



Moderni tietoturva

Tietoturvan työkalut

Kalle Kinnari

OPINNÄYTETYÖ
Toukokuu 2024

Tietotekniikka
Ohjelmistotekniikka, tietoliikennetekniikka ja tietoliikenneverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

KINNARI, KALLE:
Moderni tietoturva
Tietoturvan työkalut

Opinnäytetyö 54 sivua, joista liitteitä 0 sivua
Toukokuu 2024

Opinnäytetyön tavoitteena oli tutkia, millaista tietoturva nykypäivänä on, miten se on kehittynyt sekä lopuksi testata ja arvioida Microsoftin tietoturvatyökalujen toimivuutta Azuren ympäristössä.

Opinnäytetyö koostuu useista vaiheista. Ensimmäisenä esiteltiin tietoturvan perusteita, kuten sen historiaa ja evoluutiota nykypäivään. Tämä vaihe piti sisällään myös esimerkkejä nykyaikaisista uhista, joita organisaatiot saattavat kohdata.

Työn keskiössä oli Microsoftin kehittämät työkalut Defender for Cloud sekä Microsoft Sentinel. Teoreettisen osuuden jälkeen suoritettiin näiden työkalujen käyttöönottoa Azuren ympäristössä, niiden konfigurointia sekä toimintaa. Yhtenä tavoitteena oli näyttää organisaatioille tai tietoturva-ammattilaisille, kuinka tällaiset työkalut voidaan ottaa käyttöön.

Yhteenvedossa kiteytettiin nykyaikaiset ratkaisut sekä Microsoftin työkalujen hyödyllisyys modernissa tietoturvassa. Mietittiin, mihin suuntaan tietoturva on kehittymässä ja mitkä ovat tulevaisuuden haasteet ja näkymät.

ABSTRACT

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

KINNARI, KALLE
Modern Information Security
Tools of Information Security

Bachelor's thesis 54 pages, appendices 0 pages
May 2024

The goal of the thesis was to research modern day information security, how it has developed to this day and lastly, test the security tools Microsoft has to offer in an Azure environment.

The thesis had several different phases. First phase is the basics of information security such as history and its evolution to this day. It also covered some modern threats organizations can experience. Lastly the first phase covered the pillars of information security.

The core of this thesis laid within the Microsoft tools. These tools were Defender for Cloud and Microsoft Sentinel. The thesis covered their theoretical part as well as testing. The point of the testing phase was to see how organizations or security professionals can deploy, configure, and test these tools in their environment. After this the results were summarized and analysed.

All findings were compiled and analysed. Additionally, the summary covered the future of information security and the next steps of its evolution.

Key words: information security, Microsoft, defender for cloud, sentinel

SISÄLLYS

1	JOHDANTO	8
2	TIETOTURVAN PERUSTEET	9
2.1	Tietoturvan historiaa.....	9
2.1.1	Varhaiset vaiheet.....	9
2.1.2	Internetin aikakausi.....	10
2.2	Nykyaikaiset uhat	12
2.2.1	Sisäiset uhkatekijät.....	12
2.2.2	Kalastelu.....	13
2.2.3	Kiristyshaittaohjelmat.....	13
2.2.4	Virukset ja madot.....	14
2.2.5	Palvelunestohyökkäys	14
2.3	Periaatteet.....	15
3	MICROSOFTIN TIETOTURVATYÖKALUT JA -PALVELUT	16
3.1	Microsoft Defender XDR	16
3.2	Defender for Endpoint	17
3.3	Defender for Cloud	19
3.4	Microsoft Sentinel.....	20
4	CASE-TUTKIMUS: MICROSOFTIN TIETOTURVATUOTTEIDEN TESTAUS	22
4.1	Testiympäristön rakentaminen	22
4.1.1	Arkkitehtuuri	24
4.1.2	Yritystili	25
4.1.3	Azure	26
4.1.4	Defender for Cloud	29
4.1.5	Sentinel	30
4.2	Todentaminen	35
4.2.1	Avainholvi	36
4.2.2	Virtuaalikone.....	38
4.2.3	Varasto	41
4.2.4	Sentinel analytiikka.....	44
4.2.5	CSPM ja säännöt.....	46
4.3	Yhteenveto.....	47
5	JOHTOPÄÄTÖKSET JA TULEVAISUUDEN NÄKYMÄT	49
5.1	Yhteenveto.....	49
5.2	Johtopäätökset.....	49

5.3 Tulevaisuuden näkymät ja haasteet.....	50
LÄHTEET	52

LYHENTEET JA TERMIT

AV	AntiVirus Virustorjuntaohjelmisto, joka suojelee päätelaitetta haittaohjelmilta.
CSPM	Cloud Security Posture Management Palvelu, joka tekee konfiguraatitarkistukset pilvipalveluiden tietoturvan varmentamiseksi.
EU	Euroopan Unioni 27 jäsenvaltion muodostama taloudellinen ja poliittinen liitto.
EDR	Endpoint detection and response Valvoo jatkuvasti uhkiin liittyvää tietoa tietokoneilla ja muissa päätepisteissä.
IAM	Identity Access Management Hallitaan käyttäjien pääsyä arkaluonteisiin resursseihin.
ISO	International Organization for Standardization Kansainvälinen voittoa tavoittelematon standardoimisjärjestö.
IoT	Internet of Things Järjestelmä, jossa internetiin liitetyt laitteet lähettävät tietoa mahdollistaen ohjauksen tai valvonnan.
KQL	Kusto Query Language KQL on monipuolinen kieli, jonka avulla suoritetaan data-analyysia ja hallintatehtäviä
MFA	Multi-Factor Authentication Henkilön identiteetti varmistetaan useampaa eri tunnistautumistapaa käyttämällä.
MDM	Mobile Device Management Ohjelmistoratkaisu mobiililaitteiden keskitettyyn hallintaan.
MIT	Massachusetts Institute of Technology Teknillinen korkeakoulu Cambridgessä.

RBAC	Role Based Access Control Roolipohjaisen käytön hallinta.
SAS	Shared Access Signature Merkki tai tunnus joka liitetään Azure varsto -resurssin URI:hen.
SIEM	Security Information and Event Management Tietoturvan hallintajärjestelmä, joka kerää ja analysoi tietoja tietoturvapoikkeamista ja tapahtumista.
SOAR	Security Orchestration, Automation and Response Teknologia, joka auttaa koordinoimaan, suorittamaan ja automatisoimaan tehtäviä.
SQL	Structured Query Language Standardoitu kyselykieli, jolla suoritetaan kyselyjä, muutoksia tai lisäyksiä relaatiotietokantaan.
SSH	Secure Shell Protokolla, joka on kehitetty kahden suojatun tietokoneen väliseen yhteyteen.
TOR	The Onion Router TOR on verkko, joka anonymisoi verkkoliikenteen ja tekee siitä yksityistä.
URI	Uniform Resource Identifier Internetissä olevan resurssin yksilöivä tunnus.
URL	Uniform Resource Location Verkko-osoite, jonka avulla pääsee tietylle verkkosivulle.
VPN	Virtual Private Network Virtuaalinen erillisverkko, joka turvaa yksityisyyden verkossa.
WWW	World Wide Web Internetissä sijaitseva hajautettu hypertekstijärjestelmä.

1 JOHDANTO

Tietoturva on nykypäivänä keskeinen osa jokaista organisaatiota, sillä teknologian kehittyessä myös tietoturvauhat lisääntyvät ja monimutkaistuvat. Tämän opinnäytetyön tavoitteena on syventyä tietoturvan peruspilareihin, tutkia nykyaikaisten tietoturvauhkien luonnetta ja kartoittaa tehokkaita keinoja niiden torjumiseksi. Työssä käydään lyhyesti läpi tietoturvan kehityskaarta, millaista on moderni tietoturva sekä millaisia työkaluja Microsoftilla on tarjota tietoturvan parantamiseksi.

Osana työtä suoritetaan myös Case-tutkimus, jossa tutkitaan Microsoftin tarjoamia tietoturvapalveluita kuten Defender for Cloud -tuotetta sekä Microsoft Sentineliä ja sitä miten ne otetaan käyttöön. Lopuksi testataan konfiguroitu ympäristö simuloimalla hyökkäyksiä resursseihin.

2 TIETOTURVAN PERUSTEET

2.1 Tietoturvan historiaa

Tietoturva ja kyberturvallisuus ovat käsitteinä ihmisille suhteellisen uusia. Bob Thomas kehitti vuonna 1971 ensimmäisen tietokoneviruksen nimeltään Creeper. Se on matotyyppinen tietokonevirus, joka replikoi itseään ja jatkaa saastuttamista kovalevyllä, verkossa, tai missä ikinä se onkaan. Creeper itse asiassa kehitettiin tietoturvatestauksen tuloksena, jossa tutkittiin voisiko tällainen haittaohjelma olla mahdollista tehdä. (Kaspersky,n.d.)

Vaikka käsitteet ovat uusia ne eivät kuitenkaan ole asioina uusia. Esimerkiksi kryptografia, eli tiedon salausta, pohjautuu muinaisiin egyptiläisiin hieroglyfeihin. Kryptografiaa käytetään edelleen pankkikorttien salauksessa, tietokoneiden salasanoissa ja sähköisessä kaupankäynnissä. (Fortinet n.d).

2.1.1 Varhaiset vaiheet

1960-luvulla rakennettiin ensimmäinen tietoverkko nimeltään ARPANET, joka on lyhenne sanoista Advanced Research Projects Agency Network. Arpanet johti nykyisin tuntemamme ja käyttämämme internetin syntyyn. Ensimmäiset kyberhyökkäykset nähtiin jo 1970 -luvulla. Hakkeriryhmä Wizards of MIT pääsi luvatta käsiksi eri organisaatioiden tietokonejärjestelmiin, muun muassa Massachusetts Institute of Technologyn tietokonejärjestelmään. Opiskelijoiden tarkoituksena ei ollut tehdä haittaa, eivätkä he sellaista aiheuttaneetkaan. Monesta Wizards of MIT:n jäsenistä tuli tietoturva-alan uranuurtajia, ja he autoivat perustamaan MIT:n ensimmäisen tietoturvalaboratorion. (Mundzir 2023.)

Kuvan 1 mukaan ensimmäiset palomuurit tuotiin osaksi verkkoinfrastruktuuria 1980 -luvun loppupuolella. Palomuri on järjestelmä, joka on suunniteltu estämään luvaton pääsy verkkoon tai verkosta ulos. Palomuri toimii siten, että

se tarkastelee saapuvaa ja lähtevää liikennettä verkossa ja sallii, tai estää sen turvallisuuskäytäntöjen perusteella. Palomuuritekniikka kehitettiin vastauksena verkkohyökkäysten kasvavaan määrään ja parempien turvatoimien tarpeeseen. Palomuurit ovat tänäkin päivänä tehokas puolustus kyberhyökkäyksiä vastaan. (Mundzi, 2023.)

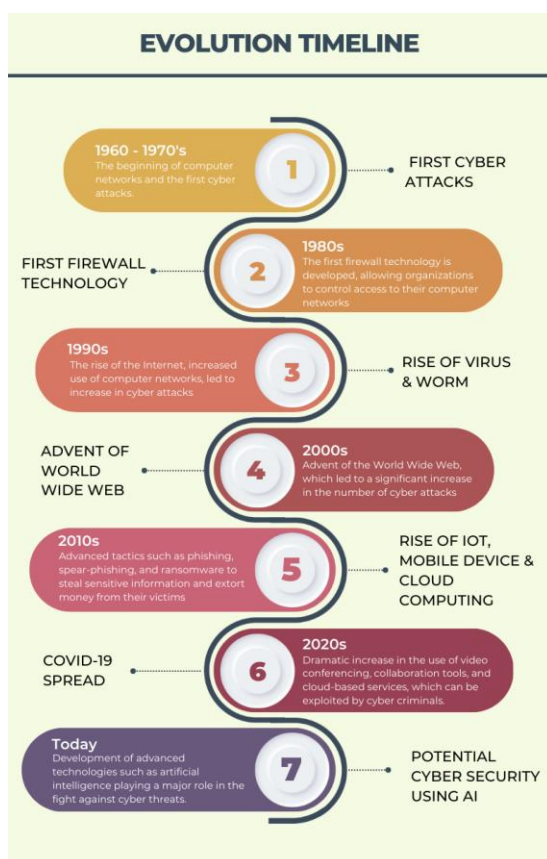
Kun verkko jatkoi kehittymistään, hyökkäysten riski kasvoi, sillä yhä useampia arkaluonteisia tietoja tallennettiin ja siirrettiin Internetin kautta. 1990 -luvulla tapahtui merkittäviä korkean profiilin hyökkäyksiä. Melissa-virus vuonna 1999 ja ILOVEYOU -mato vuonna 2000 korostivat tietoverkkojen haavoittuvuutta ja tarvetta parantaa turvallisuutta ja turvatoimia. Näihin aikoihin kehitettiin ensimmäiset versiot järjestelmistä, jotka havaitsevat tunkeutujat verkossa, ja reagoivat niihin. Järjestelmiä kutsutaan tunkeutumisenhavainnointijärjestelmiksi (IDS, Intrusion Detection System). Samoihin aikoihin kehitettiin myös parempia salaustekniikoita, joiden avulla suojattiin arkaluonteisia tietoja. (Mundzir 2023.)

2.1.2 Internetin aikakausi

Internetin eli WWW:n käyttö on muokannut yhteiskuntien ja yksilöiden käyttäytymistä merkittävimmin sitten teollisen vallankumouksen. Digitalisaatio on 2000-luvulle tultaessa muuttanut muun muassa maksutavat, kaupankäynnin, rahoituspalvelut, opiskelun ja työskentelyn. Muutos on mahdollistanut myös rikollisten ja hakkereiden hyökkäykset maailmanlaajuisesti, ja tietoverkkohyökkäykset yleistyivät tämän seurauksena räjähdysmäisesti. Lisäksi uusien haittaohjelmien, kuten vakoilu- ja mainosohjelmien, ilmaantuminen lisäsi verkkohyökkäysten aiheuttamaa uhkaa. Tietoverkkoturvallisuus kehittyi edelleen, ja uusia turvatoimia ja virustorjuntatekniikoita kehitettiin ja otettiin käyttöön. (Mundzir 2023.) Tyypillinen hyökkäys verkkopalveluissa ovat kyselykielen (SQL, Structured Query Language) -injektio, jonka avulla hyökkääjät voivat varastaa, poistaa tai muuttaa dataa. (Rapid7 n.d). Toinen samankaltainen on sivustojen välinen komentosarjahyökkäys. Tässä lisätään haittakoodia luotettaviin sivustojen sisältöön. (Kaspersky n.d).

2010-luvulla nähtiin voimakas kasvu mobiililaitteiden, IoT -laitteiden sekä erilaisten pilvipalveluiden käytössä. Myös verkkohyökkäykset muuttuivat kehittyneemmiksi ja kohdennetummiksi. Uudet hyökkäysmenetelmät ja -tavat, kuten kalastelu, kiristyshaittaohjelmat ja kohdennettu kalastus yleistyivät. Niiden avulla rikolliset pyrkivät varastamaan arkaluontoisia tietoja tai kiristämään uhreiltaan rahaa. Mobiililaitteiden hallinta-ratkaisut (MDM, Mobile Device Management) kehitettiin organisaatioiden tarpeisiin suojata ja hallita mobiililaitteita ja monivaiheinen tunnistautuminen (MFA, Multifactor Authentication) tarjosi lisäturvaa arkaluontoisille tiedoille kuten kirjautumistunnuksille. (Mundzir 2023.)

2020-luvulla ja erityisesti Korona-pandemian aikaan etätyöskentely yleistyi ja pilvipalveluiden sekä videopalaverien käyttö lisääntyi. Yksi keskeisistä haasteista oli käyttäjän etätyöpisteen ja verkon suojaaminen. Tätä varten otettiin käyttöön virtuaaliset yksityiset verkot (VPN, Virtual Private Network) ja pakotettu kaksivaiheinen tunnistautuminen.



KUVA 1. Tietoturvan evoluutio (Mundzir 2023).

