KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Marjo Laine

LOKITIETOJEN KERÄÄMINEN JA HYÖDYNTÄMINEN TIETO-TURVASSA

Opinnäytetyö
Toukokuu 2014

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Toukokuu 2014
Tietotekniikan koulutusohjelma

Karjalankatu 3
80200 JOENSUU
p. (013) 260 6800

Tekijä
Marjo Laine

Nimeke
Lokitietojen kerääminen ja hyödyntäminen tietoturvassa

Toimeksiantaja
Karelia-ammattikorkeakoulu

Tiivistelmä

Lokitiedot ovat ICT-verkossa eri järjestelmien ja sovellusten luomia tietoja, jotka kertovat järjestelmän tapahtumista. Tämän opinnäytetyön tarkoitus on selvittää, miten lokitietoja voidaan kerätä ja hyödyntää tietoturvassa. Työ koostuu lokitietojen teoriasta, muutaman lokitietoihin läheisesti liittyvän ohjelman esittelystä sekä Joensuun alueen yrityksille suunnatusta lokitietokyselystä.

ICT-verkossa lokitietoja käytetään vikatilanteiden selvittämiseen sekä mahdollisten hyökkääjien ja muiden tietoturvaongelmien ennaltaehkäisyyn ja jälkiselvityksiin. Työssä käydään läpi, mitä ja millaisia lokitiedot ovat, mistä niitä pitäisi kerätä, miten niitä käytetään ja mitä parhaita käytäntöjä niiden hallintaan liittyy. Lisäksi tarkastellaan lokitietoja perustanaan käyttäviä tietoturvasovellutuksia.

Yrityskyselyssä selvitettiin mitä mieltä eräät lokitiedoista vastaavat henkilöt ovat lokitiedoista ja omasta osaamisestaan, miten tietojen kerääminen ja hallinta on yrityksissä hoidettu sekä onko niitä tarvittu käytännössä. Kysely toteutettiin Googlen Drive-palvelulla ja lähetettiin yrityksille linkkinä sähköpostin kautta. Vähäisen osallistujamäärän vuoksi yleispäteviä tuloksia ei kuitenkaan syntynyt.

Kieli
suomi

Sivuja 49
Liitteet 2
Liitesivumäärä 5

Asiasanat

atk-järjestelmät, lokitiedostot, tietoturva,

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2014
Degree Programme in Information Technology
Karjalankatu 3
FI 80200 JOENSUU
FINLAND
Tel. 358-13-260 6800

Author
Marjo Laine

Title
Gathering and Using Log Files in Information Security

Commissioned by
Karelia University of Applied Sciences

Abstract

In an ICT-environment log files are information created by different nodes and applications conserning different events happening around the environment. The purpose of this thesis was to find out how to gather and make use of log files in information security. The paper consists of three elements: theory, presentation of applications closely related to log files and a query for businesses in Joensuu area about the log files.

Log files are commonly used in resolving technical problems and in prevention and aftermaths of security violations like attacks against the network. In this thesis questions like what are log files, how and where to gather them, how to use them and what kind of best practices one should know are covered. In addition, some applications based on log files are viewed.

The business query was about finding out what the employees responsible for log files think about them and their own know-how, how are gathering and handling the log files carried out in a company and if they have ever needed log files in some situation. The query was created with Google Drive and sent to businesses as a link within an e-mail. Due to low participation the results were not generally applicable though.

Language
Finnish

Pages 49
Appendices 2
Pages of Appendices 5

Keywords

information security, it-environment, log files

Sisältö

Lyhenteet

ELF	Extended Log Format, laajennettu lokiformaatti
HIPS	Host-based Intrusion Prevention System, isäntäpohjainen tunkeutumisenestojärjestelmä
IDS	Intrusion Detection System, tunkeutumisenhavaitsemisjärjestelmä
IDPS	Intrusion Detection and Prevention Systems, tunkeutumisen havaitsemis- ja estämisjärjestelmät
IIS	Internet Information Services, Microsoftin kehittämä palvelinohjelmistokokonaisuus
IPS	Intrusion Prevention System, tunkeutumisenestojärjestelmä
LTSV	Labeled Tab-separated Values, eräs lokiformaatti
NBA	Network Behaviour Analysis, eräs tunkeutumisenestojärjestelmän tyyppi
NIPS	Network-based Intrusion Prevention System, verkkopohjainen tunkeutumisenestojärjestelmä
NTP	Network Time Protocol, verkon aikaprotokolla
SEM	Security Event Management, turvallisuustapahtumien hallinta
SIEM	Security Information and Event Management, turvallisuustietojen ja -tapahtumien hallinta
SIM	Security Information Management, turvallisuustietojen hallinta
WIPS	Wireless Intrusion Prevention System, langaton tunkeutumisenestojärjestelmä

1 Johdanto

Lokitiedot ovat ICT-verkossa laitteiden (esimerkiksi palvelimet, reitittimet) keräämiä tietoja kyseisiin laitteisiin, eri sovelluksiin ja verkkoon liittyvistä tapahtumista. Lokitietojen avulla järjestelmänvalvoja saa tietoja verkkonsa tapahtumista, pystyy havaitsemaan ongelmat, kuten järjestelmän vikatilat, hyökkäykset tai muut tietoturvarikkomukset, ja kykenee toimimaan tilanteen edellyttämällä tavalla. Tämän opinnäytetyön tarkoituksena on selvittää ICT-verkon näkökulmasta miten ja millä näitä tietoja kerätään sekä miten niitä voidaan käytännössä hyödyntää tietoturvassa.

Opinnäytetyö koostuu teoriaosuudesta, käytännön osuudesta ja tutkimusosuudesta. Teoriaosuudessa käydään läpi lokitietojen ominaisuudet ja käyttö, käytännön osuudessa tarkastellaan muutamia lokitietoihin liittyviä ohjelmia ja tutkimusosuudessa toteutetaan kvantitatiivinen kysely lokitietojen käytöstä eräille Joensuun alueen yrityksille. Kyselyn tarkoituksena on saada teorian tueksi tietoa käytännön työelämän käytännöistä. Kysely on toteutettu Googlen Drive-palvelulla, joka mahdollistaa nopean vastaamisen ja vastaajien anonyymiyden.

2 Lokitiedot

Lokitiedot ovat minkä tahansa järjestelmän ylläpitäjän työkalu. Ideana on, että järjestelmä tuottaa toiminnastaan tietyntyyppisiä tiedotteita, joita analysoimalla ylläpitäjä saa ajantasaista tietoa järjestelmänsä toiminnasta. ICT-verkossa lokitietoja tuottavat aktiivilaitteet, esimerkiksi palvelimet, reitittimet ja palomuurit ja ne sisältävät kullekin laitteelle ominaista informaatiota. Esimerkiksi palomuuri tuottaa lokeja sen kautta kulkevista ja hylätyistä paketeista sekä omasta toiminnastaan ja järjestelmästään (Allen 2001, 157). Lokitiedot tallennetaan tiedostoon, jonka pääte on yleisimmin .log tai .txt (TechTerms.com, 2010).

Lokityyppejä ja formaatteja on monia, joten eri toimittajien laitteet ja ohjelmat eivät välttämättä tuota samaa tai edes samassa muodossa olevaa tietoa (Allen 2001, 204). Järjestelmän ylläpitäjän täytyy kuitenkin saada selvää järjestelmänsä lokiviidakosta ja tätä varten voidaan käyttää analysointiohjelmaa, joka tulkitsee järjestelmän viestit ja kertoo ylläpitäjälle tapahtumista selkokielellä. Myös varsinaiseen lokien keräämiseen on paljon vaihtoehtoja: on järjestelmien omia ohjelmia, ilmaisia tai open source -pohjaisia ohjelmia sekä täysin kaupallisia ohjelmia, joiden käytöstä maksetaan kehittäjälle.

Lokeja voidaan käyttää joko tapahtumien jälkeen syiden selvitykseen tai reaaliajassa kertomaan siitä, mitä järjestelmässä tapahtuu juuri nyt. Järjestelmänvalvojan apuna analysoinnissa ovat erilaiset ohjelmistot, tunkeutumisen havaitsemis- ja estämisjärjestelmä IDPS tai turvallisuustietojen ja tapahtumien hallintasovellus, SIEM.

Syslog on lokitietojen keräämisen standardisoitu protokolla. Se erottelee tosistaan viestin sisällön ja niiden kuljetuksen, minkä ansiosta eri toimittajien laitteet kykenevät toimimaan yhdessä. Syslogia tukevat monet laitteet ja eri alustat. (Gerhards 2009, 1.)

2.1 Lokityypit

Erilaisia lokityyppejä on useita eikä jäykkää, virallista luokittelua ole, vaan lokin tyyppi määräytyy yksinkertaisesti sillä, minkälaista tietoa sillä halutaan saada. Esimerkiksi Windows kerää oletuksena sovellus-, turvallisuus- ja järjestelmälokeja (TechTerms.com, 2010). Järjestelmänvalvojan tulisi kuitenkin itse määrittää, millaisia lokityyppejä hän tarvitsee ja konfiguroida lokien keräys sen mukaan, jotta järjestelmästä saataisiin tietoa mahdollisimman kattavasti eikä resursseja menisi hukkaan (Allen 2001, 199–200).

Paitsi niiden sisältämän tiedon, lokien tyypit määräytyvät myös niitä käyttävän järjestelmän mukaan. Esimerkiksi WWW-palvelimelle on olemassa neljä erilaista lokia:

- tapahtumaloki, joka tuottaa yhdestä tapahtumasta aina yhden merkinnän
- virheloki, joka tuottaa yhdestä virheestä aina yhden merkinnän
- selaintyyppiloki, joka sisältää tietoa selaimista, joilla www-sivua on käsitelty
- viittausloki, joka kerää http-yhteyteen liittyvää tietoa, esimerkiksi sivustolle viittaavia URL-osoitteita. (Allen 2001, 94–95.)

2.2 Lokien keräys

Koska erilaisia lokityyppejä on niin paljon, on kerääviä tahojakin useita. Laitteiden (palvelimet, verkkolaitteet) omat käyttöjärjestelmät keräävät tietoja itsestään, mutta myös sovelluksista ja käyttäjien toimista tarvitaan usein lokeja eikä niitä välttämättä saada kerättyä ilman kolmannen osapuolen lisäohjelmia. (Allen 2001, 199).

2.2.1. Käyttöjärjestelmien sisäiset ohjelmat

Koska lokit ovat tietotekniikassa oleellinen ja tärkeä asia, on ICT-verkossa käytettävillä eri laitteiden käyttöjärjestelmillä yleensä oma, sisäinen lokiohjelmansa, joka tallentaa jonkin verran ennalta määritettyjä tietoja. Palvelinpuolella käyttöjärjestelmänä käytetään yleensä Microsoft Windowsia tai Linuxia, verkkolaitteissa taas valmistajien omia järjestelmiä.

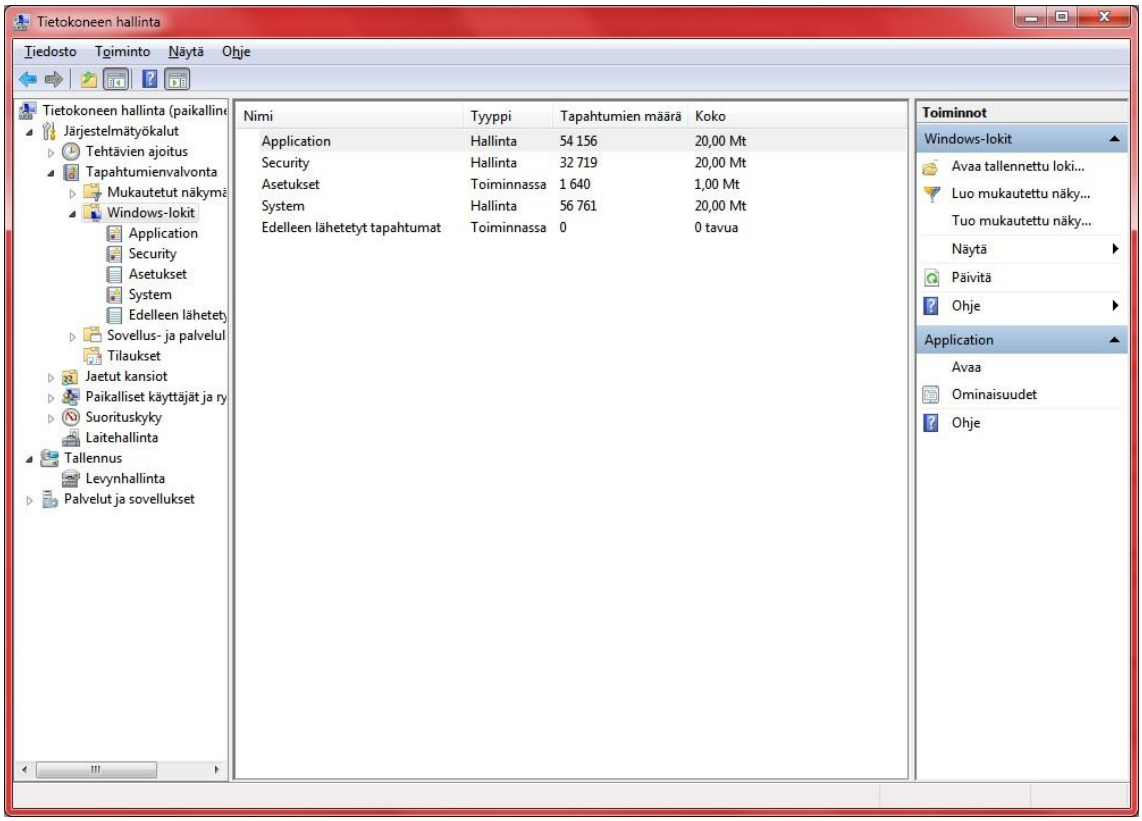
Windowsin lokiohjelman nimi on Tapahtumienvalvonta (Event Viewer). Se sisältää kaksi erilaista kategoriaa: Windowsin lokit ja sovellus- ja palvelulokit, joista ensimmäinen tallentaa koko järjestelmään vaikuttavat tapahtumat ja jälkimmäinen vain yksittäisten sovellusten tai palveluiden tapahtumat. (Microsoft TechNet, 2014.)

Windows-lokit sisältää viisi alakategoriaa:

- ohjelmatapahtumat

- tietoturvaan liittyvät tapahtumat
- sovellustapahtumat
- järjestelmätapahtumat
- välitetyt tapahtumat.

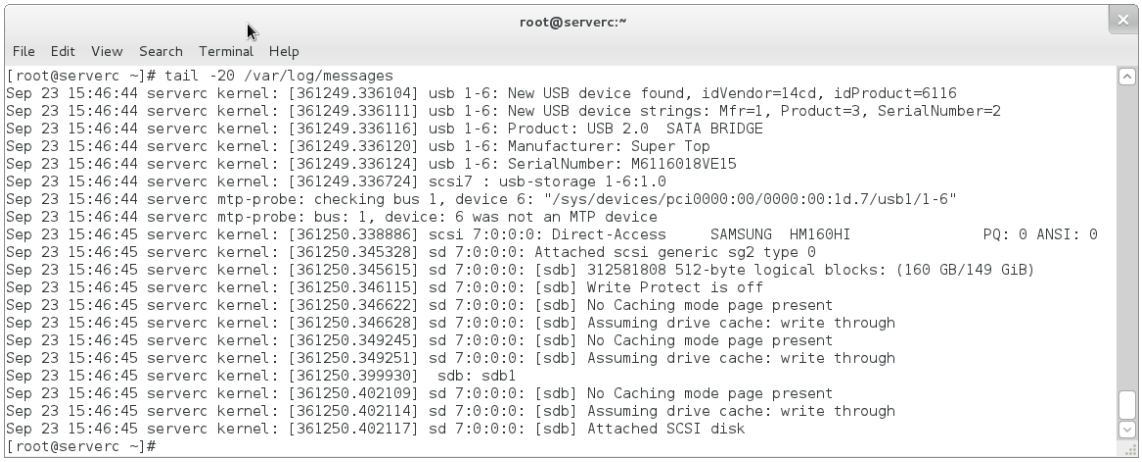
Ohjelmatapahtumiin tallentuu esimerkiksi ohjelmien tai palveluiden toiminta ja ne jaetaan virheiksi, varoituksiksi ja tiedoiksi tapahtuman vakavuuden mukaan. Järjestelmätapahtumat ovat samanlaisia, mutta kuvaavat Windowsin omaa toimintaa. Tietoturvaan liittyviin tapahtumiin kuuluvat esimerkiksi käyttäjien kirjautumiset, asennustapahtumat ovat nimensä mukaisia ja välitettyihin tapahtumiin tallentuvat muiden koneiden välittämät tapahtumat. (Microsoft TechNet, 2014.) Kuvassa 1 on kuvankaappaus Tapahtumienvalvonnasta.



