Tietoturvavalvomon käyttöönoton haasteet

Harri Rautauoma

2023 Laurea

Laurea-ammattikorkeakoulu

Tietoturvavalvomon käyttöönoton haasteet

Harri Rautauoma

Turvallisuus ja riskienhallinta

Opinnäytetyö

Kesäkuu, 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuus ja riskienhallinta

Tradenomi (AMK)

Harri Rautauoma

Tietoturvavalvomon käyttöönoton haasteet

Vuosi 2023 Sivumäärä 80

Opinnäytetyö selvittää, millaisia yleisiä haasteita tietoturvavalvomon (SOC) käyttöönottoon liittyy. Työn tilaajana toimi Laurea ammattikorkeakoulu Oy ja tavoitteena oli tuottaa soveltuvaa tietoa koulun SOC perustamista varten.

Teoreettinen viitekehys on SOC käyttöönoton menetelmät ja toiminnan kyvykkyydet sekä palvelut. Työn tietoperustana käytettiin erityisesti koulutuksen toimialaan liittyvää kansainvälistä ja kotimaista tietoturvauhkiin liittyvää tutkimustietoa sekä SOC:n perustamiseen liittyvää kirjallisuutta ja sähköisiä artikkeleita.

Opinnäytetyö perustuu neljään haastatteluun. Niissä haastateltavina oli kokeneita johtavissa tehtävissä olevia tietoturva-ammattilaisia, joilla kaikilla oli kokemusta vähintään yhden SOC:n käyttöönotosta ja palveluiden tuottamisesta useamman vuoden ajalta. Yksi haastateltavista edusti organisaatiolleen sisäisiä SOC palveluita tuottavaa, yksi palveluita ulkoa hankkivaa ja kaksi muille organisaatioille palveluita tarjoavaa toimijaa.

Opinnäytetyössä käyttöönottoon liittyviä haasteita käsitellään SOC:n käyttöönottoprojektin käynnistämisen, SOC:n arvon tuoton, sen roolin ja vastuiden sekä SOC palveluissa tarvittavien kyvykkyyksien, palveluiden ja SOC:n hankinnan näkökulmista. Teknologista näkökulmaa työssä käsitellään vain vähän.

Tuloksista käy ilmi, että SOC:n käyttöönoton suurimmat haasteet ovat organisaation olemassa olevien kyvykkyyksien tunnistaminen, SOC:n roolin, vastuiden määrittely osaksi organisaation muuta tietoturvajohtamista, SOC:n tuottamien palveluiden ja näihin palveluihin liittyvien palveluintegraatioiden määrittely ja käyttöönotto eri toimijoiden välillä.

Asiasanat: kyberturvallisuus, riskienhallinta, SOC, tietoturva, tietoturvavalvomo, organisaatioturvallisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Safety, Security and Risk management

Bachelor's Thesis

Harri Rautauoma

The Challenges of Implementing a Security Operations Center (SOC)

Year 2023 Pages 80

The thesis investigates the common challenges associated with the implementation of a Security Operations Center (SOC). The commissioning party of the thesis was Laurea University of Applied Sciences, with the purpose of producing applicable knowledge for the establishment of the school's future SOC.

The theoretical framework consists of the methods and capabilities of implementing a SOC, as well as its services. The thesis is based on research related to the education industry, both domestically and internationally, regarding information security threats, as well as literature and online articles related to the establishment of a SOC.

The thesis is based on four interviews with experienced information security professionals in leadership positions, all of whom have experience in implementing at least one SOC and providing services for several years. One of the interviewees represented an organization that produces internal SOC services, one procures services externally, and two are service providers.

The thesis discusses the challenges related to the implementation of a Security Operations Center (SOC) from the perspectives of initiating the SOC implementation project, generating value from the SOC, defining its role and responsibilities, as well as the perspectives of capabilities, services, and procurement necessary for the SOC. The technological aspect is addressed only to a limited extent in the thesis.

The results indicate that the main challenges in implementing the SOC are identifying the organization's existing capabilities, defining the role and responsibilities of the SOC as part of the organization's overall information security management, defining the services provided by the SOC and the integration of these services, and the adoption of such integrations among different stakeholders.

Keywords: organization security, cyber security, information security, risk management, SOC

Sisällys

1 Johdanto

Tarve tälle opinnäytetyölle tuli Laurea ammattikorkeakoulun Oy:n halusta vähentää tietoturvariskejään perustamalla tietoturvavalvomo (SOC). Mutta millaisia haasteita SOC:n perustamiseen liittyy? Tämä opinnäytetyö pyrkii avaamaan lukijoilleen SOC:n käyttöönottoon liittyviä haasteita.

Ammattikorkeakouluissa käsitellään paljon luottamuksellista tietoa, joiden suojaamiseksi on määritelty lakisääteisiä velvoitteita. Tietoa käsitellään opettajien, muun henkilökunnan, opiskelijoiden ja yhteistyökumppanien toimesta sekä fyysisesti että digitaalisesti. Digitaalista käsittelyä tapahtuu koulun sisäverkossa, opiskelijoille ja yhteistyökumppaneille suunnatuissa työtiloissa ja verkon ulkopuolisissa järjestelmissä.

Yliopistoilla ja korkeakouluilla on paljon kyberrikollisia kiinnostavaa arvokasta tietoa ja eri tutkimukset osoittavat, että koulutuksen toimialaan kohdistuu teollisuuden ja hallinnon alojen jälkeen kolmanneksi eniten tietoverkkorikollisuutta. Rikollisuuden määrä on myös kasvussa. Akateemiset instituutit tuottavat merkittävän osan yhteiskunnan tietoresursseista esimerkiksi tekemällä tutkimustyötä elinkeinoelämän ja julkisen talouden tarpeisiin. Aineettomien oikeuksien varastamisen lisäksi rikollisia kiinnostaa henkilötiedot, yleinen tiedon oikeudeton käyttö, kiristykset, haitan- ja vahingonteko. Koulutuksen toimialaa koskettavia yleisimpiä kyberongelmia ovat palvelunestohyökkäykset, tiedon luvaton käyttö, identiteettivarkaudet, haittaohjelmat, sosiaalinen hakkerointi, organisaation sisältä toteutettavat tietomurrot, kohdistetut edistykselliset toimijaa kohtaan räätälöidyt hyökkäykset (Advanced Persistent Threats, eli ATP's) ja kybervakoilu, jossa usein yhdistellään edellä mainittuja tekniikoita. SOC nähdään tietoturvatapahtumia käsittelevänä toimintona sekä hallinnollisella että teknisellä tasolla. Sen tehtävinä nähdään reaaliajassa tapahtuva kirjautumisten seuranta, hallinta ja tietoturvatapahtumien yhdistely. Koulutuksen toimialaa koskevina SOC:n toimintaan vaikuttavina haasteina nähdään oppilaiden ja organisaatioiden aineettomien oikeuksien suojaaminen, tasapaino organisaation työntekijöiden ja oppilaiden suojaaminen sekä tietoturvavaatimusten saavuttaminen. (Lubna, Baber & Umar 2015, 1–3, 5–6.)

Professorien Gary Rogerin ja Tina Ashfordin jo vuonna 2015 tekemän tutkimuksen mukaan koulutustoimintaa uhkaavien kyberuhkien torjuminen vaatii erityistä osaamista sekä resursseja. Tutkimuksen mukaan ongelmana on, että hyökkääjä voi suunnitella ja keskittää hyökkäyksensä yhteen ja ilmeiseen heikkoon kohtaan, kun taas koulutuksen toimijoiden on puolustauduttava monenlaisia mahdollisia hyökkäyksiä vastaan. Siinä missä yritykset voivat kiristää ja rajoittaa tiedon saatavuutta hyvinkin korkealle, opetustoimessa tiedon on oltava avoimempaa ja opiskelijoiden, tiedekuntien ja henkilökunnan saatavilla. Kyse on myös asenteista.

Useat korkeakoulut ympäri maailmaa panostavat enemmän tietoverkkojensa tietoturvapoikkeamien havainnointiin kuin niiden proaktiiviseen suojaukseen. Monien korkeakoulujen hallintoviranomaiset ovat tiedostaneet haasteet, jotka liittyvät tietojen säilyttämiseen turvassa ja sallien samalla tiedon vapaan liikkumisen ja jakamisen. (Roger & Ashford 2015, 53.)

Campbell (2021) mukaan korkeakoulut ovat haavoittuvia kyberhyökkäyksille. Kyberturvallisuuden riskiä nostaa avoin ja läpinäkyvä kulttuuri, laaja-alainen internet-yhteyksien käyttö, sekä usein vanhentuneet ja hajautetut tietojärjestelmät. Menetelminä erilaisia kiristyshaittaohjelmia ja kalasteluhyökkäyksiä on kohdistettu arkaluontoisten tietojen saamiseksi tai niiden käytön estämiseksi, uhanneet opiskelijoiden turvallisuutta ja aiheuttaneet merkittäviä taloudellisia tappioita. Vaikka korkeakoulut käyttävät erilaisia teknisiä tietoturvakontrolleja, järjestävät koulutusta ja tietoisuuskampanjoita loppukäyttäjille, niin kyberuhkat jatkavat kehittymistään. Lisäksi yleinen kyberturvallisuuden osaajapula vaikeuttaa ammattitaitoisten kyberturvan asiantuntijoiden saamista ja pitämistä korkeakoulujen organisaatioissa. Vastatakseen kasvaviin kyberturvallisuuden uhkiin, on korkeakoulujen jatkuvasti panostettava tietoturvallisuuskäytänteiden parantamiseen. Korkeakoulujen on jatkossakin investoitava sekä osaamiseen että infrastruktuuriin kyberuhkien torjumiseksi kyberturvallisuuden asiantuntijoiden palkkaaminen. (Campbell 2021.)

