jamk

Azure-pilvialustan kyvykkyyksien hyödyntäminen tietomurtotutkinnassa

Elmeri Söderholm

Opinnäytetyö, AMK
Syyskuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Söderholm, Elmeri

Azure-pilvialustan kyvykkyyksien hyödyntäminen tietomurtotutkinnassa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Syyskuu 2024, 50 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Pilvipalvelujen yleistyminen on luonut organisaatioille uusia mahdollisuuksia hallita ja ylläpitää resursse-jaan. Pilven skaalautuvuus, saavutettavuus, kustannustehokkuus sekä joustava tiedonsiirto mahdollistavat erilaisten teknologiaratkaisujen ja palveluiden luonnin.

Opinnäytetyön tavoitteena oli luoda ohjeistus Azure-pilvipalvelussa olevalle virtuaaliselle tietomurtotut-kinta-alustan luomiselle, jota työn toimeksiantajana toimivan Deloitte Oy:n kybertiimi voi käyttää referens-sinä sisäisen tietomurtotutkinta-alustan luontiin. Referenssitoteutusta voidaan myös käyttää mallina esitel-lessä ratkaisua asiakastyössä.

Opinnäytetyön tuloksena luotiin ohjeistus tietomurotutkinta-alustan luomisesta Azure-pilvipalvelussa, hyö-dyntäen pilvipalveluntarjoajien, instituuttien sekä parhaaksi todettujen lähteiden dokumentaatioita. Työssä määriteltiin myös sopiva virtuaalikone tietomurtotutkintaan pilvessä vertailemalla eri kannettavien tietoko-neiden kyvykkyyksiä suorittaa eri tietomurtotutkintaan liittyviä prosesseja.

Työn johtopäätöksenä todettiin, että käyttötarkoituksen mukaan, oikean virtuaalikoneen valitseminen vai-kuttaa tietomurtotutkinta-alustan hintaan sekä tehokkuuteen. Tämän lisäksi todettiin, että suhteellisen yk-sinkertaisella ympäristöllä pystytään toteuttamaan tietomurtotutkintaa pilviympäristössä.

Avainsanat (asiasanat)

digitaalinen forensiikka, pilvipalvelut, tietoturva, tietomurto, tietomurtotutkinta, Azure, häiriönhallinta

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Söderholm, Elmeri

Utilization of Azure’s cloud capabilities in digital forensics

Jyväskylä: JAMK University of Applied Sciences, September 2024, 50 pages

Degree Programme in Information and Communications Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Cloud services becoming increasingly more common, new possibilities have developed to manage and administer organization’s resources. The scalability, availability, cost-efficiency, and flexible data transfer of cloud allow for different technologies and services to be created.

The objective of the thesis was to create an instruction on how to create a virtual platform for investigating data breaches in Azure’s cloud solution which Deloitte Oy’s cyber team can use as a reference for creating an internal platform for forensic investigation. The reference can also be used as a model for presenting the solution in client work.

The results of the thesis was an instruction on how to build a platform to Azure’s cloud solution for investigating data breaches by utilizing cloud providers’ and institutions’ documentations among other credible sources. The research also defined a suitable virtual machine for forensic investigation in the cloud by comparing capabilities of different laptops running processes related to forensic investigation.

The conclusion of the thesis was that depending on the purpose of use, choosing the suitable virtual machine influences the cost and performance of the platform, and performing forensic investigation in the cloud can be done with relatively simple cloud environment.

Keywords/tags (subjects)

digital forensics, cloud services, information security, data breach, Azure, incident response

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Taulukot

1 Johdanto

1.1 Työn tausta

Teknologian kasvavan luonteen ja monimutkaistumisen takia, tietoturva on noussut merkittäväksi osaksi organisaatioiden liiketoimintaa. Yhä useampi organisaatio on alkanut käyttämään hyödyksi virtuaalisia ympäristöjä, jotka helpottavat ja turvaavat liiketoiminnan kannalta tärkeitä resursseja käyttäen hyödyksi pilvipalvelujen tarjoamia komponentteja. Tällä hetkellä eletään aikaa, jossa organisaatiot ovat alkaneet siirtymään perinteisestä toimipaikalla sijaitsevista konesaliratkaisuista pilvessä sijaitseviin ympäristöihin. Pilvipalvelut tarjoavat monenlaisia etuja organisaatioille ja modernit työkalut sekä palvelut suojaavat liiketoimintaa kattavasti, kustannustehokkaasti ja paremmalla varmuudella.

Kun organisaatiot alkavat siirtymään eri pilviratkaisuihin, liiketoiminnan turvaamisen kannalta on tärkeää taata kattava suoja organisaation toiminnan varmistamiseksi. Tähän liittyy erilaisten käyttäjien ja roolien sekä turvallisuuspolitiikkojen määrittäminen, lokienhallinnan, monitorointijärjestelmien ja häiriönhallintapalvelujen käyttöönottaminen.

Pilviympäristöjen yleistyminen organisaatioissa on kasvattanut myös vihamielisten tahojen aktiivisuutta pilvessä. Yhä useampi tietomurto tapahtuu jollain tavalla pilvessä, jolloin organisaation on tärkeää tietää minkälaisia hyötyjä ja haittoja, sekä minkälaisia kyvykkyyksiä pilvipalvelut tarjoavat tietomurtotutkinnalle.

1.2 Toimeksiantaja

Tämän tutkimuksen toimeksiantajana toimii Deloitte Oy. Deloitte Oy on asiantuntijaorganisaatio, joka tarjoaa neuvonantoa laajasti eri liikkeenjohdon alueilla. Deloitten palveluita ovat tilintarkastus- ja neuvontapalvelut, konsultointi, riskienhallinta- ja kyberpalvelut, yritysjärjestelyt ja vero- sekä lakipalvelut. (Deloitte n.d.)

1.3 Tavoitteet ja rajaukset

Tutkimuksen tavoitteena on tutkia Azure-pilvipalvelun kyvykkyyksiä toteuttaa tietomurtotutkintaa ja luoda ohjeistus toimeksiantajan kybertiimille hallitun tietomurtotutkinta-alustan luomisesta

Microsoftin Azure-pilviympäristössä. Opinnäytetyö on rajattu Azure-pilviympäristöön, koska se on yleisesti käytössä suomalaisissa organisaatioissa sekä se on tutkimuksen tekijälle tutuin. Valintaan vaikutti myös se, että viimeisen kahden vuoden aikana Azure on ollut AWS:ään ja Google Cloudiin verrattuna yleisin palveluntarjoaja työn toimeksiantajalle tulleisiin turvallisuusmonitorointiin liittyviin tarjouspyyntöihin. Työssä perehdytään myös toiseen yleiseen pilvipalveluun, Amazonin AWS:ään sillä tästä voidaan tulevaisuudessa tehdä myös ohjeistus tietomurtotutkintaa varten.

1.4 Tutkimusmenetelmä

Tutkimustyö on aloitettu keräämällä oleellista tietoa tietomurtojen tutkimisesta perinteisillä menetelmillä sekä pilviympäristössä. Tietoa tutkimukseen on kerätty sähköisistä artikkeleista, kirjoista, tieteellisistä julkaisuista sekä pilvipalveluntarjoajien dokumentaatioista. Tietoa on valittu ajankohtaisista ja luotettavista lähteistä ja tämän tiedon pohjalta on toteutettu referenssitoteutus tietomurtotutkinta-alustan luomisesta Azuressa.

1.5 Tutkimuskysymykset

1. **Miten organisaation pitää olla valmistautunut, että tietomurtojen tutkiminen olisi mahdollisimman helppoa Azure-pilviympäristössä?**

Tämä kysymys arvioi Azuren nykyisiä parhaita menetelmiä ja kuinka näitä voidaan hyödyntää mahdollisimman hyvin, jotta organisaation tietomurtotutkinnan kyvykkyydet olisivat mahdollisimman korkealla pilviympäristössä. Kysymyksessä siis arvioidaan Azure-ympäristön kyvykkyyksien hyödyntämistä tietomurron tutkimisessa.

2. **Miten organisaatio pystyy luomaan modernin hallitun pilvialustan tietomurtojen tutkimiselle?**

Tämän kysymyksen avulla pyritään luomaan selkeä ohjeistus tietomurtotutkinta-alustan luomisesta organisaation Azure-pilviympäristöön.

3. **Mitä moderneja työkaluja pilviympäristöt tarjoavat tietomurtotutkintaan?**

Tällä kysymyksellä pyritään tuomaan esille tämänhetkiset relevantit työkalut, jota organisaatio tarvitsee hallitun tietomurtotutkinta-alustan käytössä Azure-pilviympäristössä.

2 Johdanto pilvipalveluihin

2.1 Pilvipalvelut

Pilvipalvelut ovat palveluntarjoajien toimittamia ja ylläpitämiä palveluja, joita organisaatiot ja yksityishenkilöt voivat käyttää internetin yli. Palvelut ovat suunniteltu tarjoamaan edullisen ja helpon pääsyn sovelluksiin ja resursseihin ilman omaa sisäistä laitteistoa tai infrastruktuuria hyödyntämällä virtualisointiteknologiaa. Palveluntarjoajat ylläpitävät palveluja omilla palvelimillaan, jolloin käyttäjillä ei ole tarvetta hankkia omaa infrastruktuuria. (What is a cloud service n.d.)

Kun organisaatio tai yksityishenkilö on suunnittelemassa pilvipalveluiden käyttöönottoa, täytyy heidän päättää myös minkälaisen ympäristön he tarvitsevat. Ympäristöjä on tyypillisesti kolme erilaista: Julkinen pilvi, yksityinen pilvi ja hybridipilvi. Julkisessa pilvessä palvelut ovat saatavilla useille asiakkaille. Tässä ympäristössä käyttäjät voivat jakaa resursseja laajasti ja organisaatio voi tarjota parempia kyvykkyyksiä työntekijöilleen. Yksityisessä pilvessä palveluntarjoaja ei tarjoa palveluitaan saatavaksi käyttäjille tai tilaajille. Sovellukset ja tiedot on tällaisessa ympäristössä saatavilla ainoastaan organisaation omassa infrastruktuurissa ja ulkopuolisilla käyttäjillä ei ole pääsyä näihin. Tämänkaltaista ympäristöä käyttävät useimmiten organisaatiot, jotka hyödyntävät kehittyneempiä turvallisuusprotokollia. Nämä organisaatiot liittyvät useimmiten valtion eri osastoihin, terveydenhuoltoon tai finanssialaan. Hybridipilvi on julkisen pilven ja yksityisen pilven yhdistelmän. Tällaista ympäristöä käyttävät organisaatiot, jotka tarvitsevat yksityisen ympäristön sensitiivisen tiedon säilyttämiseen, mutta samalla haluavat tarjota käyttäjilleen pääsyn sovelluksiin ja resursseihin julkisessa pilvessä. (What is a cloud service n.d.)

2.1.1 Palvelumallit

Pilvipalveluista on tarjolla erilaisia palvelumalleja, jotka on suunniteltu tarjoamaan sopivan, kustannustehokkaan ratkaisun organisaation julkiseen pilviympäristöön. Yleisellä tasolla palvelumalleista on olemassa kolme eri perustyyppiä. Näistä palvelumalleista käytetään termejä Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) ja Software-as-a-Service (SaaS). Jokainen palvelumalli antaa erilaisen palveluratkaisun, joista organisaatio voi valita sopivimman omien tarpeidensa mukaan. (What are IaaS, PaaS and SaaS n.d.)

Infrastructure-as-a-Service (IaaS) on palvelumalli, jossa käyttäjällä on pääsy pilviympäristön infrastruktuuriin. Käyttäjä voi hallita, konfiguroida ja käyttää palvelimia, tallennuskapasiteetteja ja verkkoresursseja samalla tavalla, kuin paikallisesti sijaitsevia laitteistoja. Erona perinteiseen ratkaisuun on se, että pilvipalveluntarjoaja ylläpitää resursseja omissa konesaleissaan, eikä käyttäjällä ole pääsyä näihin. IaaS-ratkaisu tarjoaa käyttäjälle enemmän joustavuutta resurssien rakentamiseen ja resurssien määrää voidaan laskea tai nostaa tilanteen mukaan. Käyttäjän ei tarvitse kustantaa omaa konesalia, ja kapasiteetin skaalautuvuus on aina sopiva kaikkiin tilanteisiin. (What are IaaS, PaaS and SaaS n.d.)

Monet IaaS-toimittajat tarjoavat myös Platform-as-a-Service (PaaS) -palveluita. Tässä mallissa käyttäjälle tarjotaan tietokanta, käyttöjärjestelmä ja ohjelmointikieli, joita hyödynnetään pilvipohjaisten sovelluksien kehittämiseen, suorittamisen ja ylläpitoon. Selkeä hyöty tässä mallissa on nopea, kustannustehokas tapa käyttää eri sovelluksia ja järjestelmiä. Omaa alustaa ei tarvitse rakentaa ja päivityksiä, korjauksia ja muita ylläpidon tehtäviä ei tarvitse tehdä itse. (What are IaaS, PaaS and SaaS n.d.)

Näiden kahden palvelumallin lisäksi pilvipalvelut tarjoavat Software as a Service (SaaS)-ratkaisua. Tässä mallissa ohjelma on heti valmiina käyttöön eikä käyttäjältä vaadita minkäänlaista ylläpitoa. Käyttäjän tarvitsee vain luoda tunnus, selvittää mahdolliset kustannukset ja aloittaa applikaation käyttö. Palveluntarjoaja hoitaa kaiken järjestelmän hallinnan, kuten turvallisuuden, pääsynhallinnan, palvelimien ylläpidon, sekä päivityksienhallinnan. (What are IaaS, PaaS and SaaS n.d.)

2.1.2 Virtualisointi

Pilviympäristöissä resurssit pyörivät virtualisoinnin avulla. Virtualisointi on teknologia, jota käytetään laitteistojen, kuten palvelimien, tallennustilojen, verkkojen ja muiden fyysisten laitteistojen virtuaalisten versioiden luomiseen. Virtualisointi tuo laitteistojen hallitsemiseen paljon joustavuutta ja se poistaa fyysisten palvelimien rajoitukset, kuten sähkön käytön ja konesalitilat. Virtuaalilaitteiden infrastruktuuria voidaan hallita ja ylläpitää kuin applikaatiota internetissä. (What is Virtualization n.d.)

Virtualisointi tuo käyttäjälle monia eri hyötyjä, kuten useiden palvelimien hallinnointimahdollisuudet yhdellä tietokonejärjestelmällä palvelinpoolin avulla. Näin organisaatio tarvitsee vähemmän

fyysisiä palvelimia konesalissaan, säästämällä tilaa ja rahaa. Toinen hyöty on automatisoitu hallinnointi. Koska fyysiset tietokoneet ovat virtuaalisia, näitä voidaan hallinnoida käyttämällä erilaisia työkaluja, kuten luomalla määriteltyjä virtuaalikoneiden pohjia. Pohjien avulla virtuaalikoneita voidaan monistaa yhtenäisesti ilman mahdollisuutta virheisiin. Kolmas hyöty virtualisoinnissa on nopeampi palautuminen. Normaalisti jos katastrofi tapahtuu fyysisessä ympäristössä, voi palautuminen viedä tunteja tai jopa päiviä. Virtualisoidussa ympäristössä palautuminen voi tapahtua minuuteissa parantamalla liiketoiminnan jatkuvuutta ja organisaation resilienssiä. (What is Virtualization n.d.)

3 Pilvipalveluntarjoajat

Pilvipalveluja tarjoavia yrityksiä on saatavilla kattava määrä. Niin kutsutut ”Big Three” -pilvipalveluntarjoajat Microsoft, Amazon ja Google vievät 66 prosenttia pilvipalvelujen koko markkinaosuudesta maailmanlaajuisesti (Cloud Spending Growth Rate Slows But Q4 Still Up By $10 Billion from 2021; Microsoft Gains Market Share 2023).

Vaikka nämä kolme pilvipalveluntarjoajaa vievät suuren osan markkinaosuudesta, on olemassa muitakin merkittäviä pilvipalvelujentarjoajia, kuten esimeriksi kiinalainen Alibaba Cloud (Alibaba Cloud n.d).

Seuraavassa kappaleessa kerron yleisesti Azuren ja AWS:n tarjoamista peruspalveluista, joiden avulla organisaatio voi aloittaa ympäristönsä transformaatioprosessin pilveen. Kappaleessa käydään läpi pilvipalvelujen Cloud Adoption -viitekehykset, jotka ovat kriittisiä organisaation pilviympäristön jalkauttamisessa, pilvipalvelujen identiteettien ja laskutuksien hallintaa sekä minkälainen hierarkia eri pilvipalveluilla on tilauksissa, lisensseissä, tileissä ja tenanteissa.

