Heikki Järvinen

KYBERTURVALLISUUDEN NYKYISET JA TULEVAT OSAAMISTARPEET OHJELMISTOYRITYKSESSÄ - TAPAUSTUTKIMUS

PRO GRADU

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Järvinen, Heikki
Kyberturvallisuuden nykyiset ja tulevat osaamistarpeet ohjelmistoyrityksessä – tapaustutkimus
Jyväskylä: Jyväskylän yliopisto, 2020, 68 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Tutkimuksessa selvitettiin Yritys X:n kyberturvallisuuteen liittyviä avainkompetenssialueita. Tutkimus toisti aiemmin Jyväskylän yliopistossa samasta aiheesta tehdyn tutkimuksen tutkimusasetelman, mutta eri toimialalla. Tutkimuksen teoreettisena viitekehyksenä käytettiin amerikkalaista National Institute of Standards and Technologyn (NIST) kehittämää kyberturvallisuuden osaamista kuvaavaa ja luokittelevaa NCWF-viitekehystä.

Tutkimuksen kirjallisuuskatsauksessa selvitettiin kyberturvallisuuden osaamiseen liittyviä yleisiä viitekehyksiä. Katsaus keskittyi kohdeyrityksessä käytössä oleviin tai muutoin yleisesti tunnettuihin kyberturvallisuuden hallintajärjestelmiin ja standardeihin sekä kompetenssien kehittämisen työkaluihin ja viitekehyksiin. Tutkimus toteutettiin laadullisena tapaustutkimuksena ja aineistonkeruumenetelmänä käytettiin teemahaastatteluita. Haastatteluiden lisäksi tutustuttiin myös kohdeyrityksen laatujärjestelmään, turvallisuuspolitiikkaan ja turvallisuuteen liittyviin ohjeisiin.

Tutkimuksen teemahaastattelut toteutettiin kahtena erillisenä etähaastatteluna. Ensimmäisessä haastattelussa haastateltiin kohdeyrityksen turvallisuusyksikön johtajaa ja toisessa ICT-yksikön johtajaa. Molemmat haastattelut tallennettiin ja tallenteet litteroitiin. Litteroidut aineistot luokiteltiin ja analysoitiin käyttäen teorialähtöisen sisältöanalyysin periaatteita ja NCWF-viitekehystä.

Tutkimustuloksista muodostettiin kohdeyrityksen kyberturvallisuuden ydinkompetenssiesitys. Saatuja tutkimustuloksia vertailtiin myös aiemman tutkimuksen tuloksiin. Tutkimusten vertailun avulla pyrittiin laajentamaan kyberturvallisuuden osaamiseen liittyvää yleistä ymmärrystä ja tietoa.

Asiasanat: Kyberturvallisuus, ydinosaaminen, kompetenssi, ydinkompetenssi, NCWF, kyberosaaminen, kyberkompetenssi

ABSTRACT

Järvinen, Heikki
Current and future needs in cyber security competences in a software company – case study
Jyväskylä: University of Jyväskylä, 2020, 68 pp.
Information Systems, Master's Thesis
Supervisor(s): Lehto, Martti

This study examined the cyber security core competence areas at the Company X. In addition to case study approach this study replicated also a previous study research setting. That previous study examined also cyber security core competences, but in a different business sector. Both studies were conducted in the University of Jyväskylä and they both utilized the same competence framework, which was the NCWF framework, by the National Institute of Standards and Technology (NIST). The framework was used as a theoretical framework to examine and categorize the cyber competences in the research setting.

The literature view of this study examined overall cyber security competence frameworks along with other general cyber security standards and tools used to operate, develop and maintain cyber security competences, systems and operations in organizations. The research was conducted as qualitative study with case study approach. The research data was gathered with theme interviews. Along with the interviews also quality system, security policies and security guidance of the research target were examined.

Research interviews were conducted as two separate interviews. First interview was done with the Chief Security Officer of the Company X and the second with the Chief Information Officer. Both interviews were conducted remotely and recorded. Recordings were transcribed and analyzed with theory-based content analysis and NCWF framework.

Based on the findings the study presented a cyber security core competence model for the research target company. Study findings were also compared to previous study findings. With that comparison, this study aimed to enhance the general understanding and the body of knowledge in the field of cyber security competences.

Keywords: cyber security, core competence, competence, NCWF, cyber competences

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viimeiset vuosikymmenet tietotekniikan ja internetin kehityksessä ovat mullistaneet käsityksemme kommunikaatiosta sekä tietotekniikasta ja sen mahdollisuuksista. Neljä vuosikymmentä sitten tietokoneet olivat lähinnä yksittäisiä laitteita, joiden toimintakyky ja turvallisuusnäkökulmat olivat täysin erilaiset, kuin nykyisessä verkottuneessa maailmassamme. Tietojärjestelmien ja tietoon ja sen eheyteen, saatavuuteen ja turvallisuuteen liittyvät uhkat nähtiin tietojärjestelmien fyysiseen turvallisuuteen liittyvinä (Lane & Wright, 1978, s. 685). Ohjelmistojen ja käyttöjärjestelmien turvallisuus perustui yksittäisten tietokoneiden aikakaudella pitkälti salasanojen käsittelyyn. Muun tyyppisistä haavoittuvuuksista ei juurikaan ollut huolta, koska niitä ei vielä ollut. Vuosikymmeniä myöhemmin tapahtuneen internetin nousun myötä tilanne muuttui.

Vielä 2000-luvullakin voi käytössä olla tietojärjestelmiä, joiden kehitys on kenties alkanut vuosikymmen tai kaksi sitten. Kuinka tuolloin käyttöön otetut ratkaisut ja omaksutut ohjelmistotuotannon menetelmät, teknologiat tai käytännöt ovat sulautuneet nykypäivän kasvaneisiin vaatimuksiin, erityisesti kyberturvallisuuden osalta? Miten kyberturvallisuuden teknologisesta kehityksestä, osaamisen kehittämisestä ja tietoisuuden lisäämisestä on pidetty huolta ohjelmistoyrityksissä? Nähdäänkö ohjelmistotuotanto ja kyberturvallisuus erillisinä saarekkeina ja kuinka tietojärjestelmien sisäänrakennettu ja oletusarvoinen tietosuoja ja tietoturva toteutuu käytännössä?

Kuinka tietojärjestelmien suunnittelun ja ohjelmistojen tuotannon kyberturvallisuuden osaamista voidaan ymmärtää, suunnitella ja edelleen kehittää, kun huomioidaan erityisesti kyberturvallisuuden laaja-alainen osaamiskenttä? Tämän laajan osaamiskentän nähdään yleisesti koostuvan kulloisenkin liiketoiminta-alueen erityisosaamisesta sekä siihen liittyvistä tietojärjestelmien kehittämisen osaamisesta. Osaamisalueella tunnistetaan kyberturvallisuuteen liittyen lisäksi tarpeita myös verkkotekniikan, ohjelmoinnin, lainsäädännön ja regulaation sekä auditointimenetelmien osaamisalueilta. Myös ihmisen käyttäytymisen ja etiikan ymmärtäminen nähdään tärkeinä kyberturvallisuuden osaamisalueina (Shoemaker, D., Kohnke, A., Sigler, 2016).

Yllä olevasta on siis nähtävissä, että kyberturvallisuuden osaamisalue on haastava ja erittäin laaja ja sen hallinta edellyttää siihen liittyvien keskeisten

avainkompetenssien ja niiden kehityksen sekä suunnittelun hyvää hallintaa. Aiheeseen liittyvällä tutkimuksella voidaankin nähdä olevan tässä työssä keskeinen rooli aihealueen ymmärryksen lisääjänä ja kompetenssien hallinnan ja kehittämisen työkalujen mahdollistajana ja kehittämisen apuvälineenä.

Tämä tutkimus selvitti kyberturvallisuuden tämän päivän avainkompetensseja tutkimuksen kohdeyrityksessä. Lisäksi selvitettiin tutkimuksen myötä mahdollisesti esiin nousevia kompetenssien kehittämiseen liittyviä tulevaisuuden tarpeita, kohdeyrityksen liiketoiminnan osa-alueisiin liittyen. Tutkimus toisti aiemmin Jyväskylän yliopistossa samasta aihealueesta tehdyn tutkimuksen tutkimusasetelman (Willberg, 2017), mutta eri toimialalla. Tutkimus pyrki täten tapaustutkimuksen tulosten ohella lisäämään yleistä ymmärrystä kyberturvallisuuden avainkompetensseihin liittyen, laajentamalla aiemmin tutkittua toimintaympäristöä. Tutkimus toteutettiin Yritys X:n toimeksiantona.

Tutkimuksen toteutus tukeutui yllä mainitun tutkimuksen tutkimusasetelmaan ja tutkimuksessa käytettyyn teoreettiseen viitekehykseen. Viitekehyksenä molemmissa tutkimuksissa käytettiin Amerikkalaisen National Institute of Standards and Technologyn (myöhemmin NIST) tuottamaa kyberosaamisen viitekehystä (National Cyber Security Workforce Framework, myöhemmin NCWF). Aieman tutkimuksen tutkimusasetelman testaamisen ja tiedon laajentamisen lisäksi viitekehyksen arvioitiin myös soveltuvan hyvin nyt tehdyn tutkimuksen tutkimuskysymysten selvittämiseen. Tämä arvio perustui näkemykseen viitekehyksen kokonaisvaltaisesta ja kattavasta luonteesta kyberturvallisuuden kompetenssien kuvaajana. Tässä raportoitu tutkimus kartoitti ohjelmistoyrityksen toimintaan liittyvää keskeistä kyberosaamista ja sen tulevia tarpeita tämän viitekehyksen avulla.

Viitekehys kehitettiin alun perin kansallisena hankkeena Yhdysvalloissa NIST:n toimesta. Hankkeen tavoitteena oli luoda kyberturvallisuuden osaamista kuvaava ja määrittävä viitekehys ja yhteinen sanasto kyberturvallisuuden toimialueelle. Viitekehyksen tarkoituksena oli helpottaa työvoiman liikkuvuutta ja kyberturvallisuuden toimialan tehtävien määrittelyä yleisesti ja yhteisesti ymmärrettävän termistön avulla. Viitekehyksen yksi tavoite oli olla myös kansainvälisesti toimiva ja kyberturvallisuuden toimijoita palveleva malli (Shoemaker, D., Kohnke, A., Sigler, 2016).

Kuten todettua, tutkimuksen kohteena olevan yrityksen kyberosaamisen kartoittamisen lisäksi tutkimus pyrki luomaan uutta tietoa ja syntetisoimaan olemassa olevaa tietoa uuden tiedon kanssa. Tähän liittyen tutkimusraportin kirjallisuuskatsauksessa kartoitettiin käytetyn NCWF-viitekehyksen lisäksi myös muita kyberturvallisuuden osaamisen viitekehyksiä, standardeja ja työkaluja. Tämän kyberturvallisuuden hallintajärjestelmien ja standardien katsauksen arvioitiin lisäävän lukijan ymmärrystä nykypäivän kyberturvallisuuden työvoiman osaamisvaatimuksiin ja työtehtäviin liittyen. Näin arvioitiin siksi, että kyberturvallisuustyössä käytettyjen työkalujen ja standardien arvioitiin määrittävän kyberturvallisuuden työvoiman tehtäväkenttää ja sen vaatimuksia merkittävissä määrin. Katsauksen avulla lukijalle pyrittiin luomaan myös laaja käsitys organisaatioilla tänä päivänä käytettävissä olevista kyberturvallisuuden hallinta- ja kehitysmalleista, työvoiman osaamista kuvaavien ja luokittelevien mallien ohella. Tämän lisäksi kuvauksen arvioitiin yhdessä tutkimuksen tulosten kanssa

viitoittavan näin myös tietä uusien työkalujen käytölle, organisaatioiden kyberturvallisuuden osaamisen tuloksekkaassa kehittämisessä yleisemminkin.

1.1 Tutkimuksen tarkoitus

Tutkimuksen tarkoitus oli selvittää kohdeyrityksen kyberturvallisuuden avainkompetenssit, ja tuoda esiin tutkimuksen myötä niihin mahdollisesti liittyviä kehitystarpeita. Tutkimus toisti Nils Willbergin Jyväskylän yliopistossa aiemmin tekemän tutkimuksen tutkimusasetelman (Willberg, 2017). Tutkimus käytti aiemman tutkimuksen kanssa samaa NCWF viitekehystä. Sama tutkimusasetelma ja viitekehys mahdollistivat myös tapaustutkimusten tulosten vertailun.

1.2 Tutkimuskysymys

Tutkimuksen ongelmanasettelu oli kaksijakoinen. Tutkimuksen varsinainen tutkimuskysymys oli: Mitkä ovat kohdeyrityksen kyberosaamisen keskeiset kompetenssit (ydinkompetenssit). Tämän lisäksi tutkimuksessa koottiin myös tietoa kyberturvallisuuden kompetensseihin mahdollisesti liittyvistä tulevaisuuden tarpeista. Koska tutkimus toisti aiemmin tutkitun tutkimuksen tutkimusasetelman ja käytti samaa teoreettista viitekehystä, selvitettiin tutkimuksessa myös sitä, mitä eroja ja yhtäläisyyksiä tämän ja aiemmin tehdyn kompetenssitutkimuksen tulosten välillä mahdollisesti oli.

1.3 Tutkimuksen rakenne

Tutkimus alkoi aihealueen kirjallisuuskatsauksella ja keskeisten käsitteiden määrittelyllä. Tämän jälkeen tutkimus eteni Suomen kyberturvallisuuden nykytilan tarkastelun ja kuvauksen kautta tutkimuksessa käytetyn viitekehyksen esittelyyn. Tämän lisäksi aihealuetta taustoitettiin luomalla katsaus muihin saman tyyppisiin standardeihin, ohjeistoihin ja viitekehyksiin. Taustoituksessa keskityttiin NCWF -viitekehystä vastaaviin, sitä täydentäviin tai kohdeyrityksessä jo käytössä oleviin tai siellä jo sovellettaviin viitekehyksiin tai standardeihin. Näin muodostettiin kokonaisnäkemys tällä hetkellä kohdeyrityksessä ja muualla vastaavissa ympäristöissä mahdollisesti käytössä olevista työkaluista ja menetelmistä kyberosaamiseen ja yrityksen tietoturvaan liittyen.

Tutkimus toteutettiin laadullisena tapaustutkimuksena. Aineistonkeruumenetelmänä käytettiin puolistrukturoituja teemahaastatteluita, jotka toteutettiin toimeksiantajayrityksen kyberturvallisuudesta vastaavan (myöhemmin CSO Office) ja tietojärjestelmäympäristöstä (myöhemmin CIO Office) vastaavan yksikön kanssa.

2 KIRJALLISUUS

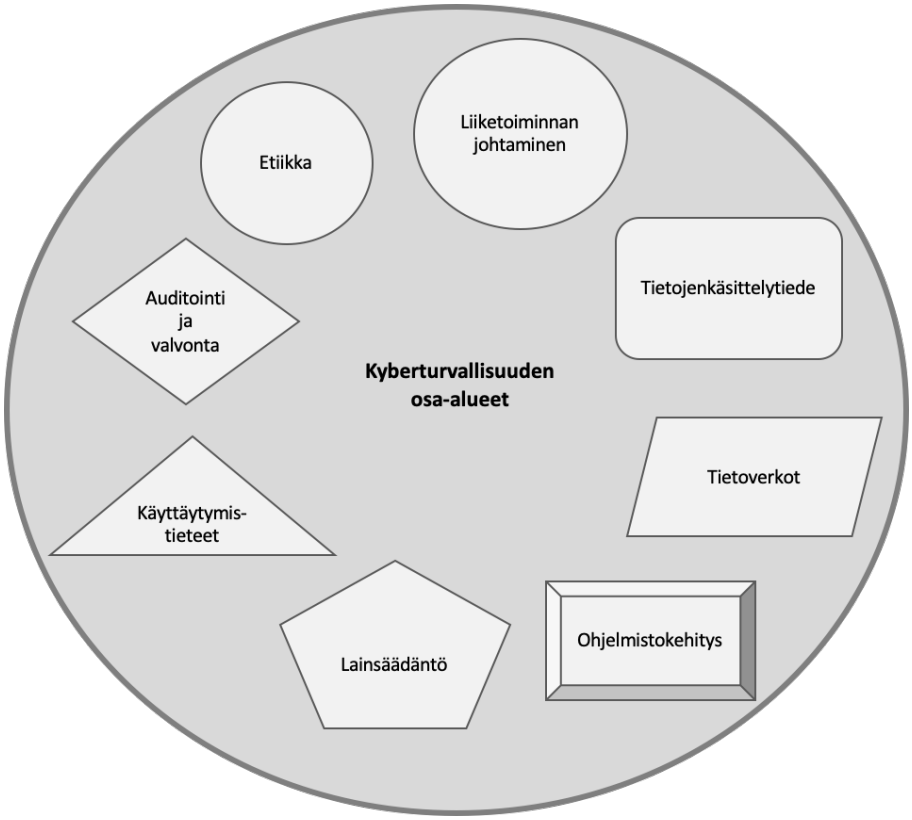
Tässä kappaleessa kuvataan tutkimuksen taustatekijöitä ja keskeisimpiä teoriasisältöjä siihen liittyen. Taustan kuvaus alkaa kyberturvallisuuden, kompetenssin ja ydinkompetenssin käsitemäärittelyllä. Tämän jälkeen tutustutaan yrityksiin kohdistuviin kyberturvallisuuden uhkiin ja kyberturvallisuuden nykytilaan Suomessa. Kyberturvallisuuden yleisen tilannekuvan jälkeen kartoitetaan yleistä kyberturvallisuuden teoreettista viitekehystä, tutustumalla tutkimuksessa käytettyyn NCWF-viitekehykseen ja muihin yleisiin kyberturvallisuuden osaamiseen liittyviin viitekehyksiin ja standardeihin.

Lopuksi luodaan katsaus kyberturvallisuuden monimuotoisuuden haasteisiin ja sen osalta erityisesti ohjelmistotuotantoon liittyviin kyberturvallisuuden piirteisiin. Katsauksen avulla pyritään muodostamaan kokonaisvaltainen ymmärrys kyberturvallisuuteen liittyvän toimialueen kompetensseihin liittyvistä tarpeista ja toimialueen nykytilasta. Yleisesti käytössä olevien viitekehysten ja hallintamallien kartoituksella pyritään syventämään käytössä olevien työkalujen ymmärrystä ja niiden suhdetta kyberturvallisuuden kompetenssivaatimuksiin.

2.1 Kyberturvallisuuden määritelmä

Kyberturvallisuus on käsitteenä vielä kohtalaisen uusi ja myös laaja käsite. Käsitteen määrittävän osuuden, sanan ”kyber” katsotaan tulevan kreikan kielen sanasta ”kybereo”, joka tarkoittaa (”ohjata”, ”opastaa”, ”hallita”). Sanan merkitys liittyy yleensä digitaalisessa muodossa olevan tiedon käsittelyyn ja hallintaan. (Sanastokeskus TSK, 2018). Käsitteellä tarkoitetaan yleensä myös fyysisen ja digitaalisen maailman yhteenliittymää. Kyberfyysistä maailmaa ja siihen liittyvää turvallisuutta. Suomen Turvallisuuskomitea linjasi termin määrityksen Kyberturvallisuusstrategiassa vuonna 2013 näin: ”*Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoiminta- ympäristöön voidaan luottaa ja jossa sen toiminta turvataan.*” (Turvallisuuskomitea, 2013). Yhdysvaltain kansallinen standardien ja teknologian instituutti (NIST) linjaa termin sanakirjassaan tarkoittamaan kykyä puolustaa kyberulottuvuudessa olevia resursseja kyberhyökkäyksiltä (NIST, 2020).

Yhdysvaltalaista NCWF-viitekehystä käsittelevässä kirjassa kyberturvallisuuden monipuolisia osa-alueita kuvataan seuraavan kuvion (Kuvio 1) mukaisesti.



Kuvio 1 Kyberturvallisuuden osa-alueet (Shoemaker ym., 2016, s. 7 mukaan)

Shoemaker ym. (2016) mukaan kyberturvallisuus koostuu yllä mainituista kahdeksasta osa-alueesta. Seuraavassa on avattu näiden osa-alueiden kuvauksia Shoemakerin ym. mukaan.

> *"Liiketoiminnan johtaminen on merkittävä osaamisalue kyberturvallisuudessa, sillä se vaikuttaa organisaation turvallisuuspolitiikan luomiseen, jatkuvuuden suunnitteluun, henkilöstöhallintoon sekä sopimuksiin ja vaatimusten mukaisuuteen liiketoiminnan toteuttamisessa".*

> *"Tietojenkäsittelytieteen osaamisalue on merkittävä kokonaisuus. Sen menetelmien ja siihen liittyvän osaamisen avulla organisaation sähköisessä muodossa oleva talletettu tieto ja sen käsittely voidaan turvata".*

> *"Edellä mainitun tietojenkäsittelyn lisäksi toinen keskeinen osaamisalue kyberturvallisuudessa on tietoverkkoihin liittyvä osaaminen. Sen osa-alueen avulla voidaan organisaation tietojen siirto toteuttaa turvallisesti".*

> *"Ohjelmistokehityksen osaamisalueen avulla varmistetaan turvallinen ohjelmistojen tuotanto, tietoturvatestaus sekä turvallinen ohjelmistojen provisiointi ja elinkaaren hallinta."*

"Lainsäädännöllinen osaaminen on keskeistä kyberturvallisuudessa erityisesti yksityisyyden suojan ja immateriaalioikeudellisten kysymysten osalta. Myös kyberrikosten tutkintaan ja syyteprosesseihin liittyvä osaaminen on tärkeää osaamista tässä viitekehyksessä."

"Käyttäytymistieteiden osaamisalueen merkitys korostuu erityisesti henkilöstön koulutukseen liittyen."

"Jopa etiikan voidaan katsoa liittyvän organisaation informaatio-omaisuuden käyttöön ja suojaamiseen liittyvissä aiheissa."

(Shoemaker, D., Kohnke, A., Sigler, 2016, ss. 5–7)

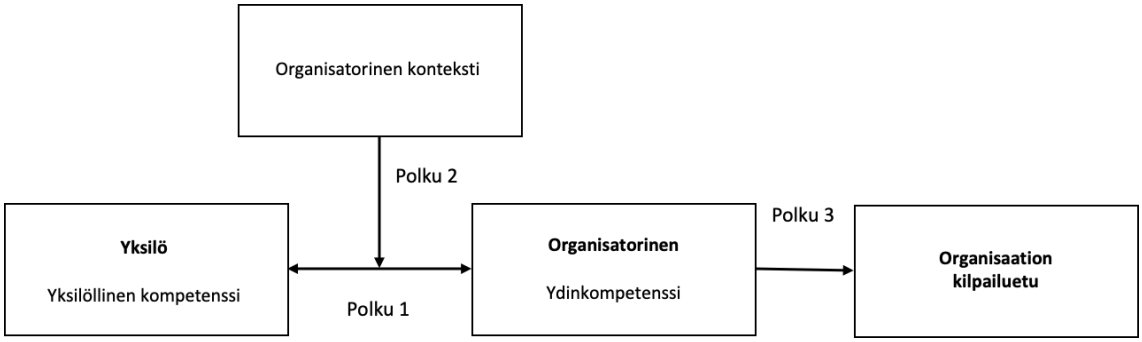
2.2 Kompetenssin määritelmä

Kompetensseilla tarkoitetaan yleisesti ja tarkoitettiin myös tämän tutkimuksen yhteydessä yrityksen henkilöstön osaamista ja taitoja, joita tarvitaan yrityksen kilpailukyvyn aikaansaamiseksi ja kehittämiseksi. Kompetenssien johtamisen tulisi näkyä yrityksen toiminnan tehostumisena ja parempina toimintatapoina, tuotteina, palveluina, innovaatioina sekä lopulta parempana tuloksena (Viitala Riitta, 2014).

