Haaga-Helia
ammattikorkeakoulu Oy

Microsoft Sentinel: Pilvipohjaisen SIEM-ratkaisun käyttöönotto ja parhaat käytännöt

Oliver Lahti

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2021

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä
Oliver Lahti

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Microsoft Sentinel: Pilvipohjaisen SIEM-ratkaisun käyttöönotto ja parhaat käytännöt

Sivu- ja liitesivumäärä
38

Organisaatioiden omaksuessa uusia tietoteknisiä ratkaisuja, kasvaa julkipilvipalvelujen käytön määrää vauhdikkaasti. Samalla tarve kokonaisvaltaiselle tietoturvahäiriöhavainnoinnille kasvaa, niin paikallisissa kuin pilviympäristöissä. SIEM-tuotteet ovat yleistyvä ratkaisu vastaamaan lokien hallinnan sekä poikkeavien tapahtumien havainnointiin hybridiympäristöissä.

Opinnäytetyön tarkoituksena oli selvittää toiminnallisen tutkimuksen avulla, miten yritys ottaa käyttöön pilvipohjaisen SIEM-ratkaisun parhaita käytäntöjä noudattaen. Työssä käytettiin toimintatutkimusta, jossa tutkija osallistuu tutkittavan kohteen eli SIEM-ratkaisun käyttöönottoon. Tutkimuksessa oli olennaista, että tutkija työskentelee itse yrityksessä ja tuntee tutkimuskohteen.

Toimeksianto keskittyi Microsoft Sentinel SIEM-tuotteen tutkimiseen ja käyttöönoton kuvaamiseen. Tutkimus toteutettiin keskittyen Microsoft Sentinelin ydintoiminnallisuuksiin, sisältäen tietoturvakriittisten lokien hallinnan, tietoturvahäiriöiden havainnoinnin SIEM-ratkaisulla sekä automaation hyödyntämisen. Toimeksiantoon tutkittiin myös Microsoft Sentinel -ratkaisun parhaita käytäntöjä kustannusten hallinnan, muiden tietoturvatuotteiden integraation sekä datan visualisoinnin osalta.

Toimeksiannon tuloksena tuotettiin parhaiden käytäntöjen kuvaus Microsoft Sentinelin käyttöönottoon vaikuttavista osa-alueista Sulava Oy:n käytettäväksi. Toimeksiannon dokumentoituja kuvauksia voidaan käyttää niin uusissa käyttöönotoissa kuin jo käyttöönotettujen ympäristöjen jatkokehityksessä.

Asiasanat
Microsoft Sentinel, SIEM, Tietoturva, Pilvipalvelut, Microsoft Azure, XDR

Sisällys

Käsitteet 1
1 Johdanto 2
1.1 Tausta 2
1.2 Tavoitteet ja toimeksiantaja 2
2 Tietoturva Microsoftin pilviympäristössä 4
2.1 Azure Active Directory Identity Protection 5
2.2 Microsoft 365 Defender for Endpoint 5
2.3 Microsoft 365 Defender for Identity 6
2.4 Microsoft 365 Defender for Office 365 6
2.5 Microsoft Defender for Cloud Apps 7
2.6 Microsoft Defender for Cloud 7
2.7 Microsoft Sentinel 8
3 Microsoft Sentinelin käyttöönotto 11
3.1 Vaatimukset 11
3.2 Log Analytics 11
3.3 Microsoft Sentinel 12
3.4 Kustannusten hallinta 13
3.4.1 Log Analyticsin hinnoittelu 14
3.4.2 Microsoft Sentinelin hinnoittelu 15
3.4.3 Ratkaisun kokonaishinta 16
3.5 Datalähteiden määritys ja liittäminen 16
3.5.1 Azure Active Directory 17
3.5.2 Office 365 18
3.5.3 Azure Activity 19
3.5.4 Microsoft 365 Defender -tuotteet 20
4 Tietoturvauhkien havainnointi 24
4.1 Jatkuva havainnointi 24
4.1.1 Automaation hyödyntäminen 25
5 Datan visualisointi 27
5.1 Workbook-näkymien muokkaaminen 27
6 Yhteenveto ja pohdinta 29
Lähteet 32
Liitteet 35

Käsitteet

ARM	Azure Resource Manager, Azuren hallinnointiin tarkoitettu palvelu
AWS	Amazon Web Services, Amazonin julkinen pilvipalvelualusta
Azure	Microsoftin julkinen pilvipalvelualusta
CASB	Cloud Access Security Broker, pilvitietoturvan monipuolinen valvontaratkaisu
Datalähde	Lokidataa luova lähde, tyypillisesti sovellus tai palvelu, joka tukee lokien siirtämistä toiseen sijaintiin
Dataliitin	Tekninen ratkaisu, joka mahdollistaa datan siirtämisen sijainnista toiseen
EDR	Endpoint Detection and Response, päätelaitevalvonnan ratkaisu
GCP	Google Cloud Platform, Googlen julkinen pilvipalvelualusta
IaaS	Infrastructure As A Service, infrastruktuuri tarjottuna palveluna
IOC	Indicator Of Compromise, tietoturvassa käytetty nimike uhkatiedolle
Konesali	Sijainti, jossa pilvipalvelutarjoaja ylläpitää vaadittua laitteistoa, jolla palveluja tarjotaan
KQL	Kusto Query Language, Microsoftin kyselykieli
PaaS	Platform As A Service, alusta tarjottuna palveluna
PAYG	Pay-As-You-Go, Azuressa käytettävä hinnoittelumalli
Rooli	Pääsynhallinnassa käytetty nimitys, joka kuvaa tiettyä pääsytasoa
SaaS	Software As A Service, sovellus tarjottuna palveluna
SOAR	Security Orchestration, Automation and Response, automaatiotoimien sekä integration ulkoisiin alustoihin mahdollistava ratkaisu
SOC	Security Operations Center, tietoturvavalvomo
XDR	Extended Detection and Response, useista tietoturvatuotteista koostuva ympäristön valvontaan ja korjaaviin toimenpiteisiin keskittyvä kokonaisuus

1 Johdanto

1.1 Tausta

Pilvipalvelujen yleistyessä ja palvelujen käytön laajentuessa oman organisaation konesalien ulkopuolelle, siirtyy myös tietoturvan ylläpitämisen tarve uuteen ympäristöön. Yleinen ongelma tietoturvalle oleellisten tapahtumien valvonnassa, joka koskee niin uusia pilviympäristöjä kuin vanhoja paikallisympäristöjä on näkyvyyden puute. SIEM (Security Information and Event Management) -tuotteet ovat tyypillinen ratkaisu puutteellisen näkyvyyden paikkaamiseen. SIEM-ratkaisun tavoitteena on tuottaa kattava kokonaiskuva ympäristön tietoturvasta keräämällä lokeja määrätyistä lähteistä ja havaitsemalla poikkeavia tapahtumia, tietoturvahäiriöitä, lokitetusta datasta.

Modernit SIEM-ratkaisut eivät rajoitu pelkästään lokien keräämiseen ja häiriöiden havaitsemiseen, vaan mahdollistavat myös tarvittavat jatkotoimenpiteet. Tietoturvahäiriöitä havaittaessa tulee löydökset myöskin tutkia, mieluiten ennalta määritetyn prosessin mukaisesti. SIEM-ratkaisut tukevat usein tutkintatarvetta toiminnallisuuksilla, jotka mahdollistavat syväluotaavamman katsauksen lokitettuun tietoon häiriöhavainnon yhteydessä. Myös automaatiotoimintojen hyödyntäminen on vahvasti suositeltavaa, jotta häiriöhavaintoihin voidaan vastata riittävällä nopeudella ja mahdollisimman tehokkaasti.

Microsoft Sentinel on Microsoftin vuonna 2019 julkaisema pilvipohjainen SIEM-ratkaisu. Microsoft Sentinel rakentuu ja toimii täysin Microsoftin omalla Azure-julkipilvialustalla. SIEM-ratkaisuna Sentinelin toiminta keskittyy tietoturvakriittisten lokien käsittelyyn, kuten poikkeamien havainnointiin sekä tutkintaprosesseihin. Julkisella pilvialustalla toimiva Sentinel erottuu perinteisistä SIEM-ratkaisuista hyödyntämällä pilvinatiiviuuttaan jatkuvan kehityksen mallilla.

1.2 Tavoitteet ja toimeksiantaja

Tässä opinnäytetyössä hyödynnetään toiminnallista tutkimusotetta. Tutkimuksen tavoitteena on kuvata Microsoft Sentinelin toiminnallisuus kattavasti, samalla dokumentoiden käsitellyt aiheet ja niiden käyttöönotto ohjeistavaan malliin. Projektin aikana rakentuu Microsoft Sentinelin käyttöönotossa ja ylläpidossa avustava dokumenttipohja, jota voidaan myös tulevaisuudessa laajentaa ohjelmiston kehittyessä. Opinnäytetyö tuotetaan toimeksiantona Sulava Oy:lle.

Sulava Oy on konsultointi- ja koulutuspalveluita tarjoava yritys, joka erikoistuu Microsoftin pilvipalveluratkaisuihin. Sulava Oy toimii Suomessa niin Helsingissä kuin Kuopiossa, mutta myös kansainvälisesti Yhdistyneissä Arabiemiirikunnissa, Sveitsissä ja Saksassa.

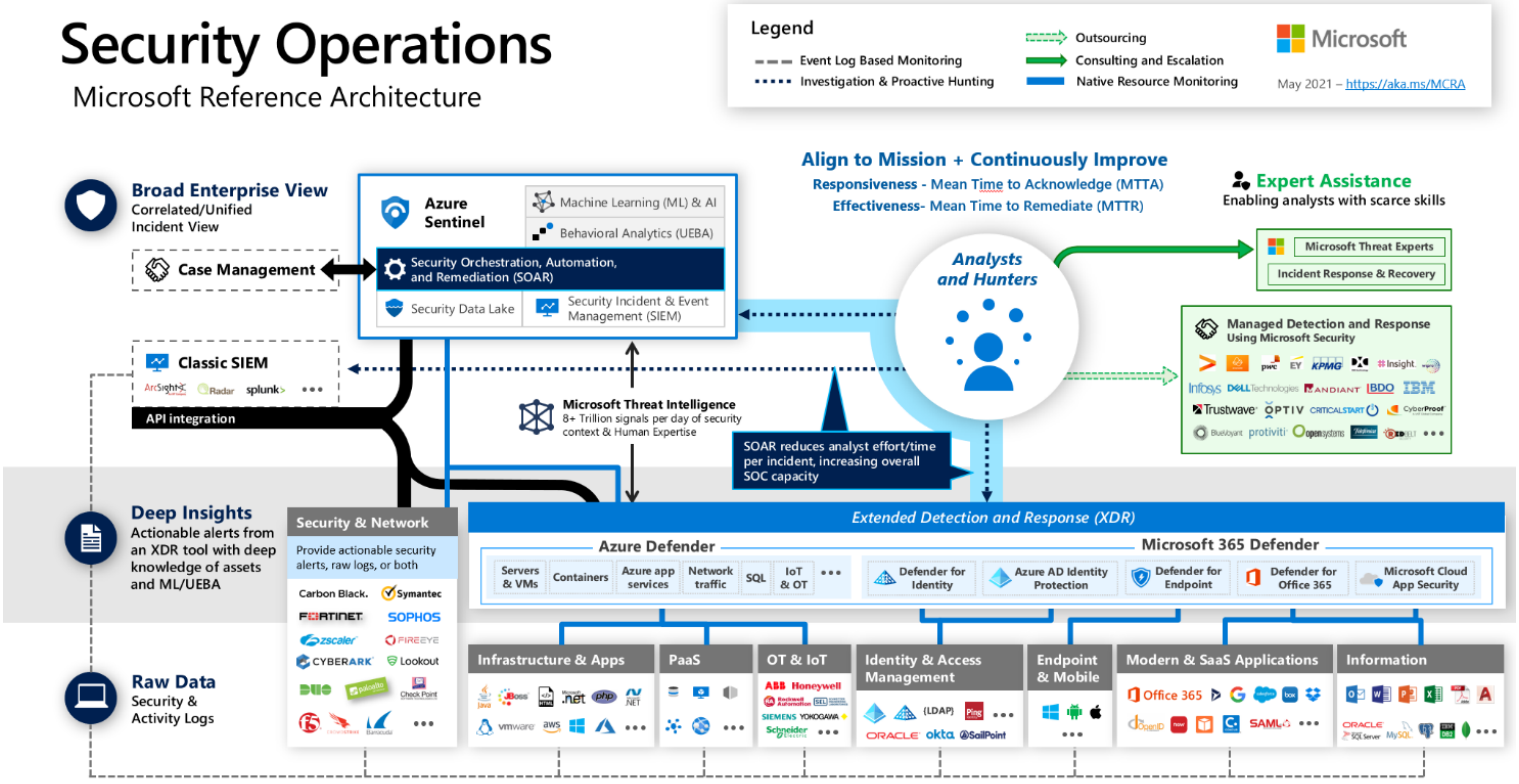
Sulava Oy tarjoaa Sentinelin käyttöönottoa ja ylläpitoa palveluna asiakkailleen. Projektin tavoitteena on tuottaa yrityksen käyttöön dokumentaatio, jota hyödyntää käyttöönotoissa sekä ylläpidon tehtävissä. Projektiin aiheeseen liittyviä dokumentointeja on tuotettu jo Microsoftin puolesta sekä Sulava Oy:n toimesta. Näitä töitä hyödynnetään projektin aikana suuremman kokonaisuuden luomiseksi.

Projektin hyötynä voidaan valmista parhaiden käytäntöjen dokumentaatiota käyttää Sulavan asiakasprojekteissa toteutusten laadun ja tehokkuuden varmistamiseksi.