3.1 Microsoft Azure

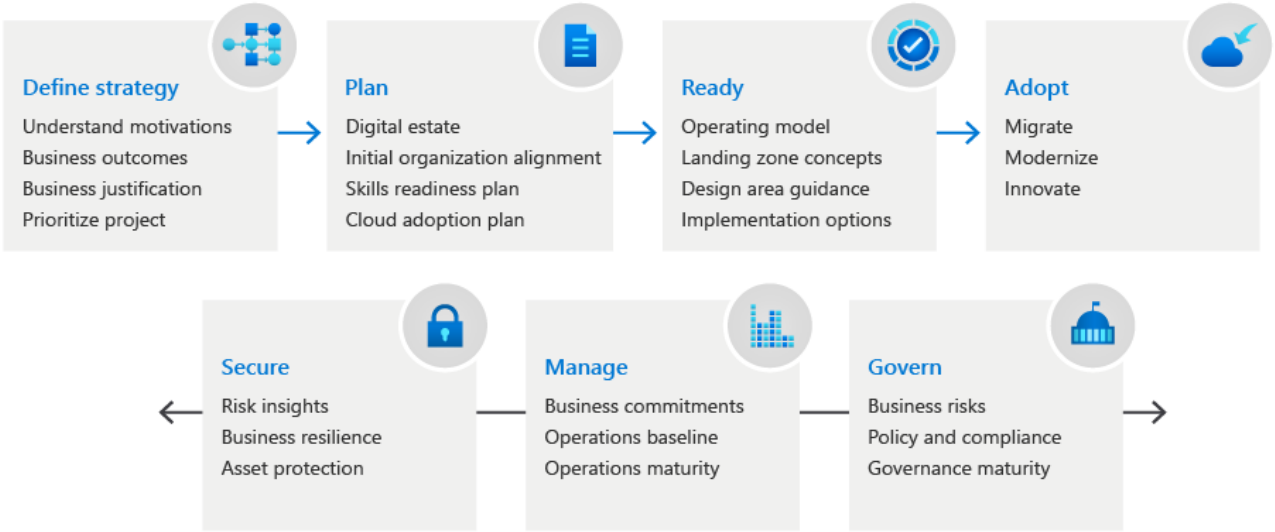
Microsoftin luoma pilvipalvelu Azure on julkinen pilvialusta, joka tarjoaa laajan valikoiman pilvipohjaisia palveluja IaaS, PaaS ja SaaS -kyvykkyyksillä. Azure sisältää valtavan määrän palvelimia ja tietoverkkojärjestelmiä, jotka suorittavat paljon erilaisia applikaatioita. Näiden applikaatioiden tehtävänä on määrittää ja operoida virtualisoituja laitteistoja ja ohjelmia Azuren palvelimilla. (How does Azure work 2023.)

3.1.1 Microsoft Entra ID

Vanhalta nimeltään Azure Active Directory, Microsoftin Entra ID on identiteetin- ja pääsynhallinnan palvelu, jonka avulla määritellään käyttäjien roolit ja oikeudet, jotta organisaatiossa olevat pääsevät käyttämään ympäristön sisäverkossa sekä ulkopuolella olevia resursseja. Näitä resursseja voivat olla esimerkiksi Azure Portal tai Microsoft 365. (What is Microsoft Entra ID 2024.)

3.1.2 Microsoft Cloud Adoption Framework

Microsoft tarjoaa Cloud Adoption -viitekehystä, joka hyödyntää parhaita saatavilla olevia käytäntöjä liiketoiminnalle ja teknologioille tärkeiden strategioiden luomiseksi ja toteuttamiseksi. Viitekehys tarjoaa dokumentaatiota, työvälineitä ja muita ohjeistuksia, jotta organisaation liiketoiminta saadaan tehokkaasti implementoitua pilveen. Viitekehys sisältää lukuisia metodologioita, jotka ovat kaikki osa laajaa pilviratkaisuimplementoinnin elinkaarta (ks. kuvio 1). (What is the Microsoft Cloud Adoption Framework for Azure 2023.)



Kuvio 1. Azuren Cloud adoption elinkaari (What is the Microsoft Cloud Adoption Framework for Azure 2023)

Pilvipohjaisen infrastruktuurin luominen muuttaa tapaa, jolla organisaatio toimii resurssien ja palveluiden luomisessa, käytössä ja turvaamisessa. Perinteisessä infrastruktuurimallissa, organisaatio omistaa, ylläpitää ja turvaa täysin oman teknologiansa. Pilviratkaisussa, resursseja toimitetaan ja käytetään ainoastaan organisaation tarpeiden mukaan. Azure ja muut pilvipalvelut tarjoavat

suurta joustavuutta erilaisten pilviteknologiainfrastruktuurien suunnittelussa. Tästä huolimatta, on organisaation tärkeä ymmärtää omat tarpeensa ja metodologiat, jotta onnistunut pilvipohjainen infrastruktuuri saadaan luotua. Pilveen adoptointi alkaa ennen kuin sopivaa pilvipalveluntarjoajaa on edes valittu. Viitekehyksen on tarkoitus auttaa päätöksentekijöitä keskittymään liiketoiminnan, teknologian sekä kulttuurin strategiseen muutokseen, jotta pilveen adoptointi saadaan toteutettua onnistuneesti. (What is the Microsoft Cloud Adoption Framework for Azure 2023.)

3.1.3 Tilaukset, lisenssit, tilit ja tenantit

Microsoft Azurella on tarjolla johdonmukaiselle identiteettien ja laskutuksien hallinnalle hierarkia organisaation tilauksille, lisensseille ja käyttäjätileille. Ylimpänä hierarkiaa on itse organisaatio. Organisaatio edustaa kokonaisuutta, jossa liiketoiminta pyörii pilvessä. Organisaation tunnistaa tyypillisesti Domain Name Systemistä (DNS), suomeksi nimipalvelujärjestelmä, esimerkiksi jamk.fi. Organisaation alle sisältyy tilaukset. (Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

Tilaus on sopimus Microsoftin kanssa, jossa määritellään yhden tai useamman Microsoftin pilvialustan käyttöönotto. Tilauksessa määritellään veloitus tapahtuvan joko per käyttäjä lisenssillä tai pilviresurssin käytön mukaisesti. Microsoftin SaaS-palvelut, jotka toimivat Microsoft 365 ja Microsoft Dynamics 365 alla, käyttävät per käyttäjä lisenssiä. Pilviresurssien käytön mukaista veloitustapaa käyttävät IaaS ja PaaS -palvelut. Näiden lisäksi Azure tarjoaa koekäyttöä, jonka käyttö umpeutuu tietyn ajan tai käytön jälkeen. Koekäytön voi muuttaa maksettavaksi tilaukseksi. Organisaatio voi ottaa käyttöön useita tilauksia samaan aikaan. (Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

Lisenssit toimivat eri tavalla palvelumallista riippuen. SaaS-palvelumallissa lisenssi sallii yksittäisen käyttäjän käyttää pilvitarjonnan palveluja. Lisenssejä luovuttaa tilauksen ylläpitäjä ja siitä peritään tilaukseen sisältyen kiinteä kuukausimaksu. PaaS-palvelumallissa lisenssit ovat osa palvelun hinnoittelua. Näiden lisäksi virtuaalikoneet, jotka ovat IaaS-pohjaisia, lisälisenssien hankkiminen applikaatioiden tai ohjelmien käyttämiseen voi vaatia virtuaalikonepohjia. Joillain virtuaalikonepohjilla on lisenssiversioita asennetuista ohjelmista ja esimerkiksi kokeiluversioihin tarvitaan lisälisenssejä applikaatioista, jotta näitä voidaan käyttää kokeilun jälkeen. Nämä veloitukset ovat erillisiä Azuren tilauksesta. (Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

Microsoftin pilvipalveluissa käyttäjätilit sijaitsevat Microsoft Entra tenantissa, johon sisältyy myös käyttäjäryhmät. Jos organisaatiolla on olemassa oleva Active Directory Domain Services, voidaan Microsoft Entra synkronoida tämän kanssa Microsoft Entra Connectin avulla. (Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

Tenant on Microsoft Entra ID:seen kuuluva instanssi, joka sisältää käyttäjätilejä ja ryhmiä. Saas-palveluiden tenant on tietyssä alueellisessa sijainnissa, jossa palveluiden palvelimet ovat. Paas-palveluiden tenant, jotka sisältävät virtuaalikoneet ja joita isännöi IaaS, voidaan sijoittaa itse valitsemaan sijaintiin. Tämä sijainti voi olla missä konesalissa tahansa maailmanlaajuisesti. Microsoft 365 ja Dynamics 365 kokeiluversiossa ja maksullisessa versiossa Microsoftin tenant on ilmainen, mutta tähän tenanttiin ei kuulu Azuren palveluita. (Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

Tenanttiin voi kuulua useita tilauksia, jolloin se toimii identiteetin tarjoajana organisaatiolle. Tämä voidaan synkronoida organisaation paikallisella AD DS:llä, jolloin tenant toimii Identity-as-a-Service (IDaaS) palveluna.

Microsoftin mukaan, hierarkia voidaan tiivistää näin:

- Organisaatiolla voi olla useita tilauksia
    - Tilaukseen voi kuulua useita lisenssejä
    - Lisenssejä voi määrittää yksittäisiin käyttäjätileihin
    - Käyttäjätilit sijaitsevat tenantissa, Entra ID:ssä

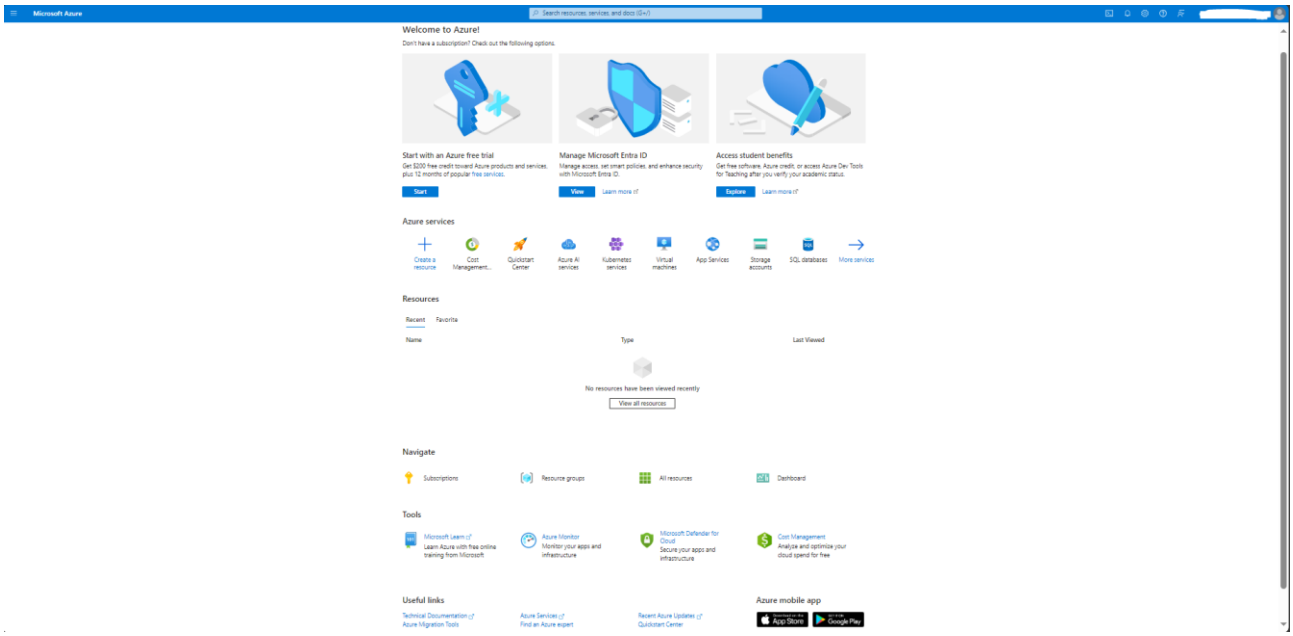
Microsoftin tarjoama esimerkki hierarkian eri tasojen suhteista:

- Organisaation voi tunnistaa julkisesta domain nimestä
    - Microsoftin 365 E3 tilaus, johon kuuluu käyttäjälisenssejä
        - Microsoftin 365 E5 tilaus, johon kuuluu käyttäjälisenssejä
        - Dynamics 365 tilaus, johon kuuluu käyttäjälisenssejä
        - Useita Azuren tilauksia
    - Yhteiseen Microsoft Entra tenanttiin sisältyvät organisaation käyttäjätilit

(Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings 2023.)

3.1.4 Azure Portal

Azure Portal on graafinen, selaimen välityksellä toimiva konsoli, jolla hallitaan käyttäjän Azure tilausta. Portaalin avulla voidaan luoda, hallita ja valvoa kaikkia Azuren pilvipalveluresursseja. Portal sijaitsee jokaisessa Azuren konesalissa, mikä tekee siitä kestävän yksittäisiä konesalivikoja vastaan sekä tukee saatavuutta lähellä olevien konesalien ansiosta. Kun käyttäjä kirjautuu ensimmäisen kerran Azure Portaliin, ensimmäinen näkymä on Azure Home. Azure Home tarjoaa näkyvyyden tilaukseesi kuuluviin resursseihin. Tarjolla on myös ilmaisia nettikursseja, dokumentaatiota, eri palveluita ja muita hyödyllisiä sivustoja, joihin tutustumalla pysyy ajan tasalla eri muutoksista ja lisäyksistä mitä organisaation olisi hyödyllistä tietää. Azure Homen lisäksi, voidaan oletussivuksi valita ohjauspaneelinäkymä. Ohjauspaneeli antaa käyttäjälle keskitetyn näkyvyyden tärkeimpiin resursseihin tilauksessasi. Ohjauspaneelia voidaan muokata omien mieltymyksien mukaan näyttämään resurssit, joita käyttäjä käyttää useimmiten, samaan näkymään. Ohjauspaneeleja voi luoda useampia ja niitä voidaan myös jakaa muille käyttäjille (ks. kuvio 2). (What is the Azure portal 2024.)



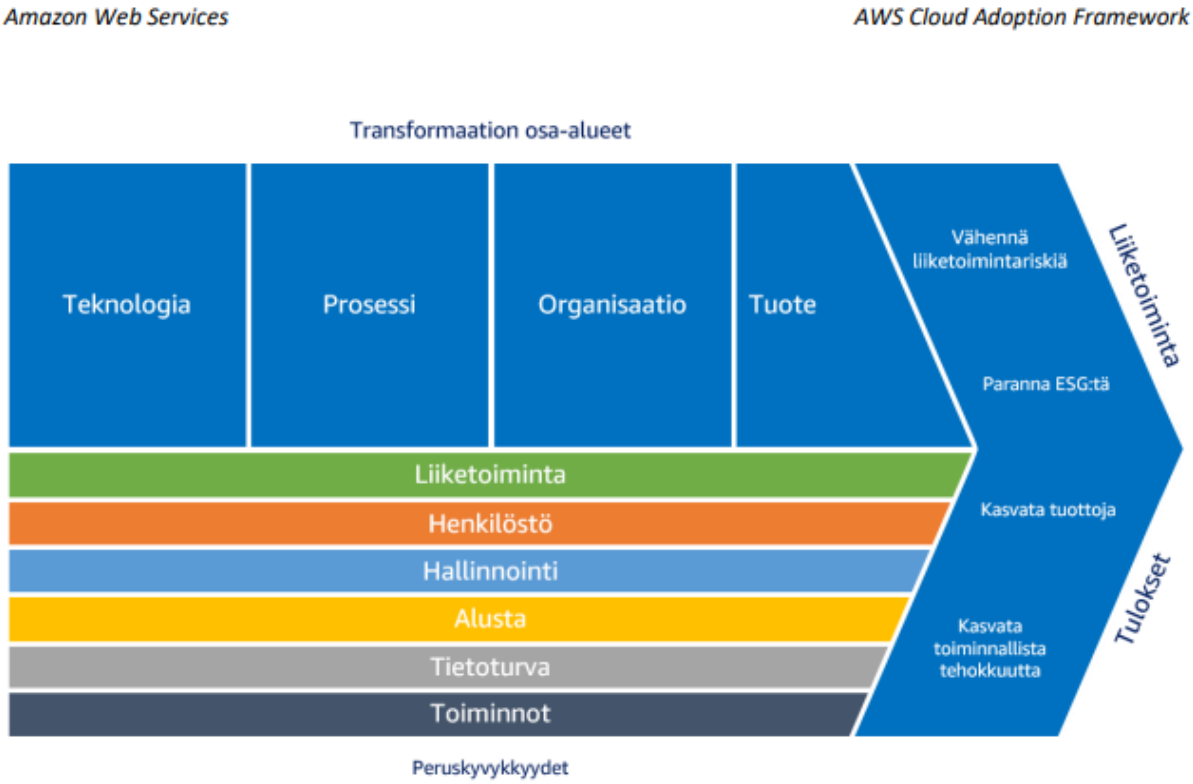
Kuvio 2. Azure Portalin Home-näkymä

3.2 Amazon Web Services (AWS)

Amazon Web Services tarjoaa yli 200 palvelua eri konesaleista ympäri maailmaa. Tämä tekee siitä maailman johtavan pilvipalvelun sisältäen laajemman valikoiman palveluja kuin mikään muu pilvipalveluntarjoaja. Palveluiden määrän lisäksi, AWS tarjoaa moninaisen valikoiman eri tarkoituksiin luotuja applikaatioita, jotta asiakas voi valita tarpeisiinsa nähden parhaan vaihtoehdon. (Cloud computing with AWS n.d.)

