Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Ville Niiranen

ATLASSIAN TUOTTEIDEN LOKITAPAHTUMIEN SAAMINEN SIEM-JÄRJESTELMÄÄN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 22 sivua

Ville Niiranen

ATLASSIAN TUOTTEIDEN LOKITAPAHTUMIEN SAAMINEN SIEM-JÄRJESTELMÄÄN

Uudistuneen tietosuoja-asetuksen myötä yritykset ovat ottaneet käyttöönsä Security Information and Event Management (SIEM)-järjestelmiä lokienhallintaan. SIEM-järjestelmien avulla saadaan organisaatioiden käyttämien työkalujen lokit seurantaan yhteen järjestelmään, jotta voidaan osoittaa, että tietosuoja-asetusta noudatetaan. Tämän opinnäytetyön toimeksiantajana toimi Combitech Oy.

Opinnäytetyö tarkastelee, miten Atlassianin tuotteiden lokitapahtumat tallentuvat SIEM-järjestelmään ja mitä kyseisellä järjestelmällä voidaan tehdä lokitapahtumien kanssa. Työ koostuu teoriaosuudesta sekä käytännön osuudesta. Teoriaosuudessa selostetaan termejä sekä työkaluja mitä opinnäytetyössä käytetään. Käytännöntyössä luodaan virtuaaliympäristö, jossa asennetaan testaukseen tarvittavat ohjelmistot.

Testiympäristön luonnin jälkeen SIEM-järjestelmä konfiguroidaan monitoroimaan opinnäytetyön aiheessa olevan ohjelmiston lokitiedostoja. Pohdinnassa todetaan, että SIEM-järjestelmä Splunk on toimiva ja opinnäytetyön tavoitteeseen päästiin.

ASIASANAT:

Atlassian, lokitiedosto, SIEM, Splunk

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2018 | 22 pages

Ville Niiranen

ATLASSIAN PRODUCTS LOG EVENTS TO SIEM SYSTEM

The new General Data Protection Regulation (GDPR) requires companies to adopt Security Information and Event Management (SIEM) systems for log management. SIEM systems are used as a tool for companies to use when demonstrating compliance with the new privacy policy.

This thesis was commissioned by Combitech Ltd. The objective of this thesis was to create a virtual test environment where it was necessary. The Splunk SIEM software was installed and configured to monitor Atlassian product log events.

After the test environment had been created, the SIEM system was configured to monitor the selected software log files. In conclusion, SIEM Splunk was proven functional and the objective of the thesis was achieved.

KEYWORDS:

Atlassian, log file, SIEM, Splunk

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET TAI SANASTO

Gartner	Kansainvälisen ICT-alan tutkimus- ja konsultointiyritys
GDPR	EU:n yleinen tietosuoja-asetus
Java	Ohjelmointikieli, ohjelmointialusta
RFC	Request for Comments
SIEM	Security Information and Event Management
Splunk	SIEM-ohjelmisto
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

1 JOHDANTO

Tämän opinnäytetyön toimeksiantona on saada Atlassian tuotteiden lokitiedostojen siirto SIEM-järjestelmään. Atlassianin tuotteina ovat Jira Software, Jira Service Desk sekä Confluence. Kyseisiä tuotteita käytetään työkaluna muun muassa projektinhallinnassa, kehitystyössä sekä tukipisteiden apuna.

Opinnäytetyön toimeksiantaja on Combitech Oy, joka oli opinnäytetyöni aikana työnantajani. Yritys käyttää Atlassianin tuotteita työvälineenä, joten siellä on tarvetta saada käyttämänsä ohjelmistojen lokitiedostot kootusti yhteen paikkaan sekä saada niistä helposti tarvittavat tiedot jatkotoimenpiteitä varten. Toimeksiantaja ei asettanut rajoitteita lokiehallinta-järjestelmän valinnassa. Valmiita SIEM- sekä lokienhallintajärjestelmiä löytyy paljon.

Opinnäytetyön käytännönosuus toteutettiin virtuaalikoneiden avulla. Käyttöjärjestelmänä toimi Linux-pohjainen käyttöjärjestelmä.

Opinnäytetyö alkaa teoriaosuudella, jossa lähestyttiin käytettyihin ohjelmistoihin, tiedostoihin sekä virtuaalikoneisiin. Käytännön osuudessa asennetaan virtuaalikone, verkkopalvelin, tietokanta sekä tarvittavat ohjelmistot. Asennuksien jälkeen ohjataan Atlassianin tuotteiden lokitiedostoja valitsemani SIEM-järjestelmän analysoitavaksi.

Opinnäytetyön lopuksi pohdin, onko valitsemani SIEM-järjestelmä suotuisa toimeksiantajalleni ja muille yrityksille.

2 KÄYTETYT TYÖKALUT

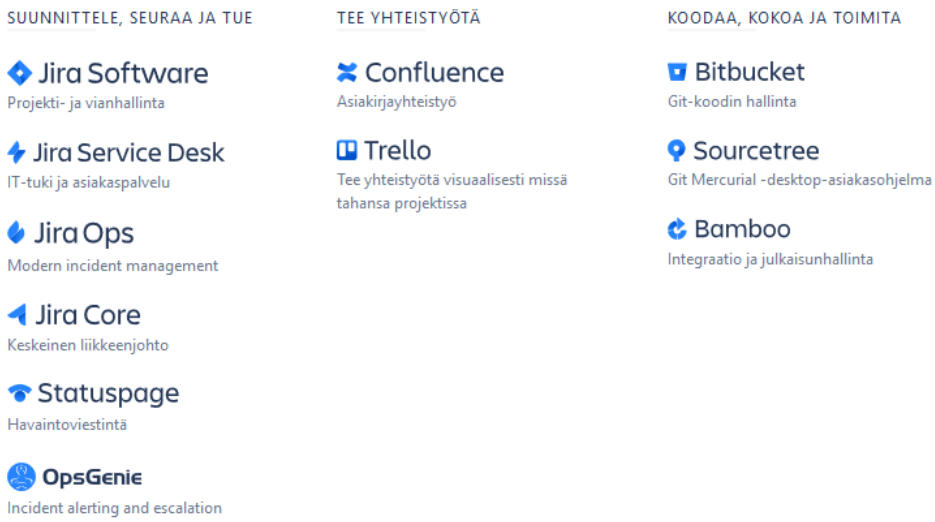
2.1 Virtuaalikone

Virtuaalikoneella tarkoitetaan tietokonetta, joka ei ole fyysisesti olemassa, vaan kyseessä on tietokonetiedosto, jota yleisimmin kutsutaan kuvakkeeksi. Toisin sanoen kyseessä on tietokone tietokoneen sisällä. Esimerkiksi työskennellessäni opinnäytetyön parissa käytin Windows 10 käyttöjärjestelmää fyysisen koneeni kanssa, mutta käytännön suoritin Linuxin Ubuntu-käyttöjärjestelmää käyttäen virtuaaliympäristössä. (Windows 2018)