2.2.1 Ydinkompetenssi

Chen ja Chang (2011) kuvaavat tutkimuksessaan kompetenssin muodostumista organisaation kontekstissa, jossa eri kompetenssit ovat vuorovaikutuksessa keskenään. Ydinkompetenssi muodostuu symbioottisessa vuorovaikutussuhteessa organisatorisen kompetenssin ja yksilön kompetenssin yhdistelmänä. Kompetenssien vuorovaikutus ja suhteet on havainnollistettu alla olevassa kuviossa (Kuvio 2).

Chenin ja Changin (2011) tutkimus nosti esiin myös organisaation mission, vision ja tavoitteiden vaikutuksen yksilön kompetenssin muodostumiseen (Polku 2). Kompetenssien vuorovaikutus on siis molemman suuntaista (Polku 1). Yksilön kompetenssi vaikuttaa organisaation ydinkompetenssin muodostumiseen (Polku 1) ja yrityksen tarpeet ohjaavat puolestaan yksilön kompetenssin muodostumista (Polku 1). Yhdessä kompetenssit muodostavat organisaation kilpailuedun (Polku 3) (Chen & Chang, 2011).



Kuvio 2 Konseptuaalinen viitekehys kompetenssien vuorovaikutuksesta ja kilpailukyvyn muodostumisesta (Chen & Chang, 2011, s. 5742 mukaan)

Myös Prahalad ja Hamel (1990) kuvaavat ydinkompetenssin muodostumista organisaatiossa prosessina, jossa organisaatio tarkastelee tekemistään objektiivisesti ja pyrkii löytämään organisaation toimintoihin liittyvät ydinosaamisalueet. Tutkijat totesivat raportissaan myös, että ydinkompetenssin löytäminen voi mahdollistaa liiketoimintamallin kehittämisen niiden ympärille. Tämä saattaa avata myös uusia liiketoiminnan malleja ja suuntia sekä kehittää kilpailukykyä paremmaksi (Prahalad & Hamel, 1990).

2.2.2 Kompetenssi kyberturvallisuudessa

Kuten kyberturvallisuus itsessään, on myös kyberturvallisuuteen liittyvien kompetenssien käsite laaja-alainen ja monitahoinen kokoelma erilaisia tietoja ja taitoja. Tästä syystä se näyttäytyy yleensä hankalasti hahmotettavana ja määritettävänä asiana.

Myös alan koulutustarjonta sekä sertifioinnit ovat monisäikeisiä ja laajoja opintokokonaisuuksia. Tästä laajuudesta johtuen esimerkiksi työnantajien osalta kompetensseihin liittyvä eksakti vaatimusmäärittely on haastavaa. Yhteismitallisen määrittelyn tarve onkin ajanut kyberalan toimijat kehittämään erilaisia viitekehyksiä, jotka pyrkivät määrittämään kyberturvallisuuden kompetenssikenttää sen tehtäviä ja vaatimuksia (Furnell ym., 2017). Yksi esimerkki tällaisesta viitekehyksestä on tässä tutkimuksessa käytetty NCWF-viitekehys. Tässä tutkimuksessa on esitelty myös muita kompetenssien hallintaan ja kehittämiseen liittyviä viitekehyksiä. Tutkimusraportti esittelee myös turvallisuuteen ja turvallisuuden hallintaan liittyviä standardeja ja koulutuskehyksiä.

Kyberturvallisuuteen liittyvä kompetenssi nähdään usein teknisluonteisena, mutta kuten jo todettua, liittyy siihen myös useita muita kompetenssialueita (Shoemaker, D., Kohnke, A., Sigler, 2016). Kyberturvallisuuden yhtenä merkittävänä osa-alueena ja kehityskohteena nähdään myös kyberturvallisuuden johtamiseen liittyvien kompetenssien kehittäminen (Kern & Peifer, 2013).

Kern ja Peifer toteavat kyberturvallisuuden johtamisessa keskeisiksi ominaisuuksiksi kyberturvallisuuden investointien suunnittelu- ja investointipäätösten perusteluiden tehokkaan kommunikoinnin organisaation johdon kanssa. Myös teknologinen kompetenssi nähdään keskeisenä ominaisuutena, kuten

myös henkilöjohtamisen ja liikkeenjohdon kompetenssit. Riskienhallinnan ja organisaation liiketoiminta-arkkitehtuurin kehittämiseen liittyvää tietotaitoa pidetään myös keskeisenä osaamisalueena kyberturvallisuuden johtamisessa (Kern & Peifer, 2013, ss. 3–4).

2.3 Kyberuhkat yrityksissä

On yleisesti tunnettua, että kyberturvallisuus on yhtä vahva, kuin sen heikoin lenkki. Kybertoimintaympäristössä tämä lenkki on usein ihminen. (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2008, s. 19). Tämä johtuu yleensä siitä, että tietokone tekee vain sen, mitä ihminen siltä pyytää. Ohjelmistot eivät kirjoita itse virheitään, eivätkä tietoturva-aukkojaan, vaan siihen johtaa ihmisen toteuttama heikko suunnittelu ja toteutus.

Organisaation henkilöstö muodostaa myös osaltaan uhkan tietojen luottamuksellisuudelle, eheydelle ja saatavuudelle erilaisten tahattomien ja tahallisten virheiden ja tietoturvaloukkausten kautta. (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2008, s. 19). Samaan aikaan alati teknistyvä ja tietoverkottuva yhteiskunta, työyhteisö ja yksilön elämä asettavat kyberturvallisuusosaamisen keskeiseen rooliin kaikilla elämän osa-alueilla.

Koska erityisesti ohjelmisto- ja muissa immateriaalihyödykkeitä tuottavissa yrityksissä ja organisaatioissa tärkein voimavara ja tuotannontekijä on ihminen, on edellä mainittuun viitaten selvää, että kyberturvallisuuteen liittyvä osaaminen nousee niissä merkittävään rooliin. Yrityksen tai organisaation onkin siksi syytä panostaa kyberturvallisuuden osaamisen kehittämiseen, varmistaakseen toiminnan jatkuvuuden ja liiketoiminnan turvallisuuden.

Paitsi merkittävä riskitekijä, yrityksen henkilöstö on asiantuntijayrityksissä yleensä myös sen tärkein tuotannontekijä ja avainresurssi. Tästä syystä asiantuntijayritysten menestyksen keskiössä on tehokas ja suunnitelmallinen johto ja henkilöstöhallinto. Näiden toimintojen tärkeänä tehtävänä on tunnistaa, ylläpitää ja kehittää yrityksen määrittämiä avainkompetensseja, joihin myös kyberturvallisuusosaaminen nykypäivänä kuuluu. (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2008)

2.4 Kyberturvallisuuden nykytila Suomessa

Kyberturvallisuuden monitahoisuus asettaa haasteen siihen liittyvälle osaamiselle. Turvallisuus on yhtäältä ihmisen ja koneen yhteistyötä ja toisaalta lainsäädäntöä ja teknisiä kompetensseja vaativaa syvällistä tietoteknistä osaamista. Kansallisen kyberturvallisuuden nykytilaa Suomessa on selvitetty mm. 2017 julkaistussa tutkimuksessa (Lehto ym., 2017). Tutkimus keskittyi Suomen 2013 julkaistun kyberturvallisuusstrategian (Turvallisuuskomitea, 2013) keskeisiin teemoihin ja tavoitteisiin sekä tavoitteiden toteutumisen selvittämiseen. Tutkimus tarkasteli kokonaisuutta enimmäkseen valtiollisesta perspektiivistä, mutta myös

osin yksityisen sektorin näkökulmasta. Yksityisen sektorin toimijat olivat kriittisen infrastruktuurin toimijoita.

Tutkimuksen tulokset osoittivat, että yritysten toiminta kyberuhkilta suojautumisen suhteen oli reaktiivista, mutta edistysaskeleita kohti proaktiivisempaa toimintamallia oltiin ottamassa. Perushaittaohjelmilta suojautuminen oli hyvällä tasolla, mutta edistyneempien haittaohjelmien osalta tilanne oli heikompi.

Kyberturvallisuuden nykytilan lisäksi, myös kyberturvallisuuden kansallista osaamista ja koulutusta on selvitetty vuonna 2019 julkaistussa ”Kyberalan tutkimus ja koulutus Suomessa 2019”-raportissa (Lehto & Niemelä, 2019). Raportti totesi kyberturvallisuuden koulutuksen laajentuneen aiemmin tutkitusta tilanteesta (Lehto & Kähkönen, 2015). Kyberturvallisuuteen liittyvässä koulutustarjonnassa on tutkimuksen mukaan tunnistettavissa nykyään kaksi eri suuntaa: 1) kyberturvallisuuteen keskittyvät koulutusohjelmat ja 2) kyberturvallisuuden integrointi osaksi muita koulutusohjelmia. Molempien mallien todetaan olevan tärkeitä alan osaamisen kehittymiselle.

Tutkimusten tuloksista on kokonaisuudessaan nähtävissä, että kyberturvallisuus on laaja ja monimutkainen kokonaisuus. Lisäksi se on myös vielä hyvin nuori ja kehittyvä toimialue. Tulosten perusteella arvioida myös, että kyberturvallisuuden operatiivinen toteutus yrityksissä, kuten myös koulutus ovat vielä kohtalaisen alkuvaiheessaan olevia kokonaisuuksia. Edistystä tässä tapahtuu kuitenkin koko ajan ja tätä tutkimusta tehdessä tilanne on jo edellä mainituista tutkimustuloksista edelleen kehittynyttä.

Yhtä kaikki, osaaminen, kompetenssien kehitys ja tietoisuuden lisääminen ovat edelleen kantavia teemoja kyberturvallisuuden parantamisessa ja turvallisuuden lisäämisessä. Tämä pätee niin yritysympäristöihin, kuin myös yhteiskunnallisellakin tasolla. Tätä taustaa vasten on hedelmällistä tutkia myös NCWF -viitekehyksen toimivuutta yritysten kontekstissa tehtävässä tutkimuksessa. Tämä siksi, että erityisesti yritysten osalta on luonnollista ja kustannustehokasta ottaa käyttöön kaikki apuvälineet tämän monimutkaisen kokonaisuuden hallinnan tehostamiseksi. NCWF -viitekehys tarjoaa omalta osaltaan tehokkaan työkalun tähän toimintaan.

2.5 NCWF -viitekehys

Tässä kappaleessa kerrotaan tutkimuksen teoreettisena viitekehyksenä käytettävästä NCWF -viitekehyksestä ja sen kehityksestä sekä sisällöstä. Viitekehys kehitettiin alun perin osana Yhdysvaltain kansallisen standardien ja teknologian instituutin kansallista kyberturvallisuuden koulutusohjelmaa: National Initiative for Cyber Education-hanketta (myöhemmin NICE). NICE -hanke oli yhteistyöhanke valtion, akateemisen maailman ja yksityisen sektorin välillä. Hankkeen tavoitteena oli kehittää viitekehys, jonka avulla kansallista kyberturvallisuuden osaamista pystyttäisiin määrittämään, standardoimaan ja parantamaan. Hanketta johti yhdysvaltalainen National Institute of Standards and Technology (NIST).

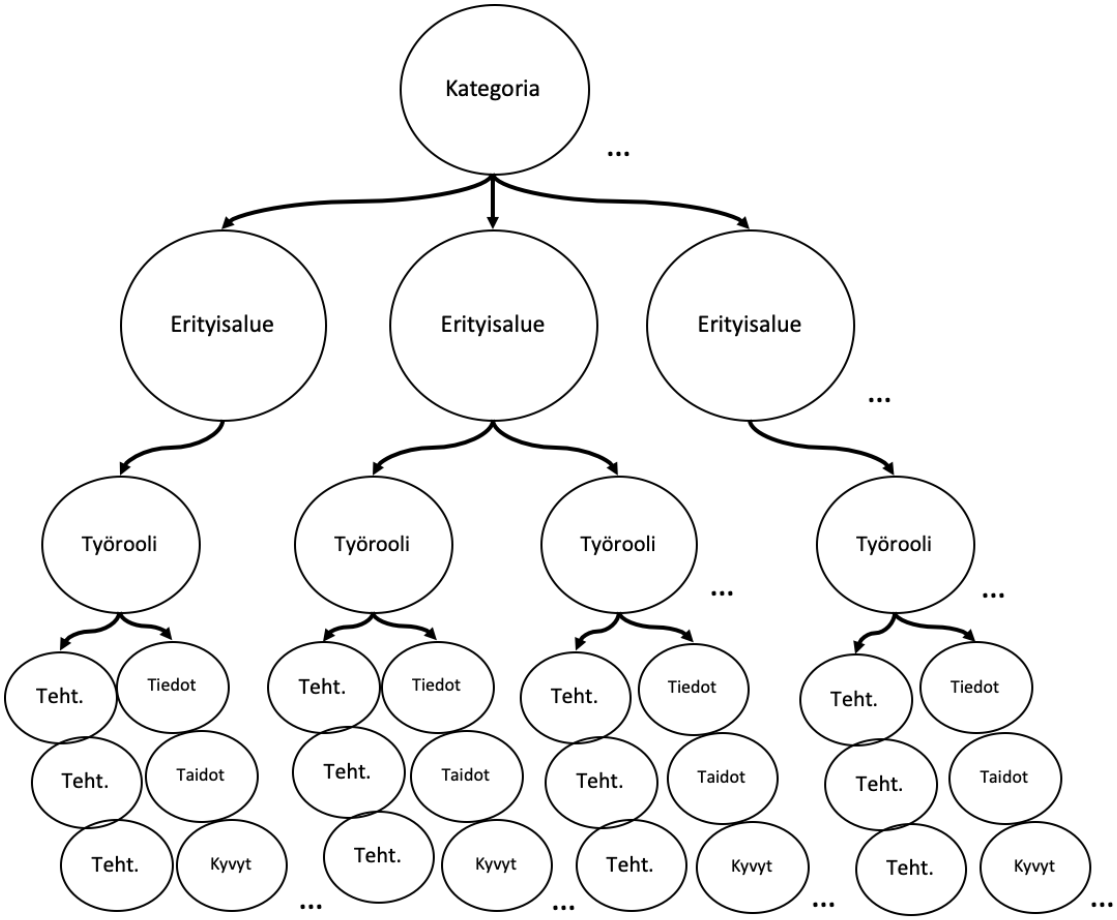
Hankkeessa pyrittiin kehittämään maanlaajuista yhteistyöverkostoa ja luomaan uutta ekosysteemiä kyberturvallisuuden toimijoiden osaamiseen ja koulutukseen liittyen. Hankkeen tähtäimenä oli kyberkyvykkään työvoiman kehittämisen tehostaminen. Hankkeessa tunnistettiin kyberturvallisuuden monimutkaisuus ja jatkuvasti muuttuva luonne. Hankkeen koulutussuunnittelu ja mallien luonti pyrki vastaamaan tämän kompleksisen ongelman tuomiin haasteisiin luomalla yhtenäisen osaamismallin, jossa kyberturvallisuuden kaikki ulottuvuudet huomioitaisiin (Newhouse ym., 2017).

NICE hankkeen lopputuloksena syntyi NCWF-viitekehys, jonka avulla pyritään hallitsemaan erilaisten organisaatioiden kyberturvallisuuden tarpeita, määrittämään kyberturvallisuuden toimialueelle yhtenäistä sanastoa, työtehtävien kategorioita, erikoistumisalueita sekä työrooleja. Mallin tarkoitus oli paitsi määrittää edellä mainitut osa-alueet, myös helpottaa työvoiman liikkuvuutta, työvoiman koulutuksen suunnittelua kansallisella tasolla. Tarkoitus oli siis luoda yhteismitallista kyberturvallisuuden käsitteistöä kansallisen yhtenäisen kyberturvallisuuden ymmärryksen lisäämiseksi. NCWF-mallin kohdeyleisönä nähtiin olevan työnantajat, työntekijät, kouluttajat ja koulutusorganisaatiot sekä erilaiset teknologioiden ja ratkaisujen tarjoajat (Newhouse ym., 2017).

2.6 NCWF-viitekehyksen rakenne

NCWF -viitekehys muodostuu neljästä eri kokonaisuudesta: kategorioista, erityisalueista, rooleista ja tehtävistä. Tässä kappaleessa kuvataan nämä kokonaisuudet sekä niiden sisällöt yleisellä tasolla. Näiden kokonaisuuksien ja mallin yleisen rakenteen avulla kyberturvallisuuden osaamista pyritään jäsentämään ja suunnittelemaan sen toiminnan toteutukseen tai koulutukseen liittyen.

Mallin yleistä rakennetta ja eri komponenttien välisiä suhteita on havainnollistettu alla olevassa kuviossa (Kuvio 3). Tämän jälkeen seuraa yksityiskohtaisempi kuvaus mallin rakenteen osa-alueista. Nyt tehty tutkimus keskittyy käsittelemään mallin kahta ylintä osa-aluetta: kategorioita ja erityisalueita. Tutkimus pyrkii selvittämään kohdeyrityksen kyberturvallisuuden avainkompetensseja näillä tasoilla.



Kuvio 3 Viitekehyksen komponenttien relaatiot (Newhouse ym., 2017, s. 6 mukaan)

2.6.1 Kategoriat (Categories)

Kategoriat luovat perustan NCWF-viitekehykselle ja ne toimivat ylätasona kyberturvallisuuden osaamisen määrittelylle. Kategorioita on yhteensä seitsemän kappaletta. Jokainen kategoria sisältää siihen liittyvät erityisalueet. Erityisalueet ovat kategoriaan kuuluvia tarkempia toimialueen toimintojen kuvauksia. Kategorioita ja niihin liittyviä erityisalueita on kuvattu alla olevassa kuviossa (Kuvio 4).

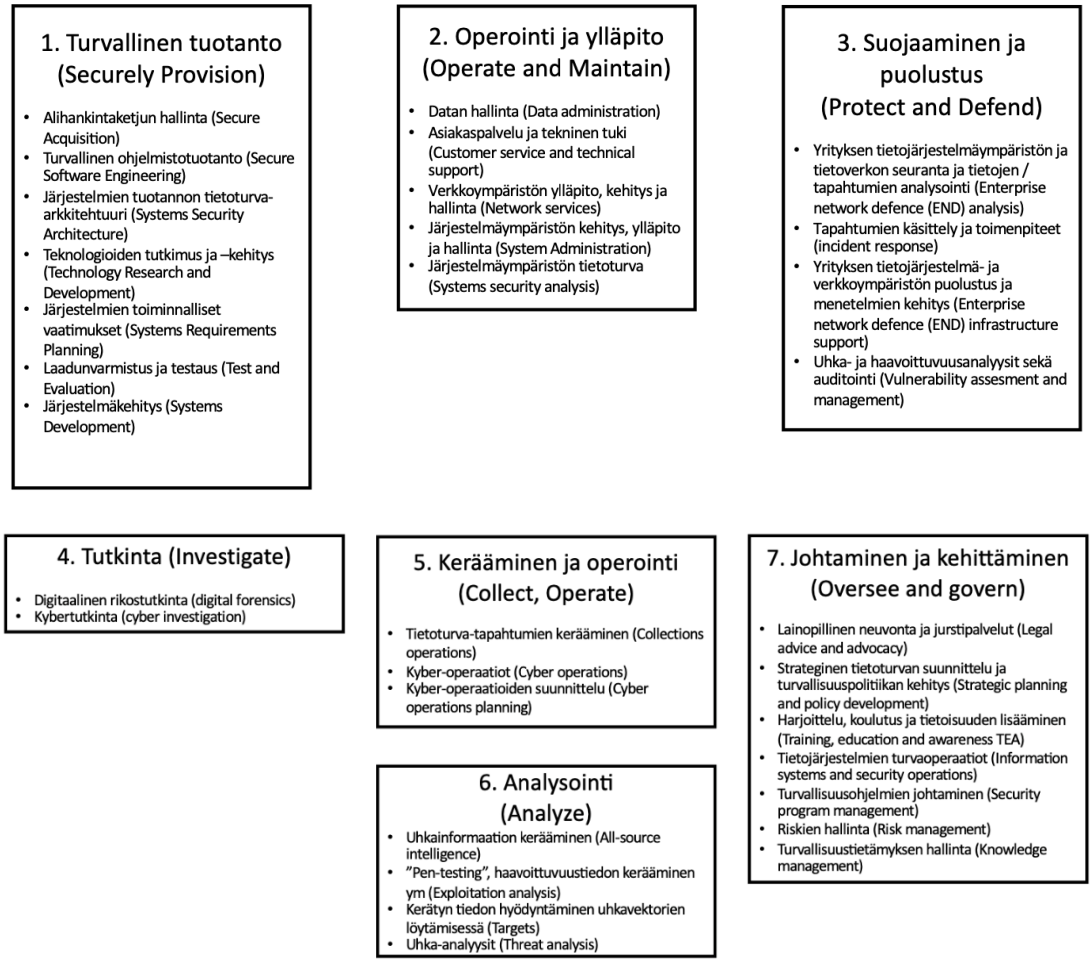
NCWF-mallin rakenne perustuu viitekehyksen tekijöiden perusteelliseen selvitykseen kyberturvallisuuden erilaisista työtehtävistä. Malli kokoaa näistä tiedoista yhtenäisen kokonaisuuden ja ryhmittelee samoja osaamisalueita jakavat työtehtävät niiden avulla loogisiksi kokonaisuuksiksi. Kokoelma auttaa lukijaa hahmottamaan kyberosaamisen ja siihen liittyvien toimialueiden rakennetta, menemättä liikaa yksityiskohtaisiin työnimikkeisiin tai työtehtävien kuvaukseen. Viitekehyksen kategoriat ja niiden sisällöt on kuvattu alla olevassa taulukossa (Taulukko 1).

Taulukko 1 NCWF Kategoriat ja niiden kuvaukset (Newhouse ym., 2017, s. 11 mukaan)

Kategoria	**Kuvaus**
1. Turvallinen tuotanto – Securely Provision (SP)	Konseptoi, suunnittelee ja rakentaa turvallisia IT-järjestelmiä (tietoverkkojen ja tietojärjestelmien kehitys).
2. Operointi ja ylläpito - Operate and maintain (OM)	IT järjestelmien tuki, hallinta (administration) ja huolto. Järjestelmien turvallisen ja tehokkaan toiminnan takaaminen.
3. Suojaaminen ja puolustus - Protect and defend (PR)	Organisaation tietoverkkoon ja järjestelmiin kohdistuvien turvallisuusuhkien Identifiointi, analysointi ja torjunta.
4. Tutkinta - Investigate (IN)	Kyberrikosten, IT-järjestelmiin ja tietoverkkoihin kohdistuvien rikosten/väärinkäytösten tutkinta. Digitaalisen todistusaineiston kerääminen.
5. Kerääminen ja operointi - Collect and operate (CO)	Kyberoperaatiot (peiteoperaatiot, palvelunesto, tiedustelutiedon keräys)
6. Analysointi - Analyze (AN)	Tiedustelutiedon analysointi ja evaluointi, tiedustelun käyttötarkoituksessa
7. Johtaminen ja kehittäminen - Oversee and govern (OV)	Organisaation kyberturvallisen toiminnan - turvallisuustyön johtaminen ja hallinta.

2.6.2 Erityisalueet (Speciality Areas)

Kategorioihin jaotellut erityisalueet ryhmittelevät kyberturvallisuuden tehtäväalueilla tunnistettuja työnkuvia, niiden yhteisten nimittäjien perusteella. Näin saadaan muodostettua kokonaiskuva laajemmista osaamiskokonaisuuksista, kuin vain yksittäisistä työtehtäviä ja -nimikkeitä tarkastellessa. Eri kategorioihin kuuluvat erityisalueet on kuvattu alla olevassa kuviossa, jossa ne on kytketty myös kategorioihin (Kuvio 4).

