LAPIN AMK
Lapland University of Applied Sciences

MICROSOFT DEFENDER FOR CLOUDIN TEKNOLOGIAKATSAUS

Lukkari Ville

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2024

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Ville Lukkari	**Vuosi**	2024
Ohjaaja	Kenneth Karlsson		
Toimeksiantaja	Lapin ammattikorkeakoulu		
Työn nimi	Microsoft Defender for Cloudin teknologiakatsaus		
Sivumäärä	24		

Tämän opinnäytetyön tarkoituksena on tehdä materiaali Microsoft Defender for Cloudista Lapin ammattikorkeakoulun tieto- ja viestintätekniikan koulutuksen käyttöön. Materiaali auttaa päättämään tarvetta tälle palvelulle sekä antaa joitain näkemyksiä sen tarpeellisuudesta ja vaativuudesta.

Työssä käytetty tieto perustuu pitkälti Microsoftin omiin dokumentaatioihin sekä ohjeisiin, jotka tarjoavat kattavan yleiskuvan Microsoft Defender for Cloudin toiminnasta ja parhaista käytännöistä sekä siitä, kuinka integraatio muihin tietoturvatyökaluihin on sujuvaa.

Opinnäytetyössä käydään läpi pilvipalveluita, GDPR- ja CCPA-asetuksia, jotka ovat keskeisiä Microsoft Defender for Cloudin käyttöönotossa. Nämä asetukset edellyttävät organisaatioilta tiukkoja toimenpiteitä henkilötietojen suojaamiseksi. Tämä tieto auttaa lukijoita ymmärtämään paremmin, kuinka Microsoft Defender for Cloud sopii laajempaan tietosuojaan ja turvallisuusympäristöön. Opinnäytetyöstä rajattiin pois Microsoft Defender for Cloudin asennus tai kustannuksiin liittyvät asiat, koska ne voivat vaihdella suuresti organisaation koosta, tarpeista ja resursseista riippuen.

Opinnäytetyön tuloksena syntyi teknologiakatsaus Microsoft Defender for Cloudista Lapin ammattikorkeakoululle. Katsaus auttaa ymmärtämään Defender for Cloudin monimutkaisuutta, sen integraatiota M365:een ja Azureen sekä merkitystä GDPR:n ja CCPA:n vaatimusten täyttämisessä. Se korostaa pilvipalveluiden keskeistä roolia tietoturvan prantamisessa ja toimii oppimateriaalina opiskelijoille ja organisaatioille, jotka harkitsevat palvelun käyttöönottoa.

Avainsanat pilvipalvelut, tietosuoja, tietotekniikka, tietoturva

Abstract of Thesis

LAPIN AMK
Lapland University of Applied Sciences

Degree Programme in Information and Communication Technology
Bachelor of Engineering

Author	Ville Lukkari	**Year**	2024
Supervisor	Kenneth Karlsson		
Commissioned by	Lapland university of Applied Sciences		
Subject of thesis	Technology review of Microsoft Defender for Cloud		
Number of pages	24		

The purpose of this thesis study was to create a resource on Microsoft Defender for Cloud for the Information and Communication Technology program at Lapland University of Applied Sciences. This resource will assist in determining the need for this service and provide insights into its necessity and complexity.

The information used in this study was largely based on Microsoft's own documentation and guidelines, which provide a comprehensive overview of the operation of Microsoft Defender for Cloud and best practices, as well as how integration with other cybersecurity tools is seamless. GDPR, and CCPA regulations, which are crucial in the implementation of Microsoft Defender for Cloud were examined. These regulations require organizations to take stringent measures to protect personal data. This information helps readers better understand how Defender for Cloud fits into a broader data protection and security environment. The installation of Microsoft Defender for Cloud or issues related to cost were excluded, as they can vary greatly depending on the size, needs, and resources of the organization.

As a result of the thesis, a "Technology Review of Microsoft Defender for Cloud" was created for Lapland University of Applied Sciences. The review helps to understand the complexity of Defender for Cloud, its integration with M365 and Azure, and its significance in meeting GDPR and CCPA requirements. It emphasizes the central role of cloud services in improving cybersecurity and serves as learning material for students and organizations considering the implementation of the service.

Key words: cloud services, data protection, information security, information technology

SISÄLLYS

ALKUSANAT

Kiitos perheelleni, joka on ollut mukana tällä pitkällä ja välillä kivisellä matkallani kohti uutta alkua. Teimme sen yhdessä. Haluan myös kiittää kaikkia, jotka oikolukivat tekstini, ehdottivat muutoksia ja arvioivat sitä.

KÄYTETYT LYHENTEET

CCPA	California Consumer Privacy Act, Kalifornian tietosuoja-laki. (Kalifornian oikeusministeriö 2023)
CNAPP	Cloud-Native Application Protection Platform (Microsoft Security 2024)
DDoS	Distributed Denial of Service (Cloudfare 2024)
EDR	Endpoint Detection and Response (Aarness 2023)
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus (Euroopan unioni 2022)
IoT	Internet of Things, Esineiden internet, (IBM 2024)
M365	Microsoft 365 (Microsoft 2024)
MCSB	Microsoft Cloud Security Benchmark (Baldwin, Bathini, & Buck 2023)
MDC	Microsoft Defender for Cloud (Curwin ym. 2023)
MFA	Multi-Factor Authentication, monimenetelmäinen tunnistautuminen (IT-Palvelut 2024)
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö (Kyberturvallisuuskeskus 2019)

1 JOHDANTO

Teknologian kehittyessä ja digitaalisen tiedon määrän kasvaessa, tietoturvan merkitys on noussut entistä tärkeämmäksi. Organisaatiot etsivät jatkuvasti tehokkaita ratkaisuja suojatakseen arkaluontoiset tiedot ja varmistaakseen liiketoimintansa jatkuvuuden. Tässä yhteydessä Microsoft Defender for Cloud tarjoaa kattavan ratkaisun pilvipohjaisten resurssien suojaamiseen.

Microsoft Defender for Cloud on Microsoftin tarjoama turvallisuusratkaisu, joka on suunniteltu suojaamaan pilvipalveluita erilaisilta uhkilta. Se tarjoaa laajan valikoiman työkaluja ja ominaisuuksia, jotka auttavat organisaatioita hallitsemaan tietoturvaa, tunnistamaan ja reagoimaan uhkiin sekä noudattamaan tietosuoja-asetuksia, kuten GDPR ja CCPA. (Chauhan 2023).

Tämän opinnäytetyön tarkoituksena on tarjota yksityiskohtainen opas Microsoft Defender for Cloudin käyttöön. Opas auttaa lukijoita ymmärtämään palvelun tarpeellisuuden, vaativuuden ja tarpeellisuuden, ja se tarjoaa näkemyksiä siitä, kuinka palvelu voi auttaa organisaatioita parantamaan tietoturvaa ja noudattamaan tietosuoja-asetuksia. On tärkeää huomata, että vaikka tämä työ keskittyy Microsoft Defender for Cloudin toiminnallisuuteen ja hyötyihin, se ei käsittele palvelun asennusta tai kustannuksia. Sen sijaan työ tarjoaa lukijoille yleiskuvan palvelusta, sen tarpeellisuudesta ja siitä, kuinka se voi auttaa organisaatioita parantamaan tietoturvaa ja noudattamaan tietosuoja-asetuksia.

Tämä opinnäytetyö käsittelee myös GDPR:n ja CCPA:n jotka tulee huomioida Microsoft Defender for Cloudin käyttöönotossa. Nämä ovat keskeisiä tietosuoja-asetuksia, jotka vaikuttavat siihen, kuinka organisaatiot käsittelevät henkilötietoja ja miten ne suojaavat näitä tietoja.

Lisäksi työssä tarkastellaan erilaisia pilvipalveluita ja niiden turvallisuusnäkökohtia. Pilvipalvelut ovat nykyään olennainen osa monien organisaatioiden IT-infrastruktuuria, ja niiden turvallinen käyttö on tärkeää tietoturvan kannalta.

Microsoftin Copilot-tekoälyä on hyödynnetty työssäni erityisesti osioissa Termit ja lyhenteet sekä Lähdeluettelo, jossa se on auttanut aakkostuksessa.

2 PILVIPALVELUT

Pilvipalveluilla tarkoitetaan internet-palveluita, joihin voidaan tallentaa esimerkiksi valokuvia, musiikkia, dokumentteja sekä muita tiedostoja. Pilvipalveluiden etuina ovat, että niihin tallennettuihin tietoihin on mahdollista päästä käsiksi millä tahansa internet-yhteydellä varustetulla laitteella, kuten tietokoneella, älypuhelimella, tabletilla tai vaikka älytelevisiolla. Kun tiedostot tai ohjelmistot ovat pilvessä, ne eivät ole omalla tietokoneella tai yrityksen omalla palvelimella vaan yrityksen palvelimella, joka tarjoaa pilvipalveluja. Käytännössä pilvi tarkoittaa palvelimien (tietokoneiden) verkostoa. (Vähälummukka 2023.) Swyx Solutions -yrityksen toimitusjohtaja Ralf Ebbinghaus on kuvaillut pilvipalvelua seuraavasti. Se on vähän kuin käyttäisit taivaalla olevaa kirjastoa, jossa voit valita erityyppisistä peleistä, elokuvista tai muista sovelluksista ja maksaa käyttämistäsi - mutta kuin kirjasto, jota et koskaan omista. (Macrae 2023.)

Pilvipalvelut jaotellaan tyypillisesti kolmeen pääluokkaan perustuen niiden tarjoamaan jalostusasteeseen. Lisäksi on olemassa useita hankintamalleja, kuten IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service). Nämä mallit määrittävät, kuinka paljon vastuuta käyttäjä haluaa ottaa hankkimastaan palvelusta. (Floor 2024, 5.)

