Jouni Vaahtera

PILVIPALVELUIDEN KYBERTURVALLISUUSUHKIEN AUTOMAATTISTEN HAVAINNOINTIKYVYKKYYKSIEN KEHITTÄMINEN KANSALLISEN TASON HAVAINNOINTIA VARTEN

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

South-Eastern Finland University of Applied Sciences

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä/Tekijät	Jouni Vaahtera
Työn nimi	Pilvipalveluiden kyberturvallisuusuhkien automaattisten havainnointikyvykkyyksien kehittäminen kansallisen tason havainnointia varten
Toimeksiantaja	Liikenne- ja viestintävirasto Traficom
Vuosi	2022
Sivut	56 sivua, liitteitä 3 sivua
Työn ohjaajat	Vesa Kankare, Kimmo Kääriäinen

TIIVISTELMÄ

Tässä kehittämistietoa tuottavassa opinnäytetyössä pyrittiin selvittämään, miten suomalaisten yritysten ja virastojen käyttämien pilvipalveluympäristöjen kyberturvallisuudesta voidaan kerätä tietoa ja muodostaa tilannekuvaa. Tilannekuva on ollut puutteellinen, koska käytössä ei ole ollut automaattisia havainnointivälineitä uhkien havainnoimiseksi ja niihin reagoimiseksi. Tavoitteena oli selvittää, miten löydetyt havainnointikeinot palvelevat Kyberturvallisuuskeskuksen tehtävää kokonaistilannekuvan muodostamisessa. Tavoitteena oli myös, että keinot olisivat hyödynnettävissä laaja-alaisesti suomalaisessa huoltovarmuuskriittisessä yritys- ja yhteisökentässä.

Tutkimuksessa käytettiin kahta eri tutkimusmenetelmää: teemahaastattelua ja kehittämistutkimusta. Teemahaastatteluissa selvitettiin, mitä menettelyitä ja työkaluja organisaatiot käyttävät pilvipalveluiden kyberturvallisuuden uhkien ja tapahtumien havainnointiin. Haastatteluun osallistui huoltovarmuuskriittisiä organisaatioita useilta eri toimialoilta. Teemahaastattelun tulosten avulla rajattiin tutkimuskohdetta sekä valittiin kehittämistutkimusosuuden kokeilukohde. Kehittämistutkimuksella selvitettiin käytännönläheistä ratkaisua tutkimusongelmaan. Siinä suunniteltiin ja toteutettiin työkalu kyberturvallisuusriskien havainnointiin. Kokeilussa haettiin tietoja organisaatioiden Microsoft Azure -ympäristöjen turvallisuuteen vaikuttavien asetusten tilasta ja verrattiin tietoja ennalta määriteltyihin suositeltaviin arvoihin. Toteutettua työkalua testattiin aidoissa tuotantoympäristöissä.

Tutkimustuloksissa löydettiin automatisoitavia keinoja havainnoida eri organisaatioiden käyttämien Microsoft Azure -ympäristöjen kyberturvallisuuden tilaa. Kokeilun tulokset osoittavat, että keskitetysti toteutettu automaattinen asiakasympäristöjen tietoturvatarkastelu on mahdollista toteuttaa. Toteutettua työkalua on mahdollista laajentaa havainnoimaan uusia ja muuttuvia uhkia. Aihe vaatii jatkotutkimusta, sillä tilannekuvan muodostaminen ei työkalun avulla ole mahdollista ilman asiantuntija-analyysiä. Yleisempi tilannekuva pilvipalveluiden turvallisuudesta edellyttää havainnointimenetelmien kehittämistä myös muita tuotealustoja ja käyttökonsepteja varten.

Asiasanat: kyberturvallisuus, pilvipalvelut, tilannekuva

South-Eastern Finland University of Applied Sciences

Degree title	Master of Engineering
Author (authors)	Jouni Vaahtera
Thesis title	Development of automated capabilities for the national level cyber security threat detection of cloud services
Commissioned by	Finnish Transport and Communications Agency Traficom
Time	2022
Pages	56 pages, 3 pages of appendices
Supervisor	Vesa Kankare, Kimmo Kääriäinen

ABSTRACT

The aim of this thesis, which produces development information, was to study how to collect data and form cyber security situational awareness of cloud services used by Finnish companies and agencies. The situational awareness has been inadequate because of the lack of automated tools for cyber threat detection and reaction. The goal was to find out how the found means of observation support the mission of the National Cyber Security Center in situational awareness reporting. In addition, it was necessary that the results should be widely applicable among the national emergency supply organizations in Finland.

Two research methods, semi-structured interview and design-based research were used in this study. Information about the methods and tools currently used by corporations in the detection of cyber security threats and incidents in cloud services were collected through interviews. Fourteen national emergency supply organizations from various lines of businesses were interviewed. The study objectives were narrowed with semi-structured interviews, and the target of the practical experiment was selected. The practical solution to the research problem was developed with design-based research. In the experiment phase of this study the tool for detecting risky cyber security configurations was developed and tested. During the experiment the data about the status of some security configurations were collected from Microsoft Azure environments of different parties. Results were compared to advisable values. The tool developed was tested in production environments.

As a result, the feasible means to collect the cyber security data from organizations' Azure environments were found. Results indicate that automated and centralized data collection of several customer environments simultaneously is possible. The tool developed and tested can be easily expanded to detect new and changing threats. There is a need for additional research since situational awareness based on collected data is not possible without additional expert analysis. The development of detection tools for different cloud service technologies and use cases is also needed to reach more general situational awareness.

Keywords: cloud services, cyber security, situational awareness

SISÄLLYS

1 JOHDANTO

Turvallisella digitaalisella toimintaympäristöllä on tärkeä rooli suomalaisen yhteiskunnan ja elinkeinoelämän digitalisaation onnistumisessa. Kyberturvallinen toimintaympäristö tuo luotettavuutta, jatkuvuutta ja turvaa. Se on myös kansainvälinen kilpailutekijä liiketoimintaansa digitalisoiville aloille sekä kyberturvallisuusalan osaajille. Yhteistyötä tarvitaan, sillä turvallisuuden osaamisalue on liian monimutkainen yksinäisille toimijoille. Kyberturvallinen toimintaympäristö voidaan varmistaa vain eri toimijoiden tietojenvaihdolla ja yhteistyöllä. (Karjaluoto ym. 2019.)

Huoltovarmuus tarkoittaa kriiseihin ja häiriötilanteisiin varautumista ja jatkuvuudenhallintaa. Näillä hallintakeinoilla turvataan elintärkeät toiminnot, jotta yhteiskunta ja elinkeinoelämä toimivat luotettavasti ja ihmiset voivat turvallisesti elää arkeaan. Yhteiskunnan huoltovarmuuden kannalta keskeisten yritysten ja organisaatioiden tulee ottaa jatkuvuudenhallinnassaan huomioon niihin kohdistuvat kyberuhat. Niiden tulee ylläpitää tarvittavaa suojautumis- ja reagointikykyä. Huoltovarmuuskeskus ja muu huoltovarmuusorganisaatio tukevat toimintaa selvityksin, ohjeistuksin ja koulutuksella. (Lehto ym. 2018.)

Yhteiskunnallisesti kyberturvallisuuden kehittämistarvetta lisää kyberriskien torjunnan tarpeen ja merkityksen kasvaminen digitalisaation edetessä (Karjaluoto ym. 2019). Erityisesti pilvipalveluiden rooli ja merkitys kasvaa digitalisaation myötä. Niitä käytetään organisaatiossa yhä arkipäiväisemmin ja laajemmin. Käyttö tulee kasvamaan edelleen runsaasti. Liiketoimintajohdolle tutkimus- ja neuvontapalveluja tuottava Gartner (2021) arvioi, että pilvipalveluihin käytetty budjetti kasvaa 23 % vuonna 2021. Toisaalta Canalys-tutkimuskeskus (2021) arvioi, että vuodesta 2018 eteenpäin käytetty budjetti on kasvanut vuositasolla 35–45 prosenttia.

Pilvipalveluita käytettäessä yrityksen tietoja käsitellään ja säilytetään sen ulkopuolella palveluntarjoajan konesaleissa. Tietoja siirretään sieltä käyttäjille julkisen internetin yli. Pilvipalveluiden tuottajat jakavat palvelualustastaan kapasiteettia jopa miljoonille asiakkaille samalla tavalla. Näiden seikkojen takia pilvipalveluiden käyttö synnyttää uusia riskejä ja uhkia, joiden havainnointiin perinteiset menetelmät ja työkalut eivät täysin sovi. Kaikissa pilvipalveluluokissa

suurin markkinaosuus on isoilla kansainvälisillä toimijoilla (Canalys 2021). Tämä muodostaa yhden uusista riskeistä, kun merkittävä osa digi-infrastruktuuria on ulkomaisessa hallinnassa, eikä uskottavia kotimaisia vaihtoehtoja ole. Se on kyberuhkiin varautumisen ja ongelmatilanteista toipumisen eli kyberresilienssin kannalta haitallista (Lehto ym. 2018).

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus (KTK) on kansallinen tietoturvaviranomainen. Se kerää tietoa, ennaltaehkäisee ja selvittää suomalaisiin viranomaisiin ja elinkeinoelämään kohdistuvia tietoturvaloukkauksia sekä tiedottaa merkittävistä tietoturvauhkista. Kyberturvallisuuskeskuksen tehtävänä on muodostaa tilannekuvaa kyberturvallisuuden tilasta Suomessa. Tilannakuvatietoa käytetään mm. päätöksentekoon, viestinnän ja neuvonnan kohdentamiseen sekä erilaisten tilannekuvatuotteiden laatimiseen – esimerkkinä KTK:n Kybersää-raportti.

KTK:n näkökulmasta sen näkymä pilvipalveluiden kyberturvallisuuden kokonaistilanteeseen tulisi olla nykyistä parempi. Käytössä olevat välineet eivät tue tilannekuvan keruuta asiakkaiden pilviympäristöistä. On kehitettävä uusia kyvykkyyksiä tätä tehtävää varten.

Tässä kehittämistietoa tuottavassa opinnäytetyössä pyritään selvittämään, miten suomalaisten yritysten ja virastojen käyttämien pilvipalveluympäristöjen kyberturvallisuuden tilannekuvatietoa voidaan kerätä automatisoidusti. Tutkimus toteutettiin Liikenne- ja viestintäviraston kyberturvallisuuskeskukselle vuosina 2021–2022. Tutkimuksessa hyödynnettiin Kyberturvallisuuskeskuksen sidosryhmiä lähtötilanteen selvittämisessä, kehittämisosuuden koeryhmänä sekä tulosten arvioinnissa.

Opinnäytetyön tavoitteena on selvittää, mitä on tehtävä, jotta pilviturvallisuuden tilannekuvan muodostamista voitaisiin automatisoida. Tavoitteena on myös tarkastella, miten voidaan hyödyntää organisaatioissa jo käytössä olevia pilviturvallisuuden työkaluja ja menetelmiä. Pyrkimyksenä on löytää teknisiä keinoja, jotka voisivat palvella Kyberturvallisuuskeskuksen tilannekuvan muodostamiseksi tarvittavan tiedon keruuta erityisesti pilvipalveluista. Tavoitteena on, että löydetyt keinot olisivat hyödynnettävissä laaja-alaisesti suomalaisissa huoltovarmuuskriittisissä organisaatioissa.

Tutkimuksen toteuttamisessa käytetään monistrategista tutkimusotetta, jossa hyödynnettiin peräkkäin kahta eri menetelmää: teemahaastattelua ja kehittämistutkimusta. Teemahaastattelut tehtiin kesällä 2021 ja niiden avulla koottiin ensin primääriaineisto ja pyrittiin rajaamaan tutkimuskohdetta sekä selkeyttämään kehittämistutkimuksen kokeilukohdetta. Teemahaastatteluihin osallistui 14 suomalaista eri toimialoja edustavaa yritystä tai virastoa. Toisessa vaiheessa kehittämistutkimuksella kokeiltiin käytännön ratkaisua tutkimusongelmaan. Kokeilu suunniteltiin syksyllä 2021 ja varsinainen kokeiluvaihe toteutettiin alkuvuodesta 2022. Kokeilun tuloksia arvioidaan suhteessa tavoitteisiin ja tutkimuskysymyksiin sekä tehdään johtopäätökset.

2 TUTKIMUSASETELMA

2.1 Tutkimusongelma ja tavoitteet

Tämän tutkimuksen tutkimusongelmana on suomalaisten yritysten- ja yhteisöjen käyttämien pilvipalveluiden kyberturvallisuuden puutteellinen kokonaistilannekuva kansallisella tasolla. Tilannekuva on puutteellinen, koska yhteiskunnan tasolla ei ole käytössä automattisia havainnointivälineitä uhkien havainnoimiseksi ja niihin reagoimiseksi. Kokonaiskuvaa muodostetaan tällä hetkellä pääosin käsityönä ja epävirallisesti sidosryhmien asiantuntijoiden välisessä vuorovaikutuksessa. Tämä on hidasta ja epätäydellistä. Puutteet eivät koske ainoastaan pilvipalveluita, vaan jossain määrin myös muuta tilannekuvan muodostamista. (Valtiontalouden tarkastusvirasto 2017; Lehto ym. 2018.)

Tilannekuvan sisällöstä tai käyttötarkoituksesta ei myöskään vallitse yksimielisyyttä. Siihen liittyy ratkaisemattomia kysymyksiä siitä, minkä tyyppistä tietoa tarvitaan, kenelle sitä jaetaan ja millä syklillä. Toisaalta kaivataan nopeatempoista välinettä akuutteihin reagointitilanteisiin, toisaalta taas analysoitua tietoa uhkista sekä tapahtuneista ja torjutuista häiriöistä ratkaisumalleineen. (Lehto ym. 2018.)

Turvallisuuskomitean laatimassa Suomen kyberturvallisuusstrategiassa on määritelty kehittämisohjelma, jonka tavoitteena on parantaa kansallisen kyberturvallisuuden kokonaistilaa. Tähän kehittämisohjelmaan liittyen on Kybertur-

vallisuuskeskuksen tehtäväksi annettu kehittää edelleen viranomaisten ja elinkeinoelämän yhteistyötä sekä keskuksen kykyä ympärivuorokautisen tilannekuvan kokoamiseksi. Tavoitteena on edistää Suomen kykyä tunnistaa tietoturvauhkia ja varoittaa niistä sekä parantaa elinkeinoelämän ja julkishallinnon mahdollisuuksia varautua tietoturvauhkiin. (Turvallisuuskomitea 2019.)

Kyberturvallisuuskeskus tekee yhteistyötä huoltovarmuusorganisaation ja siihen kuuluvien toimijoiden kanssa. Se koordinoi useita toimialakohtaisia tietoturva-asioiden tiedonvaihtoryhmiä (*Information Sharing and Analysis Centre*, ISAC) yhteistyössä toimialojen valvontaviranomaisten kanssa. Ryhmien kautta jaetaan tietoa luottamuksellisesti, kehitetään osaamista sekä muodostetaan kokonaistilannekuvaa. Vastaava tiedonvaihtoryhmä toimii myös valtionhallinnon sisällä eri virastojen välillä ja sitä kutsutaan nimellä *Virtual Incident Response Team* (VIRT).

Kyberturvallisuuskeskus palvelee huoltovarmuuskriittisiä toimijoita ja valtionhallintoa tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVAROn avulla. Järjestelmän avulla organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä. KTK varoittaa asiakkaita tekemiensä havaintojen perusteella sekä koostaa tilannekuvaa ja raportoi tietoturvatilanteesta (Traficom 2020a). Selvityksien mukaan tämä palvelu on hyvin arvostettua elinkeinoelämän keskuudessa (Lehto ym. 2018). Pilviturvallisuuden automaattinen havainnointi on vasta kehittymässä. Automaattisia havainnointikyvykkyyksiä ei ole toistaiseksi juuri ollenkaan, joten tilannekuvan muodostaminen on hyvin puutteellista.

Hallinnollisen kyberturvallisuuden puolella on jonkin verran edistytty. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) on Kyberturvallisuuskeskuksen tuottama pilvipalveluiden turvallisuuden arviointikriteeristö, jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa (Traficom 2020b). Ensimmäinen versio PiTuKrista on julkaistu vuonna 2019 ja sitä on päivitetty vuonna 2020. Pilvipalveluiden huomioimisessa on edelleen kehittämisen varaa. Kyberturvallisuuskeskus on tuottanut laajan ja monipuolisen Kybermittari-arviointityökalun yritysten ja organisaatioiden käyttöön. Tässä työkalussa pilvipalvelut

ja -teknologiat mainitaan vain muutamassa kohdassa, eikä nimenomaisia pilviturvallisuuteen liittyviä käytäntöjä ole mainittu (Traficom 2020c).

Tämä tutkimus on kehittämistutkimus, jossa tavoitteena on löytää keinoja automatisoituun pilvipalveluiden kyberuhkien havainnointiin. Niiden tulee olla riittävän laajasti huoltovarmuuskriittisessä yrityksissä ja yhteisöissä käyttöönotettavissa, jotta saavutetaan kokonaistilannekuvan muodostamiseksi tarvittava kattavuus. Keinojen tulee olla automatisoitavissa uhkatiedon keruun osalta. Lisäksi niiden tulee olla integroitavissa Kyberturvallisuuskeskuksen muihin kansallista kyberturvallisuuden tilannekuvaa muodostaviin järjestelmiin. Onnistuessaan tavoitteiden saavuttamisella on yhteiskunnallista vaikuttavuutta, koska kehitettyjen keinojen avulla voidaan ryhtyä parantamaan Kyberturvallisuuskeskuksen havainnointipalvelua.

Tutkimuskysymyksinä ovat

1. Mitä keinoja on käytettävissä, jotta pilvipalveluiden kyberturvallisuuden uhkia ja poikkeamia voidaan havainnoida automatisoidusti ja olemassa olevia työkaluja käyttäen?
2. Mitkä havainnointikeinoista ovat hyödynnettävissä laaja-alaisesti suomalaisessa huoltovarmuuskriittisessä yritys- ja yhteisökentässä?
3. Miten pilvipalveluiden havainnointikeinot palvelevat Kyberturvallisuuskeskuksen tehtävää kyberturvallisuuden kokonaistilannekuvan muodostamiseksi?

Tutkimus on rajattu selvittämään pilviturvallisuuden tilannetiedon keräämiseen liittyviä teknisiä ja toiminnallisia kysymyksiä. Tilannekuvan muodostamiseen liittyy em. lisäksi myös juridisia ja toimivaltakysymyksiä, sillä toimivaltuuksien puute estää osin toimijoiden välistä yhteistyötä (Lehto ym. 2018). Tätä ongelmaa on hyvä selvittää muissa tutkimuksissa.

2.2 Käytetyt tutkimusmenetelmät

Tässä tutkimuksessa käytetään kahta eri tutkimusmenetelmää: teemahaastattelua ja kehittämistutkimusta. Teemahaastattelun avulla pyritään rajaamaan tutkimuskohdetta sekä selkeyttämään kehittämistutkimuksen kokeilukohdetta. Tämän jälkeen kehittämistutkimuksella selvitetään käytännönläheistä ratkaisua tutkimusongelmaan.