Kuva 1. Windows Tapahtumienvalvonta.

Linux käyttää lokiensa luomiseen rsyslogd-palvelua ja tiedostot löytyvät polusta /var/logs. Kategorioita on runsaasti, esimerkiksi omat lokinsa sisäänkirjautumi-

sille, kernelille ja MySQL-palvelulle, mutta järjestelmälle löytyy myös yleinen tapahtumaloki polusta /var/log/messages (kuva 2). (nixCraft, 2013.)



Kuva 2. Linuxin tapahtumaloki. (Kuva: BasicLinuxCommands.com, 2011)

2.2.2. Kolmansien osapuolien ohjelmat

Järjestelmien omien lokien lisäksi tarjolla on kolmansien osapuolien lokiohjelmia. Nämä ohjelmat voivat olla maksullisia, ilmaisia tai vapaan lähdekoodin pohjalta kehitettyjä. Kolmansien osapuolien lokiohjelmien käyttö onkin suotavaa, sillä yhdellä ohjelmalla on mahdotonta saada kaikkea tarvittavaa tietoa. Kun loki-infrastruktuuriinsa lisää monipuolisesti erityyppisiä ohjelmia (esimerkiksi analyysiohjelmat, tunkeutumisen havaitsemis- tai estojärjestelmät), verkon tietoturva lisääntyy, sillä monta ohjelmaa havaitsee uhan paremmin kuin yksi. (Kent & Souppaya, 2006.) Esimerkkinä kolmannen osapuolen ohjelmista voidaan mainita myöhemmin tässä työssä tarkemmin esiteltävä maksullinen Alentum Softwaren WebLog Expert, ilmainen lokienhallintaohjelma Splunk sekä maailman suosituin vapaan lähdekoodin tunkeutumisen havaitsemis- ja estojärjestelmä Snort.

2.3 Lokiformaatit

Web-palvelimien luomilla tapahtumalokeilla on ennalta määrätyt formaatit ja kuten tyyppejäkin, niitä on paljon. Kolme yleisintä ovat kuitenkin standardisoitu Common Log Format, tämän laajennettu versio Combined Log Format sekä edellisiä joustavampi Extended Log Format, jotka on luotu jo 90-luvulla mutta joita käytetään yhä laajalti, esimerkiksi Extended Log Format on yhä käytössä uusimmassa Microsoft IIS:ssä (Internet Information Services) (IIS.net, 2014). Näiden lisäksi löytyy paljon muita, esimerkiksi käyttöjärjestelmien omia formaatteja, tietokantaformaatteja sekä tiettyä erotinta käyttäviä formaatteja. Erityisesti Labeled Tab-separated Values -formaattia (LTSV) on suunniteltu Common Log Formatin korvaajaksi, mutta siinä ei ole ainakaan vielä onnistuttu (Tanaka, 2014).

Common Log Format tunnetaan myös nimellä NCSA Common Log File Format ja se sisältää seitsemän kenttää: etäisännän IP-osoitteen, etäisännän tunnisteen RFC1413:n mukaisesti, käyttäjän nimen, päivämäärän ja kellonajan, pyydetyn URLin, pyynnön tilan http-koodina sekä siirrettyjen tavujen määrän (Luotonen, 1995) Loki tallennetaan ASCII-muodossa, kellonaikana käytetään aina paikallista aikaa ja puuttuvien tietojen kohdalle merkitään viiva (Nihuo Software, 2014). Kuvassa 3 näkyy esimerkki Common Log Formaatin syntaksista.

```
127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

Kuva 3. Common Log Format. (Kuva: Wikipedia, 2013.)

Combined Log Format on muuten sisällöltään sama kuin Common Log Format, mutta se sisältää kolme lisäkenttää: viittauksen (eli miltä sivustolta käyttäjä tuli), käyttäjän selaintyypin sekä evästeen (kuva 4). Kaksi ensimmäistä kenttää ovat kuitenkin vapaavalintaisia. (IBM, 2014.) Tavallisesti Combined Log Formatin sisältämät lisätiedot kuuluvat selaintyyppi- tai viittauslokeihin, mutta näiden yhdistäminen yhdeksi lokiksi helpottaa ylläpitäjän työtä (Allen 2001, 95).

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"
```

Kuva 4. Combined Log Format. (Kuva: Apache, 2014.)

Extended Log Format (ELF) kehitettiin antamaan ylläpitäjälle vapaus päättää itse, mitä tietoja kerätään, mutta se säilyttää kuitenkin useimpien analyysiohjelmistojen ymmärtämän formaatin (Hallam-Baker & Behlendorf, 2014). ELF eroaa edeltävistä formaateista siten, että se sisältää yhden rivin sijaan useita rivejä ja jokainen rivi voi sisältää joko ohjesäännön tai merkinnän. Ensimmäiset rivit sisältävät kuitenkin aina versionumeron ja luettelon kerättävistä kentistä. (IBM, 2014). Kuvassa 5 on esimerkki ELF-tiedostosta.

```
#Version: 1.0
#Date: 12-Jan-1996 00:00:00
#Fields: time cs-method cs-uri
00:34:23 GET /foo/bar.html
12:21:16 GET /foo/bar.html
12:45:52 GET /foo/bar.html
12:57:34 GET /foo/bar.html
```

Kuva 5. Extended Log Format. (Kuva: Hallam-Baker & Behlendorf, 2014.)

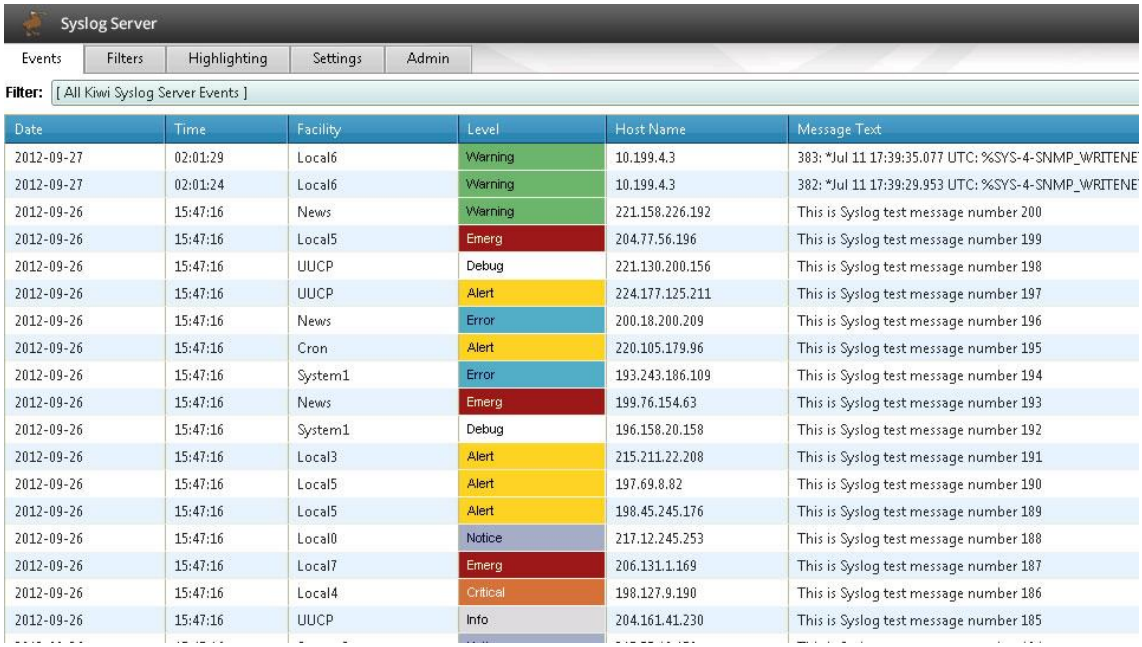
2.4 Syslog

Syslog on standardisoitu asiakas/palvelin-protokolla lokitietoja varten. Se erottelee toisistaan lokien käytön eri osat, kuten viestin luomisen, kuljetuksen ja tulkinnan, joka mahdollistaa eri järjestelmien ja ohjelmien toimimisen yhdessä. Syslogin avulla voidaan esimerkiksi luoda keskitetty syslog-lokipalvelin, johon kerätään lokitietoja useista eri laitteista ja ohjelmista (Anonymous 2001, 259).

Syslogin kehitti 80-luvulla Eric Allman Sendmail-projektille (Internetissä toimiva sähköpostien reititysjärjestelmä). Se osoittautui kuitenkin niin toimivaksi, että pian se otettiin myös muuhun käyttöön ja ensimmäinen virallinen määritys sille tehtiin 2001. (Eaton 2003, 7). Syslogia on yritetty vuosien saatossa patentoida

(kiinalainen Huawei 2006), mutta protokolla standardisoitiin tästä huolimatta 2009 (Gerhards 2009, 1).

Syslogia käytetään kaikenlaisiin lokeihin tietoturvasta ohjelmistokehitykseen. Se antaa viestille järjestelmäkoodin viestin luoneen ohjelman tyypin mukaan (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp tai local0 ... local7) ja vakavuuden, joita on yhteensä kahdeksan vakavimmasta alkaen: Emergency, Alert, Critical, Error, Warning, Notice, Info ja Debug (kuva 6). (Gerhards 2009, 9.) Syslogille on paljon vapaan lähdekoodin pohjalta tehtyjä sovelluksia viestien tulkitsemiseen.



Kuva 6. Esimerkki syslogia käyttävästä ohjelmasta. (Kuva: Kiwi, 2014.)

Syslogin haittapuolena ovat sen turvallisuusongelmat. Se käyttää UDP-protokollaa tiedonsiirtoon, mikä on TCP:tä turvattomampaa eikä varmista viestien perillepääsyä. (Gerhards 2009, 25.) Ongelman ovat osittain ratkaisseet eri sovellukset, kuten esimerkiksi rsyslog ja syslog-ng, jotka käyttävät pohjanaan syslog-protokollaa, mutta ovat lisänneet siihen ominaisuuksia, kuten suodatuksen, paremman konfiguroinnin ja turvallisemman TCP-protokollan käytön. Syslog-viestit voidaan myös salata TLS/SSL-protokollalla, mikä ei kuitenkaan sisälly itse syslog-protokollaan (Gerhards 2009, 26).

Syslog on nykyisin oletuslokiratkaisu UNIX-järjestelmissä. Sitä käytetään laajalti myös verkkolaitteissa, kuten reitittimissä ja palomuureissa, ja esimerkiksi Windowsin Event Viewerin lokit voidaan konvertoida syslog-muotoon. (Leskiw 2014.) Syslogille ei tällä hetkellä ole varteenotettavaa kilpailijaa.

3 Lokitietojen käyttö

Lokeilla on järjestelmänvalvojalle monta käyttötarkoitusta: ne auttavat etsimään vikoja laitteista, ohjelmistoista ja verkosta, havaitsemaan hyökkääjiä, tutkimaan näiden jälkiä ja lopulta niitä voidaan käyttää todisteena oikeudessa (Anonymous 2001, 258). Tästä syystä järjestelmänvalvojan tulisikin olla hyvin perillä lokin koko elinkaaresta (kerääminen, analysointi, hävittäminen) ja noudattaa tietoturvaeksperttien suosittelemia parhaita käytäntöjä.

Jotta lokeista olisi hyötyä, niitä tulisi myös aktiivisesti analysoida. Tässä järjestelmänvalvojaa auttavat erilaiset ohjelmistot, jotka voivat esimerkiksi tutkia lokeja itsenäisesti ja antaa hälytyksen tilanteen vaatiessa tai tuottaa lokien tiedoista vaikkapa taulukkoja ja kaavioita. Lokien tarkkailun tiheys olisi hyvä määrittää yrityksen tarpeen mukaan.

3.1 Lokitietojen keräämisen ja käytön parhaat käytännöt

Yleissääntönä lokeja tulisi kerätä järjestelmässä lähes kaikesta (Moeller 2010, 164). Tyypillisiä lokitietoja kerääviä tahoja ovat esimerkiksi antivirusohjelmistot, palomuurit, IDPS:t, eri laitteiden käyttöjärjestelmät sekä erilaiset sovellukset (ITBusinessEdge, 2014). Ymmärrettävästi lokitiedostoja tulee tällöin runsaasti ja ylläpitäjä joutuu tasapainoilemaan resurssien ja tietojen kattavuuden välillä. Mikäli lokeja kerätään liikaa, vaikuttaa se järjestelmän suorituskykyyn ja levytilaan, minkä takia ylläpitäjän tulisikin määrittää, mitä tietoja kerätään, eikä sokeasti haalia lokeja kaikesta mahdollisesta (Bradley 2006, 168.)

Lokien todellisen tarpeen määrittää kuitenkin yrityksen oma tietoturvapolitiikka ja yrityksen tietoturvasuunnitelmaan tulisikin kirjata myös lokien hallintasuunnitelma (Kent & Souppaya, 2006). Lokimekanismeja pystyttäessään ylläpitäjän pitäisi siis varmistaa, että saa varmasti järjestelmästä ja verkosta politiikassa määritellyt tiedot jo olemassa olevista lokeista ja mitä tietoja ylipäätänsä kerätään lokeilla ja mitä muilla tavoin, esimerkiksi käyttämällä IDPS-järjestelmää. (Allen 2001, 204–205).

Järjestelmien omien lokien vajavaisuuden takia kolmansien osapuolien ohjelmistojen käyttö on tärkeää. Järjestelmää ja verkkoa vahingoittamaan tai urkkimaan pyrkivät tunkeilijat tuntevat järjestelmien omat lokimekanismit hyvin ja opettelevat myös muuntelemaan niitä peittääkseen omat jälkensä. Ulkopuolisia ohjelmistoja ei tunneta läheskään samoin, joten niiden tuottamat tiedot ovat paremmassa turvassa ja luotettavampia hyökkäyksen sattuessa. (Anonymous 2001, 260–261.)

Lokien keräämisen ei pitäisi olla pelkkää hälytysten tutkimista, sillä jos järjestelmänvalvoja seuraa vain tunnettuja uhkia, jäävät uudet ja viekkaammat hyökkäykset ja tunkeutumiset huomaamatta. Käytössä tulisikin olla verkon tai järjestelmän perustoimintaa tallentava loki, johon myöhempiä lokitietoja voidaan verrata ja täten huomata poikkeavat toiminnot, vaikka niistä ei hälytystä syntyisikään (Barnett 2012, 37.)

Kaiken kaikkiaan lokien keruu tulisi suunnitella niin, että lokit pystyvät auttamaan verkon ja järjestelmien optimoinnissa, tallentamaan käyttäjien toimia sekä tunnistamaan hyökkäyksiä ja tunkeutujia. Ylläpitäjän olisi myös tärkeää testata aika ajoin, että lokien keruu on varmasti toiminnassa (Kent & Souppaya, 2006.)

3.1.1. Lokipalvelin ja -verkko

Paras ratkaisu lokien keruuseen olisi keskitetty, syslog-pohjainen lokipalvelin, joka keräisi lokit kaikista tarvittavista lähteistä yhteen paikkaan (Barnett 2013,

90). Jotta keskitetty lokipalvelin olisi mahdollisimman toimiva, kaikki järjestelmät tulisi ensin asettaa samaan aikaan esimerkiksi Network Time Protocolin (NTP) avulla (Kent & Souppaya, 2006). Eri lokeja tuottaville tahoille tarvitaan omat tiedostot ja tätä varten pitäisi varmistaa, että palvelimella on riittävästi tilaa. Ihan kaikkea ei tarvitse eikä kannatakaan palvelimelle tuoda: paikallisesti säilötään mahdollisimman paljon ja palvelimelle vain tärkeimmät tai käytetyimmät lokit. (Allen 2001, 158.) Ylläpitäjän tulisi siis joka tapauksessa tietää myös paikallisten lokien sijainnit eri laitteissa (Allen 2001, 205).