3.2.1 AWS Cloud Adoption Framework

AWS tarjoaa asiakkailleen Cloud Adoption -viitekehystä, joka auttaa organisaatiota hyödyntämään AWS:n eri palveluita. Viitekehys määrittelee organisaation keskeisimmät peruskyvykkyydet ja hyödyntää näitä onnistuneen pilvitransformaation toteuttamiseksi. Viitekehys jakaa peruskyvykkyydet kuuteen eri ryhmään: Liiketoiminta, henkilöstö, hallinnointi, alusta, tietoturva sekä toiminnot. Onnistunut pilvitransformaatio voidaan jakaa osa-alueisiin, jotka edustavat arvoketjua. Tähän arvoketjuun kuuluu teknologiatransformaatio, prosessitransformaatio, organisaatiotransformaatio ja tuotetransformaatio, joissa jokainen osa-alue mahdollistaa aina seuraavaan. Liiketoimintatuloksia, mitä näistä syntyy ovat suurempi liikevaihto, parempi operatiivinen tehokkuus, pienemmät liiketoimintaan liittyvät riskit sekä parempi ympäristöön, yhteiskuntavastuuseen ja hallinnointitapaan (ESG) liittyvä suorituskyky (ks. kuvio 3). (AWS Cloud Adoption Framework. Pilvipalvelupohjaisen digitalisaation kiihdyttäminen 2011.)



Kuvio 3. Pilvitransformaation arvoketju (AWS Cloud Adoption Framework. Pilvipalvelupohjaisen digitalisaation kiihdyttäminen, 2011)

3.2.2 AWS Organisations

AWS:n hierarkia koskien käyttäjienhallintaa eroaa Azuren hierarkiasta hieman. AWS Organisations on käyttäjienhallintapalvelu, joka tarjoaa useamman AWS käyttäjän hallinnan organisaation sisällä, joka luodaan ja hallitaan keskitetysti (What is AWS Organisations n.d).

Organisaatio AWS:n kontekstissa on entiteetti, joka luodaan, jotta käyttäjiä voidaan ylläpitää yhtenä kokonaisuutena. AWS:n organisaatiokonsolilla käyttäjiä voidaan seurata ja hallita yhtenäisessä näkymässä. Organisaatioon kuuluu yksi hallintaan tarkoitettu käyttäjä, jolla luodaan organisaatio ja tämän lisäksi voidaan luoda myös jäsenkäyttäjiä. Käyttäjiä voidaan organisoida hierarkkisesti, jossa juuri on korkeimpana ja tämän alapuolella on organizational unitit (OU). Näihin molempiin voidaan luoda käyttäjiä vapaasti. (AWS Organisations terminology and concepts n.d.)

3.2.3 AWS Management Console

AWS:n Management Console on palvelu, jolla hallitaan AWS:n resursseja. Konsoli on webbiapplikaatio, joka sisältää palvelukonsoleja AWS:n resursseista. Kun käyttäjä kirjautuu Management Consoleen ensimmäisen kerran, näkyviin tulee Console Home Page. Tämä näkymä sisältää jokaisen palvelun konsolit ja tarjoaa myös tietoa, jota käyttäjä voi hyödyntää oppiakseen AWS:n eri palvelujen käytöstä. Console Homea voi myös muokata omien mieltymyksien mukaan. (Getting Started with the AWS Management Console n.d.)

Console Homeen sisältyy päävalikkoja, joilla on erilaisia toimintoja. Nämä ovat Account Information, AWS Regions, AWS Service Selector, AWS Search ja AWS Cloudshell. Näiden lisäksi Homen ohjauspaneelissa on erilaisia widgettejä, jotka auttavat käyttäjää alkuun ja tarjoavat erilaista tietoa. AWS Health kerää tietoa tapahtumista, jotka voivat vahingoittaa AWS:n käyttäjiä tai infrastruktuuria. Cost and usage tarjoaa yleisnäkymän palveluista ja niiden hinnoittelusta. Favorites näyttää listan AWS palveluista, jotka käyttäjä on määritellyt suosikeiksi. Recently visited näyttää listan palveluista, missä käyttäjä on viimeksi käynyt. Trusted Advisor tarjoaa suosituksia AWS:n parhaista menetelmistä. (Getting Started with the AWS Management Console n.d.)

4 Tietomurrot ja niiden tutkinta

4.1 Tietomurto

Tietomurto on yleiskäsite sensitiivisen tiedon vuotamisesta ulkopuoliseen ympäristöön. Näin voi tapahtua vihamielisen hyökkäyksen seurauksena tai vahingossa, inhimillisen virheen takia. Tietojen jatkuva siirtyminen verkossa tekee tietomurroista suuren turvallisuusriskin ja mahdollistaa hyökkääjän kohdistamaan hyökkäykset keneen tahansa. Näitä voivat olla esimerkiksi liiketoiminnalta tärkeiden palvelimien sisältävät tiedot. (What is a data breach n.d.)

Tietomurtojen tapahtumiseen on olemassa useita tapoja ja Cloudflaren listauksen mukaisesti päätavat ovat nämä:

1. Hävinneet tai varastetut tunnukset – Yleisin tapa, jolla voidaan päästä käsiksi yksityiseen tietoon. Hyökkääjät käyttävät erilaisia tekniikoita, jotta he pääsisivät käsiksi tunnus- ja salasanatietoihin.

2. Hävinneet tai varastetut laitteet – Hävinnyt laite, esimerkiksi tietokone tai älypuhelin voi sisältää sensitiivistä tietoa ja päätyä vääriin käsiin.
3. Sosiaalinen manipulointi – Hyökkääjä käyttää psykologista manipulointia tietojen saamiseksi. Hyökkääjä voi esimerkiksi esittää olevansa joku muu, päästäkseen käsiksi sensitiiviseen tietoon.
4. Sisäiset uhat – Henkilö, jolla on pääsy suojattuun tietoon, vuotaa tiedon tarkoituksella usein omien etujen ajamiseksi. Esimerkiksi valtion työntekijä vuotaa tietoja vieraisiin maihin.
5. Haavoittuvuuksien hyödyntäminen – Organisaatioiden käyttämät sovellukset sisältävät haavoittuvuuksia, joita hyökkääjät käyttävät hyväkseen.
6. Haittaohjelmatartunnat – Monet haittaohjelmat varastavat tietoja ja valvovat käyttäjän toimia, kerätäkseen tietoja hyökkääjän omille palvelimilleen.
7. Fyysiset myyntipaikan hyökkäykset – Tämäntyyppiset hyökkäykset kohdistetaan pankkikorttitietoihin, joissa käytetään hyväksi pankkikorttien skannaukseen tarkoitettuja laitteita. Näitä voi olla esimerkiksi väärennetyt pankkiautomaatit tai hyökkääjän asentama skannauslaite oikeassa pankkiautomaatissa.
8. Tunnuksien uudelleenkäyttö – Tietomurron kautta vuodettujen tunnustietojen uudelleenkäyttö useissa eri alustoissa. Jos käyttäjä on käyttänyt samoja tunnuksia useissa eri palveluissa, voi hyökkääjä päästä käsiksi myös näihin.
9. Salauksien puute – Jos sivusto ei käytä tietojen salaamiseen SSL/TLS salausta, voi kuka tahansa monitoroida käyttäjän ja sivuston välistä liikennettä ja nähdä tiedot vapaasti.
10. Virheelliset konfiguroinnit – Jos sovellus tai sivusto on konfiguroitu väärin, voi se jättää tietoa esille. Luottamuksellista tietoa voi tällöin päätyä hyökkääjän käsiksi tai vahingossa jonkun nähtäväksi.

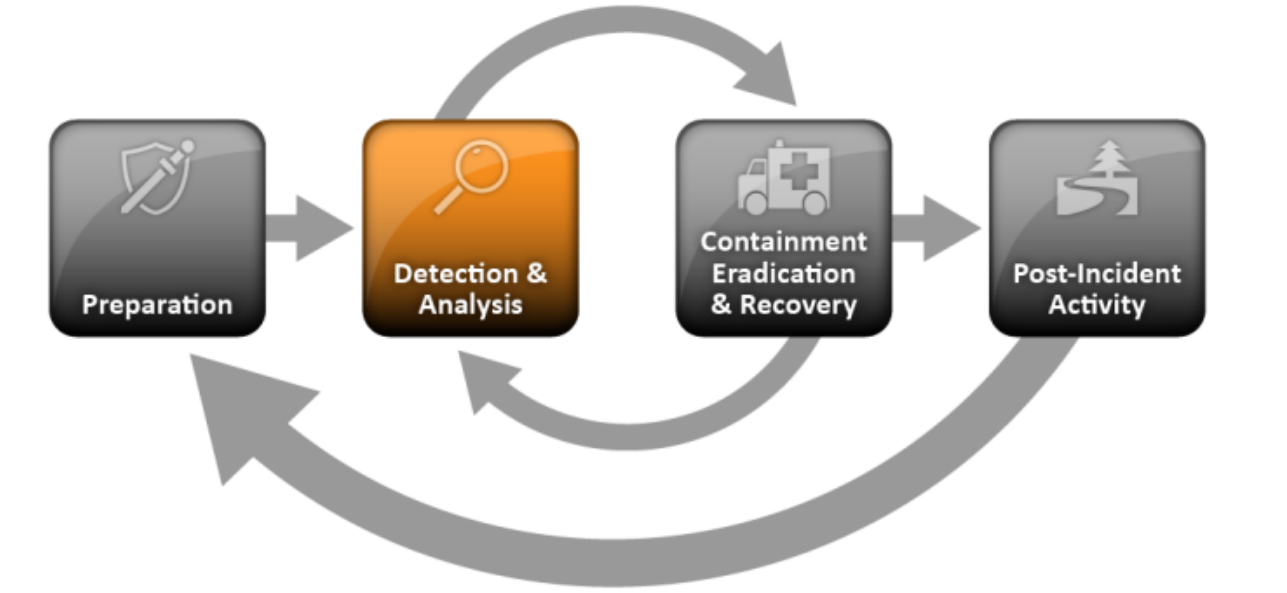
(What is a data breach n.d.)

Tietomurroista johtuneet kustannukset vuonna 2023 olivat 4.45 miljoonaa dollaria, joka on 15 prosentin kasvu viimeisen kolmen vuoden aikana (Cost of a Data Breach Report 2023). Luotettavien tietojen vuotaminen voi johtaa oikeudellisiin toimenpiteisiin, maineen vahingoittumiseen ja taloudellisiin tappioihin. Tämän lisäksi epäsuorat kustannukset kuten viestintä, erilaiset markkinointiaktiviteetit, menetetyt tulot järjestelmän käyttökatkon aikana sekä palautumisvaiheen resurssien käyttö tulevat kustantamaan organisaatiolle paljon. (How to Calculate the Cost of a Data Breach 2021.)

4.2 Häiriönhallinta

Häiriönhallinnan tarkoituksena on saada selkeyttävä kuva tietomurrosta, arvioida sen aiheuttamat vahingot ja kehittää mahdolliset jatkosuunnittelut riippuen tutkinnan tuloksista (Data Breach

Response and Investigation: 8 Steps for Efficient Remediation 2023). Häiriönhallintaan kuuluu prosessi, jonka systemaattinen noudattaminen tuo tuloksia onnistuneessa häiriönhallinnassa. Cichonskin, Millarin, Grancen ja Scarfonen (2012) luoman häiriönhallintaohjeistuksen mukaan, voidaan prosessi havainnollistaa elinkaarena neljään eri vaiheeseen: Valmistelu, havaitseminen ja analysointi, rajoittaminen, hävittäminen ja palautuminen sekä häiriön jälkeiset toiminnat (ks. kuvio 4).



Kuvio 4. NIST häiriönhallinnan elinkaari (Cichonski, Millar, Grance & Scarfone 2012)

Tätä elinkaarta käytetään yhä pohjana monien organisaatioiden ohjeistuksissa ja häiriönhallinnasta on luotu myös omia prosesseja, jotka seuraavat pääsääntöisesti samaa elinkaarta (ks. esim. Incident Response Reference Guide n.d; Kral 2011.) Jotkut organisaatiot ovat myös luoneet omia prosesseja, jotka seuraavat samaa elinkaarta omilla lisäyksillä sopimaan organisaation tarpeisiin.

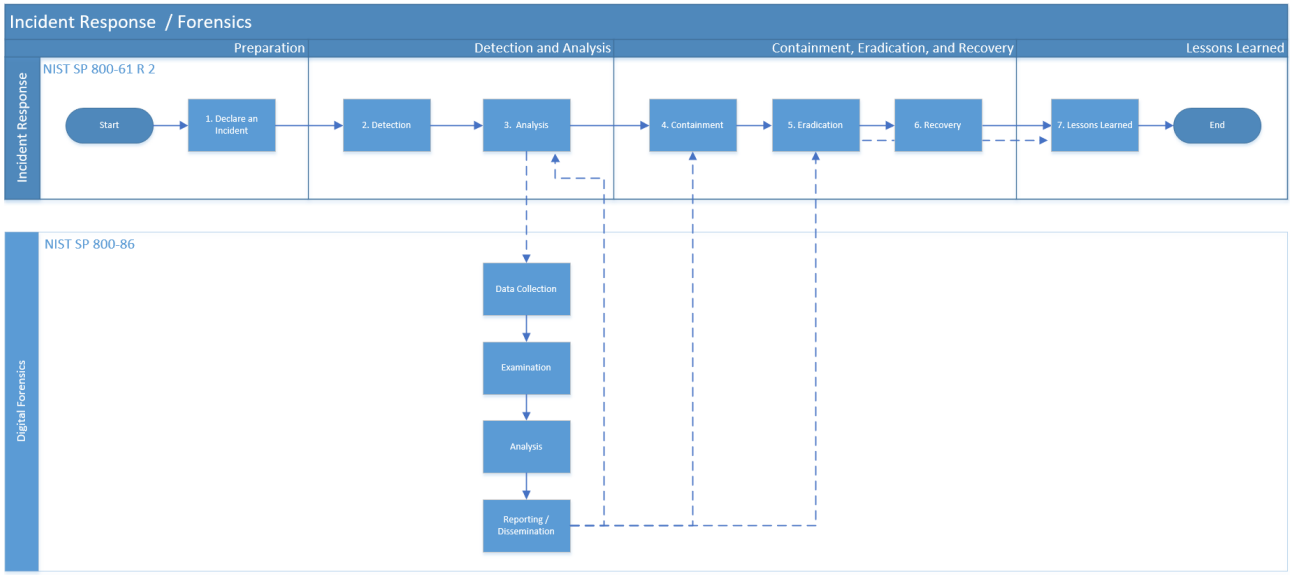
On myös hyvä huomioida, että elinkaaren prosessiin kuuluu tiivis yhteistyö eri osastojen välillä. Useasti valmisteluvaiheessa organisaation johto määrää prosessin vaiheiden kulun ja määrittelee roolit ja vastuut prosessin toteutukseen. Havainto- ja analyysivaiheen kuuluvat ovat usein osa tietoturvavalvomoa, jossa monitoroidaan ja analysoidaan mahdollisia poikkeamia, jota organisaatiossa saattaa tapahtua. Usein havainnon ensikosketus tulee tiketin kautta, joka saapuu organisaation tukeen. Kun häiriö on tunnistettu ja analysoitu, voidaan sitä alkaa rajaamaan, hävittämään ja lopulta palauttamaan häiriöstä. Myös tähän vaiheeseen osallistuu eri henkilöitä ja näitä voi olla

muun muassa erilaiset järjestelmäasiantuntijat, vastuuhenkilöt, sekä ylin johto, joka on määritellyt asianmukaiset palautumiseen liittyvät prosessit, joita noudatetaan ylätasolla kuin myös järjestelmätasolla. Tässä vaiheessa voidaan useasti palata elinkaaren aikaisempaan vaiheeseen tutkinnalta tärkeimpien lisähavaintojen tai analyysien tunnistamiseksi. Viimeisessä vaiheessa reflektoidaan häiriön tapahtumia, mietitään mikä meni pieleen, mitä on opittu ja missä voidaan parantaa. Useasti organisaatio myös vahvistaa tietojen suojauksia, päivittää eri prosesseja, sekä tarkastaa tarvittavien dokumentaatioiden paikkaansa pitävyyden sekä saatavuuden.

4.3 Tietomurtojen tutkinta osana häiriönhallintaprosessia

Vaikka Cichonskin, Millarin, Grancen ja Scarfonen (2012) NIST:n elinkaari kuvaa hyvin häiriönhallinnan eri vaiheita, ei siinä pureuduta tarkemmin itse tietomurtojen tutkintaan. Kent, K., Chevalier, S., Grance, T. & Dang, H. (2006, 25) mukaan tietomurtotutkinnan tarkoituksena on saada parempi ymmärrys tietomurrosta ja selvittää sen juurisyy. Syy tarkemmalle tutkinnalle voi olla esimerkiksi todisteiden etsiminen oikeudellisten menettelyjen ja sisäisten toimien takia, haittaohjelmatapauksien tarkempi tutkiminen tai erilaisten operationaalisten ongelmien ratkaiseminen (Kent ym. 2006, 25).

Tietomurtojen tutkinta on analyyttinen prosessi, jonka vaiheet voidaan jakaa esimerkiksi kuvion 5 mukaisesti neljään eri vaiheeseen osana häiriönhallintaprosessia: tietojen keruu, niiden tarkastelu, analysointi ja raportointi.



Kuvio 5. Tietomurtotutkinnan vaiheet osana NIST:n elinkaarta

Tietomurtojen tutkinta voidaan siis yhdistää osaksi häiriönhallintaprosessia ja tästä käytetään termiä DFIR eli Digital Forensics and Incident Response. Näiden kahden prosessin yhdistäminen auttaa lieventämään uhkia nopeammin, tekee palautumisesta tehokasta ja tuo esille todisteita, jotka olisivat voineet jäädä huomaamatta pelkässä häiriönhallintaprosessissa. Tällä ratkaisulla on kuitenkin myös haittavaikutuksia. Häiriönhallintatiimit voivat esimerkiksi tuhota todisteita poistaessaan uhkaa organisaation ympäristöstä tai tietomurtotutkijat voivat viivyttää uhan poistamista todisteiden etsinnän takia. (What is computer forensics n.d.)