2 Tietoturva Microsoftin pilviympäristössä

Microsoft Azure on Microsoftin julkinen pilvipalvelualusta, jolta se tarjoaa asiakkailleen SaaS-, PaaS- sekä IaaS-palveluja. Azure tukee myös useita ohjelmointikieliä ja kolmannen osapuolen työkaluja. Alusta on ollut saatavilla asiakkaille vuodesta 2010 alkaen. Azure on kansainvälinen alusta, josta on mahdollista hyödyntää palveluita eri konesaleista, jotka sijaitsevat eri mantereilla. (Janakiram MSV 2020)

Kehityspalvelujen tarjoamisen ohella Microsoft keskittyy aktiivisesti Azuren ja muiden tuotteidensa tietoturvan kehittämiseen. Vuonna 2021 Microsoft julkisti nelinkertaistavan budjettinsa tietoturvainvestoinneille seuraavalle viidelle vuodelle, varaten investoinneille yhteensä 20 miljardia dollaria (CNBC 2021). Microsoft tarjoaa asiakkailleen Azuressa ja muissa tuotteissaan valmiita tietoturvatoiminnallisuuksia, mutta myös erillisiä tietoturvatuotteita, joilla organisaatiot voivat suojata ympäristönsä tehokkaasti. Microsoft on tuottanut referenssiarkkitehtuurikuvauksen tietoturvatuotteistaan SOC-tietoturvavalvomon (Security Operations Center) käytössä. Kuva 1 esittää Microsoftin tietoturvatuoteperheen tuotteiden käyttöä tietoturvavalvomon kontekstissa.



Kuva 1. SOC-referenssiarkkitehtuuri (Microsoft 2021a)

Microsoftin näkemyksen mukaisesti tuotteet, joita seuraavat kappaleet kuvaavat, voidaan integroida toimimaan keskenään niin, että ne koostavat kattavan, kokonaisvaltaisen kuvan tietoteknisen ympäristön tietoturvan tilasta. SOC-referenssiarkkitehtuurikuvauksessa korostetut alueet sisältävät Microsoftin tuotteista SIEM-ratkaisun roolissa Microsoft Sentinelin, XDR-tuotteissa (Extended Detection and Response) Microsoftin Defender-tuoteperheen sekä lukuisia muita tuotteita eri tietoturvatoimittajien valikoimista. Kuva pyrkii havainnollistamaan tyypillisen tietoturvavalvomon mallia, jossa kokonaiskuva valvottavista asioista muodostuu useista, pieniestä paloista ja tuotteista. Yksi tuote tai ratkaisu ei pysty yksinään hoitamaan koko ympäristön valvontaa vaan kattavassa valvonnassa useiden lähteiden kautta tiedon keräämiseen vaaditaan lukuisia ratkaisuja. Tiedonkulun suunnittelu on myös tärkeä osa tietoturvavalvomonäkymän luomista. Vaikka tuotteet, kuten Microsoftin Defender-tuoteperhe mahdollistavat automaatiotoimenpiteiden suorittamisen, on ihmisresurssien käyttö välttämätöntä yksityiskohtaisessa valvonnassa ja häiriöiden korjaamisessa. (Microsoft 2021a)

2.1 Azure Active Directory Identity Protection

Microsoftin Azure Active Directory Identity Protection tunnistaa haavoittuvat ja riskialttiit tilit Azure Active Directoryn kirjautumisdatan perusteella. Identity Protectionin avulla yksittäisten kirjautumisten riskitasojen sekä käyttäjätunnuskohtaisten riskitasojen käsittely on mahdollista. Näihin havaintoihin huomioidaan aikaisemmat riskit ja epätavalliset tapahtumat. (Joe Savini 2021)

Alusta oppii käyttäjien historiatiedon perusteella tunnistamaan normaalin käyttäytymisen. Kun alusta havaitsee normaalista poikkeavia kirjautumisia, käyttäjän riskitaso nousee. Jokaisella kirjautumisella on oma riskitasonsa (risky sign-ins) ja lisäksi jokaisella käyttäjällä on oma riskitasonsa, joka koostuu käyttäjän aikaisempien kirjautumisten riskeistä (Risky users / aggregated risk level). (Joe Savini 2021)

Identity Protectionin havaintoja voidaan myös hyödyntää pääsynhallinnan toimenpiteissä, sekä tieto voidaan integroida muille alustoille. (Joe Savini 2021)

2.2 Microsoft 365 Defender for Endpoint

Microsoftin päätelaitteiden, kuten loppukäyttäjien tietokoneiden ja puhelinten, tai yrityksen käytössä olevien palvelimien suojaamiseen käytettävä työkalu on Microsoft 365 Defender for Endpoint (MDE). MDE on Microsoftin EDR-työkalu (Endpoint Detection and Response), joka mahdollistaa laitteiden kattavan valvonnan lokien keräämisellä ja tekoälyavusteisella tietoturvahäiriöiden havainnointikyvykkyydellä. (Ammar Hasayen 2021)

MDE ei rajoitu pelkästään kytkettyjen laitteiden seuraamiseen, vaan mahdollistaa myös niiden hallinnoinnin keskitetystä portaalikäyttöliittymästä. MDE:n piirissä olevat laitteet voidaan muun muassa tarvittaessa eristää verkoista niin, että ne eivät voi kommunikoida tietoliikenneverkkoja hyödyntäen. Tämä on hyödyllistä, kun epäillään laitteen vuotavan arkaluontoista tietoa ulkopuolisen toimijan pariin, esimerkiksi haittaohjelma-asennuksen johdosta. Myös muiden hallintatoimenpiteiden, kuten antivirus-ohjelman ajamisen käynnistys tai diagnostiikkatietojen noutaminen ovat mahdollisia. Myös ulkoisen uhkatiedon, IOC-muotoinen (Indicator Of Compromise) käyttö on mahdollista. (Ammar Hasayen 2021)

2.3 Microsoft 365 Defender for Identity

Microsoft 365 Defender for Identity (MDI) keskittyy toimialuepalvelinten suojaamiseen aktiivihakemistoympäristöissä (Active Directory). MDI kerää tietoturvakriittistä tietoa toimialuepalvelimilta käyttämällä sensoreja, jotka asennetaan palvelimille. Kerätty tieto välitetään pilvipalvelun käsiteltäväksi, ja on nähtävillä erillisen portaalikäyttöliittymän kautta. (Joe Savini 2021)

Havainnot, joita MDI tekee, keskittyvät aktiivihakemistossa tapahtuviin, epäilyttäviin toimenpiteisiin, kuten epätavallisiin autentikaatiotoimiin tai käyttäjähallinnoinnointiin. Aktiivihakemistotapahtumien tuominen pilvipohjaiseen valvontaan on tärkeää, jotta toimialuepalvelinten tietoturvaa voidaan ylläpitää ajan tasalla tehokkaasti. (Joe Savini 2021)

2.4 Microsoft 365 Defender for Office 365

Office 365 on Microsoftin kollaboraatiotuoteperhe, joka sisältää niin viestintäpalveluita, kuin myös tuottavuuteen keskittyviä tuotteita. Microsoft 365 Defender for Office 365 (MDO) keskittyy turvaamaan näitä tuotteita. Etenkin sähköpostipalvelu Exchange, pikaviestinpalvelu Teams sekä kollaboraatioalusta SharePoint ovat suojaustoimintojen keskipisteessä. MDO laajentaa näkyvyyttä kaikkien osalta ja tarjoaa laajempia kontrollitoimenpiteitä ylläpitäjille. (Sean McAvinue 2021)

Exchange Online: MDO laajentaa näkyvyyttä Microsoftin sähköpostipalvelun osalta ja mahdollistaa epäilyttävien viestien tarkemman, helppokäyttöisen tutkinnan suoraan pilvestä. Myös toiminnot, kuten sähköpostilinkkien suojaaminen ja liitetiedostojen kattavampi skannaus ovat tuettuja. (Sean McAvinue 2021)

Teams: MDO suojaa Teamsissa tapahtuvaa viestintää muun muassa skannaamalla jaetut linkit sekä mahdollistaa alustan tarkemman moderoinnin. Myös epäilyttävien toimenpiteiden valvonta tiimien ja käyttäjien hallinnan osalta on mahdollista kerätyn lokitiedon avulla. (Sean McAvinue 2021)

SharePoint: SharePointin toiminnot, kuten OneDrive voidaan suojata MDO:n avulla. Tällöin epätavalliset tapahtumat, kuten suurten tiedostomäärien lataukset tai tiedostojen julkinen jako voidaan havaita nopeasti ja tarvittaessa myös torjua ylläpitäjän toimesta. (Sean McAvinue 2021)

MDO:n käyttö on vahvasti suositeltavaa, jos Office 365 -tuotteet ovat organisaation käytössä. Lisäsuojaustoiminnot, joita palvelu tuo, nostavat ylläpitäjien toimintavalmiutta ja näkyvyyttä tietoturvan ylläpitämisen kannalta oleellisiin alueisiin. (Sean McAvinue 2021)

2.5 Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps (MDCA) on Microsoftin CASB-tuote (Cloud Access Security Broker), joka tarjoaa monipuolisen näkyvyyden, tietoliikenteen hallinnan ja kehittyneen analytiikan tietoturvauhkien tunnistamiseen ja niihin vastaamiseen. MDCA tukee monipuolisesti pilvi- ja paikallislokilähteitä, kuten palomuureja, päätelaitteita sekä monipilviympäristöjä. MDCA lukee lokeja liitetyistä lähteistä ja pystyy muodostamaan hälytyksiä epäilyttävistä tapahtumista. (Adrian Valencia 2021)

MDCA keskittyy varjo-IT:n havaitsemiseen ja organisaation käytäntöjen toteutumisen valvomiseen pilvisovelluksissa. MDCA myös seuraa käyttäjien kirjautumistapahtumia ja Office-toimintoja ja korostaa poikkeavaa käyttäytymistä tutkimussuosituksiin. Yhteenvetonäkymät tutkinnan kohteista sekä sisään tuodusta datasta helpottavat ympäristön valvontaa ja havaintoihin reagointia. (Adrian Valencia 2021)

2.6 Microsoft Defender for Cloud

Microsoft Defender for Cloud (MDC) on Microsoftin pilviturvaratkaisu, joka keskittyy suojamaan Azurea, paikallisympäristön resursseja sekä myös muiden pilvialustojen ratkaisuja. MDC yhdistää kaksi Microsoftin entistä toimintoa alleen, Security Centerin sekä Azure Defenderin. MDC:n toiminta voidaan jakaa kolmeen osa-alueeseen:

Jatkuva arviointi: MDC ylläpitää hallinnassaan olevista resursseista jatkuvaa näkymää, jolla koostetaan tietoa haavoittuvuuksista sekä tietoturvan yleisestä tasosta. Microsoft käyttää suositusten esittämiseen kehittämäänsä Secure Score -mallia, jolla ympäristön

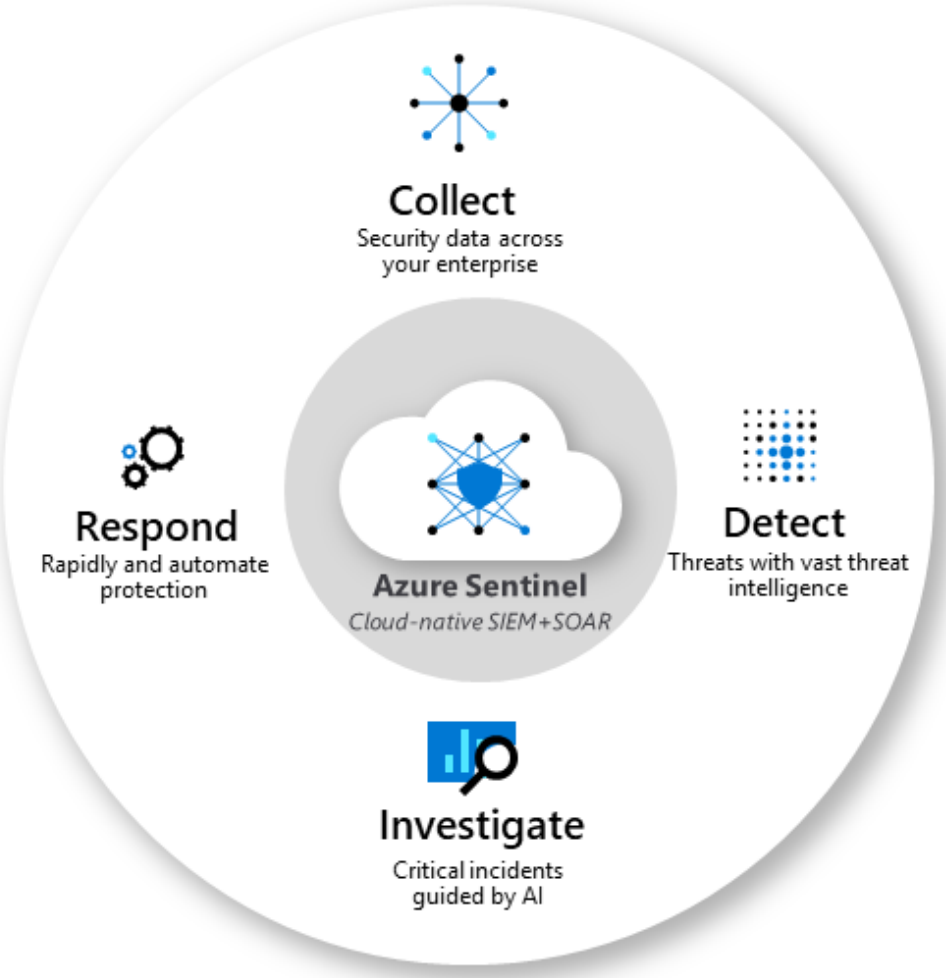
turvasuositukset pisteytetään suhteessa ympäristön toteutuneisiin toimenpiteisiin. (Microsoft 2021c)

Turvatoimet: Turvatoimien kautta Microsoft tuottaa suosituksia MDC:n piirissä oleville palveluille. Suositukset sisältävät yleisiä, parhaiden käytäntöjen mukaisia toimenpiteitä, esimerkiksi pilvessä sijaitsevien palvelimien pääsynhallintaan liittyviä suosituksia ja toimintoja. Turvatoimisuositukset on usein myös mahdollista ottaa käyttöön helppokäyttöisen ”Fix”-napin kautta. (Microsoft 2021c)

Puolustus: MDC tuottaa myös ympäristön puolustukselle kriittisiä hälytyksiä, esimerkiksi löydetyistä haavoittuvuuksista tai epäilyttävistä tapahtumista. Hälytykset valvonnan piirissä olevista resursseista ovat usein kriittisiä ja niiden hyödyntäminen ympäristön keskitetyssä valvonnassa on suositeltavaa. (Microsoft 2021c)

2.7 Microsoft Sentinel

Microsoft Sentinel on Microsoftin tarjoama pilvipohjainen SIEM-ratkaisu (Security Information and Event Mannagement). Sentinel toimii Microsoftin Azure-pilvialustalla, eikä vaadi erillisiä lisenssihankintoja toimiakseen. Microsoft julkaisi Sentinelin vuonna 2019 nimellä Azure Sentinel, mutta nimi vaihdettiin Microsoft Sentineliksi vuoden 2021 marraskuussa Ignite-tapahtuman yhteydessä (Rod Trent 2021). Kuva 2 havainnollistaa Sentinelin ydintoiminnallisuuksia.