Aineistokeruumenetelmänä tutkimuksessa käytetään kirjallisuustutkimusta sekä teemahaastatteluja. Kirjallisuustutkimuksessa selvitetään pilvipalveluiden kyberturvallisuuden havainnoinnista tehdyssä tutkimuksessa löydettyjä ratkaisuja tutkimuskysymyksiin. Lisäksi tarkastellaan kyberturvallisuuteen liittyviä standardeja, valtionhallinnon ohjeita, tietoturvan kansainvälisten ja kotimaisten asiantuntijafoorumien ja -järjestöjen julkaisuja sekä pilvipalveluntuottajien ohjeita ja dokumentaatiota.

2.2.1 Teemahaastattelu

Teemahaastattelulla selvitetään, mitä menettelyitä ja työkaluja organisaatiot käyttävät pilvipalveluiden kyberturvallisuuden uhkien ja tapahtumien havainnointiin. Teemahaastattelun käytön perusteluna on tutkimuksen reliabiliteetin ja validiteetin varmistaminen. Haastatteluissa saatujen vastausten perusteella voidaan varmistaa, että tutkimuksen kokeiluosuudessa tehtävä kokeilu kohdistuu sellaiseen pilvipalveluun ja teknologiaan, jolla on potentiaalisesti eniten vaikuttavuutta. Kokeiluun valittavia keinoja arvioidaan kriteeristöllä: arvioitu uhkien havainnointikyky, laajamittainen hyödynnettävyys yrityskentässä, aineiston keruun automatisoitavuus sekä integroitavuus Kyberturvallisuuskeskuksen muihin kokonaistilannekuvan muodostamiseksi käytettyihin palveluihin.

Teemahaastatteluun osallistuvat organisaatiot kootaan useilta eri toimialoilta ja kokoluokista. Yhteinen nimittäjä haastatelluille organisaatioille on, että ne edustavat huoltovarmuuskriittisiä toimialoja Suomessa. Haastateltavat henkilöt ovat kyberturvallisuudesta vastaavia ja kyberturvallisuusasiantuntijoita omissa organisaatioissaan. Haastateltavat ovat vapaaehtoisia ja heidät rekrytoidaan tämän tutkimuksen tilaajan omien verkostojen kautta markkinoimalla tutkimusta sekä kannustamalla osallistumaan ja siten vaikuttamaan. Haastateltavat pyritään hankkimaan siten, että pilvipalveluiden hyödyntämisen laajuus ja kypsyystaso organisaatioiden välillä olisi mahdollisimman vaihteleva. Haastateltavien joukon laajuus on kuitenkin rajallinen – noin 10–15 organisaatiota – vähentäen jonkin verran monimuotoisuutta. Kerätyn aineiston saturaatiota kyetään kuitenkin arvioimaan jo näinkin pienen joukon kesken.

Teemahaastattelu on kvalitatiivinen tutkimusmenetelmä. Sitä käytetään, kun tutkimusongelmana on ilmiö, jota ei voida tutkia määrällisellä tutkimuksella. Usein kyseessä on tutkimusalue, josta ei vielä tiedetä paljoa. Eri haastattelumenetelmien joukossa teemahaastattelu poikkeaa määrämuotoisesta kyselystä, siten että se on löyhemmin strukturoitu. Puolistrukturoidulle haastattelulle on tyypillistä, että haastattelun sisältö ja lähtökohdat on lyöty lukkoon vain osittain. Haastattelun pohjana on yleensä etukäteen laadittu lista käsiteltävistä aiheista. Käytettävissä voi olla myös haastattelijan alustus tai kysymys aiheisiin liittyen, joka käydään läpi ennen keskustelua aiheesta. (Hirsjärvi & Hurme 2008.)

Teemahaastattelun vastaajat valitaan sen perusteella, että heillä tiedetään olevan kokemusta ja asiantuntemusta haastateltavista teemoista. He voivat vastata omin sanoin ja teemoja voidaan käsitellä eri järjestyksessä tai yhdistellen. Teemahaastattelussa huomioidaan se, että vastaajien tulkinnat asioista ja heidän antamat merkitykset ovat keskeisiä. Merkitykset syntyvät osin vuorovaikutuksesta tutkijan kanssa. Tyypillisesti tutkimusjoukko on pieni, korkeintaan kymmeniä henkilöitä tai organisaatioita. (Hirsjärvi & Hurme 2008; Kananen 2017.)

Ennen haastatteluja tutkija perehtyy etukäteen tutkittavan ilmiön määrääviin piirteisiin. Tämä tehdään selvittämällä ilmiön oletettavasti tärkeitä osia, rakenteita, prosesseja ja kokonaisuuksia. Teemahaastattelun sisältörunko muodostetaan tämän analyysin perusteella. (Hirsjärvi & Hurme 2008.)

Kerätty aineisto muodostuu haastatteluista tehdyistä muistiinpanoista. Ne luokitellaan ja analysoidaan. Analyysi alkaa jo haastatteluvaiheessa ja lopuksi tehdään yhteenveto havainnoista. Analyysissä käytetään abduktiivista päättelyä, jossa tutkijalla on lähtökohtaisesti joitakin teoreettisia johtoideoita, joita pyritään todentamaan aineiston avulla (Hirsjärvi & Hurme 2008).

Tutkimuksen reliabiliteetti tarkoittaa sitä, että kahdella tutkimuskerralla, kahden tutkijan toimesta tai kahdella rinnakkaisella tutkimusmenetelmällä saadaan sama tulos (Kananen 2019). Tässä tutkimuksessa selvitettiin ensiksi organisaatioiden käyttämiä menetelmiä ja välineitä. Niiden osalta vastausten luotettiin olevan samoja kerrasta toiseen, sillä onhan kyseessä konkreettiset

tekniset ratkaisut. Toiseksi kysyttiin myös haastateltavien henkilökohtaisia näkemyksiä em. menetelmien ja välineiden tuomasta kyberturvan tasosta. Näiden vastausten kohdalla voi ihmisten käsitys ja mielipide vaihdella ajasta ja tilanteesta toiseen.

Validiteetti on toinen tutkimuksen laadullinen arviointimenetelmä. Se jaetaan sisäiseen ja ulkoiseen validiteettiin. Sisäinen validiteetti tarkoittaa johtopäätösten oikeaa syy-seuraussuhdetta ja ulkoinen validiteetti saatujen tulosten yleistettävyyttä (Kananen 2019). Teemahaastattelujen osalta sisäisestä validiteetista huolehdittiin pitämällä vastauksista tehdyt johtopäätökset riittävän yleisellä tasolla pyrkien siihen, ettei niistä tehty liian syvälle meneviä ja kenties virheellisiä johtopäätöksiä. Ulkoisen validiteetin varmistamiseksi pyrittiin saamaan haastatteluotokseen mukaan eri kokoisia ja eri toimialoja edustavia organisaatioita kohderyhmän sisältä.

2.2.2 Kehittämistutkimus

Kehittämistutkimus on eräs interventionistinen tutkimusmenetelmä. Interventiotutkimus on yläkäsite sellaiselle tutkimukselle, joka pyrkii tuottamaan muutoksia ja arvioimaan niiden vaikutuksia kohteena olevaan ongelmaan (Kananen 2017). Toisen määritelmän mukaan kehittäminen ja tutkiminen yhdistyvät teoreettisia ja kokeellisia vaiheita sisältävässä syklisessä prosessissa (Pernaa 2013). Kehittämistutkimuksen erottaa perinteisestä tutkimuksesta pyrkimys muutokseen, kun perinteinen tutkimus pyrkii vain kuvaamaan, selittämään ja ymmärtämään ilmiötä. Sana interventio viittaakin juuri muutokseen itseensä sekä niihin toimenpiteisiin, joilla muutos pyritään aikaansaamaan.

Tyypillisesti tietotekniikan alan ylemmän ammattikorkeakoulututkinnon opinnäytetyössä pyritään suunnittelemaan ratkaisu johonkin ongelmaan soveltamalla teknologiaa jollain uudella tavalla. Opinnäytetyössä tehtävässä tutkimuksessa pyritään ongelmanratkaisun kehittämisen lisäksi selvittämään, miten hyvin ratkaisu toimii. Tähän tarpeeseen soveltuvat tutkimusmenetelmistä kehittämistutkimus ja tutkimuksellinen kehittäminen (Design Science Research, DSR). Vertailtaessa näitä tutkimusmenetelmiä on niiden todettu olevan hyvin samankaltaisia (Piirainen & Gonzalez 2013).

Interventionistisen tutkimuksen lähtökohtana toimii käytännön ongelma, joka on merkityksellinen. Tyypillisesti ongelma on jonkun organisaation toimintaan liittyvä kehittämiskohde, joka katsotaan niin tärkeäksi, että sen ratkaisemiseen ollaan valmiita investoimaan. Liiketoiminnallisen merkityksen lisäksi tutkimuksella tulisi olla tieteellistä merkitystä esimerkiksi tulosten yleistettävyyden kautta, jotta sitä voidaan pitää interventionistisena tutkimuksena. (Kananen 2017.)

Interventionistinen tutkimus pyrkii vastaamaan kysymyksiin, miten tai millä keinoilla kohteena oleva ongelma voidaan ratkaista. Interventionistinen tutkimus toteutetaan syklinä, jossa ensin määritellään ongelma ja selvitetään sen syyt. Syiden selvittämisen jälkeen etsitään keino sen poistamiseksi, eli löydetään interventio. Muutos toteutetaan ja seurannan keinoin selvitetään, miten tehty muutos ongelman syiden poistamiseksi onnistui. Mikäli tulokset osoittavat, että muutos ei onnistunut palataan tarvittaessa alkuun ja toistetaan sykli. Tyypillisesti interventionaalisessa tutkimuksessa keskitytään yhteen muutossykliin ja sen tieteellisyyden arviointiin, jotta saadaan toteutettua tieteelliselle tutkimukselle tärkeä takaisinkytkentä teoriaan. (Kananen 2017.)

Pernaan (Pernaa 2013) mukaan kehittämistutkimus alkaa aina ongelma-analyysillä. Siinä tavoitteena on selvittää tarpeet, mahdollisuudet ja kipukohdat kehittämiselle. Ongelma määritellään ja sen syitä selvitetään yhteistyössä tutkimuksen työelämäasiakkaan kanssa. Tätä työtä tehdään keräämällä aineistoa eri keinoin kuten haastatteluin, havainnoiden ja dokumentteihin tutustuen (Kananen 2017). Tässä tutkimuksessa hyödynnettiin teemahaastatteluja sekä Kyberturvallisuuskeskuksen asiantuntijoita ongelman tarkemmassa määrittelyssä.

Perehtymällä ongelma-alueen teorioihin voidaan löytää keinot ongelman syiden selvittämiseksi ja ratkaisut niiden poistamiseksi. Tavoitteena on hankkia syvällinen esiymmärrys ongelmasta. Perehtymisen avulla interventiotutkimuksessa löydetään teoreettisia lähtökohtia, joilla voidaan lähestyä tutkimusongelmaa ja löytää ongelmalle ratkaisu eli interventio. Perehtymisvaiheessa tuotetaan kirjallisuuskatsaus perehtymällä teoriaan alan tutkimusten ja kirjallisuuden kautta. (Kananen 2017.)

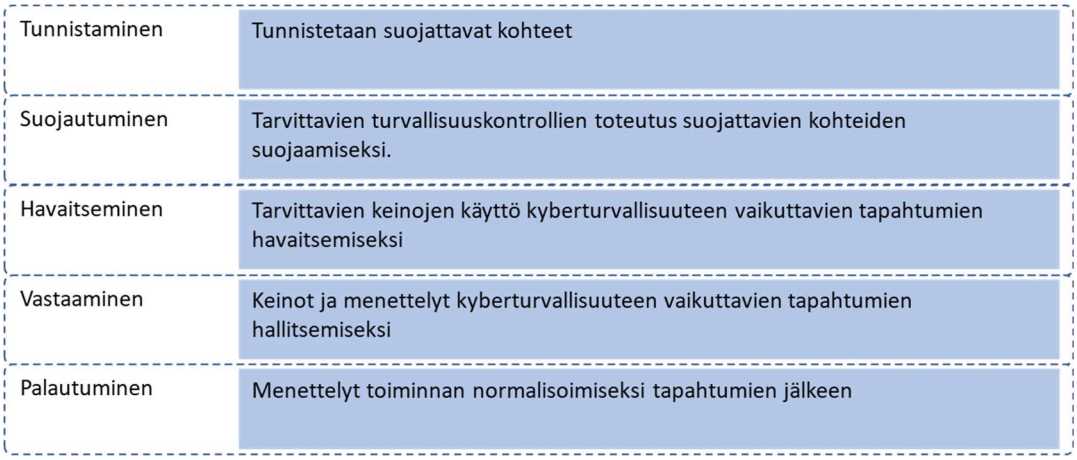
Muutoksen onnistumista ongelman ratkaisemiseksi seurataan muutoksen aikana ja sen jälkeen. Ongelman määrittelyvaiheessa on tunnistettu lähtötilanne, johon tuloksia verrataan. Vertailua voidaan tehdä myös yleisempiin teoriasta tai toimialan yleisistä mittareista johdettuihin vertailutuloksiin. Ratkaisua voidaan testata esimerkiksi testikäytön avulla, jolloin kokeilemalla ratkaisua aidossa tai lavastetussa ympäristössä voidaan mitata ja arvioida tuloksia. (Kananen 2017; Pernaa 2013.)

Tässä kehittämistutkimuksessa luotettavuutta arvioitiin ennen kaikkea kehittämiskohteen testikäytön tulosten avulla. Tuloksia arvioitiin suhteessa tutkimuskysymyksiin, teoriaan sekä kokeilun tuottamiin tuloksiin. Sisäistä validiteettia arvioitiin testikäytön sekä kokeilukohteiden ja Kyberturvallisuuskeskuksen asiantuntijoiden palautteen perusteella. Ulkoista validiteettia arvioitiin sen mukaan, miten yleistettäviä ja laajasti sovellettavia intervention keinot ovat tutkitun ongelman ratkaisuun.

3 TEOREETTINEN VIITEKEHYS

3.1 Turvallisuusuhkien havainnointi kyberturvallisuuden viitekehyksissä

National Institute of Standards and Technology (NIST) on USA:n kauppaministeriön tutkimuslaitos, jonka tehtäviin kuuluu mm. standardien kehittäminen ja käyttö (NIST 2009). NIST määrittelee kuvan 1 mukaisesti viitekehyksessään kriittisen infrastruktuurin kyberturvallisuudelle viisi päätehtävää: tunnistaminen, suojautuminen, havaitseminen, vastaaminen ja palautuminen. Kukin näistä viidestä päätehtävästä jakautuu kategorioihin ja niiden alakategorioihin. Alimmalla kategoriatasolla määritellään hyvin tarkasti kunkin tehtävän tuotokset sekä tekniset- ja hallinnolliset toimet. Lopuksi ne linkitetään kolmansien osapuolien standardeihin, ohjeisiin tai parhaisiin käytäntöihin mallin soveltajan avuksi. (NIST 2018.)



Kuva 1. Kriittisen infrastruktuurin kyberturvallisuuden viitekehyksen päätehtävät (NIST 2018)

NIST:n viitekehyksen mukaan turvallisuusuhkien havainnointiin keskitytään tunnistamisen ja havaitsemisen päätehtävissä. Havainnointiin liittyvästä kommunikaatiosta huolehditaan pääosin vastaamisen päätehtävässä. Tunnistamistehtävän aikana tehdään staattinen analyysi, eli identifioidaan ja dokumentoidaan käytössä olevat resurssit: järjestelmät, kapasiteetti ja data. Edellisen lisäksi tunnistetaan kybertoimintaympäristöön liittyvät riskit ja niiden tuomat uhat. Havaitsemistehtävä on operatiivinen. Siinä kehitetään ja otetaan käyttöön tarpeelliset toimenpiteet kyberturvallisuustapahtuman havaitsemiseksi ja tunnistamiseksi. (NIST 2018.)

Havaitsemistehtävä jakaantuu kolmeen kategoriaan: 1) poikkeamien ja tapahtumien hallinta, 2) jatkuva seuranta ja valvonta sekä 3) poikkeaminen tunnistaminen. Ensimmäisessä kategoriassa luodaan lähtökohdat ymmärrykselle kohdeympäristön toiminnasta, jotta voidaan erottaa asianmukainen ja poikkeava toiminta toisistaan. Tässä kategoriassa tapahtuu myös havaittujen kyberturvallisuustapahtumien analyysi sekä johtopäätösten teko siitä millaisesta tapahtumasta on kyse ja mihin se vaikuttaa. Hälytysten ja reagoinnin raja-arvot määritellään osana poikkeamien ja tapahtumien hallintaa. (NIST 2018.)

Jatkuvassa seurannassa ja valvonnassa seurataan kybertoimintaympäristön tapahtumia, kirjoitetaan niistä lokia ja pyritään havainnoimaan poikkeavaa tai sääntöjenvastaista toimintaa. Valvonta kohdistuu järjestelmiin, tietoliikenteeseen, käyttäjien toimintaan, ulkoisiin palveluntuottajiin sekä fyysiseen toimintaympäristöön. NIST:n mukaan myös haavoittuvuuksien skannaus on osa jatkuvaa seurantaa ja valvontaa. (NIST 2018.)

Poikkeamien tunnistamisessa hyödynnetään jatkuvassa seurannassa ja valvonnassa koottuja tapahtumatietoja eri lähteistä sekä poikkeamien ja tapahtumien hallinnassa määriteltyjä lähtöoletuksia toimintaympäristön normaalitilanteesta. Tietojen pohjalta kootaan tapahtumaraportteja ja -hälytyksiä sekä jaetaan niitä eteenpäin toimenpiteitä varten. Tunnistamisprosessia testataan ja kehitetään jatkuvasti, jotta voidaan varmistaa poikkeamien havainnointikyky. (NIST 2018.)

Poikkeamasta tai tapahtumasta kybertoimintaympäristössä tulee kommunikoida osapuolille, jotka tarvitsevat tietoa niistä. Näitä ovat mm. käyttäjät, johto, sidosryhmät ja viranomaiset. Viestinnän kohderyhmät vaihtelevat tapahtuman luonteen mukaisesti ja ne valitaan ennalta määriteltyjä kriteereitä noudattaen. Kommunikointia varten on ennalta määritelty johdonmukainen sisältö ja toimintatapa. Kommunikointi on NIST:n viitekehyksessä osa kybertilanteisiin vastaamisen päätehtävää. (NIST 2018.)

Center of Internet Security (CIS) julkaisee kyberturvallisuuden parhaita käytäntöjä CIS Controls -julkaisussaan. Tuorein versio on vuodelta 2021 ja siinä on CIS:n mukaan erityisesti huomioitu pilviturvallisuuden vaatimat näkökulmat. Tavoitteena on tuottaa hyvin kuvaavia, priorisoituja ja yksinkertaistettuja kontrolleja organisaatioiden kyberpuolustuksen parantamiseksi. Kontrollit on koottu parhaista käytännöistä ja ne on ryhmitelty suojattavien kohteiden mukaisesti ja niihin on liitetty parametreja kuten luokka ja kohderyhmä. Käytännön luokittelussa käytetään toiminnallisia kategorioita: tunnista, havaitse ja vastaa. Kohderyhmä selventää kunkin parhaan käytännön soveltuvuutta ja tarkoituksenmukaisuutta erilaisille ja kokoisille organisaatioille. (CIS 2021.)