2.2 Nykyaikaiset uhat

Nykyaikaiset uhat voidaan jakaa tietoturvauhkiin, tietoturvatapahtumiin sekä tietoturvaloukkauksiin. Tietoturvauhka viittaa ilkeältäiseen tekoon, jonka tavoitteena voi olla datan tai järjestelmän korruptoiminen, tietojen varastaminen tai organisaation ja sen järjestelmien häirintä. Tietoturvatapahtuman aikana yrityksen tiedot ovat saattaneet paljastua. Tietoturvaloukkaus on tietoturvatapahtuma, joka johtaa tietojen vuotamiseen tai verkkomurtoon.

Nykypäivänä uhkia on monenlaisia. IT-tiimeillä voi olla vastassaan muun muassa sisäisiä tai ulkoisia tekijöitä, sekä tietoihin tai infrastruktuuriin kohdistuvia uhkia, kuten botnetit, virukset ja DDoS:t. Alla käsitellään viittä nykypäivänä esiintyvää tietoturvauhkaa tai riskiä. (Techtarget 2024.)

2.2.1 Sisäiset uhkatekijät

Sisäisiä uhkatekijöitä ovat henkilöt, joilla on pääsy sisäiseen verkkoon, joko olemalla valtuutettu organisaation työntekijä tai työntekijän läheinen. Sisäisillä uhilla tarkoitetaan sitä, että tämän kaltaiset henkilöt tahallaan, tai tahattomasti käyttävät tätä pääsyä väärin vaikuttaakseen kielteisesti organisaation kriittisiin tietoihin ja järjestelmiin. (Techtarget contributor 2024.)

Huolimattomat työntekijät, jotka eivät noudata yrityksen tai organisaation asettamia liiketoimintasääntöjä ja -käytäntöjä, aiheuttavat sisäisiä uhkia. Nämä henkilöt saattavat luovuttaa tiedostaen tai tiedostomatta asiakastietoja tai kirjautumistietoja klikkaamalla kalastelu-linkkejä. Jotkut työntekijät kiertävät sääntöjä mukavuudenhalun, laiskuuden tai tuottavuuden tähden. On myös henkilöitä, jotka tahallaan tekevät tätä, päästäkseen käsiksi yritystietoihin aikeenaan myydä tai jollakin tapaa hyötyä siitä. (Techtarget 2024.)

Sisäisten uhkien ehkäisyyn auttaa työntekijöiden pääsyn rajoittaminen vain niille resursseille, joita he tarvitsevat työnsä tekemiseen. Uusille työntekijöille ja alihankkijoille tulee järjestää tietoturvakoulutus ja vasta tämän jälkeen sallia

heille pääsy yrityksen resursseihin. Uhkia ehkäisevät myös kaksivaiheinen tunnistautuminen kirjautumisessa sekä päätelaitteiden tunnistamisen ja reagointi järjestelmän (EDR, Endpoint Detection and Response) käyttöönotto työasemissa. (Techtarget 2024.)

2.2.2 Kalastelu

Phising-hyökkäykset eli tietojenkalasteluyritykset ovat tietoturvauhkia, joissa käytetään sosiaalista manipulointia tavoitteena huijata käyttäjiä rikkomaan tavanomaisia käytäntöjä ja luovuttamaan luottamuksellista tietoa, kuten nimiä, osoitteita, kirjautumistietoja, luottokorttitietoja jne. (Techtarget 2024.)

Useissa tapauksissa hakkerit lähettävät väärennetyjä sähköpostiviestejä, jotka näyttävät oikeilta, laillisilta ja tutuilta lähettäjiä tulleilta. Suosituimpia hakkereiden käyttämiä lähettäjiä ovat eBay, PayPal, ystävät, sukulaiset ja kollegat. Näiden tarkoituksena on saada käyttäjä klikkaamaan sähköpostissa tai viestissä olevaa linkkiä, joka vie heidät huijaussivustolle, jossa heitä pyydetään luovuttamaan arkaluontoisia tietoja. (Techtarget 2024.)

Merkittävin tapa ehkäistä kalastelua on kunkin käyttäjän sähköpostiosaaminen. Kunkin käyttäjän tulisi oppia tuntemaan huijaussähköpostien ja aitojen viestien hiuksenhienot erot. Organisaatiot saattavat ottaa myös käyttöön anti-phishing -sääntöjä tietoturvanhallinnassa ja -valvonnassa. Myös palomuurit toimivat hyvänä suojana kalastelua vastaan. (Techtarget 2024.)

2.2.3 Kiristyshaittaohjelmat

Ransomware eli kiristyshaittaohjelma toimii siten, että uhrin tietokone tai resurssi lukitaan yleensä salaamalla se, jolloin uhri ei pysty käyttämään laitetta tai siihen tallennettuja tietoja. Saadakseen tiedostot tai laitteen takaisin, uhrin on maksettava kiristäjälle lunnaita. Nykypäivänä Bitcoin tai muu virtuaalivaluutta on suosittu Ransomware -lunnasrahana. Ransomware voi levitä

sähköpostiliitteiden, ohjelmistosovellusten, tallennuslaitteiden tai vaarantuneiden verkkosivujen kautta. (Techtarget 2024.)

Erittäin tehokas varatoimenpide on jatkuvasti varmuuskopioida laitteet ja tiedostot, sekä päivittää sovellukset ajan tasalle. Myös käyttäjien samanlainen sähköpostien tuntemus kuin kalastelussa lisää suojaa. (Techtarget 2024.)

2.2.4 Virukset ja madot

Virukset ja madot ovat haittaohjelmia, joiden tarkoituksena on tuhota organisaation järjestelmät, tiedot ja verkko. Tietokonevirus on haitallista koodia, joka monistuu kopioimalla itsensä toiseen ohjelmaan, järjestelmään tai isäntätiedostoon. Se pysyy lepotilassa, kunnes joku tietoisesti tai tahattomasti aktivoi sen ja levittää tartuntaa ilman käyttäjän tai järjestelmän ylläpidon tietoa tai lupaa. (Techtarget 2024.)

Tietokonemato on itsestään monistava ohjelma, jonka ei tarvitse kopioida itseään isäntäohjelmaan tai vaatia ihmisen vuorovaikutusta levitäkseen. Sen päätehtävänä on tartuttaa muita tietokoneita pysyen aktiivisena tartunnan saaneessa järjestelmässä. (Techtarget 2024.)

Näitä tietoturvan uhkia ehkäistään virus- ja haittorjuntaohjelmien asentamisella kaikkiin järjestelmiin ja verkkolaitteisiin. Lisäksi tuntemus oikeaoppisesta ohjelmistojen latauksesta auttaa ehkäisemään vahinkoja. Käyttäjän ei tule ladata ohjelmistoja epäluotettavilta sivuilta. (Techtarget 2024.)

2.2.5 palvelunestohyökkäys

Distributed Denial of Service, eli hajautettu palvelunestohyökkäys, on tarkoituksellinen hyökkäys, jossa luvattomasti haltuun otetut tai vaarantuneet koneet hyökkäävät valittuun kohteeseen. Kohteena yleensä toimii palvelin, verkkosivusto tai jokin muu verkkoresurssi. Palvelunestohyökkäyksen tavoite on

tehdä ne toimintakyvyttömiksi. Yhteyspyyntöjen, saapuvien viestien tai epämuodostuneiden pakettien tulva pakottaa kohdejärjestelmän hidastumaan tai kaatumaan ja sammumaan, jolloin normaalit käyttäjät tai järjestelmät eivät voi käyttää palvelua. Tämä on hyvin yleistä nykypäivänä valtioiden hybridi-vaikuttamisessa. Palvelunestohyökkäys on myös tapa, jolla ihmiset yrittävät vaikuttaa oman valtionsa menetelmiin ja politiikkaan. Näitä henkilöitä kutsutaan haktivisteiksi. (Techtarget 2024.)

DDoS -hyökkäykset estetään käyttämällä palomuuureja sekä varastoimalla kopioita yhteyspyynnöistä, jotta vältetään yhteystulva. On hyvä myös varmistaa, että palvelimilla on kapasiteettia käsitellä voimakkaita piikkejä. (Techtarget 2024.)

2.3 Periaatteet

Tietoturva koostuu kolmesta tavoitteesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Tätä kolminaisuutta kutsutaan CIA kolmioksi, eli Confidentiality, Integrity ja Availability. (Imperva n.d.)

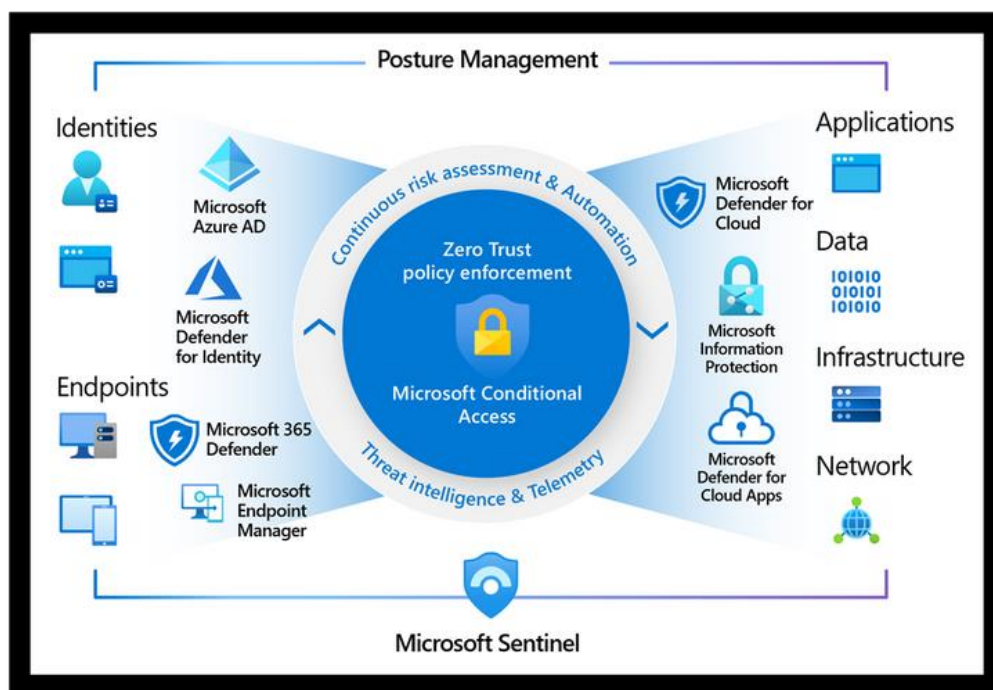
Luottamuksellisuusperiaatteen tavoite on pitää henkilötiedot yksityisinä ja varmistaa, että ne ovat näkyvissä ja saatavilla vain niille henkilöille, jotka omistavat ne tai tarvitsevat niitä organisaation tehtäviensä hoitamiseen. (Imperva n.d.)

Eheyden periaatteella varmistetaan, että tiedot ovat tarkkoja ja oikeita, eikä niitä muuteta virheellisesti vahingossa tai tahallisesti. Tarkoituksena on pitää siis tiedot turvassa luvattomilta muutoksilta. Näihin kuuluvat virheellisen tiedon lisäys, asiattomat poistot ja muutokset. (Imperva n.d.)

Saatavuus tarkoittaa kykyä suojata järjestelmät ja data siten, että ne ovat aina täysin saatavissa, kun käyttäjä niitä tarvitsee. Käytettävyyden tarkoituksena on saada IT infrastruktuuri, sovellukset ja tiedot käyttöön, kun organisaation prosessi tai organisaation asiakas sitä vaatii. (Imperva n.d.)

3 MICROSOFTIN TIETOTURVATYÖKALUT JA -PALVELUT

Microsoft tarjoaa suuren määrän erilaisia tietoturvatyökaluja asiakkailleen näiden käyttöön. Tässä osiossa käydään läpi, mitä työkaluja on tarjolla ja mitä hyötyjä ne tarjoavat käyttäjilleen. Alla olevassa kuvassa näkyy Microsoftin tarjoamat tuotteet sekä työkalut.



KUVA 2. Microsoftin tarjoamat tuotteet (Alan La Pietra 2022).

3.1 Microsoft Defender XDR

Microsoft Defender XDR on Microsoftin tietoturvaketti. Sen avulla voidaan havaita tietoturvariskit, tutkia hyökkäyksiä ja estää haitalliset toiminnot. Se koostuu monesta eri tietoturvaratkaisusta. Sen eri ratkaisuja ovat päätelaitesuojaus Defender for Endpoint, Defender for Office 365, joka on tarkoitettu Office -työkaluille sekä Defender for Identity ja Defender for Cloud Apps. (gitbit n.d). Yleensä kun puhutaan Defender XDR:stä, silloin tarkoitetaan Defender portaalia. Kaikki hälytykset, hallinta ja konfiguraatio on sijoitettu tähän portaaliin.

Defender XDR:n ominaisuuksia ovat juurikin yllä mainittu keskitetty hallinta, hyökkäysten esto reaaliajassa ja uhkien metsästys. Defender for Office 365 suojaa esimerkiksi sähköpostilaatikat haitallisilta kalasteluviesteilä, kun taas Defender for Endpoint suojaa päätelaitteen, jos haittaohjelma pääsisi työasemalle asti. Uhkien metsästyksellä tarkoitetaan datakyselyiden suorittamista raakaan dataan, jonka avulla saadaan selville hyökkäystaktiikoita ja hyökkäysmenetelmiä. (Xcitium n.d).

3.2 Defender for Endpoint

Yksi Microsoft 365 Defenderin ratkaisusta on Defender for Endpoint, joka toimii Microsoftin EDR -järjestelmänä käyttäen kehittynyttä koneoppimista ja käyttäytymisanalytiikkaa vastaten kehittyneisiin hyökkäyksiin sekä murtoihin. Tämä tuote pitää sisällään päätelaitteiden suojauksen sekä EDR -ominaisuuden (Alan La Pietra, 2022).

Defender for Endpoint on holistinen päätelaitteiden suojausratkaisu. Se suojaa laitteita muullakin tavalla, kuin pelkällä antivirusella. Sen viisi ydinominaisuutta ovat:

- Hyökkäyspinta-alan pienentäminen
Analysoi hyökkäyspinta-aloja ja pakottaa sääntöjä, jotka vähentävät hyökkäysalueita päätelaitteella (BlueVoyant nd).
- EDR
Tämän avulla havaitaan uhkia ja hyökkäyksiä reaaliajassa ja vastataan niihin (BlueVoyant nd).
- Uhkien ja haavoittuvuuksien hallinta
Auttaa vähentämään haavoittuvuuksien aiheuttamia riskejä. (BlueVoyant nd).
- Automaatio
Tutkii ja analysoi metodeja hälytysten priorisointiin sekä automaattisesti reagoi niihin. (BlueVoyant nd).
- Turvallisuuspisteytys

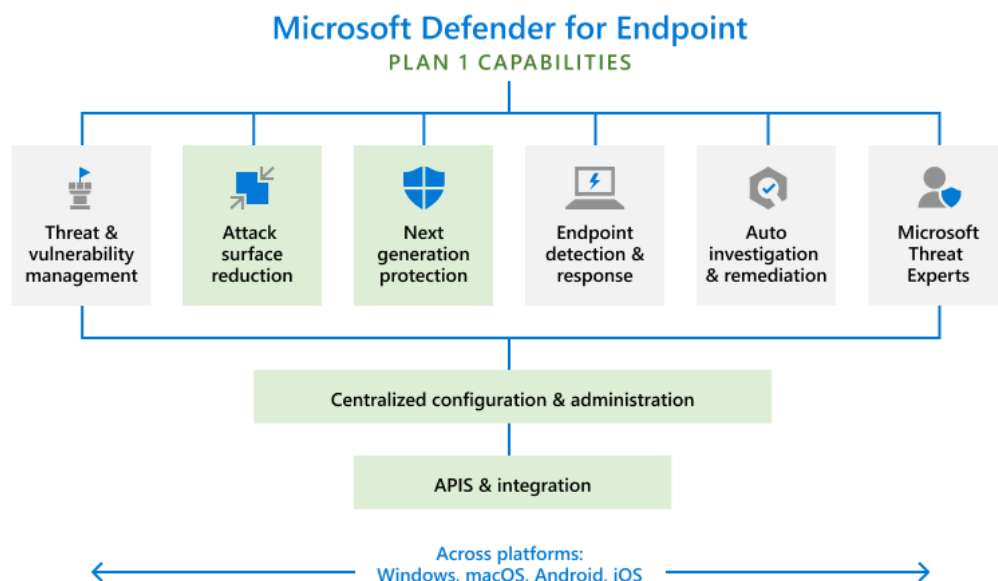
Pisteyttää turvallisuustason sovellusten, käyttöjärjestelmän, verkon ja käyttäjien mukaan (Seren Tamayo 2023).

