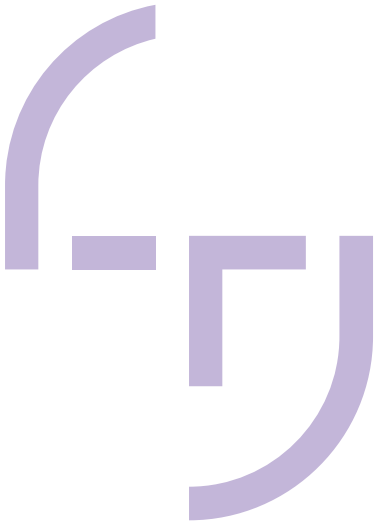
Tampereen ammattikorkeakoulu



Lokipalvelun kehittäminen OptoFidelity Oy:ssä

Pekka Parkkinen

OPINNÄYTETYÖ
Toukokuu 2022

Tieto- ja viestintätekniikan tutkinto-ohjelma

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan tutkinto-ohjelma

PARKKINEN PEKKA
Lokipalvelun kehittäminen OptoFidelity Oy:ssä

Opinnäytetyö 39 sivua, joista liitteitä kaksi sivua
Toukokuu 2022

Opinnäytetyön tarkoituksena oli tutkia OptoFidelity Oy:n palveluiden lokitietojen keräämistä eri palveluista ja kehittää järjestelmää. Työssä perehdyttiin lokijärjestelmien kehittymiseen alkuajoista nykyaikaisiin kehittyneisiin lokijärjestelmiin. Lisäksi perehdyttiin SIEM-palvelun kehittymiseen, käyttötarkoituksiin ja palvelun hyötyihin. Opinnäytetyö raportissa selvitettiin hieman SOC- ja SOAR-valvontaa.

Opinnäytetyössä tutkittiin nykyistä OptoFidelityn lokijärjestelmää Graylog:ia ja sen käyttötarkoituksia. Sitä verrattiin Microsoft Sentinel -palveluun. Minkä perusteella tehtiin päätös kahden järjestelmän välillä ja tulevasta kehityssuunnasta.

Osana opinnäytetyötä tehtiin Microsoft Sentinel SIEM-palvelun käyttöönotto ja käyttöönoton määritykset. Lisäksi pohdittiin mahdollista jatkoprojektia Microsoft Sentinel -palvelun käytön laajentamisesta.

Asiasanat: lokijärjestelmät, SIEM-palvelut, Microsoft Sentinel

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering

PARKKINEN, PEKKA
Development of a log service in OptoFidelity Oy

Bachelor's thesis 39 pages, appendices 2 pages
May 2021

Thesis purpose was understood log management in OptoFidelty. And understand how current log management is done and how to improve Graylog SIEM service.

In thesis work purpose was understand different computer logs. What are SIEM -services and how they work. And how SIEM services are done. Also, what SIEM services can do and how they help in IT security.

This project involved the introduction of the Microsoft Sentinel service deployment and adding a basic Microsoft log to Sentinel.

Results benefits OptoFidelity company and they got new SIEM service in use and how to deployment Microsoft Sentinel in future.

Key words: log management, SIEM service, Microsoft Sentinel

SISÄLLYS

1 JOHDANTO 6
2 Loki 7
3 SIEM 9
3.1 SIEM-palvelun rakenne 10
3.2 Käyttökohteita 11
3.3 Graaffinen esittämien 12
3.4 Käsittely 13
4 SOC ja SOAR 15
5 SIEM-palvelun kehitys OptoFidelity:ssä 16
5.1 Katselmus nykyiseen SIEM-palveluun 16
6 SIEM-palveluiden vertaaminen 17
6.1 Graylog Enterprice 17
6.2 Microsoft Sentinel 17
6.3 SIEM-palvelun valinta 19
7 Microsoft Sentinel käyttöönotto prosessi 20
7.1 Micrsoft Azure Resource group 21
7.2 Microsoft Azure Resource group käyttöönotto 22
7.3 Log Analytics käyttöönotto 24
7.4 Data Connectoreiden lisäys. 27
7.5 Lokien säilytys 30
7.6 Workbooks 31
8 Projektin jatkosuunnitelma 33
9 POHDINTA 34
LÄHTEET 35
LIITTEET 38

ERITYISSANASTO

DNS	Domain Name Service
ELF	Executable and Linkable Format
GEF	Geotechnical Exchange Format
Graylog	SIEM service
IPS	Intrusion Prevention Systems
IT	Information technology
JSON	JavaScript Object Notation
KQL	Kusto Query Language
Microsoft Sentinel	SIEM, SOC & SOAR service
NTA	Network traffic analysis
ODBC	Open Database Connectivity
SEM	Security event manager
SIEM	Security information and event management
SIM	Security information management
SOAR	Security orchestration, automation and response
SOC	Security Operation Center
SQL	Structured Query Language
UEBA	User and Entity Behavior Analytics
VPN	Virtual private network
W3C	Extended Log File

1 JOHDANTO

Opinnäytetyössä oli tarkoituksena tutkia yrityksen lokijärjestelmän nykytilannetta ja selvittää palvelun kehittämistä. Palvelun kehittämisen vuoksi, piti ymmärtää SIEM -palveluita ja niiden hyötyjä tietotekniikassa. Opinnäytetyössä käytiin läpi lokituksen perusajatusta, tekniikoita ja miksi tarvitaan lokijärjestelmiä. Lisäksi työssä perehdyttiin SIEM-palvelun rakenteeseen, käyttötarkoitukseen ja sen hyötyihin.

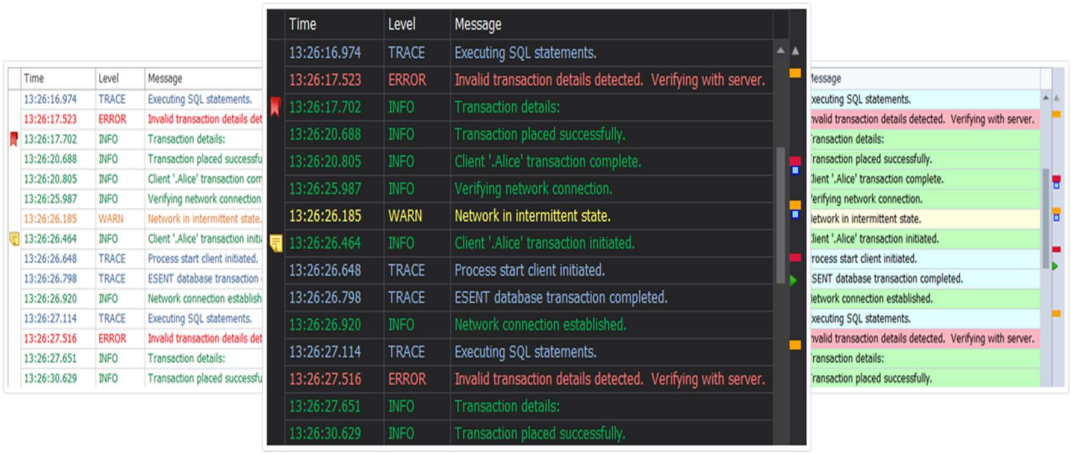
Työn tarkoituksena oli tuottaa yritykselle lokijärjestelmien vertailua kahden palvelun väliltä ja päättää kehityssuunta yrityksen lokijärjestelmän kehittämisessä. Vertailu tehtiin Graylog ja Microsoft Sentinel:n välillä.

Opinnäytetyössä tehtiin Microsoft Sentinel SIEM -palvelun käyttöönotto ja perusasetuksien määritys. Lisäksi työssä pohdittiin, kuinka Microsoft Sentinel -palvelun käyttöä voidaan laajentaa opinnäytetyön jälkeen.

Työssä oli käytetty lähteinä palveluiden tarjojien omia dokumentteja, heidän ohjeita ja videoita tuottamaan kattava selvitys.

2 Loki

Lokiviestit ovat tietokoneiden tai ohjelmien konekirjoittamia viestejä mitkä kertovat, mitä kone tai sovellus on tehnyt. Lokiviestit ovat erittäin hyödyllisiä tietokoneen tai sovelluksen tehtävien seuraamisessa, auditoinnissa ja eri ongelmien etsimisessä ja korjaamisessa. Ilman lokitusta ei voida seurata tapahtumien kulkuja.



Kuva 1. Esimerkki lokiviesteistä (LogviewPlus, n.d.)

Lokitusta on tehty tietotekniikan alkuajoista asti, joten on muodostunut useita eri formaatteja. Kaikissa formaateissa pyritään saamaan lokiviesteihin mahdollisimman paljon tietoja, mahdollisimman lyhyessä muodossa. Usein eri laitevalmistajat tai sovelluksen kehittäjät käyttävät lokiviestin sisältämässä datassa omia ennalta määriteltyä koodeja. Tällöin lokiviesteistä saadan lyhyitä, mutta haittapuolena on lokiviestien hankala lukeminen. Jolloin tarvitsee etsiä ennaltamääritetyt koodit valmistajilta. (Braden 2021.)

Yleisempiä loki formaatteja ovat:

- JSON LOG FORMAT
- Windows event log
- GEF format
- Common log format NCSA
- ELF
- W3C
- IIS
- ODBC

(Log Formats, 2020.)