Virtuaalikoneiden yksi suurimmista hyödyistä on se, että siihen tehdyistä testeistä ja kokeiluista ei seuraa minkäänlaisia vuorovaikutteita fyysiseen tietokoneeseen, joten se toimii testiympäristönä erinomaisesti. Niitä voi esimerkiksi käyttää beetavaiheessa olevan käyttöjärjestelmän tai sovelluksen testaamiseen, virustartunnan saaneiden tiedostojen tai tietokantojen tarkastelemiseen tai niihin voi myös asentaa pelkän verkkopalvelimen käyttöjärjestelmän sijasta. Myös moniajo on mahdollista, eli samaan aikaan voi pitää montaa virtuaaliympäristöä käynnissä, tietenkin fyysisen tietokoneen tehokyvyn rajoissa. Virtuaalikoneiden tehovoimaa voi myös itse asettaa tarvitsevalle tasolle. (Windows, 2018)

2.2 Atlassian ohjelmistoyritys

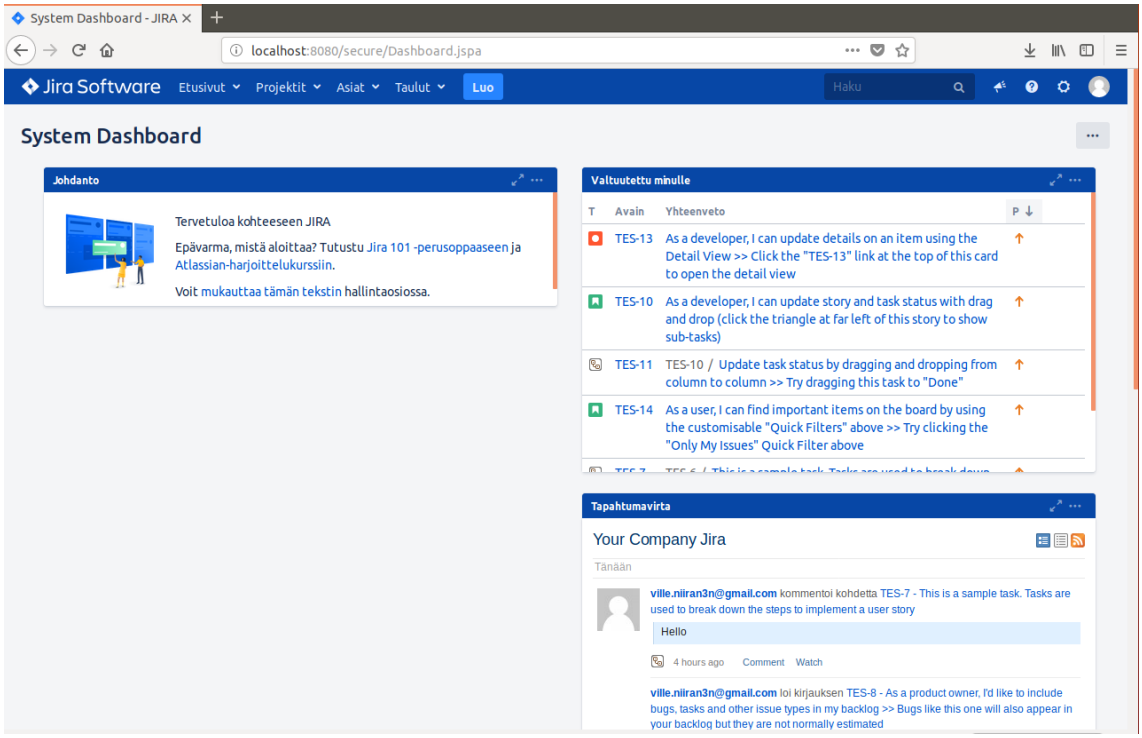
Atlassian on tietokoneohjelmistoalan yritys, joka tuottaa tuotteita ohjelmistokehittäjille, projektipäälliköille sekä yrityksen hallintaosastolle. Kuvasta 1 nähdään yrityksen tuoteportfolion. Tunnetuin tuote on Jira, jota käytetään tässä opinnäytetyössä. (Atlassian 2018)



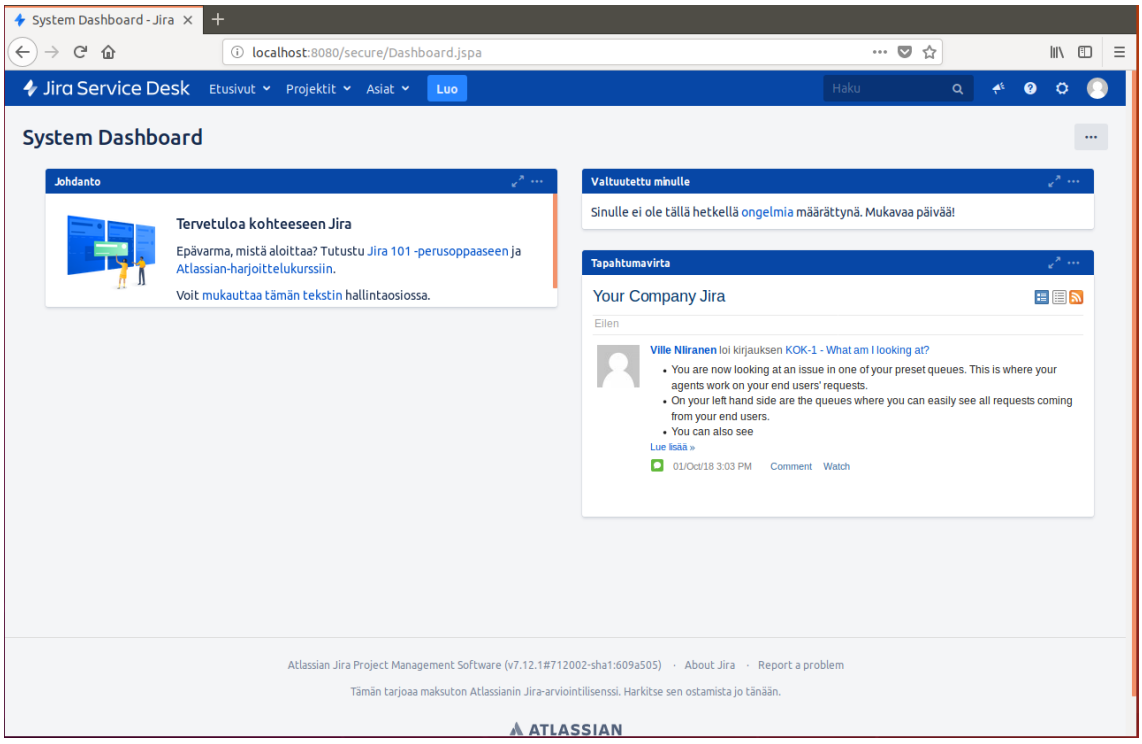
Kuva 1. Atlassian tuoteportfolio (Atlassian 2018).