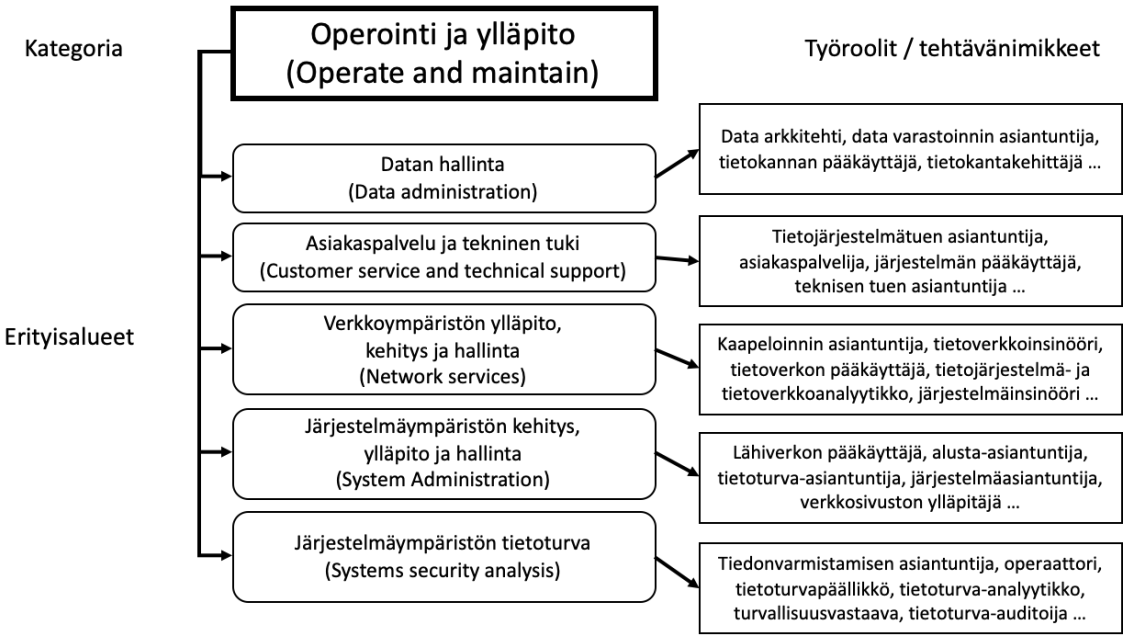


Kuvio 4 NCWF Kategoriat ja erityisalueet (Shoemaker, D., Kohnke, A., Sigler, 2016, ss. 16–47 mukaan)

2.6.3 Työroolit (Work Roles)

Malli rakentuu siis kategorioista ja niihin sisältyvistä erityisalueista. Erityisalueet on lisäksi jaoteltu niihin sisältyviin työrooleihin. Työroolit-taso kokoaa yhteen roolin tarvittavat attribuutit. Roolin attribuutteja ovat sen tehtävät, tehtävässä ja roolissa tarvittava tietämys (knowledge), taidot (skills) ja kyvyt (abilities). Attribuutit määrittyvät aina kulloisenkin työroolin tarpeiden perusteella.

Esimerkki työrooleista operointi ja ylläpitokategoriassa on havainnollistettu seuraavassa (Kuvio 5). Viitekehys sisältää samanlaisen jaottelun kaikissa kategorioissa ja erityisalueissa. Tässä on esitelty esimerkin vuoksi vain yksi. Jaottelussa käytetyt työroolit/-nimikkeet vastaavat yleisiä työnimikkeitä kategorian erityisalueilla, joten ne on helppo tunnistaa ja niitä voi verrata tai niitä voi pitää lähtökohtana markkinoilla yleisesti käytössä oleviin nimikkeisiin.



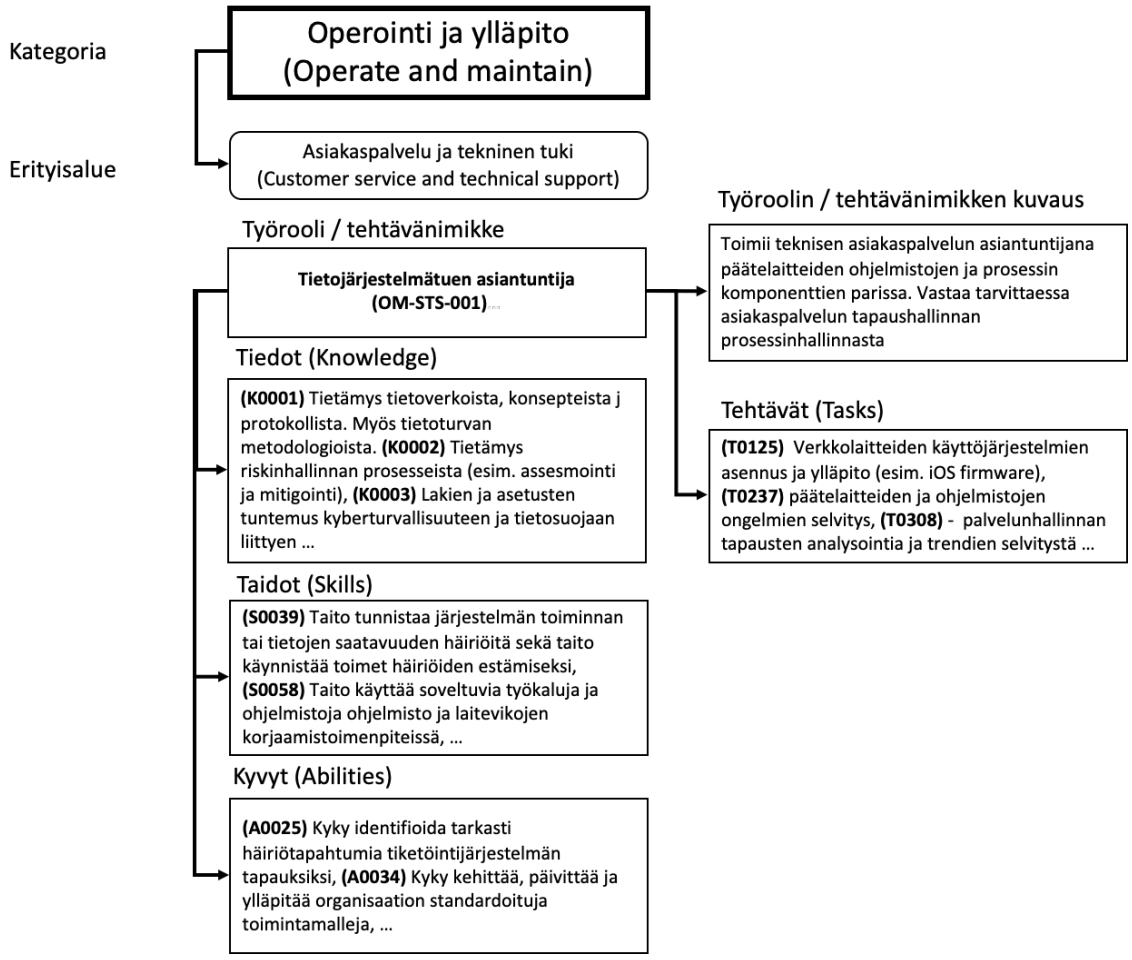
Kuvio 5 Esimerkki työrooleista: Operointi ja ylläpito-kategoria (Shoemaker, D., Kohnke, A., Sigler, 2016, s. 25 mukaan)

2.6.4 Tehtävät (Tasks)

Edellä kuvatun lisäksi viitekehys jakautuu vielä hienojakoisempiin osiin. Työrooleille on määritelty niissä yleisesti tarvittavat ja suoritettavat tehtävät.

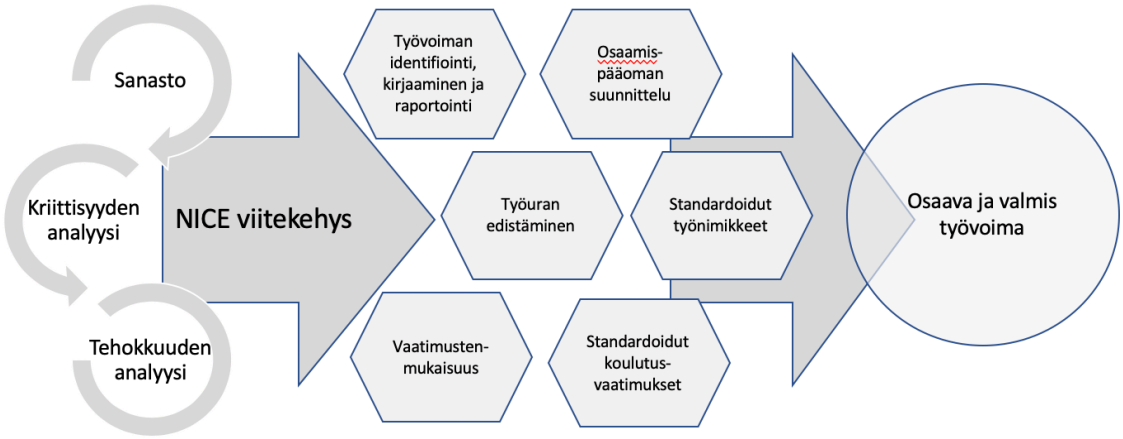
Tehtävä on työroolille tai työnimikkeelle määritetty tehtävä tai työsuorite, joka voidaan yleisesti käsittää roolille ominaiseksi. Työtehtävä muodostaa siten yhdessä muiden rooliin kuuluvien tehtävien kanssa työroolille ominaiset työtehtäväkokonaisuudet kyseisellä erityisalueella. Alla olevassa esimerkissä on kuvattu ylläpitokategoriaan liittyvän teknisen tuen työrooli ja siihen liittyviä tehtäviä. Kuvausta on laajennettu esimerkin vuoksi myös tehtävään liittyvien tietojen (knowledge), osaamisten (skills) ja kykyjen (abilities) kuvauksella (Kuvio 6).

Kuviossa ei ole kuvattu kaikkia kyseiseen tehtävään liittyviä tietoja, osaamisia tai kykyjä, koska sen tarkoitus on toimia vain esimerkkinä kuvauksen rakenteesta. Tarkempi ja kaikki tiedot sisältävä kuvaus on nähtävissä NCWF-viitekehyksestä (Newhouse ym., 2017). Tässä esitetty esimerkkikuvio havainnollistaa kuitenkin asioiden keskinäisen relaation ja kuvauksen tarkkuustason. Kuviosta on nähtävissä, kuinka yksityiskohtainen kompetenssien ja vaatimusten kuvaus käytetty viitekehys on. Vastaava kuvaus ja kuvauksien linkitys löytyy NCWF-viitekehyksen jokaisesta kategoriasta, erityisalueesta ja niihin liittyvästä tehtävästä.



Kuvio 6 Esimerkki: Työroolin tehtävät, tiedot, taidot ja kyvyt (Newhouse ym., 2017 mukaan)

Yllä kuvatun mallin avulla organisaatiot pystyvät suunnittelemaan ja toteuttamaan tehokkaita kyberturvallisuuden organisaatiota ja ohjelmia. Tämän lisäksi mallin käyttö yleisemmin lisää myös yhdenmukaista ymmärrystä toimialueesta ja helpottaa näin ollen myös osaavan työvoiman hankintaa ja helpottaa rekrytointiprosessin vaatimusten määrittelyä. Tätä yleisen tason toimintamallia kyberturvallisuuden osaamisen hallinnassa kansallisella tasolla on havainnollistettu seuraavassa (Kuvio 7).



Kuvio 7 Viitekehyksen hyödyt rekrytoinnissa ja kompetenssien kehittämisessä (Newhouse ym., 2017, s. 9 mukaan)

2.7 Muita kyberturvallisuuden hallinnan malleja

Tässä kappaleessa on kuvattu erilaisia yleisesti tunnettuja turvallisuudenhallinnan malleja. Kuvatut mallit on valittu siten, että ne edustavat kohdeyrityksessä käytössä olevia tai sovellettuja malleja. Lista ei kuitenkaan ole kaiken kattava kokoelma yleisesti tunnetuista turvallisuudenhallinnan tai kyberkompetenssien kehittämisen malleista, vaan sen tarkoitus on toimia esimerkkinä tapaustutkimuksen viitekehyksessä. Tässä esitellyt mallit eivät myöskään ole varsinaisia kompetenssien kehitystä tai organisaation kyberturvallisuuden tehtäviä kuvaavia malleja.

Kohdeyrityksessä ja yrityksissä yleensä käytetyt mallit ovat olemukseltaan useimmiten erilaisia tietoturvan standardeja ja sertifikaatteihin tähtääviä koulutusohjelmia. Kun NICE/NCWF -viitekehyksen kaltaista mallia ei aikaisemmin ole ollut käytettävissä, ovat organisaatiot ovat soveltaneet näitä standardeja ja malleja myös kompetenssien kehityksen viitekehyksinä. Poikkeuksen muihin tässä esiteltyihin malleihin tekee IISP Skills Framework-viitekehys, joka edustaa tutkimuksessa käytetyn NCWF-viitekehyksen ohella kyberturvallisuuden kompetenssien viitekehystä. Näitä kompetenssien kehityksen viitekehyksiä ei kohdeyrityksessä ole aiemmin ollut käytössä.

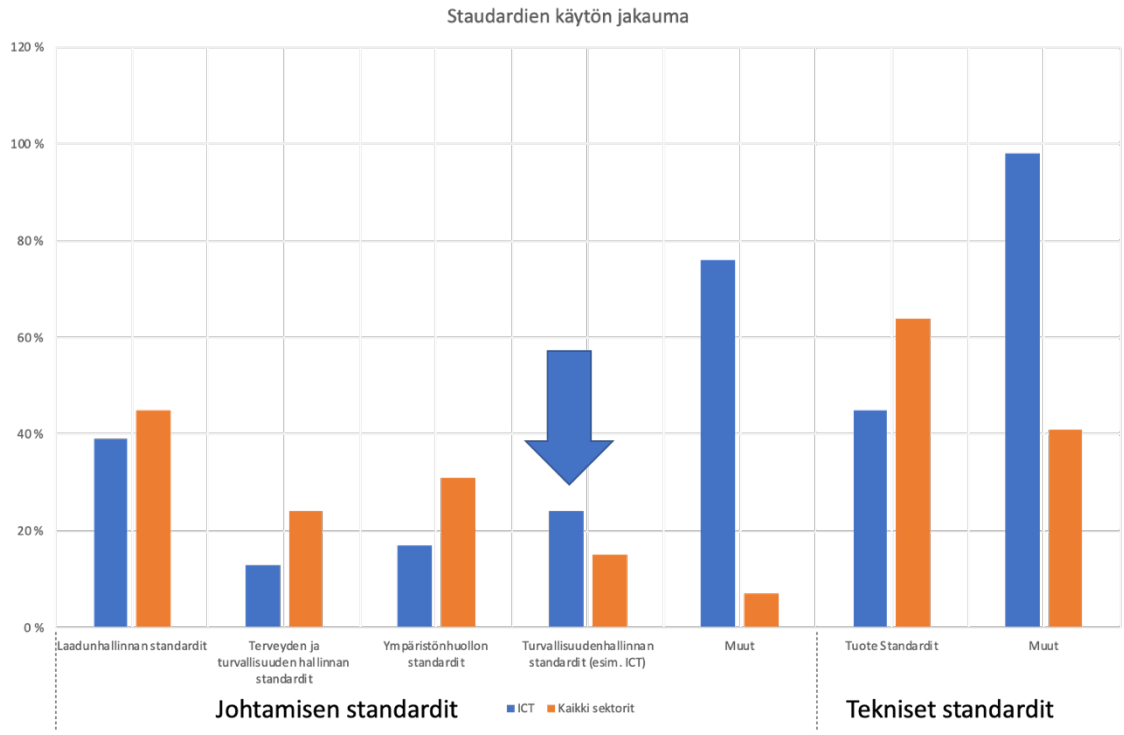
2.7.1 ISO 27000 -standardi

ISO 27000 -standardi viittaa kokonaiseen standardiperheeseen, liittyen tietoturvallisuuteen sen hallintaan, menetelmiin ja mittaamiseen. Standardi on tyypillinen organisaatioiden käyttämä referenssi, tietoturvallisuuden kehittämisessä,

mittaamisessa ja auditoinnissa. Näin on myös tämän tutkimuksen kohdeyrityksessä. Tässä kuvauksessa käsitellään vain standardin osat 27000-270005, jotka ovat suomennettuja tätä kirjoitettaessa.

Standardin osa 27000 luo yleiskatsauksen standardiin ja määrittää standardissa käytetyn sanaston. Osa 27001 kuvaa standardin vaatimukset informaatioteknologille, turvallisuustekniikoille ja tietoturvallisuuden hallintajärjestelmille. Standardin osa 27002 täydentää edellistä ja esittelee joukon tietoturvallisuuden hallintakeinojen menettelyohjeita (Code of practice). Standardin osassa 27003 annetaan ohjeita hallintajärjestelmän toteuttamiselle. Osassa 27004 ohjeistetaan hallintamenetelmien toiminnan mittaamista. Osa 27005 määrittää tietoturvariskien hallinnan vaatimuksia. (Suomen Standardisoimisliitto SFS ry, 2018, ss. 16–17).

Erilaiset standardit ja niiden käyttö on tutkitusti yleistä ICT-sektorilla, johon myös kohdeyritys toimialansa puolesta kuuluu. Erityisesti tietoturvaan liittyvien standardien käyttö on tällä sektorilla muita yleisempää. Muita alalla erityisesti käytössä olevia standardeja ovat johtamiseen ja teknologioihin liittyvät standardit (Kuvio 8) (Menon, 2018).



Kuvio 8 Vertailu standardien käytöstä ICT- ja muilla aloilla (Menon, 2018, s. 47 mukaan)

ISO 27001-standardin sisällön kuvauksesta on havaittavissa, että sen tulokulma kyberturvallisuuteen on hyvin teknisorganisatorinen. Standardi määrittää tietoturvallisuuden menetelmät, tekniikat, niiden mittauksen ja auditoinnin, mutta vaatimuksia organisaation kompetensseille ei suoranaisesti aseteta, eikä niihin liittyviä ohjeistuksia anneta. Standardin asettamaan vaatimustasoon riittävien kompetenssien ikään kuin oletetaan olevan olemassa tai kehittyvän annettujen vaatimusten pohjalta.

2.7.2 VAHTI -ohje

Toinen tunnettu ja Suomessa yleisesti tässä viitekehyksessä eri organisaatioissa myös yksityisellä puolella käytetty tietoturvallisuuden malli on valtionhallinnolle kehitetty VAHTI -ohjeistus (Valtiovarainministeriö, 2019). VAHTI-ohje on julkisen hallinnon digitaalisen turvallisuuden johtoryhmän tuottama ohjeistus valtionhallinnon tietoturvallisuuden ohjeistukseksi. VAHTI-ohje on tätä kirjoittaessa parhaillaan päivittymässä VAHTI 100 -hankkeen myötä. Tässä kuvauksessa käsitellään nykyisin voimassaolevan ohjeistuksen sisältöä.

VAHTI-ohje on seikkaperäinen ja laaja kokoelma erilaisia tietoturvaan ja tietosuojaan liittyviä ohjeita. Ohjeita löytyy niin henkilöstölle, salaukseen, auditointiin kuin toimitiloihin ja sovelluskehitykseenkin liittyen. Myös tietoverkot, toiminnan jatkuvuus ja sosiaalinen media ja sen käyttö ovat aihealueita, joihin löytyy ohjeita VAHTI-kokoelmasta. Ohjeiden määrä ei rajoitu vain tässä mainittuihin, mutta merkittävää on kuitenkin se, että varsinaisia henkilöstön osaamiseen tai kyberturvallisuuden osaamiseen liittyviä ohjeita tässäkin kokoelmassa on hyvin vähän. Kokonaisvaltaisen ymmärryksen saaminen kyberturvallisuuden kompetenssien vaatimuksista tämänkin laajan, ja yksittäisistä ohjekokonaisuuksista koostuvan, kirjaston avulla on myös haastavaa. VAHTI-ohje lähestyy kyberturvallisuutta muiden tavoin, teknisestä ja toiminnallisesta näkökulmasta, ei kompetenssien näkökulmasta.

2.7.3 CISSP

Certified Information Systems Security Professional (CISSP), vapaasti käännettynä Sertifioitu informaatioteknologian tietoturvallisuuden ammattilainen, on Amerikkalaisen ISC2 organisaation kehittämä ja ylläpitämä sertifikaatti ja siihen liittyvä koulutuskokonaisuus (ISC2, 2019). Sertifikaatti on erittäin tunnettu, arvostettu ja laaja opintokokonaisuus. Kurssiin liittyvän tentin hyväksytty suorittaminen tarjoaa suorittajalleen arvostetun CISSP sertifikaatin.

CISSP -sertifikaatin lisäksi ISC2 tarjoaa koulutuskokonaisuuksia myös muihin CISSP:n alaisiin alisertifikaatteihin. Näitä ovat alla olevassa kuviossa (Kuvio 9) mainitut sertifikaatit, joista kukin kattaa osaltaan laajemman CISSP sertifikaatin sisältöjä. Itse CISSP-sertifikaatti jakautuu kahdeksaan eri osa-alueeseen. Näitä osa-alueita ovat: 1) turvallisuuden ja riskien hallinta, 2) tila-/kiinteistöturvallisuus, 3) tietoturva-arkkitehtuuri ja teknologiat, 4) kommunikaatio- ja tietoverkkoturvallisuus, 5) identiteetin ja laitteiden hallinta (IAM), 6) turvallisuuskatselmoinnit ja -testaus, 7) tietoturvaoperaatiot ja 8) ohjelmistokehityksen tietoturva. CISSP-sertifikaatin voidaan sanoa olevan laajimpia tietoturvan osaamista mittaavista ja kehittävistä sertifikaateista ja antavan kattavan koulutussisällön ja osaamisportfolion sen suorittaneille kyberturvallisuuden ammattilaisille.

CISSP -sertifikaatin saaminen edellyttää hyväksytyn tentin suorittamisen lisäksi myös riittävää määrää verifioitua työkokemusta, joten sertifikaattiin liittyvää osaamissisältöä voi tästäkin näkökulmasta pitää hyvin laajana.

Vähemmän työkokemusta omaaville henkilöille ISC2 tarjoaa ”associate” -tason sertifikaattia, jonka voi myöhemmin kokemuksen karttuessa täydentää täydeksi CISSP -sertifikaatiksi.