Havainnointi on hajautettu CIS:n mallissa useiden eri kontrollien osalle. Tyypillisiä käytäntöjä riippuen kontrollista ovat lokitus, monitorointi ja katselmointi. Lokitus tulee toteuttaa keskitetysti ja havainnointia varten tulee ottaa käyttöön tunkeutumisen havainnointijärjestelmä (*Intrusion Detection Solution*, IDS). (CIS 2021.)

Kommunikaatio tietoa tarvitseville osapuolille on CIS:n mallissa osa kyberturvallisuustapahtumien reagointikontrollia. Reagoinnin parhaiksi käytännöiksi

esitetään kontaktitietojen ylläpito ja viestintään valmistautuminen. Toimijan on ylläpidettävä kontaktitietoja niihin sidosryhmiinsä, joiden kanssa se saattaa joutua jakamaan tietoja kyberturvallisuustapahtumasta. Näihin kuuluvat mm. kybervakuutuksen tarjoaja, viranomaiset sekä ISAC-kumppanit. Toiseksi tulee valmistautua kybertapahtuman aikaiseen kommunikaatioon ja viestintään. Tämä tarkoittaa viestintämekanismien ja varamekanismien määrittelyä ja testaamista. (CIS 2021.)

NIST:n ja CIS:n viitekehykset vertautuvat hyvin toisiinsa parhaiden käytäntöjen tasolla. Viitekehyksillä on oma lähestymistapansa: NIST:llä kyberturvallisuuden päätehtävät ja CIS:llä kyberpuolustuksen kontrollit. Käytännön suositusten ja toimenpiteiden tasolla suositeltavat tehtävät ovat samoja tai samankaltaisia. (NIST 2018; CIS 2021.)

Molemmissa malleissa on tunnistettu tarve jakaa kyberturvallisuuteen liittyvää tietoa uhista, havainnoista ja tapahtumista muiden sidosryhmien kanssa. Malleissa kommunikaatio on aina osa reagointia kybertilanteeseen. Vaikka viranomaisyhteistyö ja ISAC-yhteistyö mainitaan, ei se kuitenkaan esiinny mitenkään merkittävässä roolissa. Tietojen jakaminen ja yhteistyö eivät näiden mallien suositusten mukaan ole mitenkään erityisessä roolissa, kun varmistetaan organisaation kyberturvaa.

Kyberturvallisuuskeskus (2020c) on julkaissut Kybermittarin, joka on kansallisen kyberturvallisuuden arviointimalli ja -työkalu. Malli on kokoelma erilaisia kansallisia ja kansainvälisiä käytänteitä (mukaan lukien NIST:n viitekehys). Se luo yhtenäisen lähestymistavan kyberturvallisuuden arviointiin ja kehittämiseen Suomessa. Malli on tarkoitettu julkisten toimijoiden, yritysten ja muiden organisaatioiden käyttöön. (Traficom 2020c.)

Kybermittarin avulla voidaan muodostaa vertailukelpoista ja yhtenäistä ymmärrystä eri toimialojen toimijoiden kyberturvallisuuden tilasta. Kybermittari koostuu kyberturvallisuuden eri osa-alueita arvioivista kysymyksistä, joiden kunkin kohdalla arvioinnin tekijä pystyy määrittelemään tarkastettavan organisaation kypsyystason. Arviointi tehdään vertaamalla organisaation todellisia käytäntöjä mallin vaatimuksiin eri kypsyystasoilla. Kyberturvallisuusuhkien havainnointia arvioidaan useassa kybermittarin kysymyksessä. Saatujen tulosten

perusteella organisaatio voi päättää tarvittavista kehittämistoimista tilanteen parantamiseksi. (Traficom 2020c.)

3.2 Tilannekuvan muodostaminen ja tulosten hyödyntäminen

Kyberturvallisuuden tilannekuva tarkoittaa koottua kuvausta tietojärjestelmien tietyllä hetkellä vallitsevasta käytettävyys- ja turvallisuustilanteesta sekä kybertoimintaympäristön vallitsevasta tilasta. Kybertoimintaympäristö taas koostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvasta toimintaympäristöstä. (Sanastokeskus TSK 2018.)

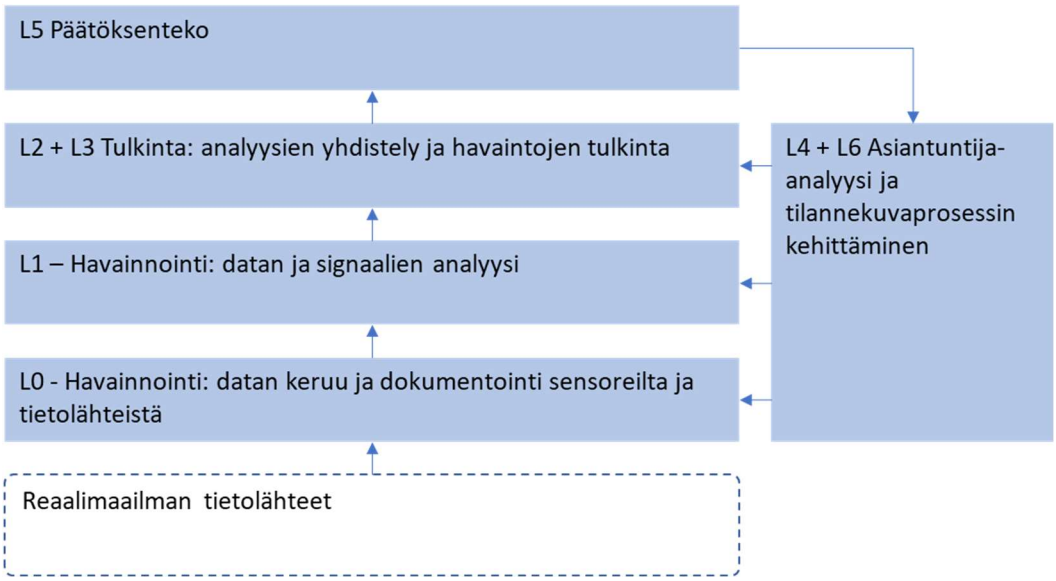
Tilannekuvaa voidaan ajatella dynaamisena prosessina, joka muodostuu yhteen vedetystä kuvauksesta, sen muodostamiseksi tarvittavasta arvioinnista sekä kaikista niistä menettelyistä, joita käytetään tietojen keräämiseksi ja ylläpitämiseksi (Endsley 1995). Tilannekuvan arvioinnissa muodostetaan tämän hetkinen kokonaiskuva asioiden ja tapahtumien välisistä suhteista kohteena olevassa ympäristössä, kun taas tilannekuva itsessään on kokonaiskuvan pohjalta käyttäjälle muodostunut mielikuva tilanteesta (Blash ym. 2012).

Tilannekuvaa tuotetaan päätöksenteon tueksi. Siinä käytetään hyväksi kerättyjä havaintoja ja niiden pohjalta tehtyjä arviointeja ja analyyseja. Tuloksia voidaan verrata tai esittää erilaisina mittareina. (Endsley 1995; Sanastokeskus TSK 2018.)

Kyberturvallisuuden tilannekuva muodostuu uhka-, häiriö- ja haavoittuvuustiedosta. Näiden tietojen avulla on mahdollista suojautua uhkatilanteilta ja selviytyä häiriötilanteista. Mitä kattavammat ja ajantasaisemmat tiedot ovat, sen paremmin tilannekuva palvelee edellä mainittua tarkoitusta. Puutteet tilannekuvassa haittaavat uhkatilanteisiin varatutumista ja loukkauksiin reagointia. (Johnson ym. 2016; Valtiontalouden tarkastusvirasto 2017.)

Tilannekuvan muodostamisen ja jäsentämisen tueksi on kuvattu Data Fusion Information Group (DFIG) -malli. Malli esittää tilannekuvan muodostamisen prosessin ja vaiheet aineiston keruusta päätöksentekoon ja reagointiin asti. DFIG-mallissa (kuva 2) erotellaan tilannekuvan rakentaminen seitsemään eri

tasoon (tasot 0–6). Näistä ylimmät tasot 4–6 keskittyvät päätöksentekoon, asiantuntija-analyysiin ja tilannekuvaprosessin jatkuvaan kehittämiseen. Alimmat tasot kohdistuvat tiedon keruuseen ja jalostamiseen tilannekuvan muodostamiseksi. Alimmalla 0-tasolla kerätään mittaustieto sensoreilta ja dokumentoidaan saatu signaali. Tasolla 1 pyritään ymmärtämään saadun signaalin merkitys tarkkailtavan kohteen kannalta, eli selvitetään, mikä on kohteen tila. Seuraavalla tasolla muodostetaan näkemys tilanteesta yhdistelemällä useiden toisiinsa sidoksissa olevien entiteettien tilan mukaan. Tasolla 3 tehdään tulkinta tilannekuvan merkityksestä – eli onko kyseessä mahdollisesti joku uhka tai vaikutus kohteelle. Joka tasolla voidaan tehdä samanaikaisesti sekä arviota nykytilanteesta tai ennustetta tilanteen kehittymisestä. (Blash ym. 2012.)



Kuva 2. Data Fusion Information Group (DFIG) -mallin 7 tasoa (Blash ym. 2012)

Kybermittarin mukaan tilannekuvan muodostamisen kypsyystasoa arvioidaan eri näkökulmista. Lokitietojen keruu suojattavista kohteista, lokien keskitetty säilytys ja tietojen hyödyntäminen tilannekuvan muodostamisessa ovat edellytyksiä kehittyneen kypsyystason toiminnalle. Järjestelmä- ja tietoliikenneympäristöjä valvotaan ja havainnoidaan säännöllisesti ja oikea-aikaisesti. Havainnointi tuottaa tarvittaessa hälytyksiä jatkotoimia varten. Valvontatoimien tulee olla linjassa arvioitujen uhkien kanssa. Tilannekuvan muodostamista ohjaavat dokumentoidut toimintatavat sekä johdon sille asettamat politiikat. Kybermittarilla arvioidaan myös, että riittävästä resursoinnista ja osaamisesta on organisaatiossa huolehdittu. (Traficom 2022.)

Tilannekuvatiedolle asetettuja tavoitteita on erilaisia riippuen tiedon käyttäjästä. Tilannekuvaa voidaan tarkastella taktisella, operatiivisella ja strategisella tasolla. Taktisella ja operatiivisella tasolla tavoitteena on koota ja jäsentää ajantasainen ja arjen tietoturvan toteuttamisen kannalta tarpeellinen tieto uhkatilanteesta sekä tarvittavista tarkistus- ja suojautumistoimista ajankohtaisen kyberturvallisuustilanteen mukaan. Tämä tieto jalostetaan kunkin kohderyhmän tarpeisiin. Strategisella tasolla tavoitteena on muodostaa johdolle tietoa päätöksenteon tueksi. Yhteiskunnan tasolla johto tarkoittaa valtiojohtoa ja kohderyhmä elinkeinoelämää ja viranomaisia. Yksittäisen organisaation tasolla taas puhutaan operatiivisesta johdosta sekä hallituksesta ja kohderyhminä ovat organisaatioyksiköt ja sidosryhmät. (Valtiontalouden tarkastusvirasto 2017; Sanastokeskus TSK 2018.)

Kerätty tieto jalostetaan tilannekuvaksi analysoimalla, suodattamalla ja koostamalla. Tämä voidaan tehdä kokonaan tai osittain automaattisesti. Usein tässä työssä hyödynnetään asiantuntijaresursseja. Koostamisen lopputuloksena syntyy erilaisia tilannekuvatuotteita ja -raportteja. Kyberturvallisuuskeskus tuottaa useita tilannekuvatuotteita organisaatioiden ja kansalaisten käyttöön. Näitä ovat mm. haavoittuvuustiedotteet, haavoittuvuuskooste, kybersää, uutiskirje, toimialakohtaiset tilannekuvaraportit sekä varoitukset merkittävistä tietoturvapoikkeamista. Näiden lisäksi tuotetaan tilannekuvaraportteja valtioneuvoston tilannekeskuksen käyttöön. (Valtiontalouden tarkastusvirasto 2017; Kyberturvallisuuskeskus 2021.)

Tilannekuvan muodostaminen edellyttää toimijoilta yhteistyötä. Organisaatioilla tulee olla valmiuksia jakaa tietoa omasta tilanteestaan ja havainnoistaan verkostossaan. Jakaminen on tärkeää ja parantaa tilannekuvan laatua. Tämä edellyttää luottamusta koko verkostoon ja siihen etteivät omat luottamukselliset tiedot päädy vääriin käsiin. Luottamusta voidaan vahvistaa teknisin keinoin, kuten poistamalla aineistosta sen lähteen tunnistamiseen ja kohdentamiseen tarvittavat tiedot tai sopimuksellisin keinoin verkoston jäsenten välillä. (Johnson ym. 2016; Skopik 2017.)

Julkinen hallinto on vastuussa kansallisen kriittisen infrastruktuurin suojaamisesta fyysisiltä ja kyberuhilta. Hallinnon tehtävänä muodostaa tilannekuva

kansallisella tasolla. Ajantasaisen kootun tiedon puute vaarantaa kriittisen infrastruktuurin vakauden (Skopik 2017). Valtiotalouden tarkastusviraston tarkastuskertomuksen (Valtiontalouden tarkastusvirasto 2017) mukaan Suomessa kyberturvallisuuden kokonaistilannekuvaa ei riittävällä tasolla keskitetysti kokoa mikään toimija. Kyberturvallisuuskeskuksella on kyllä tämä tehtävä, mutta esim. viranomaisilla tai yksityisillä yrityksillä ei ole velvollisuutta ilmoittaa tietoturvaloukkauksista. Tilannekuvan muodostaminen on hajallaan usean eri toimijan kesken. Viranomaiset ja organisaatiot joutuvat täydentämään tilannekuvaansa omin toimin. Valtiotalouden tarkastusviraston mukaan keskitetylle palvelulle olisi tarvetta.

3.3 Tiedon jakamisen haasteet verkostossa

Verkostot ovat organisaatioiden tai yksilöiden muodostamia usein epämuodollisia yhteisöjä. Verkoston toimijoita voi yhdistää esimerkiksi sama toimiala tai samat kiinnostuksen kohteet. Ne voivat olla laajoja ja kansainvälisiä. Erilaiset kulttuurit ja toimintatavat monimutkaistavat verkostoja. Verkosto toimintaympäristönä asettaa tietojenvaihdon standardoinnille ja systematisoinnille sellaisia haasteita, että ne eivät välttämättä ole kenenkään kontrolloitavissa. Tietojen keruuta ei pysty helposti standardisoimaan ja synkronoimaan. Tietosisällöistä ei saa yhteneväistä rakenteeltaan, semantiikaltaan ja versioiltaan. Verkoston rakenne ja toimintamallit muuttuvat kaiken aikaa. Rajapintojen ja tietosisältöjen täydellisen yhteensovittamisen sijasta on hyödyllisempää tunnistaa ongelmat ja selvittää, mitä on tehtävissä tilanteen parantamiseksi. Onnistuneeseen tietojenvaihtoon tarvitaan hyvin joustava tietojenvaihdon toimintaympäristö. (Blash ym. 2012.)

Toisaalta on tärkeää ottaa jo käytössä olevat turvallisuusratkaisut huomioon, kun tietojen jakoa verkostossa suunnitellaan. Tämä siksi, että tietojenvaihtoon ehdotetut ratkaisut voisivat olla osapuolista helpommin hyväksyttäviä ja kannustaa osallistumaan. Organisaatioilta ei voida edellyttää suuria investointeja verkostoa varten, vaan ehdotettujen ratkaisujen pitää hyödyntää olemassa olevaa kyberturvallisuusinfrastruktuuria. Jaetun tiedon pitää tukea nykyisiä kyberturvallisuuden toimintamalleja esimerkiksi siten, että tiedon käsittely on automatisoitavissa. Tämä tarkoittaa, että tieto jaetaan sellaisessa vakioidussa

muodossa, jossa se on helposti ladattavissa turvallisuustiedon ja -tapahtumienhallinnan (*Security information and event management*, SIEM) tai tunkeutumisenhallinnan (IDS) järjestelmiin. (Skopik 2017.)

Tutkimuksensa johtopäätöksissä Skopik (Skopik 2017) esittää, että yleisellä kansallisella tasolla tapahtuva tiedonjako ei ole parhaiten toimiva malli. Tilannekuvatiedon pitäisi olla kullekin toimialalle kohdennettua sisältäen kohderyhmälle jalostettua tietoa ja analyysiä, jotta siitä olisi konkreettista hyötyä. Lisäksi ratkaistavana on olennainen ristiriita: toisaalta näyttää olevan välttämätöntä, että laadun varmistamiseksi kyberturvallisuusasiantuntija käsittelee ja jalostaa jaettavaa tietoa, mutta toisaalta tiedonjaon pitäisi olla tehokasta ja nopeaa.

3.4 Uhkatiedon jakaminen

Kyberturvallisuudestaan kiinnostuneet organisaatiot ovat tunnistaneet tarpeen jakaa kyberuhkatietoa (*Cyber Threat Information*, CTI). Tietoa pitää jakaa ajantasaisesti ja luotettavasti, jotta voidaan parantaa kykyä tunnistaa vihamielistä toimintaa ja toimijoita sekä pienentää hyökkäyksien vaikutuksia organisaation toimintaan ja kriittisiin resursseihin. Kysymys on ennen kaikkea vuorovaikutuksesta: jaettua tietoa hyödynnetään omassa kybersuojauksessa sekä palvellaan muita verkoston jäseniä jakamalla omia havaintoja. Kehittyviin uhkiin vastaaminen vaatii yhteistoiminnassa kohdennettuja ja koordinoituja vastatoimia, sillä hyökkäykset kehittyvät koko ajan monimutkaisemmiksi, räätälöidyiksi ja koordinoiduiksi operaatioiksi. (Skopik 2017; Rantos ym. 2020.)

NIST:n ja EU:n kyberturvallisuusviraston (ENISA) mukaan CTI on tietoa, joka auttaa organisaatiota tunnistamaan, arvioimaan, valvomaan tai vastaamaan kyberuhkiin. Tiedot voivat olla esimerkiksi hälytyksiä, tunnistetietoja, uhkakuvauksia tai vaikkapa ohjeita tietoturvatyökalujen käytöstä ja konfiguroinnista jonkin uhan pienentämistä varten. (Johnson ym. 2016; ENISA 2018.)

Tyypillisesti organisaatiot jakavat uhkatietoa paljon sisäisesti esimerkiksi IT-osaston ja turvallisuusosaston välillä. Kuitenkin jakamalla uhkatietoa ulkopuolisten kanssa luottamusverkostossa, voi organisaatio hyötyä kollektiivisen verkoston vipuvoimasta. Tietojen jakamisesta on organisaatiolle useita hyötyjä.