Jira on työkalu ohjelmistokehittäjille, jotka käyttävät sitä projektinhallinnassa sekä ohjelmointivirheiden etsinnässä. Jira tuotetta jaetaan kolmessa eri paketissa. Ne ovat Jira Core, joka on yleinen projektinhallintajärjestelmä, Jira Software, joka sisältää ohjelmiston sekä ketterän projektinhallinta ominaisuuden, sekä Jira Service Desk, joka on tarkoitettu yrityksen IT-tukipalvupisteelle. Kuvat 2 ja 3 näyttävät, miltä Jiran graafinen käyttöliittymä näyttää. (Atlassian, 2018)

Confluence on Atlassianin tekemä niin sanottu wikipankki. Toisin sanoen se on yritykselle työkalu, jota työntekijät voivat käyttää lisätäkseen tiedostoja sekä luomaan verkkosivuja, josta löytyy heille oleellista informaatiota. Ohjelmisto tarjoaa edistyneen tavan luoda sivuja. Käyttäjän ei tarvitse muuta kuin käyttää valmiita sivupohjia, jotka muotoutuvat käyttäjän tarpeiden mukaan. (Atlassian, 2018)



Kuva 2. Jira Software-ohjelmiston graafinen käyttöliittymä (Virtuaalikone 2018)



Kuva 3. Jira Service Desk-ohjelmiston graafinen käyttöliittymä (Virtuaalikone 2018)

2.3 Lokitiedosto

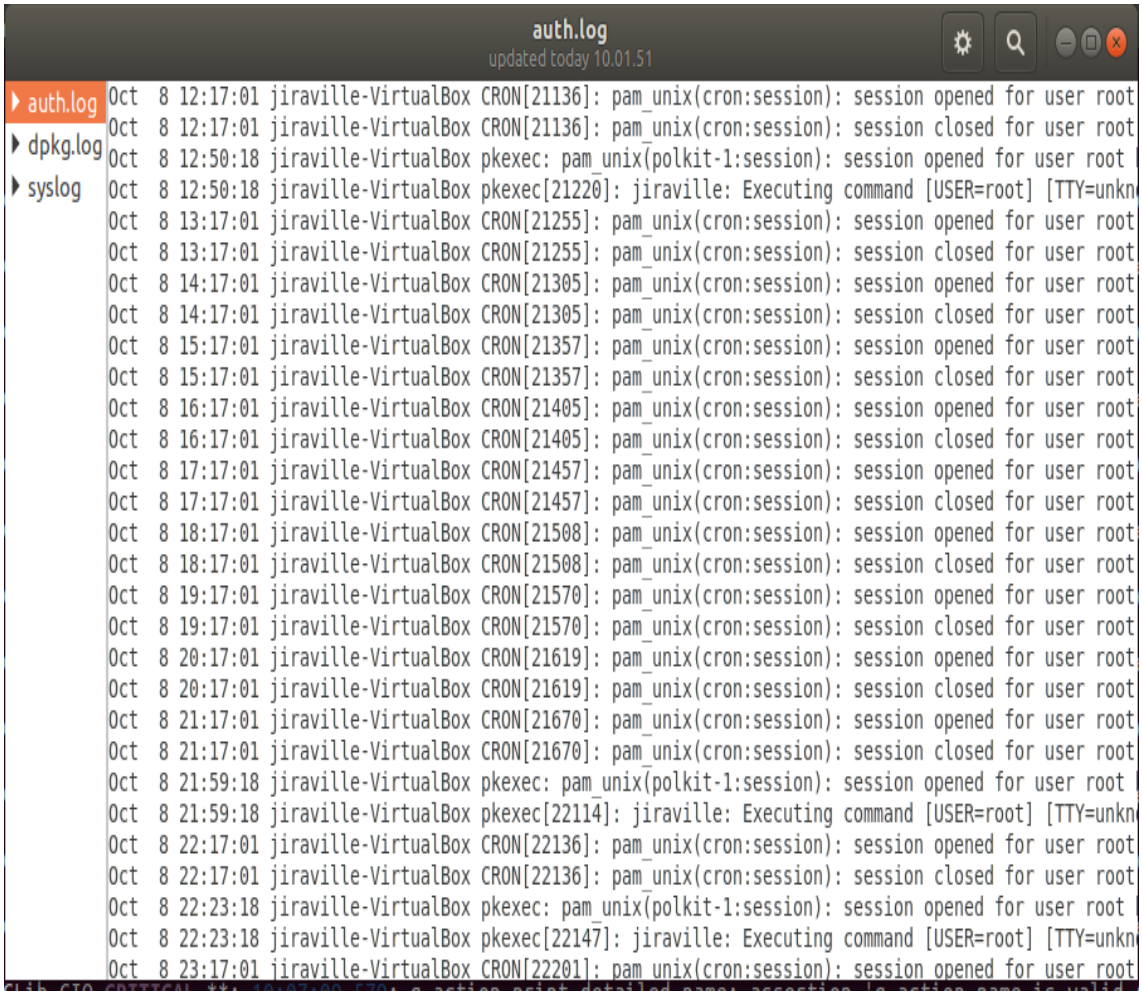
Useimmissa tietokoneissa ja ohjelmissa on lokitiedostojärjestelmä. Lokitiedostot ovat tiedostoja, joita syntyy esimerkiksi, kun tietokoneessa tapahtuu muutoksia, ohjelmistoja asennetaan tai verkkopalvelin kirjaa lokitiedostoja verkkovierailijoista. Niiden sisältö voi vaihdella suuresti, riippuen minkä tason tapahtumasta on kyse.