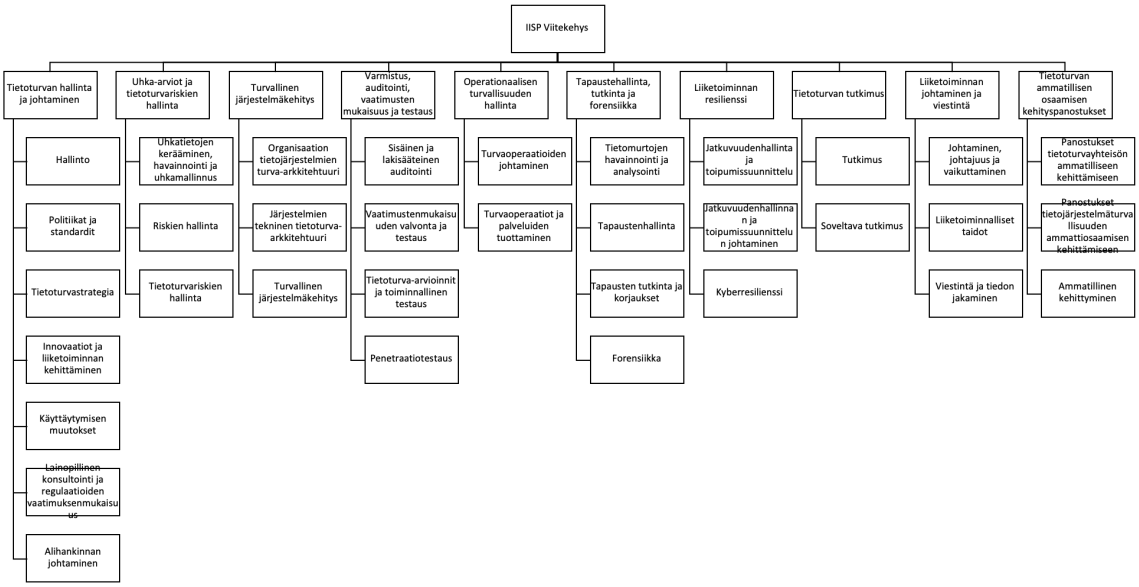
Sertifikaatin ylläpito edellyttää myös jatkuvaa opiskelua ja ajoittaisia uusinta tenttejä. Näin ollen CISSP:n voidaan katsoa olevan lähimpänä kyberturvallisuuden kompetenssien näkökulmasta turvallisuutta lähestyvää mallia. Kyseessä on kuitenkin kaupallisen toimijan määrittämä ja ylläpitämä konsepti. Avoimesta tai yleishyödyllisestä kokonaisuudesta ei siis ole kysymys, mikä on hyvin yleinen tilanne informaatioteknologian sertifioinneissa myös yleisemmin. Kuten sanottua, CISSP nauttii kuitenkin yleistä arvostusta erityisesti informaatioteknologian toimialueella ja sitä pidetään korkean osaamistason merkkinä. CISSP-sertifikaatin osaamissisältöjen ymmärtämisestä voi olla myös apua hahmotettaessa kyberturvallisuuden toimialueen kompetenssien yleisiä vaatimuksia.

Kuvio 9 ISC2 tietoturvasertifioinnit (ISC2, 2019)

2.7.4 IISP-viitekehys

Englantilaisen Institute of Information Security Professionals (IISP) vuonna 2007 tuottama kyberturvallisuuden kompetenssien viitekehys on NCWF -viitekehyksen ohella toinen kokonaisvaltaiseen kyberosaamisen ja -kompetenssien sekä näiden vaatimusten kuvaamiseen pyrkivä viitekehys. Kuten NCWF, myös IISP kehitettiin yhteistyössä akateemisten toimijoiden, yritysten ja valtionhallinnon

kesken, aikomuksena saavuttaa ”de-facto” standardin asema tässä alati kehittyvässä ja monimutkaisessa kyberturvallisuuden osaamisen ja sertifiointien kentässä. Hyvin saman tyyppinen pyrkimys siis, kuin tässä tutkimuksessa käsitellyllä NCWF -viitekehyksellä. Oheisessa kaaviokuvassa (Kuvio 10) on kuvattu skills framework -mallin rakennetta.



Kuvio 10 IISP Skills-viitekehys (Furnell ym., 2017, s. 8 mukaan)

Mallin ensimmäinen taso jaottelee tietoturvallisuuden eri toimialueet (Security Diciplines) kymmeneen eri kategoriaan. Niihin liittyviä osaamisalueita (Skills Groups) on yhteensä 33. Tämän lisäksi IISP tarjoaa kompetenssien ja osaamisen määrittelyyn tähtäävän tietämysviitekehyksen (Knowledge framework) sekä varsinaisiin työtehtäviin ja niiden sisältöjen määrittelyyn keskittyvän viitekehyksen (IIS Roles framework) (The Institute of Information Security, 2019). Koska nyt tehtävä tutkimus toistaa aiemmin tehdyn tutkimuksen (Willberg, 2017) tutkimusasetelmaa, käytetään tässä tutkimuksessa NCWF-viitekehystä. IISP Skills Frameworkin käyttö tutkimuksessa olisi kuitenkin mielenkiintoinen jatkotutkimuksen kohde, kuten myös NCWF ja IISP-viitekehysten vertailu.

2.8 Kyberosaamisen kokonaisnäkemyksen haaste

Kuten aiemmasta kyberturvallisuuden aihealueen ja nykytilan kuvauksesta sekä mallien ja viitekehysten esittelystä käy ilmi, on kyberturvallisuuden osaaminen, kompetenssit ja niiden kehittäminen suuri haaste niin valtioille kuin muillekin organisaatioille. Toimialueen yksityiskohtien paljous, alan koulutustarjonnan ja sertifikaattien kirjavuus sekä standardien ja regulaation laajat vaatimukset niin tietosuojan, kuin tietoturvankin osalta, muodostavat yhdessä laajan vaatimusten kentän (Baker, 2016). Kattavan ymmärryksen saavuttaminen sekä yhteisen kielen

ja termistön määrittely on tärkeää. Selkeät työnkuvat ja osaamisvaatimukset ovat keskeisiä avaintekijöitä onnistuneessa kyberosaamisen rekrytoinnissa (Baker, 2016, s. 20; Newhouse ym., 2017, s. 7). Tätä kaikkea tukeva koulutustarjonta yliopistoissa ja ammattikorkeakouluissa on keskeisessä roolissa tämän kaiken mahdollistajana.

Ohjelmistotuotannossa toimivat yritykset toimivat omalta osaltaan tilanteen keskiössä. Yritysten tulee oman kyberturvallisuuden lisäksi huolehtia myös omien tuotantohyödykkeidensä, eli ohjelmistojen kyberturvallisuuden ajantasaisuudesta. Ohjelmistoyritykset ovat samaan aikaan yhtäältä kybertuvallisuuden kuluttajia ja toisaalta mitä suuremmissa määrin sen tuottajia.

Paitsi kompleksinen kokonaisuus, kyberturvallisuusosaamisen tarpeen lisääntymisen on todettu olevan myös osoitus maailmantalouden ja teknologian kehityksestä. Lisääntynyt teknologia, erilaiset uudet mediat sekä tietoteknistä sektoria säätelevien normien lisääntymisen on todettu lisäävän myös kyberturvallisuuden osaajien tarvetta ja määrää. Näin todetaan mm. ISC2:n tuottamassa maailmanlaajuista kyberturvallisuuden työvoiman osaamista kartoittavassa tutkimuksessa vuonna 2013 (Suby, 2013).

Sama tutkimus toteaa ohjelmistokehityksen tietoturvan olevan suurin yksittäinen ongelmakenttä, jossa riskin määrä ei korreloi toimenpiteisiin sen ehkäisemäksi (Suby, 2013). Tutkimuksessa todettiin myös, että uudet teknologiat, kuten pilviteknologiat ja omien laitteiden käyttö työssä ja muut työympäristön muutokset, aiheuttavat lisääntyvää ja monipuolistuvaa tiedon tarvetta ja uusien teknologisten apuvälineiden käyttöä ja hallintaa myös kyberturvallisuuden osaamissektorilla (Suby, 2013, s. 4).

3 TUTKIMUSMENETELMÄT

Tässä kappaleessa kuvataan tutkimuksessa käytetty tutkimusmenetelmä ja tutkimuksen toteutukseen liittyvät yksityiskohdat ja rajaukset. Kappaleessa kerrotaan taustatietoja myös tutkimuksen toimeksiantajasta, joka on myös tapaustutkimuksen kohdeyritys.

Kohdeyrityksen kuvauksen jälkeen kappaleessa kerrotaan Jyväskylän yliopistossa aiemmin tehdyn, tätä aihealuetta tutkineen, tutkimuksen keskeisimmät havainnot (Willberg, 2017). Aiemman tutkimuksen kuvaus on tehty, koska nyt tehty tutkimus toistaa tämän aiemman tutkimuksen tutkimusasetelman. Näiden tutkimusten havaintoja myös vertaillaan myöhemmin tässä raportissa esiteltyjen tutkimustulosten esittelyn yhteydessä.

3.1 Tarkennukset ja rajaukset

Ohjelmistoyrityksen liiketoiminnan kyberturvallisuuden kompetenssien määrittely, kehittäminen ja tutkiminen ovat kokonaisuudessaan varsin laaja aihealue. Aihealueella on nähtävissä myös vaihtelua eri yritysten välillä, riippuen yrityksen toimialasta, käytetyistä teknologioista ja muista liiketoiminnan osatekijöistä (Radunović & Rüfenacht, 2016). Tämän lisäksi tutkimuksen pohjana käytetty viitekehys voi vaikuttaa tutkimuksen toteutukseen ja mahdolliseen sisältöön (Tuomi & Sarajärvi, 2018, s. 154).

Nyt tehty tutkimus rajautui tarkastelemaan kohdeyrityksen kyberosaamisen nykytilaa ja mahdollisesti tutkimuksen kautta esiin nousevia tulevaisuuden kehitystarpeita yritystasolla. Tutkimus käytti selvitystyön pohjana tutkimusraportin kirjallisuuskatsauksessa esiteltyä amerikkalaista NCWF-viitekehystä (Newhouse ym., 2017), sen laaja-alaisuuden ja yksityiskohtaisen kyberosaamisen sisällön kuvaamisen ansiosta. Viitekehys valikoitui käytettäväksi myös aiemman tutkimuksen (Willberg, 2017) tutkimusasetelman johdosta. Kohdeyrityksen koko ja sen laaja toimiala antoivat myös hyvät mahdollisuudet tutkia kyberosaamisen tarpeita laaja-alaisesti ohjelmistoliiketoiminnassa. Tämän arvioitiin osaltaan parantavan tulosten hyödynnettävyyttä myös jatkotutkimuksessa.

Varsinaista kyberturvallisuuden kompetenssien hallintajärjestelmää, kehitysmallia tai yksilötason kompetenssien yksityiskohtaista rakennetta ei kuitenkaan ollut tarkoitus tutkia tai kehittää tässä tutkimuksessa. Kompetenssien tai kyberturvallisuuden hallintamallin kehittäminen nähtiinkin potentiaalisena jatkotutkimuksen aiheena.

3.2 Tutkimusmenetelmä

Tutkimus toteutettiin laadullisena tapaustutkimuksena. Aineistonkeruutapana käytettiin puolistrukturoituja teemahaastatteluita, jotka toteutettiin

toimeksiantajayrityksen turvallisuus- ja ICT johtajien haastatteluina. Haastattelun sisällöt nojautuivat NCWF-viitekehyksen sisältöön sekä sen kategorioiden ja erityisalueiden jaotteluun. Näin aineistosta pyrittiin luomaan teoreettinen kokonaisuus (Tuomi & Sarajärvi, 2018). Tutkimuksessa tutustuttiin myös toimeksiantajayrityksen aiheeseen liittyvään dokumentaatioon ja prosesseihin.

3.3 Tutkimuksen käytännön toteutus

Tutkimushaastattelut toteutettiin kahtena erillisenä etähaastatteluna, käyttäen kohdeyrityksen Microsoft Teams-palvelua. Turvallisuusjohtajan (CSO) haastattelu tehtiin 16.4.2020 ja ICT-johtajan (CIO) haastattelu 20.4.2020. Molemmat haastattelut tallennettiin sekä Microsoft Teams-ohjelmistolla (ääni ja video) sekä mobiililaitteella (ääni). Haastateltaville toimitettiin ennen haastattelua liitteen 1 mukainen etukäteismateriaali tutustuttavaksi. Materiaalissa kuvattiin tutkimuksen sisältöä, viitekehystä ja taustatietoja. Tämän lisäksi materiaalissa esiteltiin haastattelun alustavat kysymykset (liite 1).

Tallennetut haastattelut litteroitiin ja analysoitiin sekä luokiteltiin NCWF-viitekehyksen kategorioiden ja erityisalueiden mukaisesti (Tuomi & Sarajärvi, 2018). Haastatteluaineistojen litteroinnissa käytettiin saksalaista f4transkript-sovellusta (Dresing ym., 2020b). Litteroidut aineistot analysoitiin ja luokiteltiin käyttäen saman toimittajan f4analyse tekstiaineistojen luokittelu- ja analyysisovellusta (Dresing ym., 2020a). Tekstin analyysin ja luokittelun avulla aineistosta etsittiin viitteitä ja tietoja viitekehyksen mukaisten kategorioiden ja erityisalueiden mukaisten kompetenssien nykytilasta ja mahdollisista tulevaisuuden kehitystarpeista. Analyysin perusteella tuotetut johtopäätökset on kuvattu tässä tutkimusraportissa. Saatuja tutkimustuloksia verrattiin myös Willbergin (2017) tekemän tutkimuksen tuloksiin. Vertailun tulokset on kuvattu myöhemmin tässä raportissa.

3.4 Kohdeyritys

Tutkimuksen kohdeyrityksenä oli Yritys X. Yritys on ohjelmisto- ja palveluyritys, joka auttaa asiakkaitaan kehittämään toimintaansa verkottuvassa maailmassa. Yritys toteuttaa erilaisia tietojärjestelmä- ja alustaratkaisuja sekä auttaa asiakkaitaan hyödyntämään niihin liittyvää dataa ja rakentamaan sen avulla parhaita mahdollisia asiakaskokemuksia. Yrityksen asiakkaat edustavat useita eri toimialoja ja koostuvat niin yksityisistä, kuin julkisenkin sektorin toimijoista. Kohdeyrityksellä on useita toimipisteitä ja yritys työllistää tällä hetkellä yli 1000 ohjelmistoalan ammattilaista. Yrityksen liikevaihto vuonna 2019 oli yli 100 miljoonaa euroa ja yritys on listattuna Nasdaq Helsingissä. (Yritys X, 2019)

Tietosuojasta ja kokonaisturvallisuuden hallinnasta kohdeyrityksessä vastaa yksikkö nimeltä Chief Security Office (CSO Office). Yksikön tehtävänä on

huolehtia yrityksen kokonaisturvallisuuden kaikista osa-alueista, yhdessä sidosryhmiensä kanssa. Näitä turvallisuustoiminnan osa-alueita ovat mm. kyberturvallisuus, tilaturvallisuus, turvallisuustoiminnan johtaminen. Myös tietosuojaasiat sekä turvallisuuspolitiikat, turvallisuusprosessien kehitys ja niihin liittyvät ohjeet kuuluvat yksikön vastuualueeseen. Edellä mainittujen lisäksi myös kohdeyrityksen henkilöstön turvallisuuteen liittyvän osaamisen kehittäminen, koulutuksen koordinointi ja tuotanto kuuluvat yksikön toimialueeseen.

CSO Office toimii edellä mainituilla osa-alueilla tiiviissä yhteistyössä kohdeyrityksen johdon ja liiketoimintojen sekä palveluiden tuotannon kanssa. Yksikkö tuottaa myös kybertilannekuvaa yrityksen sisäiseen käyttöön sekä kehittää kyberturvallisuuden havainnointikykyä ja muita turvallisuuden palveluita yhtiön omaan käyttöön.

Tämä tutkimus toteutettiin kohdeyrityksen toimeksiantona. Tutkimuksessa tehtiin yhteistyötä yrityksen turvallisuus- ja ICT-organisaatioiden sekä yrityksen henkilöstöhallinnon ja johdon kanssa.

3.5 Aiempi tutkimus

Kuten aiemmin on todettu, nyt tehty tutkimus toisti Willbergin (2017) Jyväskylän yliopistossa aiemmin tekemän tutkimuksen tutkimusasetelman, mutta tällä kertaa eri toimialalla. Willberg tutki kyberturvallisuuden kompetensseja ja niihin liittyviä kehitystarpeita julkisen sektorin organisaatioissa. Kohdeorganisaatioina siinä tutkimuksessa olivat Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK) ja Poliisin Kyberrikostorjuntakeskus.

Willbergin tutkimuksen teoreettisena viitekehyksenä käytettiin amerikkalaista NIST:n kehittämää NCWF-viitekehystä. Tutkimus toteutettiin tapaustutkimuksena ja sen aineistonkeruumenetelmänä käytettiin viitekehykseen nojautuvia teemahaastatteluita. Haastatteluaineistot tallennettiin ja litteroitiin. Litteroinnin perusteella havainnot luokiteltiin NCWF-viitekehyksen mukaisiin kategorioihin ja myöhemmin ydinkompetenssiesityksessä lisäksi vakiintuneeseen ja kehittyvään kompetenssialueeseen. Tutkimusaineiston analyysimenetelmänä tutkimuksessa käytettiin teorialähtöistä sisältöanalyysiä.

Willbergin tutkimuksen tutkimusasetelma ja siinä käytetyt aineistonkeruu- ja luokittelumenetelmät olivat siis samoja, kuin tässä tutkimuksessa käytetty asetelma ja menetelmät. Samoja menetelmiä ja samaa teoreettista viitekehystä soveltamalla tutkimustuloksista pyrittiin saamaan yhteismitallisia ja vertailtavia. Willbergin käyttämä tutkimusasetelma ja viitekehys nähtiin hyödylliseksi ja sen arvioitiin soveltuvan myös tässä tutkittuun tapaukseen.

Willbergin tutkimuksen keskeisenä havaintona oli, että organisaation toiminnan tarkoitus määrittää organisaation kyberturvallisuuden osaamisessa muodostuvat ja siinä tarvittavat keskeiset kompetenssit. Tutkimuksessa havaittiin myös, että organisaation itsenäisesti tai yhteistyössä muiden kanssa tuottamat kyberturvallisuuden toiminnot olivat keskeisiä tutkittujen organisaatioiden toiminnassa. Normatiiviset, eli regulaatioon tai lainsäädäntöön perustuvat toiminnot, nähtiin myös tärkeitä osaamisalueita sisältävänä ja niiden nähtiin

liittyvän organisaation normatiivisten velvoitteiden täyttämiseen. Normatiivisiin toimintoihin liittyviä kompetensseja ei tutkimuksessa kuitenkaan pidetty kohdeorganisaatioiden ydinkompetenssin osa-alueina siksi, että osa-alueisiin havaittiin sisältyvän organisaatioiden vaikutuspiirin ulkopuolella olevia osaamisvaatimuksia. Näkemys pohjautui Chenin ja Changin havaintoon, jossa ydinkompetenssin todetaan syntyvän vain yrityksen sisällä (Chen & Chang, 2010). Tutkimuksessa todettiin myös, että tutkittujen organisaatioiden kyberturvallisuuden ydinkompetenssit muodostuivat vain osasta teoreettisen viitekehyksen kategorioita.

Havaintojen NCWF-kategorioihin luokittelun lisäksi Willberg jakoi havainnot vakiintuneeseen ja kehittyvään kompetenssialueeseen. Tätä jaottelua käytettiin havaittujen ja NCWF-viitekehyksen kategorioihin jaoteltujen ydinkompetenssien hienojakoisemmassa tarkastelussa.

Willbergin perushavaintoon liittyen hänen tutkimuksessaan tutkittujen organisaatioiden kyberturvallisuuden kompetenssit nähtiin pääsääntöisesti toisistaan eriävinä ja eri kategorioihin painottuvina. Tutkimuksessa havaittiin kuitenkin myös yhteneväisyyksiä tutkittujen organisaatioiden kompetenssien painottumisen suhteen. Tätä yhteneväisyyttä nähtiin olevan erityisesti kehittyvien ydinkompetenssien osa-alueilla. Tämän arvioitiin liittyvän kyberturvallisuuden toimialueen nopeaan ja ennalta määrittämättömään kehityskulkuun.

Jatkotutkimuksen osalta aiempi tutkimus ehdotti kyberturvallisuuden syvällisen osaamisen kartoittamisen laajentamista eri typpisiin organisaatioihin. Tämän arvioitiin lisäävän relevanttien hypoteesien muodostamisen mahdollisuutta, mikä puolestaan edesauttaisi tutkimustulosten yleistettävyyttä jatkossa.

4 TULOKSET

Tässä kappaleessa kuvataan nyt tehdyn tutkimuksen tulokset. Kuvaus alkaa kohdeyrityksen kyberosaamisen nykytilan kuvauksella. Nykytilan kuvauksen jälkeen tutkimustulokset esitellään havaintojen yhteenvetona ja tämän jälkeen yksityiskohtaisemmin NCWF-kategorioittain jaoteltuna. Tutkimustulosten esittelyn jälkeen luodaan katsaus myös tutkimuksen aikana esiin nousseisiin kyberosaamisen tulevaisuuden tarpeisiin ja vertaillaan tässä tutkimuksessa saatuja tuloksia Willbergin (2017) aiemman tutkimuksen tuloksiin.

4.1 Kohdeyrityksen kyberosaamisen nykytila

Kyberturvallisuus itsessään on moninainen ja monimutkainen kokonaisuus, joka vaatii monenlaista osaamista (Menon, 2018; Niemelä, 2019; Shoemaker, D., Kohnke, A., Sigler, 2016). Tämä sama havainto nousi esiin myös tämän tutkimuksen aineistossa.

Radunović & Rüfenacht (2016) havaitsivat, että yhdistämällä kyberturvallisuuden monimutkaiseen ja laajaan kokonaisuuteen monen toimialan, teknologian ja menetelmän sekä alustan mukaisen ohjelmistotuotannon, nousee osaamisen ja hallinnan haaste moninkertaiseksi (Radunović & Rüfenacht, 2016). Sama havainto kävi esiin myös tämän tutkimuksen aineistossa. Tutkimusaineistosta kävi selväksi, että ohjelmistojen tuottajan tulee tutkitussa kokonaisuudessa hallita useita erilaisia teknologioita, alustoja ja asiakkaiden erilaisia toimialoja. Tämän lisäksi ohjelmistotoimittajan tulee hallita myös kaikkiin edellä mainittuihin osa-alueisiin liittyvät kyberturvallisuuden vaatimukset, jotka myös edellä mainituista syistä voivat olla hyvinkin erilaisia. Kaikki tämä tulee lisäksi hallita ja tuottaa oikea-aikaisesti. On siis oltava ”ajan hermolla”, seurattava aikaa ja muutosta. Samaan aikaan toiminnan ”maali” liikkuu jatkuvasti. Haastatteluissa esiin noussut havainto siitä, että ”juuri kun olet perillä, huomaat olevasi jo myöhässä” kuvaa hyvin tähän tilanteeseen liittyviä haasteita.

Tutkimusaineiston perusteella oli nähtävissä, että toimialueen palvelualustat ja ekosysteemit myös kehittyvät koko ajan. Niissä käytettävät teknologiat muuttuvat ja koko tuotannon paradigma on jatkuvassa muutoksessa. Tämän tutkimuksen aineistosta nousi esiin myös Ahmadin ja Babarin tutkimuksessaan tekemä havainto: ”Legacy-järjestelmistä” on tai ollaan siirtymässä pilviteknologioihin ja -alustoihin (Ahmad & Babar, 2014).

Tutkimuksen perusteella ohjelmistotuotannon nähtiin olevan osin muuttumassa ohjelmistojen kokonaistuotannosta eri alustojen päälle rakennettaviksi modulaarisiksi ratkaisuiksi. Jos toimittaja aiemmin tuotti koko monikerrosarkkitehtuurin mukaisen ratkaisun itse ja vastasi sen turvallisesta tuotannosta, toimituksesta ja käytöstä, on tämä sama toimittaja nyt kenties rakentamassa palveluaan osaksi jonkin pilvipalvelun ekosysteemiä. Havainnon perusteella voi päätellä, että tällaisissa skenaarioissa myös kyberturvallisuuden kokonaisuus ja

siihen liittyvä osaaminen on hyvin erilaista. Samaan aikaan toisaalla, samassa yrityksessä, saatetaan kuitenkin edelleen tuottaa ohjelmistoja perinteisellä tyylillä.