EDR on vahva työkalu ja ominaisuus Defenderissä. Se viittaa päätelaitteiden uhkien havainnointiin, niihin reagoimiseen, analysointiin ja jälkiselvittelyyn. Taulukossa 1 on listattu EDR:n ominaisuudet ja niiden tarkoitus. (Cisco. N.d).

Ominaisuus	Tarkoitus
Havaitseminen	Uhka on päässyt ympäristöön, EDR havaitsee sen.
Rajaaminen	Havaitsemisen jälkeen, uhka eristetään ja rajataan.
Tutkiminen	Tutkitaan, miten uhka on päässyt ympäristöön sekä, mitä se on tehnyt.
Eliminointi	Uhka poistetaan ympäristöstä tai järjestelmästä.

TAULUKKO 1. EDR:n ominaisuudet.

Defender for Endpoint:sta on saatavilla kaksi erilaista tilausta. Nämä ovat perustason Plan 1 ja korkeamman tason Plan 2. Perustaso pitää kuvan 3 vihreällä merkityt ominaisuudet ja korkeampi taso pitää sisällään kaikki jotka kuvassa esiintyvät. Perustason pääpiirteet ovat tehokkaampi antivirus, manuaaliset toimenpiteet sekä hyökkäyspinta-alojen vähentäminen. Molemmat tarjoavat myös konfiguraation, hallinnoinnin ja suojauksen usealla eri alustalla kuten Windowsilla, macOS:llä, iOS:llä ja Androidilla. (Siosulli ym. 2023.)



KUVA 3. Endpoint Plan 1 (Siosulli, denisebmsft, diannegali, Blake-Madden, Dansimp, sheshachary, msbemba, chrisda, v-smandalika, JoeDavies-MSFT, BrunoDal, alekyaj ja v-mathavale 2023).

3.3 Defender for Cloud

Defender for Cloud on Azure-natiivi, joten monet palvelut ja resurssit ovat valvonnassa ja suojattuna ilman erillistä käyttöönottoa. Monipilvi- tai hybridiympäristöissä palvelimet tuodaan suojauksen piiriin käyttämällä Azure Arc -komponenttia. Tämän avulla suojataan esim. on-prem palvelimet ja AWS -palvelimet. (Alan La Pietra 2022.) Defender for Cloud tarjoaa seuraavat toiminnot:

- Turvallisuuspisteytys
Tämä on ominaisuus, jonka Defender for Cloud tarjoaa organisaatioille. Se antaa ymmärryksen, kuinka hyvässä tilanteessa turvataso on ja antaa ehdotuksia sen parantamiseksi. (Kanupriya Chauhan 2023.)
- Tietoturvahälytykset
Palvelu hälyttää myös tietoturvarikkeistä tai niihin johtavista tapahtumista Security Center -portaalissa. (Kanupriya Chauhan 2023.)
- Pilviturvallisuuden hallinta
Tunnistaa ja ehkäisee virheelliset konfiguraatiot pilviympäristöissä (Ajay Kumar 2023.)
- Integraatio Microsoftin tietoturvaratkaisujen kanssa
Defender for Cloud on myös helposti integroitavissa Microsoft Sentinelin, Defender for Endpointin ja 365 Defenderin kanssa. (Kanupriya Chauhan 2023.)

Defender for Cloud suojaa mm. virtuaalipalvelimet, on-premise palvelimet sekä muut Azuressa sijaitsevat resurssit. Näitä resursseja voivat olla varastot, avainholvit ja verkkosovellukset. Se tarjoaa myös tietoturvahälytyksiä resursseihin kohdistuvista väärinkäytöistä ja hyökkäyksistä. Kaikki toiminta keskittyy Azuressa Security Centeriin, jossa on keskitetty näkymä hälytyksille sekä pilviturvallisuuden hallinnalle (CSPM, Cloud Security Posture

Management). (Dcurwin, Naveenommi-MSFT, Mattbriggs, V-alje, Taojunshen, Elazark, Rayne-wiselman, Msm Baldwin, Bmansheim, Kadrita, Bcs2022, Yehkardos, Laurabren, Memildin, 2023.)

Tämä palvelu eroaa Defender for Endpointista siten, että Defender for Cloud on tarkoitettu pilviresursseille ja pilvialustoille. Se pitää sisällään useampia eri mahdollisuuksia suojata työmäärät kuten taulukosta 2 huomataan. Defender for Cloud on erittäin muokattavissa. Sen avulla voi suojata vain niitä resurssityyppejä joita on tarve suojella.

Defender	Tarkoitus
Defender for Servers	Suojelee palvelimia
Defender for Storage	Suojelee varastoresursseja
Defender for Containers	Suojelee kontteja ja niiden sisältöjä
Defender for Key Vault	Suojelee avanholviresursseja

TAULUKKO 2.

Defender for Endpoint suojaa siis päätelaitteita, kuten työasemia. Defender for Cloud puolestaan suurempia kokonaisuuksia tai pieniä osia suuremmasta resurssiympäristöstä. Jos molemmat palvelut ovat käytössä, niin Defender for Cloud:n tuottamat hälytykset integroituvat Defender XDR:än portaaliin automaattisesti, joka toimii muiden Defender -hälytysten valvontapaikkana.

3.4 Microsoft Sentinel

Microsoft Sentinel on pilvipohjainen SIEM -ratkaisu. Sentinel rajoittui ennen hyvin pitkälti Azure resursseihin, mutta uudelleenbrändäyksen myötä monipilviympäristöjä alettiin tukemaan ja nimi muutettiin Microsoft Sentineliksi. Sentinelin avulla organisaatiot voivat kerätä dataa ja tapahtumalokeja erilaisista järjestelmistä, analysoida niitä ja tunnistaa tämän pohjalta mahdolliset uhat. (Mustafa Toroman 2023.)

Sentinelin tarjoamat ominaisuudet parantavat tietoturva- ja valvontaa hyvin paljon ja ne tuovat mukanaan ominaisuuksia, jotka ovat markkinoilla ylivoimaisia:

- Datankeruu ja integraatio

Organisaatiot voivat kerätä dataa useista eri lähteistä, kuten lokeista, tapahtumista ja hälytyksistä. Sen integraatio-järjestelmä on vertaansa vailla. Muutamalla datanjohtimella saadaan tuotua kaikki Microsoftin palvelut Sentineliin. (Kanupriya Chauhan 2023.)

- Uhkien havaitseminen ja metsästäminen
Sentinel tarjoaa kehittynyttä analytiikkaa ja koneoppimista huomataksaan poikkeamia ja uhkia reaaliajassa. Se käyttää sisäänrakennettuja sääntöjä, poikkeamahavainnointia ja käyttäytymisanalysointia huomataksaan epäilyttäviä aktiviteetteja. (Kanupriya Chauhan 2023.)
- Tapahtumien hallinta ja tutkimus
Sentinel tarjoaa myös kattavan tapahtumien hallinnan ja tutkimisen. Rikkaan visualisautensa ja interaktiivisten työkalujen avulla voi suorittaa syvällistä tutkimusta jokaisesta tapahtumasta. (Kanupriya Chauhan 2023.)

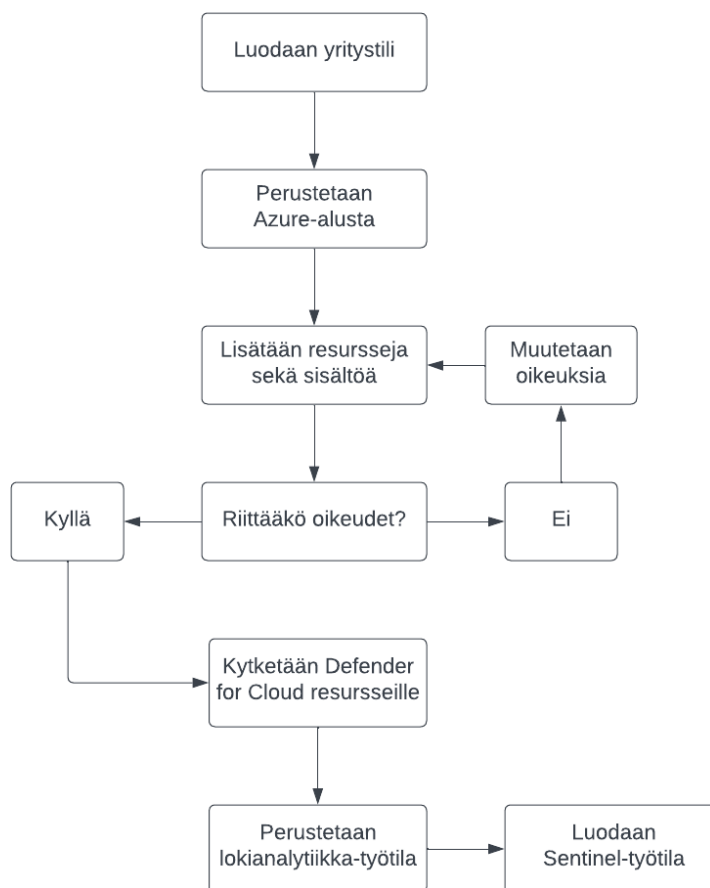
SIEM -ratkaisu on tarkoitettu havaitsemaan, analysoimaan ja vastaamaan tietoturvauxhiin reaaliajassa. Se kerää tapahtumalokeja useasta eri lähteestä ja tunnistaa normaalista poikkeavaa toimintaa sekä reagoi niihin. (Microsoft n.d). Sentinel pitää myös sisällään turvallisuus orkesterointia, automaatiota ja reagointia (SOAR, Security Orchestration, Automation, and Response). Sentinelillä voidaan suorittaa automaatiotehtäviä sen aiheuttamiin hälytyksiin ja tapahtumiin.

4 CASE-TUTKIMUS: MICROSOFTIN TIETOTURVATUOTTEIDEN TESTAUS

Tässä osiossa suoritetaan case-tutkimus Microsoftin Defender for Cloud ja Sentinel -tietoturvatyökaluista. Tavoitteena oli tutkia, miten työkalut otetaan helposti käyttöön, ja mitä ympäristön pystyttäjän tulee ottaa huomioon ennen tuotantoonvientiä. Tutkimukseen kuului aluksi myös Defender for Endpoint, mutta lisensointi syistä tämä jätettiin pois. Jotta EDR olisi toiminut odotetusti ilman mahdollisia virheitä, olisi työasemalla tullut olla Windows Professional -versio.

4.1 Testiympäristön rakentaminen

Lähdettiin luomaan testiympäristöä alla olevan kaavion mukaisella suunnitelmalla.



KAAVIO 1. Vuokaavio testiympäristön rakentamisesta.

Kun Sentinel-työtila on perustettu, lisättiin sinne oleellisia komponentteja, kuten datanjohtimia sekä analytiikkasääntöjä. Tämän avulla saadaan keskitettyä valvonta Sentineliin sekä käyttää sen analytiikkaa tapahtumien tutkimisessa.

Jotta testaamisesta saatiin sujuvampaa, määriteltiin aluksi resurssit, säännöt ja datanjohtimet joita testauksessa käytettiin. Taulukossa 3 on määritelty Azureen sijoitettavat resurssit, taulukossa 2 on Sentineliin lisättävät datanjohtimet ja taulukossa 5 on Sentineliin konfiguroitavat analytiikkasäännöt.

Resurssi	Nimi	Muut tarpeet
Virtuaalikone	Ont-test-vm1	Admin-tunnus
Varasto	ontstorage	Kontti + kuva
Avainholvi	Vault-ont-1	Avain + salaisuus
Avainholvi	Vault-111	Avain + salaisuus
Sentinel-työtila	Sentinel-test-workspace	Konfiguraatiot

TAULUKKO 3. Azuren resurssit.

Datanjohdin	Tarkoitus
Azure Key Vault	Tuoda dataa avainholvin tapahtumista.
Microsoft Entra ID	Tuoda dataa Entra ID - tapahtumista.
Subscription-based Defender for Cloud	Tuoda hälytykset Sentineliin.

TAULUKKO 4. Sentinel datanjohtimet.

Analytiikkasääntö	Tarkoitus
Brute force attacks against Azure portal	Hälyttää väsytyshyökkäyksistä Azure portaalia vastaan.
Sensitive Azure Key Vault operations	Hälyttää epäilyttävistä tapahtumista avainholvin sisällä.
Create incidents based on Microsoft Defender for Cloud alerts	Muuntaa Defender for Cloud:n tuottamat hälytykset tapahtumiksi.

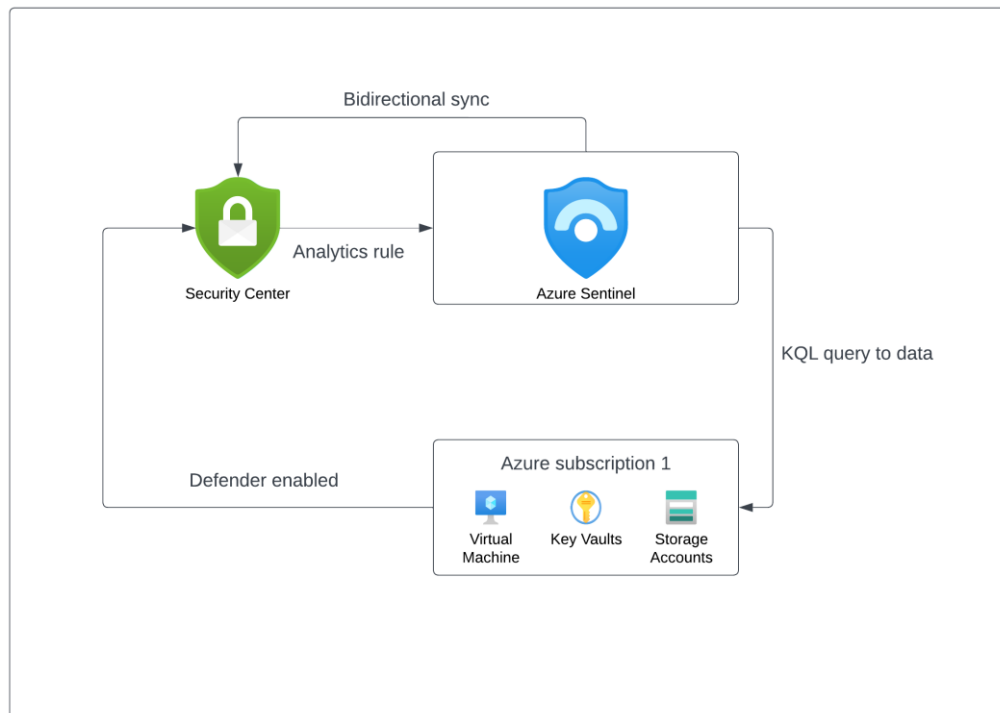
TAULUKKO 5. Analytiikkasäännöt.

Oikeassa projektissa on tärkeää miettiä etukäteen tietoturvalvannon tarkoitusta. Tällöin sääntöjä voi tulla suurikin määrä Sentineliin, riippuen toki ympäristön suuruudesta, monimutkaisuudesta sekä kriittisyydestä. Tässä testauksessa käytetään vain muutamaa sääntöä, sillä tarvetta suuremmalle määrälle ei ole.