Ja ne sisältävät perustiedot:

- Aikaleima
- Lähde
- Kohde
- Data

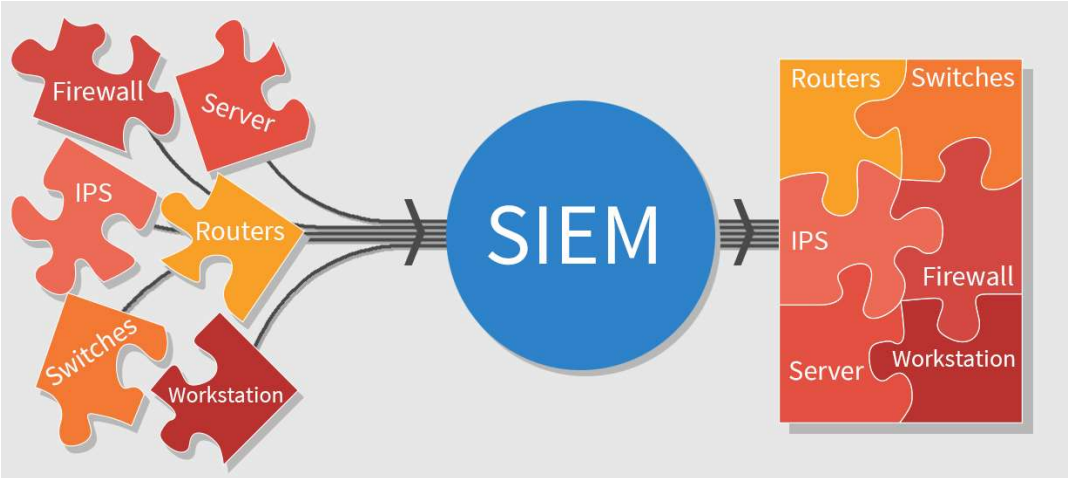
Osassa formaateissa on otettu käyttöön eri kriittisyysasteet lokiviesteille. Tällöin voidaan erottaa lokiviesteistä kriittiset virheet, virheet, yleiset lokiviestit toisistaan. Kun lokiviestejä on voitu lajitella eri kategorioihin, helpottui lokien hallinta huomattavasti. Silloin voitiin eritellä eri kategoriat toisistaan ja saada data hallittavammaksi. Kehittyneet lokijärjestelmät tarvitsevat eri kategorioita, jotta voitiin rakentaa automaattisia toimintoja.

3 SIEM

Security information and event management, tietoturvatiedon ja tapahtumien hallinta. National Institute of Standard and Technology on määritellyt SIEM-käsitteen ja se kääntyy suomeksi. Ohjelma, mikä tarjoaa mahdollisuuden kerätä dataa useista eri informatiivisesta laitteesta ja esittää toimintakelpoisen datan yhdessä käyttöliittymässä. (Kent & Souppaya 2006)

SIEM-palvelun ajatus sai alun 2000-luvun alkupuolella. Ajatuksena oli toteuttaa loikipalvelu, mikä kerää lokitiedot, sallii lokitietojen käsittelyn ja mahdollistaa automaattiset hälytykset halutuista tapahtumista

SIEM-palveluiden tarkoitus on kerätä usean eri palvelun lokitiedot yhteen paikkaan hallittavaksi kokonaisuudeksi. Lokitietoja on tuhansia rivejä, joten käsittely on tärkeää, kuitenkaan ei voida unohtaa yksittäisen rivin tärkeyttä.



Kuva 2. SIEM-palvelun toiminta. (Applebee 2015.)

SIEM-palvelussa tuotuja lokitietoja pystytään käsittelemään, tehdä niistä graaffisia kuivioita, tapahtumia voidaan analysoida, tehdä auditointi ja luoda automaattisia hälytyksiä. Eri palveluiden lokitiedoista voidaan tutkia eri tapahtumien välisiä yhteyksiä eri palveluiden välillä. Koska lokitietojen, tapahtumien ja hälytyksien avulla voidaan seurata eri tietotekniikan ympäristössä tapahtuvia tapahtumia, voidaan sanoa, että SIEM on osa tietoturvaa myös. (Applebee 2015.)

3.1 SIEM-palvelun rakenne

SIEM koostuu kolmesta eri toiminnallisuudesta Log Management, SIM ja SEM toiminnollisuuksista.

LOG Management palveluita käytetään eri palveluiden lokitietojen keräykseen, tallennukseen, arkistointiin ja lopulta datan poistoon (Wigmore 2016).

SIM, Security information management -palvelu koostuu valvottavien laitteiden lokitietojen lähettävistä agenteista, serveristä ja päätelaitteesta. SIM-palvelussa lokitiedoista pysytytään tekemään raportteja ja grafiikkaa valvotuista laitteista lokitietojen pohjalta. Dataa voidaan myös käsitellä ja tehdä dataan suodattimia. Kuitenkin yleensä kerätään kaikki lokitiedot talteen tarvittavan tutkimisen avuksi. (Awati 2022)

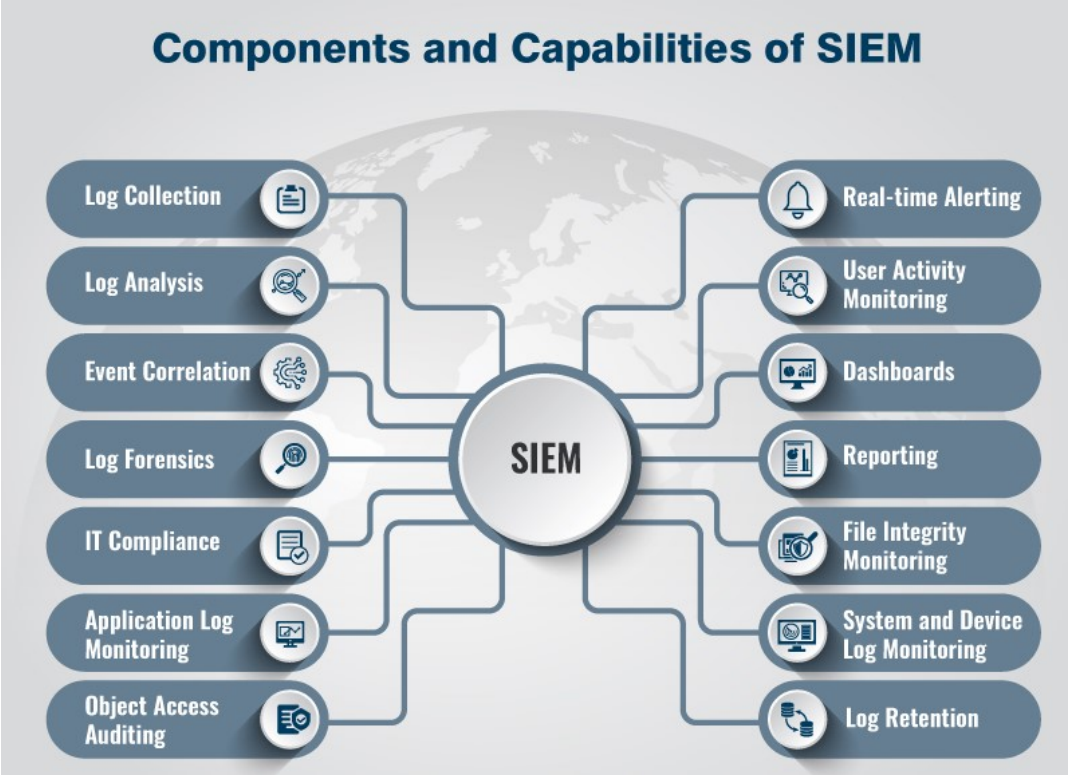
SEM, Security event manager tarkoituksena on identifioida, kerätä, monitoroida ja raportoida tietoturvaan liittyvät tapahtumat palvelussa. SEM mahdollistaa eri tapahtumien luonnin, analyysit, valvonnan ja hälytykset eri IT järjestelmissä. (Techopedia, 2015)

SIEM-palvelun rakenne koostuu lokilähteistä, jotka lähettävät lokitietoja serverille tai suoraan SIEM-palveluun. Serverille kerätyt lokitiedot välitetään SIEM-palveluun. Lokitietojen kerääminen voi tapahtua SIEM-palvelun omilla agenteilla tai lokitiedot lähetään välissä olevalle serverille suoraan laitteen tai sovelluksen omilla ominaisuuksilla.

3.2 Käyttökohteita

Käyttökohteita on useita ja jokaisella on oma roolinsa. SIEM palvelun käyttökohteita ovat:

- Lokien keräys
- Lokien tallennus ja arkistointi
- Lokitietojen suodatus
- Lokitietojen muokkaus
- Analyysien teko
- Graaffinen esitys lokitiedoista
- Audiointi
- Käyttäjän seuranta
- Automaattiset hälytykset tapahtumien perusteella
- Tietoturva rikkeiden tutkinta
- Tietoturvan kehitys



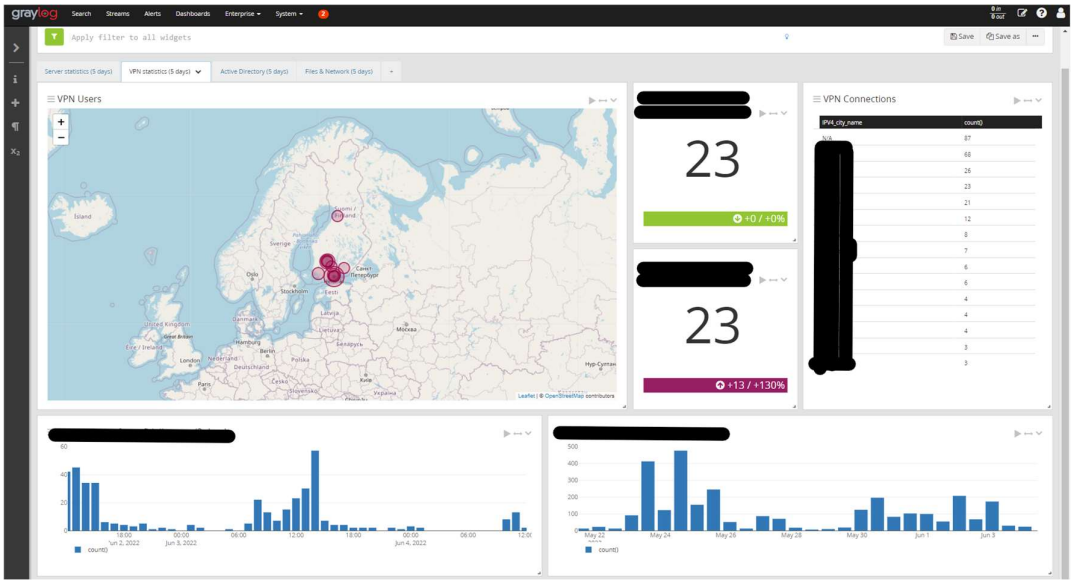
Kuva 3. SIEM-palvelun osa-alueet (Layots n.d.)