IaaS

Infrastructure as a Service on palvelu, joka tarjoaa samankaltaisia palvelinratkaisuja kuin perinteiset, omassa konesalissa sijaitsevat järjestelmät. Sen etuna on, että lisäkapasiteetti on helppo hankkia ja laitteiston ylläpidosta vastaa palveluntarjoaja. IaaS sisältää käytännössä levyjärjestelmiä, verkkoa ja palvelinresursseja. Kun tarkastellaan IaaS-kapasiteettia, huomataan, että eri pilvipalveluntarjoajien välillä on yhtäläisyyksiä kustannuksissa ja ominaisuuksissa. (Floor 2024, 6.)

Vaikka eroavaisuuksia löytyy, ne eivät usein ole ratkaisevia tekijöitä palveluntarjoajan valinnassa. Hinnoittelua määrittävät tekijät, kuten palvelininstanssien koko, kapasiteetin tyyppi (on-demand tai reserved), käyttöaika, arkkitehtuuri ja teknologiset ratkaisut, kuten konttiteknologia, ovat merkittäviä. Käyttämällä IaaS-kapasiteettia, asiakkaat säilyttävät suuren määrän kontrollia, sillä esimerkiksi

virtuaalisen instanssin siirto eri pilvipalveluiden välillä on mahdollista. Tämän tyylisiä palveluita tarjoavat muun muassa Amazon Web Services (AWS), Microsoft Azure ja Google Cloud Platform. (Floor 2024, 6.)

2.1 PaaS

Platform as a Service tarjoaa alustakomponentteja palveluna, mikä tekee sovellusten kehittämisestä yksinkertaisempaa ja nopeampaa. Kehittäjien ei tarvitse huolehtia palvelun päivityksistä tai toiminnan monimutkaisista yksityiskohdista, sillä näistä vastaa alustan tarjoaja. Lisäksi alusta automaattisesti skaalaa laskentakapasiteettia käyttökuorman mukaisesti.

PaaS-palvelut ovat keskeisessä asemassa, kun pohditaan toimittajariippuvuutta. PaaS-komponenttien käyttö johtaa vahvaan sitoutumiseen alustan toimittajaan, mikä voi olla sekä hyödyksi että haitaksi. Toisaalta valmiiden komponenttien avulla oman palvelun rakentaminen on huomattavasti kustannustehokkaampaa kuin vastaavan itse rakennetun toteutuksen. AWS:n ja Azuren kaltaiset palveluntarjoajat kehittävät jatkuvasti uusia kustannustehokkaita palveluita. Tämän ansiosta tietokantojen, analytiikan, koneoppimisen ja esineiden internetin (IoT) palvelut ovat kehittyneet merkittävästi. (Floor 2024, 7.)

2.2 SaaS

Software as a Service on palvelumalli, jossa loppukäyttäjille suunnattu sovellus tarjotaan palveluna. SaaS-palveluiden valikoima kasvaa jatkuvasti ja ne ovat yritysten eniten käyttämiä pilvipalveluita. Esimerkkejä SaaS-palveluista ovat muun muassa sähköposti, kuten O365, sekä erilaiset taloushallinnon sovellukset. (Floor 2024, 8.)

SaaS-malli tarjoaa asiakkaalle ratkaisun, jossa palveluntarjoaja huolehtii kaikista yksityiskohdista. Palvelu voidaan toteuttaa joko toimittajan omassa konesalissa tai julkisessa pilvessä, esimerkiksi hyödyntäen AWS:n PaaS-komponentteja. ITaaS (IT as a Service) on toinen esimerkki SaaS-mallista, jossa yritys hankkii kokonaisvaltaisen IT-ratkaisun palveluna. (Floor 2024, 8.)

2.3 on-premise

On-premise-ratkaisu tarkoittaa, että yrityksen laitteistot sijaitsevat yrityksen omassa tilassa. Tämä ratkaisu on erityisen hyödyllinen, jos yrityksessä on investoitu merkittävästi IT-infrastruktuuriin ja IT-osaamiseen. (Koistinen 2021.)

On-premise-ratkaisun etuja ovat täysi hallinta ja mukautettavuus. Organisaatiot voivat hallita täysin omaa infrastruktuuriaan ja mukauttaa sitä tarpeidensa mukaan. Tietoturvan kannalta on-premise on kannattava, koska tiedot säilytetään paikan päällä, ja organisaatiot voivat hallita tietoturvaa ja noudattaa tiukkoja tietosuojastandardeja. (Kemper 2021.)

On-premise-ratkaisun haittapuolia ovat suuret alkuinvestoinnit laitteistoon ja ohjelmistoihin. Lisäksi ylläpidon haasteet voivat olla merkittäviä, koska organisaation on itse huolehdittava järjestelmän ylläpidosta, päivityksistä ja tietoturvasta. (Kemper 2021.)

Kun organisaatio laajenee ja tarvitsee lisää tallennuskapasiteettia tai muita toimintoja, paikan päällä olevien palvelimien nopea skaalaaminen voi olla haastavaa. Pilvitallennuksen avulla organisaatiot voivat helposti valita laajemman paketin yhdellä klikkauksella, mutta paikan päällä olevan tallennuksen laajentaminen vaatii uuden laitteiston asentamista ja henkilöstöresurssien kohdentamista uusien järjestelmien rakentamiseen. (Morefield 2022.)

Forbesin kirjoittajan Nazariy Hazdunin mukaan on-premise-palveluiden merkittäviä etuja ovat tietoturva ja resurssien hallinta. Kun yritys hallitsee omaa fyysistä palvelintaan, sillä on täysi kontrolli ja omistusoikeus tietojen ja resurssien turvallisuuteen. Tämä tarkoittaa, että IT-tiimi voi puuttua kaikkiin mahdollisiin haavoittuvuuksiin. (Hazdun 2023.)

3 PILVIPALVELUTURVALLISUUS

Pilvipalveluiden turvallisuus on keskeinen huolenaihe monille organisaatioille ja yksityishenkilöille, jotka siirtävät tietojaan ja sovelluksiaan pilveen (Kyberturvallisuuskeskus 2019a, 6). Pilvipalveluiden turvallisuuden perusta on CIA-triadi: luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability). Nämä kolme periaatetta muodostavat tietoturvan perustan. (Fortinet 2024.)

Luottamuksellisuus tarkoittaa, että vain oikeutetut käyttäjät pääsevät käsiksi tietoihin. Eheys tarkoittaa, että tiedot säilyvät muuttumattomina ja että kaikki muutokset ovat luvallisia ja hallittuja. Saatavuus tarkoittaa, että tietoihin pääsee käsiksi. (Kyberturvallisuuskeskus 2019a, 4.)

Yllä mainittujen periaatteiden noudattaminen on välttämätöntä pilvipalveluiden turvallisuuden kannalta. Kuitenkin, kun tarkastellaan pilvipalveluiden turvallisuutta, on tärkeää ymmärtää, että turvallisuus ei ole yksinomaan tekninen kysymys. Se on myös organisaation kulttuurin, politiikan ja prosessien kysymys. (Kyberturvallisuuskeskus 2019a, 6.)

3.1 EU-SEC

EU-SEC (European Security Certification Framework) on projekti, jonka tavoitteena on luoda eurooppalainen viitekehys pilvipalveluiden turvallisuuden sertifiointijärjestelmille ja arviointikäsitteille. Tämän viitekehyksen sisällä olemassa olevat kansalliset ja kansainväliset sertifikaatit voivat toimia rinnakkain. (EU-SEC 2019.)

EU-SEC pyrkii parantamaan olemassa olevien pilvipalveluiden turvallisuuden sertifiointijärjestelmien liiketoiminta-arvoa sekä tehokkuutta ja vaikuttavuutta. EU-SEC-projekti pyrkii edistämään pilvi-infrastruktuurien luotettavuutta, turvallisuutta ja vaatimustenmukaisuutta. (EU-SEC 2019.)

Tämän tavoitteen saavuttamiseksi on täytettävä seuraavat vaatimukset EU-SEC mukaan:

- Olemassa olevat kansalliset ja sektorikohtaiset sertifiointijärjestelmät on otettava huomioon ja tasapainotettava: Tämä tarkoittaa, että EU-SEC-projektin on otettava huomioon eri maiden ja toimialojen erityisvaatimukset ja -standardit, jotta voidaan varmistaa, että sertifiointijärjestelmä on yhteensopiva ja tasapainoinen.
- Pilvipalveluntarjoajien (CPS) sertifiointikustannukset on vähennettävä: Tämä tarkoittaa, että EU-SEC-projektin on pyrittävä vähentämään pilvipalvelutarjoajien sertifiointikustannuksia, jotta sertifiointi olisi houkuttelevampaa ja saavutettavampi vaihtoehto.
- Sertifiointi- ja arviointitoiminnot, jotka voidaan hoitaa automaattisesti koneilla (esim. datan kerääminen), eivät saisi vaatia manuaalista käsittelyä ihmisten toimesta: Tämä tarkoittaa, että EU-SEC-projektin on pyrittävä automatisoimaan mahdollisimman paljon sertifiointi- ja arviointiprosesseja, jotta voidaan vähentää manuaalisen työn tarvetta ja parantaa prosessien tehokkuutta.
- Tarkkaa ja luotettavaa tietoa tulisi olla saatavilla valtuutetuille henkilöille automatisoiduin keinoin: Tämä tarkoittaa, että EU-SEC-projektin on varmistettava, että valtuutetuilla henkilöillä on pääsy tarkkaan ja luotettavaan tietoon automatisoiduin keinoin, jotta he voivat tehdä tietoon perustuvia päätöksiä. (EU-SEC 2019.)

