 GB                               |
| QRadar SIEM Event Processor Virtual 1690 | 12 GB                             | 48 GB                               |
| QRadar SIEM Flow Processor Virtual 1790  | 12 GB                             | 48 GB                               |
| QRadar SIEM All-in-One Virtual 3190      | 24 GB                             | 48 GB                               |
| QRadar Log Manager Virtual 1790          | 24 GB                             | 48 GB                               |

[106]

LogRhythmin käyttöönottovaihtoehdot

**Flexible Deployment Options**  
**High Performance Appliances**



|                             | ALL-IN-ONE (XM)<br>(Includes EM, LM, AIE) |            | DEDICATED<br>EVENT MANAGER (EM)<br>(Includes AI Engine license) |                   |                   | DEDICATED<br>LOG MANAGER (LM) |            |            | DEDICATED<br>AI ENGINE (AIE) |            |            | SITE LOG<br>FORWARDER<br>(SLF) | NETWORK<br>MONITOR<br>(NM) |
|-----------------------------|---|------------|---|-------------------|-------------------|-------------------------------|------------|------------|------------------------------|------------|------------|--------------------------------|----------------------------|
| <b>Appliance Lines</b>      | 4300                                      | 6300       | 3300 <sup>3</sup>   | 5300 <sup>4</sup> | 7300 <sup>5</sup> | 3300                          | 5300       | 7300       | 5300                         | 7300       | 9300       | 3310                           | 3300                       |
| <b>Max Archiving Rates</b>  | 10,000 MPS                                | 25,000 MPS | N/A   | N/A               | N/A               | 10,000 MPS                    | 25,000 MPS | 50,000 MPS | N/A                          | N/A        | N/A        | N/A                            | N/A                        |
| <b>Max Processing Rates</b> | 1,000 MPS                                 | 5,000 MPS  | N/A   | N/A               | N/A               | 2,000 MPS                     | 5,000 MPS  | 15,000 MPS | 5,000 MPS                    | 30,000 MPS | 75,000 MPS | N/A                            | 1 Gbps                     |

<sup>1</sup>MPS = Messages Per Second. <sup>2</sup>Individual rates vary based on customer environment/requirements. <sup>3</sup>Includes Embedded AIE License of 2,000 MPS. <sup>4</sup>Includes Embedded AIE License of 10,000 MPS. <sup>5</sup>Includes Embedded AIE License of 20,000 MPS

[13]