SIEM-palveluun eri palveluiden tai laitteiden tuoman lokitietojen avulla voidaan seurata koko ympäristössä tapahtuvia tapahtumia. Tällöin voidaan myös tutkia mahdollisia poikkeamia ja hyökkäyksiä. Kun palvelussa on ympäristön eri laitteet, voidaan luoda aikajana tapahtumista ja missä laitteissa on tapahtunut poikkeamia. Tällöin saadaan ymmärrys tapahtuman vakavuudesta. (Layots n.d.)

3.3 Graaffinen esittämien

Järjestelmistä tulee lokirivejä tuhansia useasti eri lähteistä ja ovat vaikea lukuisia. Lokirivien ymmärtäminen on haasteellista, joten niistä kannattaa muodostaa kaavioita. Graaffisen datan ymmärtäminen on helpompaa ihmiselle. Kuitenkaan ei voida unohtaa yksittäisen rivin tärkeyttä. Se voi merkitä hyvin paljon tai se muodostaa pienen osa isommasta kokonaisuudesta. Datan tulkinnassa käytetään aikavälejä, minuuteista, tunteihin, päiviin tai pidempiä aikavälejä.

Datan esittämisellä saadaan hyviä hyötyjä irti ja voidaan tuoda vaikeasti ymmärrettävä data helposti luettavaksi muillekin henkilöille, jotka eivät työskentele tietoturvan parissa.

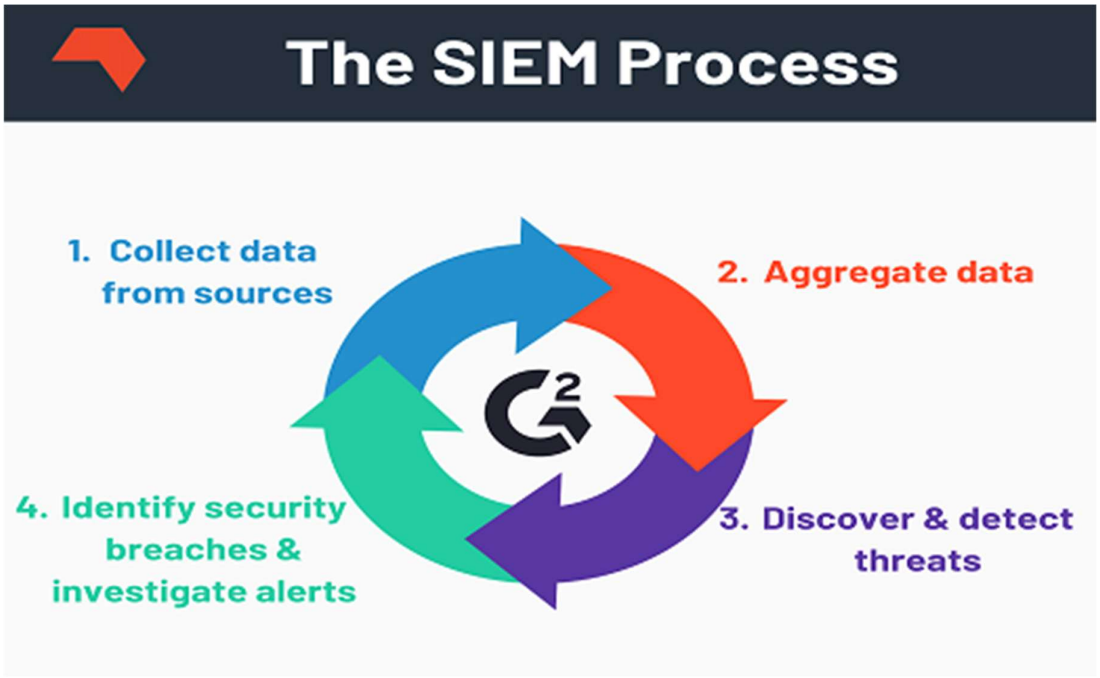


Kuva 4. OptoFidelity Graylog näkymä

Kuvasta nähdään OptoFidelity VPN yhteydet. Datan lukeminen lokiriveistä olisi mahdotonta, mutta kun data esitetään graafisesti, on helpompi ymmärtää ja tulkita dataa. Lisäksi, kun tiedetään keskiarvollinen yhteysmäärä, voidaan reagoida poikkeuksiin.

3.4 Käsittely

Jotta lokitiedoista saadaan hyötyä, pitää niitä käsitellä.



Kuva 5. SIEM-käsittely (Comodo n.d.)

SIEM-palvelussa lokitietojen käsittely aloitetaan lokitietojen tallennuksella. Järjestelmät tekevät sen automaattisesti ja siihen pystytään määrittämään ajanjakso, kuinka pitkältä ajalta lokitietoja säilytetään. Mitä pidemmältä ajalta lokitietoja säilytetään sitä parempi, mutta samalla kertyy data paljon ja prosessoinnista tulee raskaampaa.

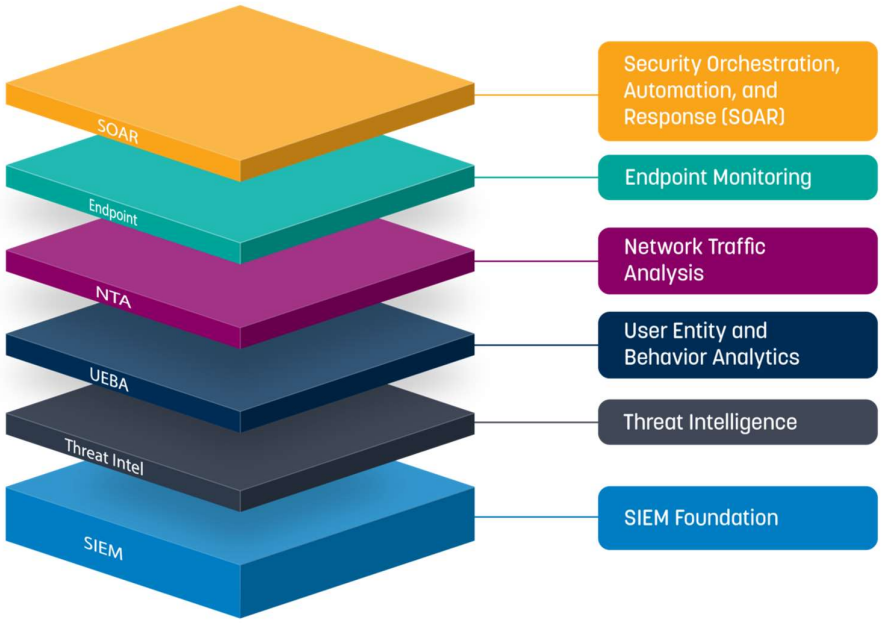
Pitemmän ajanjakson lokitiedoista voidaan seurata miten laitteen, palvelun tai käyttäjän toiminta muokkaantuu pitemmällä ajanjaksolla ja poimimaan eri muutokset.

Kun lokitietoja on kerätty, voidaan käsitellä dataa. Koska dataa on paljon, tarvitsee sitä suodattaa käyttötarkoituksen mukaisesti. Suodattamalla lokitietoja, saadaan haluttu data näkyviin kaikista lokitiedoista.

Suodatetusta lokitiedoista voidaan luoda automaattisia tapahtumia. Niiden luonnissa määritellään tarvittavat parametrit datalle, joista halutaan saada hälytyksiä. Tapahtumien ja hälytyksen tutkimisessa on tärkeää lokitietojen saatavuus. Jotta voidaan seurata tapahtumien kulkua. Tietoturva hyökkäyksen tutkinnassa on erittäin tärkeää pystyä seuraamaan, mistä, mihin ja mitä järjestelmissä on tehty murron aikana. (Comodo n.d.)

4 SOC ja SOAR

Security Operation Center, tietoturvakeskus on palvelu, mikä tuotetaan SIEM-palvelun pohjalta. SOC toiminta perustuu SIEM palveluun määriteltyjen hälytyksien tarkisteluun ja tutkimiseen. Eri hälytykset vaativat eri tason tutkimista ja osaamista. SOC-palvelut auttavat ylläpitämään järjestelmien tietoturvaa.



Kuva 6. SOAR-palvelu (Cybercode Technologies, n.d.)

SOAR, security orchestration, automation and response mahdollistaa hälytyksien reagoinnissa järjestelmän automaattiset toimenpiteet hälytykseen. Se vähentää vasteaikaa ja mahdollistaa järjestelmän ennalta määritellyt toimenpiteet tapahtumilla. Vasteajan vähentyminen auttaa estämään paremmin tietoturvahöykkäyksiä. SOAR-palveluissa on yleensä koneoppimista taustalla ja järjestelmä osaa havaita poikkeuksellista käyttämistä järjestelmissä. (Gartner Glossary n.d.)

5 SIEM-palvelun kehitys OptoFidelity:ssä

Projektin tavoitteena oli ymmärtää eri SIEM palveluita, tutkia nykyisen SIEM-palvelun kehittämisen jatkamista tai palvelun vaihtamista. Koska aikaisempi järjestelmä oli vain otettu käyttöön ja sen kehittämiseen ei ole ollut resursseja saatavilla silloin.

Kehitettävän tai uuden palvelun käyttöönoton tavoitteena oli pitää samat lokilähteet kuin nykyisessä järjestelmässä ja mahdollisesti tuoda uusia.

Projektissa oli tarkoitus myös tutkia palvelun mahdollisuutta tukea automaattisia toiminnallisuuksia ja datan analytiikka. Automaattiset toiminnallisuudet eivät kuitenkaan kuulunut opinnäytetyön projektin käyttöönottoon tai kehitykseen. Ainoastaan piti ymmärtää palvelun mahdollisuus niihin ja niitten toteuttaminen opinnäytetyön jälkeen jatkoprojektina.

5.1 Katselmus nykyiseen SIEM-palveluun

Nykyinen lokien kerääminen ja käsittely muistuttaa eniten SIM-palvelua. Kuitenkin järjestelmä on toteutettu Graylog SIEM-palvelua käyttäen.

Nykyinen järjestelmä kerää lokitietoja Linux- ja Windows -palvelimista ja verkkopuolen palveluista. Isoin osa tulee Micrsoftin palvelimista. Lokitiedot kerättiin joko suoraan Graylogin Linux serverille tai tuotiin Syslog palvelun kautta Graylogiin.