EU-SEC-projektin kehittämän viitekehyksen keskeiset näkökohdat ovat seuraavat:

- automaatio: prosessien tehostaminen ja nopeuttaminen
- hallinto: järjestelmän ja sen resurssien tehokas johtaminen
- sertifikaattien keskinäinen tunnustaminen: eri sertifikaattien yhteensopivuuden ja hyväksynnän varmistaminen
- jo sertifioitujen komponenttien uudelleenkäytettävyys: olemassa olevien, sertifioitujen komponenttien hyödyntäminen uusissa yhteyksissä
- jatkuva tarkastus ja seuranta: järjestelmän tilan ja turvallisuuden aktiivinen valvonta

- pilvipalveluiden sertifiointiprosessien kokonaiskeston ja -kustannusten vähentäminen: pilvipalveluiden sertifiointimenettelyjen tehostaminen ja kustannustehokkuuden parantaminen. (EU-SEC 2019.)

Nämä vaatimukset ja näkökohdat muodostavat yhdessä viitekehyksen, joka ohjaa EU-SEC-projektin työtä ja edistää sen tavoitteita. Tämä viitekehys on keskeinen osa projektin strategiaa ja se auttaa projektia panostamaan Digitaalisten sisämarkkinoiden strategiaan, Euroopan pilvialoitteeseen, tulevaan NIS-direktiiviin sekä yleiseen tietosuoja-asetukseen, GDPR:ään. (EU-SEC 2019.)

3.2 PiTuKri

On Kyberturvallisuuskeskuksen kehittämä työkalu, joka julkaistiin ensimmäisen kerran 29. toukokuuta 2019. PiTuKri on suunniteltu tukemaan pilvipalveluiden turvallisuuden arviointia. PiTuKri on laadittu Suomen kansallisten tarpeiden näkökulmasta ja se ottaa kantaa sekä viranomaisten kansallisiin salassa pidettäviin, että turvallisuusluokiteltuihin IV-luokan salassa pidettäviin tietoihin. (Kyberturvallisuuskeskus 2019, 3.)

PiTuKri sisältää tulkintoja ja ohjeistuksia pilvipalveluihin liittyvien riskien arviointiin. Lisäksi siihen on koottu pilvipalvelujen turvallisuuteen vaikuttavia hyviä käytäntöjä, joita voivat hyödyntää myös kaupalliset toimijat (Valtiovarainministeriö 2022, 22). Kriteeristö on hyödyllinen työkalu uusien pilvipalveluiden hankinnassa ja jo käytössä olevien pilvipalveluiden suojausten arvioinnissa (Pahlman 2024).

Kyberturvallisuuskeskus on sitoutunut jatkamaan PiTuKrin kehittämistä ja kerää parhaillaan palautetta ja ehdotuksia sen jatkokehitystä varten. Kriteeristöä voidaan käyttää myös viranomaisten julkisten tietojen suojaamiseen sekä elinkeinoelämän tarpeisiin. (Pahlman 2024.)

Esimerkiksi tietoliikenneturvallisuus on yksi PiTuKrin keskeisistä osa-alueista. Tämä on erityisen merkittävää pilvipalveluissa, joissa tieto kulkee usein verkon kautta. PiTuKri tarjoaa tarkistuslistan, joka auttaa varmistamaan, että kaikki tietoliikennetuvallisuuden kannalta keskeiset seikat otetaan huomioon. (Kyberturvallisuuskeskus 2019, 33.)

3.3 FedRAMP

Federal Risk and Authorization Management Program on Yhdysvaltain hallituksen ohjelma, joka tarjoaa standardoidun lähestymistavan pilvipalveluiden turvallisuuden arviointiin, valtuutukseen ja jatkuvaan seurantaan. FedRAMP mahdollistaa virastojen käyttää moderneja pilviteknologioita, keskittyen turvallisuuteen ja liittovaltion tiedon suojaamiseen, ja auttaa nopeuttamaan turvallisten pilviratkaisujen käyttöönottoa. (GSA 2019.)

FedRAMP koostuu kahdesta pääosasta: Joint Authorization Board (JAB) ja Program Management Office (PMO). JAB:n jäseniä ovat puolustusministeriön, kotimaan turvallisuuden ministeriön ja yleisten palveluiden hallinnon tietohallintojohtajat. JAB toimii FedRAMP:n ensisijaisena hallinto- ja päätöksentekoelimenä. FedRAMP PMO sijaitsee GSA:ssa ja tukee virastoja ja pilvipalveluntarjoajia FedRAMP-valtuutusprosessissa ja ylläpitää turvallista FedRAMP-valtuutusten arkistoa, jotta turvallisuuspaketteja voidaan käyttää uudelleen. (GSA 2019.)

3.4 NIST

National Institute of Standards and Technology on Yhdysvaltain hallituksen virasto, joka on kehittänyt useita standardeja ja ohjeistuksia kyberturvallisuuden alalla. Nämä ohjeistukset auttavat organisaatioita parantamaan tietoturvaa ja hallitsemaan kyberturvallisuusriskejä. (NIST 2024.)

Yksi tunnetuimmista NISTin julkaisemista kyberturvallisuusstandardeista on NIST Cybersecurity Framework. Tämä viitekehys tarjoaa organisaatioille ohjeistuksen kyberturvallisuuden parantamiseksi. Se sisältää parhaita käytäntöjä, jotka auttavat organisaatioita tunnistamaan, hallitsemaan ja vähentämään kyberturvallisuusriskejä. Viitekehys on suunniteltu olemaan joustava ja räätälöitävissä organisaation tarpeiden mukaan. (NIST 2024.)

NIST:n kyberturvallisuusohjeistukset kattavat laajan valikoiman aiheita, mukaan lukien pilvipalvelut, identiteetin hallinta, tietoturvan riskienhallinta, tietoturva-arkkitehtuurit, tietoturvan mittarit ja indikaattorit, sekä tietoturvan auditointi ja

sertifiointi. NIST:n julkaisemat ohjeistukset ja standardit ovat saatavilla vapaasti NIST:n verkkosivuilta. Ne ovat arvokas resurssi kaikille organisaatioille, jotka pyrkivät parantamaan kyberturvallisuuttaan. (NIST 2024.)

4 TIETOSUOJAHAASTEET

4.1 GDPR:n ja CCPA:n vaikutus pilvipalveluihin

Pilvipalvelut mahdollistavat palveluiden ja sovellusten maailmanlaajuisen saatavuuden. Tämä tuo mukanaan tietoturvaan liittyviä haasteita, koska eri maiden ja alueiden tietosuojalait ja -määräykset voivat vaihdella huomattavasti. Esimerkiksi Euroopassa GDPR asettaa tiukkoja vaatimuksia henkilötietojen käsittelylle, kun taas Yhdysvalloissa on omat tietosuojasäädöksensä, kuten CCPA, joka eroaa eurooppalaisista vaatimuksista. On tärkeää ymmärtää ja noudattaa näitä eroja, kun käsitellään tietoja eri puolilla maailmaa. (Sjoera 2021.)

CCPA ja GDPR ovat molemmat lakeja, jotka on luotu antamaan yksilöille enemmän valtaa heidän henkilötietojensa suhteen ja sääntelevät organisaatioita, jotka keräävät ja käyttävät tietoja eri tavoin. CCPA antaa Kalifornian asukkaille lisääntynyttä läpinäkyvyyttä ja kontrollia siitä, miten yritykset keräävät ja käyttävät heidän tietojaan, ja sovelletaan yleisesti organisaatioihin, jotka harjoittavat liiketoimintaa Kaliforniassa, sekä niihin, jotka käsittelevät tai jakavat Kalifornian asukkaiden henkilötietoja. Kun taas GDPR antaa Euroopan unionin asukkaille lisääntynyttä läpinäkyvyyttä ja kontrollia siitä, miten yritykset keräävät ja käyttävät heidän tietojaan, ja sovelletaan organisaatioihin EU:n sisällä ja sen ulkopuolella, jotka käsittelevät EU:n asukkaiden henkilötietoja. (Kucera 2021.)

CCPA pyrkii lisäämään läpinäkyvyyttä Kalifornian asukkaille, antaen heille mahdollisuuden ymmärtää, miten heidän tietojaan kerätään ja käsitellään. Se antaa oikeuksia kuluttajille, jotka ovat Kalifornian asukkaita, käsittelee henkilötietoja, jotka tunnistavat, liittyvät, kuvaavat tai voidaan kohtuullisesti liittää kuluttajaan tai kotitalouteen, ja sääntelee voittoa tavoittelevia yrityksiä, jotka toimivat Kaliforniassa ja täyttävät useita taloudellisia ehtoja sekä heidän palveluntarjoajiaan.
Toisaalta GDPR sääntelee tietosuojaa koko EU:ssa, korvaten joitakin tietosuojalakeja Euroopassa yhdellä yhtenäisellä viitekehyksellä. Se antaa oikeuksia tietosubjekteille, jotka ovat EU:n asukkaita, käsittelee yksilön henkilötietoja (ei sisällä kotitalouksia, vain anonymisoitu data on poikkeus), ja sääntelee tietojen ohjaajia ja prosessoreita, jotka käsittelevät EU:n yksilöiden henkilötietoja.