Lokitiedostot, jotka muodostuvat ohjelmistojen asennuksen aikana sisältävät lähtökohtaisesti tietoa tapahtumasta, jotka ovat joko lisätty taikka kopioitu tietokoneen kiintolevylle asennuksen aikana. Ne voivat myös sisältää ajan, päivämäärän, sekä mihin polkuun ne ovat asennettu. Näistä lokitiedostoista on hyötyä vianetsinnässä sekä ohjelmiston poistamisessa. (Techterms 2010)

Verkkopalvelin luo lokitiedostoja aina kun dataliikennettä syntyy verkkosivuilla. Ne sisältävät tietoja vierailijoiden IP-osoitteista, ajan jolloin vierailu tapahtui, sekä millä sivustoilla hän on käynyt. Lokitiedostot voivat myös kirjata tietoa onko vierailija lisännyt tiedostoja verkkopalvelimelle. Verkkopalvelimen lokitiedostojen tapahtumaketjua kutsutaan nimellä syslog. (Techterms 2010)

Lokitiedostot ovat tyypillisesti tekstitiedostoja (.txt) tai lokitiedostoja (.log). Lokitiedostoja voi myös tallentaa moneen eri muotoon, riippuen siitä millä ohjelmalla niitä halutaan lukea, esimerkiksi .csv-, pdf-, tai .xlsx-tiedostotyyppiin, vaihtoehtoja on monia. (Techterms 2010)

Kuvassa 4 näemme esimerkin Linux-käyttöjärjestelmän lokitiedostosta, josta saamme selville mitä se tyypillisesti sisältää: tapahtuman ajan, päivämäärän, tietokoneen nimen sekä viestin tyypin.



Kuva 4. Ubuntu käyttöjärjestelmän lokitiedosto (Virtuaalikone 2018)

2.4 Syslog

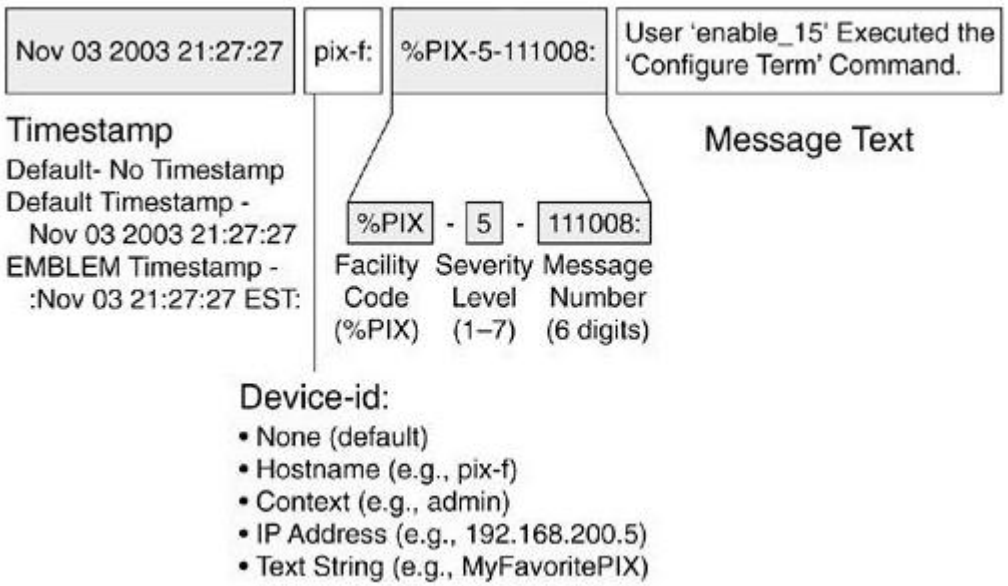
Eric Allman oli 1980-luvulla mukana projektissa, jossa hän kehitti syslogin, ja sitä ruvettiin käyttämään lokitiedostojen kirjanpidossa standardina. IETF standardisoi syslogin standardissa RFC 5424 (Cisco 2005)

Unix-pohjaisista verkkojärjestelmistä useimmiten löytyy erillinen palvelin, jota kutsutaan syslog-palvelimeksi. Sinne pyritään ohjaamaan verkossa muodostuvat lokitapahtumat, jotta ne olisivat kätevästi ja nopeasti haettavissa. Verkkojärjestelmät ja laitteet lähettävät syslog-viestejä syslog-palvelimelle, josta palvelin lähettää hälytyksiä pääkäyttäjille, mistä he näkevät viestit ja suorittavat viestin perusteella joko vianetsintää tai valvovat liiken-

nettä. Windows käyttöjärjestelmä ei suoranaisesti tue syslog-muotoa, mutta useat kolmannet osapuolet ovat tehneet ohjelmistoja, joita Windows-pohjaiset laitteet kykenevät niitä hyödyntämään. (Leskiw, 2014)

Yleisesti syslog-palvelin sisältää eräänlaisen vastaanottajan, joka ottaa viestit vastaan. Se prosessoi ja kerää kaiken datan mikä lähetetään UDP-protokollan 514 portista. UDP:n kautta tulleet viestit voivat kuitenkin jäädä huomioimatta tai niillä ei ole takuita, että ne tulevat ilmi, joten olisi kannattavampaa ohjata data TCP-protokollan portin 1468 kautta. Suuret syslog-palvelimet pitävät myös kirjaa datasta, ja ne tallentuvat palvelimen omalle tietokannalle. Suuren tietokannan vuoksi syslog-palvelimet omaavat myös hallinta- sekä suodatusjärjestelmiä, jotka automatisoivat tiedonhallintaa. Näiden avulla helpotetaan työtä, esimerkiksi kun halutaan löytää tietty data tietokannasta. Järjestelmä antaa myös hälytyksiä, jos data on hälytyksen arvoista, sekä tietoa pääkäyttäjille vianetsintää varten. (Leskiw, 2014)