4.3.1 Tutkinnan alkuvalmistelut

Ennen tutkinnan aloittamista, organisaation on tärkeää tehdä alkuvalmisteluja, sillä tutkinta sekä tiedon kerääminen ovat haasteellisia prosesseja ilman ennakoivia toimia. Alkuvalmistelut voidaan jakaa kolmeen korkean tason osa-alueeseen: Organisaation, häiriönhallintatiimin sekä infrastruktuurin valmistelut. (Luttgens, Pepe & Mandia 2016, 46.)

Organisaation ei-tekniset haasteet ovat tärkeä tunnistaa etukäteen onnistuneen tutkinnan varmistamiseksi. Yleisimmät haastealueet ovat Luttgensin ja muiden mukaan riskien tunnistaminen, toimivat häiriönhallintapolitiikat, yhteistyö ulkoistetun IT:n kanssa, globaalien infrastruktuuriongelmien tarkastelu sekä käyttäjien kouluttaminen päätelaitteiden turvallisuudesta. Riskien tunnistamisen tarkoituksena on saada korkean tason kuva yrityksen riskeistä. Näissä pyritään vastaamaan kysymyksiin: Mitkä ovat kriittisimmät omaisuudet, altistuvatko nämä heikkouksiin, mitkä ovat uhat sekä mitä rajoittavia vaatimuksia organisaation pitää noudattaa? (Luttgens ym. 2016, 47.)

Tyypilliset politiikat, joita häiriönhallintatiimi noudattaa, on sallitun käytön politiikka, turvallisuuspolitiikka, etäpääsypolitiikka sekä verkon käyttö -politiikka. Politiikkojen tulisi kattaa yleisesti sisäisten resurssien tutkinnat, näiden eristäminen sekä verkkoliikenteen häiriöt, jotta tiimi onnistuu tutkimuksessaan. Joskus tutkimuksessa hyödynnetään ulkoista tukea, jolloin organisaation on hyvä luoda prosessit, jotta vältytään mahdollisilta haasteilta tutkinnan aikana. Haasteita voi olla esimerkiksi työn hidastumiset tai lisäkustannukset. Näiden lisäksi on hyvä huomioida kansainväliset orga-

nisaatiot, joissa voidaan useasti törmätä haasteisiin, kuten eriävät säännökset maiden välillä, aikavyöhyke-eroista johtuvat tiimien koordinointiongelmat sekä tiedon saavutettavuus. Lopuksi alkuvalmisteluissa on hyvä varmistaa käyttäjien tietoisuus päätejärjestelmien turvallisuudesta. Tähän liittyy toiminnat, mitä käyttäjä voi tehdä päätejärjestelmissä, millaisia menetelmiä hyökkääjä voi käyttää sekä oikeaoppinen toiminta, kun häiriöön reagoidaan. (Luttgens ym. 2016, 47–48.)

Häiriönhallintatiimi koostuu IT:n asiantuntijoista, tutkijoista sekä ulkoisista konsulteista, joista jokaisella on eri taidot ja näkökulmat tutkinnalle. Jotta tiimi toimisi tehokkaasti, on tärkeää varustaa tiimi määrittelemällä tavoitteet, kommunikointi, tuotokset sekä resurssit. Tavoitteiden määrittely auttaa tiimiä keskittymään olennaiseen ja luo odotukset muulle organisaatiolle. Tavoitteita voi olla useita: Kaikkiin tietoturvahäiriöihin vastaaminen käyttämällä määriteltyä tutkintaprosessia, häiriön vahinkojen ja laajuuden arviointi sekä kaikkien todisteiden kerääminen ja dokumentointi liittyen häiriöön. (Luttgens ym. 2016, 50–51.)

Sujuvan sisäisen ja ulkoisen kommunikaation varmistaminen on myös tärkeää tutkinnan sujuvuuden kannalta. Sisäisessä kommunikaatiossa on oleellista muun muassa salata sähköpostiliikenne, kaikkien dokumenttien ja viestinnän luokittelu sensitiivisyyden perusteella, sähköisten tapaamisten monitorointi sekä projektinimien tai numeroinnin käyttö tutkimuksissa. Ulkoisten osapuolien kanssa kommunikointi on usein tarvittavaa ja tähän sisältyy paljon hallinnollisia ja lainsäädännöllisiä seikkoja. Tällöin organisaation on tapauskohtaisesti löydettävä paras keino siihen, miten yhteistyötä halutaan tehdä kolmansien osapuolien kanssa. (Luttgens ym. 2016, 51–52.)

Häiriönhallintatiimin tuotokset ovat erilaiset raportit, joista tärkeimmät ovat tutkinnalliset raportit. Nämä raportit voivat olla lyhyitä tiivistelmiä, jotka antavat tilannepäivityksen tutkinnasta tai ne voivat olla pitkiä yksityiskohtaisia raportteja, jossa käydään koko tutkinnan eri vaiheet läpi. (Luttgens ym. 2016, 53.)

Häiriönhallintatiimi tarvitsee resursseja onnistuakseen. Tähän sisältyy koulutukset sekä tutkintalaitteistot ja -ohjelmat. Koulutuksia häiriönhallinnasta on saatavilla paljon internetistä ja esimerkiksi SANS tarjoaa sertifikaattikursseja aiheesta (Digital Forensics Certifications n.d). Laitteistona toimii tutkijalle usein hyvin varustettu kannettava tietokone, jossa on käytössä uusimmat komponentit ja paljon muistia. Tutkijat käyttävät monia eri ohjelmia suorittaakseen tutkimustaan.

Nämä ovat yleensä yhdistelmä kaupallisia sekä ilmaisia avoimen ja suljetun lähdekoodin työkaluja. Tutkija valitsee useimmiten niitä työkaluja, jotka saavat työn suoritettua nopeinten. On hyvä olla myös useita samanlaisia työkaluja, sillä välillä jotkut työkalut eivät toimi kaikissa tilanteissa. (Luttgens ym. 2016, 54–55.)

Infrastruktuurin valmistelut ennen tietomurtotutkinnan toteuttamista on tärkeää ja Luttgensin ja muiden mukaan organisaatioilla on ollut haasteita useissa osa-alueissa. Nämä alueet voidaan jakaa kahteen: tietojenkäsittelylaitteet ja tietoverkot. Tietojenkäsittelylaitteisiin kuuluu laitteiden konfiguraatiot, omaisuuden hallinta, kyselyjen tekeminen omaisuuksista ja olemassa olevien ja uusien työkalujen instrumentointi. Tietoverkkoihin kuuluu verkon konfigurointi, segmentointi ja kulunvalvonta, dokumentaatio, instrumentaatio ja verkkopalvelut. (Luttgens ym. 2016, 61.)

4.3.2 Tiedon kerääminen

Kun tietomurtotutkinta aloitetaan, prosessin ensimmäisenä vaiheena on tiedon kerääminen. Oleellisena osana tätä vaihetta on eri tietolähteiden tunnistaminen, joita voi olla muun muassa työpöytäkoneet, palvelimet, verkkolevyt ja kannettavat tietokoneet. Näiden lisäksi tietolähteiksi voidaan tunnistaa eri varmuuskopiot, jotka tallentavat tietoa tietyltä ajankohdalta, keskitetyt lokilähteet sekä virustorjuntatyökalujen lokit. Tietoa voi löytyä monista eri lähteistä, riippuen eri sovelluksien käytöstä sekä verkon aktiivisuudesta. Lähteenä voi toimia myös ulkopuolinen organisaatio, esimerkiksi palveluntarjoajan verkkolokit. Tietolähteitä tunnistaessa onkin hyvä olla tietoinen eri lähteiden omistajista, koska tiedon tutkiminen voi hankaloitua, jos tutkittu data ei ole saatavilla oman organisaation sisällä. (Kent ym. 2006, 26–27.)

Kun relevantit tietolähteet on tunnistettu, tiedon kerääminen voidaan aloittaa. Tiedon keräämisen prosessi voi vaihdella riippuen lähteestä, mutta yleisesti prosessiin kuuluu kolme vaihetta. Aluksi on tärkeää luoda suunnitelma tiedon keräämiselle, jossa priorisoidaan lähteet. Priorisointiin vaikuttaa lähteen arvo tutkinnassa. Onko mahdollista, että lähde voidaan menettää, kuinka paljon aikaa tietolähteen hankkimiseen kuluu tai kuinka kallista lähteen hankkiminen on? Seuraavana vaiheena on itse tiedon kerääminen. Yleisesti tietoa kerätään erilaisten työkalujen avulla paikallisesti tai verkossa. Paikallinen tiedonkeruu on suositeltua, koska tällöin tutkijalla on täysi kontrolli järjestelmästä ja tiedosta. Useasti joudutaan kuitenkin turvautumaan verkon yli tutkimiseen, sillä tieto

voi olla esimerkiksi eri sijainnissa. Tiedon keräämisen jälkeen tieto täytyy vahvistaa. Tässä vaiheessa tutkijan täytyy todistaa, että kerätty tieto on pysynyt samana koko tutkinnan ajan eikä sitä ole muokattu missään vaiheessa. Tämä on tärkeää mahdollisissa oikeudellisissa toimenpiteissä. (Kent ym. 2006, 27–28.)

Tietomurtotutkinnan tiedon keräämisen parhaat menetelmät ovat Luttgensin ja muiden mukaan:

- Kaikki toiminta ja ajankohdat dokumentoidaan
- Kohtele tutkittavaa järjestelmää vaarantuneena, älä tutki ilman suunnitelmaa
- Käytä työkaluja, jotka minimoivat vaikutukset tutkittavaan järjestelmään
- Käytä työkaluja, jotka tuottavat lokia ja näistä tarkistussummat (tarkistussumma = koodi, jolla voidaan todeta, onko luettu tieto ehjää)
- Automatisoi tiedon kerääminen
- Kerää kaikki tieto volatiilisuuden varalta
- Käsittele kerättyä tietoa todisteena
- Oleta, että medialaitteessa olevat tiedot mitä yhdistät tutkittavaan järjestelmään, on vaarantunut hyökkääjälle
- Oleta käyttämäsi tunnuksesi vaarantuneiksi
- Älä tee mitään, mikä voisi aiheuttaa muutoksien tekemistä tutkittavaan järjestelmään
- Älä käytä tutkittavaa järjestelmää analyysin tekemiseen

(Luttgens ym. 2016, 141–142.)

Kuten aikaisemmin mainittiin, tietolähteitä voi olla monessa eri paikassa, mutta useimmiten todisteet löytyvät organisaatioiden kovalevyistä. Kovalevyjen monistamisessa häiriönhallintaryhmä voi luoda kolme erilaista levykuvaa käytettäväksi tutkinnassa: Täydellinen levykuva, osio levystä tai looginen kuva levystä. Täydellisessä kuvassa monistetaan kovalevyn kaikki varausyksiköt siltä hetkeltä eli käytännössä koko kovalevy monistetaan kuvaksi. Levystä voidaan myös monistaa tietty osio tai volyymi lähteenä levykuvaksi. Tällaista levykuvaa käytetään vain erityistilanteissa, esimerkiksi silloin, kun kovalevy on erityisen suuri kooltaan tai siihen on rajattu pääsy. Looginen kuva levystä on kopio tietyistä levyn tiedoista. Tämänkaltainen levykuva luodaan ainoastaan, jos muuta keinoa ei ole esimerkiksi oikeudellisissa pyynnöissä, jolloin tiettyjä tiedostoja täytyy kopioida. (Luttgens ym. 2016, 166–171.)

Kun puhutaan tiedon monistamisesta tietomurtotutkinnassa, voidaan tämä jakaa perinteiseen ja käynnissä olevan järjestelmän tiedon monistamiseen. Perinteinen monistaminen suoritetaan staattisissa levyissä eli kovalevyissä, jotka eivät ole osa järjestelmää. Tässä tavassa järjestelmä on

laitettu pois päältä ja käynnistetty erilliseen levykuvien tutkintaympäristöön tai kovalevyt on yhdistetty tutkintaan tarkoitettuun työasemaan monistamista varten. Perinteisessä tiedon monistamisessa on tärkeä käyttää write blockeria työkaluna, joka estää muokkauskomentojen tekemisen monistamisen aikana. Write blockerit ovat tärkeä osa häiriönhallintaryhmän työkaluja (ks. kuvio 6). (Luttgens ym. 2016, 173.)

Kuvio 6. Wiebetech Forensic Ultradock FUDv5.5 Write blocker

Käynnissä olevan järjestelmän tiedon monistamista käytetään keinona silloin, kun tutkinnan kohteena on erittäin kriittinen järjestelmä, jolloin sitä ei voida laittaa tutkinnan aikana pois päältä tai jos kovalevy on salattu niin, että tiedot eivät ole saatavilla, jos järjestelmä otetaan pois päältä. Tässä monistamistavassa on erityisen tärkeää dokumentoida kaikki mitä tehdään, mitä työkaluja käytetään, mitä palveluja on päällä sekä tarkat päivämäärät, koska monistamisen aikana levykuvaan tulee muutoksia, jolloin tietojen oikeudenmukaisuutta voidaan kyseenalaistaa. Näiden lisäksi monistamista ei ole suojaamassa write blocker, jonka takia tiedon käsittelyssä pitää olla varovainen, jotta todisteita ei vahingossa tuhoa kirjoittamalla levykuva uudestaan lähdelevystä. (Luttgens ym. 2016, 179–180.)

Levykuvien tekemiseen käytetään yleensä työkaluina parhaaksi koettuja työkaluja. Luttgens ja muut mainitsevat kolme työkalua levykuvien luomiseen, jotka ovat DC3dd, FTKImager ja EnCase. DC3dd on Defense Cyber Crime Centerin (DC3) luoma työkalu, jossa käytetään Unix-järjestelmien dd-komentoa perustana. Tämä komento mahdollistaa tiedostojen muuttamisen ja kopioimisen, mutta siitä puuttuu kryptografisten tarkistussummien generointi ja käyttäjäpalautteen tarjoaminen. Tämän takia on suositeltavaa käyttää työkaluna uudempaa työkalua, kuten DC3dd:tä, levykuvien luomiseen. (Luttgens ym. 2016, 175–176.)

4.3.3 Tiedon tarkastelu

Kun tarvittavat tiedot on kerätty tutkintavaiheen alussa, voidaan tietoa alkaa tarkastelemaan arvioimalla ja purkamalla tietoa. Useasta lähteestä tuotu tieto voi sisältää satojatuhansia tiedostoja, jolloin erilaisia työkaluja ja tekniikoita voidaan käyttää työtaakan vähentämiseksi. Näitä voi olla esimerkiksi erilaisten tekstien ja rakenteiden hakeminen tai eri tiedostojen sisältöjen suodattaminen oikeanlaisen tiedostotyypin löytämiseksi. (Kent ym. 2006, 30.)

4.3.4 Analysointi

Kun tietoa on kerätty ja relevantit tiedot tunnistettu, voidaan tietoa alkaa analysoimaan johtopäätöksien luomiseksi. Analysoinnissa kuuluu tunnistaa ja dokumentoida ylös tapahtumia, ihmisiä, paikkoja sekä eri kohteita, jotta eri lähteitä voidaan korreloida keskenään johtopäätöksen saamiseksi. Erilaiset työkalut pystyvät suorittamaan tätä prosessia automaattisesti esimerkiksi turvallisuustapahtumien hallintaohjelmat ja keskitetyt lokitustyökalut. (Kent ym. 2006, 30.)

4.3.5 Raportointi

Tutkintaprosessin viimeisenä vaiheena on analysointituloksien raportointi. Raportointiin voi vaikuttaa esimerkiksi tiedon puutteellisuus, jolloin tarkkaa syytä ei välttämättä löydetä ja tällöin voidaan päätyä useaan eri johtopäätökseen. Raportoinnissa on hyvä myös tietää kohdeyleisö. Esimerkiksi järjestelmän ylläpitäjää kiinnostaa eniten verkkoliikenteen statistiikka, kun taas ylempää johtoa kiinnostaa ylätason katsaus siitä mitä on tapahtunut. (Kent ym. 2006, 30–31.)

Raportointivaiheessa tutkijoiden on hyvä tunnistaa ja korjata mahdolliset ongelmat esimerkiksi politiikkapuutteet. Useasti tutkintatiimit pitävätkin muodollisia tapaamisia, joissa katselmoidaan,

mikä meni vikaan laajan häiriötilanteen jälkeen ja tehdään mahdollisia muutoksia ohjeistuksiin ja prosesseihin organisaation sisällä. Muita ongelmia voi olla esimerkiksi mitä kerätylle tiedolle tehdään tutkinnan jälkeen ja millaisia muutoksia eri kontrolleille pitää tehdä, jotta lisätietoa voidaan kerätä tulevaisuutta varten. Kun muutokset ovat astuneet voimaan, useasti organisaatioiden sisäisissä tiimeissä seurataan muutoksia dokumenttien versiohistorian avulla. Tällöin kaikki tiiminjäsenet ovat aina tietoisia muutoksista ja osaavat toimia sen mukaan. (Kent ym. 2006, 31.)