Molemmat asetukset syntyivät suojaamaan ihmisiä maailmassa, jossa kansainväliset henkilötietojen siirrot ovat yhä yleisempiä ja monimutkaisempia, ja teknologian kehitys on johtanut tietojen väärinkäyttöskandaaleihin ja monimutkaisiin kyberhyökkäyksiin. CCPA ja GDPR soveltuvat eri organisaatioihin eri tavoin, ja vaikka molempien lainsäädäntöjen soveltamisalassa on joitakin eroja, ne jakavat samanlaisia tavoitteita. Tarkastelemalla, miten ne täydentävät toisiaan, voidaan luoda skaalautuvia tietosuoja- ja tietoturvapolitiikkoja, jotka noudattavat molempia lakeja. On tärkeää huomata, että GDPR:llä on vaikutuksia myös Yhdysvalloissa toimiviin yrityksiin, huolimatta siitä, että se on peräisin Euroopasta. (Kucera 2021.)

Molemmat asetukset syntyivät suojaamaan ihmisiä maailmassa, jossa kansainväliset henkilötietojen siirrot ovat yhä yleisempiä ja monimutkaisempia, ja teknologian kehitys on johtanut tietojen väärinkäyttöskandaaleihin ja monimutkaisiin kyberhyökkäyksiin. CCPA ja GDPR soveltuvat eri organisaatioihin eri tavoin, ja vaikka molempien lainsäädäntöjen soveltamisalassa on joitakin eroja, ne jakavat samanlaisia tavoitteita. Tarkastelemalla, miten ne täydentävät toisiaan, voidaan luoda skaalautuvia tietosuoja- ja tietoturvapolitiikkoja, jotka noudattavat molempia lakeja. (Kucera 2021.)

4.2 Henkilötietojen määrittely

CCPA määrittelee henkilötiedot kaikkina tietoina, jotka tunnistavat, kuvaavat, liittyvät tai voidaan kohtuullisesti liittää kuluttajaan tai kotitalouteen. GDPR:n mukaan henkilötiedot viittaavat kaikkiin tietoihin, jotka suoraan tai epäsuorasti tunnistavat jonkun. Joitakin esimerkkejä “henkilötiedoista” ja “henkilötiedoista” ovat täydellinen nimi, sähköpostiosoitteet, viralliset asiakirjanumerot (esim. passi, ajokortti ja sosiaaliturva) ja online-tunnisteet. On tärkeää ottaa huomioon, että CCPA jättää joitakin erityisiä luokkia soveltamisalansa ulkopuolelle, kuten tietyt lääketieteelliset tiedot. Vaikka asetukset käyttävät erilaisia termejä hieman vaihtelevilla määritelmillä, “henkilödata”, “henkilötiedot” ja “henkilökohtaisesti tunnistettavat tiedot (PII)” käytetään usein vaihtoehtoisesti. (Kucera 2021.)

CCPA että GDPR on suunniteltu suojaamaan tiettyjä ryhmiä. CCPA keskittyy kuluttajiin, jotka ovat luonnollisia henkilöitä ja Kalifornian asukkaita. Toisaalta GDPR keskittyy tietosubjekteihin, jotka ovat tunnistettavissa olevia henkilöitä asuen EU:ssa. CCPA sääntelee yrityksiä, jotka ovat voittoa tavoittelevia organisaatioita, toimivat Kaliforniassa, keräävät henkilötietoja Kaliforniassa asuvilta kuluttajilta ja päättävät, miten ja miksi näitä tietoja käsitellään. Tämän lisäksi yksi tai useampi seuraavista ehdoista on täytettävä: Yrityksellä on 25 miljoonaa dollaria tai enemmän vuotuisia bruttotuloja, yritys ostaa, vastaanottaa, myy tai jakaa vähintään 50 000 kuluttajan, kotitalouden tai laitteen henkilötietoja, tai yritys saavuttaa vähintään 50 prosenttia vuotuisista tuloista myymällä kuluttajien henkilötietoja. (Kucera 2021.)

CCPA asettaa myös vaatimuksia palveluntarjoajille, jotka käsittelevät henkilötietoja yrityksen puolesta. GDPR puolestaan kohdistuu tietojen ohjaajiin, jotka ovat organisaatioita, jotka päättävät, miten ja miksi ne käsittelevät EU:n asukkaiden henkilötietoja. Lisäksi GDPR sääntelee prosessoreita, jotka käsittelevät henkilötietoja ohjaajien puolesta. GDPR soveltuu, kun tietojen ohjaaja tai sen prosessori on perustettu EU:ssa, tai kun EU:n ulkopuoliset ohjaajat käsittelevät EU:n asukkaiden henkilötietoja tarjotessaan kaupallisia tavaroita ja palveluita tai seuratessaan heidän käyttäytymistään. Sekä CCPA että GDPR vaikuttavat laajalti globaalisti toimiviin yrityksiin, joten on tärkeää arvioida, miten keräät ja käytät henkilötietoja eri alueilla. (Kucera 2021.)

CCPA:n ja GDPR:n antamat oikeudet ovat osittain päällekkäisiä. Jos yritys on jo noudattanut GDPR:ää, se on pitkälti täyttänyt myös CCPA:n vaatimukset. Näiden kahden säännöksen samankaltaisuuksien tunteminen voi auttaa yrityksiä valmistautumaan tulevien, eri maantieteellisillä alueilla voimaan tulevien säännösten noudattamiseen, jotka todennäköisesti seuraavat näitä olemassa olevia malleja. (Kucera 2021.)

“Oikeus tietää” on yhteinen periaate, jonka CCPA ja GDPR molemmat tunnustavat. Tämän periaatteen mukaan yritysten, jotka toimivat CCPA:n tai GDPR:n piirissä, tulee olla avoimia keräämiensä henkilötietojen suhteen ja siitä, miten he käyttävät näitä tietoja. Lisäksi molemmat lait tarjoavat useita muita oikeuksia. Esimerkiksi yksilöillä on oikeus saada pääsy omiin henkilötietoihinsa ja he voivat

pyytää näitä tietoja joko suullisesti tai kirjallisesti. Tietyissä tilanteissa yksilöillä on myös oikeus kieltää organisaatiota käsittelemästä heidän henkilötietojaan. Yleisesti ottaen CCPA:n ja GDPR:n suojaamat yksilöt voivat pyytää henkilötietojaan helposti käytettävässä muodossa, kuten CSV- tai XML-tiedostoina. Useimmissa tapauksissa yksilöillä on myös oikeus pyytää organisaatiota poistamaan keräämänsä tai tallentamansa henkilötiedot. (Kucera 2021.)

Kullakin säännöksellä on myös omat ainutlaatuiset oikeutensa. Esimerkiksi CCPA:n mukaan yritykset voivat tarjota taloudellisia kannustimia, jotka liittyvät henkilötietojen keräämiseen, myyntiin tai poistamiseen, jos tämä on asianmukaisesti ilmoitettu ja kuluttajat suostuvat siihen. GDPR:n mukaan päätökset, jotka tehdään pelkästään automatisoiduin keinoin (esim. algoritmit), mukaan lukien tietojen käsittely ihmisten profilointia varten, ovat sallittuja vain tietyissä olosuhteissa. (Kucera 2021.)

4.3 Tietojen käsittely

Yritykset voivat usein käsitellä henkilötietoja oletusarvoisesti CCPA:n mukaan, kunhan ne tarjoavat kuluttajille selkeän mahdollisuuden kieltäytyä henkilötietojensa myynnistä tai jakamisesta. Tämä voi tapahtua esimerkiksi bannerin, lomakkeen tai “älä myy henkilötietojani” -linkin avulla. (Kucera 2021.)

Toisaalta GDPR:n mukaan organisaatiot voivat käsitellä tietoja vain, kun vähintään yksi kuudesta laillisesta perusteesta tietojen käsittelylle pätee:

- suostumus: yksilöt voivat suostua henkilötietojensa käsittelyyn tiettyjä tarkoituksia varten, mutta he voivat peruuttaa tämän suostumuksen milloin tahansa
- sopimus: tämä tarkoittaa, että tietojen käsittely on välttämätöntä sopimuksen noudattamiseksi tietosubjektin ja tietojen ohjaajan välillä
- lakiin perustuva velvoite: tietojen käsittely on välttämätöntä tietojen ohjaajan lakisääteisen velvoitteen noudattamiseksi
- elintärkeät edut: tietojen käsittely on välttämätöntä tietosubjektin tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi
- julkinen tehtävä: jos tietojen käsittely on tarpeen julkisen tehtävän suorittamiseksi, jolla on selkeä perusta laissa

- oikeutettu etu: kun tietojen käsittely on välttämätöntä organisaation oikeutettujen etujen toteuttamiseksi tai kolmannen osapuolen etujen toteuttamiseksi. Tämä on avoimin laillinen perusta tietojen käsittelylle, ja sitä kannattaa tutkia tarkemmin. CCPA:n ja GDPR:n noudattamiseksi on tärkeää ottaa huomioon lailliset perusteet tietojen käsittelylle ja tarjota opt-in- ja/tai opt-out-suostumus tarvittaessa. (Kucera 2021.)

4.4 Rikkomusten seuraukset

Kalifornian oikeusministeri voi määrätä taloudellisia rangaistuksia, jos organisaatiot eivät noudata CCPA:ta. Maksimisakko rikkomusta kohden on 7 500 dollaria tahallisten rikkomusten osalta ja 2 500 dollaria muutoin. Kuitenkin Privacy Rights and Enforcement Act Initiative -äänestyspäätöksen hyväksyminen, joka hyväksyttiin vuoden 2020 yleisissä vaaleissa, päivittää CCPA:n luomalla Kalifornian tietosuojaviraston: elimen, jolla on valta tutkia mahdollisia noudattamattomuustapauksia, antaa määräyksiä, määrätä sakkoja ja nostaa siviilikanteita maksamattomien sakkojen perimiseksi. (Kucera 2021.)