4.1.1 Arkkitehtuuri

Kuvassa 4 on testiympäristön arkkitehtuurikaavio. Yksinkertaisuudessaan pohjalla on Azure -tilaus, joka sisältää erilaisia resursseja. Näille resursseille kytketään Azuren tarjoama suojaus Defender for Cloud päälle, jolloin hälytykset tietoturvatapahtumista tulevat Security Centeriin eli Defender for Cloud - palvelun sivulle Azuressa.

Sentinel hakee datan datanjohtimen ja analytiikkasäännön avulla, jotka toimivat myös kaksisuuntaisesti. Esimerkiksi kun tapahtuman tilaa muutetaan Sentinelissä, se vaihtuu myös Security Centerissä, jolloin hallintaa suoritetaan vain ja ainoastaan yhden palvelun kautta. Sentinel on täynnä analytiikkasääntöjä, jotka tekevät KQL -kyselyitä Azure resurssien lokitietoihin, josta se nostaa hälytyksen ja luo tapahtuman, tai mitä se on konfiguroitu tekemään.



KUVA 4. Ympäristön arkkitehtuuri.

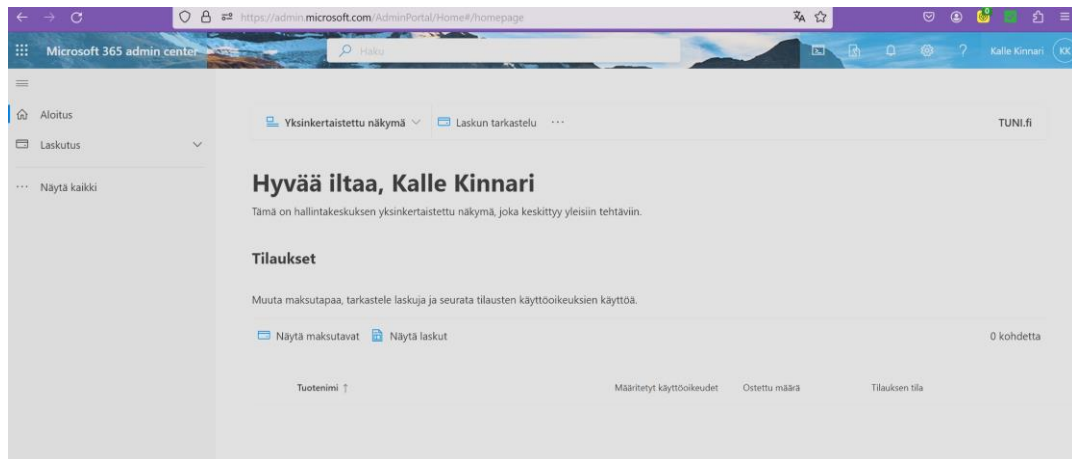
4.1.2 Yritystili

Aluksi perustettiin yksinkertainen sähköpostiosoite. Sähköpostiksi kelpaa mikä vain ja tässä tutkimuksessa käytettiin Gmail -päätteistä sähköpostia.

Seuraavaksi perustetaan Microsoft -yritystili sivulla:

<https://www.microsoft.com/fi-fi/microsoft-365/enterprise/office-365-e5?activetab=pivot:yleiskatsaustab>. Täältä käsin luotiin Microsoft E5 tili ja hyödynnettiin sen tarjoama 30 päivän kokeilujakso.

Täydennetään vaaditut tiedot. Testauksessa käytetään organisaation nimenä MD Security ja osoitteeksi muodostui mdrnsecurity.onmicrosoft.com. Täytettiin loput tiedot ja valtuutettiin tämä kaikki puhelintodennuksella. Kun kaikki tiedot on täytetty, tili on valmis. Siirrytään kuvan 5 osoitteeseen, joka on Microsoftin pääkäyttäjakeskus.

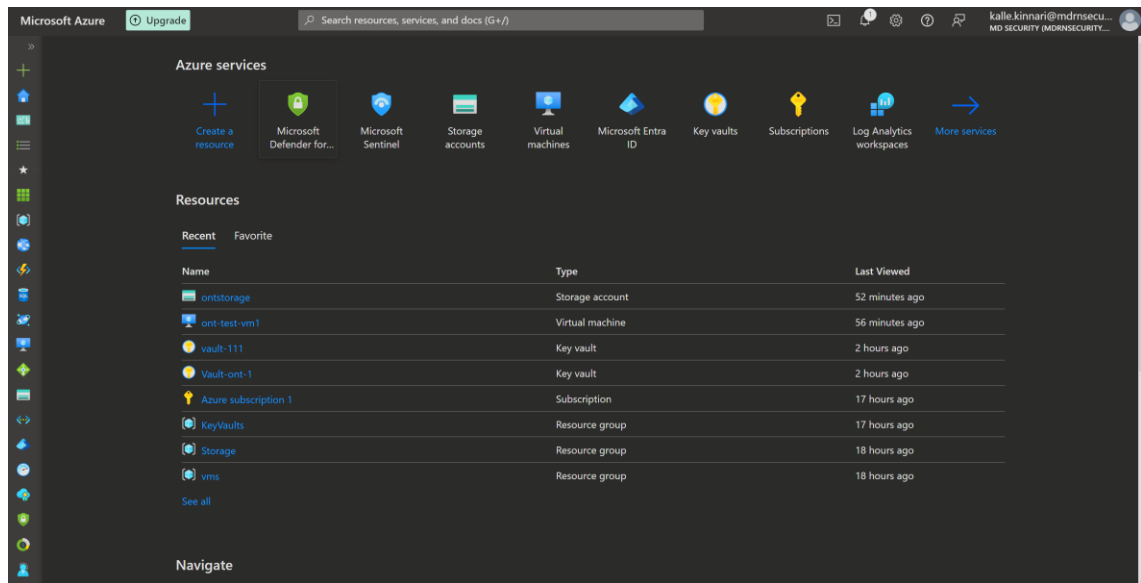


KUVA 5. Yritystili.

4.1.3 Azure

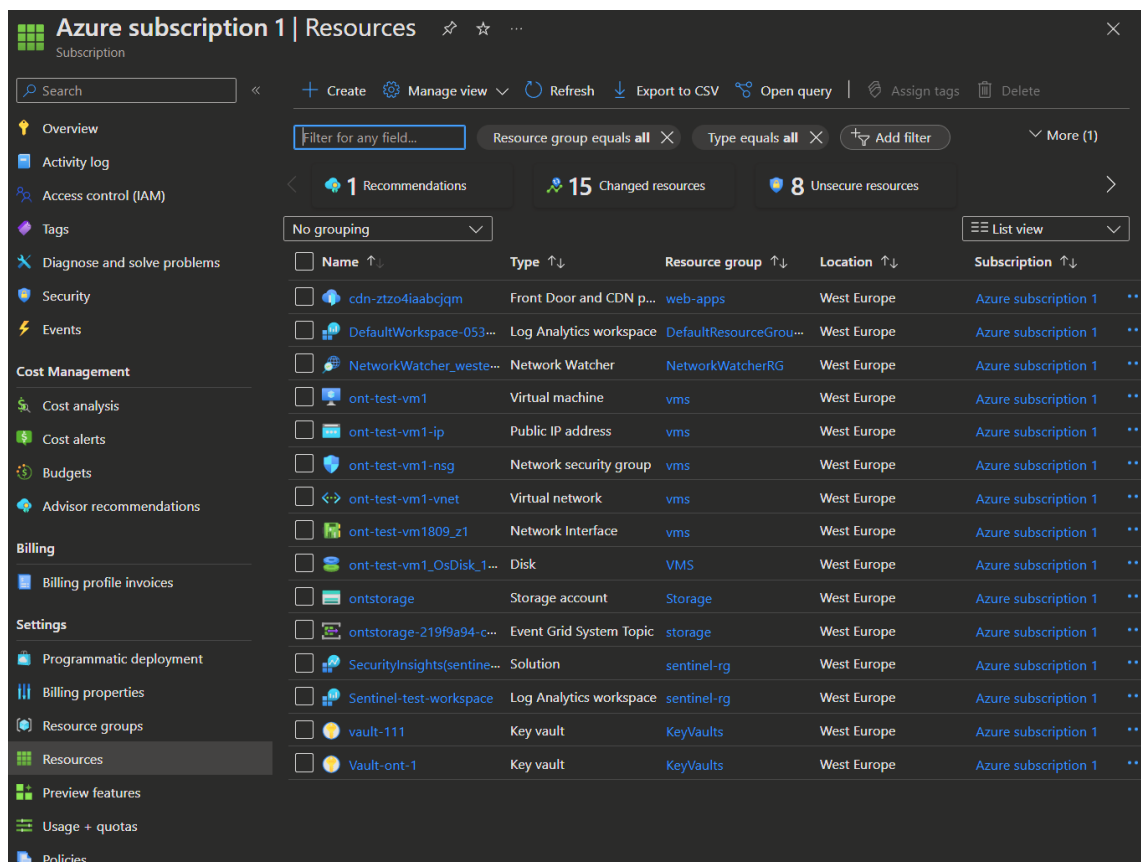
Tilin perustamisen jälkeen, tehtiin Azureen ilmainen käyttäjä, jossa saatiin käyttöön 200€:n edestä ilmaisia krediittejä, joilla ostettiin resursseja tuntiveloituksella. Lopulta tähän ei paljoa ole, varsinkaan, jos resursseja on paljon. Mutta tämänkaltaiseen testaukseen tämä oli täydellinen vaihtoehto.

Azure alustettiin sivulla azure.microsoft.com. Kirjaututtiin sähköpostilla kalle.kinnari@mdrnsecurity.onmicrosoft.com, jotta Azure tulee saman tilin alle. Tässä on muutama huomioitava asia. Tilin täytyy olla uusi ja sillä ei ole saanut suorittaa aikaisemmin Azuren kanssa mitään kokeilujaksoa. Myös puhelinnumero, jolla validoidaan käyttäjä, tulee olla sellainen, jota ei ole ennen käytetty. Kun käyttäjä on luotu, päästiin Azuren aloituspaneeliin, kuten kuvassa 6 huomataan.



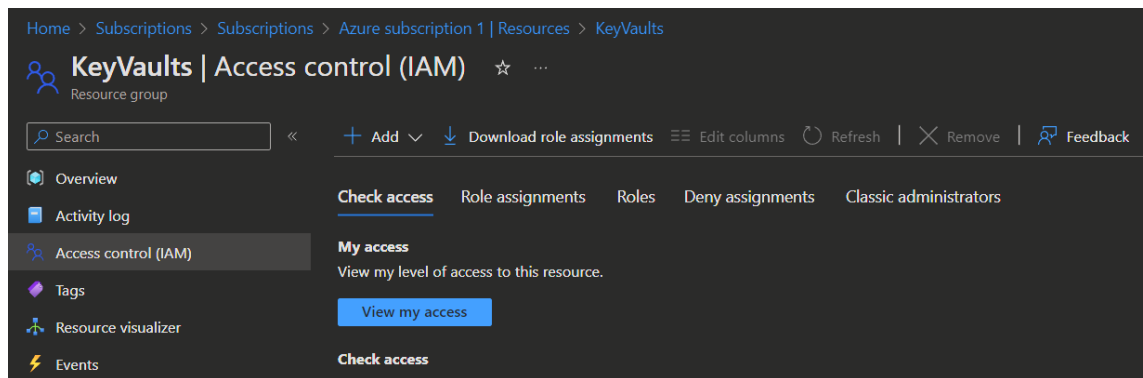
KUVA 6. Tervetuloa Azure -portaaliin.

Jotta testaus onnistuu, Azureen luotiin resursseja jo olemassa olevaan tilaukseen Azure Subscription 1. Resursseja pystyi kätevästi luomaan tilauksen Resources -välilehdeltä kohdan **5.1** määritysten mukaisesti. Kuvassa 7 on listattuna luodut resurssit.



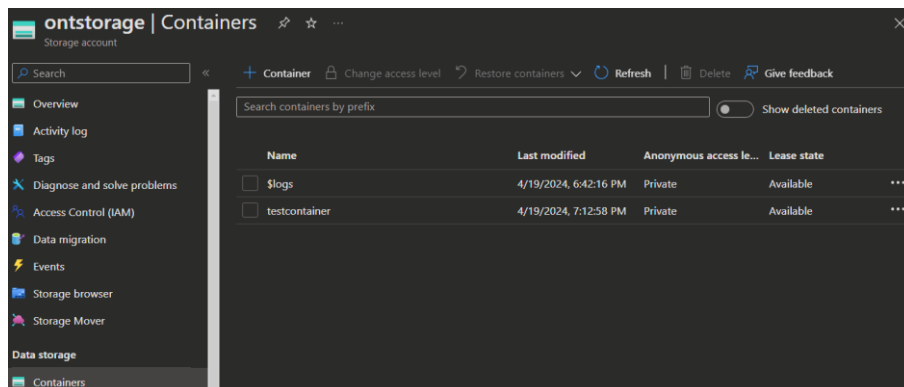
KUVA 7. Resurssilistaus.

Resurssit eivät vielä itsessään tuo arvoa testaukselle, vaan ne vaativat jonkinlaista sisältöä. Jotkin resurssit, kuten avainholvi vaati erilaisen käyttöoikeuden. Resurssia luodessa määriteltiin, että oikeudet tulee valtuuttaa RBAC -pohjalta. Eli lisättiin oikeudet kyseiseen resurssiin 'Key Vault Administrator' -roolin avulla. Roolit lisätään kyseisen resurssin identiteetti ja pääsynhallinta (IAM, Identity and Access Management) -välilehdeltä, kuten kuvassa 8 huomataan. Kun oikeudet resurssin käsittelyyn saatiin, holville luotiin avain sekä salaisuus resurssin omilla sivuilla.



KUVA 8. Key Vault -roolitus.

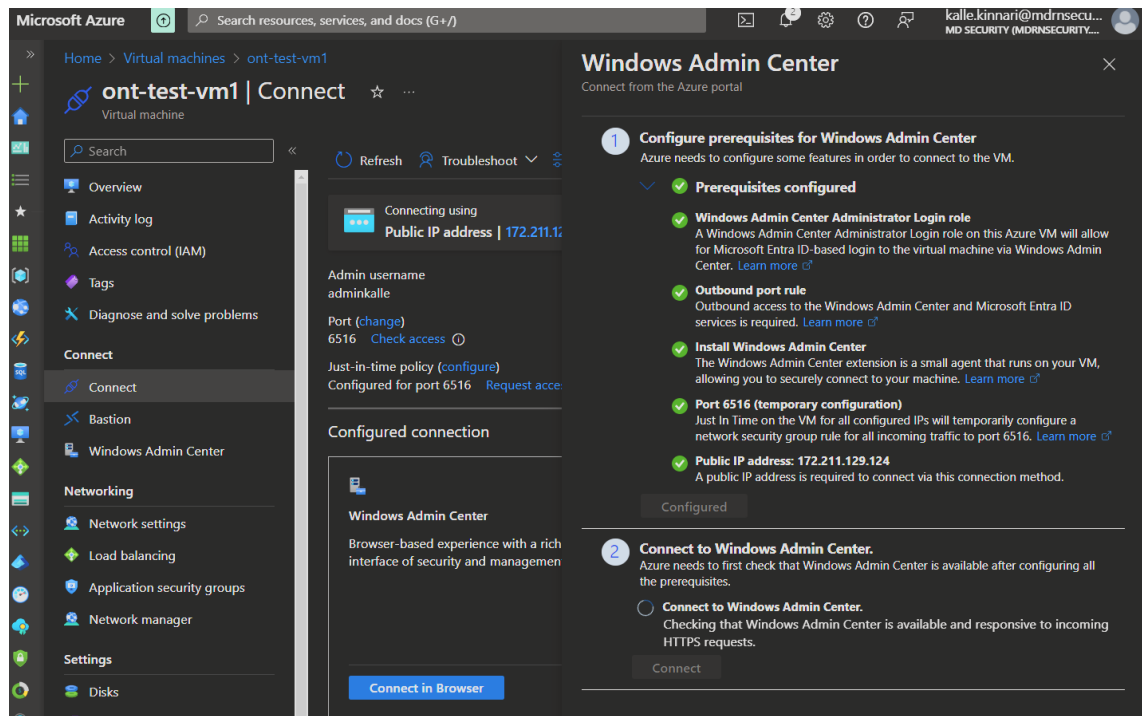
Sama toteutettiin myös varasto-resurssille. Sen sisälle lisättiin kontti, johon upotettiin kuvatiedosto. Sisältö luotiin samalla tavalla kuin avainholvissa resurssin omalla sivulla kuvan 9 mukaisesti.