Kuva 2. Microsoft Sentinelin ydintoiminnallisuus havainnollistettuna (Microsoft 2021b)

Microsoft Sentinelin toimintaa voidaan kuvata nelivaiheisesti:

Lokien kerääminen: Sentinel pohjaa toimintansa ratkaisuun tuotuihin, tietoturvatapahtumia sisältäviin lokitietoihin. Sentinel sisältää huomattavan määrän valmiita liitinratkaisuja, joilla dataa voidaan tuoda Sentinelin käsiteltäväksi nopeasti ja varmasti. Lokidatan sisään tuominen ratkaisun käytettäväksi on pakollinen vaatimus, jotta toimintoja voidaan hyödyntää. (Microsoft 2021b)

Tietoturvahäiriöiden havaitseminen: Sentinel tutkii ja korostaa havaitsemaansa poikkeavaa toimintaa lokidatasta, jota järjestelmään tuodaan. Tietoturvakriittisiä havaintoja kutsutaan tietoturvahäiriöiksi (incidents), joita Sentinel korostaa omaan näkymäänsä tutkittavaksi. (Microsoft 2021b)

Tietoturvahäiriöiden tutkiminen: Tehtyjen tietoturvahäiriöhavaintojen tutkiminen on tuettua Sentinelissä useamman ominaisuuden avulla. Myös ulkoisista lähteistä, kuten edellä

mainituista Microsoft-tuotteista tehtyjä havaintoja voidaan tutkia Sentinelin avulla. Havaittujen tietoturvahäiriöiden tutkinta on tärkeää, jotta ympäristön tietoturvatasoa voidaan ylläpitää. (Microsoft 2021b)

Automaation hyödyntäminen: Sentinel tukee myös lukuisia automaatiotoimenpiteitä, joilla hallinnoinnista, ylläpitämisestä sekä havaintoreagoinnista voidaan tehdä tehokkaampaa ja helpompaa. Sentinel on SIEM-ratkaisu, mutta sisältää myös SOAR-toiminnallisuuksia (Security Orchestration, Automation and Response), joilla ratkaisuun voidaan lisätä ulkoisia integraatioita ohjaamaan toimintaa ja lisäämään automaatiotoimia. (Microsoft 2021b)

Microsoft Sentinel on osa Microsoftin tietoturvatuotekokonaisuutta, ja vaikka ratkaisu integroituukin vahvasti muihin Defender-tuotteisiin, on se silti oma itsenäinen tuotteensa. Sentinel on kasvattanut suosiotaan SIEM-ratkaisujen keskuudessa julkaisunsa jälkeen ja Forrester-analytiikkayhtiö oli vuoden 2020 SIEM-ratkaisujen vertailussa nostanut sen johtavien tuotteiden joukkoon (Forrester 2020).

3 Microsoft Sentinelin käyttöönotto

3.1 Vaatimukset

Microsoft Sentineliä käyttöönotettaessa tulee huomioida tekijät, jotka toimivat vaatimuksina ratkaisun onnistuneelle käyttöönotolle. Sentinel koostuu kahdesta Azuressa sijaitsevasta resurssista, joista ensimmäinen on Log Analytics Workspace. Log Analytics toimii Sentinel-ratkaisun taustalla datan säilytyspaikkana sekä ikään kuin moottorina kokonaisuudelle. Itse Sentinel otetaan käyttöön Log Analytics Workspacen päälle, jolloin poikkeavien tapahtumien havainnointi datasta voidaan aloittaa. Vaatimuksina molempien resurssien käyttöönotolle on tilaus (subscription) Azuressa, jonka kautta Microsoft hoitaa varattujen resurssien veloituksen. Käyttöönottoa työstävän käyttäjän tilillä tulee myös olla riittävät käyttöoikeudet käytettävään Azure-tilaukseen, muokkaustasolla (contributor role). (Microsoft 2021b)

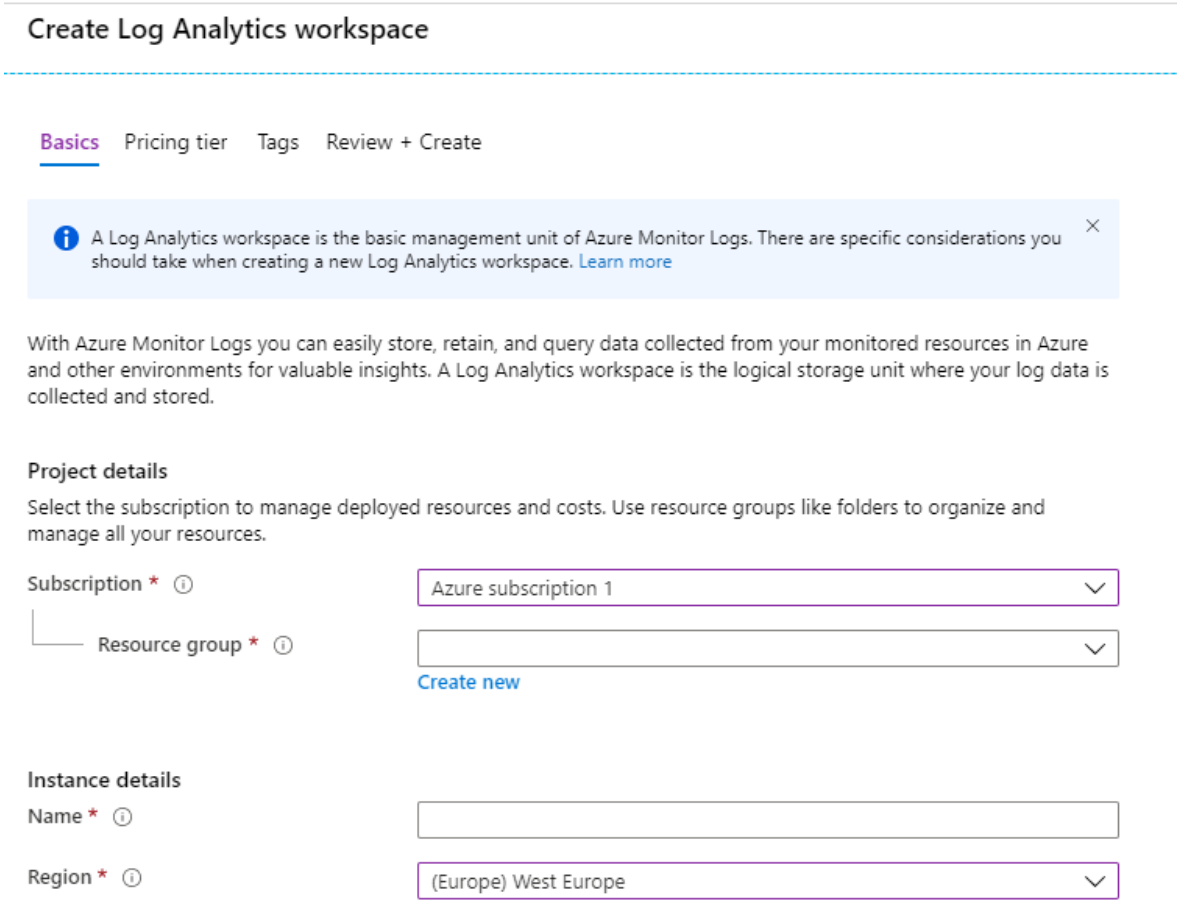
Jotta Sentineliä voidaan käyttää myös provisioinnin jälkeen, tulee vähimmäisvaatimuksena käyttäjällä olla pääsy Log Analytics Workspaceen Sentinel Reader -lukuoikeuksilla. Näitä oikeuksia voidaan hallinnoida myös ratkaisun käyttöönoton jälkeen (Microsoft 2020a). Myös datalähteiden yhdistämistä varten tarvitaan usein erillisiä järjestelmänvalvojan oikeuksia, joita luetellaan tämän opinnäytetyön osassa ”3.5 Datalähteiden määritys ja liittäminen”.

3.2 Log Analytics

Log Analytics on Azure Monitorin alainen palvelu Azuressa, joka mahdollistaa lokitietojen tallentamisen sekä vapaamuotoisen kyselyiden suorittamisen lokitietoja vasten. Log Analytics toimii siis lokitietojen tallennuspaikkana sekä kyselyalustana. Yksittäisestä Log Analytics -resurssista käytetään nimitystä ”Log Analytics Workspace”. (Microsoft 2021b)

Microsoft Sentineliä käyttöönotettaessa on Log Analytics ensisijaisen tärkeässä asemassa, sillä sen toiminta on välttämättömyys Sentinelin toiminnalle. Jotta lokien hallinta voidaan pitää mahdollisimman yksinkertaisena ja keskitettynä, on suositeltavaa, että Log Analytics Workspaceja ei provisioida yhtä enempää Azure-ympäristöä kohti. Yhden lokialustan käyttö mahdollistaa tehokkaamman lokien hallinnan sekä tekee datan käsittelystä ja hyödyntämisestä yksinkertaisempaa. Useammalle lokialustalle voi kuitenkin nousta tarve, jos talletettavien lokien säilytysaikoihin tulee tehdä datalähdekohtaisia muutoksia tai, jos lokien pääsynhallintaa halutaan hallinnoida tarkemmalla tasolla. (Microsoft 2021b)

Log Analytics Workspacen provisiointi tapahtuu Azuren Log Analytics -palvelualueelta. Uuden resurssin luominen vaatii sille määritetyn resurssiryhmän, johon resurssi sijoitetaan. Jos Log Analyticsia luodaan ensisijaisesti Sentineliä varten, on suositeltavaa luoda uusi resurssiryhmä Sentinel-resursseille jaettavaksi, jotta ratkaisukohtainen hallinnointi on helpompaa jatkossa. Konesalisijaintia valitessa on parasta hyödyntää lokaatiota, joka on Azure-ympäristön käyttöön sovittu ensisijaiseksi saliksi. Kuva 3 kuvaa Azuren näkymää, jossa Log Analytics Workspacen määritelmät asetetaan luonnin yhteydessä.



Kuva 3. Log Analytics Workspacen luontinäkymä

Workspacen luomisen jälkeen resurssi on käytettävissä ja valmiina Sentinelin asennusta varten.

3.3 Microsoft Sentinel

Kun Log Analytics Workspace on provisioitu, voidaan itse Sentinel ottaa käyttöön Azuressa. Microsoft Sentinelin lisäämisen jälkeen Log Analyticsissa sijaitsevaa dataa hyödynnetään Sentinelin kautta analytiikkasäännöillä sekä uhkien metsästyskyselyillä. Sentinelin lisääminen mahdollistaa myös uusien, helppokäyttöisten dataliittimien käytön ja kytkennän Log Analyticsiin.

Microsoft Sentinel otetaan käyttöön Azure-portaalista, siirtymällä Sentinelin palvelualueelle. Helpoin tapa tähän on hakea portaalin yleisestä hakutyökalusta ”Microsoft Sentinel”, jolloin hakutuloksiin ilmestyvä tulos ohjaa oikealle alueelle. Palvelualueella Sentinel voidaan liittää kahdella tapaa, joko painamalla ”+ Add” -painiketta vasemmasta yläreunasta tai valitsemalla ”Connect Workspace” ikkunan keskeltä. Sentinelin käyttöönotossa on hyvä huomioida, että ympäristö voi sisältää yhtäaikaisesti useamman Microsoft Sentinel -instanssin, jos käsiteltävä data on esimerkiksi eroteltu useampaan Log Analytics -tilaan, kuten aiemmassa osiossa kuvattiin. Microsoft Sentinel -instanssi voidaan kuitenkin kytkeä kerrallaan vain yhteen Log Analytics Workspaceen, joten useamman Workspacen mallissa useamman Sentinelin provisiointi on pakollista, jos kaikkea dataa halutaan käsitellä Sentinelin kautta. Microsoft Sentinel -palvelualue on Azuren portaalissa paikka, josta kaikki ympäristön Sentinelit voidaan listata. (Microsoft 2020c.)