EU:n sääntelijät voivat samalla tavalla valvoa GDPR:ää sakkojen avulla. Vaikka nämä sakot riippuvat kunkin rikkomuksen luonteesta, ne voivat nousta jopa 20 miljoonaan euroon tai jopa 4 prosenttiin yrityksen globaalista vuotuisesta liikevaihdosta. GDPR:ää hallinnoivat EU:n kansalliset tietosuojaviranomaiset. Nämä elimet neuvovat organisaatioita GDPR:n noudattamisessa ja voivat käyttää tutkintavaltaa tarkastaakseen organisaatioita, joita epäillään rikkomuksista, poistaakseen väärin hankitut tiedot ja antaakseen varoituksia, sakkoja ja kieltoja tietojen käsittelyyn. (Kucera 2021.)

Vaikka CCPA ja GDPR kohdistuvat eri maantieteellisiin alueisiin, molemmilla on globaali ulottuvuus ja ne pyrkivät luomaan sääntely-ympäristön, joka korostaa voimakkaasti yksityisyyttä. Sekä GDPR että CCPA ovat johtavia lainsäädäntöjä tietosuojan ja läpinäkyvyyden alalla, mutta noudattamisen maisema on jatkuvasti muuttuva. Kun lainsäätäjät ympäri maailmaa pyrkivät pysymään teknologian tahdissa, paras toimintatapa on toteuttaa tietojen käsittelykäytäntöjä ja noudattamispolitiikkoja, jotka voidaan skaalata ja mukauttaa tarpeen mukaan. (Kucera 2021.)

5 MICROSOFT DEFENDER FOR CLOUD – TIETOTURVA-ALUSTA

Microsoft Defender for Cloud on pilvipohjainen sovellusten suojausalusta (CNAPP), joka koostuu erilaisista turvatoimista sekä käytännöistä, jotka on suunniteltu torjumaan kyberuhkia ja haavoittuvuuksia (Curwin ym. 2023). Microsoft Defender for Cloud (MDC) tarjoaa tietoturvaratkaisun, joka suojaa pilvityökuormia ja palveluita. Se toimii paitsi Azure-pilvialustalla, myös paikallisissa ympäristöissä sekä muissa pilvialustoissa, kuten AWS:ssa ja GCP:ssä. MDC:n avulla voit hallita tietoturvaa, suojautua uhkilta ja parantaa turvallisuutta. (Chauhan 2023.)

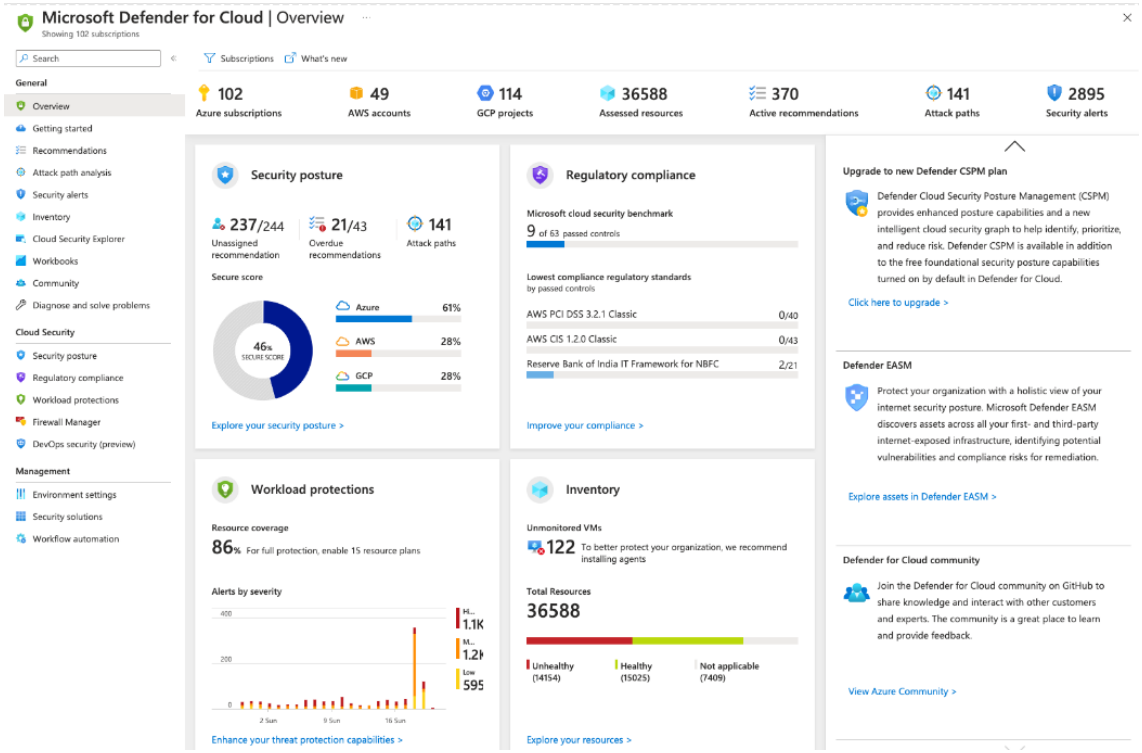
Microsoft Defender for Cloud mahdollistaa tietoturvatiimeille helpon tavan seurata ja hallita suojaustasoa, tunnistaa haavoittuvuuksia ja tutkia tietoturvahäiriöitä. Se tarjoaa yhtenäisen näkymän ja hallinnan hybridipilviympäristöissä, mikä helpottaa tietoturvatiimien suojaustason hallintaa. Lisäksi se integroituu saumattomasti muihin Microsoftin tietoturvaratkaisuihin, kuten Azure Sentinel ja Microsoft Cloud App Security, Microsoft 365 Defender for Endpoint, tarjoten kattavan tietoturvaratkaisun pilviympäristöihin. (Chauhan 2023.)

Käyttämällä kehittynyttä analytiikkaa ja koneoppia, Microsoft Defender for Cloud pystyy tunnistamaan uhkia ja reagoimaan niihin erilaisissa ympäristöissä, mukaan lukien virtuaalikoneet, säiliöt, tietokannat ja palvelimettomat resurssit. Tämä auttaa organisaatioita suojaamaan pilvityökuormiaan ja -palvelujaan monilta tietoturvauhkilta ja tarjoaa tarvittavan näkyvyyden ja hallinnan tehokkaaseen suojaustason hallintaan. (Chauhan 2023.)

MDC tarjoaa organisaatioille keskitetyn konsolin, jonka avulla voidaan seurata ja säädellä pilvitietoturvan tilaa sekä vastata reaaliaikaisesti mahdollisiin tietoturvauhkiin. Se hyödyntää tekoälyä ja koneoppimista tunnistakseen ja torjuakseen potentiaaliset uhat. Lisäksi se oppii jatkuvasti uusista tietoturvatapahtumista ja vaaratilanteista, mikä parantaa sen kykyä havaita ja reagoida uhkiin ajan kuluessa. (Chauhan 2023.)

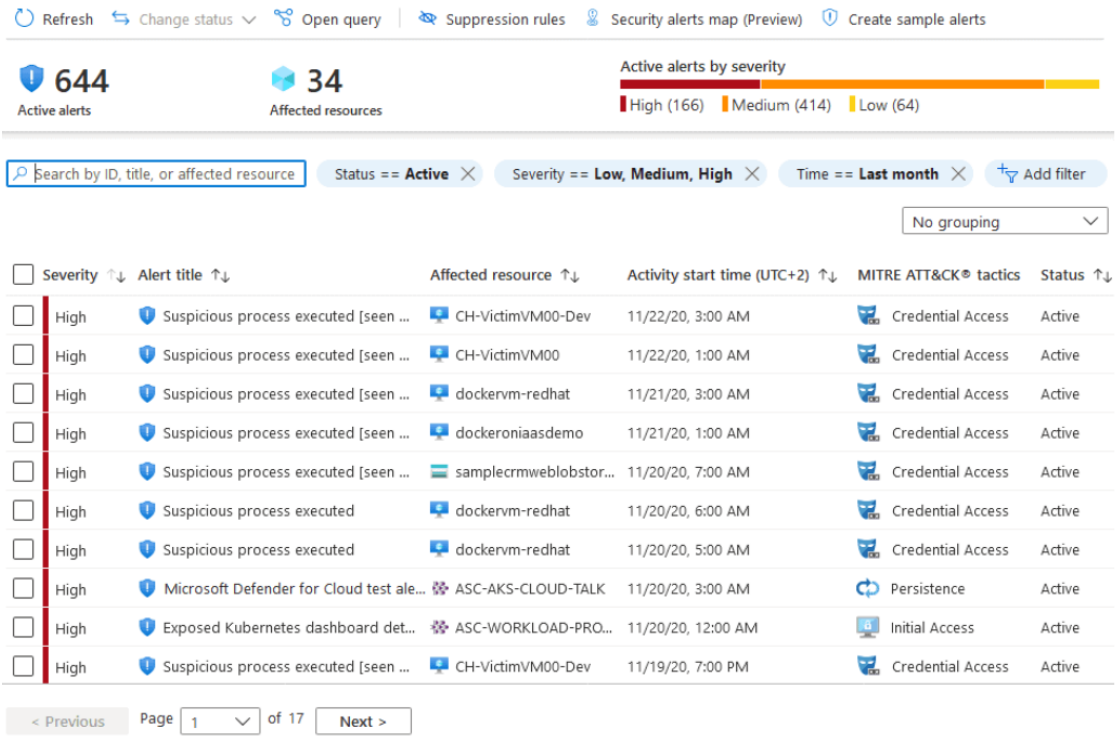
5.1 Secure Score

Kuvio 1 esittää Microsoft Defender for Cloudin hallintapaneelia tai Dashboardia. Kuten kuviosta 1:stä näkyy, Microsoft Defender for Cloud tarjoaa ymmärryksen organisaation nykyisestä tietoturvatilanteesta ja antaa suosituksia, jotka auttavat parantamaan tätä tilannetta. Secure Score on keskeinen osa tätä: mitä suurempi Secure Scoren pistemäärä on, sitä alhaisempi on riskitaso. Jos halutaan nostaa Secure Scoren prosenttiosuutta, voidaan tarkastella suositeltuja toimenpiteitä Security Centerissä. Nämä suositukset sisältävät myös ohjeet, jotka auttavat saavuttamaan tavoitteen. (Chauhan 2023.)