4.4 Tietomurtotutkintamenetelmien kehitys

4.4.1 Perinteinen tutkinta

Tietomurtotutkinta on kehittynyt vuosien varrella monimutkaisemmaksi ja hankalammaksi teknologian kehityksen rinnalla. Perinteisesti tietomurtotutkinnassa tiedot kerätään eri työkaluja fyysisestä elektronisesta laitteistosta paikalliselle tutkimuskoneelle, jonka jälkeen tietoa voidaan analysoida ja löytää todisteita tietomurrosta. Tässä kappaleessa perehdytään tarkemmin tietomurtotutkinnan metodologiaan, eri työkaluihin, tekniikoihin sekä haitallisen toiminnan tutkimiseen Windows-työasemassa.

Tietomurtotutkinnassa voidaan seurata metodologiaa, joka sisältää:

1. Tavoitteiden määrittelyn ja ymmärtämisen
2. Merkittävien tietojen keräämisen
3. Tiedon sisällön tarkastelun
4. Tarvittavien muunnoksien ja normalisointien suorittamisen
5. Metodin valitsemisen
6. Analyysin suorittamisen
7. Tuloksien arvioinnin

(Luttgens ym. 2016, 254.)

Tavoitteiden määrittelyssä täytyy olla tietoinen tilanteesta sekä saatavilla olevasta teknologiasta. Ennen analyysin tekemistä tutkijalla pitää olla hyvä ymmärrys siitä mitä halutaan määritellä, onko johtopäätöksen tekeminen mahdollista saatavilla olevasta tiedosta, mitä resursseja tarvitaan, kuinka kauan analyysiin käytetään aikaa, kelle tulokset on tarkoitettu ja mitä tuloksilla on tarkoitus tehdä. On tärkeää myös tunnistaa henkilö, joka määrittelee tavoitteet sekä pitää huolen siitä, että kaikki tiimin jäsenet tietävät kuka tämä henkilö on. Tämä vahvistaa tiimin sisäistä kommunikaatiota ja keskittymistä tutkinnan aikana. (Luttgens ym. 2016, 254–255.)

Kun tarvittava tieto, esimerkiksi levykuva on saatu, voi ensimmäisenä haasteena olla pääsy levykuvan tietoon. Jos levykuva ei ole tilassa, missä analyysiä voidaan tehdä voi tutkinta osoittautua haasteelliseksi tai jopa mahdottomaksi. Tieto voi olla esimerkiksi salattu, kompressoitu, koodattu tai olla jonkinlaisessa muokatussa formaatissa, jonka takia tutkijan on tärkeä kysyä levykuvan antaneelta henkilöltä tarkentavia kysymyksiä levykuvasta. ”Minkälaisesta kovalevystä, kopioista ja järjestelmästä on kyse?” sekä ”minkälaista salausta kovalevyssä on käytetty, minkälaista formaattia levykuvassa käytetään ja onko järjestelmä esimerkiksi pöytätietokone, kannettava vai palvelin?” (Luttgens ym. 2016, 259–260.)

Yleisimmät levykuvaformaatit mitä tutkinnassa käsitellään ovat E01, joka on lyhenne Expert Witness/EnCasesta, DD eli raakakuvat sekä virtuaalikoneiden levytiedostot VMDK ja OVF. Jos tutkijalla on käytössä kaupallinen työkalu esimerkiksi EnCase, tukee tämä useimmiten yleisimpiä formaatteja (OpenText EnCase Forensic n.d). Kaupalliset työkalut mahdollistavat yleisesti myös salattujen levykuvien tutkimisen olettaen, että tutkijalla on salauksen purkamiseen tarvittavat salasanat tai avaimet. Ei-kaupallisista työkaluista FTKImager ja FUSE ovat toimivia ratkaisuja, jotka tarjoavat samanlaisia kyvykkyyksiä kuin EnCase. (Luttgens ym. 2016, 260–261.)

Yleinen kiertotapa salauksen purkamiseen ei-kaupallisia työkaluja käyttämällä on ollut jonkinlaisen mount-työkalun käyttö, esimerkiksi OSFMount (OSFMount n.d). OSFMountilla salattu levy pystytään alustamaan omalle koneelle, jonka jälkeen siitä pystytään ottamaan levykuva ilman salausta.

Seuraavana vaiheena tutkijan on määriteltävä lähestymistapa analyysin tekemiselle. Tutkijan on kannattavaa luoda lista mahdollisista tietolähteistä, jotta kysymyksiin pystytään vastaamaan, sillä välillä todisteita voi löytyä yllättävistä paikoista. Esimerkiksi, jos tarkoituksena on löytää todisteita tietovarkaudesta, kannattaa tutkijan etsiä esimerkiksi epänormaalia käyttäjäaktiviteettia, sisäänkirjautumisia normaalien aikojen ulkopuolelta tai odottamattomien etäyhteyksien luontia. (Luttgens ym. 2016, 263–264.)

Ohjeistuksia erilaisista tavoista tutkia tietomurtoja eri järjestelmistä on monia ja esimerkiksi SANS suosittelee seuraavaa lähestymistapaa haitallisen toiminnan tutkimiselle Windows-työasemassa:

1. Todisteiden rajaaminen ja valmistelu

2. Antivirus-skannaukset
3. Vaarantumisindikaattoreiden (IOC) etsintä
4. Automatisoitu muistin analysointi
5. Todisteiden hankinta haittaohjelmien sinnikkyydestä
6. Pakkaus/entropia -tarkistus
7. Tapahtumalokien tarkastelu
8. Tietojen havainnollistaminen aikajanalla
9. Manuaalinen muistin analysointi
10. Manuaaliset kolmannen osapuolen hash-tarkastukset
11. MFT-poikkeavuudet
12. Tiedostojen aikapoikkeavuudet
13. Haittaohjelman tunnistaminen, luovutus analyytikolle

(Windows Artifact Analysis 2013.)

Tietomurtotutkinnan työasemat

Tietomurtotutkinnassa käsitellään erittäin paljon tietoa, minkä takia tutkinnassa käytetyt työasemat tarvitsevat suuren määrän muistia ja suorittimen nopeutta. Esimerkiksi Sumuri tarjoaa monia eri palveluita tietomurtotutkinnan tekemiseen mukaan lukien työasemia. Sumurilla on tarjolla sekä pöytäkoneita että kannettavia tietokoneita ja näiden hinnat vaihtelevat välillä 2 000–20 000 euroa (Online Shop - The Forensic Tools to Meet Your Needs n.d). Hinnat perustuvat työasemien teknisiin tietoihin ja näitä ovat muun muassa muistitilan koko sekä suorittimen ja näytönohjaimen nopeus. Työasemaa valittaessa on hyvä selvittää tarkasti minkälaiset suorituskyvyt ovat optimaaliset omaan käyttötarkoitukseen ja valita työasema tämän perusteella.

4.4.2 Paikallinen tutkintalaitteisto pilvessä

Tietomurtotutkinnan tekeminen pilvessä muistuttaa menetelmiltään, tekniikoiltaan ja työkaluiltaan perinteistä tutkintaa. Pilveen kohdistuneessa tutkinnassa työskennellään yhtä lailla muun muassa verkkojen, palvelimien, applikaatioiden ja tietokantojen kanssa, mutta erona perinteisen ja pilvessä tapahtuvan tutkinnan välillä on tiedonsiirtomenetelmät. Koska tieto liikkuu pelkästään pilvessä, tarvitsee tutkija tapoja käyttää hyödyksi Azuren tarjoamia ratkaisuja tehokkaan tiedon käsittelemiseen.

Pilvessä tapahtuvaa tietomurtotutkintaa voi hankaloittaa pilvipalvelujen vaihtelevat maailmanlaajuiset sijainnit. Tällöin latenssi voi nousta tietoa kerätessä ja tutkinta voi hajaantua. Tämän lisäksi

pilvipalvelut pysyvät aina päällä tutkinnan aikana, mikä voi tehdä tutkinnasta epävakaata mahdollisten muutoksien takia. (Tidmarsh 2022.)

Pilvessä tapahtuvasta tutkinnasta löytyy myös paljon hyötyjä. Tiedon saatavuus paranee, sillä tutkijalla on pääsy tietoon, vaikka tutkintaa tehtäisiin toisella puolella maapalloa. Pilvipalveluiden tarjoamat tutkintalaitteistot mahdollistavat skaalaamisen, joka sallii suuren tietomäärän käsittelemisen nopeammin esimerkiksi käynnistämällä monta analysointiprosessia samaan aikaan tai nostamalla yksittäisen resurssin tehokkuutta. (Benefits of cloud forensics 2024.)

Tutkintaympäristö pilvessä

Pilvessä tapahtuvassa tutkinnassa hyödynnetään virtualisointia järjestelmien käytössä ja tutkimisessa. Virtuaalikoneilla on samat kyvykkyydet kuin normaaleilla työasemilla, palvelimilla ja muilla järjestelmillä, joten tietomurtotutkintaa voidaan tehdä myös näitä hyödyntäen. Pilvipalveluntarjoajat tarjoavat mahdollisuuden luoda virtuaalikoneita ja määritellä näihin käyttötarkoitukset. Azure tarjoaa virtuaalikoneiden luomisessa nimeämisen, resurssien sijainnin, virtuaalikoneen koon, määrän, käyttöjärjestelmän, konfiguraatiot ja näihin liittyvät resurssit (Virtual machines in Azure 2024). Kappaleessa 5.1 käydään tarkemmin läpi, minkälainen virtuaaliympäristö tarvitaan, jotta tietomurtotutkintaa voidaan tehdä tehokkaasti Azureen tehtyä tutkintaympäristöä hyödyntäen.

5 Hallitun tietomurtotutkinta-alustan implementointi Azureen

Tässä kappaleessa käydään läpi Azuren pilviympäristöön tuodun levykuvan analysointia virtuaalikoneessa. Kappaleessa määritellään, minkälaisia vaatimuksia tutkintalaite tarvitsee onnistuneen analyysin tekemiseen, verrataan erilaisten tutkintalaitteistojen suorituskyvykkyyksiä ja hintoja, jonka lisäksi kuvataan referenssitoteutus virtuaalisesta Azuren ympäristöstä, jossa tietomurtotutkinta voidaan toteuttaa virtuaalikoneessa.

5.1 Yksittäisen levykuvan analysointi

Tässä kappaleessa käsitellään Azuren pilviympäristöön tuodun levykuvan analysointia. Kappaleessa määritellään, minkälaisia vaatimuksia virtuaalinen tutkintalaite tarvitsee onnistuneen analysoinnin tekemiseen, verrataan erilaisien tutkintalaitteistojen suorituskyvykkyyksiä ja hintoja, jonka

lisäksi kuvataan referenssitoteutus virtuaalisesta Azuren tutkintaympäristöstä, jossa tietomurto-tutkintaa voidaan toteuttaa.

Tutkija voi käyttää levykuvan analysoimiseen joko fyysistä tai virtuaalista tutkintalaitetta. Nämä laitteet voivat hyödyntää samoja analyysityökaluja tutkinnan tekemisessä. Virtuaalikoneiden vaatimukset riippuvat paljon tutkinnan monimuotoisuudesta, tiedon määrästä sekä työkaluista. Organisaatio voi käyttää virtuaalikonetta valitessaan hyödyksi Azuren Pricing Calculatoria, jonka avulla voidaan valita omaan käyttötarkoitukseen relevantit Azuren tuotteet (Pricing calculator n.d). Seuraavassa kappaleessa verrataan eri käyttötarkoituksiin tarkoitettujen Windows-laitteiden kykyjä suorittaa tietomurtotutkinnassa käytettyjä prosesseja, jonka perusteella voidaan päätellä, minkälainen virtuaalikone tarvitaan hallittuun tietomurtotutkintaympäristöön Azuressa.

5.1.1 Tutkintalaitteiden vertailu

Tutkinnan tarkoituksena on selvittää eri hintaluokan tutkintalaitteita vertaillen, hyödyntääkö tietomurtotutkinnassa käytetyt työkalut tutkintalaitteen kyvykkyyksiä kokonaisvaltaisesti sekä pohditaan tuloksien perusteella, minkälainen tutkintalaite tarvitaan Azuressa sijaitsevaan virtuaaliympäristöön.

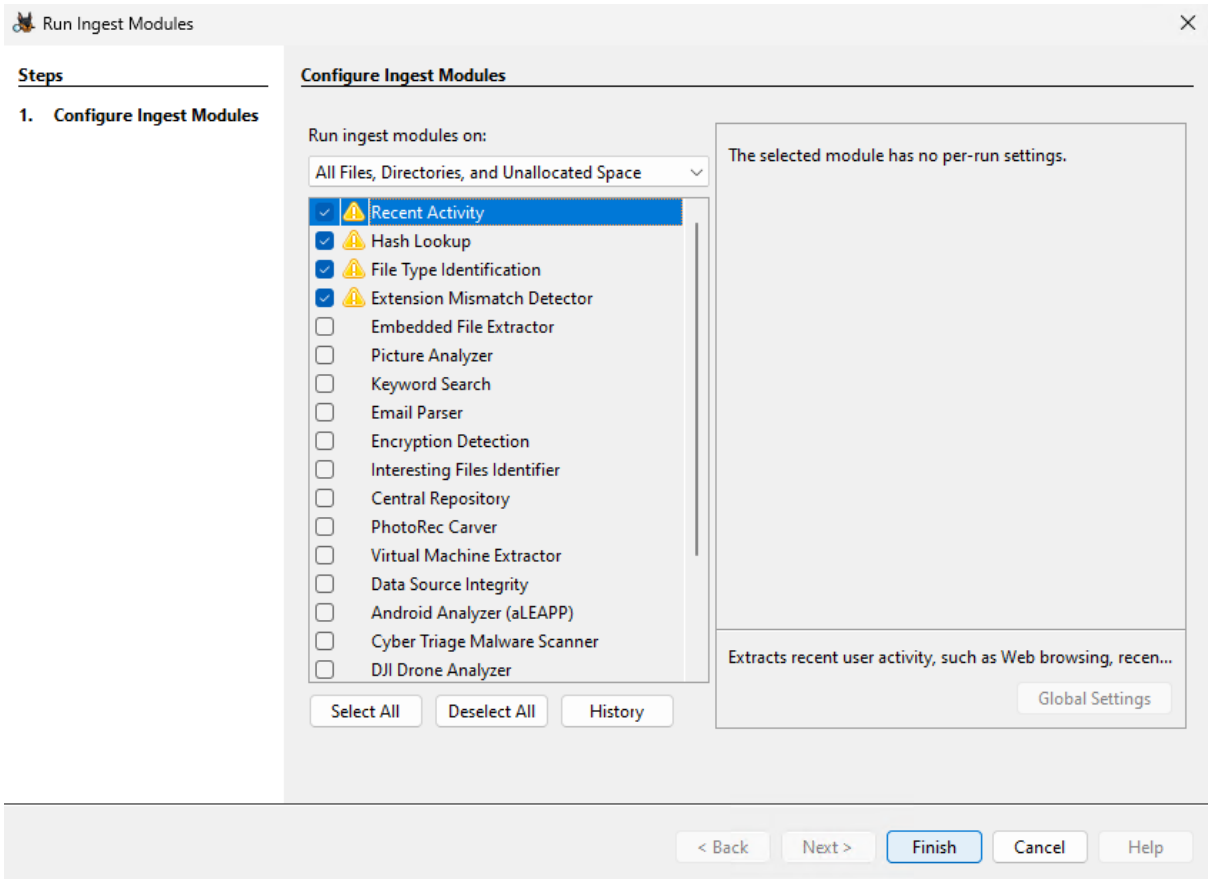
Tutkintalaitteet

Tutkinnassa käytettiin kolmea eri kannettavaa tietokonetta, joilla kaikilla on oma käyttötarkoitus ja hintaluokka. Laitteet ovat tarkoitettu toimistokäyttöön, ohjelmointikäyttöön sekä tietomurtotutkintakäyttöön. Toimistokoneeseen ja ohjelmointikoneeseen on luotu virtuaalikone erikseen tutkimuksen tekemiselle ja tietomurtotutkintakoneeseen mittaukset on tehty ilman virtualisointia. Taulukko 1 kertoo tutkintalaitteiden hinnan, prosessorin, muistin sekä cpubenchmark.net -sivuston pisteytykset jokaiselle prosessorille (CPU Benchmarks n.d).

Taulukko 1. Tutkintalaitteet

Lenovo tutkintalaite	ThinkPad X1 Yoga Gen 7	Thinkpad P1 Gen 5	Thinkpad P16 Gen 1
Hinta	n. 1500 euroa	n. 4500 euroa	n. 2400 euroa
Prosessori	i7-1265U, yksi ydin, yksi looginen prosessori	Intel i7-12800H, 14 ydintä, 20 loogista prosessoria	Intel i7-12850HX, 16 ydintä, 24 loogista prosessoria
Muisti (gigatavu)	8	64	64
CPU benchmark-sivun suorituskykypisteet	13 808	24 804	30 712

Ensimmäisessä prosessissa tutkitaan avoimen lähdekoodin Autopsy-analysointityökalun kyvykkyyksiä suorittaa erityyppisiä analysointimoduuleja samaan aikaan. Suorituskyvykkyyden testaamisessa käytettiin Smithsin (2020) tekemän analysointiharjoituksen tarjoamaa levykuvaa palvelimesta. Autopsy tarjoaa useita hyödyllisiä moduuleja oletuksena, mutta tutkinnan nopeuttamiseksi tähän valittiin neljä moduulia: Recent Activity, Hash Lookup, File Type Identification ja Extension Mismatch Detector (ks. kuvio. 7). (Autopsy User Documentation 3.1 2015.)