Yhteistyö auttaa tilannekuvan muodostamisessa, kun osaamista, tietoa ja voimavaroja voidaan jakaa. Tietojen jakaminen parantaa tilannekuvan monipuolisuutta ja syventää organisaation tietämystä. Edellisten lisäksi verkostossa luodun ymmärryksen hyväksikäyttö tekee kyberpuolustuksesta ketterämpää, kun reagointimahdollisuudet jatkuvasti muuttuviin uhkatilanteisiin paranevat. Käytettävissä on näin kollektiivista tietämystä, kokemusta ja kyvykkyyksiä, joita ei yksin toimimalla voi saavuttaa. Jakamalla uhkatietoa organisaatiot voivat paremmin tunnistaa hyökkäyskampanjoita, jotka kohdistuvat tiettyyn toimialaan tai instituutioihin. Saatua tietoa hyödyntämällä organisaatio voi tehdä parempia päätöksiä turvallisuutensa kehittämiseksi, suojautua uhilta tehokkaammin ja toipua ongelmatilanteista nopeammin. (Johnson ym. 2016; Skopik 2017; Chantzios ym. 2019.)

Uhkatiedon jakaminen edellyttää monen eri näkökulman huomioimista. Tietojenvaihtoon liittyy useita ongelmia useilla eri kerroksilla, jotka on ratkaistava ennen kuin CTI:n jakaminen on mahdollista (Rantos ym. 2020). Juridisella kerroksella on ratkaistava tietoturvallisuuteen liittyvät kysymykset, rajoitukset ja velvollisuudet tietojen jakamiseksi. Käytäntöjen ja toimintamallien kerroksella ratkaistaan, mitä tietoa jaetaan, keille jaetaan ja milloin. Semanttisella kerroksella vastataan kysymyksiin tietotyypeistä ja -formaateista sekä datan loogisesta tulkinnasta ja merkityksestä. Alimmalla eli teknisellä kerroksella kuvataan tiedonsiirron tekninen ja turvallinen toteutus. Tämä tutkimus keskittyy alimpiin kerroksiin. Käytännössä joudutaan myös ratkomaan ylempien kerrosten kysymyksiä, jotta toimiva ratkaisu on ylipäätään mahdollinen.

Uhkatiedon jakamista varten on perustettu useita viranomais- tai ISAC-verkostoja, joilla kullakin on oma tehtävänsä ja roolinsa. Verkostot voivat toimia epäformaaleina tai formaaleina verkostoina. Epäformaalit verkostot ovat keskustelevampia ja keskittyvät luottamuksen rakentamiseen, kun taas formaalit verkostot jakavat ja hyödyntävät rakenteisia ja mallinnettuja tietoja kyberuhista (Skopik 2017). ISAC verkostot ovat ENISA:n suosittelema toimintamalli, ja tietojenjakoon voidaan käyttää erilaisia työkaluja. Työkalut – kuten Open Source Threat Intelligence Platform (lyh. MISP) (MISP Project 2021) – automatisoivat tietojenvaihtoa ja tukevat erilaisia käyttö- ja pääsyoikeuksia tietoon, koska kaikilla käyttäjillä ei välttämättä ole oikeutta kaikkeen vaihdettavaan tietoon. (ENISA 2018.)

Esimerkiksi Yhdysvaltojen kyber- ja infrastruktuuriturvallisuusvirasto (CISA) operoi kriittisen kyberinfrastruktuurin tietojenjaon ohjelmaa (Protected Critical Infrastructure Information Program, PCII). Osallistuminen ohjelmaan on organisaatoille vapaaehtoista. Tietojenvaihto on luottamuksellista ja CISA:n valvomaa. Tavoitteena on ymmärtää ja tunnistaa turvallisuusuhkia ja -riskejä, haavoittuvuuksia ja niiden torjuntakeinoja sekä kriittisen infrastruktuurin rakentamisessa ja ongelmatilanteissa (CISA 2021). Vastaavia hankkeita löytyy myös muista maista tai tietylle toimialalle keskittyen.

3.5 Hyökkäys- ja hyväksikäyttömenetelmien jäsentely

Uhkatieto on kyberturvallisuusuhkiin liittyvää informaatiota, joka pyrkii auttamaan organisaatiota suojaamaan itseään uhilta tai paljastamaan vihamielisen toimijan toiminnan (Johnson ym. 2016).

NIST:n mukaan uhkatiedon päätyyppejä ovat

- **Indikaattorit** ovat teknisiä tunnisteita tai mitattavissa olevia havaintoja, joiden perusteella voidaan päätellä, onko hyökkäys mahdollinen, parhaillaan käynnissä tai tapahtunut jo aiemmin.
- **Taktiikat, tekniikat ja toimintatavat** (*tactics, techniques and procedures*, lyhennettynä TTP) kuvaavat hyökkääjän toimintatapoja. Taktiikat kuvaavat toimintaan ylätasolla, kun taas toimintatapakuvaukset voivat olla hyvin yksityiskohtaisia.
- **Hälytykset** ovat tietoja ajankohtaisista haavoittuvuuksista, hyväksikäyttökeinoista ja muista turvallisuuteen vaikuttavista seikoista.
- **Uhkatietoraportit** ovat tyypillisesti edellisiä jalostetumpaa tietoa uhkatilanteesta ja tilannekuvasta. Raportit sisältävä kohdennettua, koottua ja analysoitua tietoa päätöksenteon tueksi.
- **Työkalujen asetukset** ovat suosituksia ja ohjeita tietoturvatyökalujen ja -järjestelmien konfiguroimiseksi ja käyttämiseksi esimerkiksi indikaattoreiden tai TTP:iden havaitsemiseksi. (Johnson ym. 2016; Chantzios ym. 2019.)

Uhkatiedon lähteinä toimivat tyypillisesti organisaation sisäiset lähteet, kuten käytetyt kyberturvallisuustyökalut ja sisäinen analyysi- ja valvontatyö. Lisäksi uhkatiedon lähteinä voivat toimia ulkoiset lähteet kuten yhteisöt, palveluntarjo-

ajat ja avoimet lähteet. Palveluntarjoajat voivat olla kaupallisia toimijoita, joiden toimittama tieto on maksullista. Kaupallisuuteen liittyy usein lupaus siitä, että tiedon laatu on tarkastettua ja luotettavaa. (Chantzios ym. 2019.)

Riippumatta tiedon tyypistä uhkatiedon tulee sisältää muutamia yhteisiä piirteitä. Tiedon tulee olla ajantasaista ja käytettävissä ajoissa niin, että vastaanottaja ehtii reagoida tarvittavalla tavalla. Sen tulee olla relevanttia ja sovellettavissa vastaanottajan toimintaympäristössä. Sen on oltava myös oikein, kattavaa ja yksiselitteistä. Jaetun tiedon on tarjottava riittävällä tasolla yksityiskohtia ja viitekehystä, johon se liittyy. Viimeisenä vaatimuksena jaettavan uhkatiedon on ehdotettava keinoja toimenpiteiksi, joita vastaanottajan olisi syytä harkita tai tehdä. (Skopik 2017.)

Yhdysvaltalainen julkisrahoitteinen tutkimus- ja kehitysyhtiö MITRE julkaisee MITRE ATT&CK viitekehystä ja tietämystietokantaa hyökkääjien käyttämistä kyberturvallisuutta uhkaavista menetelmistä. Listatut hyökkäys- ja hyväksikäyttömenetelmät perustuvat tosielämän kokemuksiin ja havaintoihin. Menetelmät esitetään yhteen koottuna taulukoiksi, jotka on kohdennettu eri teknologia-alustoille kuten käyttöjärjestelmät, tietoliikenneverkot, pilvipalvelut ja konttialustat. Kohdennus auttaa viitekehyksen käyttäjää rajaamalla tiedon määrää suojattavan kohteen teknologiaa-alustan mukaan. (Strom ym. 2017; Pennington ym. 2019.)

Viitekehystä voidaan käyttää pilviturvallisuuden havainnointikohteiden määrittelyyn ja tunnistamiskeinojen valintaan. Pilvipalveluihin kohdistuvia hyökkäys- ja hyväksikäyttömenetelmiä viitekehyksessä on lueteltu yhteensä 56 kappaletta. Näistä muutamat selkeästi vain pilvipalveluihin kohdistuvia. Suuri osa listatuista menetelmistä on yleisiä ja laaja-alaisesti käytettyjä ja ne voidaan kohdistaa useimpiin teknologia-alustoihin. Pilvipalveluihin kohdistuvat hyökkäys- ja hyväksikäyttömenetelmät eivät siis välttämättä eroa muihin teknologia-alustoihin kohdistuvista menetelmistä, jolloin samat valvonta ja havainnointikeinot ovat toimivia. (MITRE 2022.)

Jokaisesta hyökkäys- ja hyväksikäyttömenetelmästä on tuotettu kuvaus, jossa esitetään hyökkääjän käyttämä toimintamalli, tavoite mihin menetelmällä pyritään sekä alusta tai teknologia johon uhka kohdistuu. Menetelmän kuvaus

noudattaa edellä esitettyä rakennetta, jossa dokumentoidaan hyökkääjien käyttämiä taktiikoita, tekniikoita ja toimintatapoja. Kuvauksessa luetellaan esimerkkejä tunnetuista toimintatavoista menetelmän hyväksi käyttämiseksi. Joissakin tapauksissa menetelmäkuvaus on jaettu vielä alimenetelmiksi, jos se on katsottu tarpeelliseksi tietämyskannan käytettävyyden parantamiseksi ja alimenetelmien erityispiirteiden esille tuomiseksi. (Strom ym. 2017; Pennington ym. 2019.)

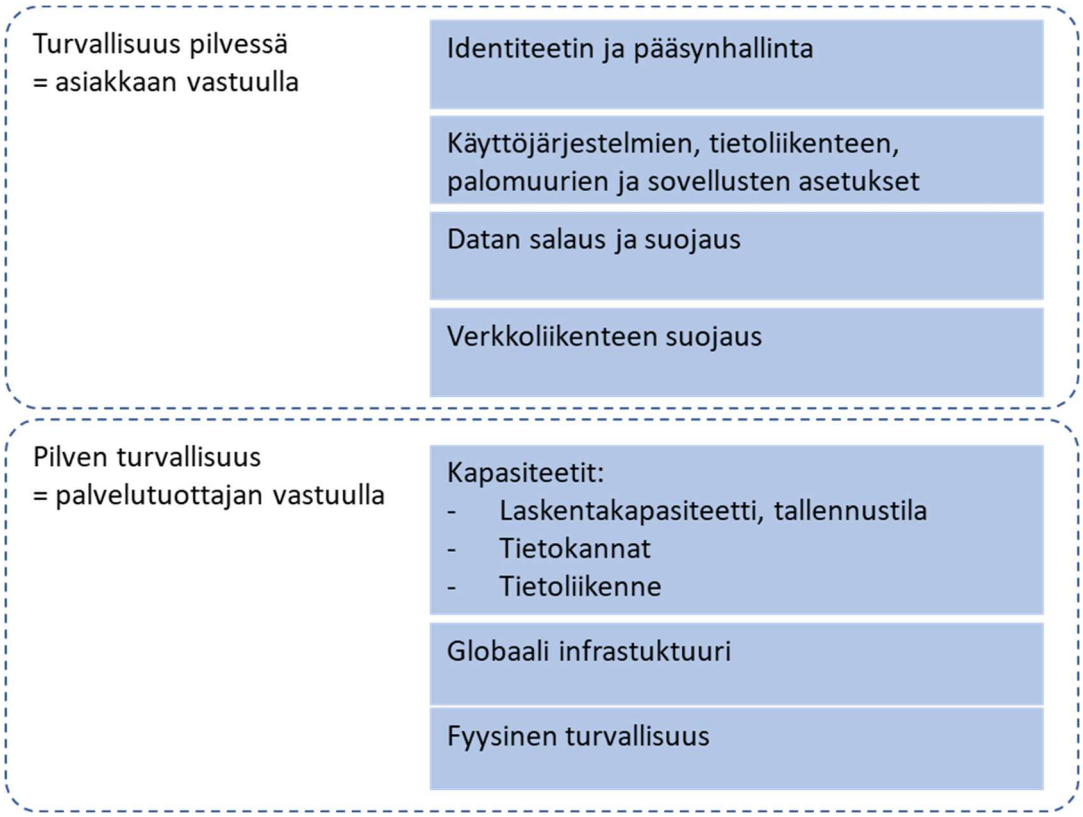
Viitekehyksessä myös on dokumentoitu hyödyllisiä keinoja menetelmien tunnistamiseksi sekä niiden vaikutusten torjumiseksi tai lieventämiseksi. Ne ovat yleistettäviä ja uudelleenkäytettäviä useiden eri menetelmien kohdalla. Tunnistamis- ja torjumiskeinot ovat valmiita konsepteja ja tekniikoita, joita käyttämällä voidaan havaita tai estää hyökkäysmenetelmien onnistunut käyttö. (MITRE 2022.)

MITRE ATT&CK viitekehyksessä on yhteensä 14 erilaista luokkaa taktisille tavoitteille, joihin hyökkääjä pyrkii. Ne ovat hyökkääjän operatiivisia päämääriä hyökkäyksen eri vaiheissa. Alussa pyritään tiedustelemalla hankkimaan hyödyllistä tietoa kohteesta, sen toiminnasta ja haavoittuvuuksista. Tämän jälkeen taktisena tavoitteina ovat pääsy uhrin järjestelmiin, oman jalansijan vakiinnuttaminen uhrin ympäristöissä sekä levittäytyminen laajemmin. Kun pääsy kohteen järjestelmiin ja tietoon on hankittu, voi tavoitteena olla vakoilu, tietojen varastaminen, resurssien hyväksikäyttö tai uhrin toiminnan häirintä. Eri hyökkäysmenetelmät voidaan linkittää yhteen tai useampaan tavoitteeseen. Jaottelu auttaa jäsentämään suojautumisen ja havainnoinnin suunnittelua, sillä se helpottaa tunnistamis- ja torjuntakeinojen valintaa, toteuttamista ja arvioimista. (Strom ym. 2017; Pennington ym. 2019.)

Soveltamisen yksinkertaistamiseksi erilaisten pilvipalveluiden kanssa, viitekehys on jaettu viiteen alaryhmään: Office 365, Azure AD, Google Workspace, SaaS ja IaaS (Strom ym. 2017). Jako on tehty yleisimpien kaupallisten pilvipalvelutuotteiden ja -käyttökonseptien mukaan. Hyökkääjien käyttämät TTP:t eroavat eri pilvipalveluratkaisujen välillä jonkin verran, jolloin jako alaryhmiin yksinkertaistaa mallia. Eri pilvipalvelut ovat niin erilaisia uhkien ja hyväksikäyttömenetelmien osalta, että erittely on ollut perusteltua tehdä.

3.6 Pilviturvallisuuden vastuunjakomalli

Suuret globaalit pilvipalveluntuottajat esittelevät hyvin samankaltaiset mallit palveluiden kyberturvallisuuden vastuunjaosta palveluntuottajan ja asiakkaan välillä. Esimerkiksi Amazon Web Services (AWS) määrittelee käsitteet pilven turvallisuus ja turvallisuus pilvessä (englanniksi *security of the cloud* ja *security in the cloud*) (kuva 3). Tässä pilven turvallisuus tarkoittaa pilvipalvelualustan tarjoamaa turvallisuutta, josta AWS palveluntuottajana ottaa vastuun. Turvallisuus pilvessä vastaavasti tarkoittaa sitä osaa palvelun turvallisuudesta, josta asiakkaan on itse huolehdittava ja kannettava vastuu. (Amazon Web Services s.a.)



Kuva 3. Pilviturvallisuuden vastuunjakomalli (Amazon Web Services s.a.)

Pilven turvallisuus on siis palvelutuottajan vastuulla ja sillä on vahva motiivi pitää turvallisuus kunnossa. Onhan kyseessä palvelu, jonka liiketoimintamenestys riippuu asiakkaiden luottamuksesta. Pitääkseen huolta vastuustaan alustansa turvallisuuden varmistamiseksi palveluntuottaja tekee paljon valvontaa, ylläpitää reagointikykyä sekä tuottaa asiakkaille raportteja tilanteesta.

Turvallisuus pilvessä on puolestaan asiakkaan vastuulla. Asiakkaan on huolehdittava käyttämiensä palvelukomponenttien asetuksista ja konfiguraatioista, datan yhtenäisyydestä ja salauksesta, tietoliikenteen suojauksesta sekä käyttäjien ja käyttöoikeuksien hallinnasta. Näiden lisäksi asiakkaan on kannettava vastuu myös omien järjestelmiensä ja sovellustensa turvallisuudesta, joita suoritetaan pilvialustalla.

Pilvipalvelut ovat monimutkaisia. Ylläpitäjien ja sovelluskehittäjien osaamisessa voi olla puutteita ja virheitäkin sattuu. Virheet ja puutteet asiakkaalle kuuluvissa turvallisuutta varmistavissa tehtävissä avaavat hyökkäyspinta-alaa hyväksikäyttäjille. Näiden ehkäisemiseksi pilvipalveluiden tuottajat pyrkivät tarjoamaan asiakkaiden käyttöön välineitä kyberturvallisuusriskien pienentämiseksi. Tällaisia välineitä ovat muun muassa erilaiset valmiit tietoturvaraportit ja itseauditointityökalut. (Amazon Web Services s.a.)

3.7 Pilvipalveluiden havainnointi ja uhkavektorit

Uhkien havainnointia ja uhkavektoreiden tunnistamista pitää tehdä pilviympäristöjen erityispiirteet huomioiden. Esimerkiksi ylläpidon erityispiirteenä on, että se voidaan suorittaa aina ohjelmallisesti ja on hyvin helposti automatisoitavissa. Käsin tehtävään ylläpitoon on toki käytettävissä myös hallintakäyttöliittymiä. Asiakkaan tulee valvoa, tapahtuuko ylläpitokerroksella poikkeavaa toimintaa tai niiden yrityksiä. Erityisenä tarkkailun kohteena tulee olla identiteetin ja pääsynhallinta. Tietoliikenneverkko toteutetaan pilvipalvelussa myös täysin ohjelmallisesti. Verkon liikenteen poikkeamia tulee analysoida kuten perinteisissä ympäristöissäkin. Lisäksi on valvottava verkon hallintakerrosta ja tapahtumia, jotka kohdistuvat tietoliikennekomponenttien konfiguraatioon. Monet perinteisen yritysverkko- ja konesaliympäristön käyttämät työkalut, kuten IDS-järjestelmät sekä valvonta- ja monitorointiratkaisut ovat hyvin käyttökelpoisia myös pilviympäristöissä. (CSA 2017.)

Suojattavien kohteiden tunnistaminen ja luettelon ylläpito ovat yhtä tärkeitä pilvipalveluita käytettäessä kuin perinteisissä lähiverkko- ja konesaliympäristöissäkin. Havainnoinnin painopiste pitää olla sellaisissa uhkavektoreissa, jotka korostuvat pilvessä. Näiden tunnistamisessa auttavat mm. MITRE ATT&CK –viitekehyksen esittelemät hyökkäysmenetelmät. Hyvinä esimerkkeinä ovat

käytetyt ohjelmisto- ja palvelurajapinnat. Ne ovat tärkeitä tunnistaa ja järjestää havainnoinnin piiriin erityisesti juuri pilvipalveluissa, koska niiden monipuolinen käyttö lisääntyy ja erilaisten ulkopuolisten rajapintojen käyttöönotto on hyvin helppoa. (Peiris ym. 2021.)