## NetIQ-ohjelmistovaatimukset

## Supported Operating Systems and Platforms

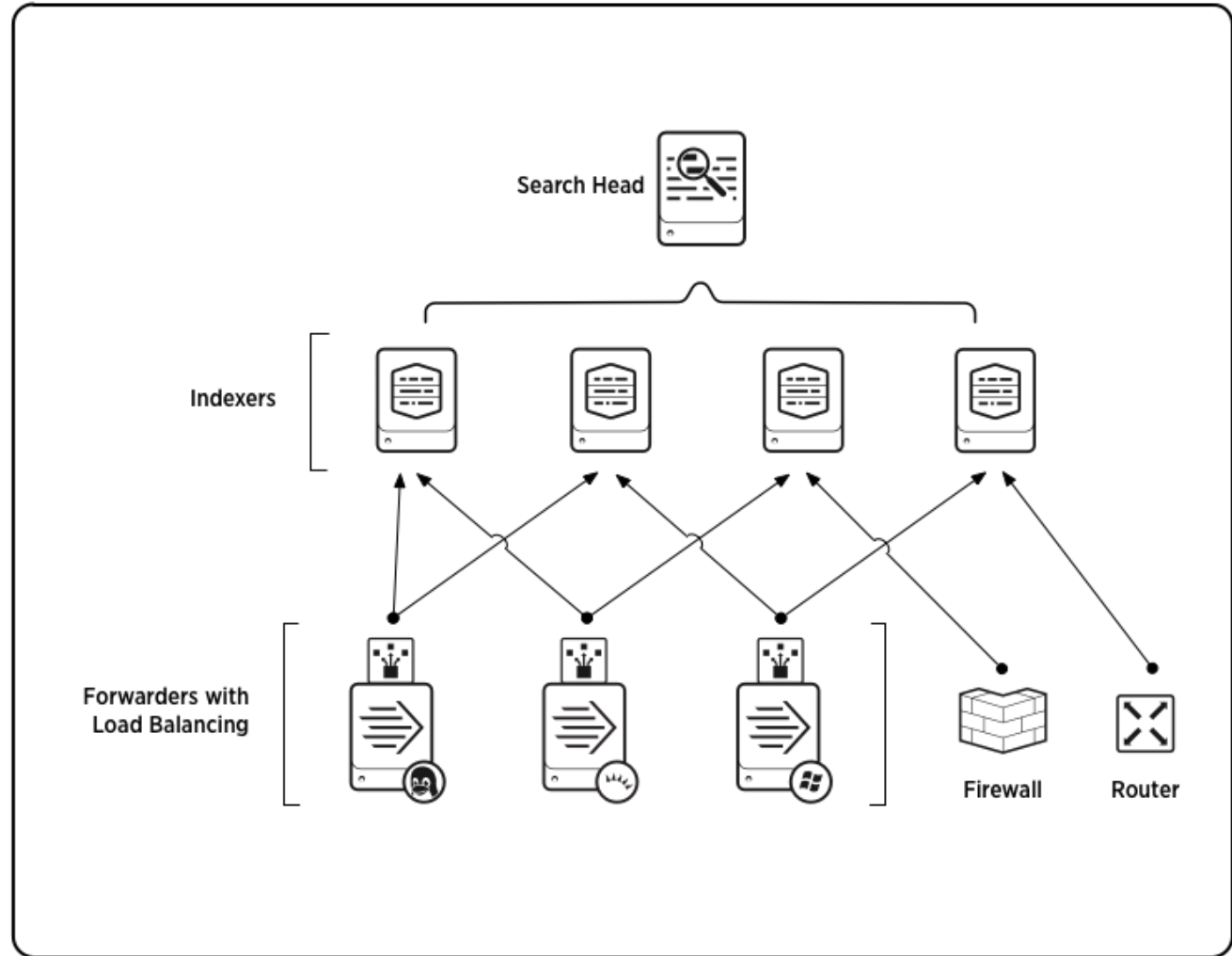
NetIQ Corporation supports the Sentinel server, Collector Manager, and Correlation Engine on the following operating systems and platforms:

| Category         | Requirement  |
|------------------|--|
| Operating System | <p>Sentinel is supported on the following operating systems:</p> <p><b>Non-FIPS mode:</b></p> <ul style="list-style-type: none"> <li>• SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit *</li> <li>• Red Hat Enterprise Linux Server (RHEL) 6.4 64-bit</li> </ul> <p><b>FIPS mode:</b></p> <ul style="list-style-type: none"> <li>• SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit</li> <li>• Red Hat Enterprise Linux Server (RHEL) 6.3 64-bit</li> </ul> <p>* Sentinel is not supported on the Open Enterprise Server installs of SLES.</p> <p>For information about new functionality and known issues in the supported SLES 11 Service Pack, see the <a href="#">SUSE Release Notes</a>.</p> |
| Virtual Platform | <p>NetIQ provides appliances that install a SLES 11 SP3 64-bit server and Sentinel on the following virtual platforms:</p> <ul style="list-style-type: none"> <li>• VMWare ESX 4.0 and 5.0</li> <li>• Xen 4.0</li> </ul>   |
| DVD ISO          | <p>NetIQ provides a DVD ISO file that installs SLES 11 SP3 64-bit and Sentinel on:</p> <ul style="list-style-type: none"> <li>• Hyper-V Server 2012</li> <li>• Hardware without an operating system installed</li> </ul> <p><b>IMPORTANT:</b> For the ISO appliance to work properly, you must disable the EFI BIOS and use the Legacy BIOS.</p>   |
| File System      | <p><b>Traditional Installations:</b></p> <ul style="list-style-type: none"> <li>• <b>On SLES systems:</b> Sentinel supports ext3 and XFS file systems.</li> <li>• <b>On RHEL systems:</b> Sentinel supports ext4 and XFS file systems.</li> </ul> <p><b>Appliance Installations:</b></p> <p>Sentinel uses the ext3 file system.</p> <p>For more information on file systems, see <a href="#">Overview of File Systems in Linux</a> in the <i>SLES 11 Storage Administration Guide</i>.</p>   |