Microsoft Sentinelin liittäminen haluttuun Log Analyticsiin kestää tyypillisesti vain lyhyen hetken, jonka jälkeen portaalin näkymä siirtyy automaattisesti luotuun Sentineliin. Vaikka Sentinel on onnistuneesti provisioitu ja liitetty haluttuun Log Analytics Workspaceen, ei sen käyttöönotto ole valmis ennen jatkokonfiguraatioita. Mikäli Log Analytics Workspace, johon Sentinel on liitetty, sisältää jo ennestään dataa, tai sitä liitetään Sentinelin omien liittimien ulkopuolisista lähteistä, voi Sentinel alkaa käsittelemään dataa välittömästi. Jos kytketty Workspace on kuitenkin vasta luotu Sentinelin kanssa, ei se luonnollisestikaan sisällä dataa käsiteltäväksi. Ensimmäinen toimenpide Sentinel-ratkaisun provisioinnin jälkeen tulisikin olla tarkastaa, että kaikki halutut dataliittimet ovat käytössä, ja että data halutuista lähteistä saapuu onnistuneesti Log Analyticsiin Sentinelin käsiteltäväksi. (Microsoft 2020c.)

3.4 Kustannusten hallinta

Asiakkaiden näkökulmasta Microsoft Sentinelin hintakertymä on yleinen kiinnostuksen kohde, joka nousee esiin hyvin varhaisessa vaiheessa ratkaisusta puhuttaessa. Tämä on luonnollista, sillä Sentinelin natiivi pilvipohjaisuus erottaa sen muista perinteisistä SIEM-ratkaisuista ja samalla sen hinnoittelumalli on poikkeuksellinen moneen muuhun palveluun verrattuna. Koska Sentinel koostuu Azuressa aina vähintään kahdesta erillisestä resurssista, Log Analytics Workspacesta ja Sentinel-instanssista, on tärkeää hahmottaa jo alussa, että myös hinnan laskeminen ratkaisulle tapahtuu laskemalla kummankin resurssin erilliset hinnat yhteen. Kummankin resurssin hintaa laskettaessa, tulee kuitenkin huomioida tiettyjä poikkeuksia, jotka koskevat Log Analyticsia ja Sentineliä.

3.4.1 Log Analyticsin hinnoittelu

Log Analyticsin hintaa arvioitaessa tulee määritellä käytettävä laskutustapa. Jos käytössä on oletuksena toimiva Pay-As-You-Go (PAYG) -malli, joka pohjautuu täysin palvelun käytön määrään, on tarkka hinta arvioitavissa sisään otetun datan määrän sekä säilytettävän datan määrän perusteella. PAYG-mallin etuna on se, että ratkaisun käytöstä maksetaan täysin käyttöasteen mukaisesti, jolloin ylimääräisiä kustannuksia ei ominaisuuksista, joita ei välttämättä hyödynnettäisi. Log Analyticsin laskutus pohjautuu datamäärässä laskettuna aina sisään otettuihin gigatavuihin, joten PAYG-mallin mukaisesti Log Analyticsin hinta kuukausittain määräytyy täysin sisään otettujen gigatavujen perusteella. Log Analyticsissa ei ole kiinteää hintaa sisään otetulle gigatavulle, sillä hinta vaihtelee konesalikohtaisesti sekä kysynnän ja tarjonnan mukaan. Esimerkiksi Länsi-Euroopan konesalissa (Amsterdam) sijaitsevan Log Analyticsin hinta saattaa olla gigatavukohtaisesti tänään 2,5€, mutta huomenna 2,2€. Hinnan vaihtelun mahdollisuus on hyvä huomioida, kun rakennetaan ympäristöä, jossa sisään otettua dataa kertyy päivittäisellä tasolla useampi gigatavu. Log Analyticsiin sisältyy PAYG-mallissa aina myös 5 gigatavua ilmaista dataa kuukausittain. (Microsoft 2020b.)

Log Analyticsin toinen hinnoittelumalli tunnetaan Azuressa ”Capacity Reservation” -nimikkeellä. Nimensä mukaisesti tällä mallilla on mahdollista varata etukäteen tietty määrä kapasiteettia Log Analytics -palvelusta päivittäistä datan lokitusta varten. Kapasiteetin varaaminen mahdollistaa kiinteän hinnoittelumallin hyödyntämisen, jos tiedetään jo ennestään, kuinka suuria määriä dataa Log Analyticsiin päivittäin tullaan keräämään. Päivittäisiä varauksia on mahdollista hyödyntää sadasta gigatavusta päivässä eteenpäin viiteensataan gigatavuun päivässä. Sadan gigatavun päivittäisen kapasiteetin varaaminen tarjoaa 15% alennuksen PAYG-hinnasta, kun taas viidensadan gigatavun päivittäinen varaus tuottaa 25% alennuksen PAYG-hinnasta. Jos päivässä sisään otettu datamäärä ylittää varauksen määrän, laskutetaan ylittävä data PAYG-mallin mukaisesti. Koska suurien datamäärien lokittaminen Log Analyticsiin käy suhteellisen kalliiksi verrattuna esimerkiksi paikallisessa konesalissa säilytettävään dataan, on kapasiteettivarausten hyödyntäminen järkevää, jotta kokonaiskustannusta voidaan laskea pienemmäksi. (Microsoft 2020b.)

Sen lisäksi, että Log Analyticsin hinnoittelu pohjautuu sisään otettujen gigatavujen määrään, tulee myös erikseen huomioida datan säilytyskustannukset palvelussa. Datan säilyttäminen on Log Analyticsissa mahdollista kahden vuoden ajan sisäänottohetkestä ja veloitus tapahtuu kuukausittain palvelussa sijaitsevien gigatavujen määrän mukaisesti. Kuten sisäänottohinnan kanssa, myös datan säilytystä koskeva gigatavukohtainen hinta vaihtelee päivittäin, eikä sisällä kiinteää summaa. Summa on kuitenkin huomattavasti pienempi kuin sisään otossa laskutettava hinta. Esimerkiksi Länsi-Euroopan konesalissa sijaitsevan

Log Analytics Workspacen gigatavukohtainen säilytyshinta on noin yhdeksän ja yhdentoista sentin välillä. (Microsoft 2020b.)

Datan säilytyksessä tulee kuitenkin huomioida myös muut tekijät, jotka vaikuttavat hinnan alenemiseen. Log Analyticsissa säilytettävä data on aina 31 päivää ilmaista. Tämä tarkoittaa sitä, että jos palveluun tuotua dataa säilötään vuoden ajan, kertyy datasta aina säilytyskustannuksia vain 334 päivän ajalta, koska ensimmäiset 31 päivää ovat kaikelle datalle aina ilmaisia säilytyksen kannalta. Oletusalennuksen lisäksi, jos Log Analytics Workspaceen kytketään Microsoft Sentinel -instanssi, pidentyy ilmainen säilytysaika kaiken datan osalta 90 päivään. Näin ollen, laskettaessa Sentinel-ratkaisussa hyödynnettävän datan säilöntäkustannuksia, on aina huomioitava, että datan kokonaissäilytysajasta vähennetään 90 päivää kustannusten laskemisessa. (Microsoft 2020b.)

3.4.2 Microsoft Sentinelin hinnoittelu

Kun lasketaan Sentinel-ratkaisun kokonaishintaa, tulee myös käyttöönotetun Sentinelin hinta huomioida Log Analyticsin hinnan lisäksi. Sentinelin hintamalli on kuitenkin hyvin samantyyppinen kuin Log Analyticsin suhteen ja pohjautuu täysin sisään otettujen gigatavujen määrään. Hinnoittelumallit ovat myös samat kuin Log Analyticsissa, tarjolla on edellä mainittu PAYG-malli sekä päivittäisiin kapasiteettivarauksiin perustuva malli. Sentinelissä hinnat ovat tyypillisesti hieman pienempiä kuin Log Analyticsissa, mutta niiden vaihtelun vuoksi kiinteää gigatavukohtaista hintaa ei voida määrittää. Päivittäiset kapasiteettivaraukset ja niiden tarjoamat hinnanalennukset ovat tarjolla taas 100 ja 500 gigatavun välillä ja alennukset vaihtelevat 50% ja 60% välillä. (Microsoft 2020c.)

Datan säilytyskustannuksia ei tarvitse huomioida Sentinel-instanssin hinnanlaskussa, sillä kustannus pysyy Log Analyticsissa. Sentinelissä on myös muutama poikkeus tiettyjen datalähteiden suhteen, jotka on kannattavaa huomioida hintaa laskettaessa. Lähtökohtaisesti kaikki data, joka Sentineliin kytkettyyn Log Analytics Workspaceen tuodaan laskutetaan täysihintaisena, mutta poikkeuksina toimivat seuraavat datalähteet:

- Azure Activity
- Office 365 (SharePoint, Exchange ja Teams)
- Kaikki hälytysdata Microsoftin Defender -tuotteista

Nämä poikkeukset huomioiden, jos tarkoituksena olisi lokittaa esimerkiksi vain Azuren tilauksien alaisia operaatioita ja Officen SharePointin käyttöä, ei Sentinel-instanssille kertyisi ollenkaan Log Analyticsista erillistä hintaa. Näistä lähteistä koituvat säästöt voivat olla suuremmissa ympäristöissä huomattaviakin, eikä niiden hyödyntämiseen tarvita erillisiä konfigurointitoimenpiteitä. (Microsoft 2020c.)

Viimeisenä huomioitavana asiana on myös hyvä nostaa esiin Sentinelin käyttöönotossa hyödynnettävä koeaika. Kun Sentinel-instanssi luodaan, ei sen käytöstä veloiteta erikseen ensimmäisen kuukauden aikana. Tämä mahdollistaa siis ratkaisun lyhytaikaisen testaamisen toivotussa ympäristössä, mutta ei tarjoa tuotantoon tarkoitetulle käytölle suurempia etuja. Sentinelin koeaika on voimassa aina automaattisesti provisiointihetkestä 31 päivää. (Microsoft 2020c.)

3.4.3 Ratkaisun kokonaishinta

Microsoft Sentinel -ratkaisun kokonaishinta tulee siis laskea aina vähintään kahden eri resurssin hinnan huomioiden, jotta tarkka kokonaishinta ratkaisulle voidaan muodostaa. Koska hinnat eivät ole kiinteitä Log Analyticsin tai Sentinelin osalta, Microsoft tarjoaa reaaliaikaisen hintanäkymän kummallekin palvelulle:

- Log Analytics: https://azure.microsoft.com/en-us/pricing/details/monitor/
- Sentinel: https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/

Sentinelin hinta määräytyy siis yleisimmin gigatavukohtaisen käytön perusteella. Tämän vuoksi ympäristöön tuotavan datan määrä ratkaisee suurimmaksi osaksi myös ratkaisun kokonaiskustannuksen. Kun Sentinelin käyttöönottoa lähdetään suunnittelemaan, on budjetointi välttämätöntä, jottei hyödynnettävän datan aiheuttama kustannus nouse liian suureksi. Koska hinta muodostuu pilveen tuodun datamäärän perusteella, voi joissakin tilanteissa olla taloudellisesti kustannustehokkaampaa pitää esimerkiksi paikallisista lähteistä, kuten palvelimista lokitettava data erillisessä, paikallisessa SIEM-ratkaisussa ja keskittyä Sentinelin osalta vain pilvipalveludataan. (Microsoft 2020c.)

3.5 Datalähteiden määritys ja liittäminen

Microsoft Sentinelin toiminta SIEM-ratkaisuna pohjautuu dataan, jota taustalla toimivaan Log Analyticsiin lokitetaan. Tämän vuoksi käyttöönoton tärkeimpiä vaiheita on datalähteiden määritys sekä niiden liittäminen. Ennen kuin lokilähteitä voidaan alkaa kytkemään Sentinelin havainnoitavaksi, on ensisijaisen tärkeää kartoittaa lokituksen tarpeet, jotta säilöttävä data on tarpeellista ja kaikkiin havainnointitarpeisiin voidaan vastata. Tekninen kytkentä voidaan aloittaa vasta, kun oikeista lähteistä on sovittu tarkkaan ja niiden sisältö sekä vaikutus on ymmärretty. (Microsoft 2021b)

Kun tarvittavia datalähteitä määritetään, tulee samalla pohtia Sentinelistä tavoiteltavia toiminnallisuuksia. Tullaanko dataa lokittamaan vain säilömistarkoituksella, vai onko tarkoitus havainnoida mahdollisia poikkeamia tai uhkia? Kuinka pitkään dataa on tarve/voidaan

säilyttää? Tuleeko datan olla saatavilla kaikille vai vain rajatuille käsittelijöille. Näihin kysymyksiin vastaaminen avustaa arkkitehtuurin suunnittelussa ja tulevaisuudessa mahdollisten muutosten tekemisessä. (Microsoft 2021b)