Konfiguraatioiden hallinnasta ja ohjelmistopäivityksistä on pidettävä huolta. Käytetyt järjestelmät ja komponentit on syytä koventaa. Koventamisessa tietoturvaan vaikuttavat konfiguraatiomääritykset muutetaan oletusmäärityksistä tietoturvallisempiin määrityksiin. Puutteet tai virheet kovennuksissa voivat avata tunkeutujalle reitin palvelujen haltuunottoon. Yrityksen käyttämä pilviympäristö voi muuttua verrattain usein, kun uusia virtuaaliresursseja, tietoliikenneyhteyksiä ja rajapintoja perustetaan ja vanhoja poistuu. Muutokset on helppo toteuttaa ohjelmoimalla ja automatisoimalla. Muutoksien yhteydessä kovennukset voivat kuitenkin unohtua, varsinkin kun ylläpitotyö ei pilviympäristössä ole aina keskitetty vaan jakaantuu eri toimijoille organisaatiossa. (Peiris ym. 2021.)

Monet pilvipalveluiden käyttöskenaariot kannustavat jatkuviin muutoksiin. Palveluita voidaan lisätä ja poistaa kapasiteettitarpeen mukaan. Asiakas voi tehdä kustannusoptimointia sammuttamalla tarpeettomia resursseja. Käyttökohteet ja -tarpeet voivat muuttua nopeasti esimerkiksi liiketoiminnan ketterän kehittämisen vuoksi.

Ylläpidon käyttäjätunnusten ja muiden korotettujen käyttöoikeuksien aktiviteetin valvonta ja väärinkäytösten havainnointi on erityisen tärkeää. Ylläpito-oikeuksien haltuunotto antaa tunkeutujalle vapaat kädet toteuttaa tavoitteensa. Pilvipalveluiden peruspiirre on se, että ne ovat saavutettavissa kaikkialta verkosta ja ovat avoimia ulkoisille yhteydenotoille. Tämä voi houkutella puoleensa vihamielisiä toimijoita kokeilemaan ja etsimään luvatonta pääsyä. (Peiris ym. 2021.)

3.8 Pilviturvallisuuden arviointikriteeristö

Kyberturvallisuuskeskus on laatinut ja julkaissut Suomen kansallisista tarpeiden näkökulmasta laaditun pilviturvallisuuden arviointikriteeristön. Kriteeristö

on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Sen tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta, kun käytetään pilvipalveluita. Kriteeristöä voidaan hyödyntää myös julkisten tietojen suojaamisessa sekä yrityksien ja muiden organisaatioiden tarpeisiin. (Traficom 2020b.)

PiTuKri on hyödyllinen tämän tutkimuksen näkökulmasta, koska se on laadittu suomalaisen kyberturvallisuuden tarpeiden näkökulmasta. Se on viranomaisen kanta tarvittaviin toimiin salassa pidettävän tiedon suojaamiseksi. Kriteeristö kohdistuu nimenomaan pilvipalveluihin ja se on tarkoitettu käytettäväksi laajasti viranomaisten ja elinkeinoelämän käyttöön Suomessa.

PiTuKrissa kuvattavat turvallisuusvaatimukset on laadittu niin, että salassa pidettäviin tietoihin kohdistuvat tyypillisimmät riskit pysyvät siedettävällä tasolla (Traficom 2020b). PiTuKria voidaan käyttää yleisimpiin pilvipalveluiden toteutusmallien arviointiin, kuten yksityiseen pilveen, yhdistelmäpilveen ja julkiseen pilveen. Samoin se soveltuu IaaS-, Paas- ja Saas-palveluiden arvioimiseen. Kriteeristön käyttö edellyttää tapauskohtaista soveltamista, koska pilvipalvelut ovat erilaisia ja niiden käyttötapaukset ovat vaihtelevia.

Pilvipalveluiden tyypillisen vastuunjakomallin mukaisesti osa tietojen suojauksesta kuuluu palveluntarjoajan ja osa asiakkaan vastuulle. Tarkasteltavan käyttötapauksen mukaan voivat kriteeristön vaatimukset kohdistua palveluntarjoajan vastuulla olevaan osuuteen, yksin asiakkaan vastuulla olevaan osuuteen tai sekä palveluntarjoajan että asiakkaan vastuilla oleviin osuuksiin. Vaatimukset eivät ole kaiken kattavia, vaan niitä pitää tulkita kohteena olevan käyttötapauksen näkökulmasta. Kriteeristön käyttö edellyttää edellä mainituista syistä riittävää kyberturvallisuuden osaamista. (Valtiovarainministeriö 2020.)

Pilviturvallisuuskriteeristön laadinnassa on hyödynnetty useita ulkomaisia kriteeristöjä ja standardeja. Näitä ovat Saksan tietotekniikan turvallisuusviraston (Bundesamt für Sicherheit in der Informationstechnik, BSI) ja Cloud Security Alliancen (CSA) kriteeristö sekä ISO-standardit ISO27001 ja ISO27017. PiTuKrissa on hyödynnetty myös kansallista Katakri-kriteeristöä. (Traficom 2020b.)

4 TUTKIMUSTULOKSET

Tässä luvussa raportoidaan tutkimustulokset sekä vastataan tutkimusongelmiin ja linkitetään tulokset aiempaan tutkimukseen. Ensin käydään läpi teemahaastatteluna tehdyn lähtötilannekartoituksen kulku, tulokset ja johtopäätökset. Tämän jälkeen raportoidaan toteutetun interventionistisen kokeilun toteutus ja tulokset. Lopuksi esitetään tulosten perusteella muodostettu synteesi, johtopäätökset ja jatkotutkimusaiheita.

4.1 Lähtötilannekartoitus ja tulokset

Teemahaastatteluihin osallistui 14 organisaatiota Kyberturvallisuuskeskuksen sidosryhmistä. Organisaatiot edustivat pääosin huoltovarmuuskriittisiä toimialoja. Ne olivat sekä yrityksiä, että julkishallinnon yhteisöjä ja osallistuivat vapaaehtoisina haastatteluihin. Haastateltavat asiantuntijat edustivat joko organisaatioiden turvallisuusyksiköitä tai tietohallintoa.

Haastatteluissa pyrittiin selvittämään lähtötilanne siitä, mikä on yritysten käyttämien pilvipalveluiden kyberuhkien havainnoinnin laajuus tällä hetkellä sekä miten yhtenäinen tai hajanainen käytettyjen menettelyjen ja työkalujen kenttä on. Lisäksi selvitettiin, miten luottavaisia organisaatiossa ollaan tilannekuvan laatuun. Saatuja vastauksia käytettiin tämän tutkimuksen ja Kyberturvallisuuskeskuksen toteutettavuustutkimusprojektin sisällön määrittelyyn ja kohdentamiseen.

Vastauksia tarkastellaan yleisellä yhteenvetotasolla. Tämä on perusteltua kahdesta syystä: muutamat organisaatiot asettivat ehdoksi, etteivät ole valmiita osallistumaan ja jakamaan tietoa, jos niiden käyttämät välineet ja menettelyt tulevat näin julkisiksi. Toisaalta haastattelut olivat tutkimuksen kannalta lähtötilanteen arviointia tutkimuksen suuntaamiseksi eivätkä siten varsinainen tutkimuskohde. Tässä raportissa esitetään ainoastaan sellaisia vastauksia, jotka jossain määrin saturoituvat, eli esiintyvät suurimmassa osassa vastauksia tai saavat useita mainintoja eri haastateltavilta.

4.1.1 Taustatiedot

Haastattelun taustoituksena selvitettiin pilvipalveluiden käytön laajuutta ja luonnetta organisaatiossa. Haastattelujen kysymykset ja aihepiirit on lueteltu liitteessä 1. Laajuutta arvioitiin kysymällä pilvipalveluihin käytetyn budjetin suhdetta IT:hen kokonaisuutena käytettävään rahaan. Luonnetta taas arvioitiin sen mukaan, mikä oli haastateltavien näkemys eri pilvipalvelukategorioiden käytön suhteellisesta osuudesta. Tarkasteltavia kategorioita olivat IaaS-, PaaS- ja SaaS-palvelut. Kysymyksissä kysyttiin myös, miten yritys arvioi kategorioiden käytön kehittyvän lähitulevaisuudessa. Lopuksi kysyttiin, miten haastateltava arvioi pilvipalveluiden käytön liiketoimintakriittisyyttä omalle organisaatiolleen.

Vastauksista selvisi, että pilvipalveluiden käytön laajuudessa oli organisaatioiden välillä suurta vaihtelua. Ääripäinä joukossa olivat organisaatiot, jolla pilvipalveluiden käyttö oli vasta alkamassa ja toisaalta organisaatiot, joiden IT:n strategisessa fokuksessa oli käyttää pilvipalveluita kaikessa mahdollisessa mihin se soveltuu. Haastatteluista noin kolmannes käytti pilvipalveluihin alle 10 % IT-budjetista, yli kolmannes 10–50 % ja muutama yli 50 %. Muutama organisaatio ei tiennyt pilvipalveluiden kustannusten osuutta kokonaisuudesta. Kaikki vastaajat kertoivat suunnitelmista lisätä pilvipalveluiden käyttöä.

Kaikki pilvipalvelukategoriat (IaaS, PaaS ja SaaS) olivat käytössä. SaaS-palveluiden käyttö oli laajinta ja niitä käytti jokainen haastateltu organisaatio. Suurimmalla osalla haastatelluista Saas-palveluja oli palvelukategorioista käytössä eniten sekä palveluiden määrän suhteen että käyttäjien määrän suhteen. IaaS- infrastruktuuripalveluita käytetiin yli puolessa organisaatioista.

PaaS-alustapalvelut olivat käytössä kolmessa neljästä organisaatiossa. Niitä käytettiin yleensä omaan käyttöön kehitettyjen tai räätälöityjen järjestelmien suoritusympäristönä. Microsoftin Azure -pilvipalveluteknologia oli yleisin valinta. Muut palveluntuottajat olivat selkeästi vähemmistönä haastateltavien keskuudessa.

Kysyttäessä käytettyjen pilvipalvelujen liiketoimintakriittisyyttä moni vastaaja arvioi asiaa käytettävyyden näkökulmasta. Näin tarkasteltuna käytössä olevia

pilvipalveluita pidettiin liiketoiminnan kannalta pääosin tärkeinä tai hyvin tärkeinä, mutta aivan äärimmäisen kriittisiä ne olivat vain harvoilla. Useimpien organisaatioiden mukaan lyhyet ohimenevät häiriöt pilvipalveluissa varmasti häiritsevät liiketoimintaa, mutta eivät estä sitä.

4.1.2 Menettelyt ja välineet

Haastattelun tavoitteena oli selvittää, mitä menettelyitä ja välineitä organisaatioilla on käytössään pilvipalveluiden kyberturvallisuusuhkien havainnoimiseksi. Saatuja tietoja käytettiin tutkimuksen kokeiluvaiheen kohteen täsmentämiseen ja valintaan. Haastattelun teemat oli ryhmitelty viiteen ryhmään: lokitus- ja monitorointi, konfiguraationhallinta, haavoittuvuuksienhallinta, käyttäjän- ja pääsynhallinta sekä Saas-palvelut. Lisäksi keskusteltiin muutamista kaikille ryhmille yleisistä aiheista.

Laajimmin käytetty pilvipalvelualusta IaaS ja PaaS -palveluihin oli Microsoftin Azure -alusta. Useilla käyttäjillä on käytössään sen laajempi lisensiointisopimus (E5), joka tarjoaa monin muiden ominaisuuksien lisäksi monipuoliset tietoturvatyökalut lokitukseen ja monitorointiin. Vastaajat myös ilmoittivat käyttävänsä näitä ominaisuuksia aktiivisesti. Kolmansien osapuolien tuotteita lokitukseen ja monitorointiin käytettiin myös noin puolessa organisaatioista. Niiden osalta ei löytynyt yhteistä nimittäjää, vaan käytettyjen välineiden valikoima oli laaja.

Pilviympäristöjen konfiguraationhallinta ei ole juuri lainkaan automatisoitua tai oli jonkin verran automatisoitua. Haastattelujen perusteella vaikuttaa siltä, että konfiguraation automaatioon on panostettu suurissa organisaatioissa tai sellaisissa organisaatioissa, joissa ydinliiketoiminta itsessään on digitaalista. Käytetyissä välineissä tuotteiden kirjo oli laaja.

Ympäristöjen vakioinnin merkitys oli ymmärretty organisaatioissa hyvin ja suurimmassa osassa oli pyritty vakioimaan niitä ainakin joltain osin. Vakiointia oli kohdistettu eri asioihin: toimittaja- ja hankintavaatimuksiin, pilviympäristön hallintamalliin, infrastruktuuriin, sovellusarkkitehtuuriin ja suoritusympäristöön.

Lähes kaikki organisaatiot hyödynsivät palveluntuottajien parhaita käytäntöjä ja suosituksia. Niitä pidettiin yleisesti hyödyllisinä tietoturvan parantamiseksi. Suosituksia pitää jonkin verran soveltaa tapauskohtaisesti, mutta ne ovat helposti lähestyttäviä ja käyttökelpoisia työkaluja. Organisaatiot toivoivat viranomaisilta apua ja tukea parhaiden käytäntöjen hyödyntämiseksi.

Haavoittuvuuksien hallinnassa hyödynnettiin laajasti pilvipalveluntuottajien tarjoamia välineitä ja tietoturvaraportteja. Myös kolmansien osapuolien tuotteita käytettiin edellä mainittujen ohessa. Vastaajien joukossa oli jonkin verran epäselvää mikä on oman organisaation tilanne ja käytetyt välineet haavoittuvuuksien hallinnan osalta.

Palveluille ei juuri lainkaan tehdä jatkuvaa auditointia tai penetraatiotestauksia. Jatkuvan auditoinnin käsite oli monelle vastaajalle vieras. Ajoittaisia auditointeja tai tarkastuksia tehtiin kyllä järjestelmille, etenkin kun kyseessä oli joku merkittävä muutostilanne kuten uuden sovelluksen käyttöönotto tai iso sovelluspäivitys. Penetraatiotestausta ei joko tehty lainkaan tai sitä tehtiin satunnaisesti. Sovelluksen penetraatiotestaus kuului joissakin organisaatiossa ensikäyttöönoton yhteydessä suoritettavaan tarkastukseen, mutta myöhemmin sitä enää tehty.

Haastateltavilta kysyttiin, mitä välineitä he käyttävät käyttäjien pääsyn- ja käyttäjähallinnan muutosten monitorointiin ja reagointiin. Haastateltavat jäivät usein pohtimaan kysymystä ja miettimään, mitä muutosten monitorointi tarkoittaa. Pääsääntöisesti tähän tehtävään olivat käytössä pilvipalvelujen tuottajien tarjoamat välineet käyttäjien- ja pääsynhallintaan. Tämän lisäksi ei nähty tarvetta erillisille välineille muutosten seuraamiseksi ja valvomiseksi.

Käyttäjä- ja identiteetinhallinnan yhteydessä kysyttiin myös sitä, käyttävätkö organisaatiot jotain yleisesti tunnettua mallia kyberturvallisuuden viitekehyksenään. Suurin osa vastaajista ei maininnut ainuttakaan. Tietosuoja-asetus ja ISO 27001 saivat joitakin mainintoja. Muutamissa vastauksissa mainittiin omaan toimialaan tai liiketoimintaympäristöön liittyviä standardeja tai viranomaismääräyksiä, jotka joltain osin käsittelevät tai sivuavat kyberturvallisuutta.

Lopuksi menettelyiden ja välineiden osuudessa keskusteltiin haastateltavien kanssa hyvin yleistäen, mitä menettelyjä tai työkaluja heillä on käytössä palveluna ostettavien sovellusten (SaaS-palvelut) monitorointiin ja valvontaan. Käytännöt vaihtelivat organisaatioiden välillä. Jonkin tasoisia teknisiä valvontakeinoja oli käytössä 60 prosentissa organisaatioista. Eniten oli toteutettu käyttäjähallinnan integraatioita omaan AD-hakemistopalveluun. Keskitetyn käyttäjähallinnan ohessa saadaan valvontanäkymä käyttäjien oikeuksiin ja sisäänkirjautumisiin. Muutamassa tapauksessa oli pystytty tekemään integraatio SaaS-palvelun ja organisaation oman valvontajärjestelmän välille.

Monet organisaatiot olivat valinneet SaaS-palveluiden osalta kyberturvallisuuden monitorointiin ja valvontaan sopimuksellisen mallin. Siinä palvelutuottajan kanssa on sovittu tietoturvaan liittyvien uhkien ja riskien hallinnasta ja raportoinnista. Tässä mallissa teknistä valvontaa ei ole juuri lainkaan. Kaikilta osin tähän vaihtoehtoon ei oltu tyytyväisiä ja koettiin, että usein asiakas joutuu tyytymään palvelutuottajan määrittelemiin sopimusehtoihin ja toimittamiin tietoihin, eikä vaikuttamismahdollisuutta ole. Asiakkaan tehtäväksi jää sopeutua ja luottaa toimittajaan. Palveluntuottajien hallintakäyttöliittymien tai -raporttien ei erityisemmin katsottu olevan hyödyllisiä tietoturvan monitoroinnissa ja valvonnassa.

Haastatelluissa organisaatioissa on tyypillisesti korkea ulkoistusaste tietoturvan operatiivisten palveluiden osalta. Tämä koskee myös havainnointia ja tilannekuvan muodostamista. Monissa tapauksissa käytettävät työkalut tulevat toimittajilta osana palvelupakettia. Toimintamallit ja käytännöt suunnitellaan ja sovitaan kuitenkin yleensä yhteistoiminnassa. Välineitä ei ole oikeastaan lainkaan räätälöity omia tarpeita vastaamaan, vaan on tyydytty valmisratkaisuihin. Räätälöinnin kalleus ja valmisratkaisujen monipuolisuus olivat joidenkin haastateltavien mainitsemia syitä räätälöinnin vähäiseen kiinnostukseen.

Välineitä ja menettelyitä kartoitettaessa kysyttiin lopuksi havainnoinnin ja reagoinnin automaatioasteesta. Yli puolet organisaatioista luonnehti, että tietoturvapoikkeamien havainnoinnin automaation taso on korkea. Suurin osa piti kuitenkin oman reagointikyvykkyytensä automaatiota vähäisenä. Useilla vastaajilla ei ollut selkeää kuvaa organisaationsa havainnoinnin ja reagoinnin auto-

maation tilasta. Onnistuneissa toteutuksissa – joissa reagointia on menestyksekkäästi automatisoitu – on vastausten mukaan keskitytty tiettyjen usein esiintyvien, tärkeiden ja helposti toteutettavien toimenpiteiden automatisointiin pyrkimättä mitenkään erityisen laaja-alaiseen toimenpidekattavuuteen.

4.1.3 Tilannekuvan laatu

Teemahaastatteluissa kysyttiin haastateltavilta heidän käsitystään pilvipalveluiden kyberturvallisuuden tilannekuvan laadusta. Kysymyksillä pyrittiin selvittämään miltä osin tilannekuvaan oltiin tyytyväisiä ja miltä osin se kaipaa parantamista. Tavoitteena oli näin selvittää, mitä kehittämiskohteita on ja miten tietoa voisi käyttää tutkimuksen kohdentamisessa.