Lokipalvelimen suojaukseen tulisi kiinnittää erityistä huomiota. Palvelimessa kannattaa sallia vain ja ainoastaan portti 514 eli UDP-portti (tai mikä tahansa järjestelmänvalvojan määrittämä käyttämätön portti), jota pitkin syslog-liikenne kulkee (Anonymous 2001, 260). Salasanoja ei lokien mukana kannata tuoda ollenkaan tai ainakin ne pitäisi salata erityisen huolellisesti, sillä väärät salasanat poikkeavat oikeista yleensä hyvin vähän (Allen 2001, 204). Mahdollisten etäyhteyksien tulisi olla salattuja ja jos lokeja halutaan siirtää, olisi hyvä käyttää yksisuuntaista laitetta eli laitetta josta data liikkuu vain yhteen suuntaan tai write-once-mediaa (media, johon voi kirjoittaa vain kerran, esimerkiksi cd-levy) (Anonymous 2001, 259). Yleensäkin lokitiedostojen asetukset palvelimella tulisi määritellä niin, että lokitiedostoihin voi lisätä tietoja, mutta olemassa olevaa dataa ei voi muuttaa (Allen 2001, 218).

3.1.2. Palomuuri ja lokit

Yksi ICT-verkon tärkeimmistä lokien tuottajista on palomuuri. Sen nimenomainen tehtävä on estää ja havainnoida tunkeilijoita, joten sen lokitiedostot ovat siksi erittäin merkittäviä verkon turvallisuuden kannalta. Palomuurin lokien konfiguroiminen kannattaakin tehdä erityisen huolellisesti, sillä huonot keräysperusteet täyttävät levytilan äkkiä turhista lokeista ja tekevät analysoinnin työlääksi. Nykyisiin, älykkäämpiin palomuureihin saa kuitenkin lisättyä palvelunestohyökkäysten tarkistuksia, IPS-toimintoja (Intrusion Prevention System) sekä protokolla-analyysimahdollisuuksia, jotka osaavat rajoittaa hälytykset vain ja ainoas-

taan oikeisiin uhkiin, mikä vähentää turhien lokien ja työn määrää (Woody 2013, 237.)

Aluksi tulisi määrittää, millaisista paketeista lokeja oikein kerätään. Näitä määritelmiä kutsutaan lokisäännöiksi. Sääntöjen suhteen pitäisi huolehtia erityisesti se, ettei lokipaketteja mene paketinsuodatukseen ja näin synny ikuista silmukkaa. Palomuurin lokitiedostoja varten pitäisi määritellä mikä on niiden sijainti ja koko, miten tiheästi tietoja syntyy, kenellä on niihin käyttöoikeus ja mitä salausta käytetään. (Allen 2001, 158–159.) Myös palomuurin käyttäytyminen lokien täyttymisen jälkeen, esimerkiksi antaako laite hälytyksen vai kirjoittaako vanhan tiedon päälle, tulisi selvittää tietoturvan parantamiseksi. Palomuuriin kannattaakin lisätä jonkinlainen arkistointijärjestelmä vanhoja lokitietoja varten (Kent & Souppaya, 2006).

Palomuurin pitäisi myös osata tehdä hälytys tärkeistä tapahtumista, vaikka ainakin osan näistä hälytyksistä voi antaa tehtäväksi myös keskitetylle lokipalvelimelle. Hälytyksen pitäisi syntyä ainakin epäonnistuneista sisäänkirjautumisista, suodatussääntöjen muutoksista tai poistamisesta, aina kun palomuuriin on kirjauduttu onnistuneesti, palomuurin tärkeitä tiedostoja on muuteltu tai järjestelmässä on jokin ongelma, esimerkiksi tilan vähyys. Analysoinnin kannalta olisi myös helpointa, mikäli palomuuri kykenisi tuottamaan jonkinlaisia yhteenvetoja toiminnastaan ja hälytyksistä. Konfiguroinnin jälkeen ylläpitäjän tulisi myös testata palomuurin toiminta. (Allen 2001, 159–161.)

3.2 Analysointi

Jotta lokeista lopulta olisi oikeasti hyötyä, on lokitietoja analysoitava joko manuaalisesti tai jollakin ohjelmalla. Ensin mainittu tapa on kuitenkin todella hankala, hidas ja vaatii ylläpitäjältä lähes mahdottomia, joten jonkin analysointiohjelman hankinta onkin todella suositeltavaa. Ohjelmistoja löytyy sekä kaupalliselta että vapaan lähdekoodin puolelta ja yleisesti näiden tehtävä on kasata lokien antamat tiedot ihmiselle helpommiksi ymmärtää käyttäen apuna esimerkiksi erilaisia kaavioita ja tilastoja.

Lokeja olisi hyvä tarkkailla rutiininomaisesti, sillä näin saadaan tietoa verkon toiminnasta normaaliolosuhteissa ja mahdollisiin ongelmiin päästään puuttumaan mahdollisimman nopeasti. Lokien tutkimisen tiheyteen vaikuttaa esimerkiksi verkon tärkeys ja riskialttius: vähemmän tärkeille ja riskialttiille verkoille riittää lokien tutkiminen esimerkiksi muutaman päivän välein, kun taas korkean riskin verkkoja olisi hyvä tarkastaa useita kertoja päivässä (ITBusinessEdge, 2011).

3.3 Havaitseminen ja hälytykset

Kun lokit on kerätty ja analysoitu, joko manuaalisesti tai ohjelmistoa apuna käyttäen, voidaan lopputuloksesta havaita ongelmia esimerkiksi verkkoresurssien käytössä tai tunkeilijan muodossa. Järjestelmänvalvoja voi nähdä ongelmat vertailemalla analyysin tuloksia verkon oletusarvotilaan. Jos oletusarvotilaa ei ole määritetty, järjestelmänvalvojalla ei ole mahdollisuutta arvioida oman verkkonsa sen hetkistä toimintaa. Havainnoinnin jättäminen yksin järjestelmänvalvojalle on kuitenkin melko epäkäytännöllistä (Allen 2001, 158).

Ongelmien havainnointi voidaan jättää myös jonkin ohjelman tai laitteen (IDPS, SIEM) tehtäväksi ja tällöin kyseinen ohjelma tai laite hälyttää järjestelmänvalvojan huomatessaan oletusarvotilasta poikkeavaa toimintaa. Hälytyksen voi määritellä annettavaksi automaattisesti tiettyjen tapahtumien tai ehtojen täyttyessä ja kriittisissä tilanteissa hälytys voi olla akuuttikin, esimerkiksi sähköposti tai tekstiviesti järjestelmänvalvojalle tai muulle tietoturvahenkilölle (Allen 2001, 206). Tämä tapa on manuaalista havainnointia huomattavasti tehokkaampaa.

3.3.1. Tunkeilijoiden havaitsemis- ja estämisjärjestelmät

Oma lukunsa ovat myös IDS (Intrusion Detection System) ja IPS, jotka keräävät informaatiota, analysoivat tiedon itsenäisesti ja toimivat havaitessaan uhan. Ne ovat hyviä käytännön esimerkkejä lokien käytöstä tietoturvassa, sillä ne kerää-

vät, analysoivat, tekevät hälytyksen tai toimivat tarpeen vaatiessa hyökkääjää vastaan eli suorittavat koko lokiprosessin itsenäisesti. Niitä voidaan myös käyttää mm. yrityksen tietoturvapolitiikan testaukseen ja olemassa olevien uhkien dokumentointiin. IDPS onkin nykyisin yrityksille erittäin tärkeä, lähes välttämätön verkon osa. (Scarfone & Mell, 2007.)

IDS on laitteena passiivinen ja suorittaa lähinnä tarkkailua, hälytyksiä ja raporttien luomista. Se tarkkailee liikennettä ja vertailee sitä ennalta luotuihin sääntöihin. IDS vaatii kuitenkin huolellisen konfiguroinnin, sillä muuten täysin laillisellakin liikenteellä on suuri riski joutua hälytyksen kohteeksi, mikä taas teettää paljon turhaa työtä järjestelmänvalvojalle. (Gigamon, 2014.)

Siinä missä IDS tarkkailee verkkoa ja suorittaa hälytyksiä, voi IPS lisäksi pyrkiä estämään hyökkääjän toimia. Keinoinaan IPS käyttää hälytysten lisäksi mm. pakettien hylkäämistä, yhteyksien nollaamista ja epäilyttävien IP-osoitteiden estämistä. IPS:t voidaan myös jakaa neljään eri luokkaan.

- verkkopohjaiset, tarkkailevat koko verkkoa analysoimalla protokollien toimintaa
- langattomat, tarkkailevat langatonta verkkoa
- isäntäpohjaiset, tarkkailevat ja suojaavat yhtä isäntäkonetta
- verkon käyttäytymisanalyysi, jossa verkkoliikennettä tarkkaillaan jotta löydettäisiin normaalista poikkeavaa verkkoliikennettä aiheuttavat uhat. (Boyles 2010, 249.)

IDS:n paikka verkossa on DMZ:lla tai palomuurin yhteydessä, IPS taas sijoitetaan verkkoliikenteen lähteen ja päämäärän väliin (esimerkiksi ulkoverkko ja palvelin). IDPS:n hyöty on siinä, että ne kykenevät havaitsemaan hyökkäykset, jotka jäävät palomuurilta huomaamatta, esimerkiksi palvelunestohyökkäys tai epäilyttävät sisäänkirjautumisyritykset. (Gigamon, 2014.) IDPS ei kuitenkaan korvaa palomuuria tai virustentorjuntaohjelmaa, vaan on tarkoitettu niiden lisäksi luomaan turvallisempaa verkkoa (Webopedia, 2005).

3.3.2. Turvallisuustietojen ja -tapahtumien hallinnointi

Mitä suurempi verkko yrityksellä on, sitä enemmän lokeja siitä kerätään ja sitä enemmän tietoa on käsiteltävänä. Koska manuaalisesti kaiken sen tietomäärän analysoiminen on hankalaa, on markkinoille kehitetty verrattain uusi apuväline, SIEM. SIEM koostuu kahdesta osasta, SEMistä (Security Event Manager) ja SIMistä, (Security Information Manager) joita molempia voidaan käyttää myös erikseen. (Cysec, 2012.)

SIMiä kutsutaan myös lokien hallinnaksi ja se on osa, joka kerää ja varastoi lokit sekä raportoi niistä. SEM taas on osa, joka analysoi lokit ja suorittaa hälytykset. SIEM on kehitetty vuonna 1997 ja vielä tälläkin hetkellä kehittyy kovalla tahdilla. Se on hyvin älykäs tietoturvaratkaisu, sillä yksittäisten tapahtumien sijaan se osaa etsiä yhteyksiä eri tapahtumien välillä, mikä erottaakin sen IDPS:stä. Esimerkiksi yksittäisten sisäänkirjautumisten raportoinnin sijaan SIEM saattaa löytää huolestuttavan yhteyden sisäänkirjautumisen, epäilyttävän kellonajan ja käyttäjän yhtäkkiä lisääntyneiden oikeuksien välillä ja tehdä tästä hälytyksen järjestelmänvalvojalle. Lopullinen älykkyys määrittyy kuitenkin ohjelmiston tekijöiden taitojen perusteella, sillä SIEM toimii käyttöönoton jälkeen automaattisesti eikä sitä tarvitse itse konfiguroida. Siksi SIEMin ollessa kyseessä, yrityksen kannattaakin panostaa siihen kunnolla. (Cysec, 2012.)

3.4 Lokitiedot oikeustoimissa

Suomen laissa on lokitietojen käytöstä muutamia kohtia, mutta suurimmaksi osaksi ne koskevat henkilörekistereitä. Loki muuttuu henkilörekisteriksi, jos sen perusteella voidaan tunnistaa eri henkilöitä ja tällöin sitä täytyy kohdella laissa määritetyllä, henkilörekisterin edellyttämällä tavalla. Laiminlyönnit voivat johtaa rikostutkintaan. (Valtiovarainministeriö 2009, 21–22.)

Poliisi voi pyytää ja käyttää lokeja muiden tietorikosten kuin salassapitorikosten selvittämiseksi. Salassapitorikoksissa viestinnän lokitietoja suojelee tietosuojalaki, joka ei anna lokeja välittävälle organisaatiolle käsittelylupaa tietoihin, ellei

se ole itse selkeästi viestinnän osapuoli, ja täten organisaatio ei voi lokeja poliisille luovuttaa. Poliisi voi myös pakkokeinolain perusteella organisaatiota säilyttämään datan muuttumattomana, mikäli on syytä epäillä, että tutkinnalle tärkeitä tietoja saatetaan muokata jälkeenpäin. Kaikissa tapauksissa poliisin on kuitenkin perusteltava pyyntönsä lokien saamiseksi. (Valtiovarainministeriö 2009, 50–51.)

4 Ohjelmistojen tarkastelu

Tässä osiossa on tarkoituksena tarkastella lähempää yhtä lokien analysointiohjelmaa, yhtä IDS:ää ja yhtä SIEMiä ja siten esitellä näitä lokeihin ja tietoturvaan liittyviä sovelluksia käytännössä. Lokien analysointiohjelmaksi olen valinnut Alentum Softwaren WebLog Expertin, IDS:ksi Cyberarmsin Intrusion Detection and Defense Systemin (IDDS) ja SIEMiksi ManageEnginen EventLog Analyzerin. Ohjelmia ei ole valittu millään erityisellä perusteella. Käyttöjärjestelmänä on Windows 7 64-bit.

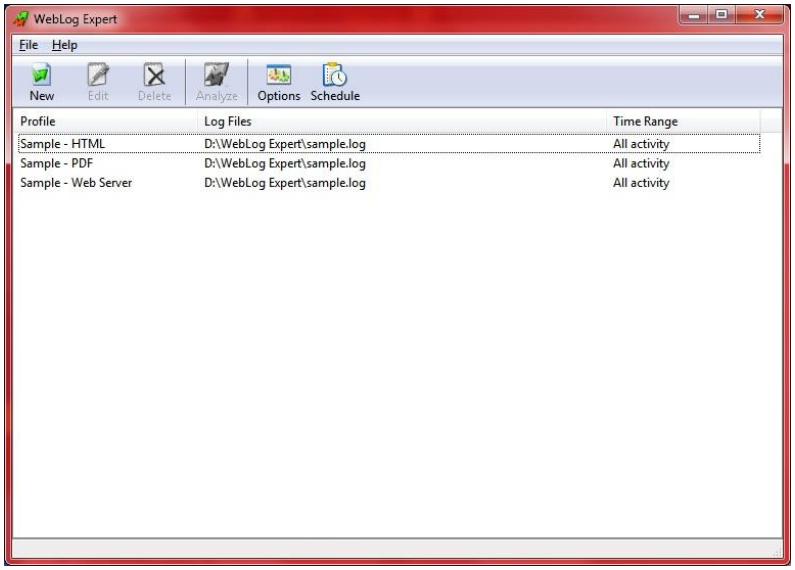
4.1 Lokien analysointi – Alentum Software WebLog Expert

Alentum Software on israelilainen ohjelmistoyritys, joka tarjoaa web-palvelimien käyttöön liittyviä ohjelmia, kuten esimerkiksi sivukarttoja ja RSS-syötteen muokkaukseen tarvittavia työkaluja. WebLog Analyzer on hyvin yksinkertainen web-palvelimille tarkoitettu lokien analysointiohjelma, joka antaa tietoja palvelimella sijaitsevan sivuston käyttäjistä, esimerkiksi näiden lataamista tiedostoista, selaamista sivuista ja käyttämistä reiteistä erilaisina tilastoina ja kaavioina. Ohjelmasta on tarjolla kolme eri maksullista versiota, Standard, Professional ja Enterprise, ja näiden lisäksi vielä ilmainen versio, Lite. Ohjelman kieli on englanti.