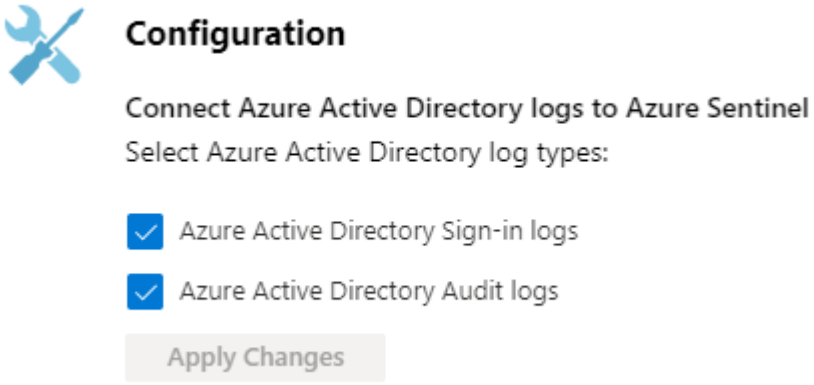
Sentineliin on mahdollista kytkeä dataa niin pilviympäristöistä kuin paikallisista lähteistä. Pilvinatiivina ratkaisuna Sentinel on alusta alkaen suunniteltu joustavaksi datalähteiden liitännän suhteen. Alustaan on mahdollista tuoda lokidataa Microsoftin omista tuotteista, mutta myös muista kolmannen osapuolen palveluista, kuten vaikka Amazonin pilvialusta Amazon Web Servicesistä (AWS), Google Coud Platformista (GCP) tai oman konesalin toimialueen ohjauspalvelimelta (domain controller). Pilvipalveluna Sentinel on helposti saatavilla eri sijainneista, minkä ansiosta myös datan tuominen pilveen on mahdollista eri ympäristöistä. Jos dataa tuodaan Sentineliin valmiiksi rakennettujen dataliittimien sijaan toisella tapaa, on tärkeää varmistaa, että datan vastaanotto ja käsittely on tuettua Sentinelissä. Esimerkiksi syslog, tyypillinen standardi datan käsittelyssä, on tuettu Sentinelissä, ja lokeja voidaan lähettää alustalle erillisen syslog-palvelimen kautta. Päivitetty lista Sentinelin tukemista datalähteistä on saatavilla Microsoftin dokumentaatiosivuilla https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources. (Microsoft 2021b)

Alla oleva listaus sisältää kuvauksen dataliittimistä, jotka ovat hyvien käytäntöjen mukaisesti hyödynnettäviä lähestulkoon kaikissa ympäristöissä. Ennen varsinaista teknistä kytkentää on tärkeää tarkistaa, että kaikkiin vaatimuksiin datan liittämisessä kyetään vastaamaan. Kaikki Sentinelin sisäiset dataliittimet sisältävät kuvauksen vaatimuksista, joiden tulee täyttyä ennen kuin dataa voidaan lähteä tuomaan Sentinelin kautta Log Analyticsiin.

3.5.1 Azure Active Directory

Azure Active Directoryn (AAD) dataliitin sisältää mahdollisuuden lokittaa Sentinelin kautta Log Analyticsiin kahdentyyppisiä lokeja; auditointilokeja sekä sisäänkirjautumistietoja. Nämä lokityypit ovat SIEM-ratkaisuille hyvin tyypillisiä ja sisältävät monia, etenkin käyttäjien identiteetin kannalta oleellisia tietoja, joita voidaan hyödyntää ympäristön suojaamisessa. Esimerkiksi kirjautumistietojen perusteella voidaan helposti selvittää, onko käyttäjätunnuksilla tehty kirjautumisyrityksiä luvattomista maista. Vastaavasti auditointilokit voivat paljastaa hälyttäviä roolikorotuksia, jotka voivat olla riski ympäristön turvallisuudelle.

Kuva 4 esittää AAD-dataliittimen kytkentätoimintoa.



Kuva 4. Näkymä liitetystä AAD-datasta

Azure Active Directory -datan kytkentä on yksinkertaista, mutta pelkkä pääsy Sentineliin itseensä ei riitä liitännän suorittamiseen. Jotta liitäntä voidaan tehdä, tulee seuraavien vaatimusten täyttyä:

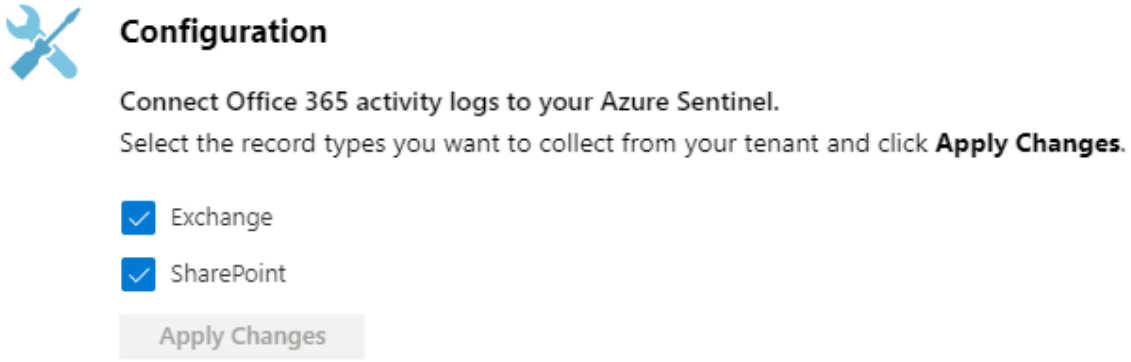
- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Azure Active Directoryn diagnostiikka-asetuksiin
- Tilauksen, joka Log Analyticsilla on käytössä, tulee olla rekisteröitynyt ”Microsoft.Insights” -resurssintarjoajaan (tämän pitäisi olla jo toteutunut, jos Log Analytics Workspace on otettu käyttöön)
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa
- Azure Active Directory -hakemiston tulee olla lisensointitasoltaan P1 tai P2

AAD-datan kytkennän jälkeen datan siirtymisessä käytettäväksi kestää noin 15–30 minuuttia. Tämän jälkeen dataa voidaan hyödyntää niin analytiikkasääntöjen määrittämisessä kuin visualisointinäkymien luomisessa. (Microsoft 2020d.)

3.5.2 Office 365

Office 365 -dataliitin sisältää halutusta Office-pilviympäristöstä tuotavan tiedon SharePointin, Exchangen ja Teamsin osalta. Tämä data sisältää esimerkiksi SharePointin osalta OneDrivessa tehdyt operaatiot ja Exchangesta muun muassa käyttäjien aktiviteetit, kuten sähköpostin lähetyksen tai luodut välityssäännöt. Teams-data sisältää toimenpiteet, kuten kanavien luonnin ja poistamisen tai käyttäjähallinnan muutokset.

Kuva 5 esittää Office 365 -dataliittimen kytkentätoimintoa.



Kuva 5. Näkymä liitetystä Office 365 -datasta

Office 365 -datan kytkentä on yksinkertaista, mutta pelkkä pääsy Sentineliin itseensä ei riitä liitännän suorittamiseen. Jotta liitäntä voidaan tehdä, tulee seuraavien vaatimusten täyttyä:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa

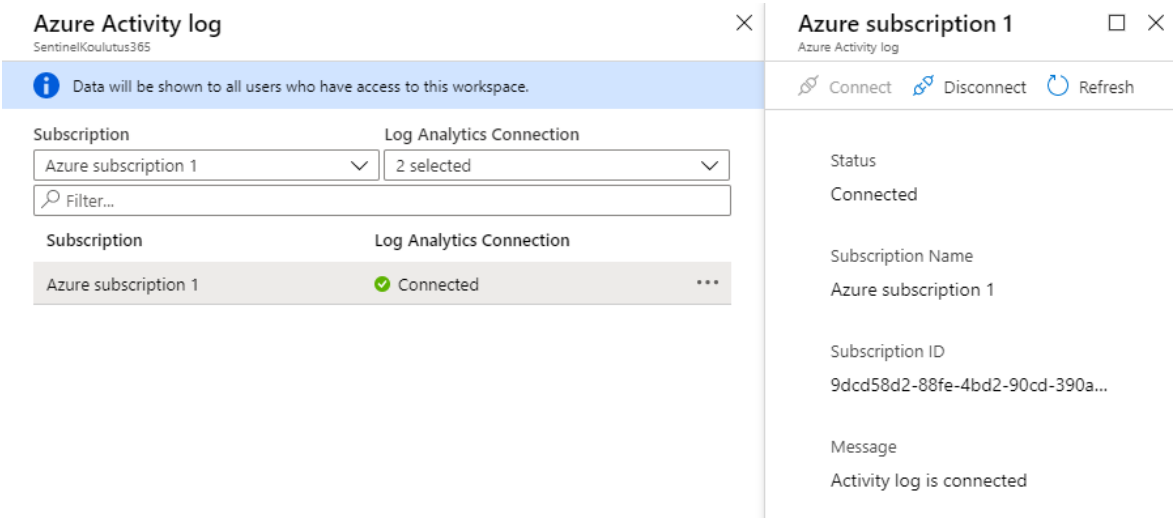
Erillinen vaatimus, jota Microsoft ei listaa liittimessä, on auditointilokien päälle kytkentä Officen puolella. Tämä voidaan tehdä PowerShellilla tai Officen ”Security & Compliance Centeristä”. Jos Office-tenantti sisältää E3- tai E5-tason lisenssejä, on auditointi automaattisesti kytkettynä päälle. Office 365 -datan kytkennän jälkeen datan siirtymisessä käytettäväksi kestää noin 15–30 minuuttia. Tämän jälkeen dataa voidaan hyödyntää niin analytiikkasääntöjen määrittämisessä kuin visualisointinäkymien luomisessa. (Microsoft 2020e.)

3.5.3 Azure Activity

Azure Activity -dataliitin mahdollistaa Azuren sisäisten tilauksien lokien tuomisen Sentinelin havainnoitavaksi. Näihin lokeihin sisältyvät operaatiot, jotka toteutetaan Azuren tilauksiin, esimerkiksi uusien resurssien luominen, poistaminen tai uusien pääsyoikeuksien jako. Koska Azuressa voi olla käytössä useampia tilauksia, liitetään halutut tilaukset yksitellen liittimen kautta. Azure Activity -datan kytkeminen on helppoa, mutta jotta se onnistuu, tulee ennakkovaatimuksiin vastata:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla vähintään lukuoikeus tilaukseen, joka halutaan liittää lokituksen piiriin

Kuva 6 esittää Azure Activity -dataliittimen kytkentätoimintoa.



Kuva 6. Näkymä liitetystä Azure-tilausdatasta

Activity-lokit siirtyvät käsiteltäväksi tyypillisesti noin 15–30 minuutin välillä liitännästä. (Microsoft 2020f.)

3.5.4 Microsoft 365 Defender -tuotteet

Sentinel ei ole ainut Microsoftin tarjoamista tietoturvatuotteista. Microsoftin 365 Defender -tuotteet ovat työkaluja, jotka auttavat teknisten ympäristöjen kokonaisvaltaisessa suojaamisessa. Nämä sisältävät neljä erillistä Defender -tuotetta Microsoft 365 -ympäristöjen suojaamiseen:

- Microsoft Defender for Endpoint: Päätelaitteiden suojaamiseen tarkoitettu EDR-tuote (Endpoint Detection and Response)
- Microsoft Defender for Office 365: Sähköpostin ja Office -ratkaisujen suojaamiseen tarkoitettu tuote
- Microsoft Defender for Identity: Paikallisten toimialuepalvelimien suojaamiseen tarkoitettu tuote
- Microsoft Cloud App Security: Monipuolinen sovellusten ja käyttäjien valvontaan tarkoitettu CASB-tuote (Cloud Access Security Broker)

Näiden lisäksi kytkettäviin tuotteisiin voidaan myös suositella Azure Active Directory Identity Protectionia, joka ei sinällään kuulu Defender -tuoteperheeseen, mutta suojelee ja riskiluokittelee ympäristön käyttäjiä kirjautumistapahtumien perusteella.

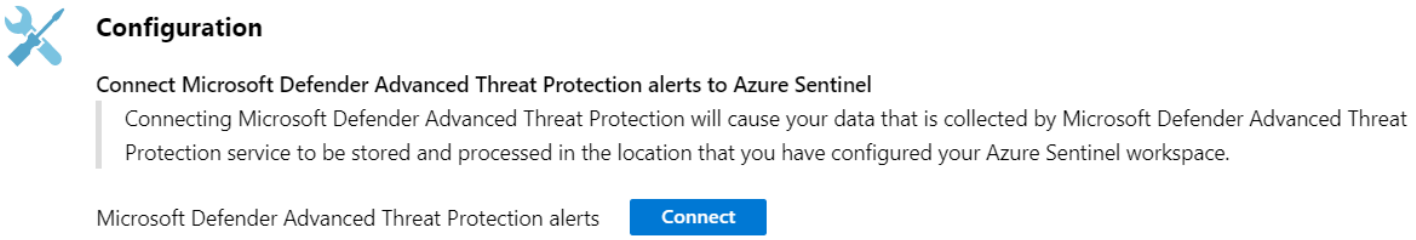
Defender-tuotteet käyttävät osittain samaa dataa, jota Sentinel voi hyödyntää, joten olisi turhaa tuoda samaa dataa Sentineliin uudestaan, jos analytiikka voidaan suorittaa toisella alustalla. Tämän vuoksi data, joka Defender -tuotteista tuodaan, ei ole niin sanottua ”raa-kadataa” käsittelemättömässä muodossaan, vaan jo valmiiksi analysoitua, hälytyksen muotoon käännettyä tietoa. Sentineliin siis liitetään muilta Defender-alustoilta vain suoria hälytyksiä, joita alustat muodostavat omilla kyvykkyyksillään. Kaikkien Microsoft Defender -tuotteiden liittäminen on Sentinelissä yksinkertaista, mutta nämäkin lähteet sisältävät Sentinelistä eriäviä vaatimuksia, joiden tulee täyttyä, jotta lokitus Log Analyticsiin voidaan suorittaa:

Microsoft Defender for Endpoint:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa
- Tenantissa tulee olla tuettu lisenssi Defender for Endpointille

(Microsoft 2020h.)

Kuva 7 esittää Defender for Endpointin -dataliittimen kytkentätoimintoa.