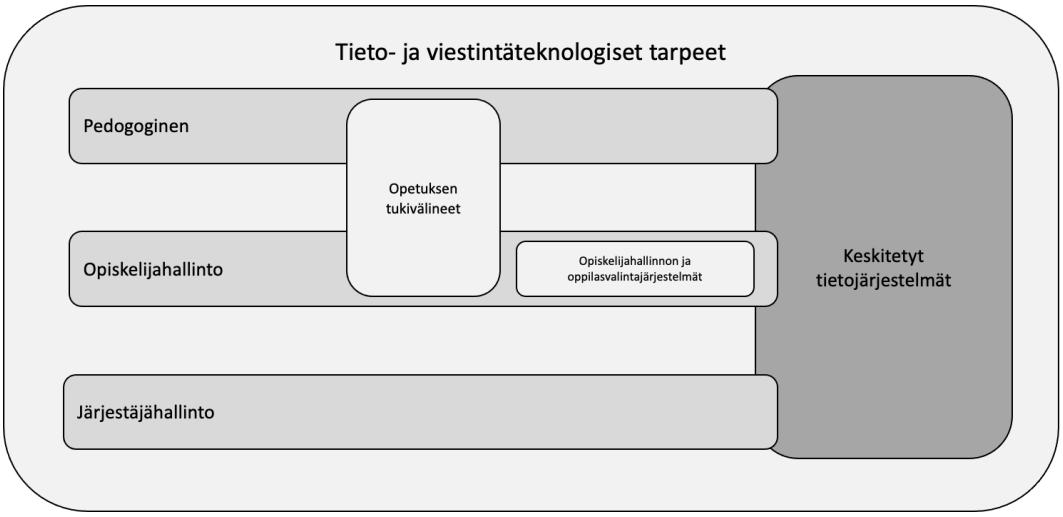
1.1 Opinnäytetyön tausta

Ammattikorkeakoulut ovat julkisia osakeyhtiöitä, joilla on opetushallituksen vaatimusten lisäksi erillisiä niiden liiketoimintaan liittyviä normaaleja tarpeita suojata tietoa ja toimintaa. Liiketoiminnan suojaamiseen liittyy strategian toteutumiseen, maineeseen, talouteen, operatiiviseen toimintaan ja henkilöturvallisuuteen liittyviä riskejä (kuvio 1).

Kuvio 1: Riskikategoriat (mukaillen Ilmonen ym. 2010, 65)

Opetushallitus määrittelee korkeakoulujen tietojen, järjestelmien ja palveluiden suojaamisesta sekä normaali- että poikkeusoloissa. Keinot tietojen suojaamiseksi voivat olla joko hallinnollisia ja/tai teknisiä. Tietoturvallisuus pitää huomioida kattavasti eri osa-alueet huomioiden. Opetushallitus on ohjeistuksessaan jakanut tietoturvallisuuden alueeseen: hallinnollinen ja organisatorinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Opetushallitus painottaa, että koulutuksien järjestäjillä tulee olla oma tietoturvapolitiikka, johon on kirjattu ne periaatteet, joita koulussa tietoturvan osalta noudatetaan. Politiikkaan kirjataan esimerkiksi käyttäjien oikeudet ja velvollisuudet, käyttöoikeusperiaatteet, oikeus käyttää omia laitteita tai asentaa ohjelmistoja. Merkittävä osa kouluissa ja oppilaitoksissa käsiteltävistä suojattavista tiedoista on henkilötietoja. Opetushallitus määrittelee, että oppilaiden henkilötiedot tulee suojata ulkopuolisilta eli kaikilta niiltä tahoilta, jotka eivät tarvitse tietoja omassa tehtävässään. Tiedot tulee suojata joko vahingossa tapahtuvalta tai laittomasti tapahtuvalta hävittämiseltä, muuttamiselta, luovuttamiselta tai siirtämiseltä. Salassa pidettävien tietojen kohdalla nämä vaatimukset korostuvat. Kouluissa tai oppilaitoksissa käsiteltävän tiedon rekisterinpitäjä toimii opetuksen tai koulutuksen järjestäjä. Myös tietosuojavastaava on nimettävä. (Opetushallitus 2021.)

Oppilaitosten tieto- ja viestintäteknologiset tarpeet voidaan jakaa pedagogisiin, opiskelijahallinnon ja järjestäjähallinnon tarpeisiin (kuvio 2). Pedagogisilla tarpeilla tarkoitetaan kaikkia niitä työvälineitä, käyttäjästä riippumatta, joita käytetään opetuksen tukena. Opiskelijahallinnon tarpeisiin kuuluu edellisten työvälineiden lisäksi opiskelijahallinto- ja oppilasvalintajärjestelmät. Järjestäjäorganisaation tarpeilla tarkoitetaan tietohallinnon vastuulla olevia keskitettyjä järjestelmiä, joilla mahdollistetaan yhden kirjautumisen kautta pääsy esimerkiksi matkanhallinnan tai taloushallinnon järjestelmiin. (Opetushallitus 2021.)



Kuvio 2: Mukaillen: Tieto- ja viestintäteknologiset tarpeet oppilaitoksissa (Opetushallitus 2021)

Suomessa henkilötietojen tietosuojasta määritellään erillisessä tietosuojalaissa ja sitä sovelletaan kaikkeen henkilötietojen käsittelyyn lukuun ottamatta henkilötietojen käsittelyyn rikosasioissa ja kansallisen turvallisuuteen liittyvissä asioissa. Niitä varten on säädetty omat erityislait. Opetustoimessa henkilötietojen salassapito ratkaistaan usein julkisuuslainsäädännön avulla mutta käsittelyyn vaikuttaa myös moni muu säädös. Ammattikorkeakoulujen toiminnasta on säädetty erillinen ammattikorkeakoululaki (932/2014), jonka 6. luvun 40 §:ssä on erikseen määritelty arkaluonteisten tietojen käsittelystä. Pykälässä on määritelty, että henkilötietojen käsittelyyn sovelletaan tietosuojalakia (1050/2018). Lisäksi ammattikorkeakouluja koskevia muita keskeisiä säädöksiä ovat laki viranomaisten toiminnan julkisuudesta (621/1999) sekä asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Huomioitavaa kuitenkin on, että laki viranomaisten toiminnan julkisuudesta (621/1999) 3. luvun 9–12 §:ien mukaan tiedonsaantioikeus koskee vain niitä asiakirjoja, joista viranomainen määrää ja lähtökohtaisesti näiden asiakirjojen tulee olla merkityksellisiä joko oppilaalle tai henkilökunnalle. Säädöksissä asetetut salassapitovaatimukset voivat olla joko ehdottomia tai ehdollisia. Mikäli on kysymys ehdottomasta salassapidosta, ei viranomaisella ole valtaa poiketa salassapitovaatimuksista. Mikäli säädöksessä on määritelty asiakirja erikseen salassa pidettäväksi, niin sen kopiota tai tulostetta ei saa näyttää tai luovuttaa ulkopuolisille millään keinoin. Mikäli asiakirja on osittain salassa pidettävä, on huolehdittava, että salassa pidettäviä osia siitä ei luovuteta ulkopuolisten käyttöön. Osassa lainsäädäntöä annetaan viranomaiselle oikeus arvioida salassapitoa, sen vaikuttavuutta ja laajuutta. Tällöin annettava tieto ei saa haitata tai vaarantaa suojattavaa etua. Salassapitoon vaikuttaa keskeisesti kaksi asiaa: lähtökohta, jonka perusteella kaikki viranomaisten asiakirjat ovat julkisia ja tätä julkisuusperiaatetta rajaava lainsäädäntö. (Vehkamäki, Lahtinen & Vanttaja 2018, 8, 10, 15, 19; 621/1999, 9–12 §; 932/2014, 40§; 1030/1999; 1050/2018.)

Kehittääkseen tietoturvaansa ja varmistaakseen koulua koskevien intressien saavuttamisen, on Laurean tavoitteena SOC:n käyttöönotto. Sen avulla halutaan pienentää tietoturvariskejä, parantaa tiedonkäytön tilannekuvaa ja seurantaa sekä kontrolloida vaaditun turvallisuustason säilymistä.

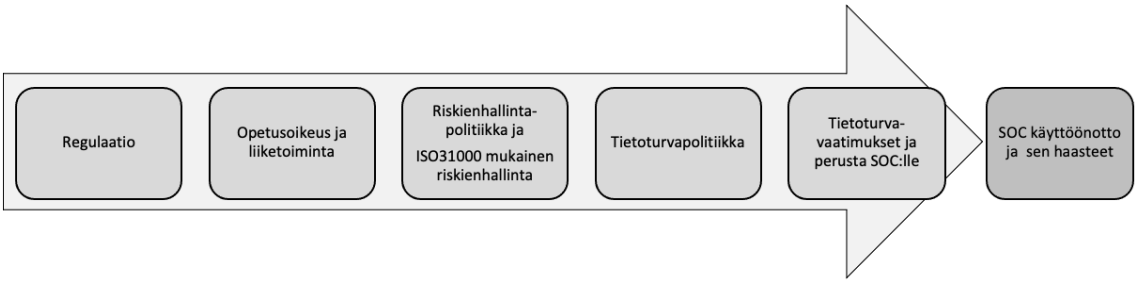
1.2 Aiemmat tutkimukset ja nykytila

SOC:ien käyttöönottoa harkitaan useassa suomalaisessa organisaatioissa, mutta onko tietoa saatavilla? Miten käyttöönottoa suunnitteleville voisi tuottaa tietoa tässä työssä onnistumiseksi? Opinnäytetyön alustavan tiedonhaun yhteydessä selvisi, että tietoturvan kehittämiseen liittyviä artikkeleita, kirjallisuutta, tutkimustietoa ja eritasoisia opinnäytetöitä löytyy paljon. Kuitenkin SOC perustamista ja käyttöönottoa käsitteleviä kirjoja löytyy vain muutama. Internetistä löytyneiden artikkeleiden kirjoittajina on monesti samoja henkilöitä kuin kirjojen kirjoittajinakin tai niissä viitataan samoihin kirjoittajiin kuin kirjojen kirjoittajatkin ovat. Suoraan SOC:n käyttöönottoa käsitteleviä opinnäytetöitä en kuitenkaan löytänyt ainuttakaan.