**NetIQ-laitteistovaatimukset**

| Category                        | Description  | Demo All-in-One (not intended for production)                          | Medium Distributed Agent-less Data Collection  | Medium Distributed Agent-based Data Collection                    | Large Distributed Agent-less Data Collection (Raw Data Stored)                                    | Large Distributed Agent-less Data Collection (Raw Data Not Stored) | Extra Large            |
|---------------------------------|--|--|--|---|---|--|------------------------|
| Retained EPS Capability         | The events per second rate processed by real-time components and retained in storage by the system.  | 100 EPS  | 3000 EPS   | 2500 EPS  | 11000 EPS   | 13000 EPS  | 13000+ EPS             |
| Operational EPS Capability      | The total events per second rate received by the system from event sources. This includes data dropped by the system's intelligent filtering capability before being stored and is the number used for the purposes of EPS-based license compliance. | 100 EPS  | 3000+ EPS  | 2500+ EPS   | 11000+ EPS  | 13000+ EPS   | 13000+ EPS             |
| Network Flows per Minute        |  | 300 FPM  | 60000 FPM  | Not Applicable  | 60000 FPM   | 60000 FPM  | 60000+ FPM             |
| <b>Sentinel Server Hardware</b> |  |  |  |   |   |  |                        |
| CPU                             |  | Intel(R) Xeon(R) CPU E5420 @ 2.50GHz (4 CPU cores), no hyper-threading | Intel(R) Xeon(R) CPU X5355 @ 2.66GHz (4 core) CPUs (8 cores total), no hyper-threading | Two AMD Opteron 2431 @ 2.40 GHz (6 cores per CPU; 12 cores total) | Two Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz (8 core) CPUs (16 cores total), with hyper-threading |  | Contact NetIQ Services |
| Primary Storage                 | Locally cached data for higher search performance.   | 500 GB 7.2k RPM drive  | 5 x 300 GB SAS 15k RPM (Hardware RAID 0)   | 3 x 146 GB SAS 10K RPM (RAID 0, stripe size 128k)                 | 5 TB, 8 x 600 GB SAS 15k RPM (Hardware RAID 0, stripe size 128k)                                  |  |                        |
| Secondary Storage               | Includes a copy of the data in the primary storage.  | Not Used   | Not Used   | Not Used  | Not Used  |  |                        |
| Memory                          |  | 4 GB   | 24 GB  | 16 GB   | 128 GB  |  |                        |

# Klusteroitu Splunk-järjestelmä



## Splunk-järjestelmävaatimukset

### Windows operating systems

The table lists the Windows computing platforms that Splunk Enterprise is available for.

| Operating system  | Architecture | Enterprise | Free | Trial | Universal Forwarder |
|---|--------------|------------|------|-------|---------------------|
| Windows Server 2003 and Server 2003 R2                  | x86 (64-bit) |            |      |       | ✓                   |
|   | x86 (32-bit) |            |      |       | ✓                   |
| Windows Server 2008                                     | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
|   | x86 (32-bit) | ***        | ***  | ***   | ✓                   |
| Windows Server 2008 R2, Server 2012, and Server 2012 R2 | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
| Windows 7   | x86 (64-bit) |            | ✓    | ✓     | ✓                   |
|   | x86 (32-bit) |            | ***  | ***   | ✓                   |
| Windows 8   | x86 (64-bit) |            | ✓    | ✓     | ✓                   |
|   | x86 (32-bit) |            | ***  | ***   | ✓                   |
| Windows 8.1   | x86 (64-bit) |            | ✓    | ✓     | ✓                   |
|   | x86 (32-bit) |            | ***  | ***   | ✓                   |

\*\*\* This version of Splunk Enterprise is supported but is not recommended on this platform and architecture.