Kuvasta 5 nähdään esimerkki mitä syslog-viestit sisältävät: Aikaleima, milloin kyseinen tapahtuma tai viesti on luotu, laitteen nimi, mikä ohjelma on viestin luonut, viestin vakavuus, viestin numero sekä viestin teksti. Niiden maksimipituus on standardisoitu 1024 tavuun, minimipituutta ei ole määritelty. (Stackify 2017)

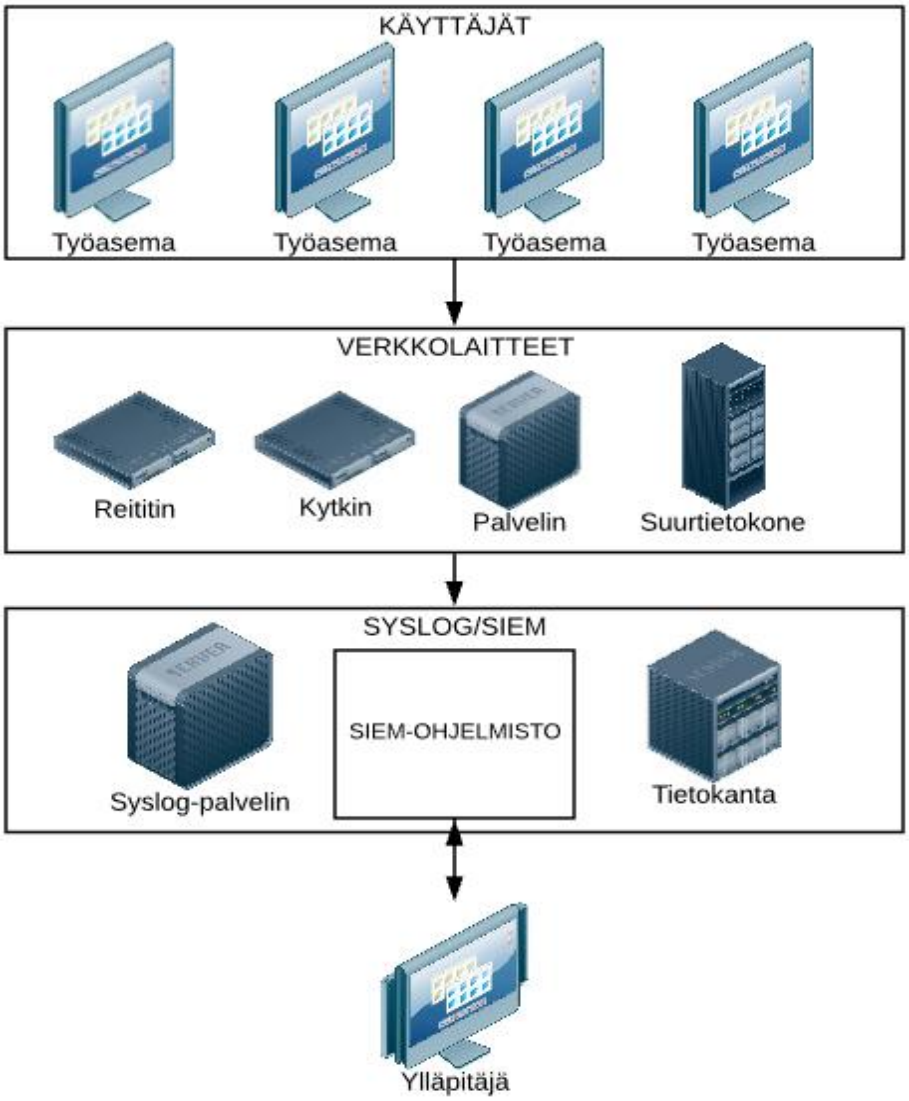


Kuva 5. Esimerkki syslog-viestin sisällöstä (Stackify 2018)

2.5 SIEM-järjestelmä

Nykyaikana tietoturvaratkaisut ovat yrityksen koosta huolimatta elintärkeitä. Suurimalla osalla yrityksillä on virustorjuntaohjelmistoja sekä palomuureja. Hyvä lisä tietoturvaan on hankkia SIEM-järjestelmä (Security Information and Event Management). SIEM-järjestelmä on tietoturvaohjelmisto, joka ottaa vastaan kaikki tapahtumat, mitkä tapahtuvat yrityksen tai organisaatioiden tietojärjestelmissä, tietokoneista verkkopalvelimiin. (Paul Rubens, 2018)

Miksi SIEM-järjestelmä pitäisi hankkia, kun useilla yrityksillä on jo virustorjunnat sekä palomuurit? Yksi käyttötapa SIEM:n takana on, että se kykenee ennakoimaan hyökkäykset analysoimalla tapahtumia yrityksen tietojärjestelmissä. Yritykset luovat niin paljon dataa tänä päivänä, että ihminen ei kykene sitä kaikkea analysoimaan ja erottelemaan mikä on vaarallista ja mikä on vaaratonta, jos yritys joutuvat hyökkäyksen kohteeksi. Paul Rubens (2018) kertoo, että ICT-alan tutkimus- ja konsultointiyritys Gartnerin mukaan yhdellä pienellä SIEM-järjestelmällä voi olla jopa 300 tapahtuma lähdettä, jossa voi muodostua 1500 tapahtumaa sekunnissa, joiden koko voi olla jopa 800 gigatavua. Tällainen määrä dataa on ihmismielelle aivan liikaa analysoitavaksi käsin. SIEM-järjestelmä on reaaliaikainen tapahtumien analysoija, joka antaa reaaliaikaisen hälytyksen, jos se huomaa pahanenteisiä tapahtumia. Kuvassa 6 on yhteenveto SIEM-järjestelmästä. (Rubens, 2018)



Kuva 6. SIEM-järjestelmä.