KUVA 9. Varasto -resurssi.

Jotta virtuaalikonetta on mahdollista testata, tulee varmistaa yhteydenotto virtuaalikoneelle. Resurssia luodessa siihen lisättiin pääkäyttäjä-tunnus, jotta kirjautuminen on mahdollista. Azure tarjoaa eri vaihtoehtoja yhdistämiselle kuten paikallisen RDP -yhteyden, natiivin SSH -yhteyden, Bastionin, Serial

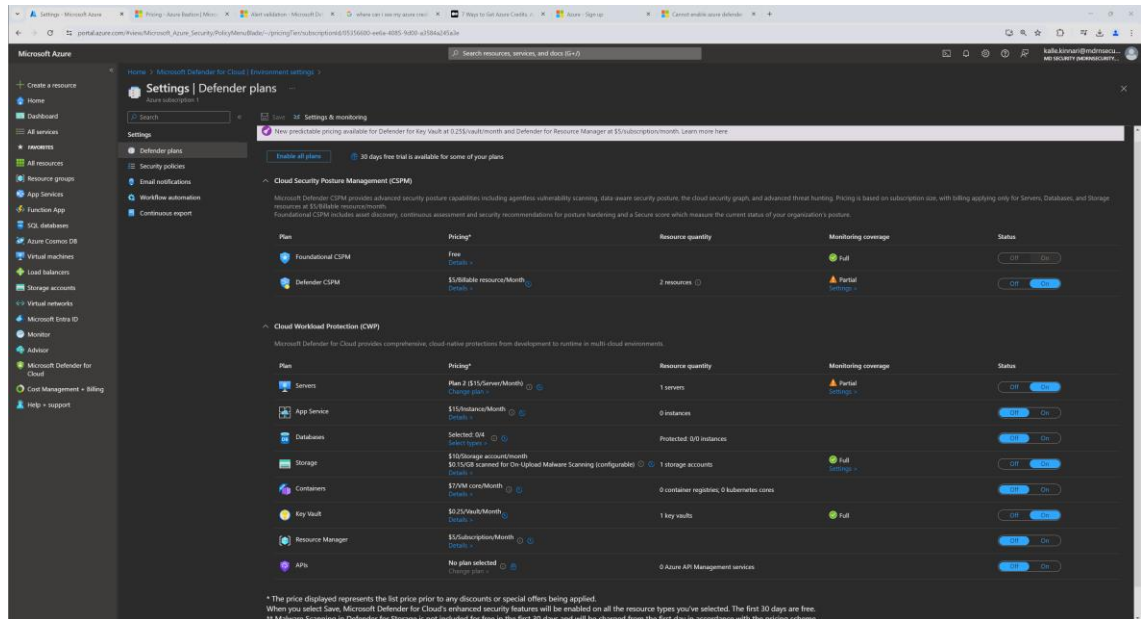
konsolin ja Windows Admin Center:n. Kuvassa 10 valittiin yhdistämiskeinoksi Windows Admin Center.



KUVA 10. Virtuaalikoneelle kirjautuminen.

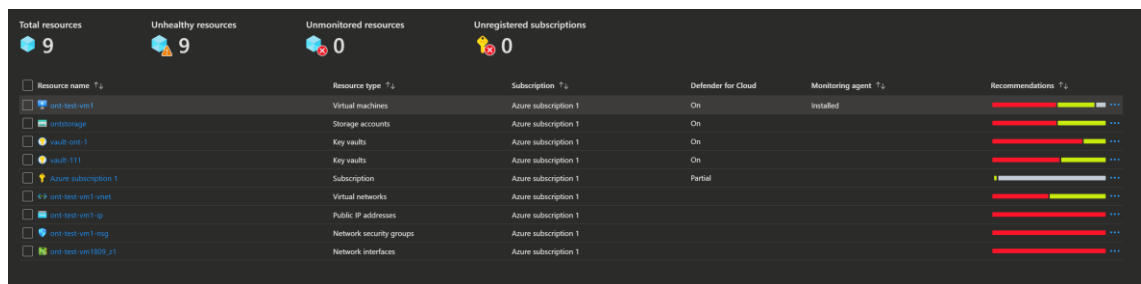
4.1.4 Defender for Cloud

Resurssien ja sisällön luomisen jälkeen oli aika kytkeä Defender for Cloud päälle. Defenderin käyttöönotto on hyvin yksinkertaista. Azure haun kautta haettiin Defender for Cloud, jossa navigoidaan 'Environment settings' -välilehdelle. Kuvan 11 mukaisessa näkymässä Defender kytketään päälle sekä sitä on mahdollista mukauttaa organisaation tarpeiden mukaan.



KUVA 11. Defender -tilauksen mukauttaminen.

Kuvassa 12 varmistettiin, että resurssit ovat suojattuja Defenderin kytkennän jälkeen, jossa kesti noin tunti.

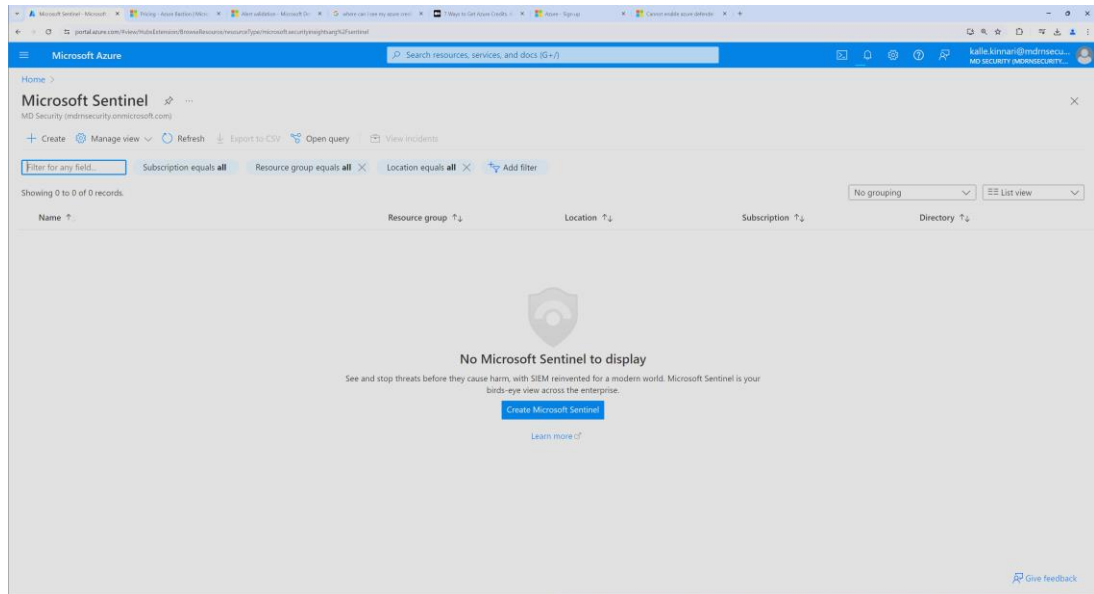


KUVA 12. Defenderin tarkistus resursseissa.

Synkronoinnin jälkeen täydennettiin ympäristöä vielä hieman, lisäämällä CSPM ja ISO 27001:2013 käytännöt koko ympäristölle. Oikeassa projektissa ei välttämättä tätä tarvitse tehdä, sillä käytäntöjen seuranta vaihtelee jokaisessa projektissa. Tämä tehtiin kuvan 11 näkymässä 'Security policies' -välilehdellä.

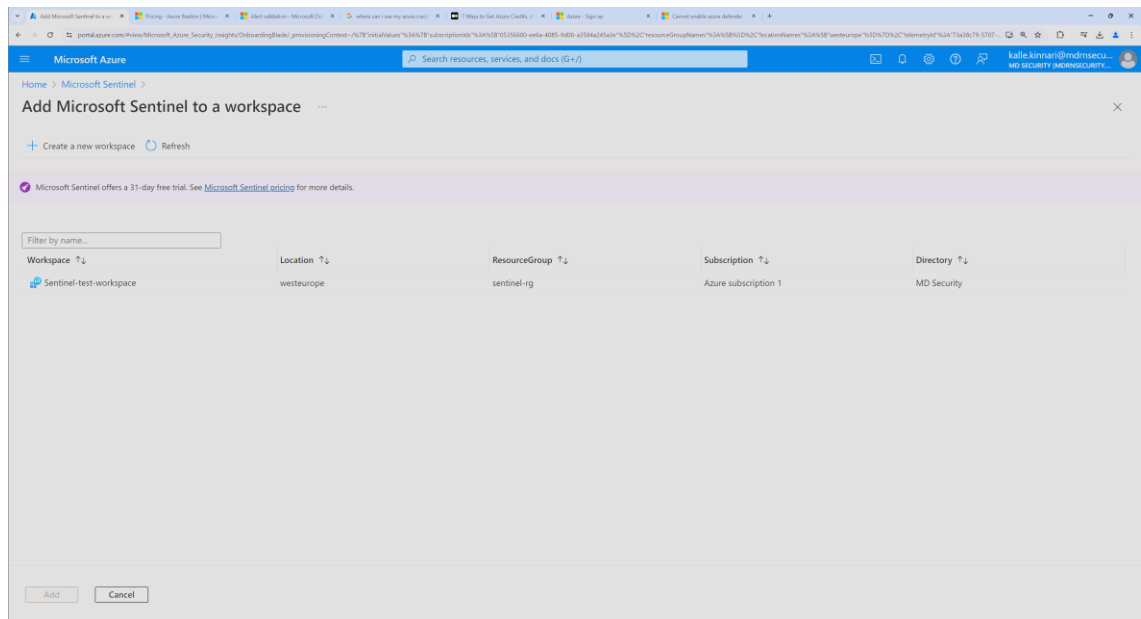
4.1.5 Sentinel

Viimeisenä osana rakentamista luotiin Sentinel -työtila, joka toimii kaiken keskuksena. Työtilaa luodessa, Azure kehottaa luomaan lokianalytiikka-työtilan, joka toimii pohjana Sentinelille kuten huomataan kuvassa 13.



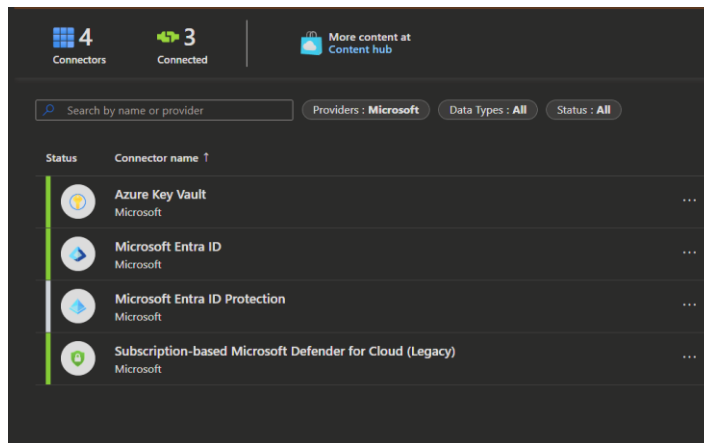
KUVA 13. Lokianalytiikka -työtilan luonti.

Kun lokianalytiikka-työtila oli luotu, sen päälle voitiin perustaa Sentinel-työtila, kuten alla olevasta kuvasta huomataan.



KUVA 14. Sentinel -työtilan luonti.

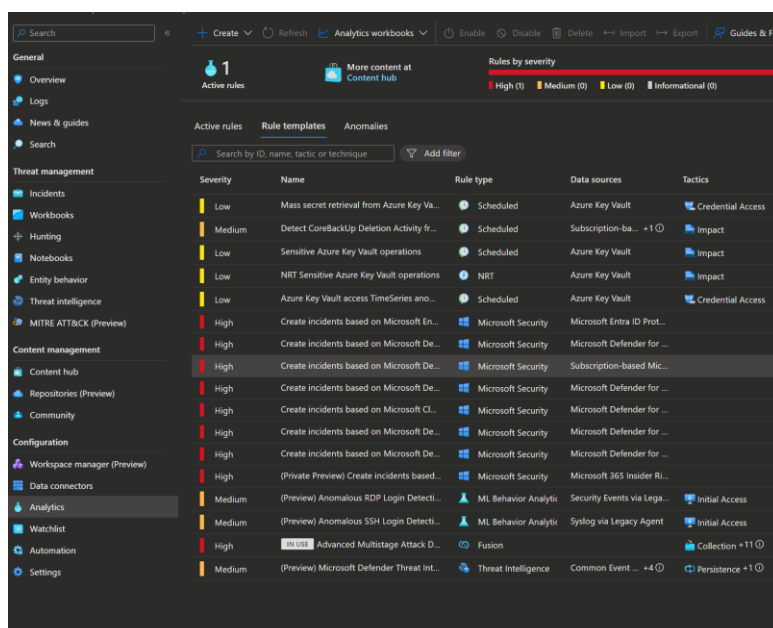
Seuraavassa vaiheessa lähdettiin konfiguroimaan Sentineliä ja liittämään se osaksi suurempaa valvontakokonaisuutta. Tässä tutkimuksessa ei ollut kauheasti vaihtoehtoja konfiguroinnin osalta, koska ympäristö rajoittuu pilviresursseihin. Konfiguraatio toteutettiin osan **5.1** määritysten mukaisesti. Alla olevassa kuvassa on käytetyt datanjohtimet.



KUVA 15. Datanjohtimet

Jokainen datanohdin tuo valmiita sääntöjä, jotka voi ottaa suoraan tai pienillä muutoksilla käyttöön. Kuvassa 16 näkyy erilaisia valmiita sääntöjä.

Analytiikkasäännöt löytyvät 'Analytics' -välilehdeeltä. Täällä luotiin määritysten mukaiset säännöt testiympäristölle. Sääntöjä voidaan myös luoda itse, mutta se vaatii hyvää KQL -tuntemusta.



KUVA 16. Analytiikkasäännöt.

Kuvassa 17 luotiin analytiikkasääntö, joka kääntää Defender for Cloud:n tuottamat hälytykset tietoturvatapahtumiksi. Tämä ei vaadi minkäänlaista KQL -logiikkaa, sillä se hakee datanjohtimen avulla Defender -palvelusta tulleet hälytykset.

Dashboard > Microsoft Sentinel | Analytics >

Analytics rule wizard - Create a new Microsoft Security rule

Create incidents based on Microsoft Defender for Cloud

General Automated response Review + create

Create an analytics rule that creates incidents based on alerts generated in another Microsoft security service.

Analytics rule details

Name *

Create incidents based on Microsoft Defender for Cloud

Description

Create incidents based on all alerts generated in Microsoft Defender for Cloud

Status

☒ Enabled

Analytics rule logic

Microsoft security service *

Microsoft Defender for Cloud

Filter by severity

☐ Any

☒ Custom

Severity *

4 selected

Include specific alerts

Only create incidents from alerts that contain the following text in the alert name

Exclude specific alerts

Only create incidents from alerts that do not contain the following text in the alert name

Next : Automated response >

KUVA 17. Analytiikkasäännön luonti.

Seuraavaksi luotiin yksi automaattiosäätö, joka nimittää tapahtumille omistajan Kalle Kinnari. Tämän tarkoitus oli testata havainnollistaa automaation perustoiminta. Säännön laukaisijana toimii se, että Sentineliin luodaan tapahtuma Defender for Cloud hälytyksen perusteella. Kuva 18 näyttää automaattiosäännön luontiprosessin analytiikkasääntöä konfiguroitaessa.

Create new automation rule

Automation rule name *

Assignee automation

Trigger

When incident is created

Conditions

If

Incident provider Equals All

AND

Analytic rule name Contains Current rule

+ Add

Actions

Assign owner

Kalle Kinnari
kalle.kinnari@mdrsecurity.onmicrosoft.com

+ Add action

Rule expiration

Indefinite Time

Order

1

KUVA 18. Automaatio analytiikkasäännölle.