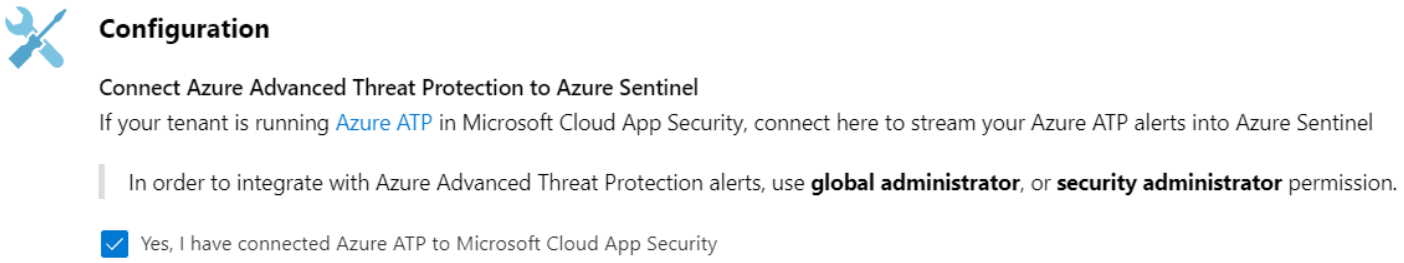


Kuva 7. Defender for Endpointin dataliitin

Microsoft Defender for Identity:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa
- Tenantissa tulee olla tuettu lisenssi Defender for Identitylle

Kuva 8 esittää Defender for Identityn -dataliittimen kytkentätoimintoa.



Kuva 8. Defender for Identityn dataliitin

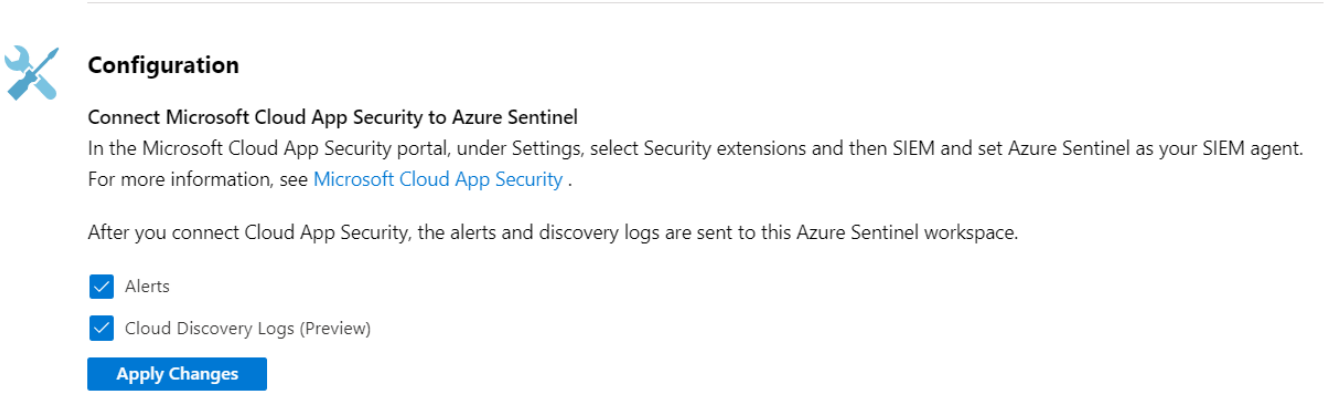
Defender for Identityn kanssa on hyvä huomioida, että liitäntä hälytyksistä tehdään Sentineliin Defender for Cloud Appsin kautta, joten Defender for Identityn tulee olla liitettynä ensin Defender for Cloud Appsiin. (Microsoft 2020i.)

Microsoft Defender for Cloud Apps:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa
- Tenantissa tulee olla tuettu lisenssi Defender for Cloud Appsille

(Microsoft 2020j.)

Kuva 9 esittää Microsoft Defender for Cloud Appsin -dataliittimen kytkentätoimintoa (kuvassa tuotteen vanha nimi ”Microsoft Cloud App Security”).



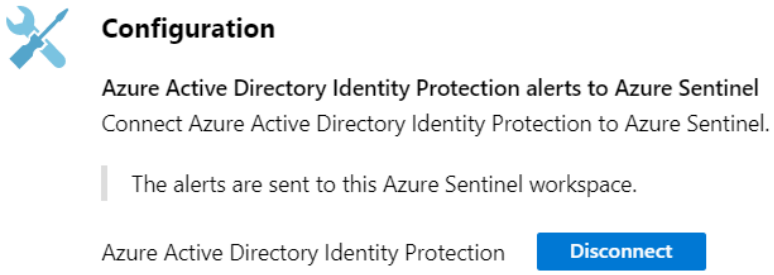
Kuva 9. Microsoft Defender for Cloud Appsin dataliitin

Azure Active Directory Identity Protection:

- Liittäjällä tulee olla luku- ja kirjoitusoikeudet Log Analytics Workspaceen
- Liittäjällä tulee olla ”Global Administrator”- tai ”Security Administrator” -rooli Azure Active Directoryssa
- Azure Active Directory -hakemiston tulee olla lisensointitasoltaan P1 tai P2

(Microsoft 2020g.)

Kuva 10 esittää Azure Active Directory Identity Protectionin -dataliittimen kytkentätoimintoa.



Kuva 10. AAD Identity Protectionin dataliitin

Microsoftin tietoturvahälytysten tuominen Sentineliin muilta alustoilta rikastaa dataa Sentinelissä sekä avustaa poikkeamien tutkimustyössä.

4 Tietoturvauhkien havainnointi

SIEM-ratkaisuna Microsoft Sentinel ei keskity pelkästään datan lokitukseen ja säilöntään. Uhkien ja poikkeamien havainnointi on yksi ratkaisun tärkeimpiä tehtäviä ja suurin osa Sentinelin toiminnallisuuksista tukeekin näitä toimenpiteitä. Käyttöönotossa havainnointikyvykkyyden varmistaminen on vaihe, johon tulee keskittyä heti datalähteiden liittämisen jälkeen, jotta sisään tuodun datan hyödyntäminen voidaan aloittaa.

4.1 Jatkuva havainnointi

Microsoft Sentinelin kyvykkyys muodostuu ennen kaikkea kyvystä havainnoida, tutkia ja ehkäistä tietoturvauhkia. Jotta havainnointia voidaan toteuttaa, tulee Sentinelin olla kytkettynä Log Analytics Workspaceen, joka sisältää raakadataa ratkaisun käsiteltäväksi. Sentinelissä ”Analytics”-analytiikkatoiminnallisuus mahdollistaa juuri havainnoinnin jatkuvan toteuttamisen ja tarvittaessa myös automatiikan hyödyntämisen. Analytiikkasääntöjä määrittämällä voidaan Sentinel konfiguroida luomaan tutkittavia poikkeamia ”Incidents”-alueelle Azureen lokitetun datan pohjalta. Analytiikkasääntöjä voidaan ottaa käyttöön kahdessa muodossa, ”Scheduled query”-sääntöinä ja ”Microsoft incident creation”-sääntöinä. Scheduled query -muotoiset säännöt ovat vapaamuotoisia kokonaisuuksia, joihin voidaan määrittää kattavakin toimintalogiikka, jolla tutkittavia poikkeamia havaitaan. Esimerkiksi jos haluttaisiin korostaa kirjautumistapahtumia, jotka tapahtuvat Suomen ulkopuolella virheellisten yritysten jälkeen onnistuneina, olisi kyselyn kirjoittaminen ja lisääminen sääntöön mahdollinen käyttäen kirjautumislokeista löytyvää IP-osoitetietoa, jolloin osuman löytymisen jälkeen korostettaisiin tapahtumasta tutkittava poikkeama. Havaintosäännöt kirjoitetaan käyttäen Microsoftin KQL-kyselykieltä (Kusto Query Language). (Sergiy Prystaiko 2021)

Toinen sääntötyyppi, Microsoft incident creation -sääntö, ei tue vapaamuotoisia kyselyjä, joilla datasta voitaisiin hakea tuloksia, vaan korostaa yksinomaan Microsoftin tietoturvatyökaluista tulleista hälytyksistä omia tutkintatapauksiaan. Nämä säännöt mahdollistavat nopeamman poikkeamakorostuksen luonnin Sentineelin tulevista hälytyksistä, mutta eivät tue yhtä kattavia sääntölogiikoita kuin Scheduled query -säännöt. Analytiikkasääntöjä luodessa on tärkeää ymmärtää, kuinka ajastaminen tapahtuu ja kuinka tutkimustapauksia luodaan. Tuntemalla alustan toiminta, voidaan ehkäistä ylimääräisten hälytysten ja tutkintatapausten luontia, jotka tyypillisesti hankaloittavat ratkaisun käsittelyä ja ylläpitoa. (Sergiy Prystaiko 2021)

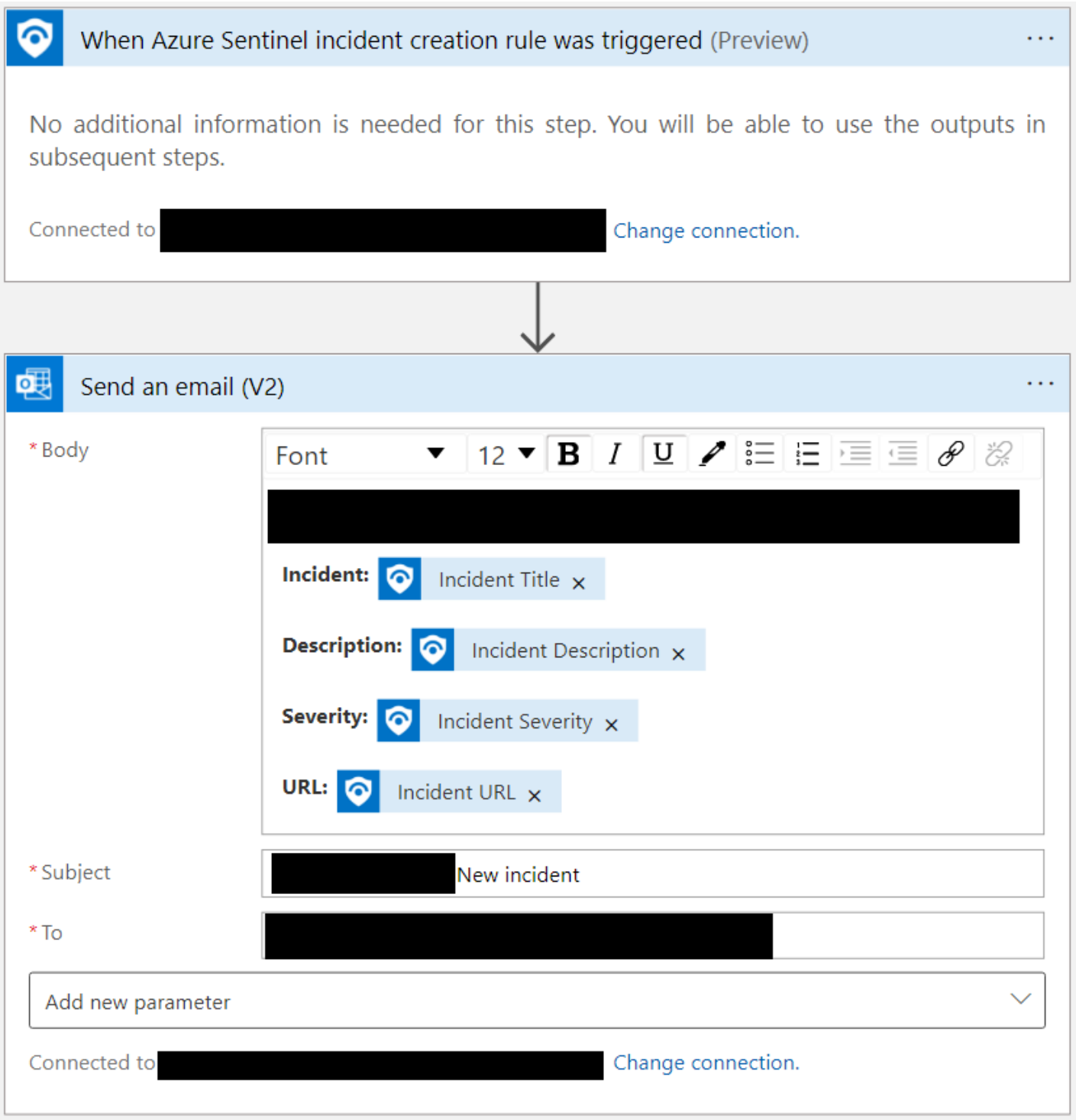
Analytiikkasääntöjä voidaan kytkeä päälle itsetehtyinä tai valmiista pohjasta luotuina. Microsoft ylläpitää Sentinelissä pohjakantaa, jota voidaan hyödyntää lokilähdekohtaisesti. Onkin suositeltavaa, että Sentineliä käyttöön otettaessa hyödynnetään kannasta jo löytyviä sääntöjä ympäristön mahdollisuuksien mukaisesti. (Sergiy Prystaiko 2021)

4.1.1 Automaation hyödyntäminen

Microsoft Sentinel tukee automaation hyödyntämistä tietoturvahäiriöiden havainnoinnin yhteydessä. Automaatiota voidaan toteuttaa kahdella tapaa; hyödyntämällä automaatiosääntöjä (automation rules) tai pelikirjoja (playbooks). Automaatiosääntöjä voidaan käyttää yksinkertaisten toimenpiteiden suorittamiseen, kuten häiriölöytöjen vakavuusasteen muuttamiseen tai omistajatiedon muokkaamiseen. Automaatiosäännöillä voidaan myös kohdentaa erillisiä, kattavampia pelikirjoja ajamaan itsensä määritettyjen ehtojen täyttyessä. Pelikirjat ovat puolestaan vapaamuotoisempia prosesseja, joihin voidaan määrittää kattavia määrä tapahtumia, myöskin ehdollisesti toteutuen. Pelikirjat ovat teknisemmältä nimeltään Azuressa käytettäviä Logic App -resursseja, joita on myös mahdollista hyödyntää Microsoft Sentinelin lisäksi muissa yhteyksissä tai yksittäisinä automaatioprosesseina. (Bridewell Consulting 2020)

Automaatiota käyttöön otettaessa, tulee miettiä tarvetta aina yksittäisten valvontasääntöjen kautta. On oleellista miettiä, voiko havaitusta häiriöstä seuraavia toimenpiteitä automatisoida, onko se tarpeellista ja ennen kaikkea, mikä häiriöhavainnon virheellisen aktivoitumisen todennäköisyys on. Jos on todennäköistä, että häiriöhavainto tehdään virheellisesti, on parempi hyödyntää yhteydessä automaatioprosessia, joka ei tee li. Esimerkkinä käyttäjätunnuksen lukitseminen on täysin mahdollista, mutta ei kannattavaa, jos uhkahavainnosta ei voida olla varmoja riittävällä todennäköisyydellä. Hyvänä esimerkkinä yleisestä automaatiomallista, jota voidaan soveltaa kaikkien havaintojen kanssa, voidaan käyttää viestintäautomaatiota, jossa määritetään viesti lähetettäväksi tietoturvavastaaville, kun uusi havainto syntyy. (Bridewell Consulting 2020)

Yksinkertaisen viestintäautomaation pohja on kuvattu kuvan 11 esittämässä Logic App -kuvauksessa, jolla uudesta tietoturvahäiriöhavainnosta lähetetään tieto sähköpostitse.