Kuvio 1. MDC Hallintapaneeli (Curwin ym. 2024)

Kuvio 2 esittää, kuinka Secure Score määritetään. Kuten kuvio 2:sta näkyy, jokaiselle tietoturvasuositukselle on annettu tietty pistemäärä. Kun noudatat näitä suosituksia, Secure Scoren pistemäärä kasvaa automaattisesti. Jokaisella suosituksella on enimmäispistemäärä ja nykyinen pistemäärä. (Chauhan 2023.)



Kuvio 2. Turvallisuushälytykset (Chauhan 2023)

5.2 Pistemäärän määrittäminen

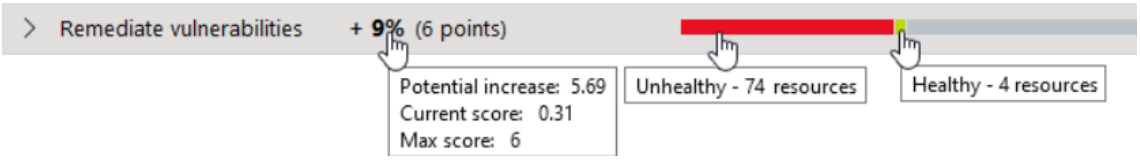
Kuvio 3 ja 4 esittävät, kuinka Secure Scoren pistemäärä määritetään. Kuten kuvioista näkyy, jokaisen turvatoimenpiteen nykyinen pistemäärä heijastaa sen sisällä olevien resurssien tilaa. Turvallisuuspistemäärä muodostuu yksittäisten turvatoimenpiteiden pisteistä. Jokainen suosituksen piiriin kuuluva resurssi vaikuttaa turvatoimenpiteen pistemäärään. (Curwin ym. 2024).

Yhtälö, jolla määritetään turvatoimenpiteen saama pistemäärä, on:

$$Secure\ score\ for\ a\ single\ security\ control = \frac{Max\ score}{Healthy + Unhealthy}\ x\ Healthy$$

Kuvio 3. Turvallisuuspisteet yhden ohjaimen osalta (Curwin ym. 2024)

Esikatselusuosituksissa löytyvät resurssit eivät sisälly turvallisuuspistemäärään. Esimerkiksi, jos maksimipistemäärä on 6 ja terveiden sekä epäterveiden resurssien summa on 78, lasketaan pistemäärä jakamalla 78 kuudella (6), jolloin saadaan 78/6=0.0769. Tämä kerrotaan terveiden resurssien määrällä (tässä tapauksessa 4), jolloin saadaan nykyinen pistemäärä: 0.0769*4=0.31. (Curwin ym. 2024.)



Kuvio 4. Pisteytyksen vihjeet (Curwin ym 2024)

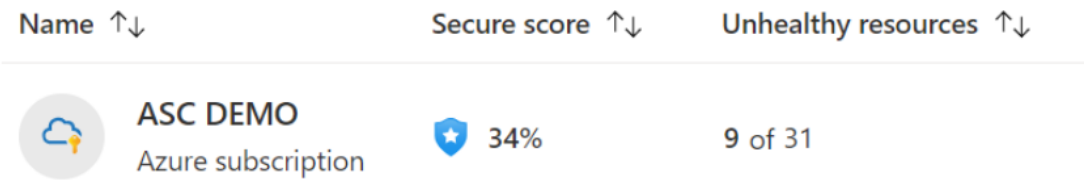
5.3 Pistemäärän laskeminen

Kuvio 5 ja 6 esittävät, kuinka turvallisuuspistemäärät lasketaan yksittäiselle tilaukselle tai integraatiolle. Kuten kuviosta näkyy, esimerkkitapauksessa on yksi tilaus tai integraatio, jossa on mahdollisuus käyttää kaikkia turvatoimenpiteitä, jolloin enimmäispistemääräksi muodostuu 60 pistettä. Tämä prosessi on esitetty yhtälössä, joka laskee turvallisuuspistemäärät yksittäiselle tilaukselle tai integraatiolle. (Curwin ym. 2024.)

$$Secure\ score\ for\ a\ subscription = \frac{\sum current\ scores\ for\ all\ controls}{\sum maximum\ scores\ for\ all\ controls}\ x\ 100$$

Kuvio 5. Yksittäinen tilaus (Curwin ym. 2024)

Tähän mennessä on kertynyt 29 pistettä mahdollisesta 60 pisteestä. Turvatoimenpiteiden osiossa ‘Mahdollinen pistemäärän kasvu’ näytetään, kuinka monta pistettä on vielä mahdollista saavuttaa. Tässä tapauksessa on vielä mahdollista saada 32 pistettä. (Curwin ym. 2024.)



Kuvio 6. Esimerkki yhdestä tilauksesta (Curwin ym. 2024)

Kuvio 7 esittelee laajan valikoiman kontrollitoimenpiteitä, jotka on suunniteltu parantamaan tietoturvaa ja kasvattamaan kokonaispistemäärää. Toimenpiteet, jotka ulottuvat haavoittuvuuksien korjaamisesta hallintaporttien suojaamiseen, tarjoavat jokainen mahdollisuuden parantaa pistemäärää ja vahvistaa suojauksia. Kuvio 7 esittää yhtälön, joka on identtinen integraation kanssa. Ainoa ero on, että sana ”tilaus” on vaihdettu sanaksi ”integraatio”. Tämä korostaa integraation merkitystä tietoturvan tehostamisessa - jokainen toimenpide ei ole erillinen, vaan

osa kokonaisvaltaista prosessia, joka johtaa parempaan tietoturvaan. (Curwin ym. 2024.)

Controls	Potential score increase
> Remediate vulnerabilities	+ **9%** (6 points)
> Secure management ports	+ **9%** (5 points)
> Enable encryption at rest	+ **6%** (3 points)
> Restrict unauthorized network access	+ **4%** (2 points)
> Enable DDoS protection on Vnet	+ **3%** (2 points)
> Apply system updates	+ **3%** (2 points)
> Manage access and permissions	+ **3%** (2 points)
> Remediate security configurations	+ **3%** (2 points)
> Apply data classification	+ **2%** (1 point)
> Encrypt data in transit	+ **2%** (1 point)
> Adaptive application control	+ **1%** (1 point)
> Enable auditing and logging	+ **1%** (1 point)
> Enable endpoint protection	+ **1%** (1 point)
> Enable MFA Completed	+ **0%** (0 points)
> Additional best practices	+ **0%** (0 points)

Kuvio 7. turvallisuus suositukset yhden osion kohdalta (Curwin ym. 2024)

5.4 Useiden tilausten pistemäärä

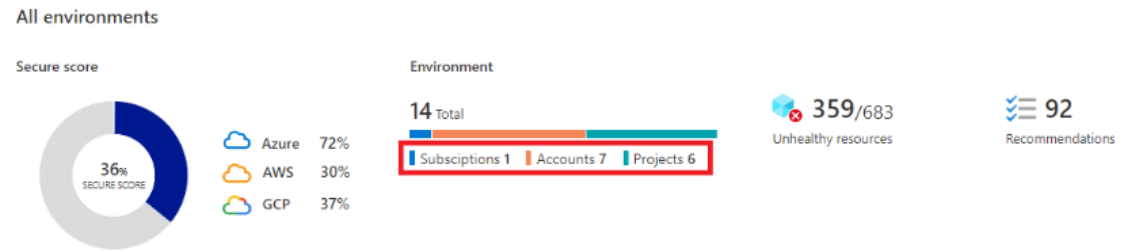
Tässä osiossa tarkastellaan, kuinka useiden tilausten ja integraatioiden turvallisuuspistemäärä määritetään. Tämä on erityisen tärkeää organisaatioille, jotka käyttävät useita tilauksia ja integraatioita ja haluavat ymmärtää, kuinka niiden turvallisuus vaikuttaa kokonaispistemäärään. Kuvio 8 osoittaa yhtälön, kuinka pisteet lasketaan useille tilauksille. (Curwin ym. 2024.)

$$Secure\ score\ multiple\ subscriptions = \frac{\sum (subscription\ score\ x\ subscription\ weight)}{\sum Weights\ for\ all\ subscriptions}\ x\ 100$$

Kuvio 8. Turvallisuuspistemallin laskenta useille tilauksille (Curwin ym. 2024)

Kuvio 9 jatkaa tätä analyysiä ja esittää, kuinka useiden tilausten ja integraatioiden turvallisuuspistemäärä määritetään. Kuten kuvioista näkyy, useiden tilausten ja integraatioiden yhteispistemäärä ottaa huomioon kunkin tilauksen ja integraation painoarvon. Defender for Cloud laskee tilausten ja integraatioiden suhteelliset painoarvot perustuen esimerkiksi resurssien määrään. (Curwin ym. 2024.)