Tärkeimpinä teknisinä ominaisuuksina WebLog Expert tukee Apachen ja IIS:n lokitiedostoja ja tunnistaa lokiformaatin automaattisesti. Lokit se lataa FTP:n tai HTTP:n kautta ja ne voi lähettää sähköpostilla eteenpäin. Tuotetut raportit ovat

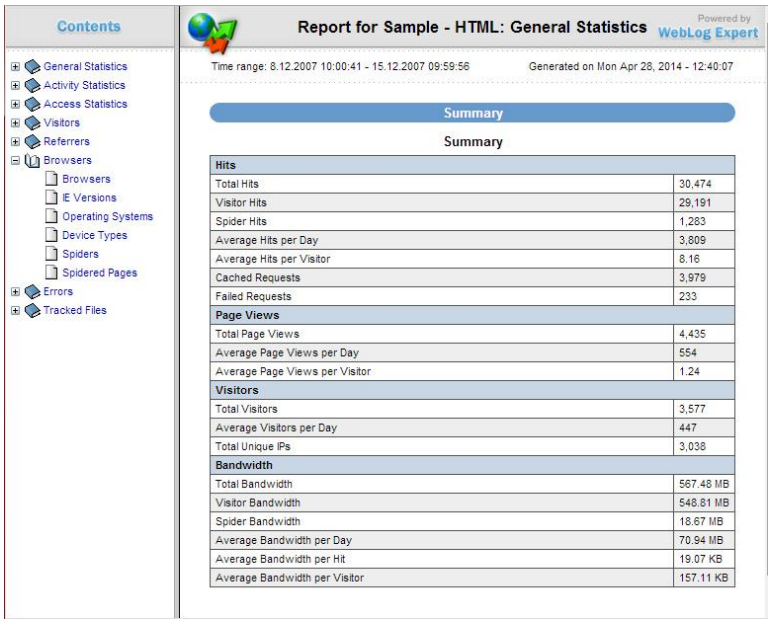
muotoa HTML, PDF tai CSV ja myös pakattuja tiedostoja voidaan lukea (CZ tai ZIP). Lisäksi ohjelma sisältää sisäänrakennetun web-palvelimen.

WebLog Expertin Internet-sivuilla on mahdollista ladata ilmainen 30 päivän testiversio Standard/Professional/Enterprise-ohjelmasta, joista olen tähän esittelyyn valinnut Professional-version. Kun avaan ohjelman, eteen ilmestyy hyvin helppokäyttöisen näköinen ikkuna, jossa on muutamia esimerkkiprofiileja valmiina tutkittavaksi (kuva 7). Valittavanani on lisäksi kolme toimintoa: uuden profiilin rakentaminen, asetusten muokkaaminen sekä ajoitettujen tehtävien luominen.



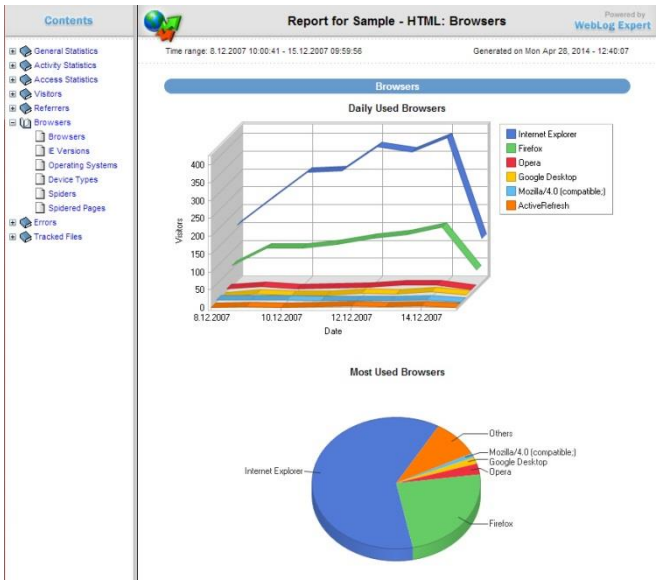
Kuva 7. WebLog Expertin aloitusikkuna.

Otan ensimmäiseksi tarkasteluun esimerkkiraportit. Tarjolla on sekä HTML, PDF ja Web Server –versiot, joissa kaikissa on samat tiedot. Valitsen HTML:n ja raportti avautuu selaimeen. Kuvassa 8 näkyy raportin etusivu, jossa on esitetty kerättyjen tietojen ajankohta, raportin luomisen aika sekä web-palvelimen yleisimpiä tilastoja yhteenvetona.



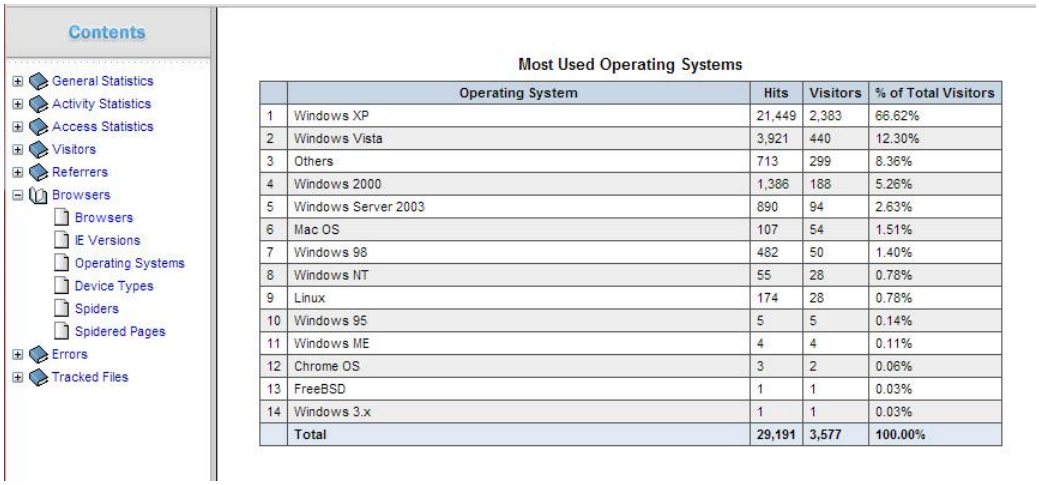
Kuva 8. Raportin etusivu.

Vasemmalla on puu, josta löydän lisätietoja sivuston aktiivisuudesta, käytetyistä materiaaleista, käyttäjistä, sivustolle viittaavista lähteistä, käyttäjien selaimista, sivuston virheistä sekä erityisseurannassa olevista tiedostoista. Olen esimerkin vuoksi avannut Browsers-kohdan jonka alta löytyy lisätietoja kaavioina (kuva 9).



Kuva 9. Selaintiedot kaavioina.

Samat tiedot näkyvät sivulla myös taulukkomuodossa (kuva 10). Samanlaisia kaavio ja taulukko -yhdistelmiä löytyy kaikista kohdista. Tieto on siis helposti hahmotettavissa ja ymmärrettävässä muodossa, kuten analysointiohjelmassa kuuluukin olla.

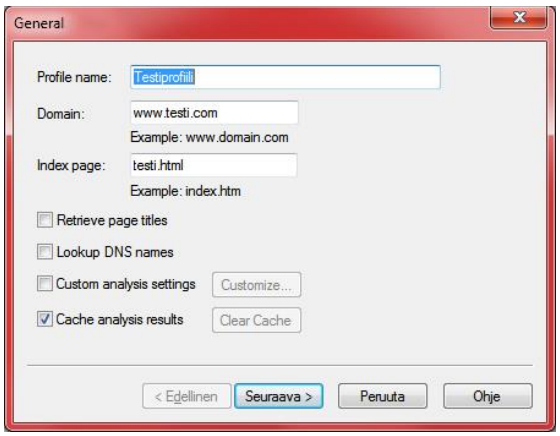


Most Used Operating Systems

	Operating System	Hits	Visitors	% of Total Visitors
1	Windows XP	21,449	2,383	66.62%
2	Windows Vista	3,921	440	12.30%
3	Others	713	299	8.36%
4	Windows 2000	1,386	188	5.26%
5	Windows Server 2003	890	94	2.63%
6	Mac OS	107	54	1.51%
7	Windows 98	482	50	1.40%
8	Windows NT	55	28	0.78%
9	Linux	174	28	0.78%
10	Windows 95	5	5	0.14%
11	Windows ME	4	4	0.11%
12	Chrome OS	3	2	0.06%
13	FreeBSD	1	1	0.03%
14	Windows 3.x	1	1	0.03%
	Total	**29,191**	**3,577**	**100.00%**

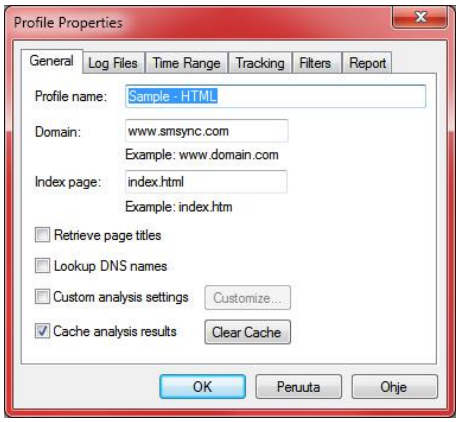
Kuva 10. Käytetyimmät selaimet taulukkona.

Raportit tehdään profiilien mukaan ja niitä voi luoda, muokata ja poistaa ohjelman aloitusikkunassa. Profiilin rakentaminen aloitetaan valitsemalla New, minkä jälkeen ohjelma ohjaa käyttäjän uuden profiilin luomisen läpi. Tässä vaiheessa valitsen uuden profiilin toimialueen ja sivuston etusivun (kuva 11), lokien sijainnin ja formaatin, miltä ajanjaksolta lokia kerätään, mahdolliset erityistarkkailtavat tiedostot ja suodattimet sekä raporttien sijainnin ja formaatin.



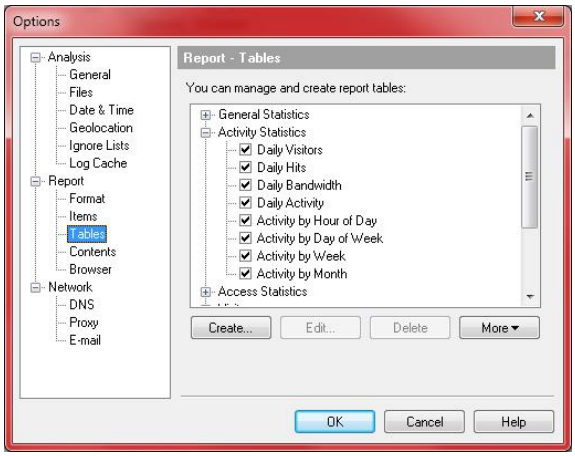
Kuva 11. Uuden profiilin luominen.

Näitä kaikkia voin kuitenkin myöhemmin muokata klikkaamalla profiilia listasta ja sen jälkeen valitsemalla Edit. Muokkausvalikossa on valittavinani täsmälleen samat asiat kuin luontivalikossakin eli yleiset, lokien yksityiskohdat, ajankohta, erityishuomiota vaativat tiedostot, suodattimet ja raporttien tiedot (kuva 12). Profiilin voi myös poistaa aloitusikkunan Delete-kohdasta.



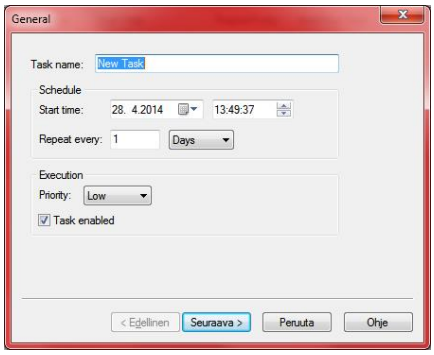
Kuva 12. Profiilien muokkaus.

Profiilien lisäksi myös ohjelmassa itsessään on muokkausvaraa Options-valikossa. Siellä voin hioa analysoinnin yksityiskohtia, esimerkiksi analysoitavia tiedostomuotoja, raporttien tietoja sekä verkkoasetuksia kuten välityspalvelimia. Kuvassa 13 olen esimerkkinä avannut Report-valikon alta Tables-vaihtoehdon, josta voin muokata raportissa näkyviä tietoja.



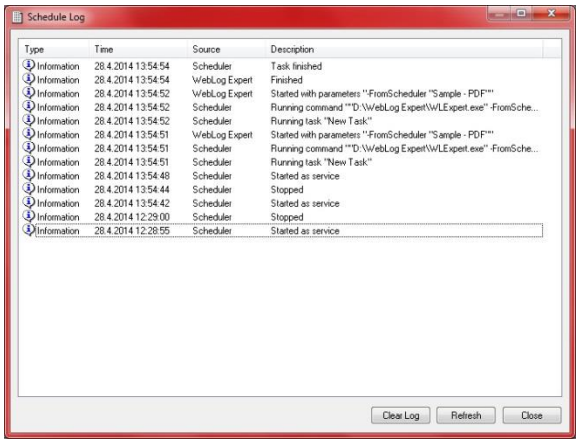
Kuva 13. Ohjelman asetukset.

Viimeisenä toimintona ohjelmassa on aikataulujen luonti, jossa voin asettaa profiileille analysointiajankohdat. Näitä ajankohtia kutsutaan tehtäviksi ja voin hallinnoida niitä aloitusikkunan kohdasta Schedule. Ohjelmassa ei ole valmiina yhtään esimerkkitehtävää, mutta voin luoda niitä yhtä yksinkertaisesti kuin profiilejakin: määritän tehtävälle nimen, kellonajan, kuinka usein tehtävä toistetaan, prioriteetin, profiilin, jolle tehtävä asetetaan, sekä mahdolliset ennen ja/tai jälkeen tehtävän suoritettavat komennot. Kuvassa 14 on aloitettu tehtävän luominen.



Kuva 14. Tehtävän luonti.

Kuten profiilejakin, voin muokata ja poistaa myös tehtäviä. Tämän lisäksi Aikataulu-ikkunasta löytyy mahdollisuus suorittaa jokin tehtävä juuri nyt, loki tehtävien toiminnalle (kuva 15) sekä asetukset, josta voin määrittää, millä käyttäjällä tehtävät ajetaan, jos ei paikallisella.



Kuva 15. Tehtävien loki.

4.2 IDS – Cyberarms Intrusion Detection and Defence System (IDDS)

Cyberarms on yhdysvaltalainen tietoturvayhtiö, jonka pääpaikka sijaitsee Kaliforniassa. Sen ainoa tuote on Intrusion Detection and Defence System (IDDS), joka on monikäyttöinen tunkeutujan havaitsemisjärjestelmä Windowsille. IDS-ominaisuuksiensa lisäksi se osaa suojata myös Exchangea, Sharepoint- ja SQL-palvelimia sekä etätyöpöytä- ja terminaalipalveluita.

IDDS käyttää Windowsin omaa Tapahtumienvalvontaa uhkien tarkkailuun ja konfiguroi myös Windowsin omaa palomuuria puolustautumaan dynaamisesti. Myös käyttäjä voi muokata ohjelmistoa suojaamaan kohteita mielensä mukaan ja päättämään millaisten uhkien takia ja miten ohjelma reagoi sekä määrittelemään luotetut verkot, joista hälytyksiä ei tule. Ohjelma on hyvin kevyt eikä vaikuta juurikaan järjestelmän suorituskykyyn.

IDDS:stä on saatavilla maksullisen version lisäksi myös riisuttu ilmaisversio, jota olen tässä esittelyssä käyttänyt. Ilmaisversio eroaa maksullisesta siinä, ettei se tuota lainkaan raportteja ja kykenee suojaamaan vain viideltä hyökkäykseltä päivässä (Taulukko 1). Yrityskäyttöön ilmaisversio ei siis sovi, mutta testaukseen kyllä.

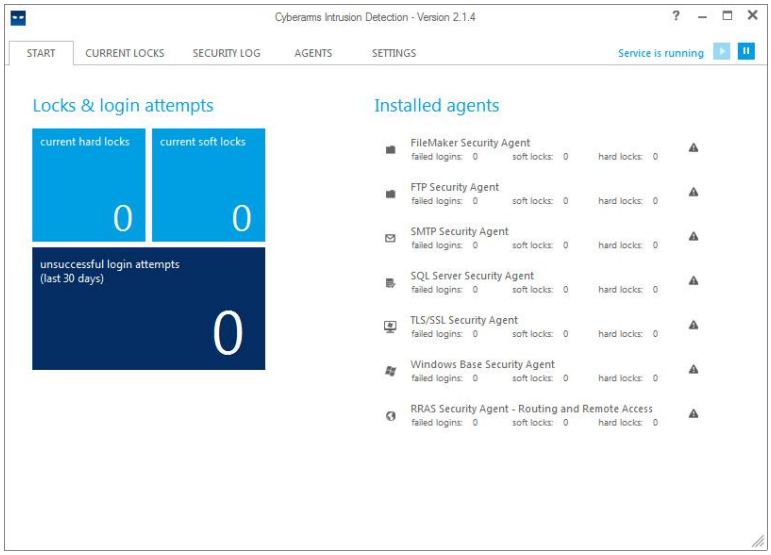
Taulukko 1. Versioiden vertailu.