Kuvio 7. Autopsy-analysointityökalun suoritettavat moduulit

Autopsy's User's Guide (2015) mukaan Recent Activity kerää käyttäjän viimeisimmät tapahtumat, joita voi olla asennetut ohjelmat, käytetyt dokumentit ja internetin selailu. Hash Lookup tunnistaa ja kerää tunnistettuja tiedostoja, jotka käyttävät hash-settejä, File Type Identification yhdistää tiedostotyyppejä binääriallekirjoituksien mukaan ja Extension Mismatch Detector merkitsee tiedostot, joilla ei ole standardin mukaisia laajennuksia perustuen tiedostotyyppiin. (Autopsy's User Guide 2015.)

Seuraavassa prosessissa tutkitaan tutkittavan kuvalevyn MFT-tiedoston jäsentämisnopeutta. Master File Table eli MFT on Windowsiin kuuluva tiedostojärjestelmä, joka sisältää tiedot kaikista kansioista ja tiedostoista levyllä. MFT on tärkeä tutkintalähde, sillä siitä löytyy paljon tietoa tietojärjestelmän aktiviteeteista ja se on useasti lähde, josta todisteet tietomurrosta löydetään. (The MFT: The Forensic Investigator's Secret Weapon 2024.)

Jotta MFT:tä voidaan tutkia, täytyy siitä aluksi tehdä luettava tiedosto. MFT:n jäsentämiseen on olemassa Eric Zimmermanin luoma MFTECmd työkalu, jonka avulla MFT voidaan jäsentää ja tulokset voidaan syöttää haluttuun tiedostotyyppiin, esimerkiksi json tai csv. (Eric Zimmerman Tools n.d.)

MFT voidaan hakea esimerkiksi Autopsyn avulla tutkittavasta levykuvasta, jonka jälkeen se voidaan siirtää haluttuun polkuun, jossa se jäsennetään. Tähän käytettiin Powershell-komentokehotetta hyödyksi. MFTECmd:n suorittamiseen tarkoitettu komento ei ole monimutkainen, mutta suorituksen mittaamiseen tarvitaan measure-command -komentoa. Komentoon määritellään polku, johon MFT on tuotu Autopsyn avulla, joka on tässä tapauksessa luodussa MFT-kansiossa polussa C:\MFT. Tämän jälkeen tiedot tallentuvat csv-tiedostona Reports-kansion alle. Huomiona myös se, että komento pitää suorittaa polussa, jossa MFTEcmd-työkalu sijaitsee. Tässä se on ”C:\tools\net6” polussa (ks. kuvio 8).

```
PS C:\tools\net6> measure-command {.\mftecmd -f 'C:\MFT\$MFT' --csv C:\Reports\ }
```

Kuvio 8. MFTEcmd-komento

MFT-jäsentämisen suoritusaika vaihtelee jokaisella suorituskerralla, joten tarkemman tuloksen saamiseksi tarvitaan useita suorituksia. Tätä varten loin Powershell-skriptin, joka suorittaa MFTECmd-komennon kolmekymmentä kertaa, jonka jälkeen skripti listaa kaikki suoritusajat tekstitiedostoon (ks. kuvio 9).

```
PS C:\tools\net6> $filePath = "C:\Reports\results.txt"
PS C:\tools\net6>
PS C:\tools\net6> for ($i = 1; $i -le 30; $i++) {
>>     $result = Measure-Command {
>>         & .\mftecmd -f 'C:\MFT\$MFT' --csv C:\Reports\
>>     }
>>
>>     $executionTime = $result.TotalMilliseconds
>>     $output = "Execution Time: $executionTime ms`n$result`n"
>>
>>     $output | Out-File -FilePath $filePath -Append
>> }
```

Kuvio 9. Powershell-skripti suorituskertojen laskemiseen ja listaamiseen

Tämän jälkeen siirsin tulokset Exceliin tarkemman analyysin tekemiseksi. Seuraavassa kappaleessa tarkastellaan analysointiprosessien tuloksia ja esitellään johtopäätökset tutkintalaitteiden vaatimuksista analysoinnin tekemiseen.

Tulokset ja johtopäätökset

Autopsy-moduulien suoritusnopeuksien tulokset saatiin käyttämällä Autopsyn Ingest Progress Snapshot -ominaisuutta. Ominaisuus on tarkoitettu tarkastelemaan meneillään olevia moduulisuorituksia ja tämän jälkeen moduulien lopullisen suoritusajan tulokset saadaan selville. (Autopsy User Documentation 4.5.0 2018.)

Moduulista ja levykuvasta riippuen, suoritusnopeudet voivat vaihdella paljon. Tässä tapauksessa toimistokoneessa kesti pisimpään suorittaa moduulit. Hash Lookup ja File Type Identification -moduuleissa kesti noin 6 sekuntia, Recent Activity -moduulissa noin yksi sekunti ja Extension Mismatch Detector -moduuli oli valmis melkein välittömästi (ks. kuvio 10).

Module	Duration
Hash Lookup	00:06:01.319 (49%)
File Type Identification	00:04:22.922 (35%)
Recent Activity	00:01:27.816 (12%)
Saving Results	00:00:12.777 (1%)
Extension Mismatch Detector	00:00:06.619 (0%)

Kuvio 10. Toimistokoneen Autopsy-tulokset

Ohjelmointi- ja tietomurtotutkintakoneen tulokset olivat hyvin samanlaisia keskenään (ks. kuvio 11 ja 12).

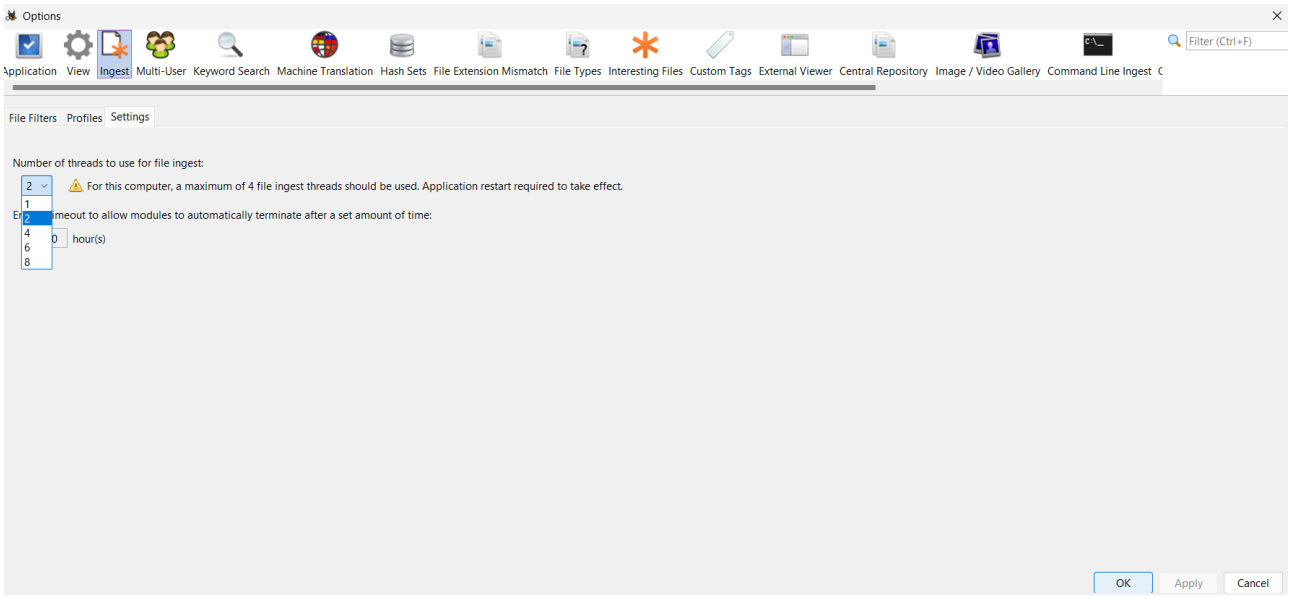
Module	Duration
Hash Lookup	00:02:33.325 (64%)
File Type Identification	00:00:55.135 (23%)
Recent Activity	00:00:24.825 (10%)
Saving Results	00:00:03.383 (1%)
Extension Mismatch Detector	00:00:02.103 (0%)

Kuvio 11. Ohjelmointikoneen Autopsy-tulokset

Module	Duration
Hash Lookup	00:03:05.650 (57%)
File Type Identification	00:01:10.711 (21%)
Recent Activity	00:00:59.169 (18%)
Saving Results	00:00:08.179 (2%)
Extension Mismatch Detector	00:00:00.319 (0%)

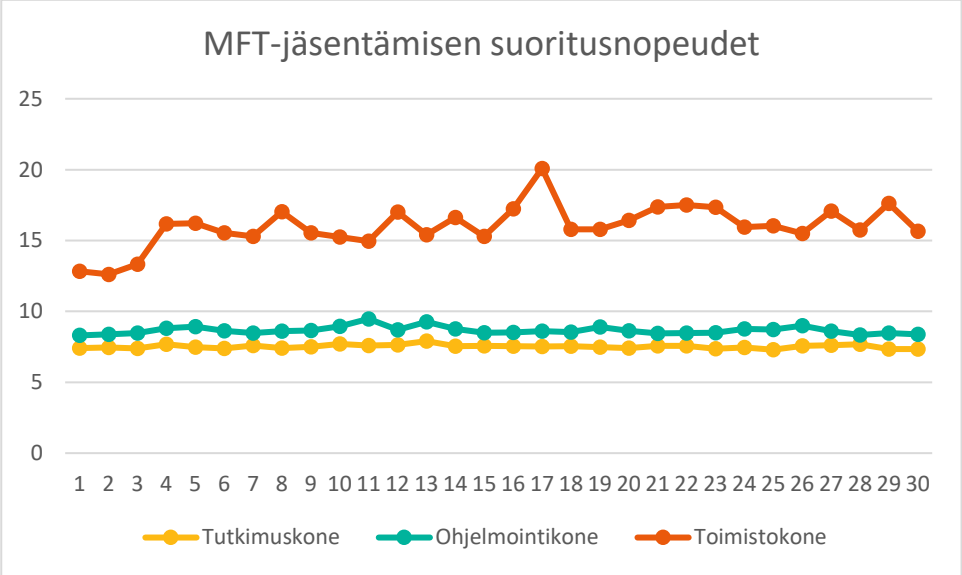
Kuvio 12. Tietomurtotutkintakoneen Autopsy-tulokset

Järjestelmästä ja levykuvan koosta riippuen on tärkeää säätää moduulien ajoasetuksia suorituskyvyn optimoimiseksi. Erityisesti säikeiden määrän muuttaminen voi nopeuttaa ajosuoritusta ja tätä voi säätää Ingest-asetuksista (ks. kuvio 13). (Optimizing Performance 2019.)



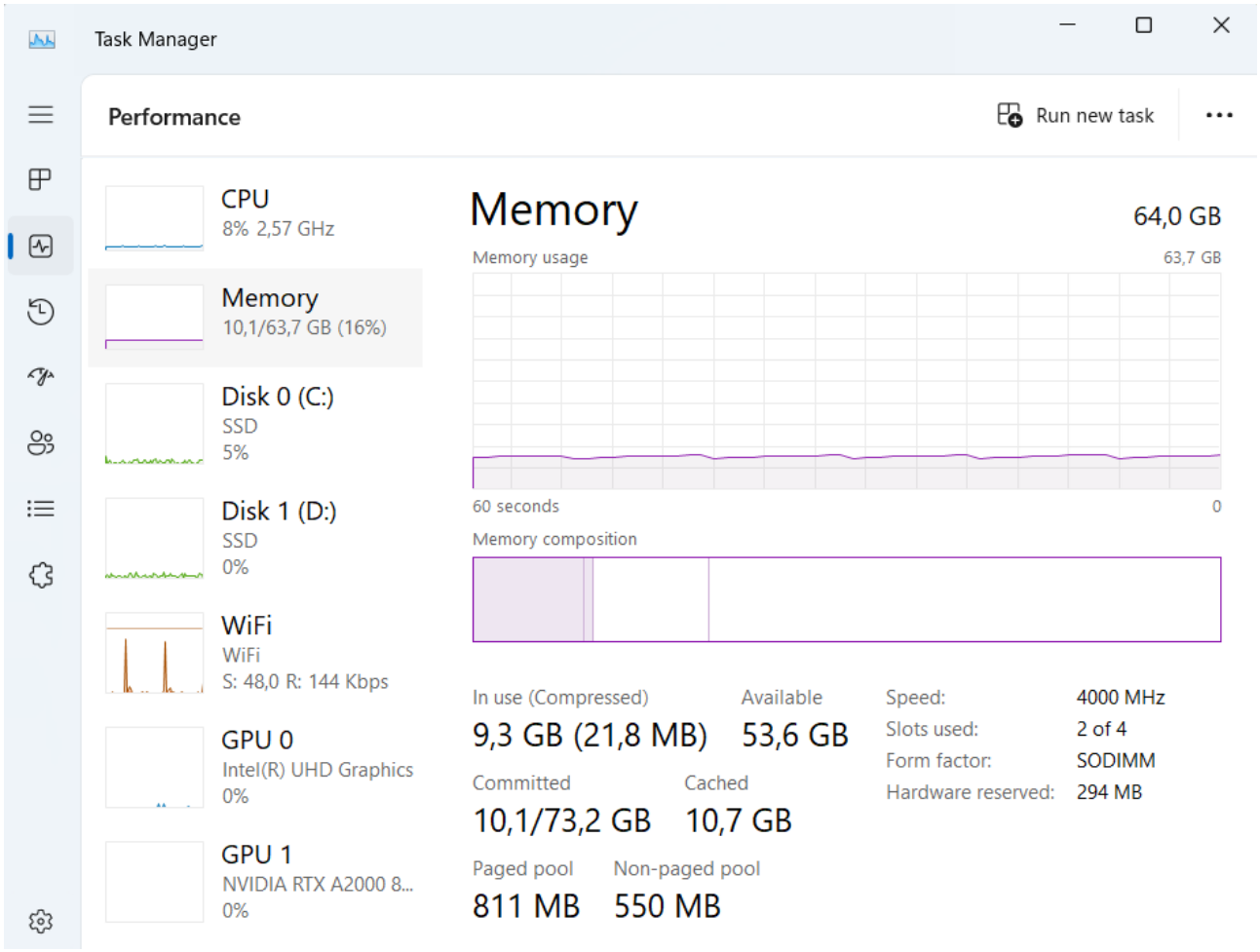
Kuvio 13. Säikeiden määrän muuttaminen Autopsyn asetuksista

Koska MFT jäsentämisen kesto vaihtelee, suoritin komennon kolmekymmentä kertaa ja laskin näistä tuloksista keskiarvon. Tietomurtotutkintakoneen keskiarvonopeudeksi sain tulokseksi noin 7,5 sekuntia, ohjelmointikoneelle noin 7,8 sekuntia ja toimistokoneen nopeudeksi noin 16 sekuntia, eli tietomurtotutkintakone oli näistä nopein. Kuviosta 14 näkee suoritusnopeuksien eroavaisuudet MFT-jäsentämisessä.



Kuvio 14. MFT-jäsentämisen suoritusnopeudet

Kuten tuloksista voi päätellä, tutkimuskoneen ja ohjelmointikoneen tulokset ovat melkein samat molemmissa analysointiprosesseissa, kun taas toimistokoneen tulokset ovat yli kaksi kertaa hitaammat. Windowsin Resource Monitoria tarkkailemalla, voidaan todeta, että nopeampi prosessori ja säikeiden määrä vaikuttavat analysointiprosessien nopeuteen. Tutkimuskoneessa ja ohjelmointikoneessa on molemmissa 64 gigatavua muistia, joten vertailua ei voida tehdä sen perusteella. Ilman ylimääräisiä prosesseja tutkimuskoneessa, muistia on varattuna 6,6 gigatavua. Analysointiprosessin aikana kone vie 9,3 gigatavua muistia. Alla olevasta kuviosta näkee, kuinka paljon MFTEcmd:n suorittaminen käyttää muistia tutkimuskoneessa (ks. kuvio 15).



Kuvio 15. Tutkimuskoneen muistinkäyttö MFTEcmd-prosessin aikana

5.1.2 Referenssitoteutus

Tässä kappaleessa kuvataan minkälaisen tutkintaympäristön Azureen tutkija tarvitsee, jotta levykuvan analysointi pystytään toteuttamaan käyttäen Azuren tarjoamia moderneja komponentteja ja työkaluja. Tämän lisäksi valitsin virtuaalikoneen, joka tukee tutkintalaitteiden vertailussa saatuja tuloksia ja johtopäätöksiä ja vertailen tietomurtotutkintalaitteen sekä valitun virtuaalikoneen hintoja kolmen vuoden ajalta. Lopuksi havainnollistan tutkintaympäristöä arkkitehtuurikuvalla, joka perustuu ohjeistuksen mukaisiin Azuren komponentteihin ja työkaluihin.

Virtuaalikoneen valitseminen

Tutkimuslaitteiden vertailusta voidaan todeta, että prosessori vaikuttaa paljon analysoinnin tekemiseen. Azuren virtuaalikonetarjonta on jaettu käyttötarkoituksien, kustannuksien ja suoritusnopeuksien mukaan eri sarjoihin, jonka takia on hyvä ymmärtää mihin eri käyttötarkoituksiin virtuaalikoneet on tarkoitettu. A-sarjan virtuaalikoneet tarjoavat hyvän kustannustehokkaan ratkaisun ensikertalaiselle, mutta tehokkaamman, isompien tietomäärien käsittelemiseen on suositeltavaa valita virtuaalikone D-sarjasta. D-sarjan virtuaalikoneet tarjoavat tehokkaampia komponentteja virtuaalikoneisiin, mutta ovat myös kalliimpia verrattuna A-sarjaan. (Virtual Machine series n.d.)