Kunkin tilauksen ja integraation nykyinen pistemäärä lasketaan samalla tavoin kuin yksittäisen tilauksen tai integraation kohdalla, mutta lopuksi sovelletaan painoarvoa yhtälön mukaisesti. Kun havaitaan useita tilauksia ja integraatioita, turvallisuuspistemäärä arvioi kaikki resurssit, jotka kuuluvat kaikkiin käytössä oleviin politiikkoihin (Policy), ja ryhmittelee ne. Ryhmittely näyttää, miten ne yhdessä vaikuttavat kunkin turvatoimenpiteen maksimipistemäärään. (Curwin ym. 2024.)



Kuvio 9. Turvallisuuspisteet useille tilauksille, kun kaikki kontrollit ovat käytössä (Curwin ym 2024)

Yhdistetty pistemäärä ei ole keskiarvo, vaan se on arvio kaikkien tilausten ja integraatioiden resurssien tilasta. Siirryttäessä Suositukset-sivulle ja mahdollisesti saatavien pisteiden yhteen laskemisen jälkeen huomataan, että se on nykyisen pistemäärän (22) ja maksimipistemäärän (58) välinen ero. (Curwin ym 2024.)

5.5 Valvontamekanismit

Microsoft Cloud Security Baseline (MCSB) on tärkeä työkalu organisaatioiden tietoturvan hallinnassa. Se sisältää useita valvontamekanismeja, jotka ovat loogisia ryhmiä turvallisuussuosituksia. Nämä mekanismit kuvaavat organisaation haavoittuvia hyökkäyspintoja, kuten verkkoliikennettä, käyttäjätunnuksia ja salasanoja, sekä tietojen käsittelyä ja tallennusta. (Curwin ym. 2024.)

Organisaation tietoturvatilanteen arvioimiseksi MCSB tarjoaa pisteytysjärjestelmän, joka perustuu kunkin valvontamekanismin pistemäärään. Mitä korkeampi pistemäärä, sitä parempi organisaation tietoturvatilanne on. Pistemäärä paranee ainoastaan, kun kaikki suositukset on korjattu. Tämä tarkoittaa, että organisaation on aktiivisesti seurattava ja korjattava turvallisuusongelmia parantaakseen pistemääräänsä. (Curwin ym. 2024.)

Kuten Taulukko 1 osoittaa, eri turvallisuusmekanismeilla on erilaiset pistemäärät. Jotta saadaan kaikki mahdolliset pisteet valvontamekanismilta, kaikkien resurssien on noudatettava kaikkia valvontamekanismin sisällä olevia turvallisuussuosituksia. Esimerkiksi MDC antaa useita suosituksia hallintaporttien turvaamiseksi. Kaikkien suositusten korjaaminen on välttämätöntä turvallisuuspistemäärän parantamiseksi. (Curwin ym. 2024.)

Turvallisuuspistemäärän parantamiseksi, suositukset suositusluettelosta voidaan korjata manuaalisesti jokaiselle resurssille tai käyttämällä Korjaa-vaihtoehtoa useiden resurssien ongelmien nopealle korjaukselle. Lisäksi suositusten toteuttaminen tai kieltäminen auttaa varmistamaan, että käyttäjät eivät luo resursseja, jotka vaikuttavat negatiivisesti pistemäärään (Curwin ym. 2024.)

Taulukko 1. Tietoturvakontrollit (mukailleen Curwin ym. 2024)

Turvallisuuspistemäärä	Turvallisuusmekanismi
10	MFA (Kaksivaiheinen tunnistautuminen) Käyttö
8	Hallintakanavien suojaaminen
6	Järjestelmäpäivitysten käyttöönotto
4	Turvallisuusmääritysten säätäminen
4	Käyttöoikeuksien valvonta
4	Tietojen salaus tallennusvaiheessa
4	Tietoliikenteen suojaaminen salauksella
4	Ei-toivotun verkkoliikenteen estäminen
3	Mukautuvan sovellusvalvonnan käyttöönotto
2	Sovellusten suojaaminen DDoS-hyökkäyksiltä
2	Päätelaitesuojauksen käyttöönotto
1	Lokituksen ja tarkastuksen seuranta
0	Lisäsuojauksen käyttöönotto
0	Turvallisuusstandardien parhaiden käytäntöjen käyttöönotto

5.6 MDC:n ja Azuren Integraatio

Tässä kerrotaan pääpiirteittäin, miten integraatio tapahtuu MDC:n ja Azuren välillä. Tämä toimenpide on monimutkainen ja vaatii monen eri tietotekniikka ryhmän yhteistyötä.

Microsoft Defender for Cloud ja Azuren integraatio on prosessi, jossa yhdistetään kaksi Microsoftin pilvipalvelua parantaakseen tietoturvaa ja hallintaa. Tässä prosessissa MDC, joka on pilvipohjainen tietoturvaratkaisu, voidaan integroida Azureen, joka on myös Microsoftin pilvipalvelualusta.

Integraation aloittamiseksi organisaatio ja Microsoft tekevät yhteistyötä ja sopivat tarvittavien palveluiden määrästä. Tämä on integraation tilausprosessin ensimmäinen vaihe. Tämän jälkeen tulee esiasennusvaihe, jossa tehdään päätös siitä, miten Azure Stack Hub, joka on paikan päällä oleva versio Azure-palveluista, liitetään organisaation datakeskukseen. Tässä vaiheessa Microsoft tarjoaa työkalun, joka auttaa keräämään kaikki tiedot, jotka ovat välttämättömiä onnistuneen integraation kannalta. (Manheim, Buck, Altimore & Briggs 2022.)

Esiasennusvaiheen jälkeen seuraavaksi tulevat integraatio, validointi ja kuljetusvaihe. Tässä vaiheessa tarkistetaan, että sivusto on valmiina vastaamaan verkon, virran ja jäähdytyksen tarpeisiin. Tämän jälkeen suoritetaan asennus kohteessa, jossa varmistetaan, että asiakkaan verkkoteknikko on läsnä. Asennuksen jälkeen suoritetaan jälkiasennus, jossa Azure Stack Hub Marketplace syndikaatio rekisteröidään ja varmistetaan. Tämä palvelu mahdollistaa Azure-palveluiden käytön paikan päällä. (Manheim ym. 2022.)

On tärkeää huomata, että Microsoft Defender for Cloudin käyttöönotto vaatii vähintään yhden suunnitelman aktivoimista jokaisessa tilauksessa, jossa halutaan käyttää liitännäistä. Tämän toimenpiteen suorittamiseksi toimenpiteen suorittajalla on oltava Security Admin -rooli tilauksessa. (Manheim ym. 2022.)

5.7 MDC:n ja M365:n integraatio

Microsoft Defender for Cloud voidaan myös integroida yrityksessä Microsoft 365 palvelupaketteihin, jolloin saadaan useita etuja. MDC:n ja M365:n yhteiskäyttö tarjoaa lisäturvaa Windows- ja Linux-laitteille, riippumatta siitä, ovatko ne isännöity Azure-pilvessä, hybridipilvissä tai monipilviympäristöissä. Tämä laajennettu turvallisuus on yksi tärkeimmistä eduista. (Curwin ym. 2024.)

Lisäksi MDC:n ja M365:n integraatio mahdollistaa havaitsemisen ja vastauksen laajentamisen. Tämä sisältää riskipohjaisen haavoittuvuuden hallinnan ja arvioinnin, hyökkäyspinnan vähentämisen, käyttäytymispohjaisen ja pilvipohjaisen suojauksen, päätepisteen havaitsemisen ja vasteen (EDR), automaattisen tutkimuksen ja korjauksen sekä hallitut edistyneet uhkien metsästykset (Advanced hunting). (Curwin ym. 2024.)

MDC:n ja M365:n yhteiskäyttö myös yksinkertaistaa pilven löytämistä ja mahdollistaa laitepohjaisen tutkimuksen. Tämä on erityisen hyödyllistä organisaatioille, jotka haluavat ymmärtää ja hallita pilviympäristöjään paremmin. (Gold ym. 2024.)

MDC:n ja M365:n integraatio mahdollistaa tehokkaamman riskienhallinnan. Jos riskialttiiksi tunnistettu käyttäjä on käyttänyt tiettyjä laitteita, näiden laitteiden tarkastelu voi paljastaa mahdollisia riskejä. Samoin, jos riskialttiiksi tunnistettu laite on ollut tiettyjen käyttäjien käytössä, näiden käyttäjien tarkastelu voi paljastaa lisää potentiaalisia riskejä. Tämä parantaa huomattavasti organisaation kykyä hallita ja minimoida riskejä. (Gold ym. 2024.)

MDC:n yhdistäminen M365:n kanssa keskittyy lähinnä tietoturvan tehostamiseen ja uhkien tunnistamiseen. Tämä kattaa laajemman turvallisuuden Windows- ja Linux-laitteille, olivatpa ne sitten Azure-pilvessä, hybridipilvissä tai monipilviympäristöissä. Se myös laajentaa havaitsemis- ja vastauskykyjä, mukaan lukien riskipohjainen haavoittuvuuden hallinta ja arviointi, hyökkäyspinnan pienentäminen, käyttäytymispohjainen ja pilvipohjainen suojaus, päätepisteen havaitseminen ja vaste (EDR), automaattinen tutkimus ja korjaus sekä hallitut metsästyspalvelut. (Gold ym. 2024.)

Kuten on mainittu Microsoft Q&A- sivustolla MDC:n integraatio Azure-pilvipalveluun keskittyy enemmän infrastruktuurin turvallisuuteen. MDC on suunniteltu suojaamaan Azure-tilauksia ja niiden resursseja. Se voidaan laajentaa AWS:ään, GCP:hen ja paikan päällä oleviin palvelimiin palvelimien, SQL:n ja säiliöiden seurantaan. MDC ei tarjoa virustorjuntaominaisuuksia. Sen alisovellus, Defender for Servers, on suunniteltu erityisesti palvelimille. (Blumhardt 2022.)