Tuotujen lokitietojen pohjalta on luotu eri palveluiden graafisia esitysmalleja. Palvelussa esitettiin, palvelimien kokonaisloki määrä per palvelin, VPN yhteyksien määrä, verkkolevyjen käyttö ja tiedostojen poisto, tulostimien käyttö, DNS pyynnöt, Microsoft Active Directoryn muokkaukset ja lisäykset ja virheelliset kirjautumiset.

Nykyisessä ympäristössä ei ole toteutettu automaattisia hälytyksiä. Koska seuranta on tehty ihmisten avulla, niin vasteaika ei ole samaa kuin automaattisissa hälytyksissä

6 SIEM-palveluiden vertaaminen

SIEM-palveluita on olemassa useita ja jokaisessa omat vahvuudet ja heikkoudet. Tutkimme nykyisen järjestelmän Graylog Enterprice ja Micrsoft Sentinel SIEM-palveluita.

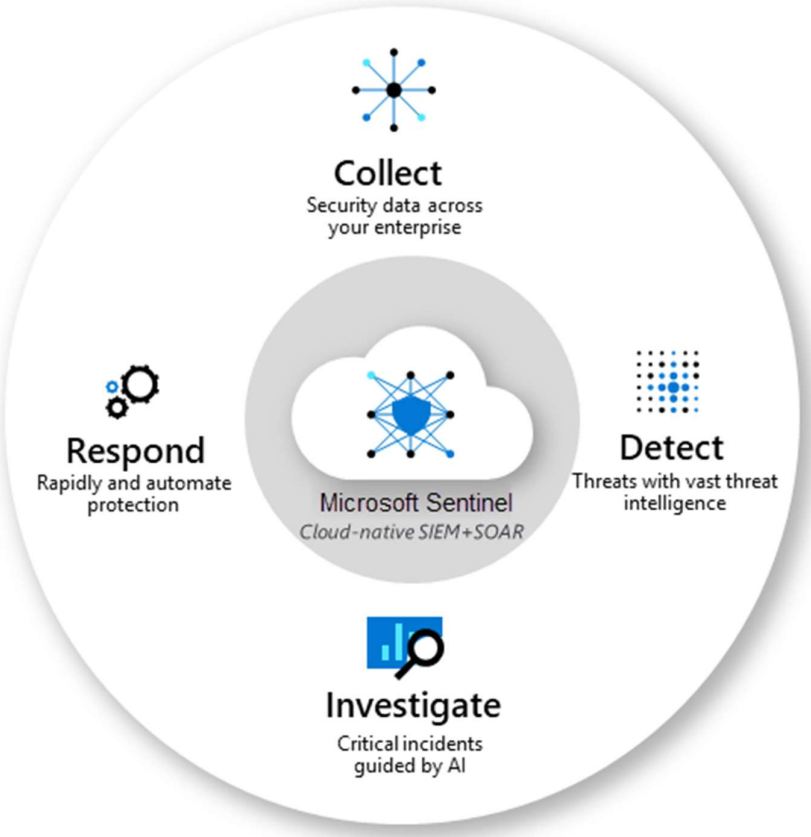
6.1 Graylog Enterprice

Graylog on Log Management ja SIEM-ratkaisu. Palvelun kehitys alkoi 2009 Hampurissa, perustajana Lennart Koopman. Hän alkoi kehittämään avoimen lähdekoodin Log Management ja SIEM ratkaisua. Tuotteen ensimmäinen asiakasjulkaisu oli 2016 ja käyttäjiä palvelulla on yli 50 tuhatta vuonna 2022.

Palvelu on toteutettu ohjelmana ja toimii Linux käyttöjärjestelmässä. Palvelu on toteutettu JAVA ohjelmistokielellä ja tietokanta on MongoDB. Palvelu mahdollistaa SIEM palvelun eri ominaisuuksia, lokien keräys ja arkistointi, suodattaminen, graaffiset esitytavat. (About Graylog n.d.)

6.2 Microsoft Sentinel

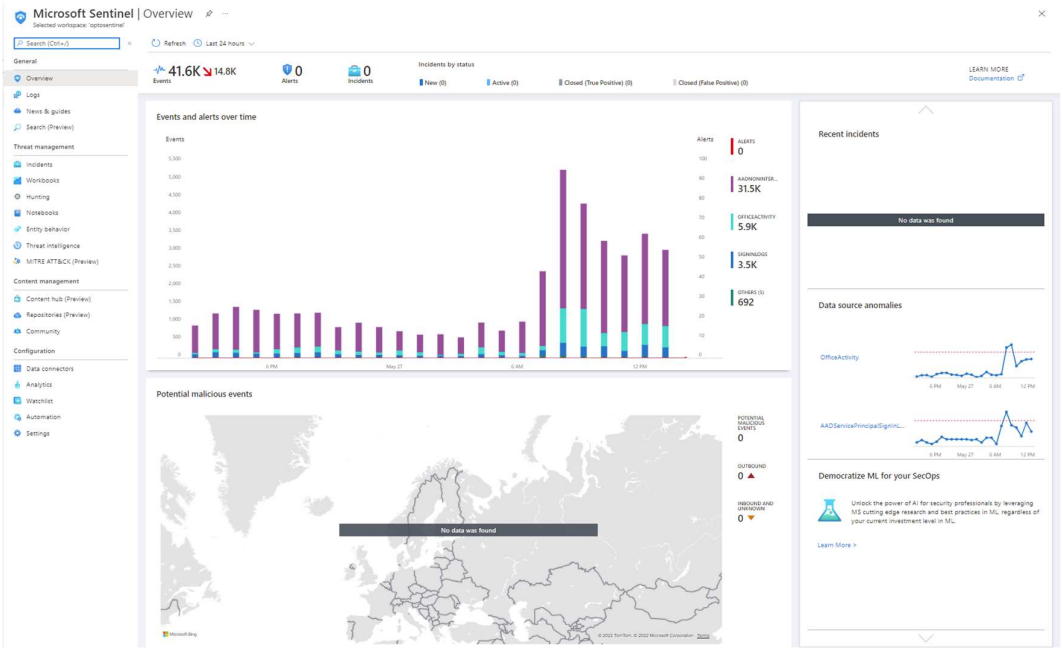
Pilvipohjainen SIEM, SOC ja SOAR palvelu.Microsoftin julkaisi palvelun 2019 syyskuussa nimellä Azure Sentinel. Palvelu on toteutettu Microsoft Azure ympäristöön. Palvelu toteuttaa SIEM ratkaisuja, mahdollistaa SOC toimintaa ja sisältää SOAR ominaisuuksia. Palveluun voidaan tuoda lokitiedot ja niitä voidaan käsitellä. Ja niistä voidaan tehdä graafisia kaavioita eli Workbookeja.



Kuva 7. Microsoft Sentinel -palvelun kuvaus. (What is Microsoft Sentinel?, 2022)

Lokitietoja voidaan myös analysoida, käyttäen Micrsoftin tekoälyä. Lokitiedoista voidaan etsiä ja tutkia niitä käyttämällä Hunting ominaisuutta. Microsoft Sentinel mahdollistaa myös hälytyksiin automaattisia toimenpiteitä, Playbooks.

Microsoft Sentinel mahdollistaa eri kehittäjien tuottamien lokilähteiden, graafiset kaaviot, data analysoinnin, ja automaattisten toimenpiteiden tuonnin käyttämällä palvelun Content Hub:ia.



Kuva 8. Micrsot Sentinel portaalin näkymästä

Palvelun perusnäkymää voi muokata ja siinä voi esittää haluttua data. (Dispensa, 2019)

6.3 SIEM-palvelun valinta

SIEM-palvelun valinta ei ollut helppo, kuitenkin selkeiden näkemyksien myötä päädyttiin aloittamaan Microsoft Sentinelin käyttöönotto. Koska yrityksen eri palvelimet ja palvelut oltiin viemässä pilvipalveluihin ja suureksi osaksi Micrsoftin Azure ympäristöön. Oli järkevää toteuttaa lokien kerääminen ja käsittely saman palvelun sisällä. Microsoft eri lisenssit mahdollistivat tietyt Microsoftin omien palveluiden lokien siirtämisen ilmaiseksi Microsoft Sentinel -palveluun. Suurin osa kerättävästä lokitiedoista oli peräisin Microsoft palveluista ja integraatiot helpottivat SIEM-palvelun käyttöönottoa.

Jos olisi haluttu jatkaa Graylog:n kehittämistä, vaihtoehtoina olisi ollut siirtää lokitiedot Micrsoftin Azuresta omalle palvelin ympäristöön ja sieltä siirretty sieltä Graylog-palveluun. Tai vaihtoehtoisesti aloitettu migraatio Graylog Enterprices ja Graylog Cloud välillä. Kuitenkin lokitiedot haluttiin pilvipalveluun ja pois omasta palvelin ympäristöstä.

7 Microsoft Sentinel käyttöönotto prosessi

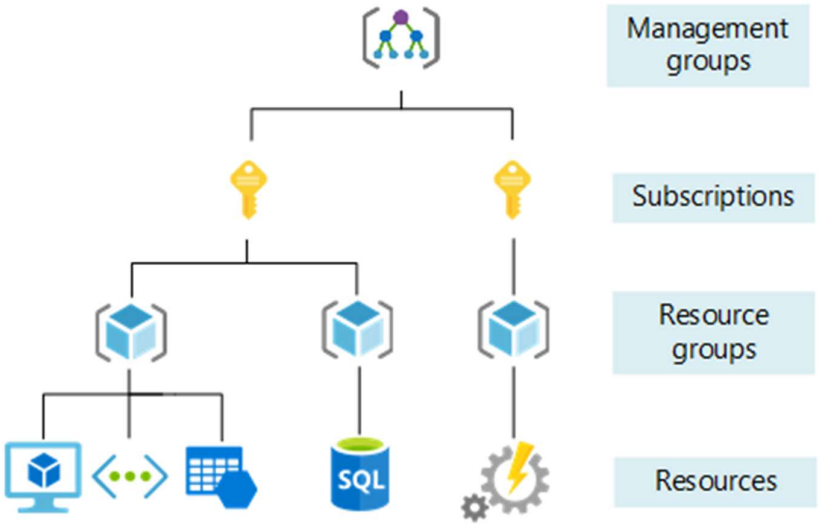
Tarkoituksena oli toteuttaa Microsoft Sentinelin käyttöönotto ja tuoda yleisemmät Azure palvelussa olevien palveluiden lokitiedot Microsoft Sentinel palveluun. Microsoftin omat palvelut, Azure Active Directory ja M365. Tavoitteena oli saada luotua Micrsoft Sentinel perusympäristö ja kartoittaa Sentinelin laajentamisen mahdollisuudet lokitietojen keräämiseen muista yrityksen palvelimilta. Lokitiedoista oli tarkoitus toteuttaa graafinen esitystapa. Käyttöönotossa selvitettiin Microsoft Azure ympäristöä ja Microsoft Sentinel -palvelun asetuksien määrittämistä.