Kuva 11. Viestintäautomaation pohja

5 Datan visualisointi

Microsoft Sentinel tukee sisään tuodun datan käsittelytoiminnallisuutena myös datan visualisointia. Visualisoinnin natiivityökaluna käytetään Azuren workbook-resursseja, joita voidaan tallentaa Azureen pysyvinä näkyvinä. Workbookeja käytetään Azuressa lokidatan, metriikoiden sekä ulkoisten datalähteiden visualisointiin. Tuettuja visualisointimetodeja ovat muun muassa tekstit, kuvaajat, taulukot sekä kartat. Workbookit tukevat myös useamman datalähteen käyttöä, joten samaan raportointinäkymään voidaan tuoda tietoa samanaikaisesti eri sijainneista (Javier Soriano, 2020).

Microsoft Sentinel käyttää workbookeja ensisijaisena datan visualisointikeinona. Sentinel sisältää huomattavan määrän valmiita workbook-pohjia (templates), joilla sisään tuodusta datasta voidaan korostaa hyödyllistä tietoa. Microsoftin esituottamat pohjat on jaoteltu eri dataliitinten mukaisesti Sentinelissä käytettäväksi niin, että yleisimmät, tietoturvalle oleelliset korostukset saadaan välittömästi esitettyä. Workbook-pohjia löytyy tyypillisesti jokaista, Microsoftin toimesta virallisesti tuettua dataliitintä kohti vähintään yksi kappale. Yleisimpiä sisään tuotuja lokeja kohti, esimerkiksi Azure Active Directory -dataa, saattaa Microsoftin toimesta olla valmiina useampi pohja. Workbook-pohjia päivitetään Microsoftin toimesta säännöllisesti, etenkin uusien dataliitinten julkaisun yhteydessä. (Matthew Lowe 2020)

Sentinelin omat valmiit, esirakennetut workbookit korostavat lähdekohtaisesti keskeisiä asioita käsittelijälle. Jos tarkoituksena on visualisoida esimerkiksi ympäristön kirjautumislokia, saattaa esirakennettu workbook korostaa eri kirjautumissijainteja, poikkeavia kirjautumisia, käytettyjä päätelaitteita tai muita, tietoturvan kannalta mielenkiintoisia tekijöitä näkymässään. Näiden näkymien personointi yksilöllisiin, oman organisaation tarpeisiin on kuitenkin suositeltavaa ja usein välttämätöntä. Mahdollisuus integroida lokitieto Microsoftin raportointityökalu PowerBI:hin on mahdollista, joskin datan luvulle on määrättyjä rajoitteita, jos raportointi toteutetaan PowerBI:n kautta. (Matthew Lowe 2020)

5.1 Workbook-näkymien muokkaaminen

Vaikka Microsoft tarjoaakin workbook-näkymistä omat pohjansa, on workbookien muokkaaminen ja luominen suositeltavaa. Etenkin datalähteet, joita Microsoft ei virallisesti tue, vaativat oman, muokatun näkymänsä luonnin. Workbookien luonti onnistuu suoraan Microsoft Sentinelin omasta käyttöliittymästä, ”workbooks”-alueelta. (Matthew Lowe 2020)

Uuden workbookin kehittäminen alkaa aina samasta pohjasta Sentinelistä käynnistettynä. Pohjaa voidaan muokata valitsemalla ”Edit”-valinta vasemmasta yläkulmasta, jolloin

muokkausnäkymä aukeaa. Muokkaustilassa workbookiin voidaan vapaasti lisätä kyselyjä ja samalla päättää, missä muodossa ne visualisoidaan. Hyvänä käytäntönä workbookin rakentaminen kannattaa aloittaa lisäämällä ylös suodatusmahdollisuus, jolla visualisoitavaa datanäkymää voidaan suodattaa määritettyjen ehtojen mukaisesti. Esimerkiksi yleinen, kaikkiin kaavioihin vaikuttava aikavälin suodatin (Time Range parameter) on hyvä lisätä kaikkiin workbookeihin. (Matthew Lowe 2020)

Workbookeja voidaan muokata myös ”Advanced Editor” -toiminnon kautta valitsemalla ”</>”-ikoni. Tilassa workbookia voidaan käsitellä JSON-kielen muodossa. Workbookin näkymää editorissa voidaan vaihtaa ”Gallery Templaten” sekä ”ARM Templaten” välillä. Nämä kokoavat workbook-näkymän samaa kieltä käyttäen, hiukan eri muotoon. Liite 1 (hälytyskooste-workbook) toimii esimerkkinä workbookista Gallery Template -muotoisena. Hälytyskoostenäkymä sisältää tietoa halutulta aikaväliltä Sentinelin ”securityAlerts”-lokitiedosta. Näkymä koostaa yhteenvetona yleisimmät havaitut hälytykset sekä havaitut hyökkäystaktiikat. (Matthew Lowe 2020)

Workbookeja ei kuitenkaan tarvitse aina aloittaa puhtaalta pöydältä vaan myös Microsoftin valmiita, esirakennettuja pohjia voidaan lähteä mukauttamaan. Vaateena tälle on, että alkuperäisestä ”template”-pohjaversiosta tallennetaan erillinen workbook, jota voidaan sitten mukauttaa vapaasti ilman, että alkuperäinen pohjamalli muuntuu. Valmispohjat ovat usein hyvä lähtökohta kattavampien, omaan tarpeeseen räätälöityjen näkymien luomiseen. Valmispohjat sisältävät myös paljon käteviä KQL-kyselyitä, joista voidaan ottaa mallia ja joita voidaan kopioida suoraan sellaisenaan myös toisiin workbookeihin. (Matthew Lowe 2020)

Tietoturvakriittisten löydösten visualisoinnin lisäksi voidaan workbookeja myös suhteessa Sentinelin käyttötarkoitukseen hyödyntää muiden lähteiden esittämiseen. Esimerkiksi sisään tuodun datan määrän seuraaminen onnistuu helpoiten workbookien avulla, mikä avustaa ympäristön ylläpidossa sekä kustannusten hallinnassa. Myös sisäisten tapahtumien, kuten Sentinelin käytön valvonta onnistuu helposti workbookeilla. Näiden valmispohjien yhdistely on kannattavaa lähes jokaisessa ympäristössä niiden yleishyödyllisyyden ansiosta. (Nate Ruzicka 2021)

6 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli tutkia Microsoft Sentinelin toimintaa käytännössä ja muodostaa helppokäyttöinen, parhaita käytäntöjä korostava kuvaus ratkaisusta helpottamaan tulevia käyttöönottoja asiakasprojekteissa. Sentinelin tutkimus tehtiin toiminnallisesti asiakasprojektien yhteydessä niin, että käytännön työssä saatua kokemusta pystyttiin soveltamaan opinnäytetyön työstämisessä. Yleisten käytäntösuositusten, etenkin hinnoittelumallin sekä liitettävien datalähteiden näkökulmasta sovellettavan kokemuksen saaminen useammasta asiakasympäristöstä oli välttämätöntä. Tutkimustavoitteet, jotka työlle määrättiin, täyttyivät tarpeen mukaisesti.

Tutkimuskysymyksenä opinnäytetyötä ohjaamassa toimi; Mihin Microsoft Sentinelin käyttöönotossa tulee keskittyä, ja mitkä tekijät vaikuttavat käyttöönottoon eniten? Keskittyminen etenkin SIEM-ratkaisun käyttöönottoon varsinaisen arkipäiväisen käytön sijasta ohjasi opinnäytetyön laajuutta ja keskittymispisteiden valintaa voimakkaasti. Siinä missä kustannusten hallinta on äärimmäisen oleellinen osa käyttöönottoa kaikissa projekteissa, olisi esimerkiksi tutkimisprosessien ja kyvykkyyksien kuvaaminen ollut aiheellisempaa, jos työssä olisi keskitytty tuotantokäyttöön ja kehitykseen. Toimeksiantajan tarpeen huomioiden käyttöönoton kuvaus osoittautui kuitenkin enemmän aiheelliseksi.

Tutkimustyössä SIEM-ratkaisun käyttöönotosta havaittiin varhaisessa vaiheessa, kuinka merkittävässä asemassa etenkin kustannusten hallinnointi on käyttöympäristöissä. Jatkuvien kulujen selvittämisen merkitys ja ennakoiva hallinnointi koettiin lukuisissa asiakasprojekteissa merkittäväksi tekijäksi, minkä vuoksi aihetta päätettiin käsitellä painotetusti myös opinnäytetyön tuottamassa kuvauksessa. Kustannukset, ja ennen kaikkea niiden arviointi, osoittautuivat usein ratkaisevaksi tekijäksi siinä, missä kapasiteetissa ja millä kyvykkyyksillä Sentineliä päätettiin hyödyntää SIEM-ratkaisuna. Gigatavukohtainen hinnoittelumalli sallii joustavuuden ratkaisun lopullisen hinnan määräämisen suhteen, mutta ohjaa myös rajaamaan ja suunnittelemaan tarkkaan hyödynnettävän datan määrää.

Työssä korostettiin myös datalähteiden liittämistä, joka toimii oleellisena osana SIEM-ratkaisun käyttöönottoa. Etenkin Microsoft-pohjaiset datalähteet valikoituivat suosituslistalle ja parhaiden käytäntöjen korostukseen niiden helpon teknisen toteutuksen, sekä edullisemman käsittelymallin vuoksi. On myös huomioitava, että koska Microsoft Sentinel on Microsoftin omalla Azure-alustalla toimiva ratkaisu, on käyttöönottavalla organisaatiolla hyvällä todennäköisyydellä myös muita Microsoftin palveluita käytössä. Tästä johtuen näiden lähteiden korostaminen tietoturvakriittisinä sekä hyvinä valvonnan kohteina koettiin tärkeäksi.

Haasteena opinnäytetyön työstämisessä oli myös Sentineliin sovellettava jatkuvan kehityksen malli Microsoftin toimesta. Pilvipohjaisena tuotteena Sentineliin julkaistaan jatkuvasti uusia ominaisuuksia ja vanhoja toimintoja päivitetään, eikä muutosseuranta ole aina niin helppoa. Microsoft julkaisee muutoslokia uusista kehityksistä sivuillaan, mutta tiedot eivät usein ole kovin yksityiskohtaisia, eikä muutosloki aina sisällä ajankohtaisinta tietoa. Tästä johtuen tehokkain tapa muutosten seurannassa onkin ollut ulkoisten lähteiden, kuten konsulttien kirjoittamien blogien seuraaminen. Nämä lähteet auttoivat myös huomattavasti parhaiden käytäntöjen kartoittamisessa opinnäytetyötä työstettäessä. Tieteellisten lähteiden osalta tietoa Microsoft Sentinelistä on yhä kaksi vuotta ratkaisun virallisen julkaisun jälkeen saatavilla vähän, mistä johtuen toiminnallinen ja käytännönläheinen tutustuminen ratkaisuun oli mielestäni oikea.

Oman oppimisen osalta opinnäytetyön aihe oli erinomainen ja sen vaikutus työssä suoritettaviin tehtäviin huomattava. Microsoft Sentinelin käyttöönotot erityyppisissä asiakasorganisaatioissa ovat opinnäytetyön työstämisen aikana muodostuneet osaksi työni rutiinia, sekä toimeksiantajayrityksen palvelutarjontaa. Käytännön tekemisen kautta Sentinelin opiskelu ja parhaiden käytäntöjen dokumentointi on ollut huomattavasti helpompaa ja työn laadun ja merkityksen osalta parempaa kuin vaihtoehtoinen, teoriapainotteisempi ratkaisuun tutustuminen. Erilaisissa asiakasympäristöissä olen saanut todistaa korostettuna niin ratkaisun hyviä kuin huonoja puolia sekä sitä, kuinka oikeaoppisesti ratkaisun vahvuuksia tulee soveltaa eri ympäristöihin.