3 KÄYTÄNTÖ

3.1 Testiympäristön luonti

Opinnäytetyön käytännön osuus alkoi asentamalla tietokoneeseen Oracle VM Virtualbox-ohjelmisto, joka on käyttöjärjestelmien virtualisoija. Ohjelma valittiin aikaisempien käyttökokemusten perusteella. Atlassianin tuotteille valittiin käyttöjärjestelmäksi Ubuntu (Debian Linux), koska se on opiskeluaikana tullut tutuksi. Kun virtuaalikäyttöjärjestelmät saatiin asennettua, oli koneelle asennettava Java-ohjelmisto. Atlassianin tuotteet ovat Java-pohjaisia, joten ne tarvitsevat Java-ohjelmiston toimiakseen. Java-ohjelmisto asennettiin seuraavilla komennoilla

sudo add-apt-repository ppa:webupd8team/java

sudo apt update; sudo apt install oracle-java8-installer

Seuraavana vuorossa oli Atlassianin Jira Software-ohjelmiston asentaminen Ubuntu-käyttöjärjestelmään. Atlassianin tuotteilla on kattava määrä materiaalia asentamisesta kaikille tuetuille käyttöjärjestelmille.

Ohjelmiston asennus tapahtui vaiheittain. Ohjelmisto ensin ladataan, ajetaan asennustyökalu, määritellään ohjelmiston asetukset. Ohjelma kysyy asennusvaiheessa, haluaako käyttäjä käyttää omaa tietokantaa, Atlassian tarjoaa myös omaa tietokantaa kokeilukäyttöä varten. Atlassian tukee seuraavia tietokantoja: PostgreSQL, MySQL, Oracle sekä Microsoft SQL Server. Testiympäristööni valitsin PostgreSQL, tietokantojen välillä ei suorituskyvyllisesti ole suurta eroa. Opinnäytetyöhön valikoitui PostgreSQL. Asensin postgresql-tietokannan käyttämällä Ubuntun komentoriviä seuraavalla komennolla:

sudo apt-get install postgresql postgresql-contrib

Koneen asennettua tietokantaohjelmiston, oli vuorossa tietokannan sekä käyttäjien luominen.

sudo su - postgres

Yllä olevalla komennolla siirrytään postgresql-palvelimeen.

psql

Siirrytään pääkäyttäjäksi.

CREATE SCHEMA nimi**;**

CREATE USER tunnus **PASSWORD** ‘salasana’**;**

CREATE DATABASE tietokantanimi;

CREATE USER käyttäjänimi **WITH ENCRYPTED PASSWORD** ‘salasana’;

GRANT ALL PRIVILEGES ON DATABASE tietkoantanimi **TO** käyttäjänimi;

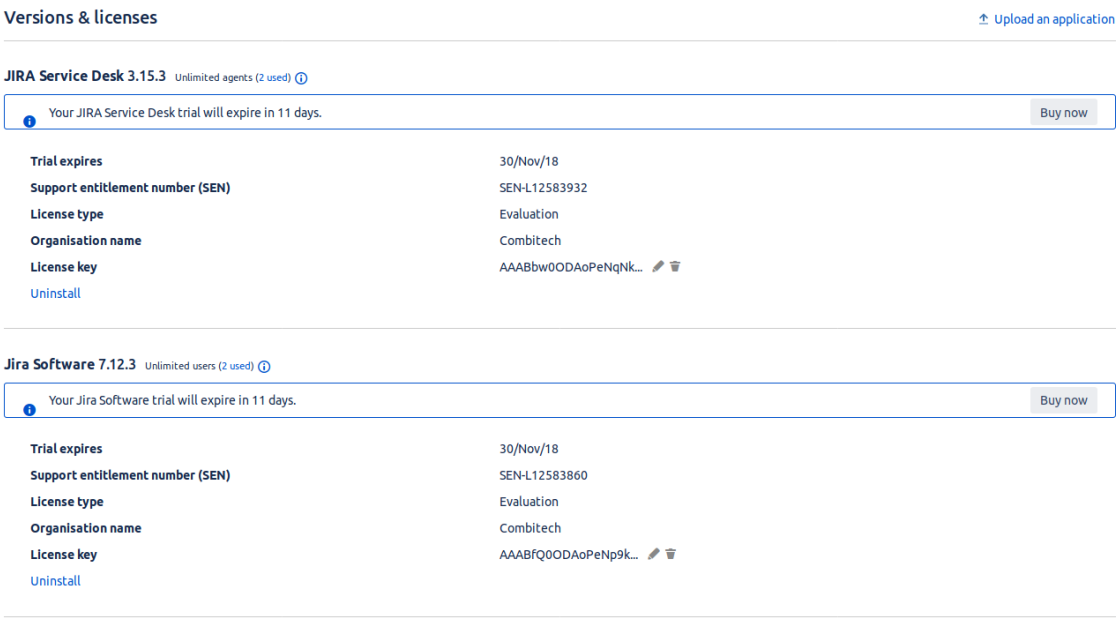
Yllä olevilla komennoilla loin PostgreSQL tietokannan ja käyttäjän. Tietokannan asennettua, jatkettiin Jira-ohjelmiston asennusta. Kuvassa 7 näyttökaappaus asennusvaiheesta, jossa kysytään asentajalta käyttääkö hän Jira-ohjelmiston tarjoamaa tietokantaa vai omaa.

Kuva 7. Jira ohjelmiston tietokannan liittäminen (Virtuaalikone 2018).

Tietokannan lisäämisen jälkeen, asennusvaiheessa kysytään tuoteavainta. Atlassian tarjoaa 30 päivän ilmaisen kokeilujakson. Ilmaisen 30 päivän tuoteavaimen saa, kun luo käyttäjätunnuksen Atlassianin verkkosivuilla.

Tämän jälkeen asennusvaiheessa seuraa ylläpitäjätason käyttäjän luonti, SMTP-palvelimen integrointi, ja sen jälkeen on asennus valmis Jira-Softwaren kanssa. Jira-Softwaren webosoite on löydettävissä selaimen avulla. Jiran verkkosivuksi asetettiin palvelimen IP-osoite sekä portti 8080, tässä tapauksessa http://127.0.0.1:8080.

Jira Software-ohjelmiston asennuksen jälkeen oli vuorossa Jira Service Desk:n asennus. Service Deskin voi asentaa joko suoraan samalle alustalle kuin Jira Software, tai sen voi asentaa erilliselle palvelimelle. Testiympäristöön valittiin ensimmäinen vaihtoehto, saadaksemme täyden integraation. Jira Softwaren käyttöliittymästä pystyy asentamaan Service Deskin samalle palvelimelle. Kuten kuvasta 8 nähdään, että testiympäristössä on samalle palvelimelle asennettu Software sekä Service Desk.