Edellä kuvattu nähtiin tyypillisenä ongelmakenttänä monialaisen ja suuren ohjelmistotuottajan toimintaympäristössä myös yleisemmälläkin tasolla. Sama haaste nousi esiin myös tutkimuskirjallisuudessa. Samat jatkuvan muutoksen ja monialaisen ongelmakentän havainnot nousivat esiin myös tämän tutkimuksen aineistoissa. Monialainen toiminta, erilaiset asiakkaat, erilaiset teknologiat, alustat ja ekosysteemit luovat haasteellisen toimintaympäristön myös kyberturvallisuudelle.

Alla olevassa taulukossa (Taulukko 2) on listattu tutkimusaineistosta esiin nousseiden havaintojen määrät NCWF-viitekehyksen kategorioihin luokiteltuna. Taulukko sisältää myös viitekehyksen ulkopuolisten havaintojen sekä muiden aineistosta esiin nousseiden ja tutkimuksen ulkopuolelle rajattujen havaintojen määrät. Näitä havaintoja on kuvattu myöhemmin tässä raportissa.

Taulukko 2 Tutkimuksen kohdeyrityksen haastatteluaineiston luokittelujen määrä kategorioittain

NCWF-kategoriat ja viitekehyksen ulkopuolisten havaintojen kategoriat	**Luokitteluita (kpl)**
0. Viitekehykseen liittyvät yleiset havainnot	19
1. Turvallinen tuotanto (Securely provision)	24
2. Operointi ja ylläpito (Operate and Maintain)	24
3. Suojaaminen ja puolustus (Protect and defend)	2
4. Tutkinta (Investigate)	3
5. Kerääminen ja operointi (Collect, Operate)	6
6. Analysointi (Analyze)	13
7. Johtaminen ja kehittäminen (Oversee and govern)	10
Muut havainnot	14

Haastatteluaineiston luokittelun perusteella voitiin päätellä, että kyberosaamisen tarve jakautui kohdeyrityksessä varsin laajasti lähes koko viitekehyksen alueelle. Jakautumisen arvioitiin kuvaavan kyberturvallisuuden osaamistarpeen laajuuden lisäksi myös siihen liittyvää resurssienhallinnan ja investoinnin haastetta. Tämä haaste nousi esiin myös haastatteluaineistossa. Viittausten painottuminen tiettyihin kategorioihin antoi myös viitteitä ydinkompetenssin mahdollisista painopistealueista.

Seuraavissa kappaleissa on kuvattu yksityiskohtaisemmin haastatteluaineistosta tehtyjä havaintoja osaamisen nykytilasta viitekehyksen eri kategorioissa. Tarkastelu tehtiin yritystasolla ja sen avulla pyrittiin hahmottamaan yrityksen kyberosaamisen ydinkompetenssia sen nykytilanteessa.

4.1.1 Turvallinen tuotanto (Securely provision)

Haastatteluaineiston luokittelun perusteella turvallinen tuotanto voitiin nähdä keskeisimpänä kategoriana kohdeyrityksen liiketoimintaan liittyen. Yhdessä operointi ja ylläpito -kategorian kanssa ne muodostivat haastatteluaineiston perusteella Kohdeyrityksen kyberturvallisuuden osaamisen keskeisimmän osa-alueen. Tässä kappaleessa on kuvattu havaintoja turvallisen tuotannon erityisalueiden osalta.

Alihankintaketjun hallinta nähtiin aineiston perusteella tarpeellisena ja keskeisenä osaamisalueena turvallisen tuotannon kategoriassa. Sen voitiin ajatella olevan siis ydinkompetenssin yksi osa-alue. Kyberturvallisen toimintamallin nähtiin kohdistuvan vaatimuksena aina koko alihankintaketjuun. Toimittajaan (kohdeyritys) kohdistuvat vaatimukset nähtiin vyörytettävän aina myös toiminnassa mukana oleville alihankkijoille. Ohjelmistotoimittajan nähtiin vastaavan alihankkijan työstä aina kuten omasta työstään. Kohdeyrityksen laatujärjestelmän todettiin myös sisältävän ohjeistuksen ja prosessikuvauksen alihankintaketjun hallintaan ja siihen liittyviin toimenpiteisiin.

Aineiston perustella nähtiin, että kohdeyrityksen turvallisen ohjelmistotuotannon operatiivisesta työstä vastaavat yrityksen eri liiketoiminta-alueet, jotka tuottavat tietojärjestelmätuotteita, integraatioita, analytiikkaa ja muita asiakasratkaisuita. Turvallisen ohjelmistotuotannon prosessi oli kuvattu kohdeyrityksen laatujärjestelmässä ja sitä kehittää ja linjaa yrityksen Chief Technology Office (CTO Office), yhdessä sidosryhmiensä kanssa. Turvallisen ohjelmistotuotannon prosessi nähtiinkin yhtiön toimialasta johtuen vahvasti itsenäisenä osaamisalueena ja näin ollen se voitiin nähdä myös yhtenä keskeisenä kyberturvallisuuden ydinkompetenssialueena.

Järjestelmien tuotannon tietoturva-arkkitehtuuri voitiin nähdä olevan osana kohdeyrityksen laatujärjestelmän turvallisen ohjelmistotuotannon prosessia. Näin ollen myös tämä osa-alue oli keskeistä kyberturvallisuuden osaamista kohdeyrityksessä. Sama koski myös järjestelmien toiminallisia vaatimuksia, laadunvarmistusta ja testausta sekä järjestelmäkehitystä. Myös teknologioiden tutkimus ja tuotekehitys nähtiin olennaisena osana järjestelmien kehitystä kohdeyrityksen liiketoiminta-alueilla sekä sen keskitetyissä arkkitehtipalveluissa.

Kuten yllä olevasta voidaan havaita, koko turvallisen tuotannon kategoria nähtiin keskeisenä osaamisena kohdeyrityksen liiketoiminnassa. Haastattelumateriaalista nousi esiin kuitenkin myös haaste, joka liittyy tähän kokonaisuuteen. Haasteena nähtiin yhtenäisen ja kattavan tuotanto- ja turvallisuusprosessin kehittäminen ja noudattaminen. Korkealle tasolle jäävän prosessin todettiin olevan yleispätevä, mutta ei antavan riittävästi yksityiskohtaisia ohjeita ja hyötyjä päivittäiseen työskentelyyn. Aineistossa todettiin myös, että prosessin jäädessä irralleen päivittäisestä tekemisestä, sen kehittäminen päivittäisiä haasteita vastaavaksi muodostuu myös haastavaksi. Yksityiskohtaisemman prosessin kehittäminen nähtiin myös haastavana, yhtiön laajan toimialueen ja siihen liittyvien erityyppisten asiakasvaatimusten sekä käytettyjen erilaisten teknologioiden takia. Tällä hetkellä toimintaprosesseja on kuvattu laajalti yhtiön laatujärjestelmässä. Toimintamallien jatkokehityksessä tulisikin kiinnittää tähän tutkimusaineistosta esiin nousseeseen monialaisuuden haasteeseen erityistä huomiota.

4.1.2 Operointi ja ylläpito (Operate and Maintain)

Haastatteluaineiston perusteella ja luokitteluviittausten määrän perusteella, operointi ja ylläpito -kategoria nousi toiseksi keskeiseksi osaamisalueeksi kohdeyrityksen liiketoiminnan kyberosaamisessa. Kategorian ensimmäinen osa-alue Datan hallinta arvioitiin keskeiseksi toiminnaksi, jota johtaa yrityksen tietohallinto (CIO Office). Nykytilassaan toiminnan nähtiin olevan järjestelmävetoista, mutta siinä tunnistettiin myös tarve tarkastella osa-aluetta enemmän informaation näkökulmasta, ilman järjestelmäkytkentöjä. Tällä tarkastelulla uskottiin saavutettavan informaation luottamuksellisuuden, integriteetin ja saatavuuden näkökulmasta parempi tulos, kuin järjestelmäkeskeisellä lähestymisellä. Tämä näkökulma olisi hyvä huomioida kohdeyrityksen datan hallinnan erityisalueen mahdollisessa jatkokehityksessä.

Myös asiakaspalvelu ja tekninen tuki nousivat haastatteluaineistoissa keskeisen ydinkompetenssin rooliin. Tältä osin kohdeyrityksessä onkin tehty jo aiemmin asiakaspalvelun ulkoistuksen purku ja siirto omaan hallintaan. Tähän kehityskulkuun on aineiston mukaan johtanut oman tuotannon maturiteettitason kasvu sekä erityisvaatimukset, joita ulkoisen tuottajan on ollut hankala toteuttaa. Palvelutuotanto toimii siis jo nykyisellään myös kyberturvallisuuden kokonaisuuden osana, vaikka sillä on myös tekninen ja infrastruktuuria muiltakin osin palveleva funktio kohdeyrityksen omassa toiminnassa ja asiakasrajapinnassa.

Verkkoympäristön ylläpito, kehitys ja hallinta nähtiin myös keskeisenä osaamisalueena. Tätä pidettiin haastatteluaineistojen perusteella jopa osin poikkeuksellisena, mutta perusteltuna kohdeyrityksen tyyppisessä ympäristössä. Perusteltua tästä teki toimialueen yksityiskohtien määrä ja laajuus. Ulkoistamista verkkoympäristön hallinnan osalta oli aineiston mukaan harkittu, mutta sopivaa kumppania siihen ei ollut toistaiseksi löytynyt. Näin ollen toimintaa ja kompetenssia tämän osa-alueen osalta oli lisätty ja kehitetty. Tämä oli osaltaan vaikuttanut myös siihen, että oman järjestelmäympäristön kehityksen ja tietoturvan kompetenssi oli kasvanut ja myös ne osa-alueet nähtiin keskeisenä osaamisalueena. Toimintoja kuitenkin tarkastellaan kriittisesti ja tilanteen jatkuvan muutoksen luonteesta johtuen ulkoistuksen mahdollisuutta arvioidaan ajoittain.

Yhteenvetona operointi ja ylläpito osiosta voidaan aineistojen perusteella todeta, että toiminta kategorian alueella nähtiin tärkeänä, mutta ei kaikelta osin välttämättömänä yrityksen liiketoiminnan kannalta. Asiakaspalvelu ja verkkoympäristön ylläpito nähtiin näistä keskeisimpänä ja myös hankalimmin ulkoistettavana erityisalueina. Näiden erityisalueiden uskottiinkin näistä syistä pysyvän kyberosaamisen keskiössä myös jatkossa. Muilta osin panostusta kategoria-alueella tarkastellaan palveluntarjoajien maturiteetin ja oman ulkoistusvalmiuden parantuessa.

4.1.3 Suojaaminen ja puolustus (Protect and defend)

Suojaaminen ja puolustus kategorian voitiin aineiston perusteella sanoa olevan yritykselle tärkeä osa-alue sen turvallisen toiminnan takaamiseksi.

Liiketoiminnan kannalta sen ei kuitenkaan nähty välttämättä olevan yrityksen ydinkompetenssin alueella.

Haastattelumateriaalin perusteella voitiin arvioida, että kompetenssi tällä osa-alueella oli kuitenkin varsin kehittynyttä kohdeyrityksessä. Tämän arvioitiin tapahtuneen osittain operointi ja ylläpito kategoriassa olevan verkkoympäristön hallinnan kompetenssin kehittymisen myötä. Osa-alueiden kehityksessä voitiinkin tältä osin nähdä olevan myös kategorioiden välistä yhteistoimintaa: Verkonhallinnan kompetenssilla voi olla yhteys myös suojaaminen ja puolustus alueen kompetenssin kehittymiseen. Tutkimuslöydökset tukisivat tätä havaintoa.

Tutkimushavaintojen perusteella voitiin todeta, että kompetenssi kategorian alueella oli ollut riittävää nykyisten liiketoiminnan tarpeiden osalta. Kompetenssi oli aineiston perusteella muodostunut osin itsenäisestä ja yhteistoiminnallisesta kokonaisuudesta. Suojaaminen ja puolustus kategorian nähtiin olevan jatkossakin pääosin yhteistoiminnallisen mallin alueella. Näin siksi, että kyseessä ei ole varsinainen organisaation ydinliiketoimintaa välittömästi palveleva osa-alue.

4.1.4 Tutkinta (Investigate)

Tutkinta kategorian erityinen ja myös kohdeyrityksen liiketoiminnasta poikkeava luonne nousi esiin tutkimusaineistoissa. Kokonaisuus nähtiin erittäin vaativana niin henkilöstön kompetenssin kuin resursoinninkin näkökulmasta. Myös mahdolliset taloudelliset investoinnit kategorian vaatimusten mukaiseen kehitykseen nähtiin merkittävinä.

Kategoria todettiin kokonaisuutena kuitenkin tarpeelliseksi turvallisen toiminnan ja kyberongelmien selvittelyn näkökulmasta. Organisaation tarpeen tällä alueella todettiin painottuvan yhteistoiminnalliseen toimintamalliin. Yhteistoiminnallisen mallin uskottiin kuitenkin vaativan myös tietyn tasoista osaamista organisaatiolta itseltään, jotta yhteistoiminta olisi tehokasta. Tutkimusaineiston perusteella tämän osaamisvaatimuksen arvioitiin olevan tyypillistä myös muiden kategorioiden yhteistoiminnallisissa kokonaisuuksissa. Tämän arvioitiin tarkoittavan käytännössä sitä, että tutkinnan kategoria-alueella organisaatiolla tulisi olla riittävästi esimerkiksi forensiikkaan liittyviä kompetensseja, jotta yhteistoiminnallinen malli olisi mahdollinen. Kategorian osaamisalueen todettiin olleen nykytilanteessa pääosin yhteistoiminnallista. Sen arvioitiin pysyvän yhteistoiminnallisena myös jatkossa.

4.1.5 Kerääminen ja operointi (Collect, Operate)

Kerääminen ja operointi kategoriaa pidettiin tutkimusaineistojen valossa tärkeänä osa-alueena. Aineistossa nousi esiin erityisesti tietoturvatapahtumien keräämiseen liittyvän osaamisen painottuminen. Tämän erityisalueen tehtäviä oli nykyisellään tuotettu itsenäisesti ja siihen haluttiin panostaa enemmän myös jatkossa. Keräämiseen ja operointiin liittyvän toiminnan uskottiin olevan kasvusuunnassa alan toimijoiden keskuudessa yleisemminkin.

Aineiston perusteella oli nähtävissä myös, että tämän erityisalueen sisällä oli useita yksityiskohtia, jotka vaikuttivat siinä tarvittavaan kompetenssiin. Pääosin osaaminen oli alueella samaa, mutta esimerkiksi pilviratkaisujen nähtiin edellyttävän tietyn tyyppistä erityisosaamista siihen liittyvistä teknologioista johtuen. Tämä osaaminen nähtiin olevan hyvin erilaista, kuin perinteisemmän ohjelmistotuotannon ratkaisujen (Legacy) kanssa toimittaessa. Myös keräämisen sisältöihin ja analyysiin liittyvän kompetenssin arvioitiin vaihtelevan merkittävästi teknologioista tai ratkaisuista riippuen. Esimerkiksi pilvialustojen nähtiin tarjoavan valmiita ja pitkälle vietyjä työkaluja keräämisen ja analysoinnin käyttöön, kun taas perinteisemmän SIEM-ratkaisun (Security Incident and Event Management) operoinnin arvioitiin vaativan laajempaa osaamispohjaa niin käytetyn tuotteen, kuin palveluratkaisun teknisen toteutuksenkin suhteen. Tietoturvatapahtumien keräämisen erityisalueella nähtiin organisaation oman tarpeen ja siihen liittyvän tuotannon ohella myös uuden liiketoiminnan kehitysmahdollisuuksia.

Tietoturvatapahtumien keräämiseen nähtiin liittyvän olennaisena osana aina myös analysoinnin erityisalue, koska vain tapahtumien analyysilla datasta voidaan jalostaa tietoa päätöksentekoa varten. Tämän nähtiin olevan keskeistä myös mahdollisessa uudessa liiketoimintamallissa. Tällä osa-alueella nousi esiin myös muualla haastatteluaineistossa esiin noussut kysymys oman tuotannon maturiteettitasosta: Mitä pidemmällä oma kyvykkyys ja maturiteettitaso on, sitä mahdollisempana nähtiin, että siitä syntyy oman tarpeen täyttämisen ohella myös uutta liiketoimintaa. Tällä nähtiin olevan vaikutusta myös ulkoistamiseen ja sitä kautta organisaation kompetenssitarpeeseen. Mitä korkeampaa toiminnan maturiteettitason ja osaamisen arvioitiin olevan, sitä tehokkaampana nähtiin myös toiminta ja epätodennäköisempänä toiminnan ulkoistaminen.

4.1.6 Analysointi (Analyze)

Analysointi-kategoria nousi aineistossa esiin merkittävänä, mutta tällä hetkellä enemmän yhteistoiminnallisesti toteutettuna tehtäväkategoriana. Kategoriassa nähtiin aiemmin kuvattu yhteys kerääminen ja operointi kategorian tietoturvatapahtumien keräämisen kanssa. Sen osalta todettiin myös, että kategorian toimialueella olisi paljon kehitettävää. Haavoittuvuustiedon kerääminen ja kerätyn tiedon hyödyntäminen nähtiin myös keskeisenä yhtiön kyberturvallisuuden näkökulmasta.

Aineiston perusteella voitiin todeta, että kerääminen ja operointi sekä analysointi kategoriat tulisivat nousemaan keskeiseksi osaamisalueeksi, mikäli näihin panostettaisiin enemmän jatkossa. Tarvetta panostukselle nähtiin myös haavoittuvuustiedon keräämiseen ja kerätyn tiedon hyödyntämiseen liittyen. Uhkaanalyysit erityisalue nähtiin myös tärkeänä osaamisalueena.

Yhteenvetona kategoriasta voidaan todeta, että analysointi kategoria nähtiin kokonaisuudessaan keskeisenä ja tavoitteellisesti itsenäisen kompetenssin kokonaisuutena. Aineiston perusteella voitiin todeta, että kategoria oli keskeistä ydinkompetenssialuetta. Aineisto osoitti kuitenkin myös, että osaamista tässä

kategoriassa voidaan ostaa ulkopuolelta, jolloin kompetenssi olisi yhteistoiminnallista. Tällä hetkellä toiminnan nähtiin olevan yhteistoiminnallista, mutta sen tarpeen uskotaan kasvavan ja kompetenssin kääntyvän enemmän itsenäisen kompetenssin suuntaan.

4.1.7 Johtaminen ja kehittäminen (Oversee and govern)

Johtaminen ja kehittäminen-kategoria oli aineiston perusteella vahvasti kohdeyrityksen ydinosaamisen aluetta. Tämä oli nähtävissä mm. siitä, että lainopillisen neuvonnan erityisaluetta oli vahvistettu viime vuosina, Data Privacy Officerin (DPO) rekrytoinnilla yrityksen tietoturvayksikköön (CSO Office). Tällä oli lisätty Euroopan tietosuojalainsäädännön vaatimusten mukaisuutta yhtiön toiminnassa. Myös henkilöstön harjoitteluun, koulutukseen ja tietoisuuden lisäämiseen kyberturvallisuuden osa-alueilla oli panostettu. Kyberturvallisuuden toimialueella lisääntyneitä tehtäviä varten yhtiön tietoturvayksikön henkilömäärää oli myös lisätty sisäisten rekrytointien avulla.

Johtaminen ja kehittäminen-kategoriaan kuuluvaan harjoittelu, koulutus ja tietoisuuden lisääminen-erityisalueeseen oli myös panostettu viime vuosina lisäämällä oman koulutustuotannon määrää. Tähän erityisalueeseen arvioitiin panostettavan merkittävästi myös jatkossa. Turvallisuustietämyksen lisääminen olikin nostettu yhtiössä myös viralliseksi tavoitteeksi vuodelle 2020.

Turvallisuusohjelmien johtaminen oli myös keskeistä osaamista kohdeyrityksessä. Tällä osa-alueella oli kuitenkin haastatteluaineistojen perusteella nähtävissä vielä tarve kehittää toimintaa reaktiivisesta toimintamallista enemmän proaktiiviseen suuntaan. Riskienhallinta oli aineiston perusteella myös voimakkaassa kehitysvaiheessa. Siihen oli panostettu merkittävästi niin henkilöstön, kuin teknologioidenkin osalta ja tämän työn arvioitiin jatkuvan myös tulevaisuudessa.

4.2 Kohdeyrityksen kyberosaamisen tulevaisuuden tarpeet

Kuten aiemmasta aineiston analyysista voidaan päätellä, on kohdeyrityksen kyberturvallisuuden kompetenssitarve jakautunut laajasti lähes koko viitekehyksen kategoria-alueelle. Tämä päätelmä oli nähtävissä myös haastatteluaineistoissa. Niissä nousivat esiin vahvasti myös kompetensseihin liittyvät investoinnin ja kannattavuuden näkökulmat.

Kyberosaamisen kehittäminen ydinkompetenssiksi nähtiin aikaa vievänä ja kalliina prosessina. Sen kehittämistä arvioitaessa tulisi harkita tarkkaan mikä osaaminen olisi syytä hankkia itselle ja miltä osin osaamista kannattaisi ostaa palveluna. Tämä näkemys nousi selvästi esiin aineistoista. Toisaalta haastatteluaineistosta oli nähtävissä myös, että kyberturvallisuudessa on osa-alueita, jotka nähtiin vaikeasti ulkoistettavina niihin liittyvien yksityiskohtien tai toiminnan tehokkuuden kannalta.

Alla olevassa taulukossa on esitetty yhteenveto kategorioiden mukaisten erityisalueiden ja kompetenssien jakautumisesta tutkimuksen aineiston perusteella. Listassa olevat kompetenssi-/erityisalueet on jaoteltu myös sen perusteella, kuuluvatko ne aineiston analyysin perusteella itsenäisen / ydinkompetenssin, yhteistoiminnallisen tai normatiivisen toiminnan malliin.

Taulukko 3 Yhteenveto tutkimuksen kohdeyrityksen kyberturvallisuuden kompetensseista ja niiden jakautumisesta kategorioihin ja toimintamalleihin

Kategoria	**Itsenäinen / ydinkompetenssi**	**Yhteistoiminnallinen**	**Normatiivinen**
Turvallinen tuotanto (securely provision)	Turvallisen tuotannon nähtiin säilyvän ydinosaamisalueena. Yhtenäisen tietoturvaprosessin jatkokehittämisen ja siihen liittyvän osaamisen lisäämisen arvioitiin olevan keskeistä myös tulevaisuudessa.		
Operointi ja ylläpito (Operate and maintain)	Operointi ja ylläpito nähtiin asiakaspalvelun ja verkkoympäristön ylläpidon osalta keskeisenä osaamisalueena. Sen arvioitiin myös säilyvän sellaisena vielä todennäköisesti pitkään. Tällä kompetenssin osa-alueella nähtiin tarvetta ylläpidolle ja kehittämiselle.	Operoinnin ja ylläpidon yhteistoiminnallisen osan arvioitiin kasvavan jatkossa. Esimerkiksi järjestelmäympäristön painotuksen siirtyessä enemmän pilviratkaisujen käyttöön, oman järjestelmäympäristön osaamisen vaatimusten arvioitiin muuttuvan. Saman muutoksen arvioitiin koskevan myös järjestelmäympäristön tietoturvan kompetenssia.	
Suojaaminen ja puolustus (Protect and defend)		Suojaaminen ja puolustus kategoria nähtiin tärkeänä osa-alueena, mutta sen luonteen nähtiin olevan pääosin yhteistoiminnallista. Omaa investointia kompetenssin kehittämiseen tällä osa-alueella ei nähty järkevänä.	