Opinnäytetyön työstämisen menetelmä oli projektin aikana toimiva, mutta aikataulullisesti työn teko pitkittyi huomattavasti alkuperäisestä suunnitelmasta etenkin toimeksiantajan kautta tehtyjen projektien vaikutuksen vuoksi. Tämä vaikutti negatiivisesti työn kehitykseen, vaikkakin pidempiaikainen tutustuminen paransi lopulta ymmärrystä Sentinelin osalta. Pitkäaikaisvaikutuksen osalta käytetty aika tulee hyvällä todennäköisyydellä olemaan kuitenkin hyvin tuottoisaa, huomioiden ratkaisun yleistymisen suomalaisella IT-kentällä ja toimeksiantajan asiakkuuksien keskuudessa. Jälkikäteen opinnäytetyön työstämistä kriittisesti ajatellen, ymmärrän, että varsinkin tarkemmalla aikatauluttamisella sekä aikatauluun sitoutumisella olisi opinnäytetyö itsessään kuitenkin saavuttanut paremman muodon, sekä sen hyötykäyttö olisi voitu aloittaa aiemmin toimeksiantajan käytössä. Myös ohjauksen parempi hyödyntäminen sekä aktiivisempi viestiminen projektin eri osapuoliin työstämisen aikana olisivat todennäköisesti parantaneet lopputulosta.

Microsoft Sentinelin kehittyessä, myös ratkaisun käyttöönottoon vaikuttavat osatekijät tulevat muuttumaan tulevien päivitysten myötä painoarvossaan. Tästä johtuen pilvipohjaisen SIEM-ratkaisun käyttöönottoon ohjaavia ohjenuoria ei voida kirjoittaa ylös vain kerran,

vaan ohjeistusta tulee ylläpitää ja päivittää myös ratkaisun kehityksen ohella. Kuvaus, joka opinnäytetyössä tuotettiin, palvelee kuitenkin hyvin suhteessa lähitulevaisuuden käyttöönottoihin, eivätkä painotetuimmat tekijät todennäköisesti tule vaihtumaan Sentinel-ratkaisun osalta lähiaikoina.

Lähteet

Adrian Valencia 2021. How to Get Cloud-Ready With Microsoft Cloud App Security. Luettavissa: https://www.avepoint.com/blog/protect/microsoft-cloud-app-security/. Luettu Luettu 26.11.2021

Ammar Hasayen 2021. P1: Microsoft Defender for Endpoint – Architecture. Luettavissa: https://blog.ahasayen.com/p1-microsoft-defender-for-endpoint-architecture/. Luettu 26.11.2021

Bridewell Consulting 2020. Automating Azure Sentinel: Using Playbooks to extract data. Luettavissa: https://www.bridewellconsulting.com/automating-azure-sentinel-using-playbooks-to-extract-data. Luettu 21.11.2021

CNBC 2021. Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem. Luettavissa: https://www.cnbc.com/2021/09/08/microsofts-20-billion-and-cybersecuritys-big-spending-problem.html Luettu: 14.11.2021

Forrester 2020. The Forrester Wave™: Security Analytics Platforms, Q4 2020. Luettavissa: https://reprints2.forrester.com/#/assets/2/108/RES157496/report. Luettu: 24.11.2021

Janakiram MSV 2020. A Look Back At Ten Years Of Microsoft Azure. Luettavissa: https://www.forbes.com/sites/janakirammsv/2020/02/03/a-look-back-at-ten-years-of-microsoft-azure/. Luettu 19.11.2021

Javier Soriano 2020. Making your Microsoft Sentinel Workbooks multi-tenant (or multi-workspace). Luettavissa: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/making-your-microsoft-sentinel-workbooks-multi-tenant-or-multi/ba-p/1402357. Luettu 26.11.2021

Joe Savini 2021. Microsoft Identity: Demystifying Defender for Identity and Azure Identity Protection. Luettavissa: https://redcanary.com/blog/microsoft-azure-identity/. Luettu 24.11.2021

Matthew Lowe 2020. Azure Sentinel Workbooks 101. Luettavissa: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-workbooks-101-with-sample-workbook/ba-p/1409216. Luettu 02.12.2021

Microsoft 2020a. Quickstart: On-board Microsoft Sentinel. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard Luettu: 05.05.2020.

Microsoft 2020b. Azure Monitor pricing. Luettavissa: https://azure.microsoft.com/en-us/pricing/details/monitor/. Luettu 05.05.2020.

Microsoft 2020c. Microsoft Sentinel pricing. Luettavissa: https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/. Luettu 05.05.2020.

Microsoft 2020d. Connect data from Azure Active Directory. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-active-directory. Luettu 05.05.2020.

Microsoft 2020e. Connect data from Office 365 Logs. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365. Luettu 05.05.2020.

Microsoft 2020f. Connect data from Azure Activity log. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-activity. Luettu 05.05.2020.

Microsoft 2020g. Connect data from Azure AD Identity Protection. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection. Luettu 05.05.2020.

Microsoft 2020h. Connect alerts from Microsoft Defender Advanced Threat Protection. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-microsoft-defender-advanced-threat-protection. Luettu 05.05.2020.

Microsoft 2020i. Connect data from Azure Advanced Threat Protection (ATP). Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-atp. Luettu 05.05.2020.

Microsoft 2020j. Connect data from Microsoft Cloud App Security. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-cloud-app-security. Luettu 05.05.2020.

Microsoft 2020k. Connect data from Azure Activity log. Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-activity. Luettu 05.05.2020.

Microsoft 2021a. Microsoft Cybersecurity Reference Architectures. Luettavissa: https://github.com/MicrosoftDocs/security/blob/main/Downloads/microsoft-cybersecurity-reference-architectures.pptx?raw=true. Luettu 17.11.2021

Microsoft 2021b. What is Microsoft Sentinel? Luettavissa: https://docs.microsoft.com/en-us/azure/sentinel/overview. Luettu 19.11.2021

Microsoft 2021c. What is Microsoft Defender for Cloud? Luettavissa: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction. Luettu 19.11.2021

Nate Ruzicka 2021. Microsoft Sentinel Workbooks that All SOCs Should Have. Luettavissa: https://cybermsi.com/blog/operations/azure-sentinel-workbooks-that-all-socs-should-have/. Luettu 02.12.2021

Rod Trent 2021. Security News Now – Microsoft Ignite 2021 Sentinel Edition. Luettavissa: https://azurecloudai.blog/2021/11/02/security-news-now-microsoft-ignite-2021-sentinel-edition/. Luettu 19.11.2021

Sean McAvinue 2021. Configuring Microsoft Defender for Office 365. Luettavissa: https://practical365.com/configuring-microsoft-defender-for-office-365/. Luettu 26.11.2021

Sergiy Prystaiko 2021. Creating Microsoft Azure Sentinel Rules in Your SIEM Instance. Luettavissa: https://socprime.com/blog/creating-microsoft-azure-sentinel-rules-in-your-siem-instance/. Luettu 02.12.2021

Liitteet

Liite 1. Hälytyskooste-workbook (Gallery Template)


```
{
  "version": "Notebook/1.0",
  "items": [
    {
      "type": 9,
      "content": {
        "version": "KqlParameterItem/1.0",
        "parameters": [
          {
            "id": "d840630a-80c6-4703-869b-5a7e3768ab55",
            "version": "KqlParameterItem/1.0",
            "name": "TimeRange",
            "type": 4,
            "isRequired": true,
            "value": {
              "durationMs": 172800000
            },
            "typeSettings": {
              "selectableValues": [
                {
                  "durationMs": 300000
                },
                {
                  "durationMs": 900000
                },
                {
                  "durationMs": 1800000
                },
                {
                  "durationMs": 3600000
                },
                {
                  "durationMs": 14400000
                },
                {
                  "durationMs": 43200000
                },
                {
                  "durationMs": 86400000
                },
                {
                  "durationMs": 172800000
                },
                {
                  "durationMs": 259200000
                },
                {
                  "durationMs": 604800000
                },
                {
                  "durationMs": 1209600000
                },
                {
                  "durationMs": 2419200000
                },
                {
                  "durationMs": 2592000000
                },
                {
                  "durationMs": 5184000000
                },
                {
                  "durationMs": 7776000000
                }
              ],
              "allowCustom": true
            },
            "timeContext": {
              "durationMs": 86400000
            }
          }
```

```
    ],
    "style": "pills",
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces"
   },
   "name": "parameters - 4"
  },
  {
   "type": 11,
   "content": {
    "version": "LinkItem/1.0",
    "style": "bullets",
    "links": [
     {
      "id": "5d64bdf9-a8b9-4637-91f5-fe67636b1bb3",
      "cellValue": "https://attack.mitre.org/tactics/enterprise/",
      "linkTarget": "Url",
      "linkLabel": "MITRE ATT&CK Tactics",
      "preText": "",
      "style": "link"
     }
    ]
   },
   "name": "links - 5"
  },
  {
   "type": 3,
   "content": {
    "version": "KqlItem/1.0",
    "query": "SecurityAlert\r\n| summarize count() by Tactics\r\n| order by count_ desc;",
    "size": 3,
    "title": "Detected MITRE ATT&CK Tactics",
    "timeContext": {
     "durationMs": 172800000
    },
    "timeContextFromParameter": "TimeRange",
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces",
    "visualization": "tiles",
    "tileSettings": {
     "showBorder": false,
     "titleContent": {
      "columnMatch": "Tactics",
      "formatter": 1
     },
     "leftContent": {
      "columnMatch": "count_",
      "formatter": 12,
      "formatOptions": {
       "palette": "auto"
      },
      "numberFormat": {
       "unit": 17,
       "options": {
        "maximumSignificantDigits": 3,
        "maximumFractionDigits": 2
       }
      }
     }
    }
   },
   "customWidth": "50",
   "name": "Detected MITRE ATT&CK Tactics"
  },
  {
   "type": 3,
   "content": {
    "version": "KqlItem/1.0",
    "query": "SecurityAlert\n| summarize count() by AlertName\n| order by count_ desc;",
    "size": 0,
    "title": "Most common alert types",
    "timeContext": {
     "durationMs": 172800000
    },
    "timeContextFromParameter": "TimeRange",
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces",
    "visualization": "piechart",
    "tileSettings": {
```

```
      "showBorder": false,
      "titleContent": {
        "columnMatch": "AlertName",
        "formatter": 1
      },
      "leftContent": {
        "columnMatch": "count_",
        "formatter": 12,
        "formatOptions": {
          "palette": "auto"
        },
        "numberFormat": {
          "unit": 17,
          "options": {
            "maximumSignificantDigits": 3,
            "maximumFractionDigits": 2
          }
        }
      }
    },
    "graphSettings": {
      "type": 0,
      "topContent": {
        "columnMatch": "AlertName",
        "formatter": 1
      },
      "centerContent": {
        "columnMatch": "count_",
        "formatter": 1,
        "numberFormat": {
          "unit": 17,
          "options": {
            "maximumSignificantDigits": 3,
            "maximumFractionDigits": 2
          }
        }
      }
    },
    "mapSettings": {
      "locInfo": "LatLong",
      "sizeSettings": "count_",
      "sizeAggregation": "Sum",
      "legendMetric": "count_",
      "legendAggregation": "Sum",
      "itemColorSettings": {
        "type": "heatmap",
        "colorAggregation": "Sum",
        "nodeColorField": "count_",
        "heatmapPalette": "greenRed"
      }
    }
  },
  "customWidth": "50",
  "name": "query - 2"
},
{
  "type": 3,
  "content": {
    "version": "KqlItem/1.0",
    "query": "SecurityAlert\r\n| summarize count() by AlertSeverity\r\n| order by count_ desc;",
    "size": 0,
    "timeContext": {
      "durationMs": 172800000
    },
    "timeContextFromParameter": "TimeRange",
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces",
    "visualization": "tiles",
    "tileSettings": {
      "showBorder": false,
      "titleContent": {
        "columnMatch": "AlertSeverity",
        "formatter": 1
      },
      "leftContent": {
        "columnMatch": "count_",
        "formatter": 12,
        "formatOptions": {
          "palette": "auto"
```

```
            },
            "numberFormat": {
              "unit": 17,
              "options": {
                "maximumSignificantDigits": 3,
                "maximumFractionDigits": 2
              }
            }
          }
        }
      },
      "customWidth": "50",
      "name": "query - 3"
    },
    {
      "type": 3,
      "content": {
        "version": "KqlItem/1.0",
        "query": "SecurityAlert\r\n| summarize count() by AlertName\r\n| order by count_ desc;",
        "size": 3,
        "title": "All alerts by sum",
        "timeContext": {
          "durationMs": 172800000
        },
        "timeContextFromParameter": "TimeRange",
        "queryType": 0,
        "resourceType": "microsoft.operationalinsights/workspaces",
        "visualization": "table"
      },
      "customWidth": "50",
      "name": "query - 2"
    },
    {
      "type": 3,
      "content": {
        "version": "KqlItem/1.0",
        "query": "SecurityAlert\r\n| summarize count() by AlertSeverity, bin(TimeGenerated, 1d)",
        "size": 3,
        "title": "Security Alerts Over Time by Severity",
        "timeContext": {
          "durationMs": 172800000
        },
        "timeContextFromParameter": "TimeRange",
        "queryType": 0,
        "resourceType": "microsoft.operationalinsights/workspaces",
        "visualization": "linechart"
      },
      "name": "SecurityAlertsOverTimebySeverity"
    }
  ],
  "fallbackResourceIds": [
    "/subscriptions/6352c0a1-3e5f-45c6-8802-e343dde30017/resourcegroups/sentinel-rg/providers/microsoft.operation-
alinsights/workspaces/siemdemo"
  ],
  "fromTemplateId": "sentinel-UserWorkbook",
  "$schema": "https://github.com/Microsoft/Application-Insights-Workbooks/blob/master/schema/workbook.json"
}
```