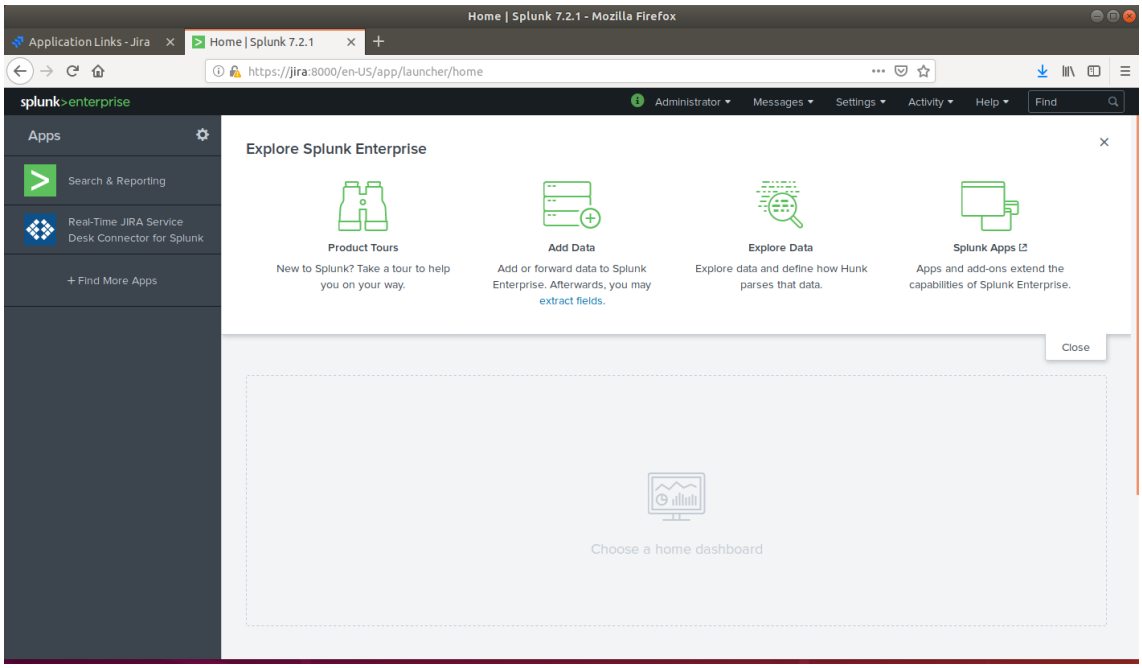
Kuva 8. Jira Ohjelmistot (Virtuaalikone).

Confluence asennetaan erilliselle palvelimelle, jonka asennus toteutuu samalla tavalla kuin Atlassianin Jira-ohjelmistot. Confluencen asennettua erilliselle palvelimelle seuraavaksi oli vuorossa yhdistää se Jira-palvelimelle. Se toteutetaan Jiran verkkosivustolla muodostamalla applikaatiolinkki.

Atlassianin ohjelmistoihin on mahdollista liittää Active Directory, joka on erillinen palvelin, joka toimii organisaatioissa käyttäjätunnusten pankkina. Se ylläpitää sekä yhdistää käyttäjät ohjelmistoon sekä antaa selkeitä rooleja onko käyttäjillä valtuuksia käyttää tai hallinnoida ohjelmistoja. Testiympäristö ei tarvinnut tätä asetusta tehtävänantoa varten.

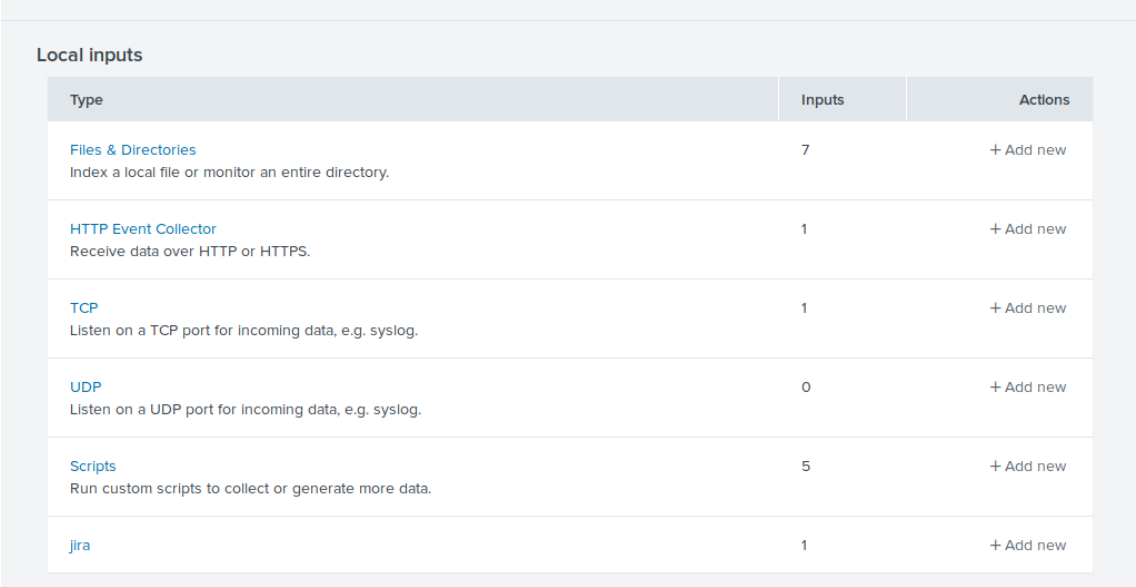
3.2 Splunk-järjestelmä

SIEM-järjestelmäksi valikoitui Splunk. Splunkin verkkosivuilta www.splunk.com löytyy dokumentaatiota sen asennuksesta eri käyttöjärjestelmälle. Järjestelmä asennettiin samalle palvelimelle kuin Jira-ohjelmistot. Kuvasta 9 näemme, asennus on saatu valmiiksi ja ohjelmisto on valmiina käytettäväksi sille asetetulle websivustolle, tässä tapauksessa osoitteessa http://127.0.0.1:8000.



Kuva 9. Splunk käyttöliittymä (Virtuaalikone).