SOC teemaan liittyviä ylemmän AMK opinnäytetöitä ovat tehneet muun muassa Keltanen (2019) Measuring outsourced Cyber Security Operations Center, jossa työn tavoitteena oli selvittää millä tavalla Cyber Security Operation Center -palvelua voi mitata, Forsberg (2022) ylempi AMK työ, Measuring the technical performance of a security operations center, jossa hän selvitti tietoturvavalvomon teknistä suorituskykyä, Lindström (2018) AMK opinnäytetyö, Next Generation Security Operations Center, jossa hän selvitti kuinka SOC:n toimintaa voidaan tehostaa. Lisäksi löytyy lukuisia eritasoisia opinnäytetöitä, joissa on SOC:a on käsitelty osana tutkielmaa esimerkiksi yhtenä tietoturvaprosessin toimijana tai SOC:n käyttämien työkalujen näkökulmasta. Tämän perusteella vaikutti SOC:n perustamista ja käyttöönottoa käsittelevälle opinnäytetyölle olevan tarvetta.

1.3 Tavoite

Tämän opinnäytetyön tavoitteena on tuottaa tietoa SOC käyttöönottoa harkitseville tai suunnitteleville organisaatioille. Osana tietoturvan kehittämistyötä Laurea halusi selvittää SOC käyttöönottoon liittyviä haasteita. SOC nähdään mahdollisuutena varmistaa, että koulun politiikoissa ja strategioissa asetetut tietoturvatavoitteet saavutetaan ja rajoja ei ylitetä (kuvio 3). SOC:n käyttöönottoon liittyvät edut ja haasteet ovat kuitenkin geneerisiä ja kaikkia sen käyttöönottoa harkitsevia organisaatioita koskettavia.



Kuvio 3: Opinnäytetyössä käytetty hypoteesi Laurean SOC:n käyttöönoton haasteiden arviointiin.

Yleisten SOC:n käyttöönottoon liittyvien haasteiden selvitystarpeen lisäksi, opinnäytetyön tilaaja toi esille tarpeen selvittää millaisia haasteita on, mikäli SOC:n tuottamat palvelut ja tietoturvan hallintajärjestelmä eli Security Incident and Event Management (SIEM) teknologia hankittaisiin erikseen. Tämän asian selvittäminen otettiin tähän opinnäytetyöhön tois'sijaisena tavoitteena.

Palvelu- ja teknologiavalintojen eriyttäminen nähdään Laurean tietoturvatoiminnan kehittämisen joustavuutta lisäävänä tekijänä. Työkalujen omistajuuden pitäminen Laureassa nähdään mahdollisuutena ja kykynä operoida palveluita itse tai hankkia operointipalvelut joustavasti markkinoilta. Yhtenä haasteena tilaaja toi myös esille opinnäytetyön tilaamisen valmistelun yhteydessä Laurean, yhtenä julkishallinnon toimijana, tarpeen tehdä määräajoin

toistuvia jo olemassa olevien palveluiden kilpailutuksia. Eriyttämällä teknologia ja palvelut halutaan pienentää riskiä tietoturvan kehittämiseksi tehtyjen aineettoman omaisuuden investointien, kuten tietojärjestelmiin kuvattujen tietoturvan käyttötapausten ja kontrollien, uudelleen tekeminen palveluoperaattorin vaihtuessa.

1.4 Lähestymistapa ja tutkimuskysymykset

Tämä opinnäytetyö on muodoltaan laadullinen. Työn aineisto syntyi asiantuntijahaastatteluilla ja niistä saatu aineisto analysoitiin teemoittelemalla. Haastatteluita ohjaavana runkona käytettiin SOC käyttöönottoon soveltuvaa ”5 Steps to Building and Operating an Effective Security Operations Center (SOC)” mallia, joka perustuu Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Lifecycle Approach to Network Design and Implementation metodologiaa.

Opinnäytetyön teoreettinen viitekehys hankittiin perehtymällä aihealueeseen liittyvään SOC palveluiden käyttöönottoon liittyvään kirjallisuuteen ja erilaisiin aiheeseen liittyviin artikkeleihin. Lisäksi pyrittiin löytämään tietoa, jossa käsiteltiin tietoturvauhkia ja poikkeamia opetustoimessa. Avoimista tietolähteistä haettiin tietoa toteutuneista tietoturvapoikkeamista, SOC palveluiden käyttöönottoon liittyvää ja sen palveluostamisessa huomioitavia asioita. Tuomalla lukijalle halutiin avata opinnäytetyön lukijalle SOC palvelun merkitystä tietoturvallisuuden varmistamisessa osana muuta tietoturvakokonaisuutta.

Päätutkimuskysymys:

- Millaisia haasteita yleisesti on tai voi olla SOC käyttöönotossa?

Tarkentava tutkimuskysymys:

- Millaisia vaikutuksia olisi päätöksellä eriyttää tietoturvan SIEM hallintajärjestelmän hankinta SOC:n käyttöönotosta?

1.5 Rajaukset

Tässä opinnäytetyössä SOC käyttöönotto käsittää sen perustamiseen ja operoinnin suunnitteluun liittyvän tekemisen, valittavan SOC palveluvalikoiman, tuottamistavan ja tarvittavat kyvykkyydet SOC:n palveluiden tuottamiseksi. Käyttöönottoon liittyviä tekijöitä ja haasteita tarkastellaan käyttämällä SOC tietoturvavalvomon käyttöönottoon liittyvää kirjallisuutta, niissä kuvattuja menetelmiä ja viitekehyksiä. SOC:n teknologiavalintoja, operointia ja jatkuvaan kehittämiseen liittyviä kysymyksiä ei tässä opinnäytetyössä käsitellään vain yleisellä tasolla. Laurea ammattikorkeakoulu Oy:n riskienhallintapolitiikassa edellytetään SFS-ISO 31000 (2018) riskienhallinnan standardin käyttöä ja sen vuoksi opinnäytetyössä riskienhallintaa tarkasteltiin erityisesti tämän standardin näkökulmasta. Laurean riskienhallinta- ja turvallisuuspolitiikat

eivät ole julkisia asiakirjoja ja niitä ei sellaisenaan tulla liittämään osaksi tätä opinnäytetyötä.

Muita soveltuvia ja mahdollisia viitekehyksiä olisivat olleet esimerkiksi ISO/IEC 27005:2018, NIST SP 800-39, OWASP Risk Rating Methodology ja DoD Risk Management Framework (RMF). Niiden käyttö kuitenkin rajataan tämän opinnäytetyön ulkopuolelle.

1.6 Toimeksiantajan esittely

Opinnäytetyön tilaajana on Laurea ammattikorkeakoulu ja sen vuoksi työ sisältää myös tutkimustietoa tietoa koulutuksen toimialan tietoturvatarpeista ja -uhkista. Laurea ammattikorkeakoulu on osakeyhtiö ja sen liiketoimintaan liittyy luottamuksellista tietoa, jota sen tulee suojata. Laurean liiketoiminnan keskeisin perusta on sen opetusoikeus. Sen saaminen ja pitäminen edellyttää, että koulu noudattaa Suomen opetustoiminnalle asetettuja lakeja ja asetuksia. Osa koululle annetuista vaatimuksista koskee erityisesti tietoturvaa. Yhtiön yleisten regulaatioisten intressien ja liiketoimintaan liittyvien riskien ohjaamiseksi Laurealla on käytössään riskienhallinta- ja tietoturvapolitiikka. Politiikkojen ja niihin liittyvien strategioiden eli kehittämisohjelmien avulla Laurean ylin johto määrittelee ylätason vaatimukset koulun tietoturvalle, viestii organisaatiolleen ja sidosryhmilleen koulun riskinottohalukkuutta ja -rajoja sekä näihin liittyvää kehittämistyötä.

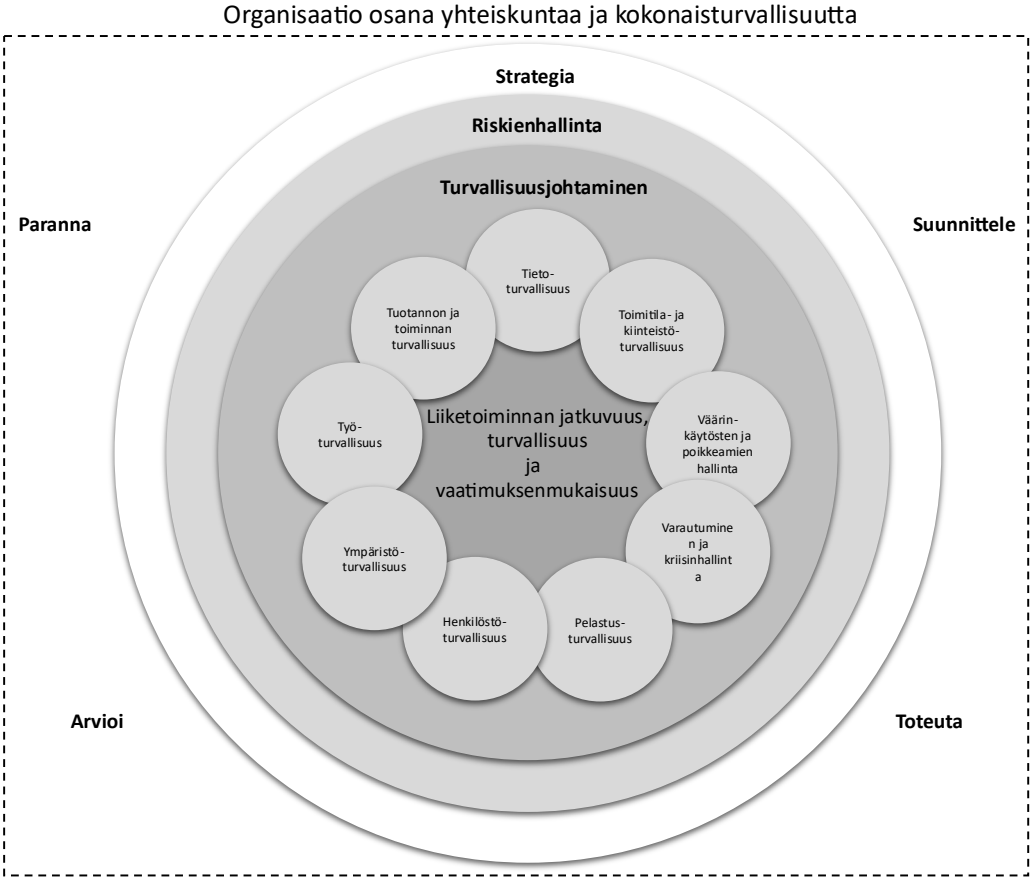
2 Kyberturvallisuus

Kyberturvallisuuden pääluku alalukuineen muodostaa tämän opinnäytetyön teoreettisen tietopohjan ensimmäisen osan. Luvuissa avataan lukijalle turvallisuuden, turvallisuusjohtamisen, riskienhallinnan ja tietoturvan käsitteet sekä kyberturvallisuuden tilannekuvaa sekä yleisesti että opetuksen toimialalla.