Microsoft Azuren hinnat vaihtelivat eri data keskuksien välillä ja tilaaja voi valita vapaasti haluamansa data keskuksen. Koska Microsoftin lokitiedoissa on henkilötietoihin viittaavaa tietoja, haluttiin pitää data Euroopan sisällä. Henkilötietoja vastaavan tiedon siirtämistä Euroopan alueen ulkopuolelle, olisi vaatinut omat selvitykset ja hyväksynnät. Joten data pidettiin Euroopan alueella.

Microsoftin omat laskurit määrittivät hinnat Microsoft Sentinel palvelulle ja Graylogin datan perusteella voitiin tehdä arvioita laskuriin. Liitteiden 1 ja 2 vertailulla voitiin sanoa hinta North Europe (Irlanti) oli halvempi vaihtoehto kuin West Europe (Alankomaat). Kuitenkin käytettiin West Europen data keskusta, koska latenssi ja muut OptoFidelity:n Resource group:t ovat myös Alankomaan datakeskuksessa.

7.1 Micrsoft Azure Resource group

Microsoft Sentinel käyttöönotto vaati Microsoft Azure palvelun ja tilauksen. OptoFidelityllä oli kummatkin, joten piti vain luoda uusi Azuren Resource group.

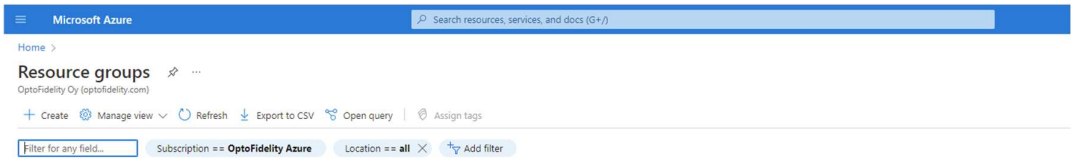


Kuva 9. Azure rakenne (Organize your Azure resources effectively, 2021)

Microsoft Azure:n Resource Groups mahdollistavat eri palveluiden jakamisen usealle eri Resource Group:lle. Tällöin pystytään erittelemään yrityksen eri palveluita Microsoft Azure:n sisällä, jolloin käyttäjänhallinta on helpompaa. Eri Resource group:t voivat kommunikoida keskenään, jos se sallitaan. Resource Group avulla pystyttiin myös erottamaan eri palvelut tilauksen laskulle, mikä helpotti talouspuolta.

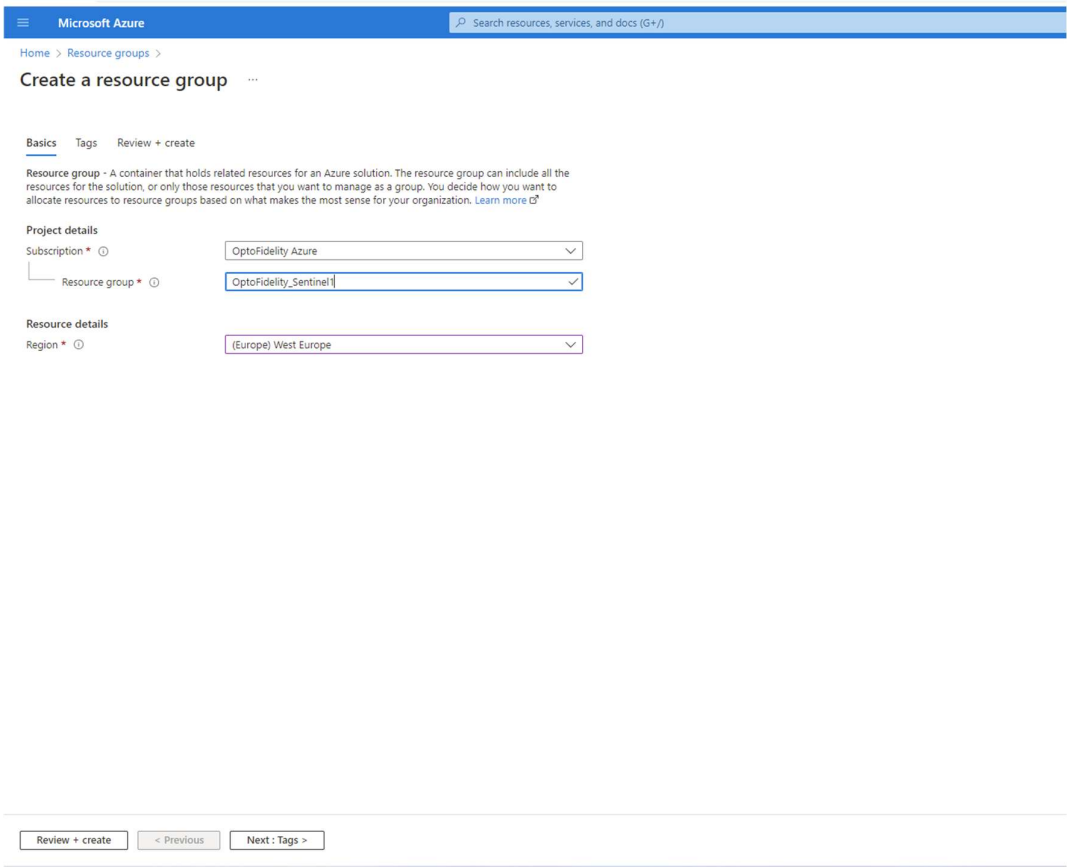
7.2 Microsoft Azure Resource group käyttöönotto

Microsoft Azure Resource group käyttöönotto toteutettiin Microsoftin Azure portaalissa. Käyttöönotto oli suoraviivainen prosessi.



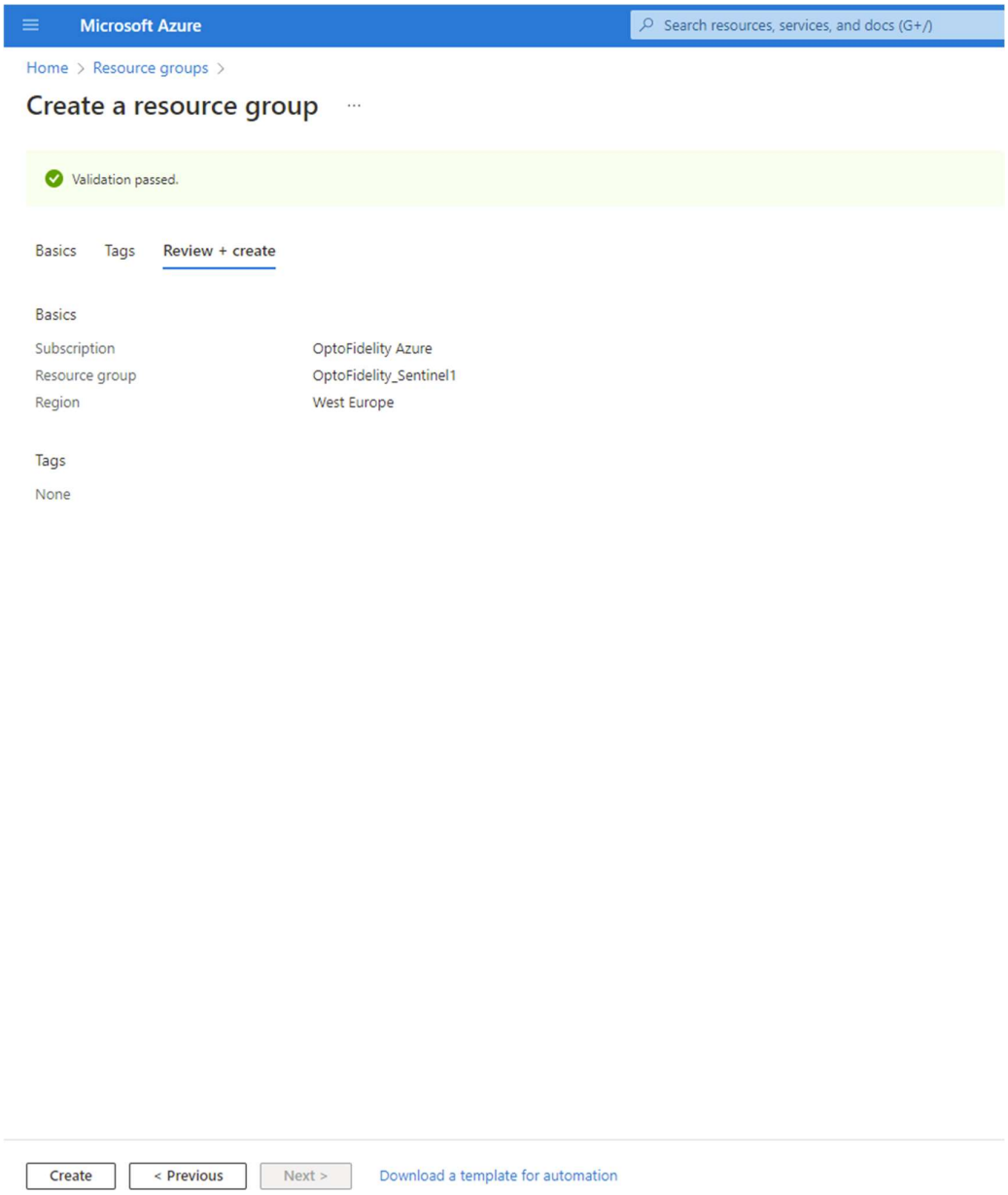
Kuvakaappaus 3. Azure Resource group teko.