### Unix operating systems

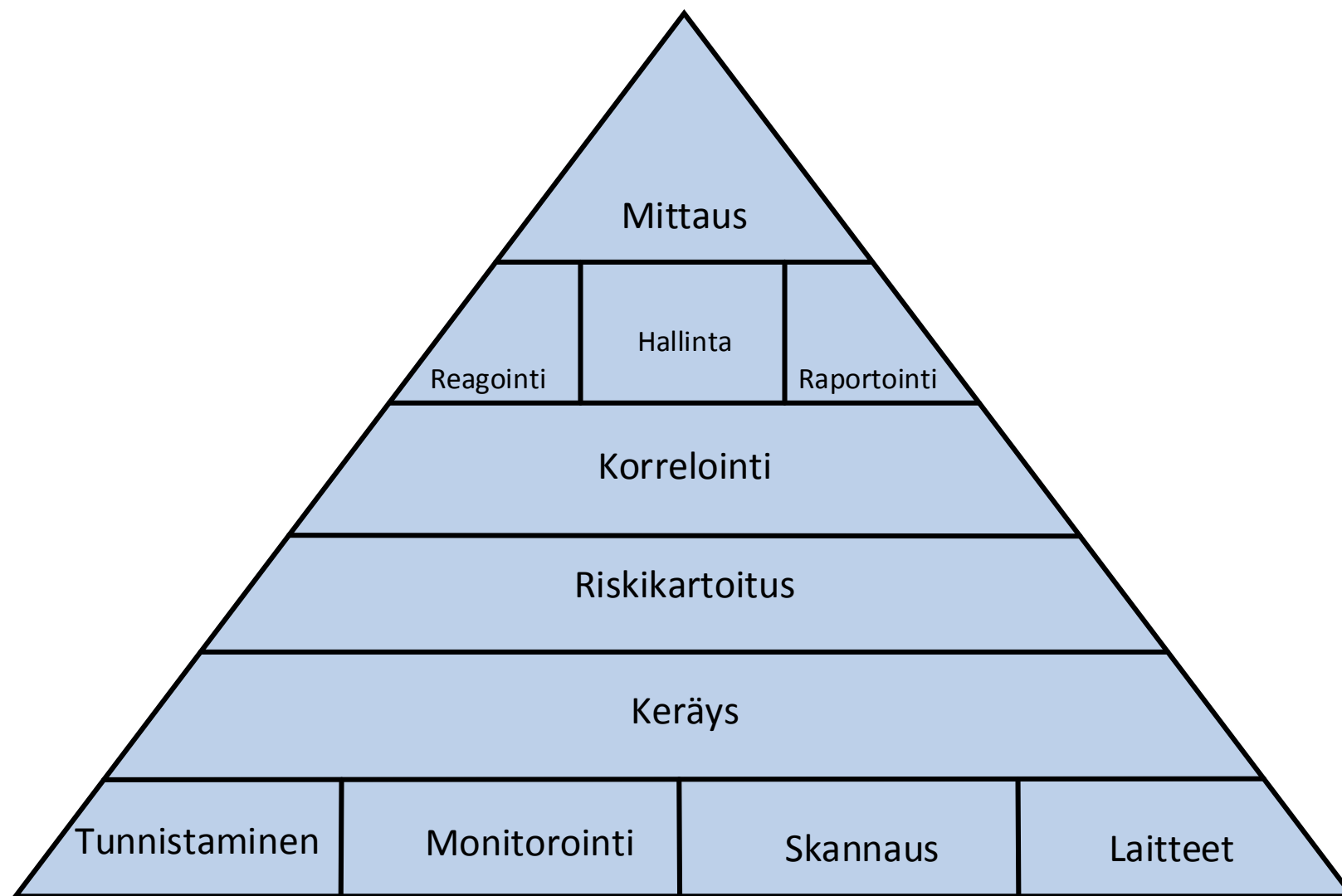
| Operating system         | Architecture | Enterprise | Free | Trial | Universal Forwarder |
|--------------------------|--------------|------------|------|-------|---------------------|
| Solaris 10 and 11*       | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
|                          | SPARC        | ✓          | ✓    | ✓     | ✓                   |
|                          | x86 (32-bit) | *          | *    | *     | *                   |
| Linux, 2.6+              | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
|                          | x86 (32-bit) | ✓          | ✓    | ✓     | ✓                   |
| Linux, 3.0+              | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
|                          | x86 (32-bit) | ✓          | ✓    | ✓     | ✓                   |
| PowerLinux, 2.6+         | PowerPC      |            |      |       | ✓                   |
| zLinux, 2.6+             | s390x        |            |      |       | ✓                   |
| FreeBSD 7**              | x86 (32-bit) |            |      |       | ✓                   |
| FreeBSD 8                | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
|                          | x86 (32-bit) |            |      |       | ✓                   |
| FreeBSD 9                | x86 (64-bit) | ✓          | ✓    | ✓     | ✓                   |
| Mac OS X 10.8 and 10.9   | Intel        | ✓          | ✓    | ✓     | ✓                   |
| AIX 6.1 and 7.1          | PowerPC      | ✓          | ✓    | ✓     | ✓                   |
| HP/UX† 11i v2 and 11i v3 | Itanium      |            |      |       | ✓                   |