(jatkuu)

Taulukko 3 (jatkuu)

Tutkinta (Investigate)		Tutkinta-kategoria nähtiin vaativana ja merkittäviä investointeja vaativana osa-alueena. Sen luonne oli ollut tähän mennessä yhteistoiminnallinen ja sellaisena sen uskotiinn pysyvän myös jatkossa.	
Kerääminen ja operointi (Collect and operate)	Kategoria nähtiin tärkeänä osaamisalueena ja alueella nähtiin myös potentiaalisia liiketoiminnan kehittämismahdollisuuksia. Kategoria nousi tärkeäksi etenkin hybridimallisessa toimintaympäristössä, jossa legacy-järjestelmät ja pilviratkaisut muodostavat liiketoimintaympäristön kokonaisuuden.	Transformaatio liiketoiminnan toimintaympäristön legacy-järjestelmistä kohti pilviratkaisuja, saattaa muuttaa tämän osa-alueen osaamisvaatimusten sisältöä enemmän yhteistoiminnalliseen suuntaan. Peruskompetenssia keräämisen ja operoinnin osalta arvioitiin tarvittavan kuitenkin myös tässä toimintamallissa.	
Analysointi (Analyze)	Analysointi-kategoriassa nousi esiin selvästi tiedon analysointi erityisesti tietoturva-tapahtumien keräämiseen ja uhka-analyysiin liittyen. Toiminta oli tällä hetkellä ollut yhteistoiminnallista, mutta tähän osaamisalueeseen olisi tarkoitus panostaa jatkossa enemmän.		

(jatkuu)

Taulukko 3 (jatkuu)

Johtaminen ja kehittäminen (Oversee and govern)	Johtamisen ja kehittämisen kategoria nähtiin selvänä ydinosaamisalueena. Tälle alueelle oli viime aikoina panostettu ja panostusten uskottiin jatkuvan myös tulevaisuudessa. Kategoria nähtiin ydinosaamisalueena, joka tukee myös muita viitekehyksen kategorioita ja mahdollistaa niiden toiminnan ja kehittymisen.		

Normatiivinen toimintamalli ei näy yllä olevassa yhteenvedossa eriteltynä, mutta se nousi esiin haastatteluaineistoissa. Sen nähtiin yleisesti ilmentyvän regulaation, lakien ja asetusten muodossa, joita kohdeyritykseen ja sen toimintaan kohdistuu. Näitä vaateita nähtiin tulevan niin tietosuojalainsäädännöstä, kohdeyrityksen toimiessa rekisterinpitäjänä tai -käsittelijänä, kuin myös asiakasvaateina ja yleisen lainsäädännön vaateina.

Normatiivisen toimintamallin nähtiin korostuvan erityisesti julkisen puolen asiakashankkeissa, joissa erilaiset vahvat sääntelyt asettivat vaateita kohdeyritykselle järjestelmätoimittajana. Tästä syystä esimerkiksi toimitilaturvallisuus oli yleisesti kohdeyrityksessä korkeaa tasoa. Erityisiin korkean turvallisuuden tiloihin ja niiden kehitykseen oli myös panostettu merkittävästi viimevuosina. Kohdeyrityksen yleistä ohjelmistotuotannon prosessia oli myös kehitetty vastaamaan näitä korkeita turvallisuusvaatimuksia. Erilaisten normatiivisten vaateiden nähtiinkin kattavan yhtiön toimintaa niin laajalla alueella ja poikkileikkaavasti koko viitekehyksen alueella, että niitä ei tästä syystä eritelty viitekehyksen kategorioihin, vaan normatiivisen mallin vaateiden nähtiin pätevän tässä tapauksessa kaikissa kategorioissa.

4.3 Tulosten vertailu aikaisempaan tutkimukseen

Samaa viitekehystä ja tutkimusasetelmaa käyttäneessä Willbergin (2017) tutkimuksessa kohdeorganisaatioina olivat Poliisin Kyberrikostorjuntakeskus ja Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK). Molempien aiemmin tutkittujen organisaatioiden toimiala oli suurelta osin poikkeava nyt tutkitun kohdeorganisaation toimialan kanssa. Toimialojen erilaisuudesta huolimatta oli organisaatioiden toiminnoissa kuitenkin löydettävissä yhtäläisyyksiä. Erityisesti yhtäläisyyksiä nyt tutkitun kanssa havaittiin Puolustusvoimien Johtamisjärjestelmäkeskuksen toiminnassa. Poliisin Kyberrikostorjuntakeskuksen toiminta voitiin nähdä myös osittain saman tyyppisenä, kuin kaksi edellä mainittua. Poliisitoiminnan painotuksen ollessa kuitenkin vahvasti rikostorjunnassa ja -tutkinnassa,

nousivat sen toimialueen erityisvaatimukset vahvasti esiin aiemman tutkimuksen tuloksissa. Tämä aiheutti eroa myös nyt tutkitun toimialan ja Poliisitoiminnan välillä. Alla olevassa taulukossa on esitetty yhteenveto ydinkompetenssien vertailuista aiemmin tutkittujen ja nyt tutkitun organisaation välillä. (Taulukko 4).

Taulukko 4 Ydinkompetenssien vertailu aiempaan tutkimukseen (Willberg, 2017)

Kategoria	**Yritys X / Tämä tutkimus**	**PVJJK Willberg (2017)**	**Kyberrikostorjuntakeskus Willberg (2017)**
Turvallinen tuotanto (Securely provision)	X	X	
Operointi ja ylläpito (Operate and Maintain)	X	X	
Suojaaminen ja puolustus (Protect and defend)		X	
Tutkinta (Investigate)			X
Kerääminen ja operointi (Collect, Operate)	X		X
Analysointi (Analyze)	X		
Johtaminen ja kehittäminen (Oversee and govern)	X	X	X

Päähavainto yhtäläisyyksistä tutkimusten välillä liittyi kybertoiminnan yleiseen laajuuteen ja kompetenssialueiden laajaan hajautumiseen viitekehyksen eri osa-alueille. Hajautumista oli voimakkaimmin tämän tutkimuksen kohdeyrityksen osaamisalueella ja seuraavaksi voimakkaimmin Puolustusvoimien Johtamisjärjestelmäkeskuksen toiminnassa. Kompetenssien jakautumisessa oli nähtävissä myös yhtäläisyyksiä tämän tutkimuksen kohdeyrityksen ja Puolustusvoimien Johtamisjärjestelmäkeskuksen välillä, erityisesti turvallisen tuotannon ja operoinnin ja ylläpidon osa-alueilla.

Toinen merkittävä havainto yhtäläisyydestä oli toiminnan jakautuminen ydinkompetenssin ja yhteistoiminnallisen mallin välillä. Puolustusvoimissa yhteistoiminta painottui oman laajan resurssin käyttöön, mutta tämän tutkimuksen kohdeyrityksessä painotus oli yhteistyökumppaneiden ja alihankkijoiden käytössä. Tätä selittivät osaltaan myös Puolustusvoimien erityisvaatimukset toiminnan turvaamiseen ja tietojen salaamiseen liittyen. Tästä syystä voitiin arvioida, että ulkopuolisten alihankkijoiden käyttö tietyissä toiminnoissa oli vähäisempää. Vähäistä ulkoistusta tuki mahdollisesti myös Puolustusvoimien oman resurssin laajuus, jolloin alihankintaa voitiin tehdä myös oman organisaation sisällä.

Yhteenvetona aiemman tutkimuksen tuloksista voidaan todeta, että sen tutkimuskohteiden erityisluonteesta johtuen siinä painottuivat kyberrikosten tutkimus ja kyberpuolustuksen osaamisrakenteet. Nyt tutkitun kohdeyrityksen osaamisalue näyttäytyi edellisistä poiketen laajempana ja monimuotoisempana. Tästä samasta syystä myös kyberturvallisuuden osaamisen monimuotoisuuden haaste korostui kohdeyrityksessä. Lisähaasteen toi myös monialainen toimiala sekä liiketoiminnan tuotto-odotukset ja niiden vastapuolella olevat investointitarpeet kybertuvallisuuden toimintoihin. Erityisen haastavana kompetenssien hallinta ja kehittäminen nähtiin kaupallisen toimijan osalta siinä tapauksessa, että kyberturvallisuuden tuottamiseen liittyvä toiminta ei ole läheisessä korrelaatiossa organisaation ydintekemisen tai -liiketoiminnan kanssa tai se ei ole sitä välittömästi palvelevaa. Organisaation liiketoiminnallinen ydinkompetenssi ei siis välttämättä ole sama, kuin kyberturvallisuuden ydinkompetenssi. Näin kyberturvallisuuden ydinkompetenssi nähdään investointina ja vain välillisesti liiketoimintaa palvelevana kokonaisuutena, kun se aiemmassa tutkimuksessa saatettiin nähdä organisaation lisäarvon tuottamiseen liittyvänä ydinkompetenssina tai tuotannontekijänä.

5 JOHTOPÄÄTÖKSET

Tässä luvussa kuvataan tutkimuksen tuloksista tehdyt johtopäätökset kohdeyrityksen kyberturvallisuuden ydinkompetensseihin liittyen. Lisäksi kuvataan tutkimusaineistosta esiin nousseet kohdeyrityksen kyberkompetenssiin liittyvät tulevaisuuden kehitystarpeet.

5.1 Kohdeyrityksen kyberosaamisen ydinkompetenssi

Tutkimuksen tulokset osoittivat, että kohdeyrityksen kyberturvallisuuden osaamisen jakautuminen viitekehyksen luokittelun mukaisesti oli varsin laajaa. Tuloksien jakauman kappalemääristä (Taulukko 2) on kuitenkin nähtävissä myös osaamisalueiden keskittymistä. Näissä keskittymissä sijaitsevat havaintojen mukaan myös kohdetyrityksen ydinkompetenssit. Ydinkompetenssien analyysin perusteella oli nähtävissä myös osaamisen painottuminen yrityksen liiketoimintaan liittyvään osaamiseen: ohjelmistokehitykseen ja siihen liittyvän turvallisen tuotannon vaatimuksiin.

Ohjelmistojen tuotannon lisäksi kohdeyrityksen keskeistä ydinosaamista olivat sen omaan tietojärjestelmäympäristöön ja verkkoratkaisuihin sekä asiakaspalveluun liittyvät kyberturvallisuuden kompetenssit. Myös kyberturvallisuuden johtaminen, henkilöstön osaamisen ja tietoisuuden lisääminen kyberturvallisuuteen liittyen olivat kohdeyrityksen kyberturvallisuusosaamisen keskeisiä elementtejä. Näihin asioihin yrityksessä olikin panostettu merkittävästi viime vuosina.

Tutkimustuloksista oli nähtävissä myös kompetenssien laajan jakautumisen aiheuttama haaste kompetenssien hallinnalle sekä myös laajaan jakaumaan liittyvä haaste riittävälle investointitasolle, kompetenssien ylläpitämiseen ja kehittämiseen liittyen. Nämä haasteet oli kohdeyrityksessä tunnistettu ja panostuksia kyberturvallisuuden kompetenssien osa-alueisiin ja niiden kehittämiseen oli tehty. Kyberkompetenssien kehitystyö ja siihen liittyvät investoinnit nähtiin tärkeänä myös tulevaisuudessa. Tämän tutkimuksen tulosten arvioitiin toimivan hyvänä lähtökohtana ja suunnannäyttäjänä tässä kehitystyössä.

Varsinaisten kyberturvallisuuteen liittyvien toimintojen kehittämisen ohella tämän tutkimuksen tulokset voivat antaa työkaluja myös yrityksen henkilöstöhallinnon käyttöön, jossa arvioitiin jatkettavan jo aiemmin aloitettua henkilöstön osaamisprofiilien kartoitusta ja siihen liittyvää kehitystyötä.

Yhteenvetona tutkimushavainnoista voidaan todeta, että kyberturvallisuuden ja siihen liittyvien toimintojen nähtiin olevan kiinteä osa kohdeorganisaation toimintaympäristöä, liiketoimintaa ja ohjelmistojen kehittämiseen liittyvää työtä. Tästä syystä tätä toimintaa ja sen kompetenssien kehittämistä tai siihen liittyviä investointeja ei tulisi nähdä erillisenä saarekkeena, vaan tuotantoon kiinteästi integroituvana ja liiketoiminnallista lisäarvoa tuovana kokonaisuutena. Kyberturvallisuuden kompetensseja ja niihin liittyviä prosesseja tulisikin siksi kehittää samalla, kun kehitetään organisaation muita tuotantokyvykkyyksiä ja prosesseja.

Tutkimuksen tuloksista oli nähtävissä kohdeyrityksen kyberturvallisuuteen liittyvät ydinkompetenssit ja niiden jakautuminen viitekehyksen alueelle. Tämän lisäksi ydinkompetenssien maturiteettitaso jaoteltiin vielä vakiintuneeseen ja kehittyvään kompetenssin alueeseen. Luokittelu tehtiin haastatteluaineistoista esiin nousseiden tietojen perusteella. Luokittelu on kuvattu alla olevassa taulukossa (Taulukko 5). Taulukko muodostaa myös kohdeyrityksen ydinkompetenssiesityksen.

Vakiintuneella tarkoitetaan tässä esityksessä ydinosaamisalueita, jotka ovat vakiintuneet kohdeyrityksen toiminnassa. Kehittyvillä puolestaan tarkoitetaan kompetensseja, jotka ovat vasta kehityskaarensa alkuvaiheessa tai vasta suunnitteilla. Ydinosaamisalueiden maturiteettitason jaottelu noudattelee myös Willbergin (2017) tutkimuksessaan käyttämää jaotteluperiaatetta ja tarjoaa näin mahdollisuuden vertailla tämän tutkimuksen löydöksiä edellisen tutkimuksen löydöksiin myös tältä osin.

Taulukko 5 Kohdeyrityksen ydinkompetenssit

Kategoria	**Vakiintunut**	**Kehittyvä**
Turvallinen tuotanto (Securely provision)	• Alihankintaketjun hallinta • Turvallinen ohjelmistotuotanto • Järjestelmien toiminnalliset vaatimukset	• Järjestelmien tuotannon tietoturva-arkkitehtuurit. • Teknologioiden tutkimus ja -kehitys • Laadunvarmistus ja testaus
Operointi ja ylläpito (Operate and Maintain)	• Asiakaspalvelu ja tekninen tuki • Verkkoympäristön ylläpito • Järjestelmäympäristön kehitys, ylläpito ja hallinta	• Datan hallinta • Järjestelmäympäristön tietoturva
Kerääminen ja operointi (Collect, Operate)		• Tietoturva-tapahtumien kerääminen • Kyber-operaatiot
Analysointi (Analyze)		• Uhkainformaation kerääminen • Pen-testing, haavoittuvuustiedon kerääminen
Johtaminen ja kehittäminen (Oversee and govern)	• Lainopillinen neuvonta ja juristipalvelut • Strateginen tietoturvan suunnittelu ja turvallisuuspolitiikan kehitys	• Harjoittelu, koulutus ja tietoisuuden lisääminen • Turvallisuusohjelmien johtaminen • Riskien hallinta • Turvallisuustietämyksen hallinta

5.2 Kohdeyrityksen kyberosaamisen tulevaisuuden tarpeet

Kohdeyrityksessä oli investoitu kyberturvallisuuden kehittämiseen lisäämällä kyberturvallisuuteen keskittyvän yksikön (CSO Office) henkilömäärää ja laajentamalla sen toimintoja sekä luomalla ja kehittämällä kokonaisturvallisuutta ohjaavia prosesseja ja ohjeistusta. Koko organisaation henkilöstön kyberturvallisuuden osaamiseen liittyviä panostuksia oli myös tehty viime vuosina. Tätä työtä on syytä jatkaa myös tulevaisuudessa. Tämän tutkimuksen tulosten uskotaan antavat lähtökohtia ja tietoa tähän työhön.

Paitsi ydinkompetenssit, yllä olevasta taulukosta (Taulukko 5) on nähtävissä myös ydinkompetenssin erityisalueisiin liittyvät kehittyvät kohteet. Niiden osalta kehitystyötä olisi mahdollista jatkaa tämän tutkimuksen tulosten ja NCWF-viitekehyksessä erityisalueille määriteltyjen tehtävien, taitojen ja osaamisvaatimusten lisämäärittelyiden avulla. Jatkokehitystyön yhteydessä olisi hyvä tarkastella myös kulloisenkin erityisalueen ja tehtävän mahdollista yhteistoiminnallista luonnetta. Tarkastelu tulisi suhteuttaa myös yrityksen liiketoimintaan ja sitä kautta investointihalukkuuteen kyseisellä alueella. Myös normatiiviset vaatimukset tulisi ottaa huomioon aihealueiden tarkastelussa. Näin muodostettaisiin kokonaisnäkemys organisaation kyberturvallisuuden toimintojen jatkokehityksestä, jossa investoinnit kanavoitaisiin ydinkompetenssien kannalta merkittävimpiin kokonaisuuksiin. Tämän työn myötä kyberturvallisuuden kompetenssit paitsi turvaisivat yrityksen toimintaa ja sen jatkuvuutta, muodostaisivat ne myös merkittäviä tuotannontekijöitä ja toimisivat kilpailuedun luojina.

6 POHDINTA

Tässä tutkimuksessa selvitettiin Yritys X:n kyberturvallisuuden ydinkompetensseja ja niihin mahdollisesti liittyviä tulevaisuuden tarpeita. Työssä käytettiin amerikkalaista kyberturvallisuuden kompetensseja kuvaavaa ja luokittelevaa NCWF-viitekehystä. Tutkimuksen tutkimusasetelma perustui ja sen tuloksia myös vertailtiin aiemmin Jyväskylän yliopistossa tehtyyn tutkimukseen (Willberg, 2017). Tämän vertailun avulla haluttiin laajentaa yleistä kyberturvallisuuden osaamiseen liittyvää tietoa ja ymmärrystä, erilaisten organisaatioiden osalta sekä testata aiemmin kehitettyä tutkimusasetelmaa.

Tutkimuksen kirjallisuuskatsauksessa taustoitettiin tutkimuksen aihealuetta ja tutustuttiin tutkimuksessa käytetyn viitekehyksen lisäksi myös kohdeyrityksessä käytössä oleviin ja muihin yleisesti tunnettuihin kyberturvallisuuden hallintamalleihin, standardeihin ja kompetenssien viitekehyksiin.

Tutkimushaastatteluista saadun aineiston perusteella pystyttiin havaitsemaan kohdeyrityksen merkittävimmät kyberturvallisuuden osaamisalueet ja niihin liittyvät yksityiskohdat. Havaintojen perusteella muodostettiin kohdeyrityksen ydinkompetenssiesitys (Taulukko 5). Tutkimusaineistossa nousi esiin myös tulevaisuuden kehitystarpeita, jotka myös raportoitiin tässä tutkimusraportissa.

Tutkimuksessa käytetty tutkimusasetelma todettiin toimivaksi tässä tutkimuksessa, koska sen avulla saatiin selvitettyä tutkimuskysymykset. Näin ollen voidaan myös todeta, että tutkimusasetelman testaaminen onnistui ja tutkimusasetelman voidaan todeta soveltuvan tämän tyyppiseen tutkimukseen. Tästä tiedosta voi olla hyötyä myös tästä tutkimuksesta mahdollisesti kumpuavassa jatkotutkimuksessa.

Nyt tehdyssä tutkimuksessa nousi esiin myös havaintoja, jotka tutkimuksen aiheen rajauksen perusteella jätettiin varsinaisen tutkimuksen ulkopuolelle. Aiheita on kuitenkin kuvattu lyhyesti tässä luvussa, koska niiden arvo kohdeyrityksen sisällä on merkittävä. Havainnot toimivat omalta osaltaan myös jatkotutkimusten tietopankkina, mikä myös puoltaa niiden kirjaamista raporttiin.

6.1 Kyberturvallisuuden monisäikeinen kokonaisuus

Tutkimuksen aineistossa nousi keskeisenä havaintona esiin kyberturvallisuuden monisäikeinen kokonaisuus ja siihen liittyvät kompetenssienhallinnalliset ja liiketoiminalliset haasteet. Tämä näkyi myös kohdeyrityksen kyberturvallisuuden kompetenssien jakautumisena laajasti viitekehyksen alueelle. Havainto oli saman suuntainen myös aiemmassa tutkimuksessa. Myös tutkimuskirjallisuus tukee tätä havaintoa. Kyberturvallisuuden voidaankin todeta olevan monipuolinen kokonaisuus, joka perinteisen teknisen näkökulman lisäksi kattaa myös useita muita osaamisalueita (Shoemaker, D., Kohnke, A., Sigler, 2016, ss. 3–16).

Monipuolisten ja monialaisten vaatimusten ja jatkuvan toimintaympäristön muutoksen johdosta kyberturvallisuus ja sen kompetenssien hallinta on haastava kokonaisuus kohdeorganisaation lisäksi organisaatioille yleisemmälläkin tasolla.

Kyberturvallisuuden eri osa-alueiden osaamisen kehitys ja ylläpito vaativat merkittäviä taloudellisia investointeja, jotka eivät välttämättä aina ole yhtäläisiä organisaation tehtävän ja liiketoiminnan tarpeiden kanssa. Turvallisuus voidaan tästä syystä nähdä asiana, joka jää tai jätetään liian vähälle huomiolle. Monipuoliseen kokonaisuuteen liittyvänä ja kompetenssien kehittämistä vaikeuttavana tekijänä nähdään myös kyberturvallisuusalan koulutuksen haasteet. Alan koulutuksella on suuri haaste tarjota organisaatioille riittävän osaavaa työvoimaa. Tähän liittyvät myös Niemelän (2019) tutkimuksessaan tekemät havainnot. Niemelä toteaa korkean työvoiman kysynnän ja vähäisen osaavan työvoiman tarjonnan aiheuttavan haasteita organisaatioiden kyberturvallisuuden hallinnalle ja kehittämiselle (Niemelä, 2019).

6.2 Kompetenssin kehittämisen työkalut

Edellä mainittujen haasteiden lisäksi tutkimustuloksista oli nähtävissä, että kyberturvallisuuden kompetenssien kehittämiseen ja hallintaan soveltuvia työkaluja, kuten tässä tutkimuksessa käytetty viitekehys, ei kohdeorganisaatioissa ole otettu laajamittaiseen käyttöön. Yleisesti käytössä olevat työkalut, viitekehykset ja standardit ovat keskittyneet organisaation kyberturvallisuuden hallintamalleihin, turvallisuuden järjestelmiin, regulaatioon tai teknologiaan. NCWF-viitekehys onkin piristävä poikkeus tässä työkaluvalikoimassa. Sen hyödyntämistä kyberturvallisuuden kompetenssien hallinnassa ja kehittämisessä olisi hyödyllistä pohtia niin kohdeyrityksessä, kuin toimialalla yleisemminkin.

Kyberturvallisuuteen olisi hyvä suhtautua pelkän yksipuolisen teknisen tai hallintajärjestelmälähestymistavan sijasta holistisemmin. Tämä voisi toteutua esimerkiksi huomioimalla paremmin kyberturvallisuuden kehityksessä myös henkilöresurssit ja niihin liittyvät kompetenssit sekä kompetenssien kehitystarpeet. Teknologisen näkökulman yhdistäminen resurssien ja kompetenssien hallinnan näkökulmaan voisi tarjota hyvän pohjan myös turvallisuuden hallintajärjestelmien kehittämiselle ja teknologioiden omaksumiselle.

Tutkimuskirjallisuuden ja tämän tutkimuksen tulosten valossa voidaan todeta, että yksiselitteinen kyberturvallisuuden kompetenssien jäsentäminen viitekehyksen avulla voi auttaa organisaatioita hahmottamaan kyberturvallisuuteen liittyviä tarpeita ja niihin olennaisesti liittyviä kompetensseja. Tämä puolestaan voi auttaa organisaatioita luomaan selkeän tilannekuvan ja kehityspolun kyberturvallisuuden parantamiseen ja siihen liittyvien kompetenssien kehittämiseen. Tämä kaikki yhdessä voi parantaa yrityksen turvallisen toiminnan lisäksi myös sen kilpailukykyä ja luotettavuutta. Näin menetellen kyberturvallisuuden kompetenssit voivat kehittyä kuluerän sijasta yrityksen keskeisiksi tuotannontekijöiksi ja tukea yritystä liiketoiminnan kehittämisessä.