Käyttöönotto prosessi aloitettiin etsimällä Resource Groups hallinta.



Kuva 10. Azure Resource group nimeäminen

Nimettiin resource group ja nimeksi annettiin OptoFidelity_Sentinel. Samassa vaiheessa määriteltiin lisäksi Micrsodtf Azure tilaus ja mihin alueen datakeskukseen Resource group lisättiin. Valittu aikaisemman pohdinnan mukaisesti Länsi-Eurooppa, Europe West Europe.

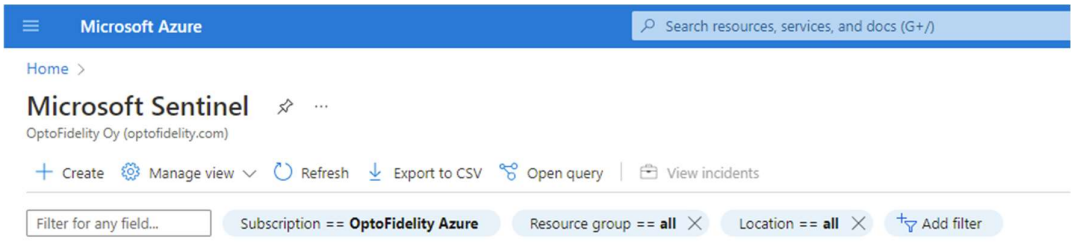


Kuva 11. Azure Resource group määritysten tarkistus

Kun määritykset oli tehty ja tarkistettu, luotiin uusi Reseurce group. Microsoft Sentinel voi ottaa myös käyttöön jo olemassa olevaan Resourse group:iin. Resource group:n käyttöönoton jälkeen, käyttöönottoa jatkettiin Log analytics:n määrittämisellä.

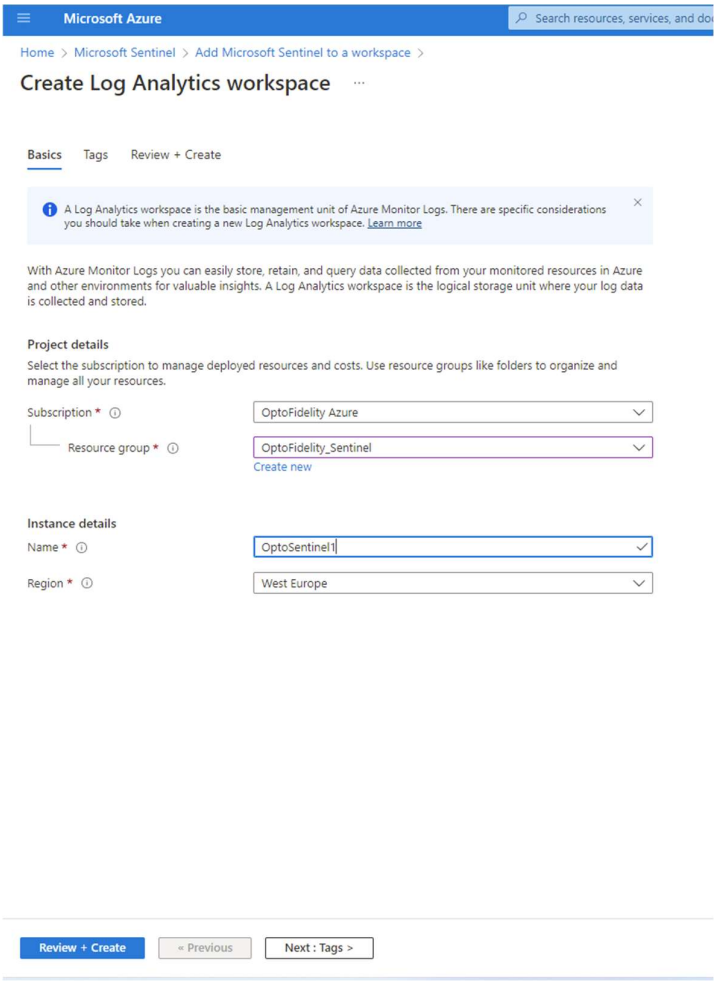
7.3 Log Analytics käyttöönotto

Luotiin Log Analytics workplace, mikä liitettiin Resource Grouppiin OptoFidelity Sentinel.



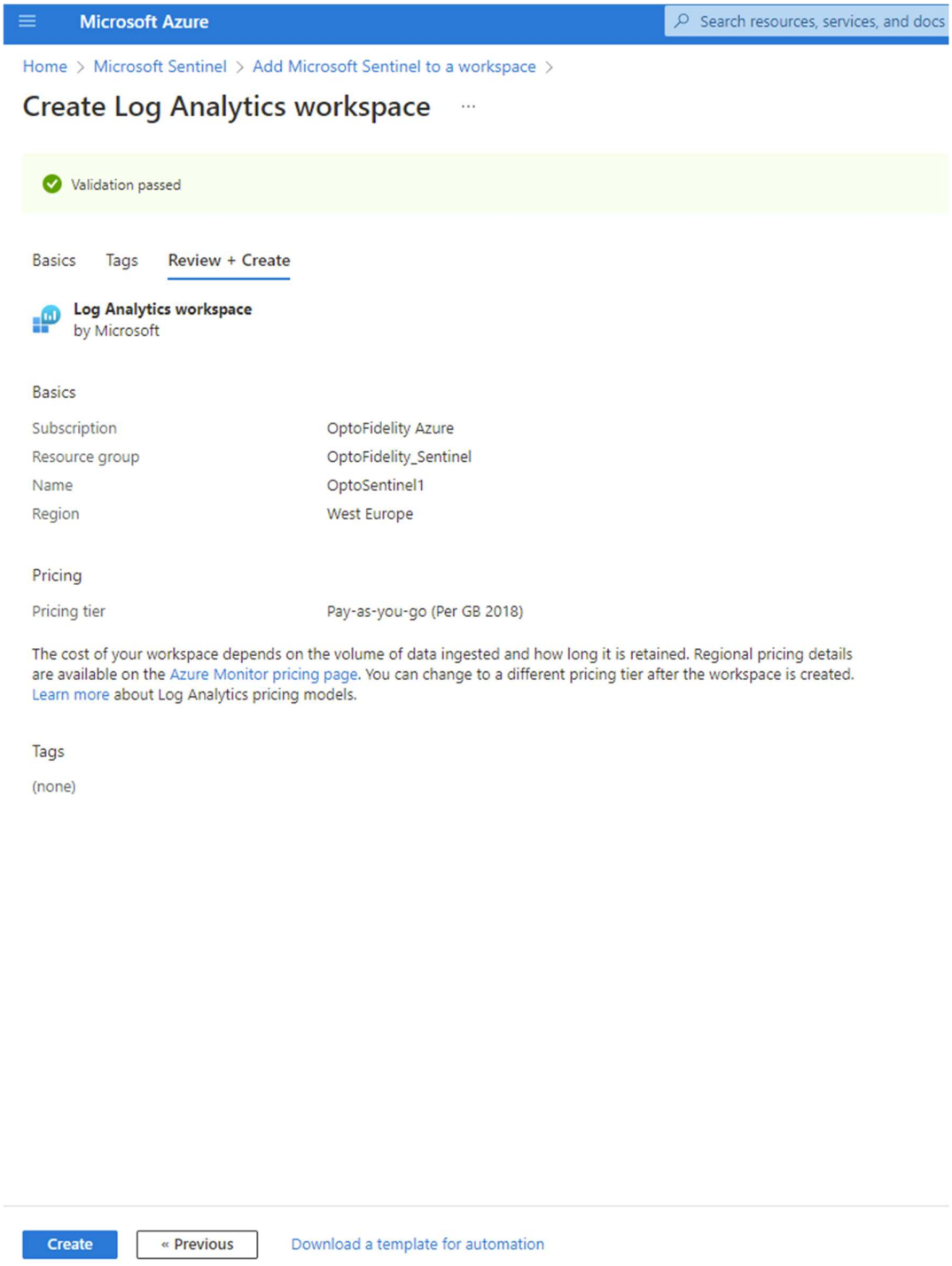
Kuva 12. Log Analytics workplace teko

Log Analytics käyttöönotto tehtiin Microsoft Sentinel alta, ja luotiin uusi Log analytics worksplace.



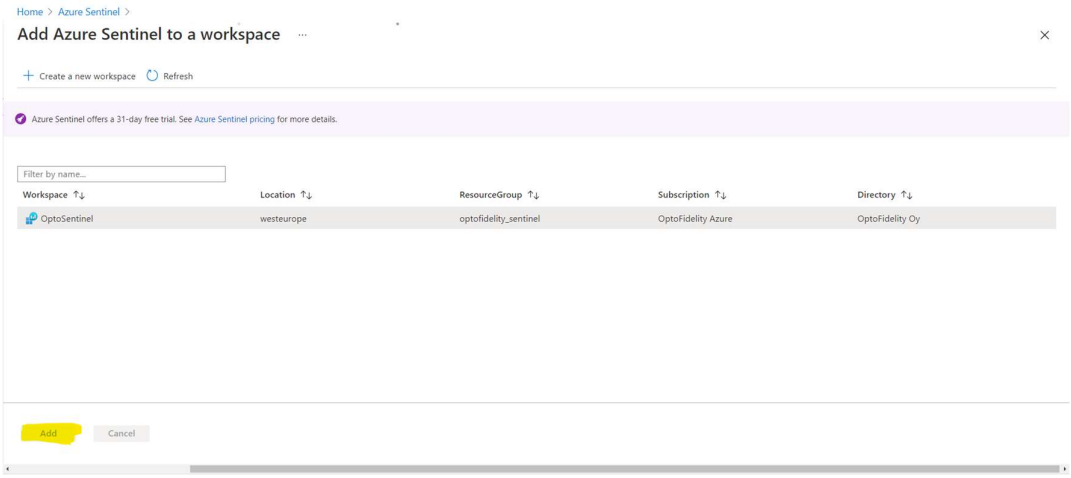
Kuva 13. Log Analytics workplace määritys

Käyttöönotossa määriteltiin Azure tilaus, OptoFidelity Azure. Resource Groupiksi valittiin äsken tehty OptoFidelity_Sentinel. Ja se nimettiin OptoSentinel:ksi ja valittiin alueeksi West Europe.