\* Splunk Enterprise is available and supported on Solaris 10. Solaris 11 does not support 32-bit Splunk Enterprise installs.

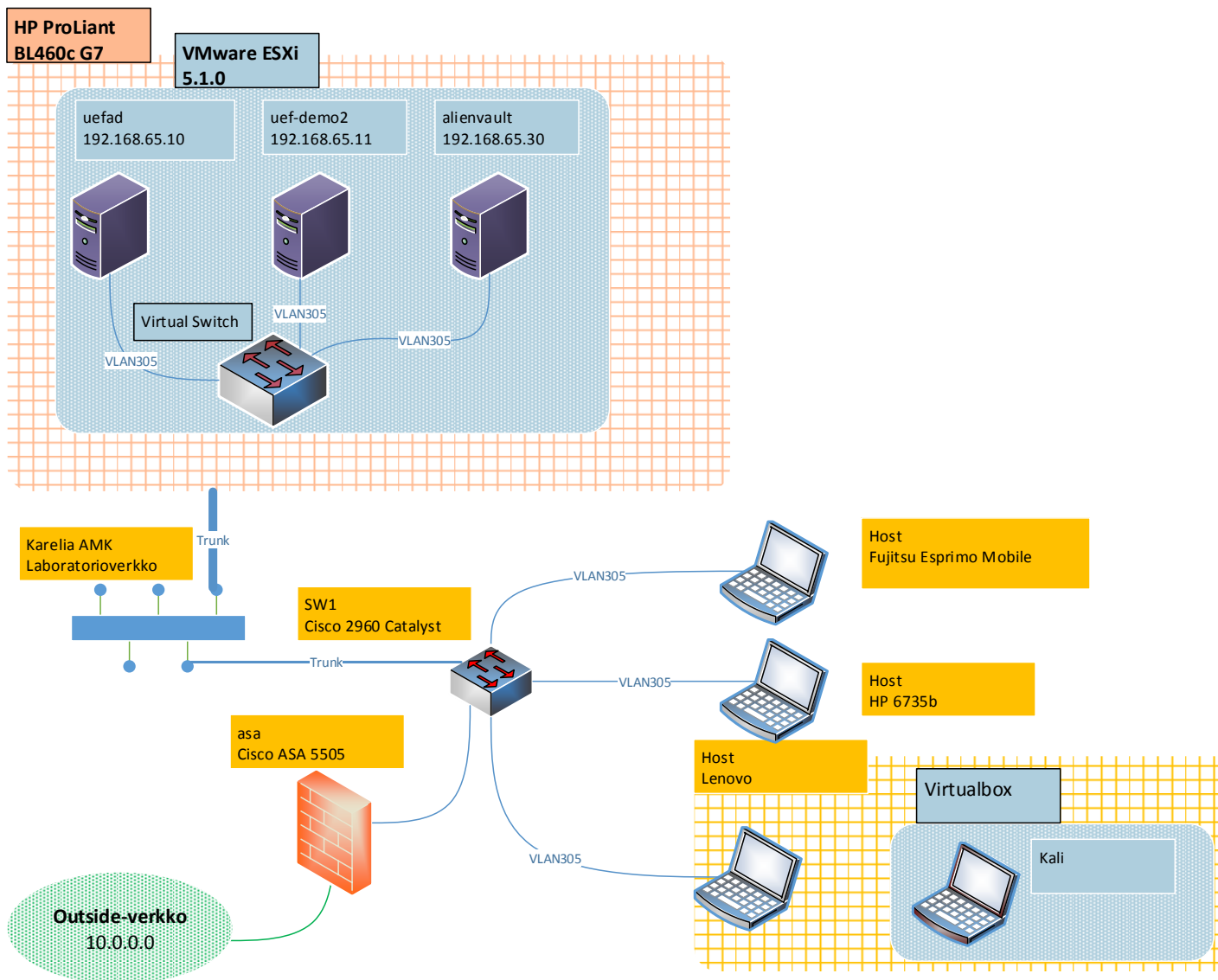
\*\* Read the notes on FreeBSD 7 compatibility below.