Vastausten mukaan uhkien havainnointi on tehokasta ja palvelee tarkoitustaan vähintään joillain pilviturvallisuuden osa-alueilla. Useita mainintoja sai identiteetinhallinta ja identiteetin väärinkäytöksien valvonta. Pilvipalveluntoimittajien tarjoamiin perustietoturvapalveluihin oltiin kokonaisuutena tyytyväisiä. Ulkoisten palvelukeskuskumppaneiden (*Security Operations Center*, SOC) havainnointi- ja reagointikyky nostettiin esille usein hyvässä valossa.

Puutteita uhkien havainnoinnissa lueteltiin runsaasti. Suurin osa vastaajista otti esille, että havainnointi on jossain määrin puutteellista ja sekavaa. Useampi vastaaja nimesi seuraavia puutteita: pirstaleinen ja epäselvä tilannekuvanäkymä, heikko näkymä Saas-palveluihin ja monitoimittajaympäristön epäselvät vastuut. Se, miten laajasti omat palvelut ja rajapinnat ovat avoimena ja näkyvissä muille käyttäjille, oli epäselvää ja koettiin vaikeaksi hallita. Käyttäjille on myös epäselvää, mitä komponentteja ja ominaisuuksia palvelut pitävät sisällään. Edellisten lisäksi joissakin organisaatioissa koettiin ongelmia ns. varjo-IT:n kanssa. Käyttöönottoja tehtiin omavaltaisesti sisäisten prosessien ohi, sillä omat sisäiset pelisäännöt siitä, miten ja kuka pilvipalveluita hankkii ja ottaa käyttöön, olivat epäselviä.

Havainnoinnin välineiden keskinäisen integroinnin mahdollisuudet olivat vastaajien mukaan hyvät. Integraatio toimii erityisen hyvin palveluntuottajan

omien välineiden kesken. Eri toimittajien välillä integrointi on vastaajien mukaan mahdollista, mutta osin puutteellista ja haastavaa. Erilaisia standardeja ja rajapintoja on käytettävissä havaintojen tietojenvaihtoa varten.

Vastaajia pyydettiin pohtimaan, onko pilvipalveluiden kyberturvallisuudessa jotain ominaisuuksia, jotka parantavat selvästi nykyisten prosessien ja kyvykkyyksien tasoa tai tuovat selvästi uusia kyvykkyyksiä. Useita mainintoja saivat resurssienhallinta ja päivitystenhallinta. Infrastruktuurin tuottamista ohjelmallisesti (*Infrastructure as a code* -konsepti) pidettiin merkittävänä uutena kehitysaskeleena. Microsoftin Azure-alustan osalta nostettiin esiin identiteetin ja pääsynvalvonta AzureAD-hakemistopalvelussa sekä Microsoftin Azure-alustaan liittämät tietoturvapalvelut ja -työkalut. Moni vastaaja oli sitä mieltä, että tietoturva kehittyy ja paranee kokonaisuutena nopeammin pilviympäristöissä kuin perinteisissä ympäristöissä on totuttu.

Haastateltavilta kysyttiin millä pilviturvallisuuden osa-alueilla on heidän mielestään eniten tarvetta turvallisuusuhkien havainnoinnille. Suurin osa mainitsi verkkoliikenteen havainnoinnin pilven ja julkisen internetin reunalla. Useissa vastauksissa tuli esille myös käyttäjien toiminnan havainnointi, konfiguraatioiden hallinta sekä muutokset ja Saas-palveluiden monitorointi. Huolta herätti myös se, että haavoittuvuuksien hallinta ei ole täysin omissa käsissä, vaan siinä luotetaan paljon palveluntuottajaan.

4.1.4 Organisaatioiden odotukset kansalliselta pilvitilannekuvalta

Teemahaastattelun päätteeksi kysyttiin vastaajien odotuksia Kyberturvallisuuskeskuksen tilannekuvatuotteiden kehittämisestä. Pilvipalveluiden mukaan ottamista pidettiin useimmissa vastauksissa tärkeänä ja tarpeellisena. Palvelulta toivottiin selkeyttä ja konkretiaa. Jotkut vastaajat näkivät hyvänä vertailukohtana Kyberturvallisuuskeskuksen HAVARO-palvelun ja toivoivat KTK:n laajentavan sitä koskemaan myös pilvipalveluja. Lisäksi toivottiin tukea tilannekuvan automatisaatiolle, jossa manuaalivaiheita olisi vähän ja tarvittaessa voitaisiin rakentaa asian kulku hälytyksestä toimenpiteeksi saakka.

4.2 Käytännön työkalun kokeilu

Teemahaastatteluna tehdyllä lähtötilannekartoituksella selvitettiin, mitä välineitä ja menetelmiä huoltovarmuuskriittiset organisaatiot käyttävät pilviturvallisuuden havainnointiin. Selvityksen perusteella Microsoftin Azure -pilvipalvelualusta oli kohderyhmässä yleisimmin käytetty. Se valittiin kokeilun kohteeksi, koska näin saavutettiin kokeilulle riittävä laaja-alaisuus ja kattavuus kohderyhmänä olevassa yrityskentässä.

Laaja-alaisuuden lisäksi eräänä ennalta asetettuna tavoitteena oli toteuttaa ratkaisu, jossa käytetään hyväksi yritysten jo käytössä olevia havainnointimenetelmiä ja -välineitä. Lähtötilannekartoitus ei tuonut esille mitään tiettyä tietoturvatuotetta tai -palvelua, jota olisi yleisesti käytetty organisaatioissa. Sen sijaan havaittiin, että Azure-pilvipalvelualustan käyttäjät hyödynsivät jonkin verran alustan toimittajan tarjoamia havainnointimenetelmiä ja -välineitä. Useimmat yritykset olivat esimerkiksi investoineet sellaisiin tuotelisensseihin, jotka tarjosivat heidän käyttöönsä perusmuotoisia käyttäjälisenssejä edistyneempiä tietoturvaominaisuuksia mm. uhkien havainnointiin. Näiden seikkojen vuoksi kokeilussa päätettiin käyttää hyväksi pilvipalvelualustan itsensä tarjoamia rajapintoja sekä tietoja ympäristön turvallisuuden tilan arvioimiseksi.

Edellä mainituilla perusteilla voidaan sanoa, että tutkimuksen tavoitteena ollut laaja-alainen sovellettavuus Kyberturvallisuuskeskuksen asiakasyritysten kentässä saavutettiin, vaikka mukana ei ollutkaan muita globaaleja pilvialustatoimittajia. Jatkotutkimuskohteena on kuitenkin pyrittävä selvittämään kokeilussa toteutetun konseptin sovellettavuutta muihin käytetyimpiin pilvialustoihin.

4.2.1 Suunnittelu ja toteutus

Käytännön kokeilun suunnittelussa ja toteutuksessa käytetiin hyväksi Kyberturvallisuuskeskuksen asiantuntijoita ja ulkoisia konsultteja. Tutkimuksen tekijän ja asiantuntijoiden muodostaman työryhmän kesken selvitettiin kerättävissä olevia tietoja ja tunnistettiin sen perusteella analysoitavia kohteita. Kokeilun tarkastelukohteiksi valikoitiin joukko pilvipalvelualustan asetuksia, joilla on käytännön vaikutus asiakkaan käytössä olevan alustan turvallisuuteen. Valitut asetukset ovat sellaisia, joiden määrittely yleensä kuuluu asiakkaan vastuulle.

Erotuksena tavanomaiseen tietoturvatarkastukseen tai -auditointiin pyrittiin hyödyntämään automaatiota tiedon keruussa sekä luomaan edellytyksiä jatkuvalle havainnoinnille. Perinteisessä mallissa tietoturva-asiantuntija käy läpi asiakkaan järjestelmäympäristön käytännössä manuaalisesti tai omia työkalujaan käyttäen. Hän pyrkii löytämään sieltä puutteellisia tai virheellisiä konfiguraatioita, joilla on mahdollisesti vaikutusta ympäristön kyberturvallisuuteen. Tässä kokeilussa suunniteltiin ja toteutettiin tiedonkeruutyökalu, jolla vastaava läpikäynti on mahdollista toteuttaa automatisoidusti ja keskitetysti kohdistaen se useisiin asiakasympäristöihin. Työkalua kutsuttiin nimellä Traficom Risk Score. Kokeilulle asetettuja tavoitteita olivat tiedon keruun automatisointi, keskittäminen ja integrointi Kyberturvallisuuskeskuksen tarpeisiin. Asetettuihin tavoitteisiin löydettiin ratkaisuja työkalua kehitettäessä.

Tarkasteltavaksi valitut asetukset vaikuttivat työryhmän arvion mukaan palvelun koko asiakasilmentymän turvallisuuteen. Virheellinen asetus tai liian löyhästi rajattu käyttöoikeus voi synnyttää tietoturvauhan, joka kohdistuu saman aikaisesti useimpiin palvelukomponentteihin asiakkaan pilvipalvelussa. Toisaalta tarkasteltavaksi valitut asetukset ovat laajasti hyödynnettyjä ja voivat olla käytössä hyvin erilaisissa pilvipalvelun käyttövaihtoehdoissa. Näitä ovat suppeasti käytetyt Saas-palvelut ja laajat asiakastarpeisiin räätälöidyt pilvi-infrastruktuuriratkaisut, joten kohteiden valinnat tukivat kokeilun tavoitetta laaja-alaisesta hyödynnettävyydestä heterogeenisessä käyttäjäkunnassa.

Tiedonkeruun kohteeksi valittiin 34 sellaista konfiguraatiokohdetta, joilla arvioitiin olevan merkitystä asiakkaan ympäristön kyberturvallisuudelle. Kunkin kohteen osalta arvioitiin lisäksi, mikä olisi oletusarvoisesti oikea tapa toteuttaa kyseinen konfiguraatio sekä pyrittiin vertaamaan tätä Microsoftin määrittelemiin parhaisiin käytäntöihin, jos sellainen oli saatavilla. Valinnassa vältettiin päällekkäisyyksiä Azure-ympäristöön valmiiksi rakennettujen tarkastusvälineiden tuottamien raporttien kanssa. Asiantuntijatyönä pyrittiin valitsemaan erityisesti suomalaisten organisaatioiden näkökulmia ja käyttötapauksia.

Tarkastettaviin kohteisiin määriteltiin kerättävät tiedot, joiden perusteella voitiin arvioida kohteen asetusten tila. Keruun toteuttamiseksi selvitettiin tarvittavat

komennot ohjelmointirajapinnoille. Kohteisiin liitettiin myös tekstikuvaus kohteen merkityksestä kyberturvallisuudelle sekä oletus- tai vertailuarvo, johon asiakasympäristöstä kerättyä dataa vertaamalla voitiin päätellä kohteen sen hetkinen turvallisuuden taso. Tavoitteena oli saada selkeitä kyllä- ja ei-vastauksia sen mukaan, oliko kohteessa ongelma vai ei.

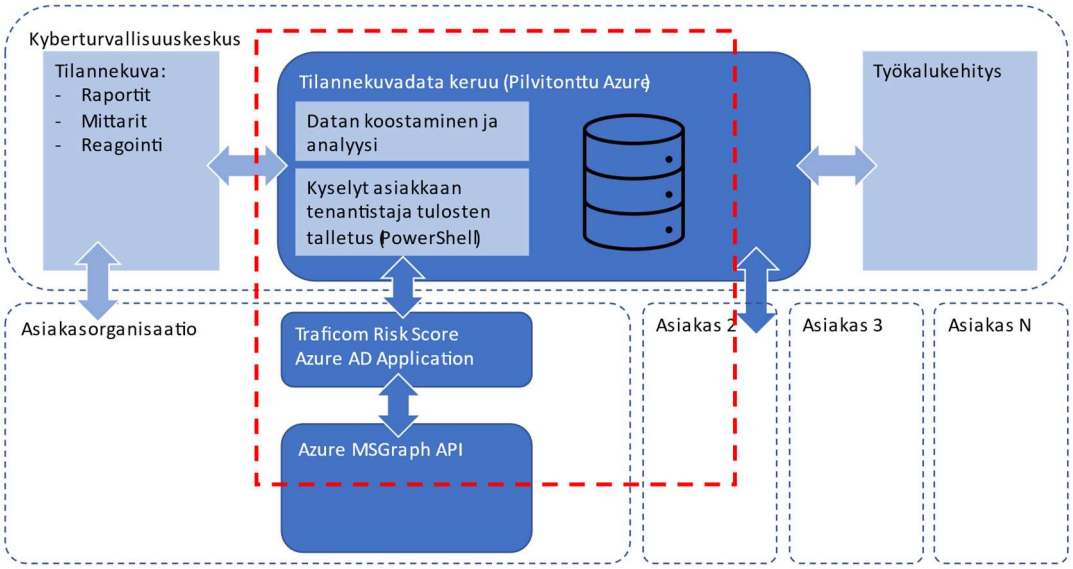
4.2.2 Tekninen ratkaisu

Pilvipalvelualustoille on tyypillistä, että niiden infrastruktuuri on määriteltävissä täysin ohjelmallisesti. Tämä tarkoittaa, että kaikki käytettävät resurssit ja asetukset voidaan luoda, ylläpitää ja poistaa ohjelmoimalla. Ominaisuus koskee niin virtuaalikoneita, tietoliikennettä, tallennuskapasiteettia kuin myös sovelluksia ja käyttäjähallintaa. Pilvipalvelualustat tarjoavat ohjelmoitavaa hallintaa varten omia työkalujaan ja ohjelmointirajapintojaan. Azuressa on käytettävissä REST API -mallin mukainen yhdyskäytävä Ms Graph, jolla voidaan mm. ylläpitää ympäristöjä ja kerätä sieltä tietoa.

Rajapintoja voidaan ohjelmoida lähes kaikilla käytettävissä olevilla ohjelmointivälineillä. Näin ollen ohjelman kehittäjä voi valita melko vapaasti omien tarpeidensa mukaan käytettävät välineet. Joissakin välineissä on kuitenkin valmiina sisäänrakennettuna tukea alustojen ohjelmalliseen operointiin. Microsoftin PowerShell on ohjelmointityökalu ja ajoympäristö, jossa on valmiina kirjastot Azuren rajapintojen tehokkaaseen käyttöön.

Azure-ympäristö tarjoaa suoraviivaisen teknisen ratkaisun kokeilussa tarvittavaan reittiin tietojen keräämiseksi asiakkaiden ympäristöistä. Azure Active Directory -sovellukset ovat kolmansien osapuolien tuottamia sovelluksia, joita asiakkaat voivat aktivoida käyttöönsä. Kolmas osapuoli operoi sovellusta omassa Azure-ympäristössään. Asiakas ottaa sovelluksen käyttöön valtuuttamalla sille sovitulla tavalla pääsyn omaan ympäristöönsä. Kun käyttöönotto on tehty, voi kolmannen osapuolen sovellus tehdä erilaisia toimenpiteitä asiakkaan ympäristössä annettujen oikeuksia mukaan. Tässä kokeilussa Traficom Risk Score -sovellusta käytettiin tietojen lukemiseen asiakkaan ympäristön asetusten tilasta.

Tiedonkeruutyökalun tekninen arkkitehtuuri on esitetty kuvassa 4. Tilannekuvadatan keruu ja tietojen talletus tapahtui keskitetysti. Työkalu sai pääsyn asiakkaiden Azure-ympäristöihin Azure AD Application -rekisteröinnin kautta. Kyselyt suoritettiin kokeilua varten laaditulla PowerShell -komentojonolla, joka käytti MS Graph -rajapinnan palveluita ja tietorakenteita kyselyiden suorittamiseen.



Kuva 4. Työkalun arkkitehtuuri

Sovelluksen käyttöönottoa varten laadittiin ohje, jossa sovelluksen turvallisuuteen kiinnitettiin erityistä huomiota. Asiakas määritteli käyttöönoton yhteydessä sovellukselle teknisen käyttöoikeuden, johon liitetty salasana aktivoitiin käyttöön sovelluksessa. Asiakas antoi sovellukselle oikeudet, jotka sallivat ainoastaan tietojen lukemisen asiakkaan ympäristöstä. Lisäksi oikeuksien voimassaoloaika rajoitettiin kokeilun kestoajan mukaan. Sovelluksen pääsy sallittiin vain Kyberturvallisuuskeskuksen käyttämän ympäristön osoiteavaruudesta.

Tutkimuksen tavoitteena oli ensisijaisesti löytää tekninen ratkaisu tiedon keruun automatisointiin ja laaja-alaiseen käyttöön. Tämän vuoksi kerättyjen tietojen raportointi ja analyysi jätettiin tutkimuksen aikana vähäisemmäksi. Raportointi keskittyi ennen kaikkea luettelemaan tulokset tarkastetuista kohteista sekä auttamaan tulosten tulkinnassa kuhunkin kohteeseen liitetyn sanallisen selityksen avulla. Keräystyökalu tuotti raportit sekä HTML- että JSON-muotoisina. Ensin mainittua voitiin käyttää asiakkaiden kanssa yhteiseen läpikäyntiin.

Jälkimmäistä aineistomuotoa voidaan käyttää datan ohjelmalliseen jatkokäsittelyyn, kun dataa halutaan siirtää Kyberturvallisuuskeskuksen käyttämiin tilannekuva-analyysivälineisiin.

4.2.3 Työkalun kokeilun tulokset

Tutkimuksessa toteutetussa kokeilussa testattiin työkalua neljän eri organisaation pilviympäristöissä. Kokeiluun osallistuneet organisaatiot hankittiin Kyberturvallisuuskeskuksen verkostoja hyödyntämällä. Tarkasteltavia kohteita toteutettiin kokeilua varten 34 kpl. Näiden lisäksi kerättiin erilaisia perustietoja asiakkaan pilviympäristöstä, kuten ympäristön rakenne ja käytetyt palvelukomponentit. Tarkasteltavissa kohteissa käytettiin lisäksi Azure-ympäristön tarjoamia valmiita kohteita. Tarkastelu kohdistui erilaisiin pilviympäristön toiminnallisiin kokonaisuuksiin, kuten tietoliikenteen tai pääsynhallinnan asetuksiin. Taulukossa 1 on esitetty tarkasteltavien kohteiden jaottelu ja lukumäärä toiminnallisten kokonaisuuksien mukaisesti. Taulukossa on myös lueteltu esimerkkejä toteutetuista konkreettisista tarkastelukohteista. Kaikki kokeilussa toteutetut tarkasteltavat kohteet on lueteltu liitteessä 2.

Taulukko 1. Tarkastettujen kohteiden lukumäärä, toiminnalliset kokonaisuudet ja esimerkkejä kohteista

Toiminnallinen kokonaisuus	**Kohteiden lukumäärä kokeilussa**
Yleiset tuvallisuuskyvykkyydet	2
Laitehallinta	2
Käyttäjien- ja pääsynhallinta	18
Kolmansien osapuolien sovellukset	1
Tietoliikenne	5
Tallennusresurssien turvallisuus	6
Infotiedot	7

Kullekin tarkastettavalle kohteelle määriteltiin tavoitearvo- tai kuvaus, jota verrattiin kyselyn lopputuloksena asiakkaan ympäristöstä poimittuun arvoon. Osalle kohteista voitiin määritellä tarkka ja vertailtavissa oleva arvo tavoitteen ja poiminnan välille. Mikäli poimittu arvo vastasi ennalta määriteltyä tavoitearvoa, raportille merkittiin, että ko. kohteen osalta ei ole turvallisuusriskiä.