6 POHDINTA

Tämän opinnäytetyön tekeminen ja aineiston kerääminen ovat olleet mielenkiintoisia askelia kohti syvällisempää ymmärrystäni Microsoft Defender for Cloudista. Prosessi on ollut haastava, mutta samalla erittäin opettavainen.

Olen oppinut, että Microsoft Defender for Cloudin käyttöönotto vaatii monen eri ryhmän asiantuntijoita ja sitoutumista myös Microsoftin puolelta. Käyttöönoton haasteellisuus korostuu, kun Microsoft Defender for Cloud integroidaan M365:n, Azureen tai muihin tietoturvatyökaluihin. Kuitenkin, kun kaikki asennukset ja integraatiot sujuvat hyvin, Microsoft Defender for Cloudista saadaan erittäin tehokas työkalu tietoturva-asiantuntijoiden käyttöön.

Henkilökohtaisesti olen saanut arvokasta kokemusta työssäni, jossa olen päässyt käyttämään kyseistä ohjelmistoa ja osallistumaan lukuisiin käyttöönotto palavereihin. Tämä on antanut minulle laajemman kuvan siitä, mitä tapahtuu "konepellin" alla. Lisäksi tämä prosessi on korostanut, kuinka tärkeää on ymmärtää pilvipalveluiden perusteet ja niiden turvallisuusominaisuudet.

Jatkossa näen useita mahdollisuuksia kehittää Microsoft Defender for Cloudin käyttöönottoa ja käyttöä. Esimerkiksi koulutuksen ja tuen lisääminen voisi auttaa organisaatioita paremmin ymmärtämään ja hyödyntämään Microsoft Defender for Cloudia. Lisäksi automaation kehittäminen asennus- ja integraatioprosesseihin voisi vähentää manuaalista työtä ja virheiden mahdollisuutta. Tämä voisi olla hyvä lähtökohta jatkotutkimukselle.

LÄHTEET

Aarness, A. 2023. Endpoint Detection and Response (EDR). CrowdStrike. Viitattu 11.3.2024 https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/.

Baldwin, M., Bathini, A. & Buck, A. 2023. Overview of Microsoft cloud security benchmark (v1). Viitattu 11.3.2023 https://learn.microsoft.com/en-us/security/benchmark/azure/overview.

Blumhardt, A. 2022. Difference between Microsoft Defender for Cloud and Microsoft Defender Endpoint Microsoft. Viitattu 28.2 2024 https://learn.microsoft.com/en-us/answers/questions/956836/difference-between-microsoft-defender-for-cloud-an.

Chauhan, K. 2023. Microsoft Defender for Cloud. K21 Academy. Viitattu 3.2.2024 https://k21academy.com/microsoft-azure/az-500/microsoft-defender-for-cloud/.

Cloudflare 2024. What is a DDoS attack? Viitattu 11.3.2024 https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

Curwin, D., Wiselman, R., Mansheim, B., Borsecnik, J., Krieger, E., Baldwin, M., Ta, K., Powers, B., Kardos, Y., Brenner, L., & Memildin, M. 2023. What is Microsoft Defender for Cloud? Viitattu 3.2.2024 https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction.

Curwin, D., Bernstein, A., Wiselman, R., Mansheim, B., Krieger, E., Hireka, S. B., Arviv, L., Imhutch, Downer, R., & Memildin, M. 2024. Azure Defender for Cloud: Secure Score Security Controls. Microsoft Learn. Viitattu 5.2.2024 https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#score-calculation-equations.

Curwin, D., Krieger, E., Borsecnik, J., Hireka, S. B., Janetscheck, T., Harris, A., Bernstein, A., Hansav, E., Huang, H., Mansheim, B., Mapari, A., Yu, H., PRMerger14, Norman, N., Kardos, Y., dknappettmsft, Memildin, M. Biton, A., & Naccarato, M. 2024. Integration with Microsoft Defender for Endpoint. Microsoft Learn. Viitattu 19.3.2024 https://learn.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint.

Curwin, D., Wiselman, R., Rageking8, Memildin, M., Krieger, E., Mansheim, B., Bernstein, A., Melgarejo, D., & Henderson, W. 2024. Microsoft Defender for Cloud. Microsoft Learn. Viitattu 15.2.2024 https://learn.microsoft.com/en-us/azure/defender-for-cloud/overview-page.

Euroopan unioni 2022. Yleinen tietosuoja-asetus (GDPR). Viitattu 11.3.2024 https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm.

EU-SEC 2019. EU-SEC Viitattu 26.3.2024 https://www.sec-cert.eu/.

Floor, A. 2024. Pilvipalveluiden ostajan opas, 5–8. Viitattu 26.1.2024 https://hub.solita.fi/hubfs/Oppaat%20ja%20tiedostot/Solit_Pilvipalveluiden-ostajan-opas_FI.pdf.

Fortinet 2024. What is the CIA Triad and Why is it important? Viitattu 6.4.2024 https://www.fortinet.com/resources/cyberglossary/cia-triad.

Gold, B., Borsecnik, J., Cohen, I., Curwin, D., Buck, A., & Sagir, S. 2024. Microsoft Defender for Cloud Apps integration with Microsoft Defender for Endpoint. Viitattu 25.2.2024 https://learn.microsoft.com/en-us/defender-cloud-apps/mde-integration.

Gold, B., v-chmccl., Buck, A., Curwin, D., Sagir, S., Baldwin, M., rkarlin., Cai, S., & Stewart, M. 2024. Differences between Defender for Cloud Apps and Microsoft 365 Cloud App Security. Viitattu 25.2.2024 https://learn.microsoft.com/en-us/defender-cloud-apps/editions-cloud-app-security-o365.

GSA 2019. FedRAMP. Viitattu 2.4.2024 https://www.gsa.gov/technology/government-it-initiatives/fedramp.

Hazdun, N. 2023. Cloud Versus On Premises: Advantages And Disadvantages Of Both Models. Viitattu 27.1.2024 https://www.forbes.com/sites/forbestechcouncil/2023/03/27/cloud-versus-on-premises-advantages-and-disadvantages-of-both-models/.

IBM 2024. Internet of Things. Viitattu 11.3.2024 https://www.ibm.com/topics/internet-of-things.

IT-Palvelut 2024. MFA-tunnistautuminen Microsoft-palveluihin. Viitattu 11.3.2024 https://it.uwasa.fi/guides/fi/all/MFA-tunnistautuminen+Microsoft-palveluihin.

Kalifornian oikeusministeriö 2023. California Consumer Privacy Act (CCPA). Viitattu 11.3.2024 https://www.oag.ca.gov/privacy/ccpa.

Kemper, F. 2021. On-Premises vs Cloud: Advantages and Disadvantages. Viitattu 26.1.2024 https://www.empowersuite.com/en/blog/on-premise-vs-cloud.

Koistinen, P. 2021. On Premise-, Pilvi- ja Hybridiratkaisut – mikä on paras valinta yrityksellemme? Viitattu 26.1.2024 https://www.marskidata.fi/blogi/on-premise-pilvi-ja-hybridiratkaisut-mika-on-paras-valinta-yrityksellemme/.

Kucera, D. 2021. CCPA vs. GDPR: Similarities and Differences Explained. Viitattu 27.1.2024 https://www.okta.com/blog/2021/04/ccpa-vs-gdpr/.

Kyberturvallisuuskeskus 2019a. Ohjeita pilvipalvelujen turvallisuudesta, 4,6. Viitattu 23.3.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf.

- 2019b. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) 3, 33.Viitattu 28.1.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf.

Macrae, D. 2023. Ways to explain cloud computing to a five-year-old. Viitattu 25.1.2024 https://techmonitor.ai/technology/ways-to-explain-cloud-computing-to-a-five-year-old.

Manheim, S., Buck, A., Altimore, P., & Briggs, M. 2022. Integration overview. Microsoft Learn. Viitattu 24.2.2024 https://learn.microsoft.com/en-us/azure-stack/mdc/integration-overview.

Morefield. 2022. On-Premises vs Cloud: Advantages and Disadvantages. Viitattu 27.1.2024 https://www.morefield.com/blog/on-premises-vs-cloud/.

Microsoft 2024. What is Microsoft 365? Viitattu 11.3.2024 https://www.microsoft.com/fi-fi/microsoft-365/what-is-microsoft-365.

Microsoft Security 2024. What is a CNAPP? Viitattu 11.3.2024 https://www.microsoft.com/en-us/security/business/security-101/what-is-cnapp.

NIST 2024. National Institute of Standards and Technology. Viitattu 24.3.2024 https://www.nist.gov/.

Sjoera. 2021. New EU Code of Conduct for cloud providers: not a GDPR party. Viitattu 27.1.2024 https://www.privacycompany.eu/blogpost-en/new-eucode-of-conduct-for-cloud-providers-not-a-gdpr-party.

Pahlman, S. 2024. Uusi kriteeristö ohjaa pilvipalveluiden turvalliseen käyttöön. Viitattu 28.1.2024 https://www.traficom.fi/fi/tilastot-ja-julkaisut/blogit/uusi-kriteeristo-ohjaa-pilvipalveluiden-turvalliseen-kayttoon.

Valtiovarainministeriö 2022. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa, 22. Viitattu 1.4.2024 http://urn.fi/URN:ISBN:978-952-367-906-1.

Vähälummukka, A. 2023. Pilvipalvelut. Viitattu 25.1.2024 https://peda.net/p/antti.vahalummukka/Pilvipalvelut/materiaali/pilvipalvelu.