	FREE edition	PRO edition
Unlimited monitoring for intrusions, logging	Yes	Yes
Security Agent support	Yes	Yes
- FTP Security Agent	Yes	Yes
- SMTP Security Agent	Yes	Yes
- SQL Server Security Agent	Yes	Yes
- TLS/SSL Security Agent (Remote Desktop using high encryption and TLS/SSL for transport)	Yes	Yes
- Windows Base Security Agent (monitors for invalid login using Windows authentication)	Yes	Yes
Custom Security Agent support	Yes	Yes
Custom lock out policy per Security Agent	Yes	Yes
Notification of administrator (on soft lock, hard lock, unlock)	Yes	Yes
Reports	None	Daily, Weekly, Monthly
Restrictions	defends max. five attacks per day	-
Software expires or has to be updated	No expiration	No expiration
Price	FREE	USD 199,-/EUR 149 excl. tax, licensing per server

Ohjelman asennus on helppoa. Cyberarmsin verkkosivuilta löytyy ladattavaksi pakattu zip-tiedosto, joka sisältää asennusohjelman. Ainoana vaatimuksena

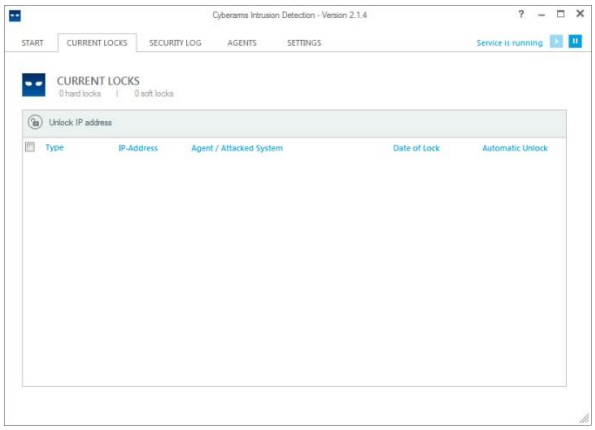
ohjelmalle on Windowsin palomuuri, jonka täytyy olla asennettu ja toiminnassa. Varsinaisen IDDS:n lisäksi asennusohjelma asentaa Microsoft .NET Framework 4.0:n, mikäli tätä ei ole jo asennettu. Asennuksen yhteydessä luodaan myös Cyberarms Intrusion Detection Service -palvelu.

Ohjelman käyttöliittymä on ulkoasultaan Windows 8:n tyylinen ja vaikuttaa ensikatsauksella hyvin yksinkertaiselta (kuva 16). Etusivulla näen yhteenvetona isoissa laatikoissa tärkeimmät tilastot, eli kaikki lukitut IP-osoitteet ja epäonnistuneet kirjautumisyritykset viimeisen kuukauden ajalta ja vieressä epäonnistuneiden kirjautumisten sekä pehmeiden ja kovien lukkojen määrät ohjelman eri osissa. Oikeasta yläkulmasta näen palvelun tilan (päällä/pois) ja voin käynnistää tai sulkea helposti.



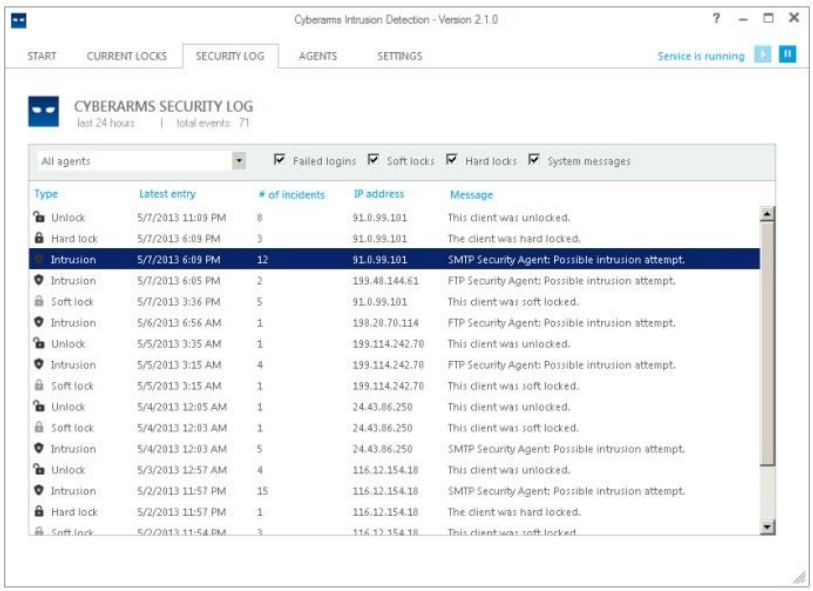
Kuva 16. Cyberarms IDDS:n aloitusikkuna.

Välilehdistä löydän lisää tilastoja ja toimintoja. Current Locks -lehdellä näkyy tällä hetkellä lukitut IP-osoitteet ja niiden lisätietoja (kuva 17). Yläreunan Unlock IP Address -kohdasta voi vapauttaa osoitteita, mikäli ohjelma on esimerkiksi estänyt jonkin turvalliseksi tunnetun osoitteen.



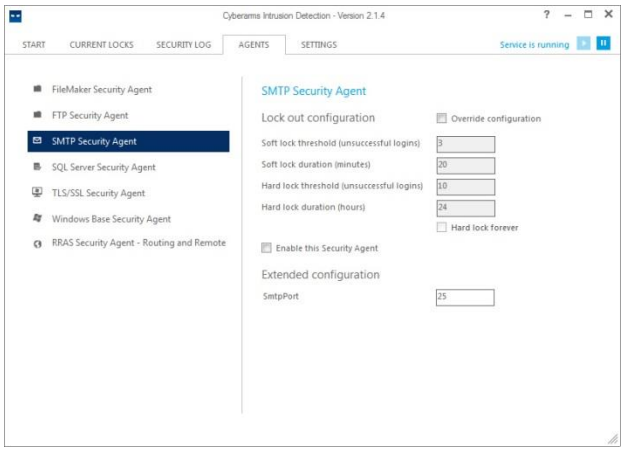
Kuva 17. Current Locks -välilehti.

Security Log -välilehdellä on ohjelman loki, joka pitää kirjaa ohjelman toiminnoista, esimerkiksi hyökkäyksistä, viimeisen vuorokauden ajalta (kuva 18). Olen esimerkiksi korostanut Intrusion-tapahtumaa. Kyseisestä tietueesta näen tapahtuman kellonajan, montako tapahtumia on ollut, mistä osoitteesta ne ovat tulleet ja tarkemman kuvauksen tapahtumasta, tässä tapauksessa ohjelman SMTP-osa on havainnut mahdollisia tunkeutumisyrityksiä. Voin myös etsiä lokista tietoja hakukriteerein, esimerkiksi ohjelman jonkin tietyn osan tuottamat tiedot tai tietyt tapahtumat.



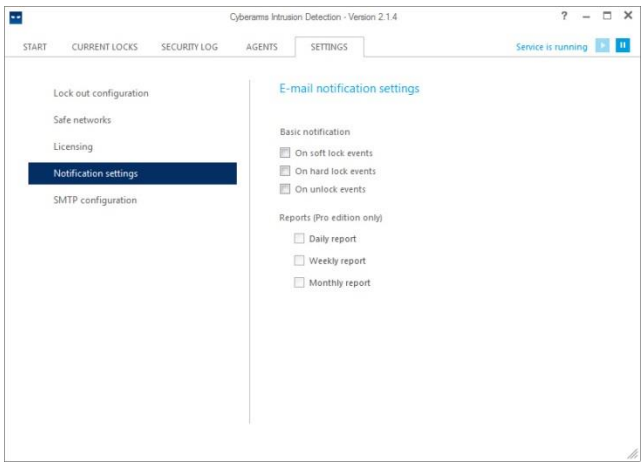
Kuva 18. IDDS:n loki. (Kuva: Cyberarms, 2014.)

Voin hallinnoida ohjelman eri lisäosien toimintaa Agents-välilehdellä(kuva 19). Asetukset ovat kaikille osille samat: käyttöönotto, perusteet pehmeälle tai kovalle lukolle (pehmeä lukko toimii varoituksena ja estää IP-osoitteen vähäksi aikaa, kova lukitus estää pidemmäksi aikaa, mikäli turvallisuusloukkauksia ilmenee vielä pehmeän lukituksen jälkeen) lukituksen kesto ja muutamalle osalle portin numero.



Kuva 19. Agenttien hallinta.

Viimeinen välilehti on asetuksille, josta voin hallinnoida yleisiä lukitsemisasetuksia (samanlaiset kuin ohjelman osille), turvallisia (sallittuja) verkkoja, lisenssiä, sähköpostihälytyksiä (kuva 20) sekä SMTP:n asetuksia. Myös asetukset ovat yksinkertaisia ja helppoja ymmärtää ja muokata.

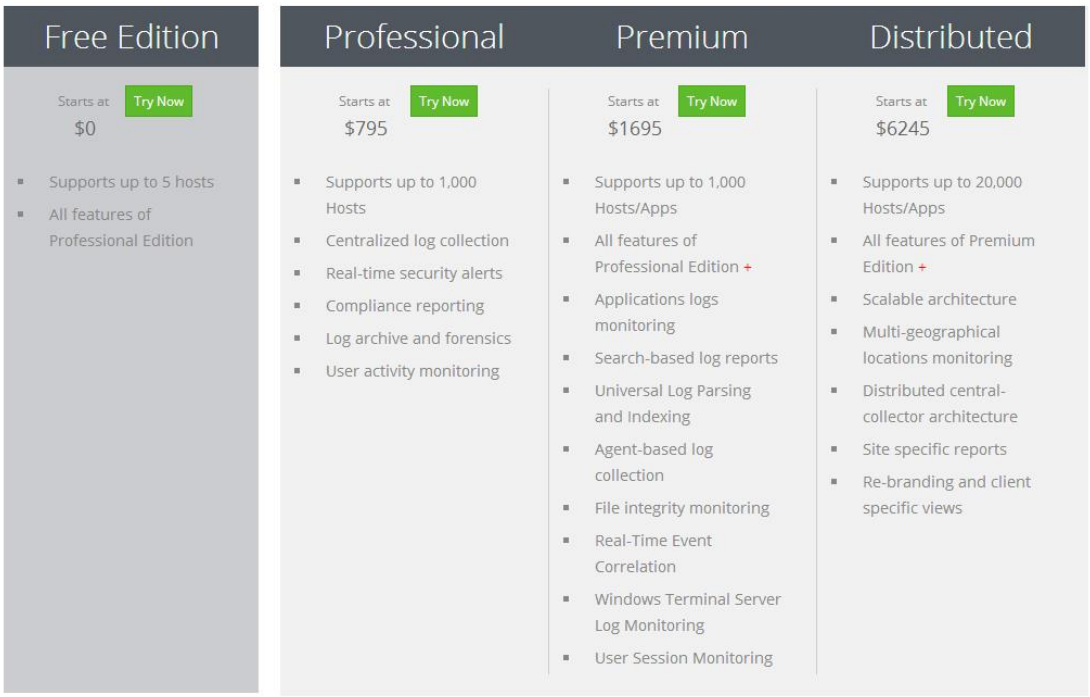


Kuva 20. Sähköpostihälytysten asetukset.

4.3 SIEM – ManageEngine EventLog Analyzer

ManageEngine on Yhdysvaltalainen IT-yritys, joka on perustettu 1996. Se kuuluu Zoho Corporationiin ja sen tuotteilla on yli miljoona käyttäjää ympäri maailman. Heidän SIEM-ohjelmistonsa nimi on EventLog Analyzer ja sillä väitetään olevan markkinoiden paras hinta-laatusuhde.

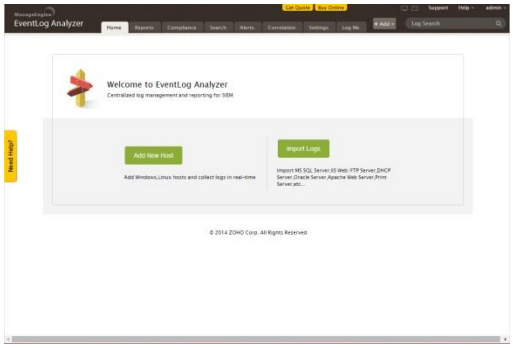
EventLog Analyzerin tärkeimpiin ominaisuuksiin kuuluvat reaaliaikaiset tapahtumien vertailut ja hälytykset, sääntöjen noudattamisesta tehdyt raportit, lokien kerääminen kaikista verkon laitteista (palomuurit, reitittimet, myös Linux-laitteet), tiedostojen ja käyttäjien valvonta sekä lokien arkistointi ja selaaminen. Ohjelmalla on neljä eri versiota, Free, Professional, Premium ja Distributed, jotka eroavat toisistaan toiminnallisuudeltaan ja hinnaltaan (kuva 21).



Kuva 21. Versioiden vertailu. (Kuva ManageEngine, 2014.)

Tässä vertailussa olen käyttänyt Premium/Professional -versiota, jonka 30 päivän kokeiluversio on ladattavissa ManageEnginen sivuilta. Kokeiluversio muuttuu automaattisesti Free-versioksi kokeiluajan kuluttua. Myös Distributed-versiosta löytyy kokeilumahdollisuus.

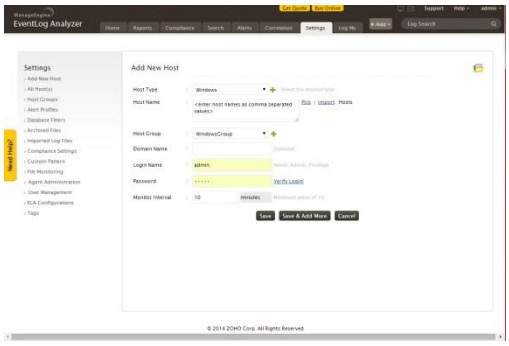
Voin valita asennuksen suoritettavaksi automaattisesti tai manuaalisesti. ManageEnginen verkkosivuilta löytyy helposti ymmärrettävä Quick Start -opas, jossa asennus ja ohjelman käyttöönotto käydään läpi askel askeleelta. Ohjelman voi asentaa palveluna tai sovelluksena, joista olen tässä käyttänyt ensimmäistä tapaa. Asennuksen jälkeen voin hallinnoida ohjelmaa verkkoselaimen kautta (kuva 19).



Kuva 22. EventLog Analyzerin etusivu.

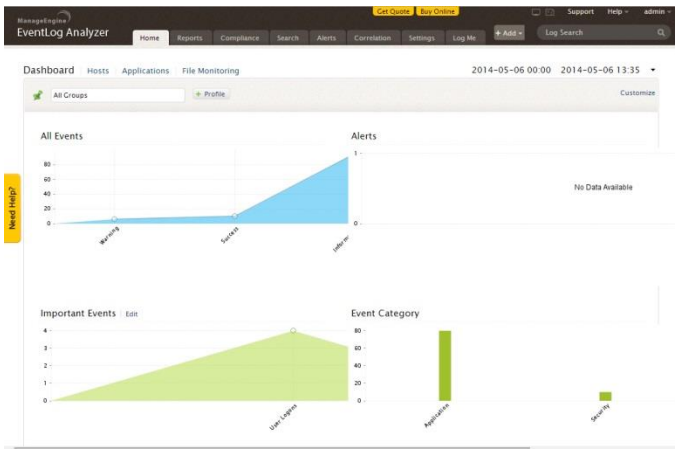
Selainkäyttöliittymä tukee Internet Exploreria, Firefoxia ja Chromea. Asennuksen jälkeen törmäsin kuitenkin ensimmäiseen ongelmaan: jos selainhallinnoinnin yrittää avata automaattisesti asennuksen jälkeen, se aukeaa Internet Exploreriin vanhana versiona (EventLog Analyzer 8) ja jää jumiin lataukseen. Hallintaikkuna täytyy siis avata käsin kirjoittamalla selaimeen http://<hostname> :8400, missä <hostname> on sen isännän nimi, jolle EventLog Analyzer on asennettu.

Ensimmäiseksi lisään ohjelmaan valvottavia laitteita toimialueelta, mikä onnistuu heti etusivulta Add New Host -napista. Myös tähän löytyy askel askeleelta etenevät ohjeet Quick Start -oppaasta. Laitteiden lisääminen tapahtuu helposti lomakkeella (kuva 23) ja niitä voi lisätä useita kerralla. EventLog Analyzerin voi asentaa myös UNIX-isännälle, mutta tällöin tarvitaan kolmannen osapuolen ohjelma konvertoimaan Windowsin lokit syslog-muotoon.