Turvallisuus käsitteenä on organisaation olotila, jossa vaaroja ja uhkia ei ole. Turvallisuus on myös tunnetila, jossa tulevaisuuden uhat ovat tunnistettuja ja niistä aiheutuvat riskit hallittuja. Turvallisuutta arvioidaan usein erilaisten näkökulmien kautta. Näitä voivat olla esimerkiksi poliittinen, psykologinen, sosiaalinen, sotilaallinen, taloudellinen, tekninen, yhteiskunnallinen ja ympäristöön liittyvä. Turvallisuus pyritään saavuttamaan riskejä poistamalla tai vähentämällä. Täydellistä turvallisuutta voi kuitenkin harvoin saavuttaa ja sen vuoksi turvallisuus onkin enemmän jatkuvasti muuttuva arvojen suojaamista tavoitteleva tila, kuin pysyvä olotila. Turvallisuuteen liittyy myös käsitteet ”Safety” ja ”Security”. Yksi tapa on määritellä Safety toiminnaksi, jolla ehkäistään turvallisuuteen liittyvien tahattomien vahinkojen syntyminen ja Security toiminnaksi, jolla pyritään estämään tahallisten vahinkojen syntyminen. (Lanne 2007, 18–19.)

Suomessa kokonaisturvallisuudella tarkoitetaan suomalaisen varautumisen yhteistoimintamallia, jossa yhteiskunnan eri toimijat, viranomaiset, elinkeinoelämä, järjestöt ja kansalaiset tekevät yhteistyötä elintärkeiden toimintojen turvaamiseksi. Kokonaisturvallisuuden periaatteet on linjattu Yhteiskunnan turvallisuusstrategiassa. Sen mukaan opetustoimi on osa Suomen huoltovarmuutta. (Yhteiskunnan turvallisuusstrategia 2017, 13, 48, 85.)

Organisaatioturvallisuudella, josta käytetään myös nimeä yritysturvallisuus, varmistetaan organisaation toiminnan jatkuvuus kaikissa tilanteissa. Organisaatioturvallisuudella tarkoitetaan organisaation henkilöstöstä, tiedosta, materiaalista, teknisestä infrastruktuurista ja ympäristöstä muodostuvaa toimintaa tai toimintojen kokonaisuutta, jossa uhat ja riskit ovat hallinnassa tai tunnetta siitä, että ne ovat hallinnassa. Organisaatioturvallisuus muodostuu henkilöturvallisuus, palo- ja pelastustoiminta, rikostorjunta, tietoturvallisuus, valmiussuunnittelu, tuotannon ja toiminnan turvallisuus, toimitilaturvallisuus, työturvallisuus, ulkomaantoimintojen turvallisuus osa-alueista. Näistä muodostuvan kokonaisuuden hallintaa kutsutaan organisaatioturvallisuuden hallinnaksi. Suojattavia arvoja ovat henkilöt, ympäristö, omaisuus, tieto ja maine. Huolehtimalla omasta turvallisuudestaan, organisaatio turvaa oman toiminnan jatkuvuuden ja kasvattaa kokonaisturvallisuutta (kuvio 4). (Kokonaisturvallisuuden sanasto 2017, 16–17; Leppänen 2006, 203; Elinkeinoelämän keskusliitto 2016, 3; Lanne 2007, 11, 14.)

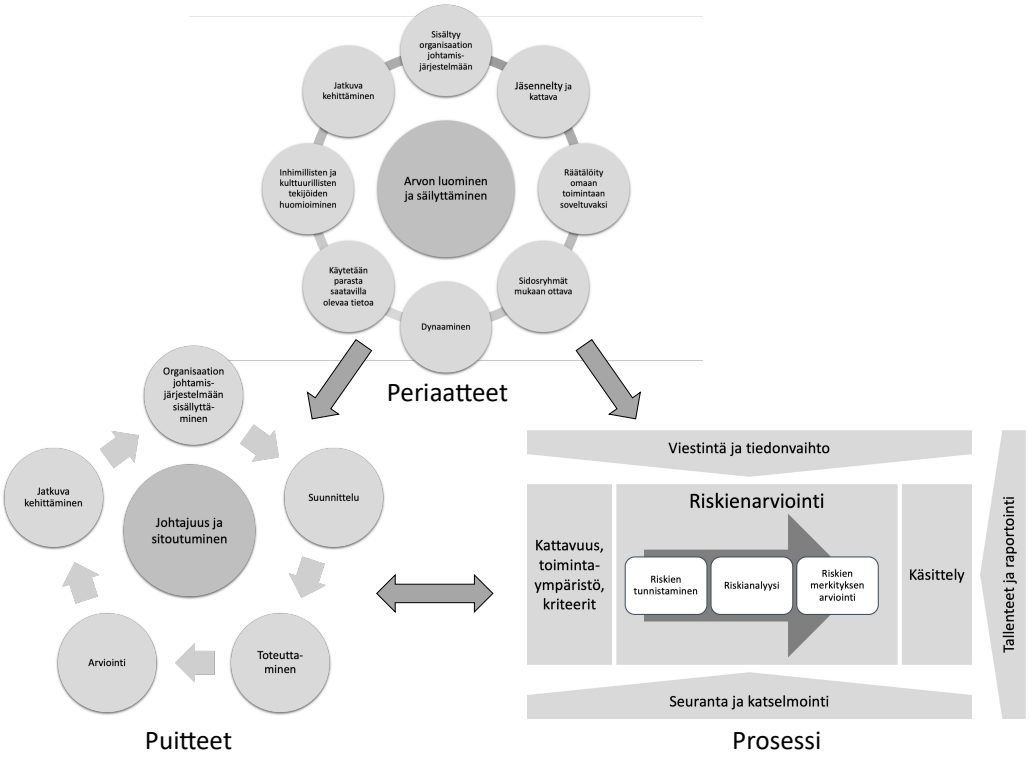


Kuvio 4: Organisaatioturvallisuus Elinkeinoelämän keskusliitto 2016, 3)

2.1 Riskienhallinta

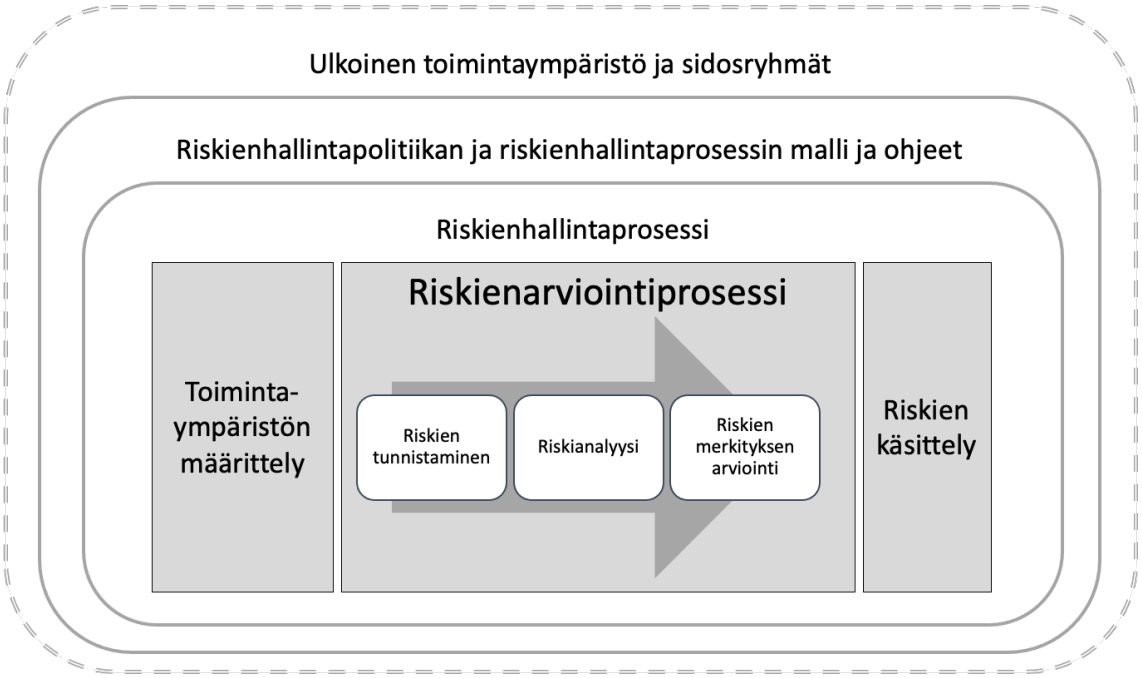
Riski (risco) tarkoittaa latinan kielessä asiaa, jonka olemassaolon uskomme tietävän ja siihen liittyy vahingon vaara eli uhka. Riskiin sisältyy oletus, että se tapahtuu yllättäen ja että siihen liittyvä tappio tai vahinko syntyy tulevaisuudessa. Riski ilmaisee epävarmuutta saavuttaa tavoitteet, se usein arvioidaan kuvaamalla jokin tapahtuma, joka poikkeaa odotetusta. Riski voi olla SFS-ISO 31000 (2018) standardin määritelmän mukaisesti myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia sekä uhkia. Standardin mukaan riskillä on jokin lähde ja riski ilmaistaan mahdollisten tapahtumien, niiden seurausten sekä todennäköisyyden yhdistelmänä. Riskin lähde on jokin tekijä, esimerkiksi uhka, joka aiheuttaa riskin. Toteutunutta riskiä kutsutaan esimerkiksi häiriöksi, tappioksi, vahingoksi tai menetykseksi. Tietoturvariski muodostuu silloin, jos tietojen suojaus on puutteellista. (SFS-ISO 31000:2018, 6; SFS-opas 73:2011; Kauppi 2022.)