Kuvassa 19 on kaikki säännöt, mitä Sentineliin konfiguroitiin. Säännöt toimivat perusajatuksella siten, että ne suorittavat KQL-kyselyitä dataan, jota saadaan datanjohtimien avulla. Sitten niille luodaan logiikka minkä pohjalta ne laukaisevat hälytyksen.

4 Active rules

More content at Content hub

Rules by severity: High (2), Medium (3), Low (0), Informational (0)

Active rules | Rule templates | Anomalies

Search by ID, name, tactic or technique

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Medium	Failed login attempts to Azur...	Scd	Disabled	Credential ...	T1110		Microsoft Entra...	4/20/2024, 7:54...
Medium	Brute force attack against Azu...	Scd	Enabled	Credential ...	T1110		Microsoft Entra...	4/20/2024, 11:3...
Medium	Sensitive Azure Key Vault ope...	Scd	Enabled	Impact	T1485		Azure Key Vault	4/20/2024, 11:2...
High	Create incidents based on Mi...	Mi	Enabled				Gallery Content	4/19/2024, 7:45...
High	Advanced Multistage Attack ...	Fu	Enabled	Col...	+11		Gallery Content	4/19/2024, 7:06...

KUVA 19. Käytettävät analytiikkasäännöt.

Kuvassa 20 on säännön 'Brute force attack against Azure Portal' -logiikka. Tämä ei tietenkään ole koko logiikka, sillä se on todella pitkä. Kuten kuvasta huomataan, kynnys epäonnistuneille kirjautumiselle on viisi kymmenen minuutin todentamis-ikkunan aikana.

```
// Set threshold value for deviation
let threshold = 5;
// Set the time range for the query
let timeRange = 30m;
// Set the authentication window duration
let authenticationWindow = 10m;
// Define a reusable function 'aadFunc' that takes a table name as input
let aadFunc = (tableName: string) {
    // Query the specified table
    table(tableName)
    // Filter data within the last 24 hours
    | where TimeGenerated > ago(1d)
    // Filter records related to "Azure Portal" applications
    | where AppDisplayName has "Azure Portal"
    // Extract and transform some fields
    | extend
```

KUVA 20. Väsyttämishyökkäyksen -logiikka.

4.2 Todentaminen

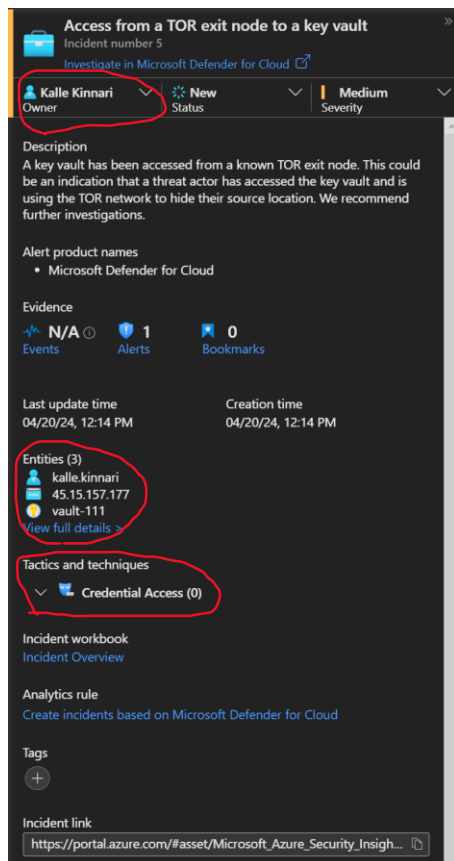
Tässä osassa varmistettiin, että kaikki komponentit ympäristössä toimivat odotetulla tavalla. Luotiin tästä testausmatriisi, joka täydennettiin testituloksien mukaan. Tapahtumat ja hälytykset käytiin myös läpi, joita testauksesta aiheutuu.

Resurssi	Komponentti	Testaustapa	Sentinel näkyvyys
Vault-ont-1	Defender for Cloud	Käsittely tor-verkossa	Näkyy
Vault-111	Defender for Cloud	Käsittely tor-verkossa	Näkyy
	Sentinel	Holvin poisto	Näkyy
Ont-test-vm1	Defender for Cloud	Ajetaan powershell-komento	Näkyy
ontstorage	Defender for Cloud	Käsittely tor-verkossa	Näkyy
		Testiviiruksen lataus	Näkyy
Entra ID	Sentinel	Useampi epäonnistunut kirjautuminen, josta seuraa onnistunut kirjautuminen	Näkyy

TAULUKKO 6. Validoinnin tulokset.

4.2.1 Avainholvi

Key Vault resurssien testaus suoritettiin siten, että ladattiin TOR -selain tietokoneelle. Avainholvin URL kopioidaan ja liitetään TOR -selaimen hakukenttään. Uudelleentunnistautumisen jälkeen, päästiin käsiksi avainholvi -resurssiin. Käytiin katsomassa holvin salaisuus sekä avain, jonka jälkeen kirjauduttiin ulos portaalista. Saadaan kuvan 21 mukainen tapahtuma Sentineliin:




KUVA 21. Avainholvin -validointi.


Tapahtuman tiedoista saadaan selville muun muassa mitkä entiteetit tapahtumaan liittyivät. Kuvassa 22 näkyy käyttäjä Kalle Kinnari, Tor:n poistumissolmu ja resurssi vault-111. Säännön automaatio toimi myös, sillä Kalle Kinnari on nyt tapahtuman omistaja. Käytettiin ip-osoite abuseipdb -palvelussa, jolloin saadaan ip-osoitteen tiedot:

45.15.157.177 was found in our database!

This IP was reported **701** times. Confidence of Abuse is **100%**. ?

100%

 This address is a Tor exit node. Neither the owner nor the provider are directly behind the offending action.

ISP	Rost LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	tor.node9.shadowbrokers.eu
Domain Name	colomna.net
Country	 France
City	Paris, Ile-de-France

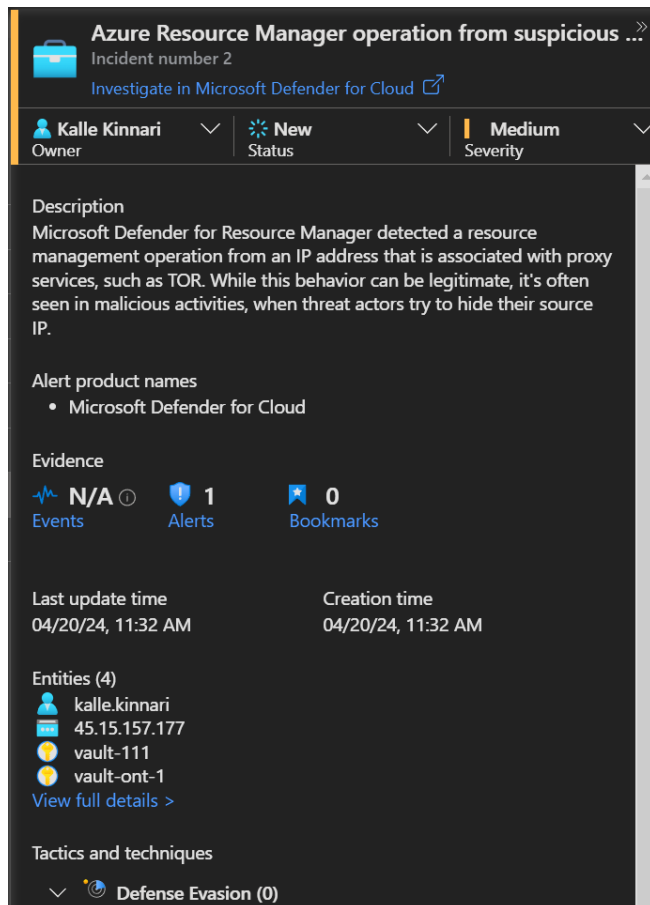
IP info including ISP, Usage Type, and Location provided by [IP2Location](#). Updated monthly.

[REPORT 45.15.157.177](#) [WHOIS 45.15.157.177](#)

KUVA 22. Abuseipdb:n tiedot IP-osoitteesta.

Analytiikka sekä Defender saavat hyvin tietoa irti tästä. Asiantuntijan on helppo aloittaa tutkinta, kun kolme keskeistä tietoa nähdään alku-analyysistä. Kuten huomataan, että Sentinel ilmoittaa myös hyökkäyksen taktiikan tai tekniikan. Tässä tapauksessa se on Credential access.

Lisäksi Defender laukaisi hälytyksen samaisesta aiheesta, mutta kohdisti sen koko toiminnalle. Kuvauksessa sanotaan, että vaikka toiminta voi olla oikeutettua, silti hälytys laukaistaan, koska hyökkääjät voivat käyttää TOR - verkkoa salatakseen alkuperäisen osoitteensa. Eli vaikka avainholvin sisältöä ei olisi luettu hyökkäyksen aikana, hälytys olisi tullut joka tapauksessa ja SOC-tiimi olisi tietoinen toiminnasta.

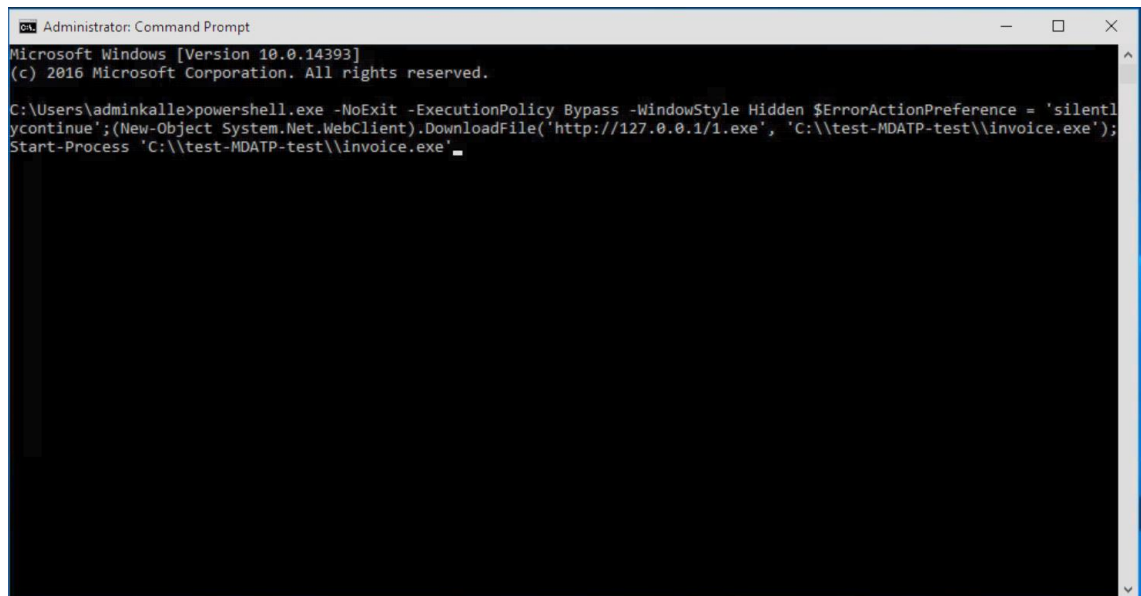


KUVA 23. Toinen avainholvi -hälytys.

4.2.2 Virtuaalikone

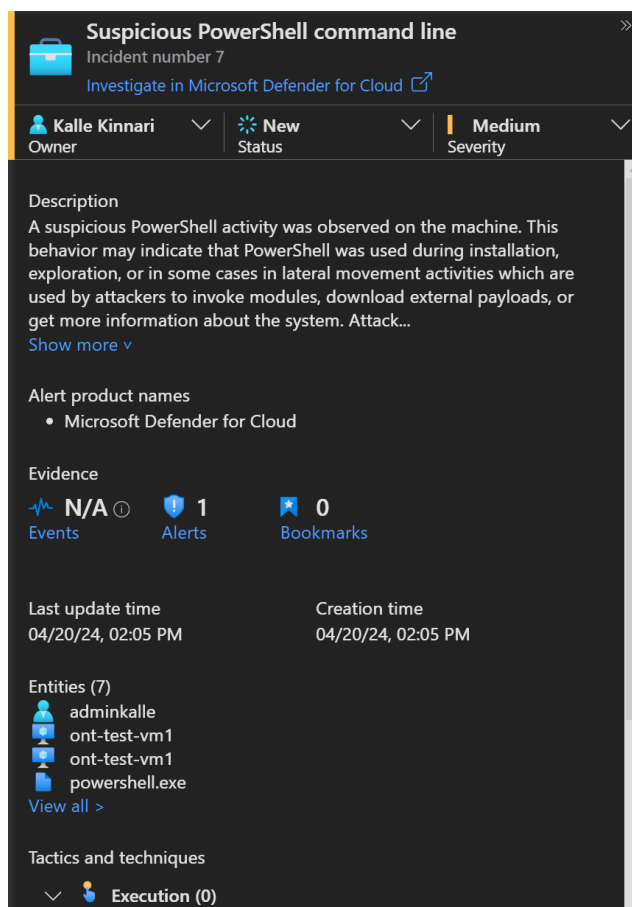
Virtuaalikoneen hyökkäyksen simuloinnin toteuttaminen oli hieman yksinkertaisempi. Se vaati sen, että kirjaudutaan luoduilla pääkäyttäjätunnuksilla virtuaalikoneelle samalla tavalla kuin resurssien testauksessa.

Seuraavaksi avataan komentokehote cmd, jossa ajetaan kuvan 24 mukainen komento, tarkoituksena tuottaa hälytys:



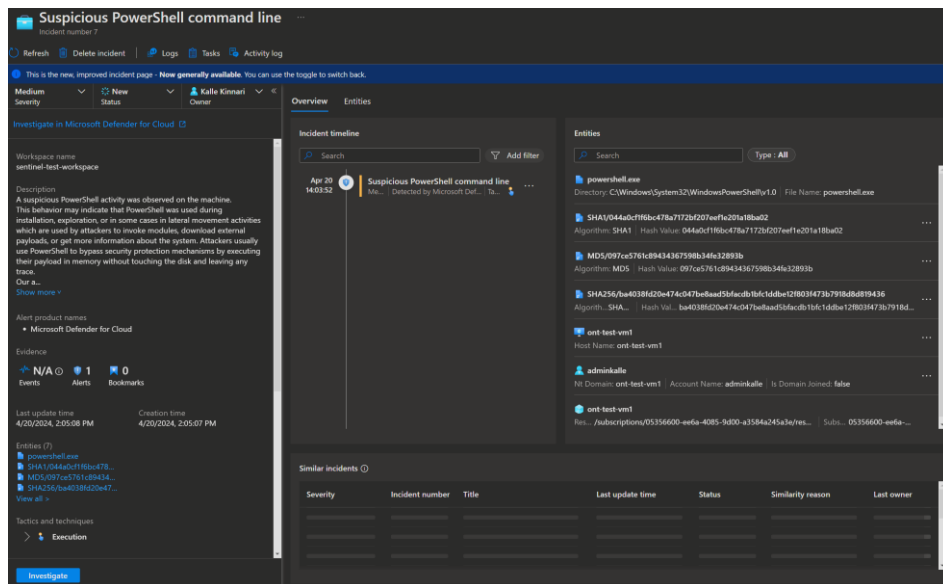
KUVA 24. Powershell -komento virtuaalikoneella.

Alla olevasta kuvasta huomataan, että testaus onnistui, sillä Sentineliin luotiin tapahtuma hälytyksestä.