Suurelle osalle kohteista oli välttämätöntä tehdä tulkintaa ennen johtopäätöksien tekemistä. Tulkintaa pyrittiin tekemään muista mittareista saadun tiedon perusteella yhdistelemällä tai keskustelemalla asiakkaan kanssa. Tulkinnan tarve saattoi johtua useasta eri seikasta, esimerkiksi tarkasteltavan kohteen tavoitearvo ei ollut helposti määriteltävissä tai se ei ollut yksikäsitteinen. Asiakkaan ympäristöstä poimittu tulos ei aina kertonut kaikkea tarkastelun kohteena olleen turvallisuusasetuksen tilasta. Oli mahdollista, että tarkastettavana ollut turvallisuusriski oli ratkaistu jollain muulla vaihtoehtoisella tavalla, eikä poimittu arvo näin ollen vastannut tyhjentävästi asiaan. Joissakin tapauksissa tarvittiin tarkempaa selvitystyötä ja keskustelua asiakkaan kanssa tarkasteltavan kohteen käytöstä ja merkityksestä kokonaisuuden turvallisuudelle, ennen kuin johtopäätöksiä ko. kohteen osalta voitiin tehdä.

Seuraavassa käsitellään kahta kokeilun tarkastelukohdetta yksityiskohtaisemmin. Tavoitteena on kuvata näiden esimerkkien avulla kohteiden käyttöä kartoitettaessa kyberturvallisuusriskejä. Esimerkeissä käydään läpi kohteiden tunnistamista, teknistä toteutusta sekä kerättyjä tuloksia ja niiden tulkintaa.

Asiakaskohtaisessa Azure-pilviympäristössä tulisi olla määriteltynä käyttäjätunnus, jota voidaan käyttää hätätilanteissa (hätäpääsy*, emergency access* tai *break the glass account*). Käyttäjätunnus on sellaisia hätätilanteita varten, jossa jostain syystä pääsy ympäristöön normaalisti käytettävillä ylläpitokäyttäjätunnuksilla on muuten estynyt. Tämä voi johtua esimerkiksi häiriöistä monivaiheisessa kirjautumisessa, kirjautumiseen vaikuttavasta konfiguraatiovirheestä tai hakemistopalvelun toiminnan sekoittaneesta haittaohjelmasta. Hätäpääsytunnus on ainoastaan tätä erityistilannetta varten määritelty käyttäjätunnus ja tunnuksen käyttöä tulee valvoa tehostetusti. Sitä ei liitetä yhteenkään henkilöön, eikä sitä pidä käyttää muuhun ylläpitotyöhön. (Microsoft 2022.)

Traficom Risk Score -sovelluksella yritettiin selvittää, oliko hätäpääsyyn tarvittava käyttöoikeus määritetty ja oikein asetettu asiakkaiden ympäristössä, vai oliko olemassa riski, että asiakas menettää pääsyn ympäristöönsä kokonaan. Valmista sisäänrakennettua tapaa selvittää hätäpääsyn käyttäjätunnus tai

käyttöoikeus ei löydetty, joten asian selvittäminen oli sopiva kohde räätälöidyn kyselyn toteuttamiseksi.

Ensimmäiseksi asiaa selvitettiin etsimällä, oliko ympäristöstä löydettävissä sellaista käyttäjätunnusta, jonka ominaisuudet sopivat hätäpääsytunnukselle määriteltyihin parametreihin (Microsoft 2022). Ympäristöstä etsittiin käyttäjätunnusta, joka kuului globaaliin ylläpitäjäryhmään ja jonka käyttöoikeuksiin ei liittynyt lainkaan ehdollisia pääsykäytäntöjä. Esimerkkejä ehdollisista pääsykäytännöistä ovat mm. pakotettu monivaiheinen tunnistautuminen tai lähdeosoitteen perusteella tehty paikkatietoon perustuva pääsyn esto.

Tuloksia automaattisesti arvioitaessa em. ehdot täyttävä käyttäjätunnus oletettiin hätäpääsytunnukseksi ja tarkasteltava kohde raportoitiin olevan kunnossa. Mikäli ehdot täyttävää käyttäjätunnusta ei löytynyt pyrittiin vaihtoehtoisesti etsimään ympäristöstä tunnus tai tunnuksia, jotka parhaiten sopisivat hätäpääsytunnuksen määritelmään. Löydetyt tunnuskandidaatit listattiin asiantuntijan tekemää jatkotarkastelua varten, jos näihin käyttäjätunnuksiin kohdistuvia ehdollisia pääsykäytäntöjä löytyi tai käyttäjä ei kuulunut globaaliin ylläpitäjäryhmään. Kokeilussa mukana olleista ympäristöistä yksikään ei täyttänyt täysin hätäpääsytunnukselle asetettuja ehtoja: määritelmän mukaista tunnusta ei joko löydetty tai se ei kuulunut globaalien ylläpitäjien ryhmään. Tulosten perusteella ympäristöjen ylläpitäjät olivat kokeneet tarpeelliseksi ja perustelluksi määritellä kaikille tunnuksille joitain ehdollisia pääsykäytäntöjä.

Toisena tarkastelukohteena selvitettiin tarkemmin yhtä hätäpääsyn erikoistilannetta. Siinä selvitettiin, onnistuuko pääsy tilanteissa, joissa yhteys yrityksen hakemistopalveluun oli poikki. Sellainen hätäpääsytunnus, joka on rekisteröity Microsoftin omaan pilvihakemistoon (onmicrosoft.com), toimii myös näissä tilanteissa. Sen sijaan yrityksen omaan hakemistopalveluun määritelty tunnus ei ole käytettävissä ja hätäpääsy voi estyä. Kokeilukohteista yli puolet täyttivät tarkastellun ehdon.

Pilvialustan palvelut ja ominaisuudet muuttuvat jatkuvasti. Muutos näkyy myös kehittyvinä turvallisuusominaisuuksina. Uusia ominaisuuksia ei välttämättä vielä ole ymmärretty ottaa käyttöön yrityksissä. Jonkin aikaa ennen tässä tutkimuksessa käynnistettyä kokeilua talvella 2022, oli Azure-hakemistopalveluun

lisätty asetus, jonka avulla uuden laitteen rekisteröinnin yhteydessä voitiin pakottaa suoritettavaksi monivaiheinen tunnistautuminen. Kokeilussa tarkistettiin tämän asetuksen tila ja havaittiin, että yksikään asiakkaista ei ollut ottanut sitä vielä käyttöön.

Tutkimuksen kannalta olennainen havainto tässä oli se, että kokeilussa sovelletuilla keinoilla voidaan helposti reagoida alustan muutoksiin ja havainnoida kehittyvää teknistä ympäristöä. Uuden ominaisuuden tilan tarkastaminen oli mahdollista toteuttaa helposti kokeilussa käytetyllä ratkaisulla. Laiterekisteröinti oli jälleen yksi kohde, jossa tarvitaan tulkintaa ennen johtopäätöksiä: kaikkien asiakasympäristöjen osalta havainto puuttuvasta asetuksesta ei ole välttämättä kriittinen, sillä laitteiden rekisteröinnin varmistamiseen voi olla käytössä muita korvaavia kontrolleja.

Kokeilun aikana saatiin kerättyä useita raportteja asiakkaiden ympäristöjen tarkasteltavien kohteiden tilasta. Näitä raportteja voitiin verrata toisiinsa aikasarjana. Kokeilua aloitettaessa arveltiin, että vertailemalla voitaisiin löytää yllättäviä muutoksia tai poikkeamia. Näitä ei havaittu lyhyen tutkimusjakson aikana. Sen sijaan havaittiin, että ympäristöissä tapahtui ajojen välillä muutoksia, jotka oletettavasti johtuvat ympäristöjen dynaamisesta luonteesta ja jatkuvasti muuttuvasta käyttötavasta. Muutoksia aiheuttivat mm. käytettyjen pilvipalveluresurssien lisäykset ja poistot.

4.2.4 Tarkastelukohteiden linkitys PiTuKriin

Kokeilussa käytettyjen tarkastelukohteet voidaan linkittää PiTuKrin osa-alueisiin ja turvallisuusvaatimuksiin. Kriteeristö on hyödyllinen tämän tutkimuksen näkökulmasta, koska se on laadittu erityisesti suomalaisen yhteiskunnan kyberturvallisuuden tarpeiden näkökulmasta. Se on selkeä ohje tarvittaviin toimiin salassa pidettävän tiedon suojaamiseksi ja kohdistuu nimenomaan pilvipalveluihin. PiTuKri on tarkoitettu laajasti eri viranomaisten ja elinkeinoelämän käyttöön Suomessa. (Traficom 2020b.)

Kokeilussa keskityttiin erilaisten konfiguraatioasetusten ja -parametrien havainnointiin käyttäjien pilvipalveluympäristöistä. Kohteena oli siis palveluiden

tekninen turvallisuus. Tämän takia kaikkia PiTuKrin osa-alueita ei pyritä käsittelemään. Kohteena olivat osa-alueet 5–8: tietoliikenneturvallisuus, identiteetin ja pääsyn hallinta, tietojärjestelmäturvallisuus sekä salaus. Esimerkiksi turvallisuusjohtaminen ja henkilöstöturvallisuus rajautuivat näin pois. Taulukoissa 2 ja 3 on lueteltu PiTuKrin edellä mainitut osa-alueet ja sekä osa niiden vaatimusteemoista. Näihin liittyen on taulukossa kuvattu esimerkkeinä kohteita, joita kokeilussa havainnoitiin.

Taulukko 2. Esimerkkejä tarkastelukohteiden linkityksestä PiTuKrin osa-alueisiin 5 ja 6

PiTuKrin osa-alue ja vaatimusteema	Esimerkkejä kokeilussa toteutetuista tarkastelukohteista
Osa-alue 5: Tietoliikenneturvallisuus	
TT-01: Tietoliikenneverkon rakenne	
	– julkisten verkko-osoitteiden staattisuus
TT-02: Yleisiä verkkohyökkäyksiä vastaan suojautuminen	
	– palomuurisäännöt rajaavat liikennettä julkisesta internetistä palveluun – suojautuminen palvelunestohyökkäyksiltä
Osa-alue 6: Identiteetin ja pääsyn hallinta	
IP-01: Käyttöoikeushallinta	
	– ylläpito-oikeudet rajattu pois normaalilta käyttäjältä – käyttäjien oikeus liittää laitteita hakemistopalveluun rajoitettu – tallennusresurssin käyttö tunnistamattomilta käyttäjiltä estetty
IP-02: Käyttäjätunnistus	
	– vanhentuneet tunnistusmenettelyt poistettu käytöstä – monivaiheinen tunnistautumisen käyttö pakotettu ylläpitotunnuksilla – ehdolliset tunnistautumiskriteerit käytössä
IP-03: Hallintayhteydet	
	– hätäpääsytunnus määritelty käyttöön – hallintayhteystiedot määriteltynä ympäristön tietoihin

Taulukko 3. Esimerkkejä tarkastelukohteiden linkityksestä PiTuKrin osa-alueisiin 7 ja 8

PiTuKrin osa-alue ja vaatimusteema	Esimerkkejä kokeilussa toteutetuista tarkastelukohteista
Osa-alue 7: Tietojärjestelmäturvallisuus	
JT-01 Jäljitettävyys ja havainnointikyky	
	– ympäristön ohjelmistolisenssit ovat riittävän kattavat ja mahdollistavat havainnointikyvyn toteuttamisen
JT-02 Järjestelmäkovennus	
	– tallennusresurssin salaus vähintään TLS versiossa 1.2
Osa-alue 8: Salaus	
SA-01 Salauskäytännöt ja avainhallinta	
	– tallennusresurssien avaimia vaihdetaan säännöllisesti
SA-02 Salaus fyysisesti suojatun alueen ulkopuolella	
	– tallennusresurssien asetukset estävät turvattomat tiedonsiirrot

Taulukoiden 2 ja 3 perusteella voidaan nähdä, että tarkasteltavia kohteita voidaan määritellä ja toteuttaa useimpiin PiTuKrin osa-alueisiin ja vaatimusteemoihin. Työkalulla kokeiltua menetelmää voidaan siis käyttää laaja-alaisesti pilvipalvelun turvallisuuden arviointiin. Siten se vahvistaa merkittävällä tavalla teknistä pilviturvallisuutta. Koska pilvipalveluiden turvallisuuden arviointikriteeristön laadinnassa on hyödynnetty useita ulkomaisia kriteeristöjä ja standardeja, voidaan sitä pitää tämän tutkimuksen näkökulmasta hyvin kattavana viitekehyksenä. Kun tarkasteltavat kohteet ja niiden tuottamat tulokset linkitetään PiTuKriin, palvelee se Kyberturvallisuuskeskuksen tehtävää kyberturvallisuuden kokonaistilannekuvan muodostamisessa.

5 JOHTOPÄÄTÖKSET JA POHDINTA

Tutkimuksen tavoitteena oli löytää keinoja automatisoituun pilvipalveluiden kyberturvallisuusuhkien havainnointiin ja tilannekuvan muodostamiseen. Keinojen tuli olla laajasti käyttöönotettavissa huoltovarmuuskriittisissä yrityksissä ja yhteisöissä, jotta voitiin saavuttaa riittävä markkinakattavuus. Kokeilun kohdistaminen Microsoftin Azureen oli kattavuuden näkökulmasta perusteltua, sillä

teemahaastatteluissa kootun lähtötilanneanalyysin mukaan merkittävä osa suomalaisia huoltovarmuuskriittisiä organisaatioita käyttää Azure -pilvipalvelualustaa ainakin yhtenä vaihtoehtoisena pilvipalveluiden tuotantoalustanaan.

Vaikka Azureen keskittymällä saavutetaankin merkittävä kattavuus, on tosiasia, että kaikki yritykset eivät sitä käytä. Useilla muillakin pilvitoimittajilla on asiakkaita Suomessa. Globaalien vaihtoehtojen lisäksi yritykset käyttävät pienempien toimijoiden pilvipalveluita, jotka ovat usein jotain tiettyä käyttötarkoitusta varten räätälöityjä. Infrastruktuuri- ja alustapalveluiden lisäksi on suuri joukko erilaisia sovelluspalveluita pilvessä, joilla on laaja käyttäjäkunta. Teemahaastattelujen perusteella samalla yrityksellä voikin olla käytössään eri tarkoitusta varten useita sovellus- ja alustapalveluita. Laajaa kattavuutta on siis vaikea saavuttaa.

Tutkimuksen tavoitteena oli löytää keinoja automatisoida tietojen keruuta. KTK:n kohderyhmä on laaja, käsittäen suuren joukon suomalaisia organisaatioita. Näin ollen katsottiin datan keruun automatisoinnin olevan välttämätöntä tehokasta tilannekuvan muodostamista varten. Kokeilun tulokset osoittavat, että keskitetysti toteutettu automaattinen asiakasympäristöjen tietoturvatarkastelu on mahdollista toteuttaa.

Kokeilun teknisen ratkaisun ominaisuudet tarjoavat työkalun käyttäjälle mahdollisuuden uudistaa tarkastelun kohteita jatkuvasti. Kehittäminen tekee mahdolliseksi palvelun laajennettavuuden sekä antaa mahdollisuuden reagoida uusiin nouseviin uhkiin. Rajoitteena toimivat myönnetyt lukuoikeudet asiakasympäristöihin sekä kyselyrajapinnan jotkin puutteet. Kokeilussa käytetty työkalu on asiakkaan näkökulmasta varsin vaivaton. Se ei edellytä asiakkaiden investoivan maksullisiin pilviresursseihin, jotta kyselyt voidaan suorittaa. Näin ollen ylimääräisiä kustannuksia syntyy oikeastaan vain tulosten käsittelyyn käytettävistä asiantuntijaresursseista.

Asiakkaat ovat kokeilun kokemusten perusteella valmiita tilannekuvatiedon jakamiseen. He olivat valmiita avaamaan pääsyn ympäristöihinsä viranomaiselle, joka kerää dataa muodostaakseen tilannekuvaa. Kokeilun aikana saatiin kritiikkiä eräältä asiakkaalta siitä ovatko sovellusta varten pyydetyt lukuoikeudet tarpeellisia kaikessa laajuudessaan. Palaute oli aiheellista ja lukuoikeuksia

supistettiin kokeilun aikana. Kokeilussa käytetyn sovelluksen turvallisuusasetuksia tulee rajata huolellisesti, mikäli vastaavaa ratkaisua otetaan tulevaisuudessa tuotantokäyttöön. Pääsynhallinta on tehtävä sovellussertifikaatilla sekä tarkemmin määriteltyjä lukuoikeuksia käyttäen.

Kokeilussa kehitetyllä sovelluksella voidaan jossain määrin havainnoida kyberturvallisuusuhkia eri Azure-ympäristöissä. Kokeilua suunniteltaessa arvioitiin, että valituilla tarkasteltavilla kohteilla on merkitystä asiakkaan pilviympäristön kyberturvallisuudelle. Kerättyjen raporttien perusteella näin voitiin perustellusti todeta, sillä tarkasteltavien kohteiden todellisia arvoja voitiin verrata tavoitearvoihin ja vertailtaessa pystyttiin tekemään johtopäätöksiä turvallisuuden tilasta. Kerätty data ei aina muodostanut selkeää yksikäsitteistä tietoa siitä, oliko kyseinen arvioitavana ollut kohde kunnossa vai ei. Usein vaadittiin asiantuntijan analyysiä ja jatkoselvitystä, jotta voitiin varmistua tuloksesta. Tarve asiantuntijan tulkinnalle oli yhdenmukainen havainto teoreettisen tarkastelun kanssa (luku 3.3).

Tutkimuksen tavoitteena oli myös löytää keinoja tilannekuvan muodostamiseksi. Verrattaessa kokeilun tuloksia DFIG-malliin voidaan havaita, että tilannekuvan muodostamisessa päästiin tyypillisesti tasolle 2, jossa voitiin muodostaa ymmärrys tarkastellun kohteen tilasta ja verrata sitä tavoitearvoihin tai asiantuntija-analyysiin kohteesta. Jossakin yksittäisissä tarkastelukohteissa voitiin arvioida, että tuloksissa yllettiin parhaimmillaan DFIG-tasolle 3. Työkalulla voitiin tehdä tilannekuvan muodostamista edistävä tulkinta siitä, että kohteessa on asetusvirhe tai vaihtoehtoisesti kohde on kunnossa.

Kehitetty työkalu oli selkeimmin aihio jatkuvan auditoinnin välineestä. Se soveltui hyvin jonkin tietyn suojattavan kohteen turvallisuuskontrollin tai -asetuksen tilan selvittämiseen. Työkalu ei tässä muodossa tuottanut yksikäsitteisiä SIEM-tapahtumia tai tilannekuvaraporttia. Väline tuotti paljon raakadataa, jota ei voinut käyttää edellä mainittuihin käyttötarkoituksiin sellaisenaan. Data vaati jalostamista tiedoksi, jotta sitä voitiin käyttää yhteenvedoksi, hälytyksiksi tai tilannekuvaraportiksi.