Kuva 14. Log Analytics workplace määritysten tarkistus

Tarkistuksen jälkeen luotiin Log Analytics workspace, mihin liitettiin Microsoft Sentinel.



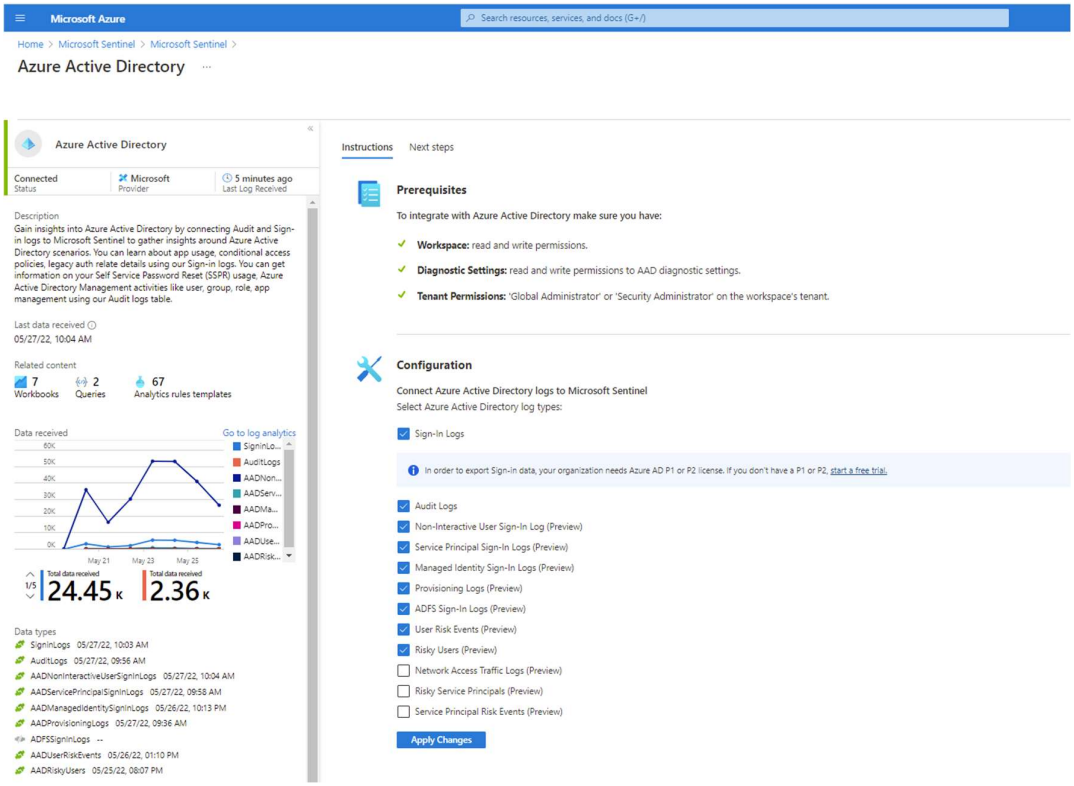
Kuva 15. Microsoft Sentinel lisäys

Log Analytics workspace alle lisättiin Microsoft Sentinel. Määrityksien jälkeen oli luotu tarvittavat ympäristöt Microsoft Sentinel toiminnalle ja voitiin alkaa määrittämään Microsoft Sentinel:ä. (Quickstart: On-board Microsoft Sentinel, 2022)

7.4 Data Connectoreiden lisäys.

Lokilähteiden lisäys toteutettiin Microsoft Sentinelissä Connectoreiden avulla. Microsoft:lla oli laaja valmis valikoima, josta löytyi Microsoftin omien palveluiden Data connector:ta ja muiden yrityksien Data connector:ta. Microsoft kehittää jatkuvasti omia palveluita ja niiden määrä on myös kasvanut huimasti alkupäivistä. (Microsoft Sentinel data connectors, 2021)

Microsoft oli toteuttanut eri Data Connector:den lisäämisen yksinkertaiseksi ja helpoksi.



Kuva 16. Azure Active Directory data connector:n lisäys

Data Connectorin lisäys tehtiin Data Connectors alta. Valittiin haluttu palvelu ja yllä olevan esimerkki kuvan mukaisesti lisättiin Azure Active Directory. Valittiin halutut lokilähteet ja hyväksyttiin muutokset. Alla listattu yhdistetyt Data Connectorit

Yhdistetyt lokilähteet:

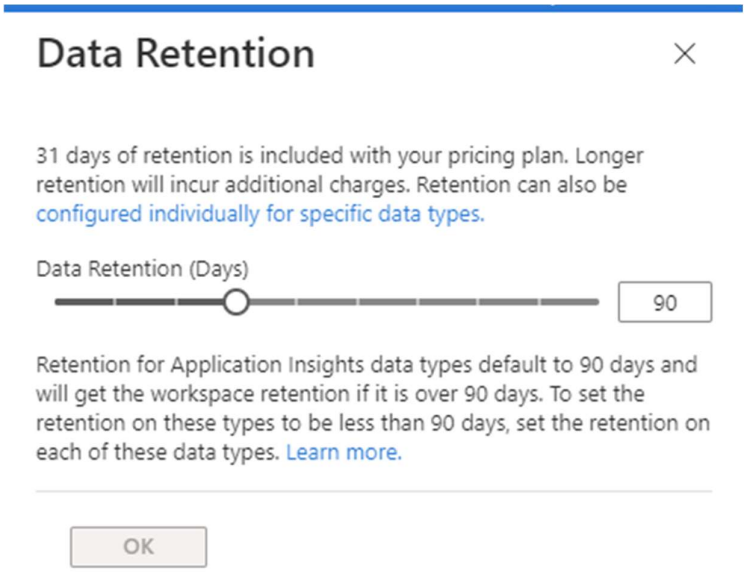
- Azure Active Directory
- Sing-In Logs
- Audit Logs
- Service Principal Sign-In Logs (Preview)
- Managed Identity Sign-In Logs (Preview)
- Provisioning Logs (Preview)
- ADFS Sign-In Logs (Preview)
- User Risk Events (Preview)
- Risky Users (Preview)
- Azure Active Directory Identity Protection
- Office 365
- Exhange
- SharePoint
- Teams

Yhdistetyillä lokilähteillä seurattiin Microsoft ympäristön tapahtumia hyvin ja saatiin tietoon Microsoft:n palveluihin kirjautumiset ja Microsoft avulla tehdyt kirjautumiset toisiin palveluihin. Henkilöihin tai ryhmiin tehdyt muutokset. (Integrate Azure AD logs with Azure Monitor logs, 2021)

Office365 lokitietojen avulla voitiin seurata Microsoftin M365 ympäristön lokitietoja sähköposteista tiedostojen jakoon.

7.5 Lokien säilytys

Kerättyjä lokeja haluttiin säilyttää Microsoft Sentinel:ssä 90 päivän ajan. Koska yrityksen asiakasvaatimukset määrittivät lokien tallessa pidon. Jos lokeja säilytetään yli 90 päivän ajan Micrsosoft Sentinel laskuttaa niistä.

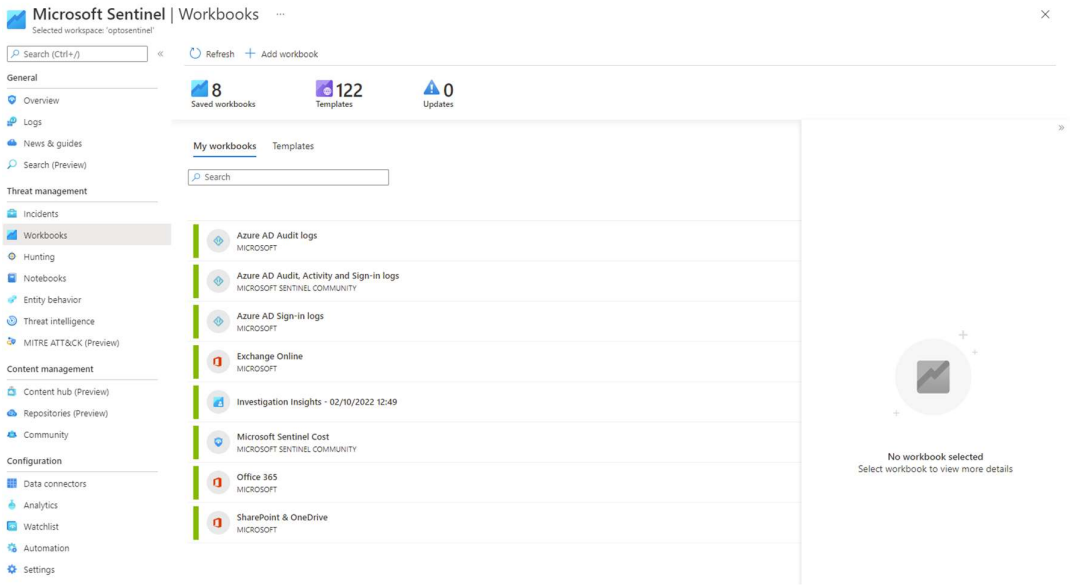


Kuva 17. Lokien säilytyksen määritys

Lokitietojen säilytyksen asetuksia muokattiin Log Analytics workspace puolella kohdassa Usage and estimated cost.

7.6 Workbooks

Micrsoft Sentinel:ssä on mahdollista esittää kerätyistä lokitiedoista graafista data. Microsoft Sentinelissä graafisen datan näkymästä käytetään nimitystä Workbooks. Worksbooks voi olla useita ja useampi helpoittaa eri lähteistä kerätyn datan esittämistä. Workbookit ovat interaktiivisia ja niitä voi muokata halutun tarkoituksen mukaisesti.