† You must use `gnu tar` to unpack the HP/UX installation archive.

## AlienVault OSSIMin toiminnallisuus



# Verkkokuva





**OSSEC-agentin asentaminen Ubuntu-palvelimeen**

```
OSSEC HIDS v2.8 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

- System: Linux uef-demo2 3.13.0-44-generic
- User: root
- Host: uef-demo2

-- Press ENTER to continue or Ctrl-C to abort. --

1- What kind of installation do you want (server, agent, local, hybrid or help)? agent
- Agent(client) installation chosen.

2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS [/var/ossec]:
- Installation will be made at /var/ossec .

3- Configuring the OSSEC HIDS.

3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.65.30
- Adding Server IP 192.168.65.30

3.2- Do you want to run the integrity check daemon? (y/n) [y]: y
- Running syscheck (integrity check daemon).

3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
- Running rootcheck (rootkit detection).

3.4 - Do you want to enable active response? (y/n) [y]: y
```

## Autentikointiavaimen lisääminen OSSEC-agenttiin Ubuntussa

```
*****
* OSSEC HIDS v2.8 Agent manager.      *
* The following options are available: *
*****
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): NCB1ZWYtZGVtbzIgMTkyLjE2OC42NS4wLzI0IDViMzg3NWFlMjBmZGU5ZTJmM2FjYTZmZmMxNTEyZTc0OUMzNTBjZjdmN2ViMjJlOGYxNjA0ZGVjM2U3ZWZlOTE=

Agent information:
  ID:4
  Name:uef-demo2
  IP Address:192.168.65.0/24

Confirm adding it?(y/n): y
```

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

Building configuration...

Current configuration : 3721 bytes

!

! Last configuration change at 13:30:38 UTC+2 Mon Jan 26 2015 by admin

!

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime localtime

service password-encryption

!

hostname SW1

!

boot-start-marker

boot-end-marker

!

enable secret 5 \$1\$DwhY\$cgEPHMKa1CPI5KKqy/8wf/

!

username admin password 7 12290404011C03162E7A65

no aaa new-model

clock timezone UTC+2 2

system mtu routing 1500

ip subnet-zero

!