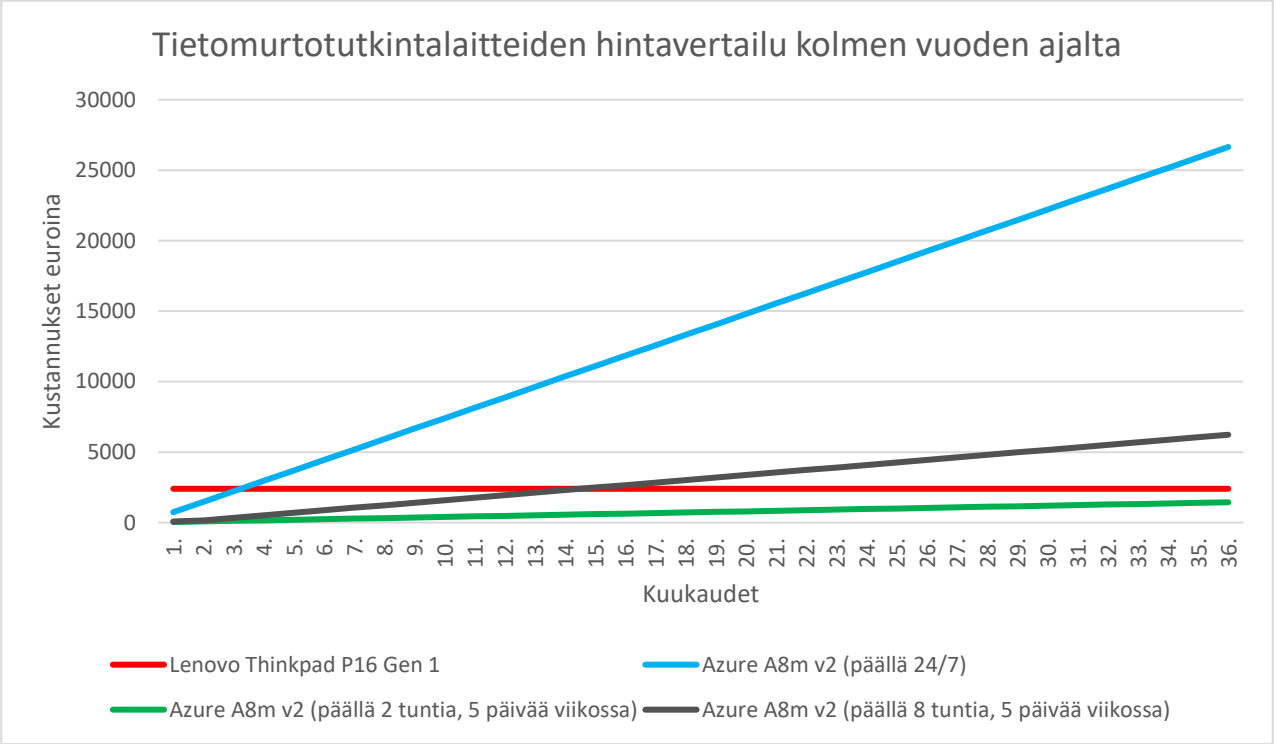
Tätä työtä varten valitsin A-sarjaan kuuluvan A8m v2 -virtuaalikoneen, joka tarjoaa 8 säettä, 64 gigatavua muistia ja 80 gigatavua välimuistia. Tällä virtuaalikoneella on kohtalainen suorituskyky ja Pricing calculatorin (n.d) mukaan tämän hinta on noin 1 euro tunnissa. Tallennuslevyjä valitsin käyttöjärjestelmälevyn lisäksi kaksi 1000 gigatavun HDD-levyä. Levykuvat voivat olla kooltaan useita satoja gigatavuja, jonka takia näihin kannattaa varata tarpeeksi tilaa. Näillä valinnoilla virtuaalikoneen hinnaksi tulee arviolta 740 euroa kuukaudelta. (Pricing calculator n.d.)

D-sarjasta olisi voinut myös käyttää esimerkiksi D16as v5 virtuaalikonetta, jossa on 16 säettä ja 64 gigatavua muistia. Välimuistia tässä virtuaalikoneessa ei ole ollenkaan ja hinta on noin 1 euro 70 senttiä tunnilta. Tässä koneessa on myös tehokkaampi prosessori, joka voi nopeutta tutkinnan aikaa, jolloin voidaan myös säästää kuluissa. Virtuaalikoneen valitseminen riippuu paljon tiedon käsittelyn määrästä ja käytöstä, jonka takia virtuaalikoneen käyttötarkoitusta täytyy punnita omien tarpeiden mukaan. Tämän virtuaalikoneen hinnaksi tulee noin 1400 euroa kuukaudessa, kun lasketaan mukaan samat tallennuslevyt kuin halvemmassa vaihtoehdossa. (Pricing calculator n.d.)

Tietomurtotutkintalaitteiden hintavertailu

Azurella on erilaisia hinnoitteluvalintoja virtuaalikoneisiin. Nämä ovat pay as you go, 1 year saving plan ja 3 year saving plan (Windows Virtual Machines Pricing n.d). Hinnoittelua valitessa täytyy tietää virtuaalikoneen käyttötarkoitus ja sen elinkaari. Esimerkiksi kolmen vuoden virtuaalikoneen käytöstä Azure tarjoaa 45 prosenttia alennusta kuluista, mutta se on toisaalta kiinteä hinta, joten jos virtuaalikonetta ei käytetä jatkuvasti, voi pay as you go -malli olla sopivampi tällöin. (Windows

Virtual Machines Pricing n.d.) Alla oleva kaavio havainnollistaa tietomurtotutkintalaitteen eli Lenovon Thinkpad P16 Gen 1 kulut kolmelta vuodelta, joka on kiinteä hinta noin 2400 euroa, sekä Azuren saman virtuaalikoneen kulut eri käyttömäärällä pay as you go -mallilla. Kaavio havainnollistaa kustannukset koneessa, joka on päällä koko kolmen vuoden ajan, koneessa, joka on virka-aikana päällä eli 8 tuntia päivässä, 5 päivää viikossa, sekä koneessa, joka on päällä 2 tuntia päivässä 5 päivää viikossa. Kaaviossa ei huomioida Lenovon tietomurtotutkintalaitteen mahdollisia huoltokuluja tai uuden tietomurtotutkintalaitteen ostamista, jos oletetaan, että Lenovon tietomurtotutkintalaitteen elinkaari päättyy kolmen vuoden päästä (ks. kuvio 16).



Kuvio 16. Tietomurtotutkintalaitteiden hintavertailu kolmen vuoden ajalta

Kuten kuviosta näkee, virtuaalikoneen päällä pitäminen jatkuvasti tuottaa yli 25000 euron kulut kolmessa vuodessa. Sen sijaan toisissa virtuaalikoneissa on huomattavasti pienemmät kustannukset. Virtuaalikone, joka on päällä 2 tuntia ja 5 päivää viikossa, on halvempi vaihtoehto kolmen vuoden ajalta kuin Lenovon tietomurtotutkintalaite. Myös virka-aikana oleva virtuaalikone on halvempi vaihtoehto ensimmäisen vuoden ajan, jonka jälkeen kustannukset kuitenkin nousevat Lenovon laitteesta.

Tietomurtotutkinta-alustaan tarvittavat komponentit ja työkalut

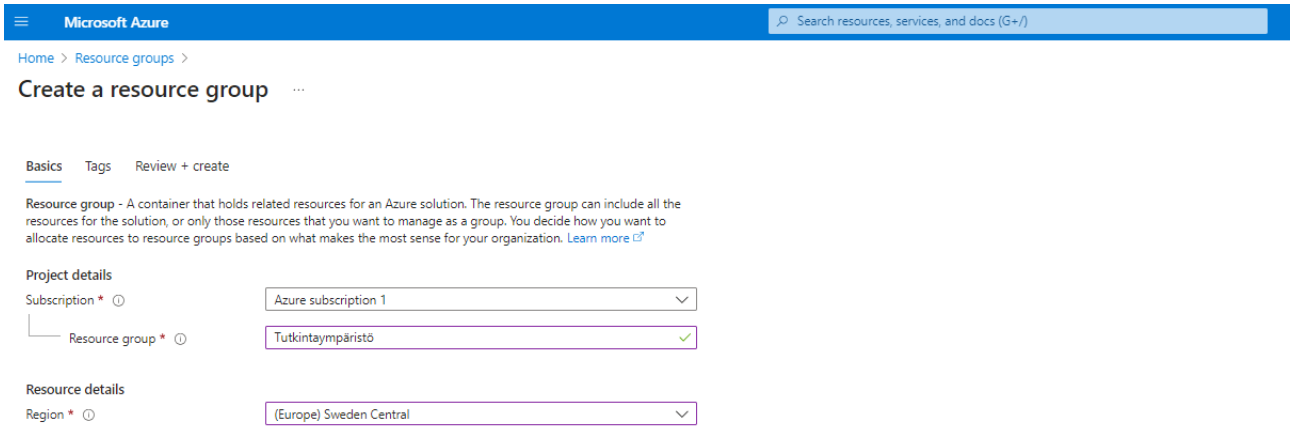
Tietomurtotutkintaan tarkoitettu Azure-tutkinta-alusta, jolla voidaan esimerkiksi analysoida levykuvia, voidaan luoda Microsoftin parhaita menetelmiä käyttäen. Tutkintaan tarkoitettu virtuaalikone tarvitsee Azure-tilauksen, komponentteja ympäristön luomiselle, sekä tiedonsiirtoon tarkoitettuja työkaluja. Azuren luoman ohjeistuksen mukaan virtuaalikone tarvitsee seuraavia komponentteja toimiakseen virtuaaliympäristössä:

- Resurssiryhmän
- Tallennuslevyjä
- Virtuaaliverkon
- Azure Bastionin
- Azure Storage tilin
- Azure Storage Explorerin
- Azure Monitorin
- Azure Backupin
- Defender for Cloudin

(Run a Windows VM on Azure n.d.)

Resurssiryhmä on Azuren palvelu, joka sisältää eri resursseja. Saman elinkaaren omaavat resurssit ovat suositeltavaa pitää samassa resurssiryhmässä, sillä tällöin resursseja voidaan ottaa käyttöön, monitoroida sekä seurata näiden kustannuksia samasta paikasta. Resurssiryhmän poistaminen poistaa kaikki ryhmässä olevat resurssit, mikä on kätevää esimerkiksi erilaisissa testauksissa, joissa ryhmiä luodaan lyhytaikaiseen käyttöön. Resurssiryhmät luodaan Azuren Resource Managerilla, ja tämän kautta käyttäjä pystyy luomaan resurssiryhmiin esimerkiksi virtuaalikoneita, tietokantoja sekä virtuaaliverkkoja. (What is Resource Manager n.d.)

Tässä toteutuksessa resurssiryhmään lisätään kaikki tutkintaympäristöön kuuluvat komponentit, jotta ympäristön hallinnointi olisi mahdollisimman selkeää ja tehokasta. Resurssiryhmä luodaan Azure portaalista hakemalla ”Resource groups”, valitsemalla ”Create”, jonka jälkeen valitaan tilaus, resurssiryhmän nimi sekä sijainti resurssiryhmälle (ks. kuvio 17).



Kuvio 17. Resurssiryhmän luonti

Azure tarjoaa useita erilaisia tallennuslevyjä käyttäjälle virtuaalikonetta luodessa. Tietomurtotutkinnassa on tärkeää, että tutkintalaitteelle on varattu tarpeeksi tilaa työkaluille ja tutkittavalle tiedolle. Työkalut ja tutkittava tieto kannattaa erottaa kahteen eri tallennuslevyyn, jotta tutkinta säilyy selkeänä eikä tieto sekaannu keskenään. Tämän lisäksi on suositeltavaa varata käyttöjärjestelmälle oma levy, jotta järjestelmä pyörii itsenäisesti, eikä tutkinta hidastu samalla levyllä olevien prosessien vaikutuksesta. Käyttöjärjestelmälle Azure suosittelee Premium Storagen käyttöä, jolloin tallennuslevy on solid state drive (SSD) tai puolijohdelevy suomeksi. Työkaluille ja tutkittavalle tiedolle riittää tavallinen kovalevy ja tila näihin allokoidaan tarpeen mukaan. Näiden levyjen lisäksi, virtuaalikoneessa on automaattisesti mukana välimuistilevy, joka sijaitsee virtuaalikoneen fyysisessä levyssä. Tätä levyä kannattaa käyttää vain väliaikaiselle tiedolle, sillä tiedot eivät tallennu Azureen ja ne voivat poistua uudelleenkäynnistyksessä. (Run a Windows VM on Azure n.d.)

Tutkintaympäristöön täytyy luoda erikseen virtuaalinen verkko, jotta ympäristössä olevat virtuaalikoneet voivat kommunikoida keskenään ja käyttäjät pääsevät internetiin. Jotta verkko saadaan toimimaan, pitää käyttäjän määritellä dynaamiset tai staattiset IP-osoitteet, Network interfacen (NIC) ja Network security groupin (NSG). IP-osoitteet tarvitaan virtuaalikoneen kanssa kommunikoimiseen esimerkiksi etäyhteyttä luodessa, Network interface sallii virtuaalikoneiden kommunikoimisen verkon kanssa ja Network security groupin avulla sallitaan tai estetään verkkoliikennettä virtuaalikoneisiin. (Run a Windows VM on Azure n.d.)

Näiden verkkokomponenttien lisäksi turvallisen etäyhteyden luomisen yksityisen IP-osoitteen kautta onnistuu hallitulla Azure Bastion -alustalla. Bastionin avulla virtuaalikone ei tarvitse julkista IP-osoitetta, jonka avulla virtuaalikone on suojassa julkiselta internetiltä. Bastionin avulla voidaan myös luoda turvallinen SSH tai RDP -etäyhteys virtuaalikoneeseen, jolloin tutkija pystyy yhdistämään virtuaalikoneeseen miltä laitteelta tahansa ja mistä tahansa. Tämä ratkaisu tuo joustavuutta tietomurtotutkinnalle. (Run a Windows VM on Azure n.d.)

Azuren Storage tili sisältää kaikki tarvittavat komponentit tiedon säilyttämiseen. Azure tarjoaa neljää eri tallennustilityyppiä: Standard general-purpose v2, Premium block blobs, Premium file shares ja Premium page blobs. Tässä tapauksessa levykuvan säilyttämiseen paras tilityyppi on yleiseen tallennuskäyttöön tarkoitettu Standard general-purpose v2. (Storage account overview 2024.)

Jotta levykuvaa voidaan tutkia Azuren virtuaaliympäristössä, tarvitaan Azuren tarjoamaa pilvitallennusratkaisua, Blob Storagea. Blob Storagea käytetään erilaisten tietojen säilyttämiseen esimerkiksi lokien tai varmuuskopiotietojen säilyttämiseen tai tässä tapauksessa kuvalevytiedoston tallentamiseen ja jakamiseen. (Introduction to Azure Blob Storage 2023.)

Azuressa sijaitsevan tiedon käsittelemiseen on suositeltavaa käyttää Azuren Storage Exploreria. Storage Explorer on ilmainen ohjelma, jonka avulla tutkija voi siirtää tietoa muun muassa Blob storagesta. Storage Explorer on tärkeä ohjelma tietomurtotutkinnassa tapahtuvassa tiedonsiirrossa esimerkiksi levykuvan siirrossa Blob Storagesta virtuaalikoneeseen. Storage Explorer on erillinen ladattava ohjelma, johon kirjaudutaan Azure-tilillä, jotta tietoa voidaan siirtää. (Get started with Storage Explorer 2024.)

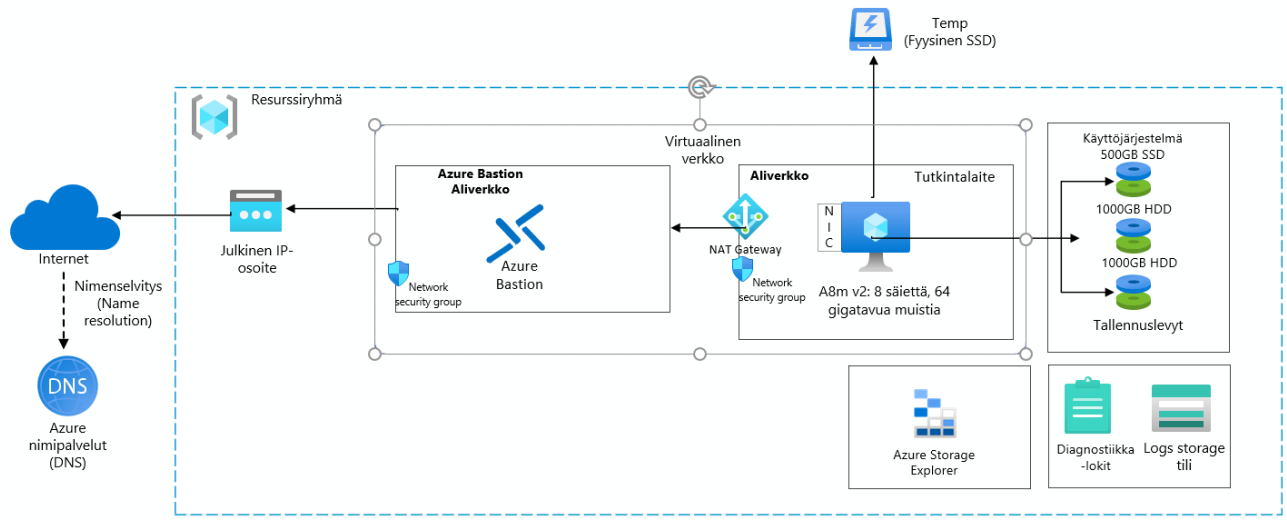
Seuraavaksi käydään läpi virtuaalikoneen turvallisuuteen liittyviä komponentteja. Azure Monitor, Azure Backup ja Defender for Cloud ovat tärkeitä palveluita turvaamaan pilven eri resursseja. Seuraavissa kappaleissa kerrotaan näiden palveluiden perustoiminnoista, mutta virtuaalisen ympäristön suojauksen parantamiseen ei perehdytä työn rajauksen takia sen tarkemmin. On kuitenkin hyvä tietää, että esimerkiksi Defender for Cloud tarjoaa valtavan määrän kyvykkyyksiä, joita voidaan käyttää hyväksi ympäristön koventamisessa.