6.3 Tutkimusalueen ulkopuoliset löydökset ja havainnot

Tutkimusaineistosta nousi esiin myös useita tämän tutkimuksen rajauksen takia sen ulkopuolelle jääviä havaintoja. Näiden havaintojen voidaan nähdä kuitenkin palvelevan tämän tutkimuksen jälkeen mahdollisesti tehtäviä kehityshankkeita niin kohdeyrityksen sisällä, kuin mahdollisia akateemisia jatkotutkimuksiakin. Tästä syystä näitä havaintoja on kirjattu tässä kappaleessa.

6.3.1 Henkilöstön osaamisprofiilien kehitys ja NCWF kohdeyrityksessä

Kohdeyrityksessä tehty henkilöstön osaamisprofiilien kehityshanke nähtiin hyvin tähän tutkimukseen liittyvänä kokonaisuutena. Tämän tutkimuksen lopputulosten uskottiin palvelevan sitä hanketta. Tästä aihealueesta olisi hyödyllistä järjestää yhteinen läpikäynti kohdeyrityksen henkilöstöosaston ja CSO Officen kanssa.

6.3.2 ISO 27001 -standardin implementointi

Yhtenä keskeisenä havaintona oli myös ISO 27001-standardin implementoinnin tarve kohdeyrityksessä. Standardi nähtiin paitsi kattavana turvallisuusjärjestelmän kehyksenä, myös yrityksen liiketoimintaa yleisemmin edistävänä kokonaisuutena. Investointihalukkuus sen implementointihanketta kohtaan arvioitiin myös suureksi. Aineistossa nousi esiin myös, että standardia ei nähty kaiken kattavana ratkaisuna yrityksen kyberturvallisuuden ja sen kompetenssien kehittämisessä. Sen arvioitiin kuitenkin muodostavan hyvin liiketoimintaa palvelevan kokonaisuuden yhdessä tässä tutkimuksessa käytetyn viitekehyksen kanssa.

6.3.3 Kohdeyrityksen laatujärjestelmään liittyvä kehitys

Aineistossa nousi esiin myös yrityksen laatujärjestelmään liittyvän keskustelun yhteydessä monialaisen ohjelmistoyrityksen kattavien prosessien kehittämisen haaste: Yksityiskohtainen prosessi auttaa jokapäiväisessä työn teossa, mutta ei sovellu kuitenkaan hyvin toisistaan eriävien liiketoimintamallien työkaluksi. Toisaalta korkealle tasolle jäävä yleinen prosessi ei palvele päivittäisen liiketoiminnan haasteista nousevia yksilöllisiä ja yksityiskohtaisia tarpeita. Laatujärjestelmän ja prosessien kehittämisen haaste onkin siis kehittää riittävän yksityiskohtainen ja yhtä aikaa riittävän yleistasoinen prosessi yrityksen eri osa-alueille. Tämä on merkityksellistä myös kyberturvallisuuden näkökulmasta, koska toistettavuus ja selkeät mallit luovat standardoidun lopputuloksen. Tällaisessa standardissa tuotantomallissa myös tietoturva ja tietosuoja on hyvin hallittavissa.

6.3.4 Kyberturvallisuus menestystekijänä

Asiakaslähtöisyys ja sen merkityksen määrittely nousi myös esiin haastatteluaineistoissa. Aineistoissa todettiin, että asiakaslähtöisyys nähdään usein asiakkaan toiveiden täyttämisenä, mutta asiakkaan ohjauksessa. Vaihtoehtoisena näkökulmana tähän nousi esiin asiakkaan toiveiden ymmärtäminen etukäteen ja niiden täyttäminen tuotteistetuilla, valmiilla ratkaisuilla.

Asiakastyöhön perustuvissa liiketoimintamalleissa tällainen etukäteisinvestointi nähdään usein kuitenkin haastavana. Samassa liiketoimintamallissa tämä haaste pätee usein myös välillisesti liiketoimintaa palveleviin toimintoihin, kuten kyberturvallisuuteen. Näihin liittyvä investointihalukkuus ei välttämättä ole korrelaatiossa tarvittavan panostuksen kanssa ja tarvittavia investointeja ei olla aina valmiita tekemän. Tähän liittyen myös kyberriskin arvioiminen nähdään myös haastavana.

Kohdeyrityksessä tilanne on tämän osalta kuitenkin hyvä ja investointeja kyberturvallisuuden kokonaisuuden hallintaan on tehty. Aihe on kuitenkin myös jatkuvan kehittämisen kohteena ja toimintaa pyritään myös tältä osin optimoimaan. Riskien hallinnan mallien, kuten ROSI (return of security investment) mallin kehittäminen onkin nähty tulevaisuuden kyberturvallisuuden tiekartalla merkittävänä kehityskohteena. Samaa kyberturvallisuuden investoinnin takaisinmaksun ongelmaa ja siihen liittyviä laskentamalleja on pohdittu myös Sonnereich ym. artikkelissa vuonna 2005. Tutkimusartikkelissa esitellään muutamia erilaisia laskentamalleja investoinnin takaisinmaksun arviointiin (Sonnenreich ym., 2005). Tämän tutkimuksen tuloksista voisi olla apua myös kohdeyrityksen tavoitteiden mukaisen jatkokehityksen suunnittelussa ja toteuttamisessa.

6.4 Tutkimuksen luotettavuus

Tieteellisen tutkimuksen validiteetin ja reliabiliteetin arviointi on keskeinen osa tutkimusta ja sen tulosten raportointia. Kvalitatiivisen tutkimuksen osalta tulosten reliabiliteetin ja validiteetin arviointi saattaa kuitenkin olla epämääräisempää tai hankalammin toteutettavissa, kuin kvantitatiivisissa tutkimusasetelmissa (Saranen-Kauppinen & Puusniekka, 2006). Tästä haasteesta huolimatta arviointia olisi hyvä tehdä myös kvalitatiivisen tutkimuksen yhteydessä, mutta on selvää, että sitä ei voida tehdä samoin ja samalla tarkkuustasolla, kuin kvantitatiivisia tutkimuksia arvioitaessa.

Kuten tässä raportissa on aiemmin todettu, nyt tehty tutkimus toteutettiin laadullisena tapaustutkimuksena, jossa aineiston keruumenetelmänä käytettiin teemahaastatteluita ja analysointimenetelmänä teorialähtöistä sisällön analyysiä. Tutkimuksen teoreettisena viitekehyksenä käytettiin amerikkalaista NCWF-viitekehystä. Käytetty tutkimusmenetelmä ja teoreettinen viitekehys valikoituivat käytettäviksi menetelmiksi koska niiden avulla arvioitiin löydettävän vastaukset tutkimuskysymyksiin ja toisaalta siksi, että tutkimus toisti aiemman tutkimuksen tutkimusasetelman ja pyrki tapaustutkimuksen tutkimuskysymysten selvittämisen ohella myös tutkimustulosten yhteismitallisuuteen ja vertailtavuuteen

aiemman tutkimuksen kanssa. Toisenlaisen viitekehyksen, esimerkiksi tässäkin raportissa esitellyn IISP Skills-kompetenssiviitekehyksen (The Institute of Information Security, 2019) käyttäminen muutoin samassa tutkimusasetelmassa olisi saattanut tuottaa erilaisia havaintoja samasta aiheesta. Käytetty viitekehys ei kuitenkaan yksinomaan ohjaa tutkimushavaintojen tekoa, vaan siihen vaikuttavat myös muut tekijät, kuten tutkijan oma näkemys ja kokemus aihealueesta sekä tutkimukseen valitut informantit. Tätä taustaa vasten sekä nyt tehdyn, että aiemman tutkimuksen tulosten vertailun perusteella, tutkimuksessa käytettyä teoreettista viitekehystä voidaan pitää melko hyvänä ja tämän tyyppiseen tutkimukseen soveltuvana viitekehyksenä.

Tutkijan pitkän (yli 20v) ohjelmistoalan työkokemuksen sekä kohdeyrityksen ja sen toimialan hyvän tuntemuksen arvioitiin jonkin verran vaikuttavan tutkimusaineiston analyysin tekemiseen, mutta ei haittaavan kuitenkaan tutkimuksen objektiivisuutta. Asetelman arvioitiin ennemminkin varmistavan tutkimuksen aineistonkeruun ja sen analyysin luotettavuutta ja sitä kautta tutkimuksen kokonaisvaliditeettia ja reliabiliteettia. Arvioinnissa otettiin huomioon kuitenkin myös, että esitetyt seikat voivat jossain määrin olla asioita, jotka vaikuttavat aineiston analyysin tekemiseen. Tämä on syytä huomioida tutkimuksen tuloksia arvioitaessa. Myös Tuomi ja Sarajärvi toteavat tämän ”puhtaiden havaintojen” haasteen kirjassaan ”Laadullinen tutkimus ja sisällön analyysi” (Tuomi & Sarajärvi, 2018, s. 166).

Teemahaastatteluiden haastateltavien (informanttien) valinta perustui tutkijan näkemykseen haastateltavien osaamisalueista ja tehtävänkuvista aiheeseen liittyen. Informanttien osaamisen ja haastattelujen määrän arvioitiin olevan riittäviä tutkimuskysymysten selvittämiseksi. Teemahaastatteluiden lisäksi tutkimuksen aikana pohdittiin myös muita informaation hankkimiskeinoja. Suunnitelmia tehtiin laajemman strukturoidun lomakehaastattelun tekemisestä, laajemmalla otannalla, kohdeyrityksessä. Myös laajennetun piirin teemahaastatteluita suunniteltiin tehtäväksi kohdeyrityksen liiketoimintayksiköiden kyberturvallisuusvastaavien haastatteluina. Nämä suunnitelmat jätettiin kuitenkin toteuttamatta, koska arvioitiin, että niistä ei olisi kohdeorganisaation resurssien käyttöön suhteutettuna merkittävää lisäarvoa tutkimuskysymysten selvittämisessä. Tämän tyyppisistä lähestymistavoista voisi kuitenkin olla hyötyä kohdeyrityksessä mahdollisesti tämän tutkimuksen jälkeen tehtävissä tutkimus- ja kehityshankkeissa.

Aiemmasta tutkimuksesta (Willberg, 2017) oli käytettävissä tätä tutkimusta tehdessä vain tutkimusraportti (Gradu-työ). Haastatteluaineistoja tai analyysiaineistoja ei ollut käytettävissä. Tutkimustulosten vertailun katsottiin kuitenkin olevan mahdollista ja hyödyllistä tällä tasolla. Vertailu arvioitiin tutkimuskysymysten näkökulmasta riittäväksi. Vertailu osoitti yhtäläisyyksiä ja eroavaisuuksia tutkimusten tuloksissa, mikä vastasi tutkimuskysymykseen myös tältä osin.

Vaikka nyt tehdyn tutkimuksen otanta, aineistot, aineistojen analyysi sekä vertailu aiempaan tutkimukseen osoittautuivat riittäväksi tutkimuskysymysten näkökulmasta, on tutkimuksen tuloksia ja niiden yleistettävyyttä arvioitaessa syytä huomioida tutkimuksen otannan ja kohderyhmän suhteellisen pieni koko. Tuloksia arvioitaessa on syytä huomioida myös, että tulkinnallisten fenomenologis-hermeneuttiseen tutkimusperinteeseen kuuluvien tutkimusmenetelmien

erityispiirteenä on tutkimuksen painottuminen ihmisen kokemukseen ja näkemykseen tutkitusta aihealueesta. (Tuomi & Sarajärvi, 2018). Kohdeyrityksen osalta tutkimuksen tuloksia voidaan kuitenkin pitää melko luotettavina ja hyvin ydinkompetenssiosaamista kuvaavina tuloksina.

6.5 Jatkotutkimusideoita

Aiemmin tässä raportissa kuvattujen ja pääosin kohdeyrityksen mahdollisiin sisäisiin kehityshankkeisiin liittyvien kohtien lisäksi tutkimuksen aineistosta ja havainnoista oli löydettävissä myös muita jatkokehitysaiheita. Näiden uskotaan olevan hyödyllisiä niin kohdeyritykselle, kuin mahdolliselle akateemiselle jatkotutkimustyölle.

Vaikka tässä tutkimuksessa ei käsitelty yksilötason kompetensseja tai niihin liittyviä työtehtäviä, tarjoaa käytetty viitekehys apua myös niiden tasojen tutkimukseen, hallintaan ja kehitykseen. Tämän tutkimuksen tuloksista arvioitiin muodostuvan hyvä pohja tällaisen kehitystyön jatkamiselle kohdeyrityksessä. Yleisemmin akateemisella sektorilla tutkimuksen tulosten arvioidaan rikastavan aiemman tutkimuksen tuloksia ja laajentavan yleistä ja yhteistä ymmärrystä kyberturvallisuuden kompetenssien luonteesta erilaisissa organisaatioissa.

Tutkimuksen tulosten ja aiemman tutkimuksen vertailun perusteella voitiin jatkotutkimuksen aihealueella nähdä hyödyllisenä useita erilaisia tutkimussuuntia. Tutkimusta arvioitiin olevan mahdollista laajentaa esimerkiksi seuraavasti: 1) tutkimuksen jatkaminen ICT-sektorilla, erilaisten yritysten parissa. Tutkimus lisäisi ymmärrystä kyberturvallisuuden kompetensseista eri tyyppisissä ohjelmisto- ja palveluyrityksissä tällä sektorilla. 2) Tutkimuksen laajentaminen julkisen sektorin toimijoiden parissa voisi laajentaa ymmärrystä myös sillä sektorilla, mikä puolestaan lisäisi tulosten yleistettävyyttä ja hypoteesien kehittämistä myös sillä toimialalla. 3.) Kolmas potentiaalinen jatkotutkimuksen kohde olisi kohdeorganisaation kyberturvallisuuden hallintajärjestelmän kehittäminen tämän tutkimuksen tulosten pohjalta.

LÄHTEET

Ahmad, A., & Babar, M. A. (2014). A framework for architecture-driven migration of legacy systems to cloud-enabled software. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2578128.2578232

Baker, M. (2016). STRIVING FOR EFFECTIVE CYBER WORKFORCE DEVELOPMENT. *Resources.Sei.Cmu.Edu*, *May*. https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473577.pdf

Chen, H. M., & Chang, W. Y. (2010). The essence of the competence concept: Adopting an organization's sustained competitive advantage viewpoint. *Journal of Management and Organization*, *16*(5), 677–699. https://doi.org/10.5172/jmo.2010.16.5.677

Chen, H. M., & Chang, W. Y. (2011). Core competence: What core you mean? - From a strategic human resource management perspective. *African Journal of Business Management*, *5*(14), 5738–5745. https://doi.org/10.5897/AJBM11.045

Dresing, T., Pehl, T., & Schmieder, C. (2020a). *f4analyse* (2.5). dr. dresing & pehl GmbH. https://www.audiotranskription.de/english

Dresing, T., Pehl, T., & Schmieder, C. (2020b). *f4transkript* (8.0). dr. dresing & pehl GmbH. https://www.audiotranskription.de/english

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud and Security*, *2017*(2), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1

ISC2. (2019). *ISC2 - Cybersecurity and IT Security Certifications and Training*. https://www.isc2.org

Kern, S. C. G., & Peifer, K. (2013). *Senior Cyber Leadership: Why a Technically Competent Cyber Workforce Is Not Enough*. https://www.tacoma.uw.edu/sites/default/files/sections/InstituteTechnology/CSFI_Report_12302013 %281%29.pdf

Lane, V. P., & Wright, F. G. (1978). Human resources systematically applied to ensure computer security. Teoksessa G. Bracchi & P. C. Lockemann (Toim.), *Information Systems Methodology* (ss. 684–695). Springer Berlin Heidelberg.

Lehto, M., & Kähkönen, A. (2015). *Kyberturvallisuuden kansallinen osaaminen* (Numero 20).

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Teoksessa *Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja* (Numero 30/2017). Valtioneuvoston kanslia.

Lehto, M., & Niemelä, J. (2019). Kyberalan tutkimus ja koulutus Suomessa 2019. Teoksessa *Informaatioteknologian tiedekunnan julkaisuja* (Vsk. 2019, Numero 83). https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

Menon. (2018). The influence of standards on the Nordic economies. *Menon publication*, *31*(31).

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). *NIST Special Publication*, *800*, 181. https://doi.org/10.6028/NIST.SP.800-181

Niemelä, J. (2019). *KYBERTURVALLISUUSALAN TYÖVOIMAN KYSYNTÄ, SAATAVUUS JA KEHITTÄMINEN VASTAAMAAN TYÖVOIMAN TARVETTA SUOMESSA PRO GRADU*. Jyväskylän yliopisto.

NIST. (2020). *Glossary | CSRC*. https://csrc.nist.gov/Glossary

Prahalad, C. K., & Hamel, G. (1990). The Core Competence of the Corporation. *Harward Business Review*, *68*(3), 79–91.

Radunović, V., & Rüfenacht, D. (2016). *CYBERSECURITY COMPETENCE BUILDING TRENDS Research report Commissioned by the Federal Department of Foreign Affairs of Switzerland*. http://creativecommons.org/licences/

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. Sanastokeskus TSK ry. www.huoltovarmuuskeskus.fi

Saranen-Kauppinen, A., & Puusniekka, A. (2006). *Menetelmäopetuksen tietovaranto [verkkojulkaisu]*. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3.html

Shoemaker, D., Kohnke, A., Sigler, K. (2016). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. CRC Press. https://doi.org/https://doi.org/10.1201/9781315368207

Sonnenreich, W., Albanese, J., & Stout N, B. (2005). Return On Security Investment (ROSI) a practical quantitative model. *Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, in Conjunction with ICEIS 2005*, *38*(1), 239–252. https://doi.org/10.5220/0002580202390252

Suby, M. (2013). The 2013 (ISC) 2 Global Information Security Workforce Study. *Iamcybersafe.Org*, *2013*, 1–28. https://iamcybersafe.org/wp-content/uploads/2017/01/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

Suomen Standardisoimisliitto SFS ry. (2018). *Tietosuojastandardit - Diasarja oppilaitoksille* (ss. 1–38).

The Institute of Information Security. (2019). *IISP - Our Frameworks*. https://www.iisp.org/iisp/Development/Our_Frameworks/iisp/Development/Our_Frameworks.aspx?hkey=47db24fd-8228-4698-be1f-ed5ef7c8c56e

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällon analyysi* (Uudistettu). Kustannusosakeyhtiö Tammi.

Turvallisuuskomitea. (2013). *Suomen kyberturvallisuusstrategia ja taustamuistio*. http://www.yhteiskunnanturvallisuus.fi

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2008). *Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta*. https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10229

Valtiovarainministeriö. (2019). *VM - Vahti-ohjeet*. https://www.vahtiohje.fi/web/guest

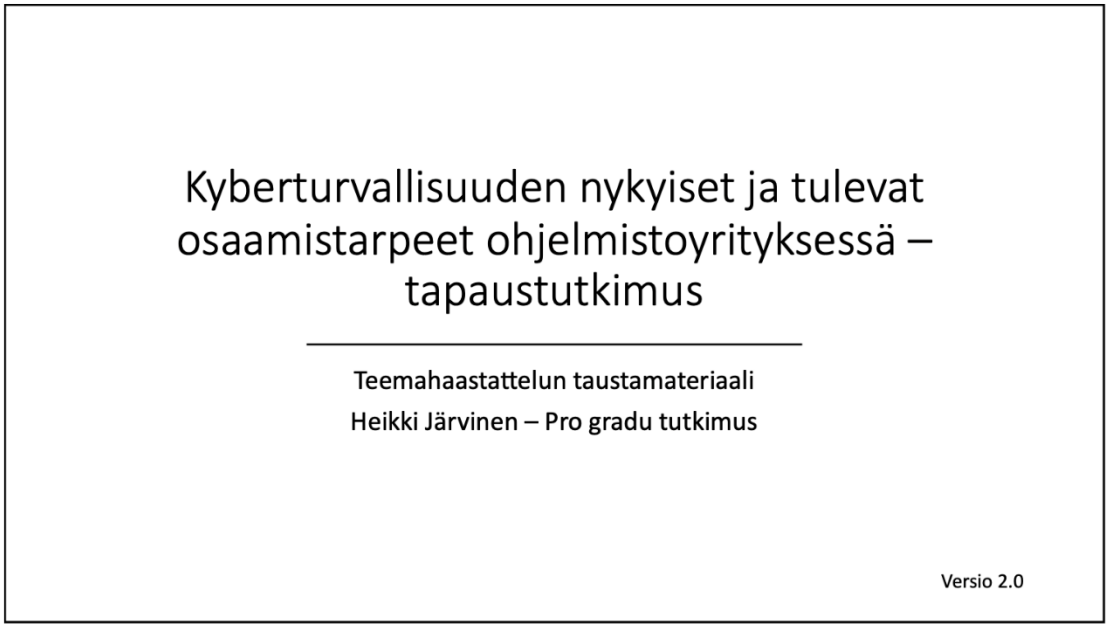
Viitala Riitta. (2014). *Henkilostojohtaminen*. Edita Publishing.

Willberg, N. (2017). *KYBEROSAAMISEN NYKYISET JA TULEVAT TARPEET JULKISEN SEKTORIN ORGANISAATIOISSA PRO GRADU*. Jyväskylän yliopisto.

Yritys X. (2019). *Vuosikertomus 2019*.

LIITE 1 TUTKIMUSHAASTATTELUN ESITIETOMATERIAALI

Tässä liitteessä on kuvattu materiaali, joka toimitettiin haastateltaville ennakkoon, tutustumista varten. Aineisto kuvaa lyhyesti tutkimusasetelman, tutkimuskohteen ja tutkimuskysymyksen. Materiaalissa kuvataan myös käytetty viitekehys. Materiaali toimitettiin PDF-tiedostona sähköpostilla noin viikkoa ennen haastatteluajankohtaa. Aineistoa käytettiin myös keskustelun pohjana haastatteluissa, jotka toteutettiin Microsoft Teams-kokouksina.

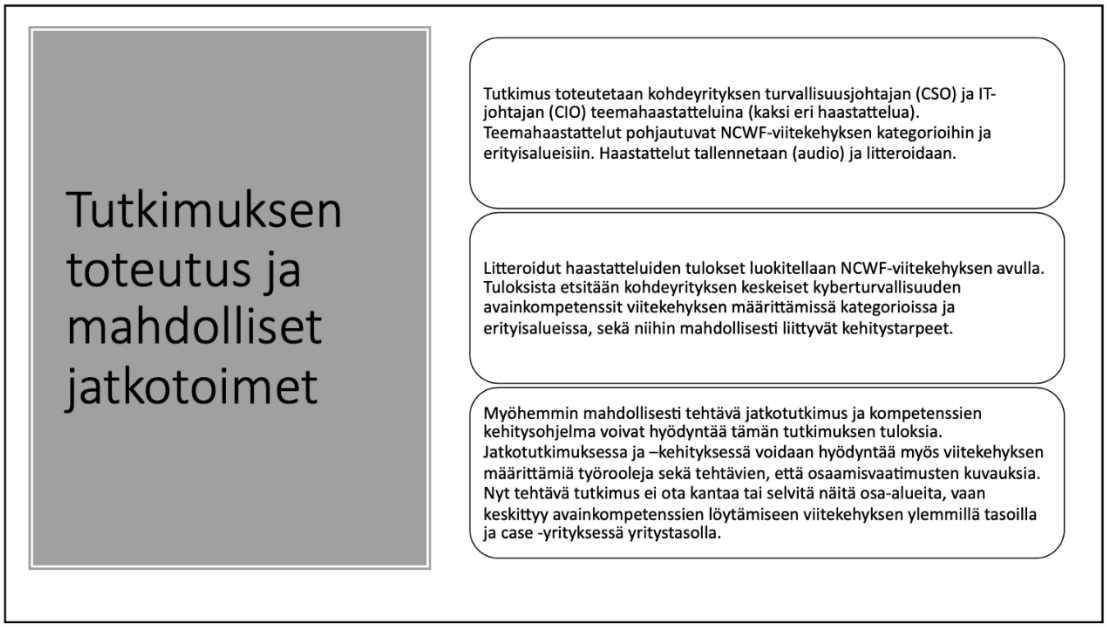


1

2


Tutkimusmenetelmä
Tutkimus toteutetaan **laadullisena tapaustutkimuksena**. Aineistonkeruutapana käytetään puolistrukturoituja teemahaastatteluita. Tutkimushaastatteluiden tulokset litteroidaan ja luokitellaan NCWF-viitekehyksen kategorioihin.