!

ip domain-name siendemo.ad

ip name-server 192.168.65.10

login on-failure log

login on-success log

!

!

!

!

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

```
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
ip ssh version 2  
!  
!  
interface FastEthernet0/1  
  switchport access vlan 305  
  switchport mode access  
  spanning-tree portfast  
!  
interface FastEthernet0/2  
  switchport access vlan 305  
  switchport mode access  
  spanning-tree portfast  
!  
interface FastEthernet0/3  
  switchport access vlan 305  
  switchport mode access  
  spanning-tree portfast  
!  
interface FastEthernet0/4  
  switchport access vlan 305  
  switchport mode access  
  spanning-tree portfast  
!  
interface FastEthernet0/5  
  switchport access vlan 305
```

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

```
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/7
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/9
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/10
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/12
```

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

```
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/16
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/17
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/18
switchport access vlan 305
switchport mode access
spanning-tree portfast
!
```

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

```
interface FastEthernet0/19
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/20
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/21
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/22
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/23
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/24
  switchport access vlan 305
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
```

**Cisco 2960 Catalyst -kytkimen konfiguraatio**

```
switchport mode trunk
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan305
  ip address 192.168.65.2 255.255.255.0
  no ip route-cache
!
ip http server
ip http secure-server
logging trap notifications
logging 192.168.65.30
!
control-plane
!
!
line con 0
  logging synchronous
line vty 0 4
  login local
  transport input ssh
line vty 5 15
  login
!
ntp clock-period 36029374
ntp server 192.168.65.10
ntp server 194.100.49.139
end
```



## Toimintamalli SSH-bruteforce-hyökkäyksen havaitsemiseen

**AV-FREE-FEED Bruteforce attack, SSH service authentication attack against DST\_IP**  
 Delivery & Attack, Bruteforce Authentication, SSH

▼ RULES

| NAME   | RELIABILITY | TIMEOUT | OCCURRENCE | FROM     | TO       | DATA SOURCE | EVENT TYPE | [...]  |
|--|-------------|---------|------------|----------|----------|-------------|------------|--------|
| SSH service authentication attempt failed detected | 1           | None    | 1          | ANY      | ANY      | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication attempt failed detected | 2           | 30      | 5          | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication attempt failed detected | 4           | 60      | 10         | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication attempt failed detected | 6           | 3000    | 100        | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication attempt failed detected | 8           | 36000   | 1000       | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication attempt failed detected | 10          | 86400   | 10000      | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 1    | ▶ More |
| SSH service authentication successful              | 10          | 10      | 1          | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 7    | ▶ More |
| SSH service authentication successful              | 1           | 10      | 1          | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 7    | ▶ More |
| SSH service authentication successful              | 10          | 10      | 1          | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 7    | ▶ More |
| SSH service authentication successful              | 10          | 10      | 1          | 1:SRC_IP | 1:DST_IP | ssh (4003)  | SIDs: 7    | ▶ More |

▶ DIRECTIVE INFO

▼ KNOWLEDGE DB

**KDB**

| DATE       | TITLE   |
|------------|---|
| 2012-01-01 | AV-FREE Bruteforce attack, SSH service authentication attack against DST_IP |

SHOWING 1 TO 1 OF 1 ENTRIES

FIRST PREVIOUS 1 NEXT LAST

### Knowledge DB

#### Description:

Brute forcing consists of systematically enumerating all possible combinations of a given username/password list. An approach is to repeatedly try guesses from a common used password/username list.