Tutkintaympäristön monitoroimiseen voidaan hyödyntää Azure Monitoria. Azure Monitor käyttää diagnostiikka- ja monitorointiresursseja, jotka keräävät ympäristöstä erilaisia metriikoita ja lokeja. Azure Monitorilla voidaan monitoroida sovelluksia, virtuaalikoneita, käyttöjärjestelmiä, kontteja, tietokantoja, verkkoliikennettä, tietoturvatapahtumia sekä kustomoituja lähteitä. (Azure Monitor overview 2024.)

Tietomurtotutkintaa tehdessä on tärkeää, että tutkittavaa tietoa ei hävitetä. Azure tarjoaa Backup-palvelua, jonka avulla käyttäjä voi varmuuskopioida virtuaalikoneensa tutkintaympäristössä. Backup-palvelua varten täytyy luoda ”vault” Azuren Backup Centeristä, joka tallentaa varmuuskopiot ja palautumispisteet. Tämän lisäksi varmuuskopioille pitää luoda politiikka, jossa määritellään varmuuskopioinnin ajankohta, säilytysaika sekä politiikkaa koskevat virtuaalikoneet. Microsoftin Quickstart: Back up a virtual machine in Azure (2024) -artikkelista löytyy lisätietoa Backup-palvelusta. (Run a Windows VM on Azure n.d.)

Turvallisen ympäristön varmistamiseksi on suositeltavaa käyttää Microsoftin Defender for Cloudia, joka tarjoaa näkymän ympäristön turvallisuustilanteeseen sekä tarjoaa ominaisuuksia, kuten päivitystenhallinnan ja antivirusohjelman tarkistamisen sekä asentamisen. (Run a Windows VM on Azure n.d.)

Kun kaikki tarvittavat komponentit on huomioitu hallitun tietomurtotutkinta-alustan pystyttämisessä Azuressa, voidaan ympäristöä havainnollistaa alla olevan kuvan mukaisella arkkitehtuurikuvalla (ks. kuvio 18).



Kuvio 18. Referenssiarkkitehtuuri tietomurtotutkinta-alustasta Azuren pilviympäristössä (Run a Windows VM on Azure n.d, muokattu)

Referenssiarkkitehtuuri kuvastaa virtuaalista Azuren ympäristöä, jossa virtuaalikone on osana virtuaaliverkon aliverkkoa. Tähän aliverkkoon saadaan yhteys Azure Bastionin kautta, johon käyttäjä voi yhdistää RDP tai SSH -etäyhteyden avulla. Tämä ratkaisu segmentoi myös verkkoa hieman, eristämällä virtuaalikoneen yksityiseen verkkoon. Kuvasta näkee myös Azure Storage Explorerin, jonka avulla esimerkiksi levykuvia saadaan siirrettyä Blob Storagesta virtuaalikoneen tallennuslevyyn, sekä lokienhallinnan, joka kerää tietoa ympäristöstä. Arkkitehtuurikuva havainnollistaa esimerkkiratkaisua tietomurtotutkinta-alustasta Azuressa ja se ei ota huomioon turvallisuuteen liittyvien palveluiden kuten Defender for Cloudia tai identiteetinhallintaan kuuluvaa Entra ID:tä. Nämä palvelut ovat kuitenkin hyvä huomioida, kun suunnitellaan ympäristön turvallisuutta ja kun mietitään millä käyttäjillä on esimerkiksi oikeudet tiedonsiirtoon.

6 Pohdinta

Tutkimuksen tarkoituksena oli selvittää, mitä organisaation tarvitsee tietää, jotta hallittu tietomurtotutkinta-alusta pystytään luomaan Azure-pilviympäristöön. Tutkimuksessa käsiteltiin yleisesti pilvipalvelumalleja, pilvipalveluntarjoajia ja näiden tarjoamia viitekehyksiä pilvitransformaatiossa sekä käsiteltiin tietomurtojen tutkintaan liittyviä metodologioita, prosesseja sekä työkaluja. Tämän lisäksi tutkimuksessa käsiteltiin Azuren eri palveluja ja resursseja, joita tarvitaan tietomurtotutkinta-alustan pystyttämisessä, sekä tuotiin esille pilviympäristön tuomia hyötyjä ja haittoja. Työssä tutkittiin eri kannettavien tietokoneiden vertailun avulla, miten analysointivaiheen prosessit vaikuttavat laitteiden suorituskykyyn, jonka perusteella voitiin päätellä, minkälaisen Azuren virtuaalikoneen tutkija tarvitsee tietomurtotutkintaan. Tuloksena saatiin listaus tarvittavista komponenteista ympäristön luomiseen sekä kuvattiin minkä takia kyseisiä komponentteja tarvitaan. Tämän lisäksi luotiin arkkitehtuurikuva ympäristöstä, joka havainnollistaa kokonaisuutta ja tuo selkeyttä toteutukseen.

Tutkimuksessa onnistuttiin käsittelemään tutkintalaitteiden suorituskykyjen vaihtelua ja Azuren virtuaalikoneiden sekä komponenttien kustannuksia. Tämän lisäksi työssä korostettiin virtuaalikoneiden käyttötarkoituksien merkittävyyttä tietomurtotutkinnassa antamalla vaihtoehtoinen va-

linta nopeammalle virtuaalikoneelle, jossa huomioitiin kuitenkin sen kalliimmat kustannukset. Tutkimuksessa tutkittiin sekä vertailtiin tietomurtotutkintaan tarkoitetun Lenovo-kannettavan kustannuksia valittuun Azuren virtuaalikoneeseen kolmen vuoden ajalta. Tässä huomioitiin Azuren tarjoamien eri hinnoitteluvalintojen merkitys kustannuksiin ja tätä vertailua havainnollistettiin kaaviolla. Lopuksi työssä luotiin onnistuneesti havainnollistava esimerkkitoteutus tietomurtotutkinta-alustasta Azuressa käyttäen apuna ajankohtaisia komponentteja ja palveluita sen luomiseen.

Tutkimuksessa olisi voinut vielä esittää tarkempaa ohjeistusta komponenttien asentamisesta, mutta Azure-tilauksen hankkiminen ja komponenttien luominen olisi aiheuttanut liian paljon kustannuksia. Ilmaisversiotakaan ei pystytty käyttämään aikaisempien kokeilujen jälkeen, jonka takia tutkimus jäi ylätason ohjeistukseen komponenttien listauksesta. Tämän takia myöskään ympäristön toimivuutta ei voitu vahvistaa käytännön tekemisellä.

Tämänkaltaisen ympäristön puute on esitetty töissä, jonka takia tutkimuksen tulokset tuovat arvoa auttamalla luomaan ympäristö sisäiseen testikäyttöön ja tuloksia voidaan myös hyödyntää esimerkkiympäristön esittämisessä asiakastyössä havainnollistamalla ympäristöä ja sen vaatimuksia asiakkaalle. Tämän lisäksi tutkintalaitteiden vertailu suorituskyvyistä ja kustannuksista antaa paremman käsityksen virtuaalikoneiden ja paikallisen tietomurtotutkintalaitteen eroavaisuuksista, joka voi auttaa virtuaalikonetta valitessa sekä asiakasneuvonnassa. Tutkimusta voidaan soveltaa myös muihin palveluntarjoajiin kuten AWS:ään tai Google Cloudiin, sillä palvelut ovat näillä samankaltaisia.

Tutkimusta voidaan jatkossa kehittää lukuisilla eri tavoilla. Ympäristön ohjeistusta voidaan laajentaa luomalla ympäristö käytännössä, pureutumalla paremmin eri palveluihin, kuten Azure Storage Exploreriin tai Storage tilin hallintaan. Tämän lisäksi tietomurtotutkinta-alustan koventamista voidaan tutkia tarkemmin hyödyntämällä Azuren tarjoamia palveluita kuten Defender for Cloudia.

Tämän lisäksi tutkimusta voitaisiin jatkokehittää tutkimalla organisaation koon merkitystä ympäristön luomisessa. Samankaltainen ohjeistus voitaisiin tehdä myös muihin pilvipalveluihin esimerkiksi AWS:ään ja Google Cloudiin ja tässä voitaisiin myös selvittää, miten tietomurtotutkintaa tehtäisiin eri pilvipalveluiden välillä. Viimeisenä jatkokehityksenä voitaisiin tutkia tietomurtotutkintamene-

telmien kehityksen seuraavaa vaihetta, jossa tutkinta on siirtynyt täysin pilveen. Tällöin tietoa analysoidaan käyttämällä hyödyksi ainoastaan pilvipalvelun resursseja, kuten Log Analyticsia, kontteja ja Blob Storagea ja tässä ratkaisussa ei ole virtuaalikoneita ja palvelimia ollenkaan käytössä.

Lähteet

Alibaba Cloud. N.d. Alibaba Cloudin etusivut. Viitattu 14.8.2024. https://www.alibabacloud.com.

Artrebultan. 2024. The MFT: The Forensic Investigator's Secret Weapon. Artikkeli Mediumin sivuilta. Viitattu 26.5.2024. https://medium.com/@artrebultan/the-mft-the-forensic-investigators-secret-weapon-e14d678122bd.

Autopsy User Documentation 4.5.0. 2018. Autopsy-työkalun dokumentaatio. Viitattu 4.6.2024. https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/ingest_page.html.

Autopsy User's Guide. 2015. Autopsy-työkalun ohjeistukset. Viitattu 26.5.2024. https://sleuthkit.org/autopsy/docs/user-docs/3.1/index.html.

AWS Cloud Adoption Framework. Pilvipalvelupohjaisen digitalisaation kiihdyttäminen. 2021. AWS:n julkaisu. Viitattu 7.3.2024. https://d1.awsstatic.com/whitepapers/International/fi/aws-cloud-adoption-framework_fi-FI.pdf.

AWS Organizations terminology and concepts. N.d. AWS:n dokumentaatio. Viitattu 7.3.2024. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html.

Azure Monitor Overview. 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 13.6.2024. https://learn.microsoft.com/en-us/azure/azure-monitor/overview.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. 2012. Computer Security Incident Handling Guide. Julkaisu oppaasta NIST:n sivuilla. Viitattu 15.2.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Cloud computing with AWS. N.d. Artikkeli AWS:n sivustolta. Viitattu 4.2.2024. https://aws.amazon.com/what-is-aws/.

Cloud Spending Growth Rate Slows But Q4 Still Up By $10 Billion from 2021; Microsoft Gains Market Share 2023. Artikkeli Synergy Research -sivuilta. Viitattu 16.5.2024. https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share.

Cost of a Data Breach Report 2023. 2023. Raportti IBM:n sivuilta. Viitattu 15.2.2024. https://www.ibm.com/reports/data-breach.

CPU Benchmarks. N.d. Viitattu 30.7.2024. PassMark Softwaren CPU benchmark -sivusto. https://www.cpubenchmark.net.

Deloitte. N.d. Deloitte-yrityksen kotisivut. Viitattu 18.1.2024. https://www2.deloitte.com/fi/fi/pages/careers/solutions/Deloitte-lyhyesti.html.

Digital Forensics Certifications. Sertifikaattisivu SANS:lta. Viitattu 14.8.2024. https://www.sans.org/cyber-security-certifications/digital-forensics-certifications/.

Getting Started with the AWS Management Console. N.d. Viitattu 7.3.2024. https://aws.amazon.com/getting-started/hands-on/getting-started-with-aws-management-console/.

Get started with Storage Explorer. 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 13.8.2024. https://learn.microsoft.com/en-us/azure/storage/storage-explorer/vs-azure-tools-storage-manage-with-storage-explorer?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json&tabs=windows.

How does Azure work? 2023. Artikkeli Microsoftin sivustolla. Viitattu 3.2.2024. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/what-is-azure.

How to Calculate the Cost of a Data Breach. 2021. Artikkeli Ekranin sivuilla. Viitattu. 15.2.2024. https://www.ekransystem.com/en/blog/cost-of-a-data-breach.

Incident Response Reference Guide. N.d. Ohjeistus Microsoftin sivuilta. Viitattu 17.2.2024. https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf.

Introduction to Azure Blob Storage. 2023. Artikkeli Microsoftin sivuilta. Viitattu 23.7.2024. https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction.

Kent, K., Chevalier, S., Grance, T. & Dang, H. 2016. Guide to Integrating Forensic Techniques into Incident Response. NIST:n ohjeistus. Viitattu 1.3.2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

Kral, P. Incident Handler's Handbook. 2011. Häiriönhallinnan ohjeistus. Viitattu 17.2.2024. https://sansorg.egnyte.com/dl/6Btqoa63at.

Luttgens, J. T., Mandia, K. & Pepe, M. Incident Response & Computer Forensics. 2016. McGraw-Hill.

Online Shop - The Forensic Tools to Meet Your Needs. N.d. Sumuri-verkkokauppa. Viitattu 10.4.2024. https://sumuri.com/product-category/categories/workstation/?orderby=menu_order.

OpenText EnCase Forensic. N.d. OpenTextin dokumentti Encase-työkalusta. Viitattu 1.8.2024. https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encase-forensic-en.pdf.

Optimizing Performance. 2019. Viitattu 5.6.2024 https://sleuthkit.org/autopsy/docs/user-docs/4.11.0/performance_page.html.

OSFMount. N.d. OSFMount -työkalun etusivu PassMark Software sivuilta. Viitattu 30.4.2024. https://www.osforensics.com/tools/mount-disk-images.html.

Pricing calculator. N.d. Microsoftin työkalu. Viitattu 13.5.2024. https://azure.microsoft.com/en-gb/pricing/calculator/.

Run a Windows VM on Azure. N.d. Artikkeli Microsoft Learn -sivuilta. Viitattu 10.6.2024. https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/windows-vm.

Smiths, J. 2020. The case of the stolen Szechuan sauce. Laboraatio DFIRMadness-sivuilta. Viitattu 22.5.2024. https://dfirmadness.com/the-stolen-szechuan-sauce/.

Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings. 2023. Artikkeli Microsoft Learn -sivuilta. Viitattu 9.2.2024. https://learn.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings?view=o365-worldwide.

Virtual machines in Azure. 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 29.4.2024. https://learn.microsoft.com/en-us/azure/virtual-machines/overview.

Virtual machine series. N.d. Esittelysivu Azuren virtuaalikonesarjoista. Viitattu 15.8.2024. https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/.

What are IaaS, PaaS and SaaS? N.d. Artikkeli IBM:n sivustolla. Viitattu 31.1.2024. https://www.ibm.com/topics/iaas-paas-saas.

What is a data breach? N.d. Artikkeli Cloudflaren sivuilta. Viitattu 15.2.2024. https://www.cloudflare.com/learning/security/what-is-a-data-breach/.

What is Computer Forensics? N.d. Blogi-julkaisu National Universityn sivuilta. Viitattu 22.3.2024. https://www.nu.edu/blog/what-is-computer-forensics/.

What is a cloud service? N.d. Artikkeli Citrixin sivustolta. Viitattu 31.1.2024. https://www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html.

What is a cloud service? N.d. Artikkeli Citrixin sivuilta. Viitattu 31.1.2024. https://www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html.

What is Microsoft Entra ID? 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 10.2.2024. https://learn.microsoft.com/en-us/entra/fundamentals/whatis.

What is Resource Manager? 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 10.6.2024. https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview.

What is the Azure Portal? 2024. Artikkeli Microsoft Learn -sivuilta. Viitattu 29.2.2024. https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-overview.

What is the Microsoft Cloud Adoption Framework for Azure? 2023. Artikkeli Microsoft Learn -sivuilta. Viitattu 8.2.2024. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/overview.

What is Virtualization? N.d. Artikkeli AWS:n sivuilta. Viitattu 3.2.2024. https://aws.amazon.com/what-is/virtualization/.

What is AWS Organisations? N.d. Käyttäjäopas AWS:n sivuilta. Viitattu 7.3.2024. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html.

Windows Artifact Analysis. 2013. SANS:n julkaisema juliste. Viitattu 28.3.2024. https://networkforensic.dk/Tools/Files/cheat-sheets/Poster_Find_Evidence.pdf.

Windows Virtual Machines Pricing. N.d. Tietoa Azuren virtuaalikoneiden hinnoitteluista. Viitattu 4.9.2024. https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/#pricing.

Zimmerman, E. Eric Zimmerman tools N.d. MFT-jäsentämisen työkalu. Viitattu 26.5.2024. https://github.com/EricZimmerman/MFTECmd.