3


Tutkimuksen toteutus ja mahdolliset jatkotoimet
Tutkimus toteutetaan kohdeyrityksen turvallisuusjohtajan (CSO) ja IT-johtajan (CIO) teemahaastatteluina (kaksi eri haastattelua). Teemahaastattelut pohjautuvat NCWF-viitekehyksen kategorioihin ja erityisalueisiin. Haastattelut tallennetaan (audio) ja litteroidaan.
Litteroidut haastatteluiden tulokset luokitellaan NCWF-viitekehyksen avulla. Tuloksista etsitään kohdeyrityksen keskeiset kyberturvallisuuden avainkompetenssit viitekehyksen määrittämissä kategorioissa ja erityisalueissa, sekä niihin mahdollisesti liittyvät kehitystarpeet.
Myöhemmin mahdollisesti tehtävä jatkotutkimus ja kompetenssien kehitysohjelma voivat hyödyntää tämän tutkimuksen tuloksia. Jatkotutkimuksessa ja –kehityksessä voidaan hyödyntää myös viitekehyksen määrittämiä työrooleja sekä tehtävien, että osaamisvaatimusten kuvauksia. Nyt tehtävä tutkimus ei ota kantaa tai selvitä näitä osa-alueita, vaan keskittyy avainkompetenssien löytämiseen viitekehyksen ylemmillä tasoilla ja case -yrityksessä yritystasolla.

4

NCWF-viitekehys

Lyhyt yleiskuvaus

5

Taustaa 1/2

- Viitekehys kehitettiin alun perin osana Yhdysvaltain kansallisen standardien ja teknologian instituutin kansallista kyberturvallisuuden koulutusohjelmaa, NICE -hanketta.
- NICE -hanke oli yhteistyöhanke valtion, akateemisen maailman ja yksityisen sektorin välillä.
- Hankkeen tavoitteena oli kehittää viitekehys, jonka avulla kansallista kyberturvallisuuden osaamista pystyttäisiin määrittämään, standardoimaan ja parantamaan.
- Hanketta johti Yhdysvaltalainen National Institute of Standards and Technology (NIST).

6

Taustaa 2/2

- NICE hankkeen lopputuloksena syntyi NCWF -viitekehys, jonka avulla pystytään hallitsemaan organisaatioiden kyberturvallisuuden tarpeet, määrittämään kyberturvallisuuden toimialueelle yhtenäinen sanasto, työtehtävien kategoriat, erikoistumisalueet sekä työroolit.
- Mallin tarkoitus oli paitsi määrittää edellä mainitut osa-alueet, myös helpottaa työvoiman liikkuvuutta, työvoiman koulutuksen suunnittelua kansallisella tasolla

7

Viitekehys tässä tutkimuksessa

8

NCWF Viitekehys tässä tutkimuksessa

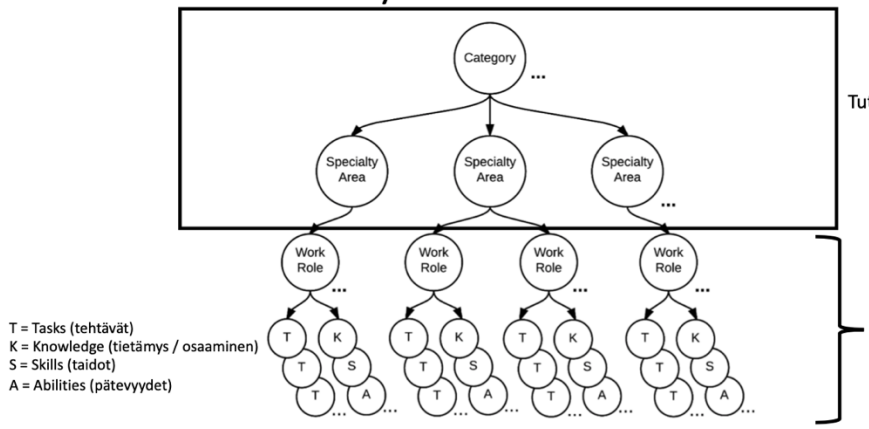


Figure 1 - Relationships among NICE Framework Components

Lähde: Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). *NIST Special Publication*, *800*, 181. https://doi.org/10.6028/NIST.SP.800-181

9

NCWF- Kategoriat

Lyhyt yleiskuvaus

10

NCWF – Kategorioiden yleiskuvaus

Kategoria	Kuvaus
1. Turvallinen tuotanto – Securely Provision (SP)	Konseptoi, suunnittelee ja rakentaa turvallisia IT-järjestelmiä (tietoverkkojen ja tietojärjestelmien kehitys).
2. Operointi ja ylläpito - Operate and maintain (OM)	IT järjestelmien tuki, hallinta (administration) ja huolto. Järjestelmien turvallisen ja tehokkaan toiminnan takaaminen.
3. Suojaaminen ja puolustus - Protect and defend (PR)	Organisaation tietoverkkoon ja järjestelmiin kohdistuvien turvallisuusuhkien Identifiointi, analysointi ja torjunta.
4. Tutkinta - Investigate (IN)	Kyberrikosten, IT-järjestelmiin ja tietoverkkoihin kohdistuvien rikosten/väärinkäytösten tutkinta. Digitaalisen todistusaineiston kerääminen.
5. Kerääminen ja operointi - Collect and operate (CO)	Kyberoperaatiot (peiteoperaatiot, palvelunesto, tiedustelutiedon keräys)
6. Analyze (AN)	Tiedustelutiedon analysointi ja evaluointi tiedustelun käyttötarkoituksessa
7. ohtaminen ja kehittäminen - Oversee and govern (OV)	Organisaation kyberturvallisen toiminnan -turvallisuustyön johtaminen ja hallinta.

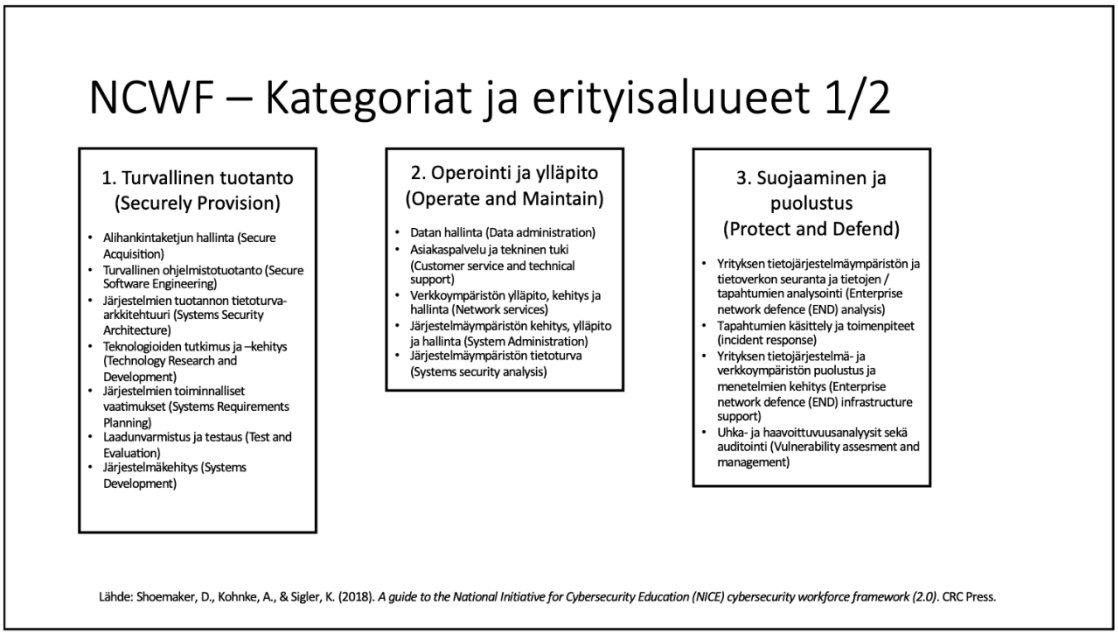
Lähde: Shoemaker, D., Kohnke, A., & Sigler, K. (2018). *A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0)*. CRC Press.

11

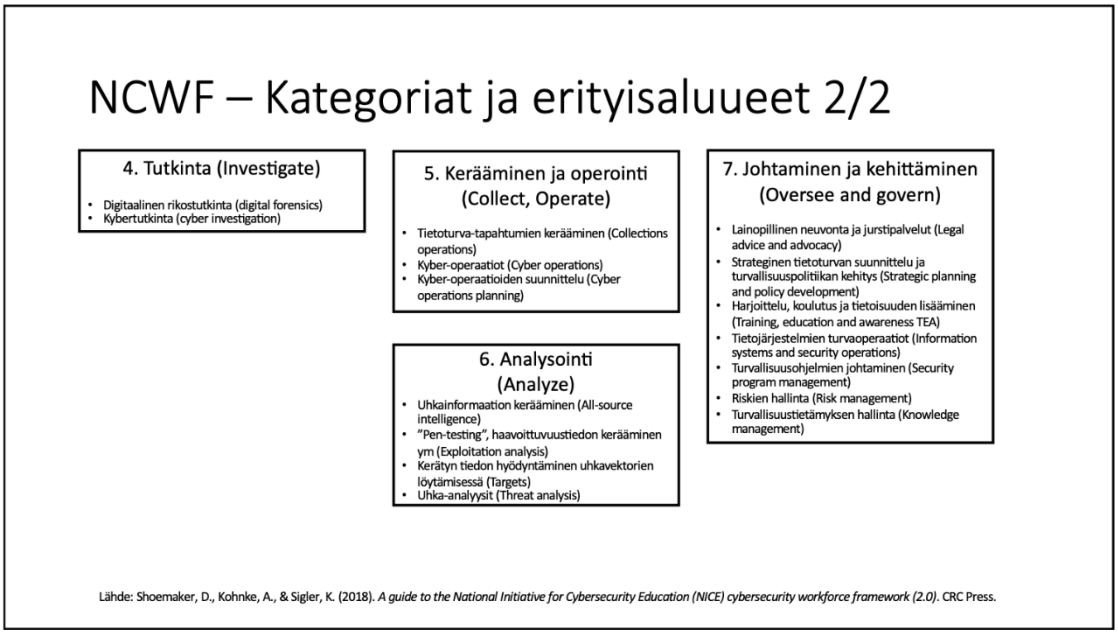
Kategoriat ja erityisalueet

Tutkimuksen kohdealue

12


NCWF – Kategoriat ja erityisaluueet 1/2
1. Turvallinen tuotanto (Securely Provision)
• Alihankintaketjun hallinta (Secure Acquisition)
• Turvallinen ohjelmistotuotanto (Secure Software Engineering)
• Järjestelmien tuotannon tietoturva-arkkitehtuuri (Systems Security Architecture)
• Teknologioiden tutkimus ja –kehitys (Technology Research and Development)
• Järjestelmien toiminnalliset vaatimukset (Systems Requirements Planning)
• Laadunvarmistus ja testaus (Test and Evaluation)
• Järjestelmäkehitys (Systems Development)
2. Operointi ja ylläpito (Operate and Maintain)
• Datan hallinta (Data administration)
• Asiakaspalvelu ja tekninen tuki (Customer service and technical support)
• Verkkoympäristön ylläpito, kehitys ja hallinta (Network services)
• Järjestelmäympäristön kehitys, ylläpito ja hallinta (System Administration)
• Järjestelmäympäristön tietoturva (Systems security analysis)
3. Suojaaminen ja puolustus (Protect and Defend)
• Yrityksen tietojärjestelmäympäristön ja tietoverkon seuranta ja tietojen / tapahtumien analysointi (Enterprise network defence (END) analysis)
• Tapahtumien käsittely ja toimenpiteet (incident response)
• Yrityksen tietojärjestelmä- ja verkkoympäristön puolustus ja menetelmien kehitys (Enterprise network defence (END) infrastructure support)
• Uhka- ja haavoittuvuusanalyysit sekä auditointi (Vulnerability assesment and management)
Lähde: Shoemaker, D., Kohnke, A., & Sigler, K. (2018). A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0). CRC Press.

13


NCWF – Kategoriat ja erityisaluueet 2/2
4. Tutkinta (Investigate)
• Digitaalinen rikostutkinta (digital forensics)
• Kybertutkinta (cyber investigation)
5. Kerääminen ja operointi (Collect, Operate)
• Tietoturva-tapahtumien kerääminen (Collections operations)
• Kyber-operaatiot (Cyber operations)
• Kyber-operaatioiden suunnittelu (Cyber operations planning)
6. Analysointi (Analyze)
• Uhkainformaation kerääminen (All-source intelligence)
• "Pen-testing", haavoittuvuustiedon kerääminen ym (Exploitation analysis)
• Kerätyn tiedon hyödyntäminen uhkavektorien löytämisessä (Targets)
• Uhka-analyysit (Threat analysis)
7. Johtaminen ja kehittäminen (Oversee and govern)
• Lainopillinen neuvonta ja jurstipalvelut (Legal advice and advocacy)
• Strateginen tietoturvan suunnittelu ja turvallisuuspolitiikan kehitys (Strategic planning and policy development)
• Harjoittelu, koulutus ja tietoisuuden lisääminen (Training, education and awareness TEA)
• Tietojärjestelmien turvaoperaatiot (Information systems and security operations)
• Turvallisuusohjelmien johtaminen (Security program management)
• Riskien hallinta (Risk management)
• Turvallisuustietämyksen hallinta (Knowledge management)
Lähde: Shoemaker, D., Kohnke, A., & Sigler, K. (2018). A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0). CRC Press.

14

Kysymyksiä kategorioihin ja erityisalueisiin liittyen

- Mitä kyberosaamista yrityksessä on nyt
- Mitä kyberosaamistarpeita nähdään olevan tulevaisuudesssa

→Mikä on keskeistä osaamista (yritystason ydinkompetenssi)
→Mitä kompetensseja / toimintoja tuotetaan itse (itsenäinen)
→Mitä kompentensseja tuotetaan yhteistyössä kolmannen osapuolen kanssa / ostetaan ulkoa (yhteistoiminnallinen)
→Lakisääteiset tehtävät ja niihin liittyvät kompetenssit (normatiivinen)

15

Syventävää tietoa viitekehyksestä

Kategoriat – erityisalueet - työroolit

Lähde: Shoemaker, D., Kohnke, A., & Sigler, K. (2018). *A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0).* CRC Press.

16

1. Securely provision

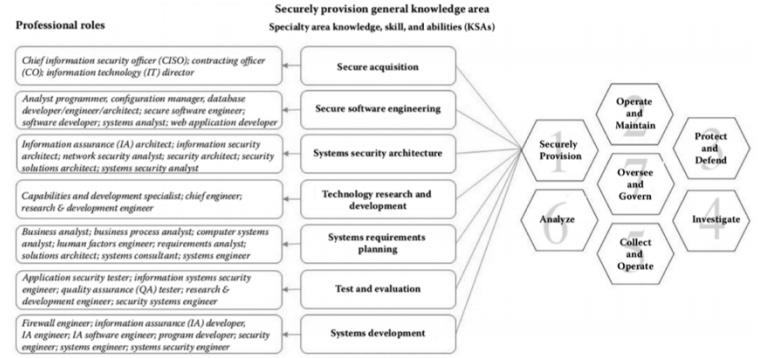


Figure 1.6 The relationship between the securely provision general knowledge area, the specialty areas, and their corresponding roles.

17

2. Operate and maintain

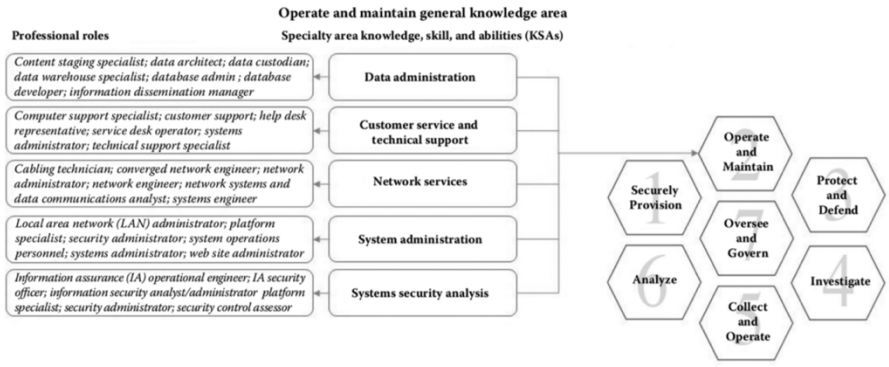


Figure 1.7 The relationship between the operate and maintain general knowledge area, the specialty areas, and their corresponding roles.

18

3. Protect and defend

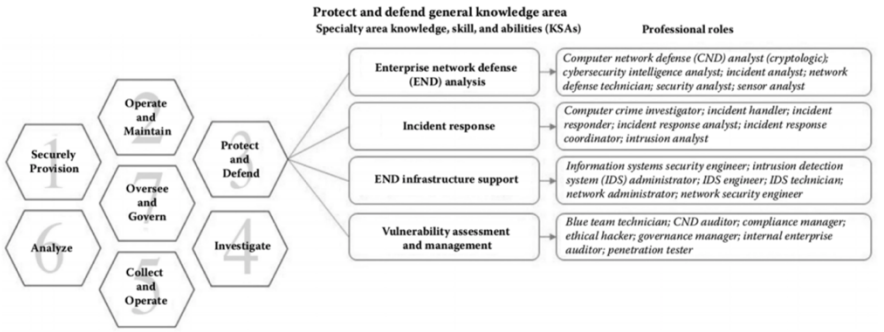


Figure 1.8 The relationship between the protect and defend general knowledge area, the specialty areas, and their corresponding roles.

19

4. Investigate

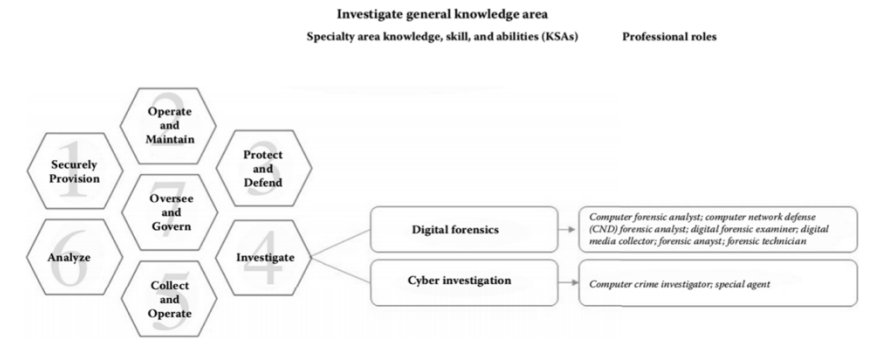


Figure 1.9 The relationship between the investigate general knowledge area, the specialty areas, and their corresponding roles.

20

5. Collect and operate

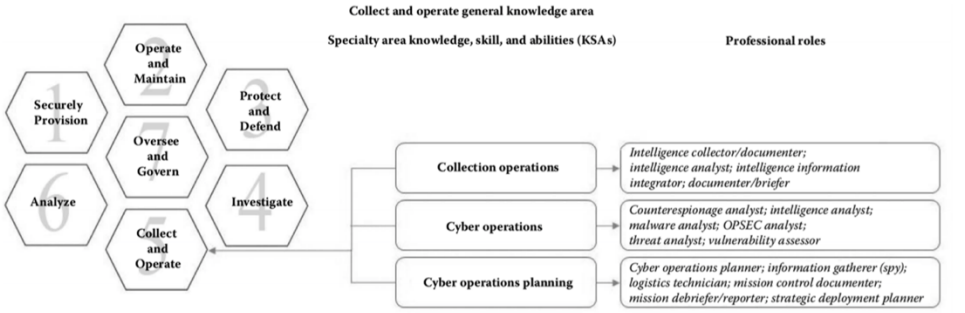


Figure 1.10 The relationship between the collect and operate general knowledge area, the specialty areas, and their corresponding roles.

21

6. Analyze

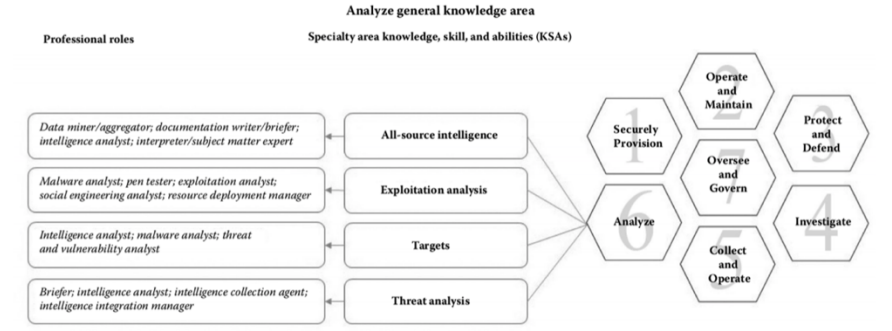


Figure 1.11 The relationship between the analyze general knowledge area, the specialty areas, and their corresponding roles.

22

7. Oversee and govern

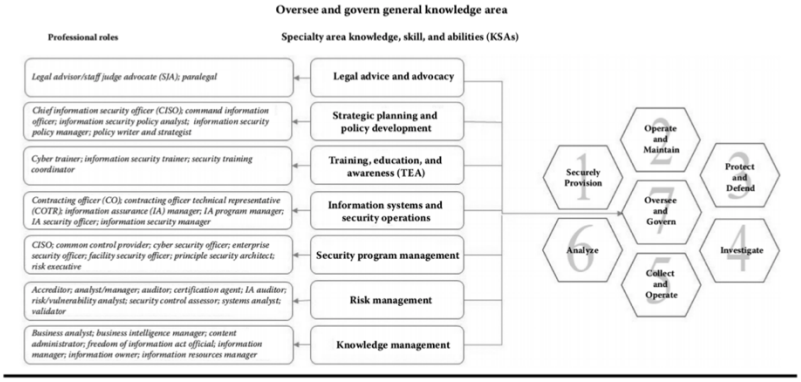


Figure 1.12 The relationship between the oversee and govern general knowledge area, the specialty areas, and their corresponding roles.

23

Lähteitä

24

Lähteitä

Olennainen taustatieto haastatteluiden taustaksi

- NIST – NCWF viitekehys (PDF)
  - Olennainen kiteytettynä: Executive Summary (s. iv)
  - Tarkempia tietoja kehyksestä
    - Kappale 2 (silmäillen läpi)

HUOM! PDF Toimitetaan erikseen liitteenä, mutta yllä linkki tiedoston lähteeseen.

Lisätietoa, jos tarvetta

- Aikaisempi tutkimus aiheesta julkisella sektorilla (Willberg, 2017)
  - Tutkimukseni toistaa Willbergin tutkimuksen tutkimusasetelman ja vertailee saatuja tuloksia

25