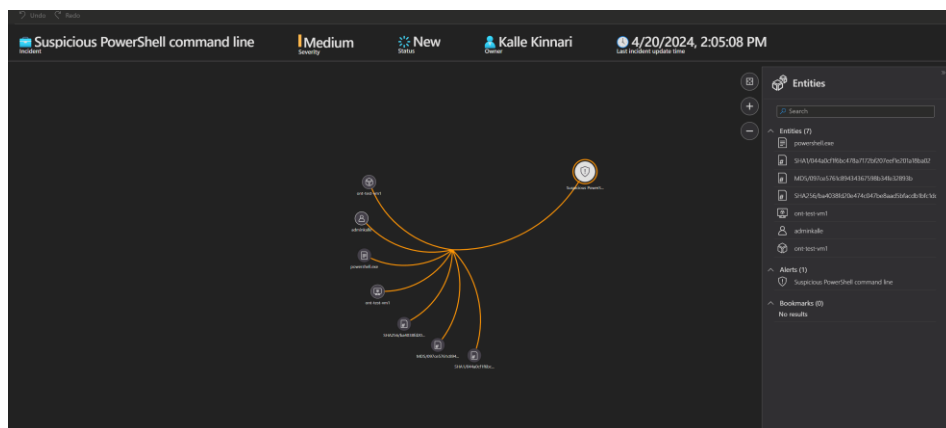
KUVA 25. Virtuaalikoneen hyökkäyksen simulointi.

Kuvasta 26 nähdään, että sama pätee kuin avainholvi -testissä, eli Defender kerää alkutietoja hyvin. Asiantuntija tietää heti, mistä koneesta on kyse, millä käyttäjällä sekä mikä työkalu liittyy tapahtumaan. Asiantuntija voi myös tutkia tapahtumaa tarkemmin painamalla 'View full details' tapahtuman alaosasta. Tässä ikkunassa asiantuntija näkee tarkemmat tiedot entiteeteistä, tapahtuman aikajanan sekä kuvauksen.



KUVA 26. Tapahtuman tutkiminen.

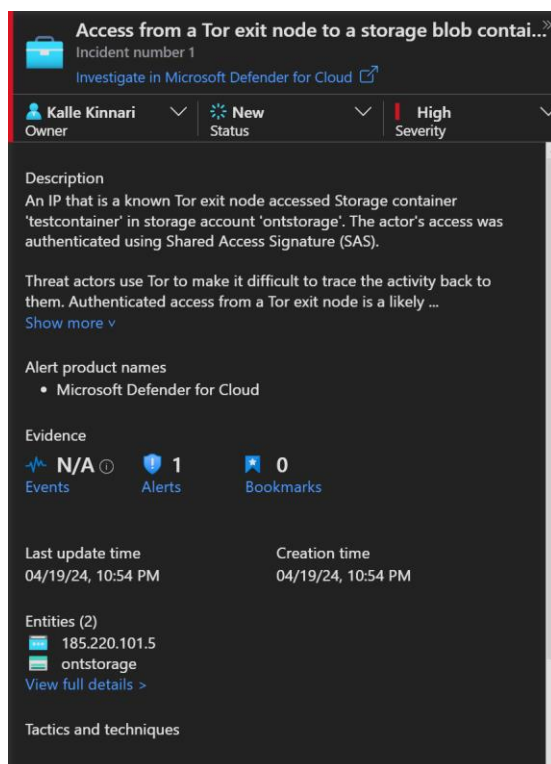
Asiantuntijat voivat tarkastella tapahtumaa myös visuaalisesti. Investigate -toiminnolla pääsee tutkimaan tapahtumaa eri tavalla kuten kuvasta 27 nähdään.



KUVA 27. Tapahtuman visualisointi.

4.2.3 Varasto

Varasti -resurssi testattiin hyvin samalla tavalla kuin avainholvi. Varasto -resurssin varastokontista löytyi ympäristön rakentamisen aikana lisätty kuvatiedosto. Kuvatiedostolle luotiin SAS-merkki sekä URI, joka liitetään TOR-selaimen hakukenttään. Näin ollen kuva näkyi vapaasti selaimessa ja Defender hälyttää pääsystä varastokappaleeseen alla olevan kuvan mukaan.




KUVA 28. Varastohyökkäyksen todentaminen.


Kuten aikaisemmissa tapahtumissa, tapahtumatiedoista saadaan jo erittäin hyvää ja arvokasta tietoa jatkotutkimusten kannalta. Syötetään IP-osoite abuseipd -palveluun ja saadaan kuvan 29 mukaiset tiedot.

185.220.101.5 was found in our database!

This IP was reported **3,739** times. Confidence of Abuse is **100%**: ?

100%

 This address is a Tor exit node. Neither the owner nor the provider are directly behind the offending action.

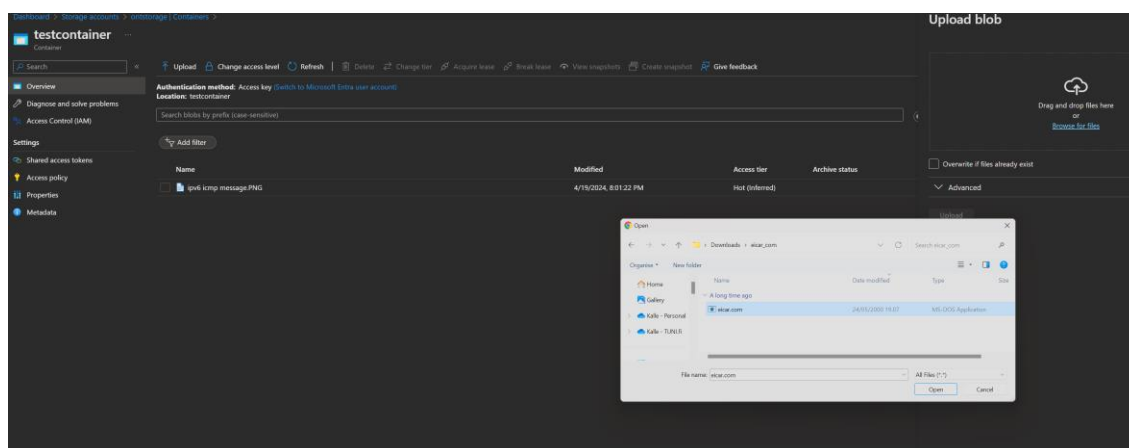
ISP	Zwiebelfreunde E.V.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	berlin01.tor-exit.artikel10.org
Domain Name	zwiebelfreunde.de
Country	 Netherlands
City	Amsterdam, Noord-Holland

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

[REPORT 185.220.101.5](#) [WHOIS 185.220.101.5](#)

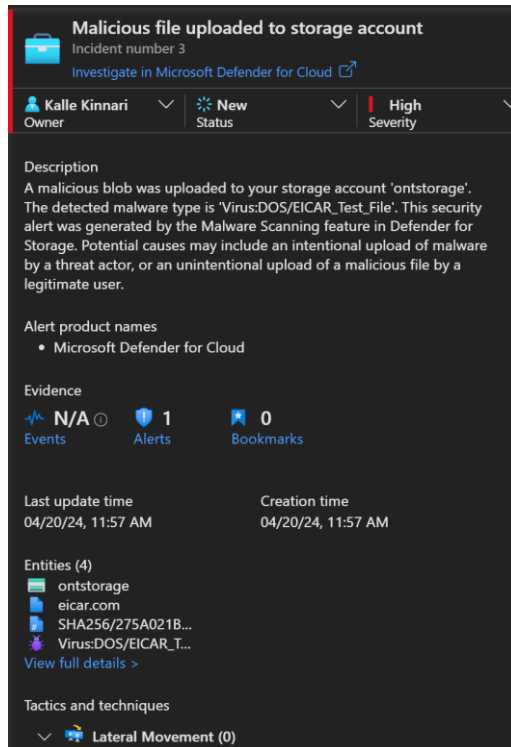
KUVA 29. IP-osoite Abuseipdb:ssä.

Varstolle suoritettiin lisäksi vielä toinen testi. Siinä testattiin haittaohjelmien skannaus-toimintoa. Varastokontin sisälle ladattiin EICAR -testiviirus kuvan 30 mukaisesti.



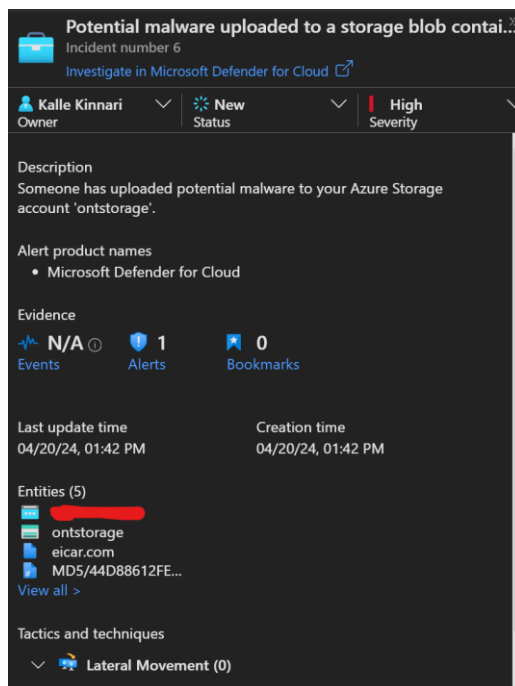
KUVA 30. Haittatiedoston lataus varastokontiin.

Kuvassa 31 on Sentineliin tulleen tapahtuman tiedot, missä testiviirus ladattiin varastokontiin.



KUVA 31. Haittatiedosto varastokontissa.


Vajaa tunti myöhemmin saatiin toinen hälytys, hieman eri entiteeteillä:



KUVA 32. Toinen ilmoitus haittaohjelmasta.

Saadaan samat tiedot kuin aikaisemmin, paitsi tässä tapauksessa käyttäjää ei saatu kiinni aivan täysin, mutta lataajan IP-osoite jäi lokeihin. Käytettiin se jälleen kerran abuseipdb -palvelussa kuvan 33 mukaan:

[REDACTED] was not found in our database

ISP	Elisa Oyj
Usage Type	Unknown
Hostname(s)	[REDACTED] .elisa-laajakaista.fi
Domain Name	elisa.fi
Country	 Finland
City	Helsinki, Uusimaa

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

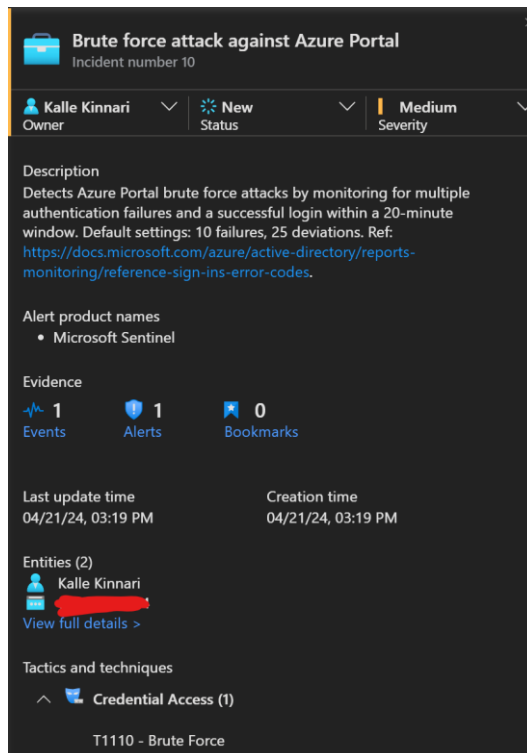
REPORT **[REDACTED]** **WHOIS** **[REDACTED]**

KUVA 33. Lataajan IP-osoite Abuseipd:ssä.

Lataajaa ei välttämättä saada tästä vastuuseen, mutta kaikki tiedot, joita tutkimuksissa saadaan, ovat tärkeitä. Tiedot voidaan luovuttaa toisessa skenaariossa esimerkiksi poliisille. Mutta vaikka testauksessa saadaan tieto, että haitallinen tiedosto on ladattu konttiin, mikään komponentti ei kuitenkaan sitä poista automaattisesti, toisin kuin työasemilla, joissa tiedosto joutuu karanteeniin.

4.2.4 Sentinel analytiikka

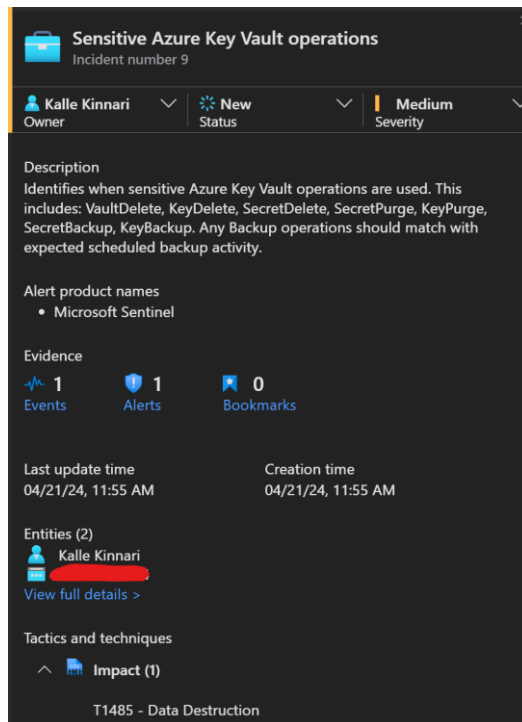
Testattiin myös, miten muut Sentineliin konfiguroidut analytiikkasäännöt toimivat. Testaus suoritettiin ensin väsyttämishyökkäyksen analytiikkalle. Simuloitiin tapahtumaa kriajutumalla epäonnistuneesti kuusi kertaa, jonka jälkeen kirjautumalla onnistuneesti. Kuvan 34 mukaisesti tästä muodostui tapahtuma Sentineliin.



KUVA 34. Brute force hyökkäys.

Hyökkääjän epäonnistuneet sekä onnistunut kirjautuminen nosti analytiikan myötä hälytyksen. Asiantuntija voi seuraavaksi tehdä tarvittavat toimenpiteet uhan poistamiseksi, kuten lukitsemalla käyttäjän ulos sekä vaihtamalla tämän salasanan.

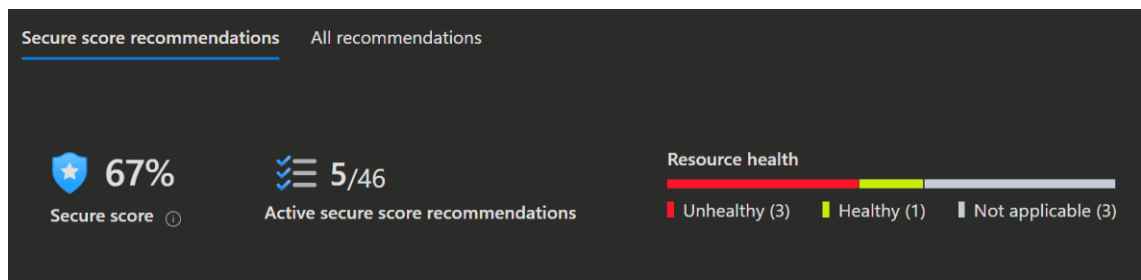
Seuraavaksi testattiin toista sääntöä, joka ilmoittaa epätavallisista tilanteista kaikissa avainholvi resursseissa. Tätä simuloitiin poistamalla toinen avainholvi siten, että se on vielä palautettavissa tietyn ajan. Kuvassa 35 huomataan, että Sentinelin analytiikka huomasi tämän tapahtuman, mutta tiedot ovat hieman puutteellisia. Tapahtumasta ei huomaa, mikä holvi on kyseessä tai mitä komentoa on käytetty.



KUVA 35. Key Vault poisto-operaatio.