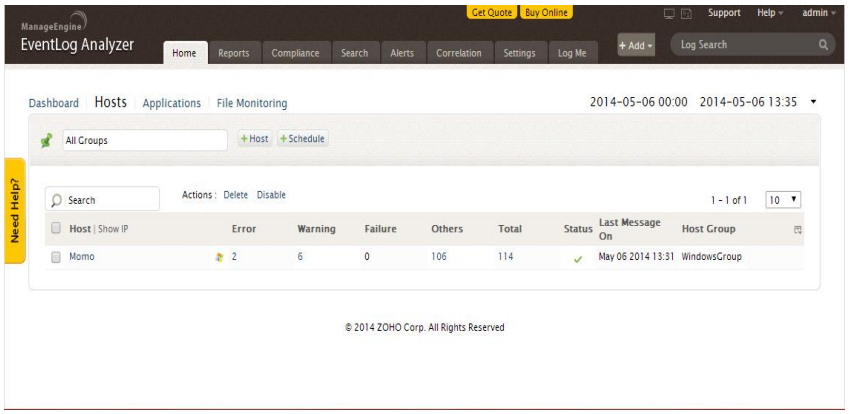
Kuva 23. Valvottavien laitteiden lisääminen.

Kun olen lisännyt laitteen onnistuneesti tarkkailtavien listalle, hallintasivun etusivu muuttuu näyttämään erilaisia tilastoja, kuten esimerkiksi hälytyksiä ja tapahtumien kategorioita, erilaisina kaavioina (kuva 24). Voin muokata näkymää mieleisekseni oikean ylänurkan Customize-valikosta. Etusivulle on ilmestynyt nyt myös välilehtiä, (Hosts, Applications, File Monitoring).



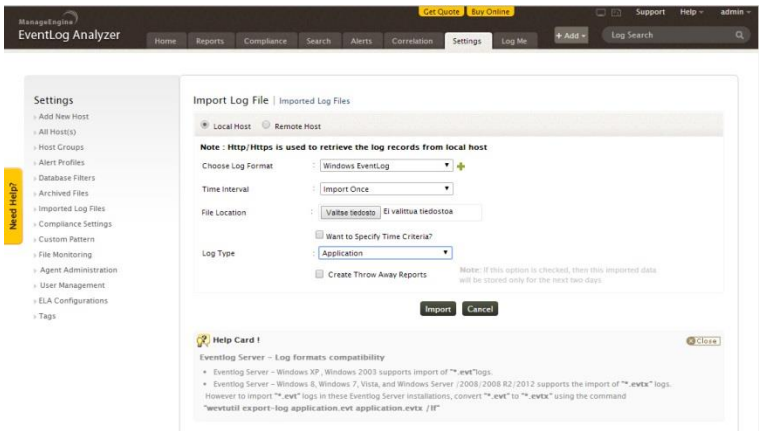
Kuva 24. Kaavioita EventLog Analyzerin etusivulla.

Hosts-välilehdeltä näkyy lisäämäni isännän lokitietoja tilastona. Kuvasta 25 näkyy, että ohjelma on alkanut onnistuneesti laskemaan koneeni antamia virheitä, varoituksia yms. Sivulla voin myös lisätä tai poistaa laitteita tai aikatauluja raporteille ja etsiä isäntiä nimen tai IP-osoitteen perusteella, mikä on isommassa verkossa erittäin hyödyllinen toiminto. Isännän nimeä klikkaamalla saan auki isäntäkohtaisen tapahtumaraportin.



Kuva 25. Hosts-välilehti.

Applications-lehdellä voin lisätä ohjelmaan Windowsin lisäksi myös muiden ohjelmien lokitiedostoja joko paikalliselta isännältä tai etänä (kuva 26). Tuetut tiedostopäätteet ovat .evt ja .evtx. Lokitiedostolle voi antaa tyypin (esim. Application, Security, System yms.) ja siitä voi tehdä halutessaan myös kertakäyttöisen, eli sitä säilötään vain kaksi päivää. Sovelluslokien lisäämisen jälkeen voin tarkastella niitä Imported Log Files -kohdasta. Viimeinen välilehti, eli File Monitoring, on tarkoitettu isäntien tiedostojen tarkkailuun ja siellä voin lisätä halutut laitteet ja tiedostopolut, joiden muokkauksista ja käytöstä pidetään kirjaa.



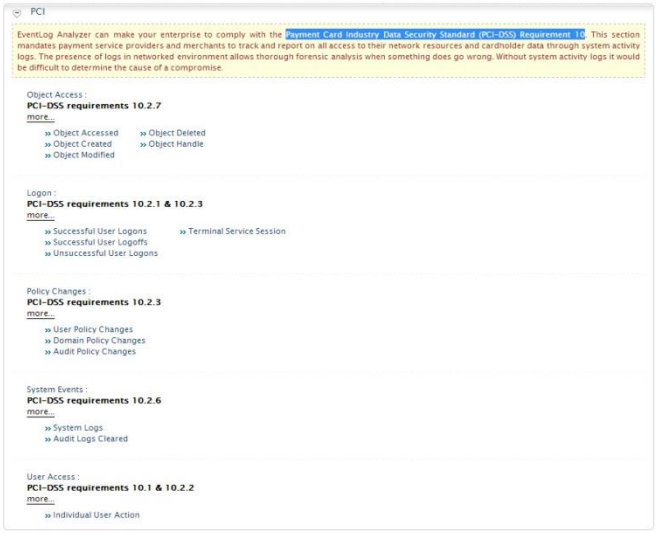
Kuva 26. Sovelluslokien lisääminen.

Etusivun lisäksi ohjelmassa on paljon muitakin välilehtiä ja toimintoja. Reports-lehdellä voin tarkastella ohjelman luomia tai tehdä omia, kustomoituja raportteja. Ohjelman luomia on paljon mistä valita: sivulta löytyy raportteja muun muassa eniten sisäänkirjautumisia keränneistä isännistä, eniten sisäänkirjautuneista

käyttäjistä ja siitä, mihin aikaan tapahtuu eniten tapahtumia (esim. varoitukset tai virheet) toimistoaikojen sisällä ja niiden ulkopuolella tunneittain (kuva 27).

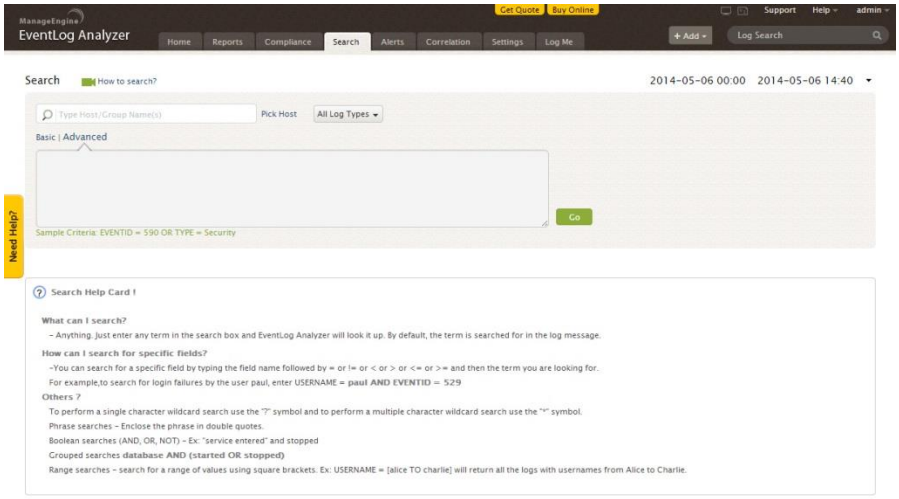
Kuva 27. Esimerkkiraportti EventLog Analyzeristä.

Compliance-välilehdellä on valmiiksi koottuja tietokokonaisuuksia esimerkiksi käytetyistä objekteista ja käyttäjien toiminnasta. Oletuksena välilehti sisältää yhdysvaltalaisia lakien tai ohjeistusten mukaisia valmiita paketteja, mutta sivulla voin luoda myös oman kokonaisuuden. Kuvassa 28 on esimerkkinä Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10:n mukainen setti tietoja.



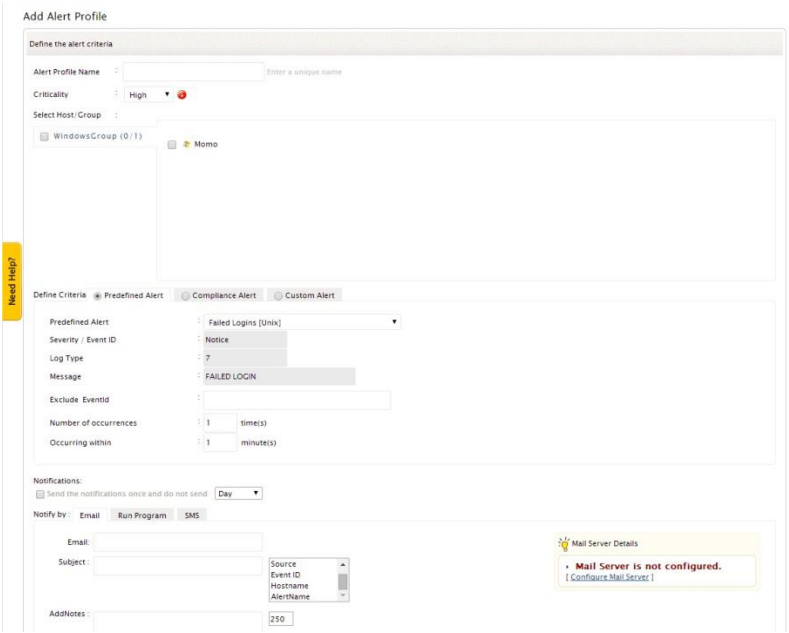
Kuva 28. Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10:n mukaiset tiedot.

Search-välilehdellä kaikista ohjelman sisältämistä tiedoista voi tehdä hakuja, mikä on lähes välttämättömyys tämänkaltaiselle ohjelmalle (kuva 29). Haun voi suorittaa joko jollekin isännälle tai ryhmälle tai sitten kaikkialta ohjelmasta ja myös halutun lokityypin (esim. Windows Event Log, syslog yms.) voi määrittää. Lisäksi löytyy myös Advanced-haku, jossa hakukriteereitään voi esittää vielä tarkemmin. Yksinkertaistettu hakutoiminto löytyy myös ohjelman oikeasta ylänurkasta.



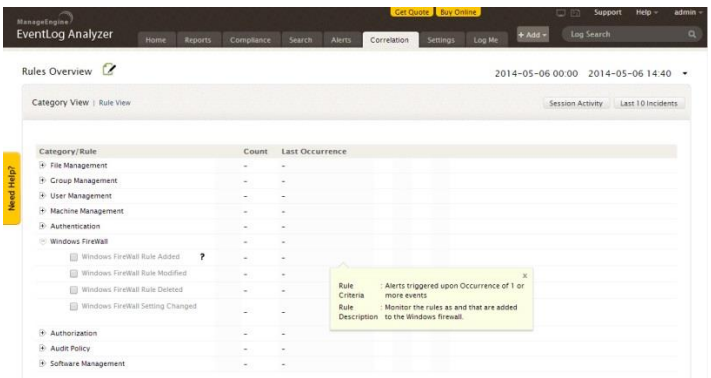
Kuva 29. Search-välilehti.

Alerts-välilehdellä voin hallinnoida hälytysprofiileja. Hälytysprofiili määrittelee sen, miten, miksi ja kuka hälytetään. Valmiita profiileja välilehdellä ei ole, vaan ne täytyy luoda itse (kuva 30). Profiilin luonnissa sille annetaan nimi, kriittisyysaste (High, Medium, Low), valitaan laite, johon profiilia sovelletaan, määritellään hälytyskriteerit joko ohjelman valmiista ehdotuksista tai oman valinnan mukaan ja lopuksi hälytyksen tapa (esim. sähköposti) ja vastaanottaja. Sivulta voin konfiguroida myös oman sähköpostipalvelimen, mikäli sille on tarvetta.



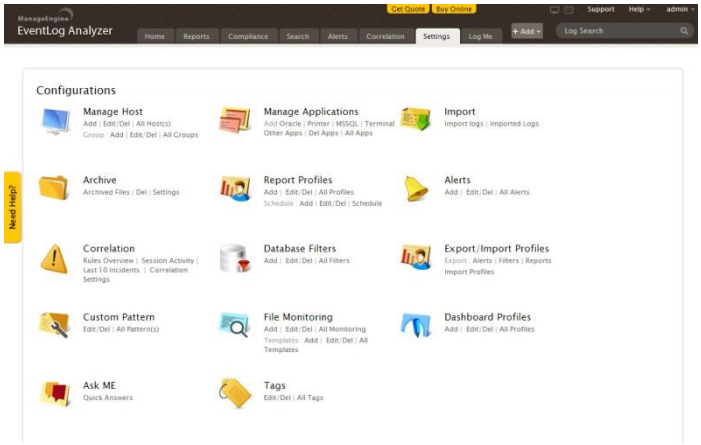
Kuva 30. Hälytysprofiilin luonti.

Correlations-välilehdellä on ohjelman varsinainen SEM-osio. Lehdellä on erilaisia sääntöjä, joita voin ottaa tai poistaa käytöstä. Säännöt on ryhmitelty omiin kategorioihinsa (esimerkiksi User Management tai Authentication) ja kukin sääntö käyttöön otettuna aiheuttaa hälytyksen, kun säännön määrittelemä ehto täyttyy. Kuvassa 31 on esimerkki Windows Firewall -kategorian sisältämistä säännöistä. Rule Added -sääntö siis aiheuttaa hälytyksen joka kerta, kun Windowsin palomuuriin lisätään uusia sääntöjä. Ohjelman sääntöjä en voi itse luoda tai poistaa, mutta välilehden kautta niistä voi lähettää palautetta suoraan ohjelman tekijöille.



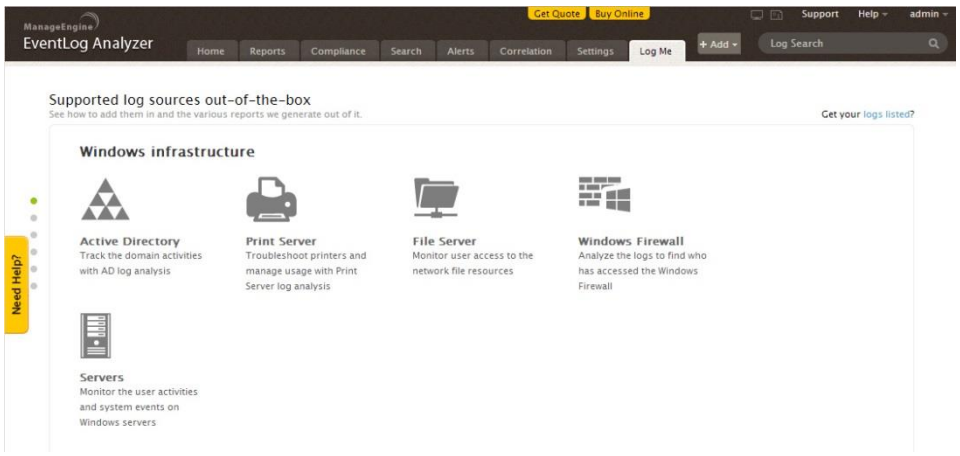
Kuva 31. Windows Firewall -sääntökategoria.

Settings-välilehdellä ovat ohjelman asetukset lajiteltuina ja kuvitettuina. Lehdeltä löytyvät kaikki edellä mainitut konfigurointimahdollisuudet ja paljon muita, sekä tavanomaisia administraattorin työkaluja, kuten esimerkiksi käyttäjäasetuksia ja järjestelmäasetuksia. Kuvassa 32 on näkymä välilehden konfiguraatioasetuksista.



Kuva 32. Settings-välilehti.

Viimeinen välilehti on Log Me, jolle on kasattu ohjeet eri laitteiden tai käyttöjärjestelmien lokien lisäämiseksi ohjelmaan. Kun jonkin laitteen tai järjestelmän ikonia klikkaa, vie ohjelma ManageEnginen verkkosivuilla sijaitsevaan lokinlisäämisohjeeseen. Ohjelma ei siis varsinaisesti sisällä ohjeita, mutta on kasannut ne helposti löydettäviksi. Kuvassa 33 on esimerkkinä Windows-infrastruktuurin eri osille tarkoitetut ikonit.



Kuva 33. Log Me -välilehti.