Riskienhallinnan tarkoitus on arvon luominen ja säilyttäminen. Riskienhallinnan kokonaisuus muodostuu periaatteista (8), puitteista (5) ja prosessista (kuvio 5). Nämä voivat olla kussakin organisaatiossa joko kokonaan tai osittain käytössä ja niiden maturiteettiaste voi vaihdella. Yksi keskeinen periaate on, että riskienhallinnan tulee olla systemaattisesti ja jatkuvasti kehittyvä kokonaisuus. (SFS-ISO 31000:2018, 5, 7–19.)



Kuvio 5: Riskienhallinnan periaatteet, puitteet ja prosessi (Riskienhallinta. Ohjeet. SFS-ISO 31000:2018, 5)

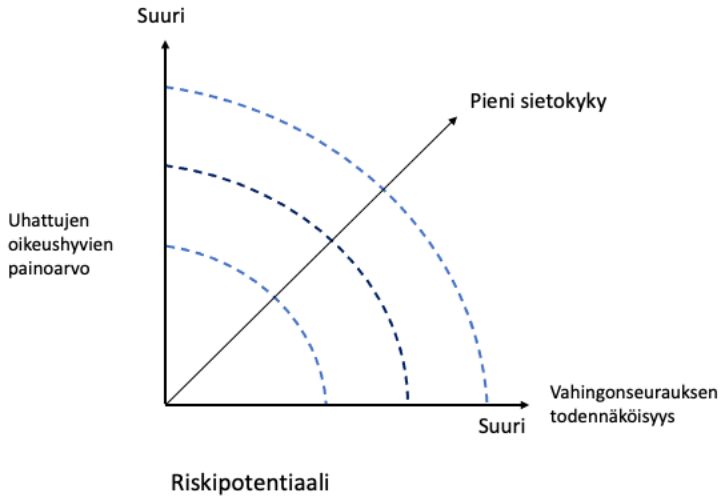
Riskienhallinta on iteratiivinen prosessi, jolla riskejä tunnistetaan ja hallitaan (kuvio 6). Hyvällä riskienhallinnalla käytettävissä olevia resursseja kohdistetaan niiden uhkien torjumiseen ja haavoittuvuuksien vähentämiseen, joista liiketoiminta saa suurimman hyödyn. Riskienhallinnalla pyritään auttamaan organisaatiota määrittelemään sille paras strategia, jolla se saavuttaa sille asetetut tavoitteet. Riskienhallinta määritellään osana organisaation hyvää hallintotapaa, se on osa organisaation johtamisjärjestelmää ja sen tulee olla osa koko organisaation sekä sen ulkoisten sidosryhmien välistä toimintaa. (Rousku 2017, 12.)



Kuvio 6: Riskienhallinnan viitekehys SFS-ISO 31000:2018. (mukaillen Rousku 2017, 12).

Yritystoimintaan sisältyy aina riskejä ja sen vuoksi niiden menestyksekäs hallinta on avain myös yrityksen tavoitteiden saavuttamiseen ja tuloksen tekoon. Oikeilla päätöksillä yritys voi menestyä ja tuottaa voittoa mutta väärillä päätöksillä se voi hukata menestymisen mahdollisuudet. Dokumenttia, jolla organisaatio kuvaa riskienhallintaan liittyvät periaatteet ja tavoitteet kutsutaan riskienhallintapolitiikaksi tai -periaatteiksi. Riskien arviointi edellyttää, että ensin niitä vastaavat uhat on tunnistettu. Näkökulmia miten uhkia kartoitetaan ja riskejä luokitellaan, on useita erilaisia. Uhka -käsite on mahdollisesti toteutuva, epätoivottu, kielteinen ja haitallinen tapahtuma, joka toteutuessaan aiheuttaisi kohteelleen ei-toivottuja ja ei positiivisia seurauksia. Usein uhkan synonyyminä käytetään myös vaara -käsitettä, joka kuvaa mahdollista riskin lähdettä. Yksi uhka voi muodostaa useamman riskin. Oleellista on, että uhat ja riskit tulee arvioida avoimesti ja kokonaisvaltaisesti. Muita riskienhallintaan liittyviä keskeisiä käsitteitä ovat vaara, riskikapasiteetti, riskinottokyky – ja halu. (Rousku 2017, 13; Valtionhallinnon tietoturvasanasto 2008, 122; VM 22/2017 Ohje riskienhallintaan, liite 1 2017, 3; SFS-opas 73: 2011, 12; Leppänen 2006, 29–32, 41.)

Riskipotentiaalilla tarkoitetaan riskin vakavuuden ja todennäköisyyden suhdetta (kuvio 7). Se voidaan ilmaista kääntäen verrannollisena eli mitä vakavammasta ja todennäköisemmästä uhasta on kyse, sitä pienempi riskin sietokyky on. (Leppänen 2006, 41).

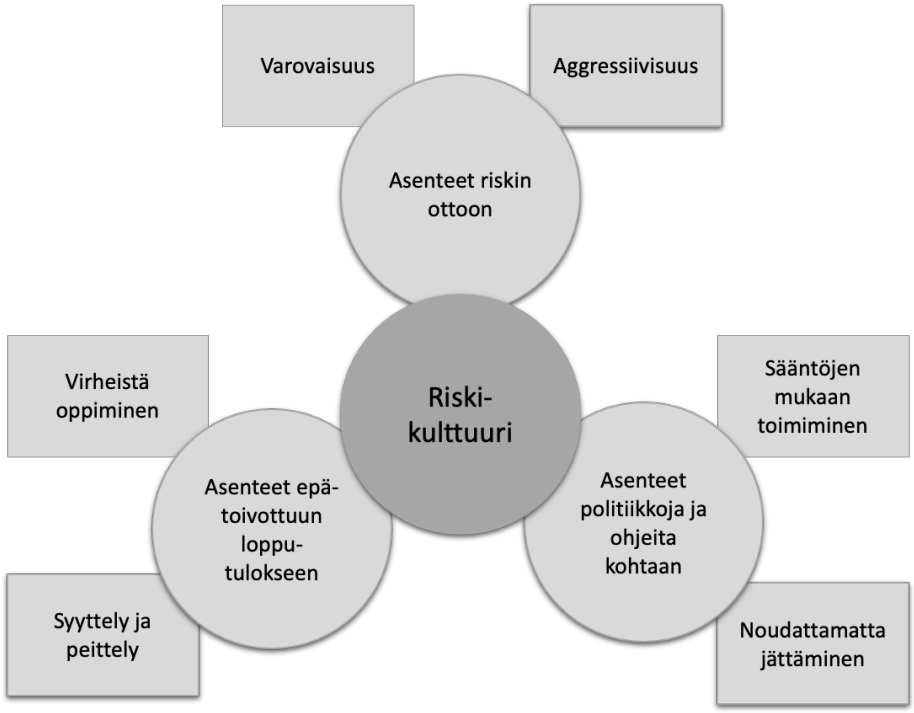


Kuvio 7: Riskipotentiaali (mukaillen Leppänen 2006, 41)

Riskipotentiaali käsitettä voidaan käyttää myös silloin kun käytettävissä ei ole riittävästi tietoa riskin suuruuden perusteluun eli tuntemattoman suuruuden ja todennäköisyyden yhdistelmänä. Vakavuuden tai todennäköisyyden kasvaessa myös riskipotentiaali kasvaa. Mikäli riskin suuruus ja todennäköisyys voidaan perustellusti arvioida, käytetään riskin suuruus -käsitettä. (Lanne & Heikkilä 2016, 4.)

Organisaatioiden riskinottohalu ja -kyky on usein erilainen. Riskin sietokyvyllä tarkoitetaan riskin suuruutta, jonka organisaation on valmis hyväksymään sen jälkeen, kun tarvittavat hallintakeinot on käyttöönotettu. Riskienottohalulla tarkoitetaan organisaation kykyä ja valmiutta ottaa riskejä, jotta se saavuttaa tavoitteensa. (Rousku 2017, 15.)

Yksi haluun ja kykyyn liittyvä merkittävä tekijä on organisaation riskikulttuuri, joka kuvastaa organisaation ja sen jäsenten asennetta riskejä kohtaan (kuvio 8). Hyvä riskienhallinta huomioi ympäristössä olevat kulttuurilliset tekijät, joilla tarkoitetaan yrityksen toimintaperiaatteisiin sisältyviä arvoja, normeja, olettamuksia ja odotuksia. Kulttuuriin vaikuttaa organisaation kommunikointi- ja ongelmanratkaisukyky, yhteistyön organisointi, johtamistapa, oppiminen ja tiedonkulku. (Turvallisuusjohtaminen 2010, 5; Lanne 2007, 31.)



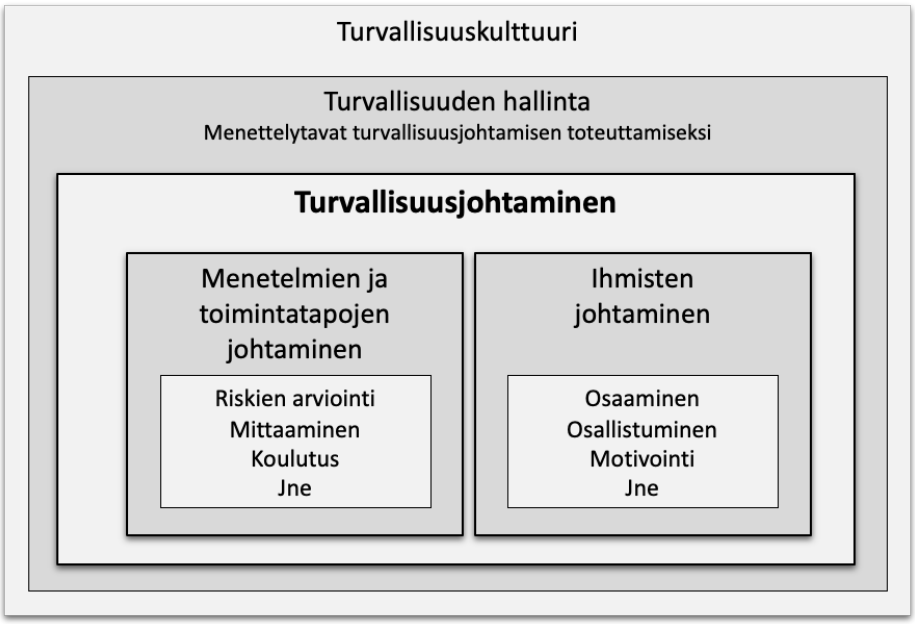
Kuvio 8: Riskikulttuuri (The CRISC Review Manual 7th Edition 2021, 42)

SFS-ISO 31000 (2018) riskienhallinnan prosessi edellyttää riskien arviointia, johon kuuluu riskien tunnistaminen, riskianalyysi ja riskin merkityksen arviointi. Riskianalyysi on pohja riskin merkityksen arvioinnille ja sen tarkoituksena on tukea päätöksentekoa. Arviointivaiheessa pyritään ymmärtämään riskiä paremmin, vertaamaan riskiä päätöksentekokriteereihin, tarkastelemaan erilaisia vaihtoehtoja ja hallintakeinoja. Arvioinnin jälkeen riski käsitellään eli valitaan ja toteutetaan menetelmä, jolla saavutetaan tunnistetun riskien haluttu uusi riskitaso. Riskinkäsittelyn menetelmäksi voidaan valita riskin poistaminen estämällä riskipitoinen tekeminen, lähteen poistaminen, todennäköisyyden tai seurausten muuttaminen, jakaminen (esimerkiksi sopimuksilla tai vakuuttamalla) tai riskien pitäminen. (SFS-ISO 31000:2018, 17–18.)