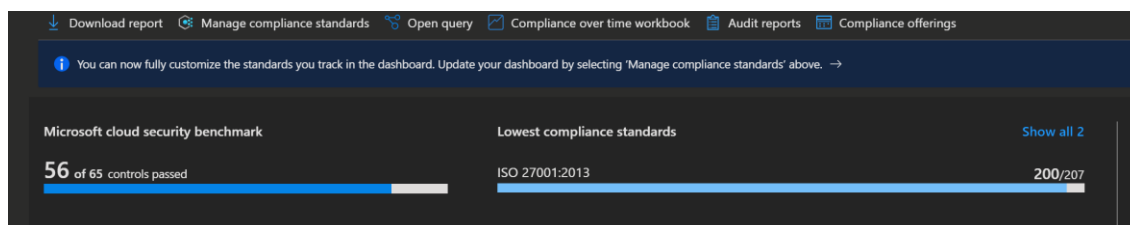
4.2.5 CSPM ja säännöt

CSPM pisteyttää nykyisen turvallisuustason Azure-ympäristössä. Se mittaa muun muassa sitä, onko MFA päällä, kuinka monta pääkäyttäjää tilauksella on ja miten turvallisia resurssien konfiguraatiot ovat. CSPM tarjoaa myös keinoja pisteytyksen parantamiseen. Tästä on helppo lähteä parantamaan turvallisuutta, sillä Azure tarjoaa joissakin tapauksissa automaattisia korjaustoimenpiteitä resursseille. Kuvassa 36 testiympäristön pisteytykseksi on annettu 67%.



KUVA 36. Secure score Defender for Cloud.

Kuvassa 37 näkyy kuinka hyvin ympäristö on konfiguroitu ISO -sääntöjen mukaan. Kuvassa näkyy myös Microsoftin pilviturvallisuuden omat vaatimukset. Suurin osa tämän ilmoittamista puutteista liittyy virtuaalipalvelimen kryptaukseen sekä datankeruuseen resursseista.



KUVA 37. Microsoft ja ISO säännöt.

4.3 Yhteenveto

Defender for Cloud tarjoaa erittäin hyvän pilviturvallisuuden analyysin CSPM:n avulla, vaikka se maksaakin jokaista resurssia kohden. Se on kuitenkin rahan arvoista, koska sen avulla turvallisuustasoa voidaan nostaa todella korkealle. Tottakai Defender for Cloud:n resurssiosuojaus on erittäin hyvä ja se havaitsee uhkia jo mahdollisessa alkuvaiheessa. Välillä hälytykset tapahtumista tulevat hieman hitaasti. Toki tämä on näkökulmasta kiinni, mutta tuote jonka tarkoitus on hälyttää resursseihin kohdistuvista hyökkäyksistä tai vakoilusta, ei saisi olla liian hidas.

Defender for Cloud voi toimia myös itsenäisesti, irrallisena Sentinelistä. Sentinel tuo paljon lisää tietoturvan valvontaan, mutta vaatii hieman syvempää osaamista datankeruun takia, lokikyselyiden sekä metsästämissä takia. Defender for Cloud tarjoaa kaikille hälytyksille keinoja, joilla hälytys voidaan hoitaa ja jatkossa ehkäistä. Lisäksi kaikki resurssit ja defender toimivat samassa ympäristössä sekä palvelu on helppo ottaa käyttöön, kirjaimellisesti vain muutaman napin painalluksella.

Sentinelin käyttö on suositeltavaa, kun käytössä on enemmän resursseja eri lohkoista, esimerkiksi Windows -työasemia, joilla on Defender for Endpoint

käytössä. Koko Microsoftin tuoteperheen voi tuoda Sentineliin ja keskittää kaiken sinne ja samalla luoda analytiikkasääntöjä.

Sentinel on myös erittäin integroitavissa. Tähän voi datanjohtimien avulla yhdistää vaikka WithSecure:n EDR ominaisuuden, jolloin hälytykset keskittyvät Sentineliin, silloin ei ole tarvetta käyttää useampaa eri portaalia uhkien hallinnointiin. Integraation voi myös viedä toiseen suuntaan, eli Sentinelistä voidaan tuoda hälytykset organisaation tikettijärjestelmään, esimerkiksi Jira Atlassianiin.

Kaikin puolin Sentinel ja Defender for Cloud ovat eteviä, ketteriä ja monipuolisia työkaluja nykyisessä tietotekniikan ja tietoturvan maailmassa. Niillä on laajat käyttömahdollisuudet sekä ne voi hallita helposti suurempiakin kokonaisuuksia. Lisäksi hinnoittelu on myös suhteellisen järkevä, esim. 15\$/kk per palvelin. Tällä hinnalla saa lokianalytiikka -agentin sekä huippuluokan virustorjunnan. Sentinelin hintnoittelu pohjautuu siihen, kuinka paljon dataa tulee työtilaan kuukaudessa. Jos organisaatio on suuri tai resursseja on valtava määrä, hinta voi nousta hyvinkin äkkiä korkealle. Tämä tosin riippuu hyvin pitkälti siitä, millaisia analytiikkasääntöjä on käytössä ja miten ne on konfiguroitu.

Kuten suuressa osassa muitakin tapauksia, Sentinelille ei ole olemassa parasta tapaa harjoittaa valvontaa. Kaikki riippuu täysin siitä, millainen budjetti on ja minkälaista valvontaa halutaan suorittaa. Nämä asiat tulee määritellä projektin alussa, ennen kuin lähtee ympäristöjä rakentamaan. Tämän pohjalta voi tutkia vaihtoehtoja ja tapoja, miten saavutetaan omalle organisaatiolle täydellinen järjestelmä.

5 JOHTOPÄÄTÖKSET JA TULEVAISUUDEN NÄKYMÄT

Tässä kappaleessa käsitellään kaikki, mitä työssä on tutkittu. Kiteytetään lyhyesti nykyaikaiset tietoturvaratkaisut ja prosessit. Kerätään yhteen johtopäätökset sekä mietitään, miltä tulevaisuus näyttää tietoturvan osalta.

5.1 Yhteenveto

Opinnäytetyössä käytiin läpi nykyaikaisia tietoturvauhkia organisaatioissa sekä miten Microsoftin työkaluilla voidaan vastata näihin, etenkin pilviympäristöissä. Lopuksi suoritettiin myös Case-tutkimus, missä testattiin Defender for Cloud -palvelun sekä Microsoft Sentinelin käyttöönottoa pilviympäristössä. Testaukseen kuului myös resurssien suojauksen todentaminen simuloimalla hyökkäyksiä näihin resursseihin.

Case-tutkimuksessa perustettiin yritystili, johon liitettiin Azure pilviympäristö, jossa on muutamia resursseja, mitä normaalissa yrityksessä voisi olla. Resurssit tuotiin Defender-suojauksen piiriin ja keskitettiin hälytykset ja analytiikka Azuren komponenteista, kuten Entra ID:stä suoraan Microsoft Sentineliin.

5.2 Johtopäätökset

Tietoturvatyökalut suojaavat yrityksen resursseja ja sen työntekijöiden dataa. Työkalujen lisäksi organisaatioilla tulee olla selkeä riskienhallintastrategia sekä jatkuva kehitys tietoturva-asioissa, koska maailma muuttuu jatkuvasti ympärillämme. Organisaatioilla tulee siis olla selkeät rajat, miten tietoturvallista työtä tehdään ja miten puolestaan organisaatio suojaa resurssejansa.

Case-tutkimus antoi arvokasta tietoa, miten puolustusjärjestelmät otetaan käyttöön Microsoftin ympäristössä ja siihen liittyvissä resursseissa. Lisäksi

suojauksen ja hälytysten testaus antoi kattavan kuvan, kuinka Defender toimii, sekä miten analytiikkaa kannattaa konfiguroida Sentinelissä, jotta saadaan ns. enemmän irti koko palvelusta, eli käytetään muitakin ominaisuuksia, kuin keskitettyä valvontaa. Toki testaamatta jäi uhkien metsästyksen, lokianalytiikan käyttö laajemmassa mittakaavassa ja automatisointi tehtävätasolla. Nämä kuitenkin ovat tärkeitä osia ja Sentinelin kantavia voimavaroja, joten jokaisen tulisi osata käyttää näitä työkalunaan taistelussa uhkia ja hyökkäyksiä vastaan. Microsoft tarjoaa tähän myös hyviä ohjeita omilla sivuillaan, sekä oleellisen sertifiointi-kurssin SC-200 Microsoft Learn:ssa.

5.3 Tulevaisuuden näkymät ja haasteet

Tekoälyn nopea kehittyminen ja integroituminen yritysmailmaan ja teknologiaan tuo paljon hyviä asioita, kuten virhemäärien pienentämistä, automaatiota ja skaalautuvuutta. Yksi suurimpia haasteita tietoturvalle on kyberhyökkäysten luonteen kehittyminen. Tekoälyn avulla rikolliset voivat jatkuvasti kehittää uusia ja hienovaraisia tekniikoita tietomurtoihin (J. Artiff, 24 2018). Vaarana on, että aloittelijatasen koodari voi luoda haittaohjelmia ja automatisoida niitä, joka lisää hyökkäyspinta-alaa entisestään.

Tekoälyn avulla voidaan myös esiintyä toisena henkilönä tai entiteettinä, esim. syvävääreennös on teknologia, jota käytetään myös sodassa tarkoituksena esiintyä tietyssä henkilönä huijaten ja demoralisoiden toisen osapuolen joukkoja. Tekoäly tuo mukanaan riippuvuutta kyseiseen teknologiaan ja perinteinen ihmistason ongelmanratkaisukyky voi heikentyä entisestään.

Vaikka uudet teknologiat ja keksinnöt tuovatkin mukanaan paljon haasteita ja riskejä, niille keksitään vastapaino. Kuten viruksille keksittiin virustorjunta, MDM mobiililaitteiden hallintaan ja palomuuuri verkon suojaksi. Tulevaisuudessa tekoälyn avulla todennäköisesti torjutaan myös sen itse tuomat ongelmat joissain määrin. Myös tietoturva-asiantuntijoiden määrä kasvaa vuosi vuodelta, joka toimii hyvänä vastapainona kehitykselle.

Tietoturvan kehittymistä voidaan myös parantaa suuremmalla skaalalla, kuten NIS2:lla Euroopan Unionissa. NIS2 on EU-direktiivi, jonka tarkoituksena on parantaa turvallisuutta tietoverkoissa ja tietoliikennejärjestelmissä. EU vaatii, että kriittisen infrastruktuurin ja palveluiden operaattorit toteuttavat tarvittavia turvatoimia ja raportoimaan tapahtumista viranomaisille. (Nis2directive. N.d.)

Tulevaisuudessa Microsoftin työkalut tulevat olemaan suuressa roolissa. Varsinkin, kun organisaatiot siirtävät resurssejaan pilveen entistä enemmän, myös kysyntä Azurelle ja sitä kautta tietoturvatyökaluille nousee myös. Microsoft on noin Kolmen biljoonan dollarin yritys, joka johtaa tietoturvamarkkinoita sen integraation sekä laajan ja toimivan tuoteperheen ansiosta.

LÄHTEET

Mundzir, The Evolution of Cybersecurity: A Journey Through the History of Computer Security, Medium-verkkosivu. Viitattu 7.4.2024

<https://mundzirmm.medium.com/the-evolution-of-cybersecurity-a-journey-through-the-history-of-computer-security-4ec9c2d74bb6>

Kaspersky, A Brief History of Computer Viruses & What the Future Holds, Verkkosivu. Viitattu 7.4.2024

<https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>

Fortinet. N.d. What is Cryptography? Verkkosivu. Viitattu 13.4.2024

<https://www.fortinet.com/resources/cyberglossary/what-is-cryptography>

Debbie Walkowski. 2019. What is the CIA Triad?. Artikkel. Viitattu 13.4.2024

<https://www.f5.com/labs/learning-center/what-is-the-cia-triad>

Cisco. N.d. What Is Endpoint Detection and Response (EDR)?. Viitattu 14.4.2024.

<https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html>

Avantech. N.d. Microsoft Defender for Endpoint Plan 2. Myytävä tuote. Viitattu 14.04.2024

[https://www.advantech.com/en/products/19bc1aad-9be7-4664-9964-2f3893c6695f/microsoft-defender-for-endpoint-\(plan2\)/mod_798e3b09-9b24-46c3-aa6e-d6193d1254b7](https://www.advantech.com/en/products/19bc1aad-9be7-4664-9964-2f3893c6695f/microsoft-defender-for-endpoint-(plan2)/mod_798e3b09-9b24-46c3-aa6e-d6193d1254b7)

Alan La Pietra. 2022. A Light Overview of Microsoft Security Products. Blog-kirjoitus. Viitattu 14.04.2024

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/a-light-overview-of-microsoft-security-products/ba-p/3256279>

Siosulli, denisebmsft, diannegali, Blake-Madden, Dansimp, sheshachary, msbemba, chrisda, v-smandalika, JoeDavies-MSFT, BrunoDal, alekyaj ja v-mathavale. 2023. Overview of Microsoft Defender for Endpoint Plan 1. Microsoft -oppimateriaali. Viitattu 14.04.2024.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide>

Imperva. N.d. Information Security: The Ultimate Guide. Viitattu 13.04.2024.

<https://www.imperva.com/learn/data-security/information-security-infosec/>

Techtarget. 2024. Top 10 types of information security threats for IT-teams. Kirjoitus. Viitattu 7.4.2024

<https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams>

Kanuprnya Ghauhan. 2023. Microsoft Defender for Cloud [AZ-500]: Everything You Should Know. Blogi-kirjoitus. Viitattu 19.4.2024.

<https://k21academy.com/microsoft-azure/az-500/microsoft-defender-for-cloud/>

Ajay Kumar. 2023. Microsoft Defender Cloud Security Posture Management (CSPM) — A Pillar for Multi Cloud Security Management. Artikkele. Viitattu 21.4.2024

<https://intouchajay.medium.com/microsoft-defender-cloud-security-posture-management-cspm-a-pillar-for-multi-cloud-security-f0f7809247>

Mustafa Toroman. 2023. What is Microsoft Sentinel and How Does It Protect Cloud and On-Premises Resources?. Blogi-kirjoitus. Viitattu 21.4.2024

<https://petri.com/what-is-microsoft-sentinel/>

Arif Ali Mughal. 2018. Artificial Intelligence in Information Security. Artikkele. Viitattu 6.5.2024.

<https://journals.sagepub.com/index.php/jamm/article/view/51/49>

Rapid7. Nd. Information Security Risk Management. Artikkele. Viitattu 6.5.2024.

<https://www.rapid7.com/fundamentals/information-security-risk-management/>

NIS2DIRECTIVE. N.d. What is the NIS2 Directive? Artikkele. Viitattu 6.5.2024.

<https://nis2directive.eu/what-is-nis2/>

Dcurwin, Naveenommi-MSFT, Mattbriggs, V-alje, Taojunshen, Elazark, Rayne-wiselman, Msmbaldwin, Bmansheim, Kadrita, Bcs2022, Yehkardos, Laurabren, Memildin. 2023. What is Microsoft Defender for Cloud? Microsoft -oppimateriaali. Viitattu 21.5.2024.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

BlueVoyant. Nd. Microsoft Defender for Endpoint: Architecture, Features, and Plans. Blogi-kirjoitus. Viitattu 21.5.2024.

<https://www.bluevoyant.com/knowledge-center/microsoft-defender-for-endpoint-architecture-features-and-plans>

Seren Tamayo. 2023. The Ultimate Guide To Microsoft Defender For Endpoint Protection. Blogi-kirjoitus. Viitattu 21.5.2024.

https://www.datalinknetworks.net/dln_blog/the-ultimate-guide-to-microsoft-defender-for-endpoint-protection

Xcitium. N.d. Microsoft XDR – Explore Features of 365 Defender. Verkkosivu. Viitattu 26.5.2024.

<https://www.xcitium.com/microsoft-xdr/>

Gitbit. N.d. What's Microsoft 365 Defender? Kurssimateriaali. Viitattu 26.5.2024.

<https://www.gitbit.org/course/ms-500/learn/Whats-Microsoft-365-Defender-z8EMM9Eu>

Microsoft. N.d. What is SIEM? Verkkosivu. Viitattu 27.5.2024.

<https://www.microsoft.com/en-us/security/business/security-101/what-is-siem>

Rapid7. N.d Web Application Vulnerabilities. Verkkosivu. Viitattu 27.5.2024.
<https://www.rapid7.com/fundamentals/web-application-vulnerabilities/>

Kaspersky. N.d. Mikä sivustojen välinen komentosarjahyökkäys on? Verkkosivu. Viitattu 27.5.2024.
<https://www.kaspersky.fi/resource-center/definitions/what-is-a-cross-site-scripting-attack>