Välilehtien lisäksi ohjelmassa on myös pienempiä toimintoja, jotka helpottavat administraattorin työtä. Oikeasta ylänurkasta löytyy Add-alasvetovalikko, josta voin lisätä pikavalintana esimerkiksi isäntiä tai hälytysprofiileja. Vasemmasta reunasta taas löytyy Need Help? -laatikko, jota klikkaamalla voin lähettää kysymyksen suoraan ohjelman tekijöille. Oikeassa ylänurkassa on myös Support-valikko, josta löytyy paljon tukitoimintoja ja -linkkejä.

4.4 Ohjelmien arviointi

WebLog Expert on hyvä esimerkki kevyestä ja helppokäyttöisestä lokien analysointiohjelmasta. Käyttöliittymässä ei ole kovin paljon toimintoja tai konfiguroinnin tarvetta, joten käyttöönotto on yksinkertaista ja käytön oppii nopeasti. Ohjelmassa on lisäksi sisäänrakennettuna hyvät ja yksinkertaiset ohjeet, jotka lähtevät aivan alkeista, joten aloittelijakin pääsee kärryille. Hintakaan ei ole pahimmasta päästä, joten tätä voisi hyvillä mielin suositella pk-yrityksille.

- Ohjelma toimii Apache ja IIS -verkkopalvelimilla ja kerää verkkotietoja näillä sijaitsevista nettisivuista
- Enterprise-versio maksaa 399,00 USD, Professional 199,00 USD ja Standard 99,00 USD

Cyberarms IDDS sopii, ainakin näin ilmaisversion perusteella, pk-yrityksille. Käyttöliittymä on yksinkertainen ja helposti opittavissa ja ohjelma suojaa monipuolisesti yritysverkkojen yleisimpiä osia. Huonoina puolina voisi mainita tiukan sidoksen Windowsiin ja sen, että kaikki ohjelman osat täytyy ottaa erikseen käyttöön, mitä käyttäjä ei välttämättä heti ensi alkuun tajua. Ohjelman hinta on myös ihan kohtuullinen ja pienellekin yritykselle saavutettavissa.

- Ohjelma toimii Microsoft Windowsilla ja suojaa FTP- ja SMTP-yhteyksiä, Microsoft Exchange Outlook Web Access -portaalia, Microsoft Office Sharepoint ja SQL -palvelimia sekä Remote Desktop -etäyhteyttä

- Professional-versio maksaa 149€, myös asiakkaan toiveiden mukaan räätälöity lisenssi mahdollinen

EventLog Analyzer vaikuttaa päälisin puolin oikein hyvältä ohjelmalta suuremmille yrityksille. Ohjelma vaatii kuitenkin vähän paneutumista ja paljon tietoa tietoturvasta ja yritysverkoista, joten käyttö on jätettävä ammattilaiselle. Suurimmalla lisenssillä on mahdollista lisätä ohjelmaan jopa 5000 laitetta, pienimmällä taas 25. Myös hintansa puolesta ohjelma on selkeästi suunnattu suuremmille yrityksille.

- Todella monipuolinen työkalu, joka sisältää kaikki yleisimmät lokien tuottajat
- Hinta määräytyy version ja laitteiden määrän mukaan: Premium-versio 1,695-9,495 USD, Professional-versio 795-5,995 USD ja Distributed-versio 6,245-29,995 USD

5 Lokitietojen käyttö eräissä Joensuun alueen yrityksissä

Tutkimuksen tarkoituksena oli selvittää, miten lokitietojen kerääminen, hallitseminen ja käyttö on hoidettu eräissä Joensuun yrityksissä. Tutkimuksessa haluttiin kartoittaa

1) Millaisiksi järjestelmänvalvojat arvioivat oman osaamisensa?
2) Miten lokitietojen kerääminen ja hallinta on yrityksessä toteutettu?
3) Millaisena järjestelmänvalvojat kokivat lokitietojen keräämisen ja hallinnan omassa yrityksessään?
4) Onko lokitietoja käytetty häiriötilanteessa ja onko niistä ollut apua järjestelmänvalvojalle?

5.1 Kyselyn järjestäminen

Kysely pidettiin kvantitatiivisena, sillä tarkoitus oli saada mahdollisimman yleispätevää tietoa, ja toteutettiin Googlen Drive -palvelulla (liite 1). Yrityksille kysely lähetettiin linkkinä sähköpostin mukana (liite 2). Kysely sisälsi pääasiassa valinta- ja monivalintakysymyksiä ja lopuksi yhden vapaan sanan laatikon. Osa kysymyksistä oli pakollisia.

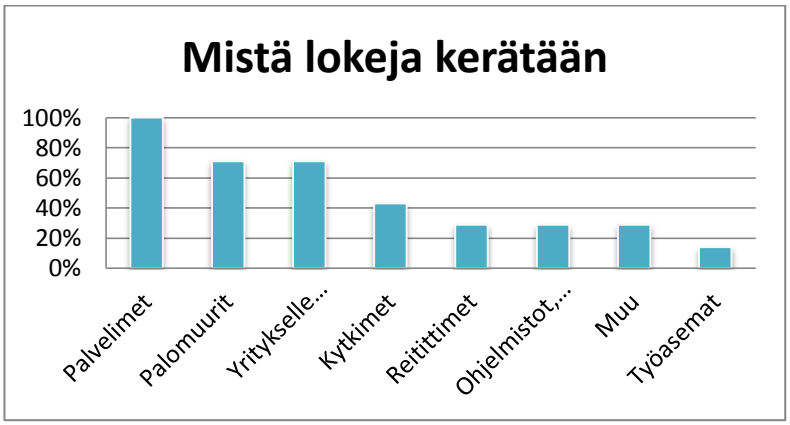
Kohderyhmänä olivat sellaiset joensuulaiset yritykset, joilla tiedetysti tai mahdollisesti on itse hallinnoitu ICT-verkko. Yritysten valinta suoritettiin yrityshakemiston perusteella ja painottui tietotekniikka-alalle. Yhteensä kohdeyrityksiä valittiin 36 ja vastauksia saatiin 7. Kysely oli virallisesti auki kolme viikkoa ja välissä yrityksille lähetettiin yksi muistutusviesti.

5.2 Kyselyn tulokset

Yritysten koko jaettiin Tilastokeskuksen tapaan kolmeen luokkaan työntekijöiden perusteella, pieni (1-50 henkeä), keskisuuri (51-250 henkeä) ja suuri (yli 250 henkeä). Suurin osa vastanneista oli pienistä yrityksistä (4 vastausta), yksi keskisuuresta ja kaksi vastaajaa suuresta yrityksestä. Verkon pääasiallinen käyttöjärjestelmä oli suurimmalla osalla Windows (5 vastausta), vähemmistönä Linux. Yhdenkään verkon pääasiallinen käyttöjärjestelmä ei ollut muu UNIX-järjestelmä tai muu näiden ulkopuolelta.

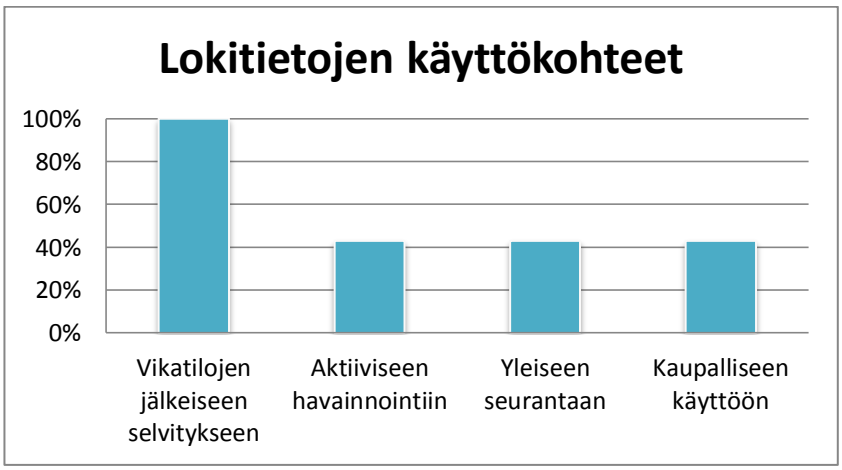
Suurimmalla osalla yrityksistä (4 vastausta) on erityinen tietoturvahenkilö tai -henkilöstöä ja lähes kaikissa yrityksissä on oma tietoturvasuunnitelma (6 vastausta), vain yksi vastaaja vastasi ”en osaa sanoa”. Kysymykseen omasta lokitietoihin liittyvästä tietotaidosta selkeästi suurin osa vastaajista vastasi ”tyydyttävä” (5 vastausta). Kukaan ei vastannut ”välttävä” tai ”ei tietotaitoa”. Kysyttäessä lokitietojen keräämisen ja analysoinnin tärkeydestä suurin osa vastasi ”Tärkeää” (4 vastausta). Kukaan ei vastannut ”Turhaa” (kuvio 6).

Kysyttäessä mistä yrityksissä kerätään lokitietoja, 7 vastasi palvelimista, 5 palomuureista, 5 yritykselle kriittisistä ohjelmista, 3 kytkimistä, 2 reitittimistä, 2 yritykselle ei-kriittisistä ohjelmista ja 1 työasemista (kuvio 1). Lisäksi tuli kaksi ”Muu” -vastausta, joista toisessa vastattiin lokeja kerättävän vierailijoista ja päätelaitteista, kuten puhelimista, ja toisessa yrityksen omista ohjelmista.



Kuvio 1. Mistä lokitietoja kerätään.

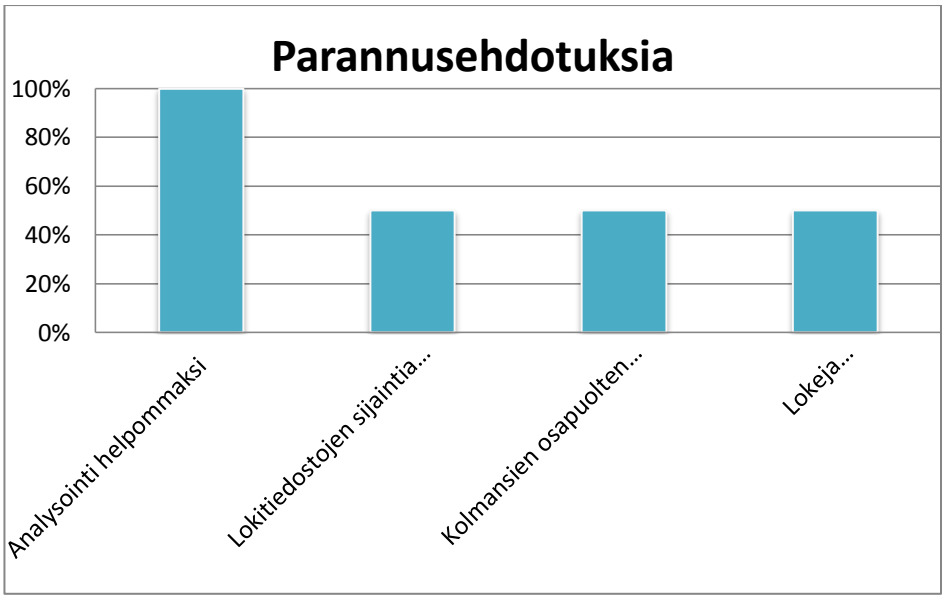
Yrityksistä 7:ssä lokitietoja käytetään vikatilojen/tietoturvaongelmien jälkeiseen vianselvitykseen, 3:ssa tietoturvauhkien aktiiviseen havainnointiin, 3:ssa verkon tilan yleiseen seurantaan ja ongelmien ennaltaehkäisyyn ja 3:ssa kaupalliseen käyttöön (kuvio 2). Yhdessäkään yrityksessä lokitietoja ei käytetty työnteon valvomiseen.



Kuvio 2. Lokitietojen käyttökohteet.

Lokien tarkastelun tiheys jakautui tasaisesti ”Useita kertoja päivässä”, ”Kerran viikossa” ja ”Harvemmin” -vaihtoehtojen välillä. Kukaan ei vastannut ”Kerran päivässä”, ”Kerran kuukaudessa”, ”Vain ongelmien ilmaantuessa”, ”Ei tarkkailla” tai ”En osaa sanoa”.

Vastaajista niukka enemmistö oli sitä mieltä, että lokitietojen hallinta ei ole hoidettu yrityksessä hyvin (4 vastausta). Niistä, jotka vastasivat edelliseen kohtaan ”Ei”, puolet ehdotti parannusehdotukseksi lokitiedostojen sijainnin keskittämistä, kolmansien osapuolten ohjelmien käyttöönottoa tai lokitietojen tiheämpää seuraamista (kuvio 11). Kaikki olivat myös sitä mieltä, että lokien analysointi pitäisi tehdä helpommaksi. Kukaan ei vastannut ”Henkilöstöä pitäisi kouluttaa lisää aiheeseen”, ”Lokitiedostojen tietoturvaa pitäisi parantaa” tai ”Lokitiedostoja pitäisi kerätä enemmän eri laitteista ja sovelluksista”.



Kuvio 3. Parannusehdotukset.

Kysymykseen ”Onko yrityksessänne/toimipaikassanne tapahtunut viimeisen viiden vuoden aikana ICT-verkon ongelmatilanteita kaikki vastaajat vastasivat ”Kyllä”. Jatkokysymykseen ”Kuinka suuri apu oli lokitietojen analysoinnista” suurin osa vastasi ”Vähäinen”. Yksi jätti kohdan tyhjäksi. Kukaan ei vastannut ”Ratkaiseva” tai ”Lokitietoja ei käytetty”. Lisäksi vapaan sanan kenttään oli saatu

yksi vastaus, jossa oli kommentoitu ”Yrityksenne verkon” olevan laaja käsite varsinkin yritykselle, joka tarjoaa verkkopalveluita. Parempi käsite olisi kuulemma ollut ”teidän tai asiakkaanne verkko”.

6 Johtopäätökset

Vastausten vähäisestä määrästä johtuen kyselystä ei saa laajaa, yleispätevää yhteenvetoa tehtyä, varsinkin kun esimerkiksi keskisuuria yrityksiä osallistui vain yksi. Lisäksi monissa vastauksissa kaikki vastaukset saivat tasaisesti ääniä, eikä esimerkiksi pienten tai suurten yrityksien yhteisiä trendejä ollut selkeästi näin pienessä otoksessa näkyvissä.

Joitain johtopäätöksiä voidaan kuitenkin tehdä asioista, joista kaikki tai lähes kaikki vastaajat olivat yhtä mieltä. Ensimmäiseksi kaikilla yrityksillä yhtä lukuun ottamatta oli varmasti tietoturvasuunnitelma, sellaisillakin, joilla varsinaista tietoturvahenkilöä/henkilöstöä ei ollut. Hyvä asia oli myös se, että kukaan ei pitänyt lokitietoja turhina.

Suurin osa vastaajista määritteli oman lokitieto-osaamisensa tyydyttäväksi, mutta kukaan vastaajista ei kaivannut henkilöstölle lisää koulutusta aiheeseen, vaikka lokitiedot koettiinkin pääasiassa tärkeiksi tai erittäin tärkeiksi. Vastaajat ovat siis tyytyväisiä oman tietotaitonsa tasoon lokiasioissa. Toki, koska taitotasot olivat kunkin vastaajan itse määriteltävissä, myös pientä oman osaamisen vähättelyä on voinut esiintyä.

Lokitietojen lähteistä kysyttäessä kaikki vastaajat kertoivat yrityksensä keräävän lokitietoja ainakin palvelimista. Palvelimien käyttöjärjestelmissä onkin usein automaattisesti päällä järjestelmän sisäinen lokiohjelma, joten tämä ei tullut yllätyksenä. Vastaajilta olisi lisäksi voinut kysyä, käyttävätkö he lisäksi jotain kolmannen osapuolen ohjelmaa, mikä on suositeltavaa. Oli myös hyvä asia, että palomuurit olivat heti palvelimien jälkeen seuraavaksi kerätyin lokilähde. Palomuurin vaikutus verkon toimintaan on kuitenkin niin suuri.

Lokien käyttötarkoituksissa yksi nousi ylitse muiden: ongelmatilanteiden jälkeinen vianselvitys. Tämä on yksi lokien peruskäyttötarkoituksista, joten hyvä että lokeja osataan näissä tilanteissa hyödyntää. Kukaan vastaajista ei vastannut kuitenkaan lokeja käytettävän työnteon seuraamiseen, esimerkiksi työntekijöiden verkkoselailun tarkasteluun. Kyseinen toiminta mielletäänkin monesti vähintään kyseenalaiseksi, joten, jos työntekijöiden toimia seurataankin, sitä tuskin kukaan haluaa myöntää.