#### Countermeasures:

- Disable unused services
- Create an access list to prevent unknown computers accessing this service and restrict remote access.
- Establishing strong password policies for your organization that includes maximum login attempts

OSSIM-tiketti

| TICKET DETAILS  |  |        |          |   |  |  |
|---|--|--------|----------|---|--|--|
| TICKET ID   | TICKET   | STATUS | PRIORITY | KNOWLEDGE DB  | ACTION                                   |  |
| ALA03   | <p><b>Name:</b> AV-FREE-FEED Bruteforce attack, login authentication attack against DST_IP</p> <p><b>Class:</b> Alarm</p> <p><b>Type:</b> Anomalies</p> <p><b>Created:</b> 2015-01-29 12:10:21 (00:01)</p> <p><b>Last Update:</b> 00:00</p> <p><b>Resolution time:</b> 00:01</p> <hr/> <p><b>In charge:</b> administrator</p> <p><b>Submitter:</b> administrator</p> <hr/> <p><b>Extra:</b> n/a</p> <hr/> <p><b>Source Ips:</b> 192.168.65.122</p> <p><b>Source Ports:</b> 0</p> <p><b>Dest Ips:</b> 192.168.65.30</p> <p><b>Dest Ports:</b> 0</p> | Closed | 3        | DOCUMENTS   |  |  |
|   |  |        |          | No linked documents   |  |  |
|   |  |        |          | LINK EXISTING DOCUMENT  |  |  |
|   |  |        |          | NEW DOCUMENT  |  |  |
| <p><b>Email changes to:</b> administrator &lt;administrator@siemdemo.ad&gt;</p>   |  |        |          | <input type="text" value="administrator"/>  | <input type="button" value="SUBSCRIBE"/> | <input type="button" value="UNSUBSCRIBE"/> |
| ADMINISTRATOR - 2015-01-29 12:11:13   |  |        |          |   |  |  |
| <p><b>Description</b></p> <p>Hyökkäys sisäverkosta SIEM-järjestelmään SSH-yhteydellä</p> <p><b>Action</b></p> <p>Tapaus otettu tutkintaan</p> |  |        |          | <p><b>STATUS:</b> Studying</p> <p><b>PRIORITY:</b> 3 Low</p> <p><b>IN CHARGE:</b> administrator</p> <p><b>SINCE CREATION:</b> 00:00</p> |  |  |
| ADMINISTRATOR - 2015-01-29 12:11:50   |  |        |          |   |  |  |
| <p><b>Description</b></p> <p>Tapaus ratkaistu.</p> <p><b>Action</b></p> <p>Ongelman aiheuttaja poistettu järjestelmästä.</p>                  |  |        |          | <p><b>STATUS:</b> Closed</p> <p><b>PRIORITY:</b> 3 Low</p> <p><b>IN CHARGE:</b> administrator</p> <p><b>SINCE CREATION:</b> 00:01</p>   |  |  |

**Cisco ASA 5505 -palomuurin konfiguraatio**

```
: Saved
:
ASA Version 7.2(4)
!
hostname asa
domain-name siemdemo.ad
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.65.3 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address 10.0.0.1 255.255.255.0
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```

**Cisco ASA 5505 -palomuurin konfiguraatio**

```
!  
interface Ethernet0/4  
!  
interface Ethernet0/5  
!  
interface Ethernet0/6  
!  
interface Ethernet0/7  
!  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name siemdemo.ad  
pager lines 24  
logging enable  
logging console emergencies  
logging trap notifications  
logging asdm informational  
logging host inside 192.168.65.30  
logging debug-trace  
mtu inside 1500  
mtu outside 1500  
icmp unreachable rate-limit 1 burst-size 1  
asdm image disk0:/asdm-524.bin  
no asdm history enable  
arp timeout 14400  
global (outside) 10 interface  
nat (inside) 10 192.168.65.0 255.255.255.0  
timeout xlate 3:00:00
```

**Cisco ASA 5505 -palomuurin konfiguraatio**

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
http 192.168.65.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh 192.168.65.0 255.255.255.0 inside
ssh timeout 5
console timeout 0

username admin password VAJC4m4PHAJfmezt encrypted privilege 15
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
```

**Cisco ASA 5505 -palomuurin konfiguraatio**

```
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6c2fa5be774822f4004cc0179246d6cd
: end
```