2.2 Turvallisuusjohtaminen ja turvallisuusjohtamisjärjestelmä

Organisaatioturvallisuuden johtamista kutsutaan turvallisuusjohtamiseksi ja sen tavoitteena on auttaa organisaatiota saavuttamaan sen strategiset tavoitteet. Turvallisuusjohtaminen perustuu turvallisuuteen liittyvien politiikoiden suunnittelusta ja toteuttamisesta, joita tehdään systemaattisesti riskienhallinnan menetelmiä käyttäen. Turvallisuusjohtaminen tarkoittaa vahinkoja ennalta ehkäisevää ihmisten, omaisuuden, tiedon ja maineen organisoitua johtamista ja sitä tukee kokonaisvaltainen koko yrityksen toimintaa koskeva riskienhallinta. Turvallisuusjohtaminen vaatii organisaatioturvallisuuden osa-alueiden lisäksi useiden muiden organisaation toimintaan vaikuttavien tekijöiden hallintaa. Yritystoiminnassa tämä tarkoittaa esimerkiksi toiminnan riskien tunnistamista liiketoiminta- ja yksikkötasoilla mukaan lukien kulttuurilliset ja maantieteelliset erityispiirteet, yritystä koskeva lainsäädäntö, asiakas- ja

sidosryhmäverkostojen vaatimukset (kuvio 9). Turvallisuusjohtaminen ja riskienhallinta ovat jatkuvia prosesseja, joilla organisaatio suunnitellun toteutuksen, seurannan ja arvioinnin kautta määrittelee ja kehittää turvallisuuden ja riskienhallinnan politiikat. Kokonaisuutta, jolla koko turvallisuusjohtamisen kokonaisuus, toimintamalli ja tietojärjestelmä kuvataan, kutsutaan turvallisuusjohtamisen portfolioksi. (Leppänen 2006, 13–15. Lanne 2007, 12.)



Kuvio 9: Turvallisuusjohtaminen (mukaillen Turvallisuusjohtaminen 2010, 6)

Organisaation ylin johto toteuttaa turvallisuusjohtamista turvallisuusjohtamisjärjestelmän avulla. Organisaation turvallisuusjohtamisjärjestelmän tulee sisältää organisaatiota koskevat turvallisuuteen vaikuttavat politiikat, turvallisuuden tavoitteet, prioriteetit, organisoitumisen vastuualueineen, riskienhallinnan, toiminnan arvioinnin, jatkuvan kehittämisen mallin ja tarvittavat resurssit. Sen tulee olla dokumentoitu lähestymistapa organisaation turvallisuuden hallitsemiseksi. Turvallisuuden johtamisjärjestelmästä voidaan käyttää myös turvallisuuden hallintajärjestelmä -nimeä. Informaatioteknologiassa yksi tunnetuimmista hallintajärjestelmistä on ISO-organisaation tietoturvallisuuden hallintajärjestelmä ISO/IEC 27001. (Kerko 2001, 24; Reiman & Oedewald 2008, 30; SFS-EN ISO/IEC 27001:2017.)

2.3 Tietoturva ja niihin liittyvien riskien hallinta

Tietoturva tarkoittaa tietoaineiston ja tietojärjestelmien suojaamista sekä kaikkia organisatorisia ja teknisiä menetelmiä, joilla tiedon eheys, saatavuus ja luottamuksellisuus turvataan. Mallia voidaan laajentaa myös hallussapidon, autenttisuuden ja hyödyllisyyden käsitteillä. (Tietosuoja 2021; Kyberturvallisuuden sanasto 2018, 15.)

Kyberturvallisuus on osa tietoturvaa ja kyberturvallisuus käsitteelle löytyy useita erilaisia kuvauksia. Craigen, Diakun-Thibault ja Purse (2014, 1, 17) selvittivät tutkimusartikkelissaan kyberturvallisuudelle annettuja erilaisia kuvauksia ja määrittelivät niiden perustella sille uuden kuvauksen, jossa kyberturvallisuus tarkoittaa organisaatiota, siihen vaikuttavaa kyberavaruutta ja siinä toimivien järjestelmien suojaamiseksi tarvittavia resursseja, prosesseja ja rakenteita, jotka kohdistuvat sen tosiasiallisiin (de jure) omistusoikeuksiin.

Yksi tunnetuimmista informaatioteknologian riskienhallinnan viitekehyksistä on ISO/IEC 27005 (2018) ja siinä käytetty riskienhallinnan prosessi perustuu SFS-ISO 31000 (2018) standardiin. Yritykset voivat sertifioitua ISO/IEC 27001 mukaisesti toimivaksi suorittamalla hyväksytyn ulkoisen auditoinnin siihen akkreditoidun toimijan toimesta. ISO/IEC 27005 määrittelee informaatioteknologian riskienhallinnan osalta toimintaympäristön määrittämiseen, tietoturvariskien arviointiin ja käsittelyyn, niiden hyväksymiseen, viestintää ja tiedonvaihtoon, seurantaa sekä katselmointiin liittyviä vaatimuksia. (SFS-ISO/IEC 27005:2018.)

Tietoturvapoikkeama voi olla jonkin tietoturvavaatimuksen täyttymättä jääminen, poikkeaman tietoturvapolitiikoiden tai -käytäntöjen rikkominen tai niiden rikkomisen välitön uhka. Käsitteenä tietoturvapoikkeamien ja -häiriöiden hallinta tarkoittaa yhden tai useamman tietoturvatapahtuman, joka voi vahingoittaa organisaation omaisuutta tai vaarantaa sen toimintoa, johdonmukaista hallintaa ja toimintamallin toteuttamista. CSIRT Services Framework (2019) määrittelee tietoturvapoikkeaman hallinnan kokonaisuuden palveluiksi, joista on organisaatiolle elintärkeä apu tietoturvahyökkäyksen selvittämiseksi ja siitä toipumiseksi. (Computer Security Incident Response Team (CSIRT) Services Framework 2019, 9; SFS ISO/IEC 27035 2016, 7; SFS-EN ISO/IEC 27000:2020, 11; Kyberturvallisuuden sanasto 2018, 16.)

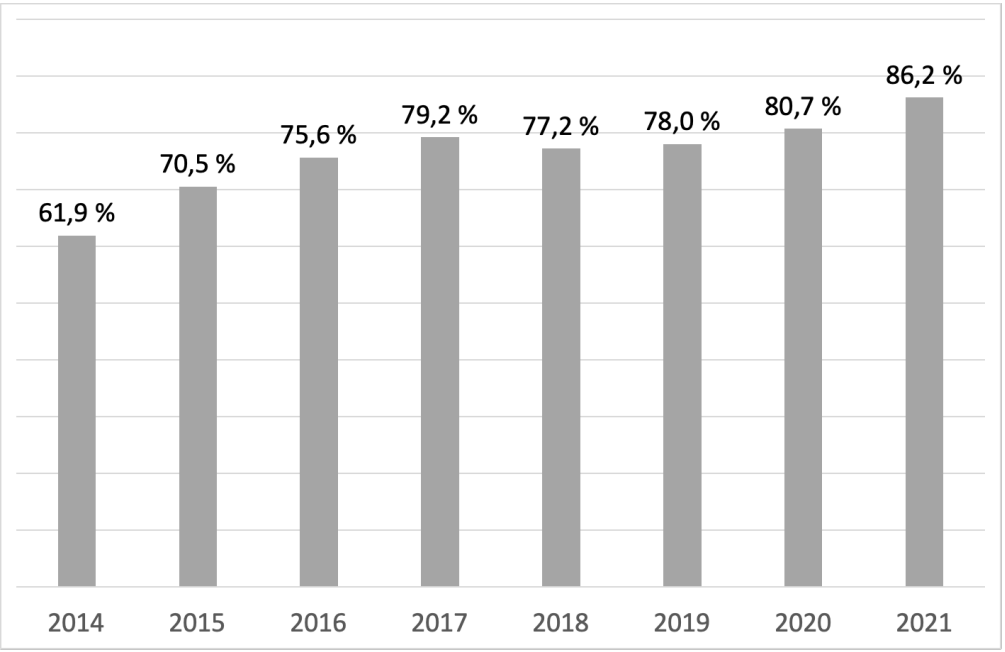
2.4 Kyberturvallisuuden yleinen tilannekuva

Luvuissa 2.4–2.5 esitetään kyberturvallisuuden ja -uhkien tilannekuvaa sekä yleisesti että korkeakouluissa.

Kyberturvallisuus tarkoittaa niitä kaikkia toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta. Kyberturvallisuus vaikuttaa organisaation toimintaan kokonaisvaltaisesti ja sen vuoksi sen tulee olla osa riskienhallintaa sekä päätöksentekoa. Kyberuhka tarkoittaa mikä tahansa potentiaalista tilanne, tapahtumaa tai toimintaa, joka voi vahingoittaa tai muuten häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti. (Euroopan kyberturvallisuuden verkosto ja osaamiskeskus 2021; Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 23.)