Lokitietojen hallinnan parannusehdotuksia kysyttäessä esille nousi kaikkien mielestä sama ongelma: lokien analysointi on vaikeaa. Käyttöjärjestelmien omat lokiohjelmat eivät juuri sisällä analysointityökaluja, joten analysointi jää järjestelmänvalvojan manuaalisesti tehtäväksi, mikä on jo aiemmin tässä työssä todettu täysin riittämättömäksi, työlääksi ja vaikeaksi tavaksi. Lisäksi Suomessa lokien analysointiohjelmien mainostaminen on vähäistä tai lähes olematonta, joten yritysten pitäisi itse osata etsiä ja valikoida sopiva ohjelma kaupallisten ja ilmaisten ulkomaalaisten ohjelmien viidakosta, mikä on haastavaa. Ei siis ihme, että analysointi koetaan vaikeaksi. Jälkikäteen ajatellen lokien hallintaa koskien kyselyssä olisi ollut hyvä selvittää myös käytetäänkö yrityksissä IDPS:ää tai SIEMiä.

Viimeiseksi todettakoon, että kyselyn perusteella jokaisessa yrityksessä tulee silloin tällöin olemaan ICT-verkon häiriötilanteita, joko teknisiä tai tietoturvaongelmia. Niihin täytyy vain osata varustautua ja lokien kerääminen on juuri sitä, oli niiden merkitys tositilanteessa kuinka pieni tahansa. Onneksi kyselyyn vastanneissa yrityksissä tämä on oivallettu ja lokitietoja onkin näissä tilanteissa käytetty hyödyksi. Tässä yhteydessä olisi tosin voinut myös kysyä, onko yrityksen lokitietoja ikinä tarvittu oikeusprosessissa.

7 Pohdinta

Valitsin aiheen, koska olen ollut aina hyvin kiinnostunut tietoturvasta ja tulevaisuudessa toiveissa olisi päästä tekemään uraa alalla. Näin tässä myös potenti-

aalia omien tietojeni päivittämiseen ja kehittämiseen. Lokitiedot ovat tietoverkkojen hallinnassa niin tärkeitä, että niiden ymmärtämisestä on varmasti hyötyä tulevaisuudessa.

Opinnäytetyöstä tuli mielestäni melko hyvä asiakokonaisuus, jossa on monenlaista asiaa lokitiedoista ja niiden käytöstä. Teoria ja käytäntö tukevat työssä toisiaan ja tietoa löytyi yllättävän paljon, vaikka lokitiedot eivät ensituntumalta vaikutakaan asialta, josta saisi kokonaisen opinnäytetyön rakennettua. Tavoitteeseen päästiin ja työssä onkin melko hyvin esitelty lokitietojen käyttömahdollisuudet ja perusperiaatteet ICT-verkossa.

Yrityskyselyn vastausprosentti jäi harmittavan pieneksi. Valmistuneesta kyselystä ei saanut juurikaan trendejä esille pienen otoksen takia. Vastauksia olisi ehkä saanut pidentämällä kyselyn aukioloaikaa, mutta toisaalta lähes kaikki saamani vastaukset tulivat kyselyn ensimmäisenä päivänä (yksi heti muistutusviestin jälkeen) eikä suinkaan tasaisena virtana koko ajanjaksolla, joten ei sekään olisi välttämättä auttanut. Toki lokitiedot ja tietoturva yleensäkin aiheena on sellainen, että joku saattaa kokea niitä koskeviin kyselyihin vastaamisen tietoturvauhkana, vaikka vastaukset olisivat anonyymejäkin. Tämä riski oli kyllä tiedossa kyselyä toteuttaessa, mutta odotin silti hieman suurempaa osanottoa.

Työ poiki minusta parikin jatkokehitysideaa, joista joku toinen voisi mahdollisesti tehdä opinnäytetyön. Esiteltäviä ohjelmia etsiessäni vastaan tuli hyvin suosittu vapaan lähdekoodin IDPS, Sourcefire-ohjelmistoyrityksen Snort. Sen asennus ja käyttöönotto Windowsille oli kuitenkin hyvin monimutkaista ja vaati tämän työn puitteisiin nähden liian paljon paneutumista, joten hylkäsin sen suosiolla. Snort on kuitenkin maailman suosituin vapaan lähdekoodin IDPS, joten sen käyttöönotto ja hallinta voisi olla hyödyllinen ja mielenkiintoinen tutkimuskohde.

Toinen mahdollinen jatkokehitysaihe on toteuttamani kyselyn laajentaminen koko maan mittakaavaan. Toki aiheena voisi olla yleisempi tietoturvakysely ja lokitiedot vain yksi sen osa, mutta jos muutaman kymmenen paikallisen yrityksen sijaan hankkisi vaikka pari-kolmesataa yritystä ympäri maan, voisi saadakin käyttökelpoisia vastauksia.

Ammatillisesti työ on antanut minulle paljon. Kuten aiemmin mainitsin, toiveissa on päästä tulevaisuudessa työskentelemään tietoturva-alalla ja vähäinenkin ymmärtämys lokitiedoista on varmasti siinä vain eduksi. Olen saanut aiheesta paljon ymmärrystä teorian muodossa, päässyt hieman käsittelemään erilaisia aiheeseen liittyviä ohjelmia ja jopa oppinut hieman lokitiedoista arkipäivän yritysympäristössä. Työn myötä olen siis alkanut ymmärtää lokitietojen merkitystä paremmin.

Lähteet

Allen, J. H. 2001. CERT Verkkotietoturvan hallinta. Helsinki: Edita.

Anonymous. 2001. Hakkerin käsikirja. Helsinki:Edita.

Apache. 2014. Log Files. The Apache Software Foundation. http://httpd.apache.org/docs/1.3/logs.html. 20.5.2014.

Barnett, R. 2012. Web Application Defender's Cookbook : Battling Hackers and Protecting Users. Somerset: Wiley.

BasicLinuxCommands.com. 2011. Check linux usb disk name. http://www.basiclinuxcommands.com/2011/09/check-linux-usb-disk-name.html. 14.5.2014.

Boyles, T. 2010. CCNA Security Study Guide. Indianapolis: Wiley Publishing.

Bradley, T. 2006. Essential Computer Security. Rockland: Syngress Publishing.

Cyberarms. 2014. Installation & Configuration. http://cyberarms.net/download-pricing/installation-configuration.aspx. 20.5.2014.

Cysec. 2012. SIEM Security Information Event Management. http://www.securityinformationeventmanagement.com/index.php. 23.4.2014.

Eaton, I. 2003. The Ins and Outs of System Logging Using Syslog. SANS. http://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168?show=ins-outs-system-logging-syslog-1168&cat=logging. 24.3.2014.

Gerhards, R. 2009. The Syslog Protocol. The Internet Engineering Task Force (IETF). http://tools.ietf.org/html/rfc5424. 5.3.2014.

Gigamon. 2014. Intrusion Detection and Prevention Systems. http://www.gigamon.com/intrusion-detection-and-prevention-systems. 23.4.2014.

Hallam-Baker, P. M. & Behlendorf, B. 2014. Extended Log File Format. The World Wide Web Consortium (W3C). http://www.w3.org/TR/WD-logfile.html. 10.3.2014

IIS.net. 2014. Log <log>. Microsoft Corporation. http://www.iis.net/configreference/system.applicationhost/log. 14.5.2014.

International Business Machines (IBM). 2014. Log File Formats. http://publib.boulder.ibm.com/tividd/td/ITWSA/ITWSA_info45/en_US/HTML/guide/c-logs.html. 10.3.2014.

ITBusinessEdge. 2011. Server Log Management Is at Heart of Network Security. http://www.itbusinessedge.com/cm/blogs/itdownloads/server-log-management-is-at-heart-of-network-security/?cs=48354. 16.4.2014.

ITBusinessEdge. 2014. Guide to Computer Security Log Management. http://www.itbusinessedge.com/itdownloads/guide-to-computer-security-log-management/88872. 8.4.2014.

Kent, K & Souppaya, M. 2006. Guide to Computer Security Log Management. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf. 30.4.2014.

Kiwi. 2014. Kiwi Syslog Server for Windows. SolarWinds Worldwide. http://www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx. 20.5.2014.

Leskiw, A. 2014. Understanding Syslog: Servers, Messages & Security. Network Management Software.

http://www.networkmanagementsoftware.com/what-is-syslog. 24.3.2014.

Luotonen, A. 1995. Logging Control In W3C httpd. The World Wide Web Consortium (W3C). http://www.w3.org/Daemon/User/Config/Logging.html. 7.3.2014.

ManageEngine. 2014. Editions. Zoho Corporation. http://www.manageengine.com/products/eventlog/eventloganalyzer-editions.html. 20.5.2014.

Microsoft TechNet. 2014. Event Logs. Microsoft Corporation. http://technet.microsoft.com/en-us/library/cc722404.aspx. 17.3.2014.

Moeller, R. R. 2010. Wiley Corporate F&A : IT Audit, Control, and Security (2nd Edition). Hoboken:Wiley.

Nihuo Software. 2014. Brief Introduction of Log File Formats. http://www.loganalyzer.net/log-analysis/log-file-format.html. 7.3.2014.

nixCraft. 2013. Linux Log Files Location And How Do I View Logs Files on Linux? http://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/. 17.3.2014.

Scarfone, K & Mell, P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. 11.3.2014.

Tanaka, Shinji. 2014. Labeled Tab-separated Values. http://ltsv.org/. 14.5.2014.

TechTerms.com. 2010. Log File Definition. http://www.techterms.com/definition/logfile. 5.3.2014.

Valtiovarainministeriö. 2009. Lokiohje. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf. 23.4.2014.

Webopedia. 2005. Intrusion Detection (IDS) and Prevention (IPS) Systems. IT-BusinessEdge. http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp. 23.4.2014.

Wikipedia. 2013. Common Log Format. http://en.wikipedia.org/wiki/Common_Log_Format. 20.5.2014.

Woody, A. 2013. Enterprise Security: A Data-Centric Approach to Securing the Enterprise. Birmingham: Packt Publishing Ltd.

Yrityskyselyn verkkolomake

Lokitietokysely

Karelia AMK Opinnäytetyö 2014 / Marjo Laine

* Required

Yrityksenne koko *

- Pieni (1-49 henkeä)
- Keskisuuri (50-249 henkeä)
- Suuri (yli 250 henkeä)

Yrityksenne verkon pääasiallinen käyttöjärjestelmä *

- Windows
- Linux
- Muu UNIX-järjestelmä
- Muu

Onko yrityksenne/toimipaikkanne palveluksessa erillistä tietoturvahenkilöä/henkilöstöä? *

- Kyllä
- Ei
- En osaa sanoa

Onko yrityksessänne tietoturvasuunnitelmaa? *

- Kyllä
- Ei
- En osaa sanoa

Continue »

20% completed

Lokitietokysely

* Required

Itsearviointi

Kuinka hyväksi arvioisitte oman tietotaitonne lokitietoja koskien? *

- Erinomainen
- Hyvä
- Tyydyttävä
- Välttävä
- Ei tietotaitoa

Kuinka tärkeänä pidätte lokitietojen keräämistä ja analysointia? *

- Erittäin tärkeää
- Tärkeää
- Ei kovin tärkeää
- Turhaa

« Back Continue »

40% completed

Lokitietokysely

* Required

Lokitiedot yrityksessä

Mistä laitteista/ohjelmistoista yrityksessänne/toimipaikassanne kerätään lokitietoja?
Voitte valita useita

- [ ] Palvelimet
- [ ] Reitittimet
- [ ] Kytkimet
- [ ] Palomuurit
- [ ] Työasemat
- [ ] Yritykselle tärkeät ohjelmistot (esimerkiksi sähköpostiohjelmat, kassaohjelmat, toiminnanohjausjärjestelmät yms)
- [ ] Ohjelmistot, jotka eivät ole yrityksen toiminnalle kriittisiä
- [ ] Other:

Miten lokitietoja hyödynnetään yrityksessänne/toimipaikassanne?
Voitte valita useita

- [ ] Tietoturvauhkien aktiiviseen havainnointiin (myös IPS/IDS)
- [ ] Vikatilojen/tietoturvaongelmien jälkeiseen vianselvitykseen
- [ ] Yrityksen verkon tilan yleiseen seurantaan ja ongelmien ennaltaehkäisyyn
- [ ] Työnteon seuraamiseen
- [ ] Kaupalliseen käyttöön (esimerkiksi nettisivuilla käyvien asiakkaiden seuraaminen)
- [ ] Other:

Kuinka usein lokitietoja tarkkaillaan yrityksessänne/toimipaikassanne? *

- ○ Useita kertoja päivässä
- ○ Kerran päivässä
- ○ Kerran viikossa
- ○ Kerran kuukaudessa
- ○ Harvemmin
- ○ Vain ongelmien ilmaantuessa
- ○ Ei tarkkailla
- ○ En osaa sanoa
- ○ Other:

Onko lokitietojen hallinta mielestänne hyvin hoidettu yrityksessänne? *

- ○ Kyllä
- ○ Ei
- ○ En osaa sanoa

Jos ei, mitä parannuksia asialle mielestäsi pitäisi tehdä? (Voitte valita useita)

- [ ] Henkilöstöä pitäisi kouluttaa lisää aiheeseen
- [ ] Lokitiedostojen tietoturvaa pitäisi parantaa
- [ ] Lokitietoja pitäisi kerätä enemmän eri laitteista ja sovelluksista
- [ ] Lokitiedostojen sijaintia pitäisi keskittää
- [ ] Lokitietojen analysointi pitäisi tehdä helpommaksi
- [ ] Kolmansien osapuolten ohjelmia pitäisi ottaa käyttöön
- [ ] Lokitietoja pitäisi seurata/käyttää useammin
- [ ] Other:

« Back | Continue »

60% completed

Lokitietokysely

* Required

Lokitiedot ja häiriötilanteet

Onko yrityksessänne/toimipaikassanne tapahtunut viimeisen viiden vuoden aikana ICT-verkon ongelmatilanteita? *

Esimerkiksi verkkohyökkäys tai tekniset vikatilanteet

- ○ Kyllä
- ○ Ei
- ○ En osaa sanoa

Jos kyllä, kuinka suuri apu oli lokitietojen analysoinnista?

- ○ Ratkaiseva
- ○ Merkittävä
- ○ Kohtalainen
- ○ Vähäinen
- ○ Lokitietoja ei käytetty

« Back | Continue »

80% completed

Lokitietokysely

Vapaa sana

Sana on vapaa. Tähän voitte kirjoittaa vapaasti, mikäli mieleenne tulee vielä jotain aiheeseen liittyvää.

« Back | Submit

Never submit passwords through Google Forms.

100%: You made it.

Esimerkki yrityksille lähetetystä sähköpostista

Lokitietokysely opinnäytetyötä varten

Laine Marjo

Vastaanottaja: <Yrityksen sähköpostiosoite>

8. huhtikuuta 2014 17:33

Marjo Laine
Karelia AMK
marjo.laine@edu.karelia.fi

8.4.2014

<Yrityksen nimi>

Hei!

Olen neljännen vuoden tietotekniikan opiskelija Karelia-ammattikorkeakoulussa ja teen kyselyä Joensuun yritysten lokitietojen käytöstä opinnäytetyötäni varten. Kysely on toteutettu Google Drivella, tyypiltään monivalinta ja vastaaminen vie joitakin minuutteja. Vastaukset käsitellään luottamuksella, niitä ei voi yhdistää vastaajiin eikä yrityksen nimeä mainita missään yhteydessä. Kyselyn tulokset esittelen opinnäytetyössäni. Ilmoitattehan, mikäli olette kiinnostuneet tuloksista ja haluatte myöhemmin linkin valmiiseen työhön. Pyydän myös ystävällisesti, että voisitte ohjata tämän sähköpostin tai kyselyn yrityksenne ICT-verkon lokitiedoista vastaavalle/tietävälle henkilölle. Kysely on auki kaksi viikkoa eli 22.4.2014 asti.

Kyselyyn pääsette tästä linkistä:
https://docs.google.com/forms/d/1VszIfg7EbAoh_yLYCod2h3c9qoz6gkQRKwLb4niP3Wc/viewform

Ystävällisin terveisin
Marjo Laine