Kokeiltu ratkaisu on laajennettavissa ja sen antamat tulokset yleistettävissä. Samat tiedot voidaan lukea kaikista ympäristöistä. Edellytyksenä kuitenkin on,

että tarkastelun kohteena olevia palvelukomponentteja on asiakkailla käytössä. Kerätyt tiedot ja arvot vaihtelivat asiakkaan ympäristön konfiguraation mukaan jossain määrin. Arvojoukko kehittyi ja muuttui ajan kuluessa, koska ympäristöt, teknologia ja palvelut muuttuivat. Tämä edellytti kyselyjen ajoittaista sovittamista muuttuvaan tilanteeseen. Muutoksen nopeudesta ei saatu tutkimuksen perusteella tietoa.

Palvelukattavuutta voidaan laajentaa ottamalla mukaan useampia palvelukomponentteja kuten vaikkapa konttiympäristöjä ja palvelimetonta tietojenkäsittelyä (*serverless computing*). Yksittäisten tarkastettavien kohteiden määrää voidaan kasvattaa merkittävästi. Kokeilussa kohteena olivat jotkin valikoidut pilvi-ilmentymän yleiset konfiguraatiot, joilla arvioitiin olevan merkitystä tietoturvan näkökulmasta, eikä niihin liittyviä valmiita Microsoftin tuottamia tarkastelutyökaluja ollut tutkimushetkellä tiedossa.

Ratkaisu on helposti laajennettavissa uusille asiakkaille. Se ei edellytä asiakkailta sitoutumista investointeihin pilvikapasiteettiin tai ohjelmistolisensseihin. Sopimus ratkaisun käyttöönotosta ja tietojen käytöstä riittää. Käyttöönottoa varten tehtiin asiakkaille kirjallinen ohje, joka osoittautui niin selkeäksi, että sen perusteella asiakkaat pystyivät tekemään oman osuutensa käyttöönotosta itsenäisesti.

Tutkimusta ja tuotekehitystä voi jatkaa eteenpäin useaan vaihtoehtoiseen suuntaan. Vastaavia automatisoituja tarkastuskohteita voi määritellä myös muihin pilvipalveluympäristöihin. Jotkut niistä tarjoavat vastaavia ohjelmointirajapintoja konfiguraatiotiedon keruuseen kuin Azure. Pilvipalvelualustat eroavat tekniikaltaan, arkkitehtuuriltaan ja palvelukonseptiltaan toisistaan. Niinpä niiden turvallisuusuhkien havainnointi muuttuu tapauskohtaisesti. Tämän takia MITTRE ATT&CK-viitekehyksessä eri pilvipalvelutuotteita ja käyttökonsepteja varten on nähty tarpeelliseksi luoda omat hyökkäysvektoreiden alakategoriat. Tarve viitekehyksen pilkkomiseksi alaryhmiksi konkretisoi sen, miten erilaisia ja toisistaan poikkeavia pilvipalvelutuotteet ja käyttökonseptit ovat uhkien ja hyväksikäyttömenetelmien osalta. Jatkotutkimuksessa olisi siis hyvä ottaa huomioon nämä erot ja pohtia olisiko järkevää ratkaista havainnointiakin saman jaon mukaan tapauskohtaisesti.

Sovelluspalvelut (SaaS-palvelut) ovat huomattavasti suljetumpia palveluita, joiden osalta olisi syytä tutkia toisenlaisia ratkaisuja. Palveluntuottajat eivät ole samalla tavalla halukkaita tai teknisesti kykeneviä avaamaan rajapintoja turvallisuuden havainnoimiseksi kuin suuret pilvi-infrastruktuuritoimittajat. Aihe on tärkeä, sillä näiden palveluiden käyttö lisääntyy, koska ne tarjoavat usein edullisia, innovatiivisia ja helposti käyttöönotettavia ratkaisuja organisaatioiden erilaisiin liiketoimintatarpeisiin. Tarve Saas-palveluiden turvallisuuden havainnoinnille tuli esille useassa haastattelussa tutkimuksen alkupuolella.

Kolmas jatkotutkimuksen aihe voisi olla kerätyn datan jatkojalostaminen valmiiksi havainnoiksi tai tilannekuvatiedoksi. Tämä pitäisi sisällään datan tarkempaa automaattista analysointia sekä tietojen yhdistelyä eri lähteistä kokonaiskuvan muodostamiseksi. Myös tarkastelukohteita tulee täsmentää ja tarkentaa, jotta saatujen tulosten perusteella voidaan tehdä selkeitä johtopäätöksiä esimerkiksi korjaavista toimenpiteistä päättämiseksi.

LÄHTEET

Amazon Web Services. s.a. Shared Responsibility Model - Amazon Web Services (AWS). WWW-dokumentti. Saatavissa: https://aws.amazon.com/compliance/shared-responsibility-model/ [viitattu 6.4.2022].

Blash, E., Bosse, E. & Lambert, D.A. 2012. High-Level Information Fusion Management and Systems Design. Norwood: Artech House. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 1.1.2022].

Canalys. 2021. Global cloud services spending exceeded US$47 billion in Q2 2021. Canalys. PDF-dokumentti. Saatavissa: https://canalys-prod-public.s3.eu-west-1.amazonaws.com/static/press_release/2021/1765417745cloud_pr_Q2_2021.pdf [viitattu 17.9.2021].

Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V.-G. & Kavallieros, D. 2019. The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. *Proceedings of the 8th International Conference on Data Science, Technology and Applications*, 369–376. Verkkolehti. Saatavissa: https://doi.org/10.5220/0007978103690376 [viitattu 21.9.2021].

CIS. 2021. CIS Controls Version 8. Center of Internet Security. WWW-dokumentti. Saatavissa: https://www.cisecurity.org/white-papers/cis-controls-v8/ [viitattu 20.9.2021].

CISA. 2021. PCII Program Factsheet. Cybersecurity & Infrastructure Security Agency. PDF-dokumentti. Saatavissa: https://www.cisa.gov/sites/default/files/publications/Fact%20Sheet%20-%20PCII%20Program-%20new%2021.pdf [viitattu 21.9.2021].

CSA. 2017. Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance. WWW-dokumentti. Saatavissa: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ [viitattu 4.4.2022].

Endsley, M.R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 1, 32–64. Verkkolehti. Saatavissa: https://doi.org/10.1518/001872095779049543 [viitattu 21.9.2021].

ENISA. 2018. Information Sharing and Analysis Center (ISACs) - Cooperative models. ENISA. WWW-dokumentti. Saatavissa: https://data.europa.eu/doi/10.2824/549292 [viitattu 23.9.2021].

Gartner. 2021. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021. Gartner. WWW-dokumentti. Saatavissa: https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021 [viitattu 15.9.2021].

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu. Helsinki: Gaudeamus. E-kirja. Saatavissa: https://kaakkuri.finna.fi [viitattu 17.9.2021].

Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J. & Skorupka, C. 2016. Guide to Cyber Threat Information Sharing. National Institute of Standards and Technology. PDF-dokumentti. Saatavissa: http://dx.doi.org/10.6028/NIST.SP.800-150 [viitattu 21.9.2021].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona : opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylän ammattikorkeakoulun julkaisuja. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi [viitattu 17.9.2021].

Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas: avain opinnäytetyön ja pro gradun kirjoittamiseen. Jyväskylän ammattikorkeakoulun julkaisuja. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi [viitattu 17.9.2021].

Karjaluoto, A., Oy, D., Parts, Ü., Oy, D., Lehtinen, R., Oy, D. & Frantti, T. 2019. Kasvua digitaalisesta turvallisuudesta : Tiekartta 2019–2030. Työ- ja elinkeinoministeriön julkaisuja 2019:17. Helsinki: Työ- ja elinkeinoministeriö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-327-405-1 [viitattu 17.9.2021].

Kyberturvallisuuskeskus. 2021. Tilannekuva ja verkostojohtaminen. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen [viitattu 17.9.2021].

Lehto, M., Limnéll, J., Kokkomäki, T. & Salminen, M. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf [viitattu 17.9.2021].

Microsoft. 2022. Manage emergency access accounts in Azure AD. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access [viitattu 20.4.2022].

MISP Project. 2021. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. MISP. WWW-dokumentti. Saatavissa: https://misp-project.org/ [viitattu 24.9.2021].

MITRE. 2022. MITRE ATT&CK. WWW-dokumentti. Saatavissa: https://attack.mitre.org/ [viitattu 5.1.2022].

NIST. 2009. NIST Mission, Vision, Core Competencies, and Core Values. National Institute of Standards and Technology. WWW-dokumentti. Saatavissa: https://www.nist.gov/about-nist/our-organization/mission-vision-values [viitattu 20.9.2021].

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg: National Institute of Standards and Technology. PDF-dokumentti. Saatavissa: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [viitattu 20.9.2021].

Peiris, C., Pillai, B. & Kudrati, A. 2021. Threat Hunting in the Cloud. New Jersey: Wiley. E-Kirja. [viitattu 1.5.2022].

Pennington, A., Appelbaum, A., Nickels, K., Schulz, T., Strom, B. & Wunder, J. 2019. Getting Started with ATT&CK. MITRE Corp. E-kirja. Saatavissa: https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf [viitattu 5.1.2022].

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. PDF-dokumentti. Saatavissa: https://tuhat.helsinki.fi/ws/files/127650174/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf [viitattu 21.9.2021].

Piirainen, K. & Gonzalez, R. 2013. Seeking Constructive Synergy: Design Science and the Constructive Research Approach. *DESRIST 2013: Design Science at the Intersection of Physical and Virtual Design*, 59–72. Berlin: Springer. Konferenssijulkaisu. Saatavissa: https://doi.org/10.1007/978-3-642-38827-9_5 [viitattu 21.9.2021].

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. & Katos, V. 2020. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers* 9 1, 18. Verkkolehti. Saatavissa: https://doi.org/10.3390/computers9010018 [viitattu 27.9.2021].

Sanastokeskus TSK. 2018. Kyberturvallisuuden sanasto. WWW-dokumentti. Saatavissa: https://termipankki.fi/tepa/fi/haku/kybertilannekuva [viitattu 17.9.2021].

Skopik, F. 2017. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. Milton: Auerbach Publishers Inc. E-kirja. Saatavissa: https://kaakkuri.finna.fi [viitattu 27.9.2021].

Strom, B., Battaglia, J.A., Kemmerer, M.S., Miller, D.P., Wampler, C., Whitley, S.M. & Wolf, R.D. 2017. Finding Cyber Threats with ATT&CK-Based Analytics. MITRE Corp. PDF-dokumentti. Saatavissa: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf [viitattu 5.1.2022].

Traficom. 2020a. Usein kysyttyjä kysymyksiä HAVARO-palvelusta. WWW-dokumentti. Saatavissa: https://www.havaro.fi/fi/ukk [viitattu 12.8.2021].

Traficom. 2020b. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf [viitattu 15.9.2021].

Traficom. 2020c. Kybermittari, Arviointityökalu. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Arviointity%C3%B6kalu_V1.xlsx [viitattu 15.9.2021].

Traficom. 2022. Kybermittari - Kyberturvallisuuden arviointityökalu. Excel-tiedosto. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittarin%20arviointity%C3%B6kalu_v2_RC_web.xlsx [viitattu 5.5.2022].

Turvallisuuskomitea. 2019. Suomen kyberturvallisuusstrategia 2019. PDF-Dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf [viitattu 12.8.2021].

Valtiontalouden tarkastusvirasto. 2017. Kybersuojauksen järjestäminen, Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Helsinki: Valtiontalouden tarkastusvirasto. PDF-dokumentti. Saatavissa: http://urn.fi/urn:isbn:978-952-499-392-0 [viitattu 17.9.2021].

Valtiovarainministeriö. 2020. Pilvipalvelujen soveltamisohje: Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille. Valtiovarainministeriön julkaisuja 2020:73. Helsinki: Valtiovarainministeriö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-367-503-2 [viitattu 4.4.2022].

Teemahaastattelun kysymykset

1. **Taustoitus I:** Perustiedot organisaatiosta

Nimi, toimiala, yhteyshenkilö, rooli/titteli
IT budjetin koko (noin)
Pilvibudjetin koko (noin)
Onko organisaatiollenne hyväksyttävää, että näistä haastatteluista kootun yhteenvedon tuloksia julkaistaan osana opinnäytetyötäni? (anonyymisti, yrityksiä mainitsematta sekä identifioimatta yrityskohtaisia menettelyjä ja teknologioita)

2. **Taustoitus II:** Organisaationne pilvipalvelujen käytön laajuus ja luonne tällä hetkellä?

IaaS, PaaS vai SaaS? (vai kaikki vaihtoehdot)
Onko näiden palveluluokkien käytön laajuus muuttumassa?
Operoitteko pilvessä tuotannon dataa vai vain esim. kehitysympäristöjä?
Miten liiketoimintakriittisiä käytetyt palvelut ovat? (esim. kuinka monta ysiä?)

3. **Menettelyt ja välineet:** Miten operatiivisesti ja teknisesti monitoroitte ja havainnoitte käytössä olevien pilviympäristöjen turvallisuutta? (välineet, tuotteet)

A) **Logging and monitoring – eli jäljitettävyys**
Käytättekö palvelutuottajien omia välineitä (kuten AWS CloudTrail)? Mitä välineitä?
Käytättekö kolmansien osapuolien tuotteita? Mitä tuotteita?
Onko käytössä kattava keskitetty lokienhallinta? (keruu/säilytys/analyysi)
B) **Configuration management**
Miten automatisoitua CM on tällä hetkellä?
Mitä työkaluja käytätte em. toiminnassa? (kuten Jenkins, Jfrog, Docker, Kubernetes tms.) Onko käytössä joku integraatioalusta pilvessä?
Kuinka standardisoitu pilviympäristönne on? Oletteko käyttäneet valmistajien best-practices -suosituksia ja mitkä ovat olleet kokemukset?
C) **Vulnerability management (Anti-malware, antivirus, WAF)**
Käytättekö palvelutuottajien omia välineitä (kuten Amazon Inspector)?

Käytättekö hyväksi palvelutuottajan omia TT-raportteja palveluistanne?
Käytättekö kolmansien osapuolien tuotteita? Mitä tuotteita?
Teettekö palvelujen jatkuvaa auditointia? Mitä työkaluja hyödynnätte?
Teettekö penetraatiotestausta sovelluksillenne? Säännöllisesti?
D) **Identity and access management**
Mitä välineitä käytätte käyttäjien pääsyn ja käyttäjähallinnan muutosten monitorointiin ja reagointiin?
Käytättekö jotain tunnettua Compliance-mallia tai automaattista auditointivälinettä pääsynhallinnan ja käyttäjähallinnan riskien selvittämiseen? (nimeä tärkeimmät?)
E) **SaaS-palvelut**
Hyvin yleistäen, mitä menettelyjä tai työkaluja käytätte palveluna ostettavien sovellusten monitorointiin ja valvontaan?

Lopuksi yleiset kysymykset tästä aiheesta:
Millainen ulkoistusaste ja työnjako teillä on ulkop. palveluntuottajien (SOC, integraattori) kanssa? • ovatko menettelyt ja välineet pitkälle heidän valitsemiaan?
Miten paljon käytettyjä välineitä on räätälöity vastaamaan tarpeitanne?
Mikä on automaation aste a) havainnoinnissa, b) reagoinnissa?

4. **Tilannekuvan laatu:** Miten hyvin em. menettelyt palvelevat turvallisuusuhkien havainnointia ja poikkeamienhallintaa?

Millä osa-alueilla havainnointi on tehokasta ja palvelee tarkoitustaan?
Onko pilvipalveluiden tietoturvassa jotain ominaisuuksia, jotka parantavat selvästi nykyisten prosessien, kyvykkyyksien tasoa tai tuomassa selvästi uusia kykyjä? (esim. Incident response kyvyt jne)
Millainen on eri välineiden keskinäisen integroinnin aste? • Täysin yhteentoimivia vs. tiedot hajallaan ja manuaalisesti yhteenkoottavia? • Miten sujuvasti havainnointi integroituu poikkeamanhallintajärjestelmiin ja -prosessiin?
Onko tunnistettuja havainnointigappeja? Mitä ja missä ne ovat?
Millä pilviturvallisuuden osa-alueilla on eniten tarvetta turvallisuusuhkien havainnoinnille? (käyttäjä-/configuraatio-/haavoittuvuuksienhallinta vai käyttäjien toiminta?)

Lopuksi keskusteltiin haastateltavan odotuksista ja toivomuksista KTK:lle.

Kokeilussa käytetyt tarkasteltavat kohteet

No	Control name	Control category
1	'AzureADPremiumP1LicenseNotAvailable'	General security capabilities
2	'AzureADPremiumP2LicenseNotAvailable'	General security capabilities
3	'WindowsDeviceEncryptionState'	Device management
4	'InsecureGuestUserSettingsInAzureAD'	IAM
5	'IntuneCompanyBranding'	Device management
6	'AzureADOrganizationalBranding'	IAM
7	'ConditionalAccessMissing'	IAM
8	'LackOfMulti-FactorAuthenticationForJoiningDevices'	IAM
9	'BreakTheGlassAccountMissing'	IAM
10	'BreakTheGlassAccountIsNotOnmicrosoft.com'	IAM
11	'NormalUsersHaveGlobalAdministratorRights'	IAM
12	'ExcessivePrivilegesForAdminsPimNotInUse'	IAM
13	'AzureIdentityProtectionFeatureIsDisabledByDefault'	IAM
14	'CombinedSecurityInfoRegistrationMissing'	IAM
15	'ExternalApplicationsConnectedToAzureADNotMonitored'	3rd party integrations
16	'AzureADDeviceJoinrightsForAllUsers'	IAM
17	'PublicIPAddressNotConfiguredAsBasicSKU'	Networking
18	'UsingDynamicIPAddressesForPublic-facingServices'	Networking
19	'AzureNSGInboundRuleIsConfiguredAsANY'	Networking
20	'AzureVirtualNetworkWithBasicDDoSProtection'	Networking
21	'StorageAccountsThatAllowInsecureTransfers'	Storage security
22	'StorageKeysAreNotRegeneratedRegularly'	Storage security
23	'StorageAccountSharedAccessSignature(SAS)TokensNotExpiringInATimelyManner'	Storage security
24	'StorageAccountIsAccessibleFromTheInternet'	Storage security
25	'StorageAccountBlobStorageWithAnonymousReadAccess'	Storage security
26	'StorageAccountMinimumTLSVersionNotTLS1.2'	Storage security
27	BlockLegacyAuthentication	IAM
28	OneAdmin	IAM
29	RoleOverlap	IAM
30	AdminMFAV2	IAM
31	MFARegistrationV2	IAM
32	TLSDeprecation	Networking
33	PWAgePolicyNew	IAM
34	SelfServicePasswordReset	IAM
	SecureScorePoints	Info
	UserCount	Info
	EnabledServices (security related)	Info
	ResourceGroups	Info
	PublicIPAddresses	Info
	NetworkSecurityGroups	Info
	StorageAccounts	Info