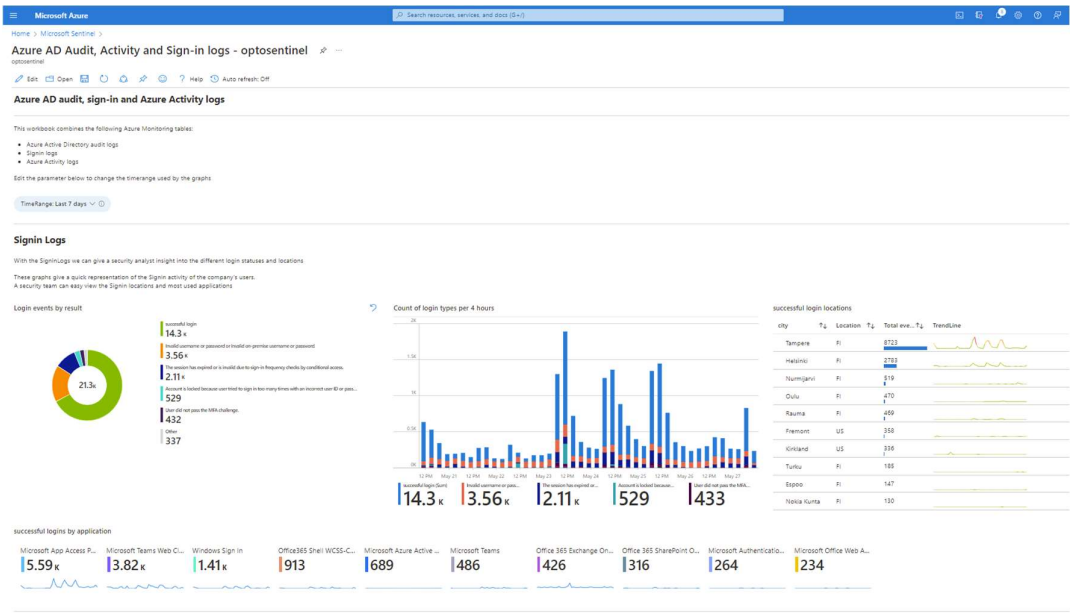


Kuva 18. Lisätyt Workbooksit

Microsoft Sentinel:ssä oli valmiita pohjia eri palveluiden lokitietojen näyttämiseen. Workbookit oli toteutettu Micrsoft Sentinel:ssä käytettävän ohjelmointikielen KQL avulla. Valmiissa pohjissa halutun palvelun lokitietojen haku oli tehty valmiiksi ja käyttöönotto tehtiin parin klikkauksen avulla.

Lisätyt Workbookit Microsoft Sentinel:iin:

- Azure AD Audit Logs
- Azure AD Audit, Activity and Sign-in logs
- Exhange Online
- Microsoft Sentinel Cost
- Office 365
- SharePoint & Onedrive



Kuva 19. Azure AD Audit Workbooks

Kuvassa esimerkki Workbookin näkymästä. Workbooks sisältöä voi muokata halutun näköiseksi. Kuitenkin on haluttu pysyä mahdollisimman paljon alkuperäisessä.

8 Projektin jatkosuunnitelma

Projektin käyttöönotto oli pintapuolinen ja keskittyi Microsoftin omien palveluiden lokitietojen lisäämiseen, käsittelyyn ja graafiseen esittämiseen.

Microsoft Sentinel -palveluun on tarkoitus siirtää nykyinen SIEM-palvelu lokilähteineen ja lisätä yrityksen eri palvelimia myös.

Projekti jatkuu yhteistyökumppanin avustuksella ja OptoFidelityn Internal IT siirtyy valvomaan projektin kehittämistä. Sen sijaan, että tekisi työtä eteenpäin.

Seuraavat askeleet projektin jatkamisessa on löytää sopiva yhteistyökumppani, jolla on osaamista SIEM, SOC ja SOAR puolelta. Koska Microsoft kehittää jatkuvasti omia ympäristöjä ja tuo lisää ominaisuuksia, on tärkeää, että yhteistyökumppanilla on osaamista useista Microsoft:n palveluista. Silloin he voivat tarjota OptoFidelity:lle parhaan kehittämistyön ja käytön tuen.

9 POHDINTA

Opinnäytetyön projektin toteutus oli haasteellinen prosessi. SIEM-palveluiden eri osa-alueiden ymmärtäminen oli haasteellista

Jotta vertailua kahden palvelun välillä voitiin tehdä, täytyi myös tietää ja ymmärtää yrityksen muut kehityskohteet. Niitä tässä työssä ei ole listattu. Vertailun toteuttaminen palveluiden välillä oli muutoin suoraviivaista ja yrityksen muut kehityskohteet määrittivät paljolti toteutusta.

Seuraava haaste oli ymmärtää laaja, vaikeasti ymmärrettävä Microsoft Azure ympäristö. Microsoft kehittää jatkuvasti omia tuotteita ja he nimeävät palveluita uudestaan. Se aiheutti myös haasteita tiedon löytämisen suhteen ja hakua piti tehdä vanhan ja uuden nimen mukaan. Tämän opinnäytetyön aikana Microsoft Azure Sentinel nimettiin uudelleen nykyiseen nimeen, Microsoft Sentinel.

Microsoft Sentinel käyttöönotossa haluttiin hyödyntää kolmannen osapuolen konsultointia. Kuitenkin prosessin aikana havaitut asiat tekivät siitä mahdotonta ja toteutus päätettiin tehdä ilman konsultointia. Tällöin tieto piti etsiä muualta ja se hidasti prosessia.

Toteutus saatiin tehtyä hieman kapeammalla määrällä, kuin tavoitteissa oli alunperin. Kuitenkin tavoitteita muokattiin projektin aikana vastaamaan työmäärää.

Lisäksi projektin jatkosuunnitelma palvelee hyvin yritystä ja oma osaaminen yrityksessä auttaa viemään projektia eteenpäin kumppaneiden kanssa.

LÄHTEET

About Graylog. n.d. Graylog. Verkkosivu. Viitattu 29.5.2022. https://www.graylog.org/about

Applebee, G. 18.6.2015. Benefits of Log Consolidation in a SIEM Environment. Verkkosivu. Viitattu 29.5.2022. https://www.pratum.com/blog/122-benefits-of-log-consolidation-in-a-siem-environment

Awati, R. 5.2022. Security information management (SIM). Verkkosivu. Viitattu 29.5.2022. https://www.techtarget.com/searchsecurity/definition/security-information-management-SIM

Braden, A. 24.5.2021. Log. Verkkosivu. Viitattu 29.5.2022. https://www.webopedia.com/definitions/log/

Dispensa, S. 26.9.2019. Azure Sentinel general availability: A modern SIEM reimagined in the cloud. Verkkosivu. Viitattu 29.5.2022.

Integrate Azure AD logs with Azure Monitor logs. 31.12.2021 Microsoft azure. Verkkosivu. Viitattu 29.5.2022. https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

Kent, K., Souppaya, M. 9.2006. Guide to Computer Security Log Management. Verkkosivu. Viitattu 29.5.2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Log Formats. 15.1.2020. Graylog. Verkkosivu. Viitattu 29.5.2022. https://www.graylog.org/post/log-formats-a-complete-guide#:~:text=A%20log%20format%20is%20a,management%20system%20that%20supports%20them

LogViewPlus. n.d. LogViewPlus. Kuva. Viitattu 1.6.2022

https://www.logviewplus.com/

Microsoft Sentinel data connectors. 18.11.2021. Microsoft Azure. Verkkosivu. Viitattu 29.5.2022. https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

Organize your Azure resources effectively. 23.12.2021. Microsoft Azure. Kuva. Viitattu 29.5.2022 https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

Quickstart: On-board Microsoft Sentinel. 26.5.2022. Microsoft Azure. Verkkosivu. Viitattu 29.5.2022. https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

Security Event Management. 8.4.2021. Techopedia. Verkkosivu. Viitattu 29.5.2022. https://www.techopedia.com/definition/25763/security-event-management#:~:text=Security%20event%20management%20(SEM)%20is,software%2C%20system%20or%20IT%20environment

Security Information and Event Management (SIEM) Solution & it's importance. n.d. Layots. Verkkosivu. Viitattu 29.5.2022. https://layots.com/security-information-and-event-management-siem-solution-its-importance/

Security Orchestration, Automation and Response (SOAR). n.d. Gartner Glossary. Verkkosivu. Viitattu 29.5.2022. https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

SIEM & SOAR. n.d. Cybercode Technologies. Kuva. Viitattu 29.5.2022 https://www.cybercodetech.com/portfolio/31-siem

What is Microsoft Sentinel?. 6.5.2022. Microsoft Azure. Kuva. Viitattu 29.5.2022 https://docs.microsoft.com/en-us/azure/sentinel/overview

What is SIEM?. n.d. Comodo. Verkkosivu. Viitattu 29.5.2022. https://www.comodo.com/what-is/the-siem-process.php

Wigmore, I. 1.2026. Log management. Verkkosivu. Viitattu 29.5.2022.
https://www.techtarget.com/searchitoperations/definition/log-management

Microsoft Azure Estimate					
Your Estimate					
Service type	**Custom name**	**Region**	**Description**	**Estimated monthly cost**	**Estimated upfront cost**
Microsoft Sentinel		West Europe	3 daily ingested logs (GB), 3 total retention (months)	€420,96	€0,00
Support			**Support**	€0,00	€0,00
			Licensing Program	**Microsoft Customer Agreement (MCA)**	
			Billing Account		
			Billing Profile		
			Total	**€420,96**	**€0,00**
Disclaimer					
All prices shown are in Euro Zone – Euro (€) EUR. This is a summary estimate, not a quote. For up to date pricing information please visit https://azure.microsoft.com/pricing/calculator/					
This estimate was created at 11/17/2021 7:44:13 AM UTC.					

Microsoft Azure Estimate					
Your Estimate					
Service type	Custom name	Region	Description	Estimated monthly cost	Estimated upfront cost
Microsoft Sentinel		West Europe	3 daily ingested logs (GB), 3 total retention (months)	€420,96	€0,00
Support			Support	€0,00	€0,00
			Licensing Program	Microsoft Customer Agreement (MCA)	
			Billing Account		
			Billing Profile		
			Total	€420,96	€0,00
Disclaimer					
All prices shown are in Euro Zone – Euro (€) EUR. This is a summary estimate, not a quote. For up to date pricing information please visit					
This estimate was created at 11/17/2021 7:44:13 AM UTC.					