Turvallisuuteen kohdistuvat kyberhyökkäykset ovat maailmalla jatkuvasti kasvussa ja ne ovat yhä monimutkaisempia, kehittyneempiä ja vaikeammin havaittavia. Yritykset tarvitsevat lisääntyneiden uhkien torjuntaan lisää resursseja, osaamista, prosesseja ja teknologiaa. (Muniz, McIntyre & Alfardan 2016, 1–2.)

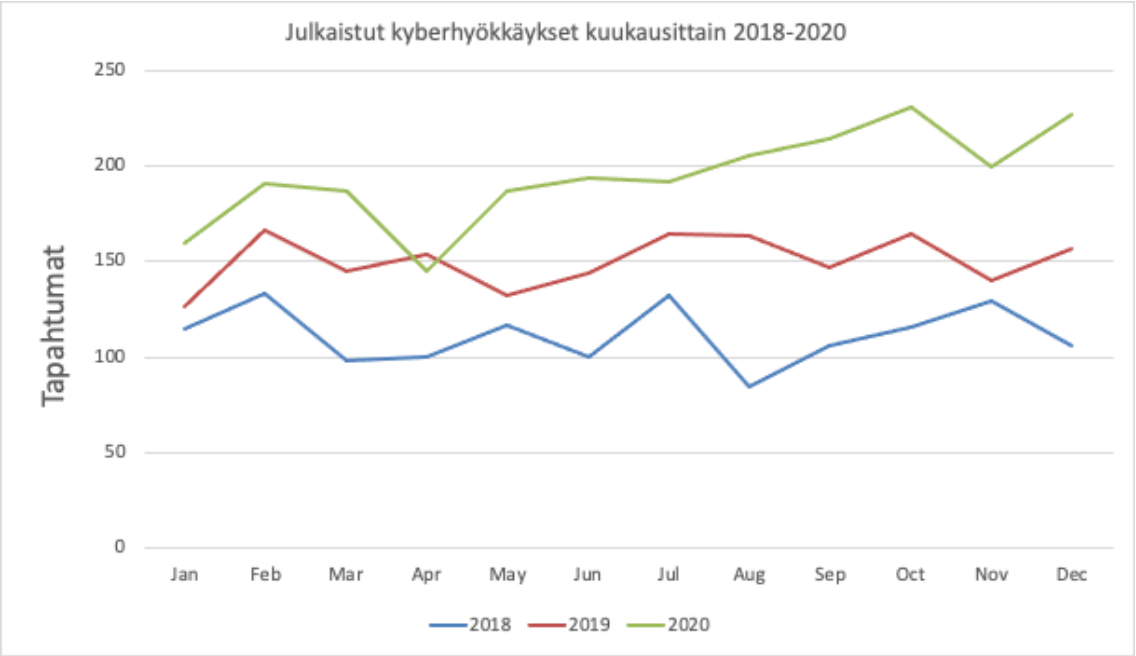
Yhdysvaltalaisen Cyberedge Group (2021) tuottaman tutkimuksen mukaan onnistuneiden kyberturvallisuushyökkäysten määrä kasvoi maailmassa eniten verrattuna vuosiin, jolloin sen aikaisemmat tutkimukset olivat tehty. Tutkimus edusti 17 Pohjois-Amerikkalaisen, Eurooppalaisen, Aasian ja Tyynenmeren alueen, Lähi-Idän Latinalaisen Amerikan ja Afrikkalaisen yrityksen, 19 eri toimialalta ja yli 500 työntekijän yritysten 1.200 IT turvallisuuden vastuuhenkilöiden näkemyksiä kyberturvallisuuden tilasta. Vuonna 2014 62 % yrityksistä ilmoitti joutuneensa onnistuneen kyberhyökkäyksen kohteeksi ja vuonna 2021 luku oli jo 86 % (kuvio 10). Kiristyshaittaohjelmista oli tullut rikollisille myös hyvin kannattavaa liiketoimintaa ja tutkimuksen mukaan 57 % kiristyshaittaohjelmien uhreiksi joutuneista yrityksistä oli maksanut lunnaita kiristyksen seurauksena. Yritysten uudet tietoturvainvestoinnit eivät kuitenkaan olleet kasvaneet samassa suhteessa ongelmien kasvuun nähden. Tietoturvainvestoinnit olivat edelleen kasvussa mutta kasvuvauhti oli hitaampaa kuin ennen ollen noin +5 % vuositasolla. Tutkimuksen mukaan yritykset käyttivät tietoturvan parantamiseksi yhä enenevässä määrin pilviratkaisuja. Vuonna 2020 36 % yrityksistä ilmoitti käyttävänsä tietoturvaan pilvisovelluksia ja -palveluita ja vuonna 2021 vastaava luku oli kasvanut jo 41 %:iin. Yritykset myös uskoivat joutuneensa yhä useammin tietoturvahyökkäysten kohteeksi. Vuonna 2014 62 % yrityksistä uskoi, että he eivät joudu seuraavan vuoden aikana onnistuneen tietoturvahyökkäyksen kohteeksi, kun vuonna 2021 vastaava luku oli enää 24 %. Tutkimus toteaakin, että tietoturva-alan ammattilaisia ei enää mitata vain kyvyistään estää kyberhyökkäyksiä, vaan myös kyvystä havaita, lopettaa ja korjata käynnissä olevat hyökkäykset. (CyberEdge Group 2021, 3.)



Kuvio 10: Vähintään yhden onnistuneen kyberhyökkäyksen kohteeksi joutuneet yritykset (tiedot: CyberEdge Group 2021, 7)

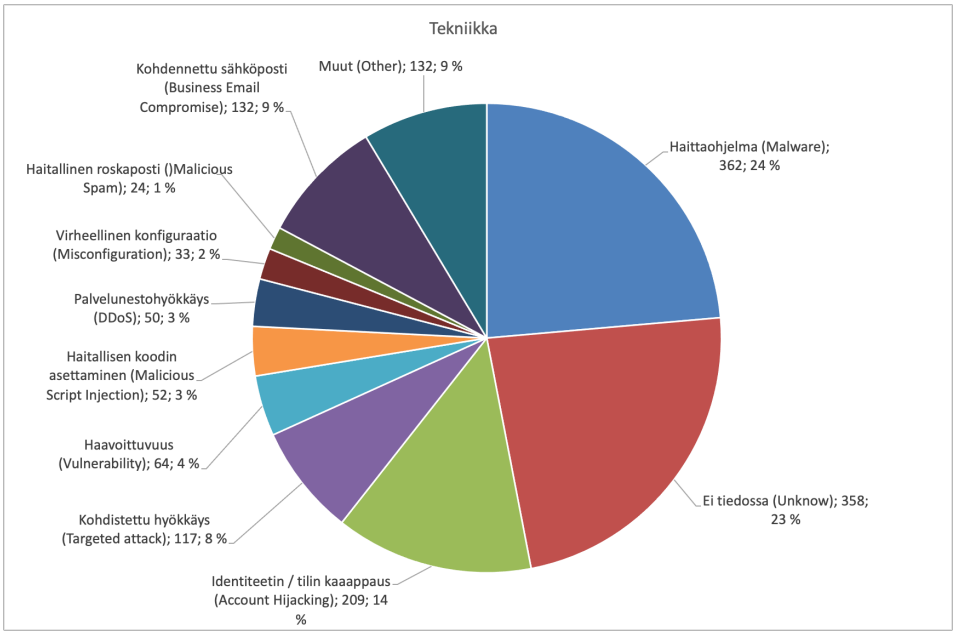
Kansainvälisen tietoturvayhtiön WithSecure Oyj (aiemmin F-Secure Oyj) mukaan rikollisten käyttämät menetelmät kehittyvät koko ajan ja tietoturvahyökkäykset tulevat jatkossa käyttämään yhä enemmän automaatiota. Tämä tarkoittaa sitä, että rikollisille organisaation tietojärjestelmissä olemassa olevien haavoittuvuuksien löytäminen helpottuu ja niiden hyödyntäminen nopeutuu entisestään. (F-Secure 2021.)

Passeri (2020) kerää tietoturvaan liittyvää tietoa avoimen lähdetiedon perusteella ja julkaisee säännöllisesti hackmageddon sivustollaan informaatioon perustuvia analyysejä. Kuvio 11 kuvaa kyberhyökkäysten määrän kasvua kuukausittain vuodesta 2018 alkaen. Informaation perusteella hyökkäysten määrä on kasvanut. (Passeri 2020.)



Kuvio 11: Julkaistut kyberhyökkäykset 2018-2020 (mukaillen Passeri 2020)

Kuviossa 12 Passeri (2020) on luokitellut tapahtuneita kybertekniikoita lähdemateriaalin perusteella. Vuoden 2020 tutkimuksen mukaan yleisin tapa (24 %) oli haittaohjelman asentaminen käyttäjän päätelaitteelle, yli 23 %:ssa tapa ei ollut tiedossa ja 14 %:ssa hyökkäys tapahtui ottamalla haltuun käyttäjän identiteetti.