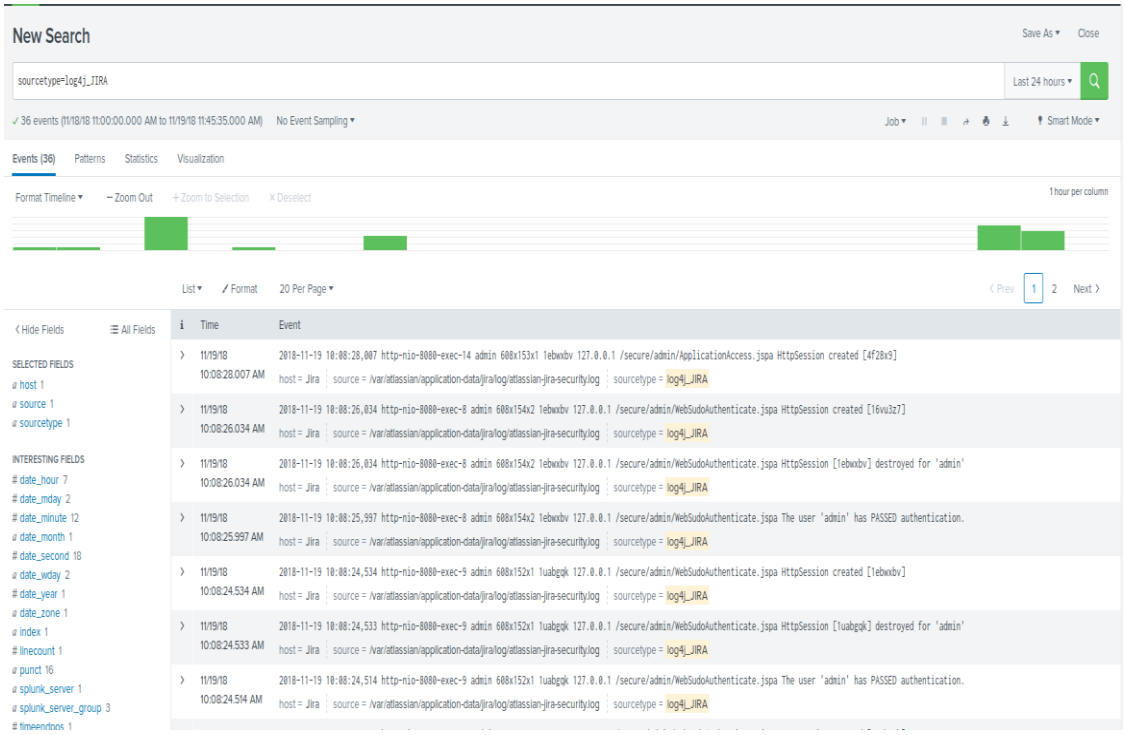
Splunkin käyttöliittymästä voidaan lisätä datasyötön: joko paikallisen tai edelleen lähetetyn syötön. Testiympäristössä Splunk asennettiin samalle palvelimelle kuin Jira, joten valittiin: paikallinen syöttö. Datasyötöt voidaan asettaa eri tavoin kuten kuvasta 10 näemme.



Kuva 10. Splunk Datasyöttö (Virtuaalikone).

Datasyötöksi asetettiin Jira-ohjelmiston atlassian-jira-security.log lokitiedoston. Jiran lokitiedostot löytyvät oletuksena palvelimen polusta: ”/var/atlassian/application data/jira/log/”. Opinnäytetyössä pyrittiin tarkastelemaan tietoturvaan littyviä lokitiedostoja, joten lokitiedostoksi valittiin atlassian-jira-security.log, jota Splunk seuraisi.

Asetuksen jälkeen oikean lokitiedoston datasyöttöä pystyy Splunkissa seuraamaan reaaliaikaisesti (Kuva 11).



Kuva 11. Jira lokitiedostot Splunkissa (Virtuaalikone).

4 POHDINTA

SIEM-järjestelmä on organisaatioiden sekä yritysten kätevä tietoturvallisuustyökalu. Niiden avulla kyetään valvomaan ja analysoimaan verkkoympäristössä tietoturvatapahtumia. Uuden tietosuoja-asetuksen myötä organisaatioiden on pidettävä eriasteisia lokienhallintajärjestelmiä, jotta niistä jäisi jonkin asteinen jäljityspolku. SIEM-järjestelmät auttavat osoittamaan, että organisaatio toimii uuden tietosuoja-asetuksen mukaisesti. Testaamani Splunk-ohjelmisto osoittautui toimivaksi lokienhallintajärjestelmäksi.

Opinnäytetyön tavoitteena oli saada Atlassianin tuotteiden lokitiedostojen siirtäminen SIEM-järjestelmään. Tavoitteeseen päästiin asentamalla paikallisesti samaan Jira-palvelimeen Splunk-ohjelmisto. Vaihtoehtoja Jiran lokitiedostojen saamiseen eri SIEM-järjestelmiin löytyy monia. Opinnäytetyössä käytetty vaihtoehto on vain yksi keino saada lokitiedostot SIEM-järjestelmään, voi todeta asennusvaiheista ja joustavuudeltaan hyväksi. Splunk-vaihtoehto on suositeltava Pk-yrityksille, jotka tarvitsevat helposti muokattavissa olevan SIEM-järjestelmän.

LÄHTEET

Aaron Leskiw 2018 Understanding Syslog: Servers, Messages & Security Viitattu 11.10.2018 https://www.networkmanagementsoftware.com/what-is-syslog

Anand Deveriya, 2005, Cisco, An Overview of the syslog Protocol viitattu 19.10.2018 http://www.ciscopress.com/articles/article.asp?p=426638

Paul Rubens, 2018 SIEM Guide: A Comprehensive View of Security Information and Event Management Tools, Viitattu 19.10.2018 https://www.esecurityplanet.com/network-security/security-information-event-management-siem.html

Microsoft. 2018 What is a virtual machine? Viitattu 2.10.2018 https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/

R. Gerhards 2009 The Syslog Protocol Viitattu 11.10.2018 https://techterms.com/definition/logfile

Stackify 2017 Syslog Tutorial: How It Works, Examples, Best Practices and More Viitattu 18.10.2018 https://stackify.com/syslog-101/

Techterms 2010 Log File Viitattu 10.10.2018 https://techterms.com/definition/logfile

Wikipedia 2018 Atlassian Viitattu 4.10.2018 https://en.wikipedia.org/wiki/Atlassian