Kuvio 12: Kyberhyökkäyksissä käytetyt tekniikat 2020 (mukaillen Passeri 2020)

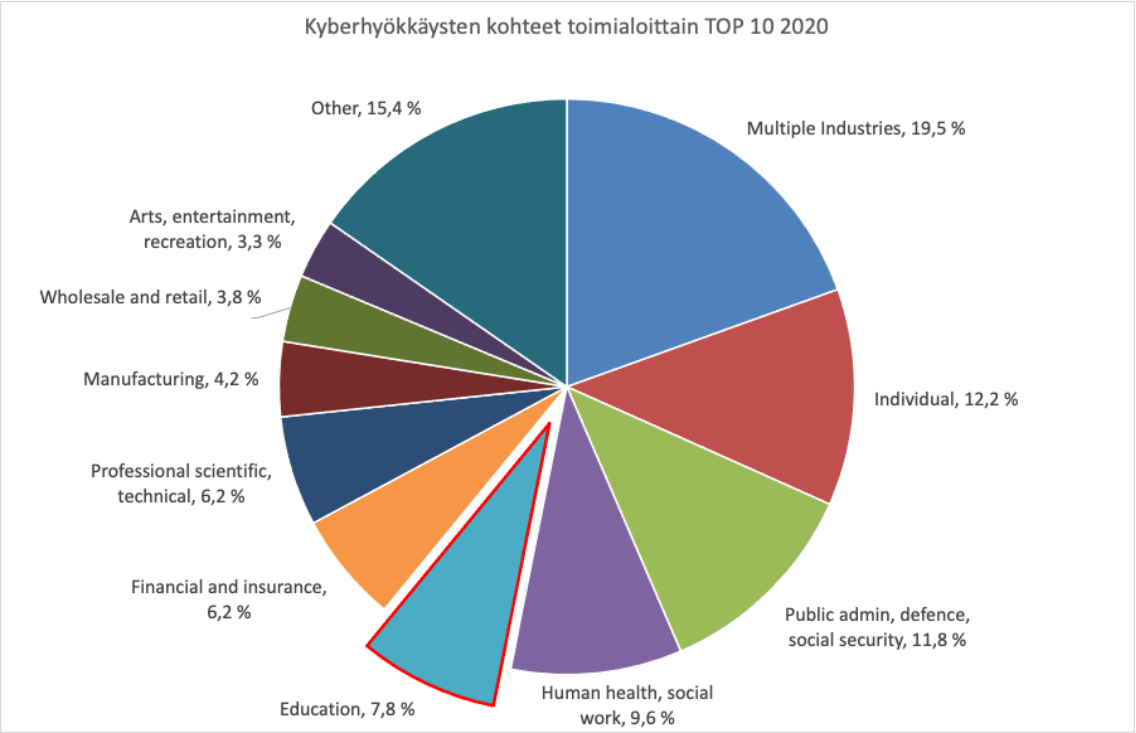
Suomessa Traficomin Kyberturvallisuuskeskus tuottaa yhteiskunnalle ajankohtaisia arvioita tietoturvatilanteesta ja yksi esimerkki tiedottamisesta ovat joka kuukausi julkaistavat Kybersää -tiedotteet. Niissä arvioidaan tietoturvan – ja suojan tilannekuvaa tietomurtojen, -vuotojen, huijauksien ja kalasteluiden, haittaohjelmien ja haavoittuvuuksien, automaation, verkkojen toimivuuden ja vakoilun näkökulmista. Tiedotteissa käsitellään ajankohtaisimpien uhkien lisäksi myös merkittävimpiä pidemmän aikavälin ilmiöitä. Tammikuussa 2023 top-5 ja 6kk - 2 v aikavälin kyberuhkiksi oli listattuna puutteet talouden ja politiikan ilmiöt, Suomeen kohdistuvat kyberympäristön uhkatason kohoaminen, puutteet tavanomaisissa torjuntatoimissa, toimitus- ja palveluketjujen tietoturva ja jatkuvuus ja kyberturvallisuusosaajien puute. Kyberturvallisuuskeskuksen helmikuun raportissa on käsitelty pidemmän aikajänteen, yli 5-vuotta, kybersään ilmiöitä. Keskus seuraa kuukausittain 12 eri ilmiötä ja kasvava tarve kyberosaajille nousee asiana myös siinä esille. (Kybersää Tammikuu 2023, 15; Kybersää Helmikuu 2023, 10.)

2.5 Kyberturvallisuuden tilannekuva opetustoimessa

Suomen opetustoimeen kohdistuneista kyberhyökkäyksistä on saatavilla esimerkiksi Kyberturvallisuuskeskuksen tai Opetushallituksen toimesta vain yksittäisiä tapaustietoja, joten tässä opinnäytetyössä tilannekuvaa muodostetaan kansainvälisen tutkimustiedon kautta.

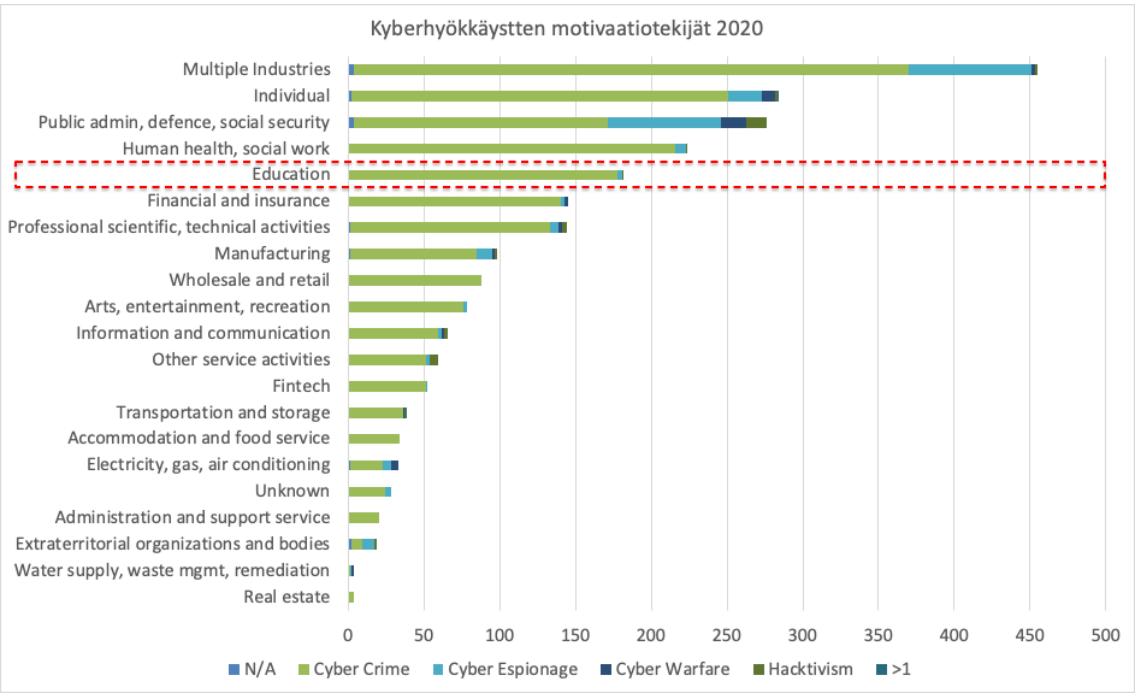
Yhdysvalloissa kolme neljäsosaa (¾) kaikista koulutukseen kohdistuneista tietomurroista kohdistuu korkeakouluihin. Yliopistot nostavat tietoturvariskit toiseksi suurimmaksi riskiksi seksuaalisen hyväksikäytön jälkeen. Lähes 90 % oppilaitoksista ei suojaa opiskelijoita ja opettajia tietojenkalasteluhyökkäyksiltä. Yhdysvaltojen liittovaltion poliisin FBI:n mukaan koulutuksen toimialaa koskeva kyberrikollisuus on myös jatkuvassa kasvussa ja Yhdysvalloissa toimiala arvioidaan vähiten kyberturvalliseksi toimialaksi. Yhtenä osoituksena tästä on, että korkeakouluilla on muun muassa kaikista korkein tulos mitattaessa löydettyjä kiristysohjelmia. Se on yli kolme kertaa enemmän kuin terveydenhuollossa ja 10 kertaa enemmän kuin finanssisektorilla on havaittu. Ennusteiden mukaan räätälöityjen hyökkäyksien määrä noin kaksinkertaistuu joka vuosi. Niitä vastaan on hyvin vaikea suojautua ja ne voivat aiheuttaa erittäin merkittäviä vahinkoja niiden kohteena oleville organisaatioille. (Povejsil 2021; Roger & Ashford 2015, 50–55.)

Passeri (2021) mukaan avoimien tietolähteiden kautta saadun tiedon perusteella vuonna 2020 opetustoimeen kohdistui eri toimialueista neljänneksi eniten (7,8 %) hyökkäyksiä jos myös yksilöihin kohdistuneet hyökkäykset huomioidaan (kuvio 13).



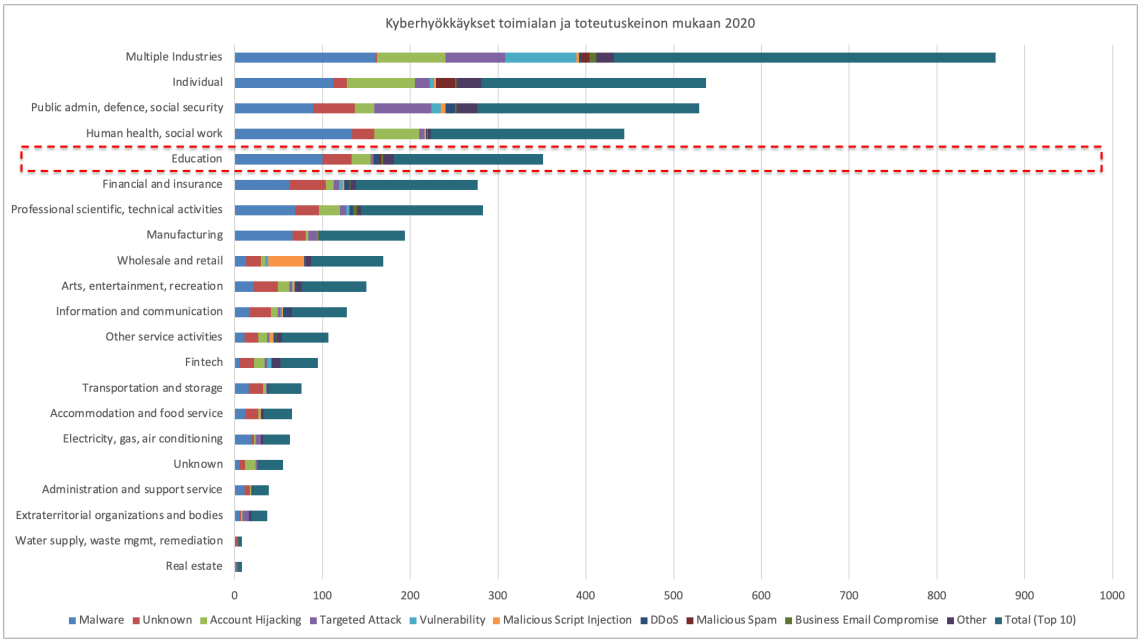
Kuvio 13: Kyberhyökkäysten kohteet toimialoittain TOP 10 2020 (mukaillen Passeri 2021)

Opetustoimeen kohdistuneissa kyberhyökkäyksissä oli suurin motivaatiotekijä (kuvio 14) saavuttaa taloudellisia hyötyjä (Passeri 2020).



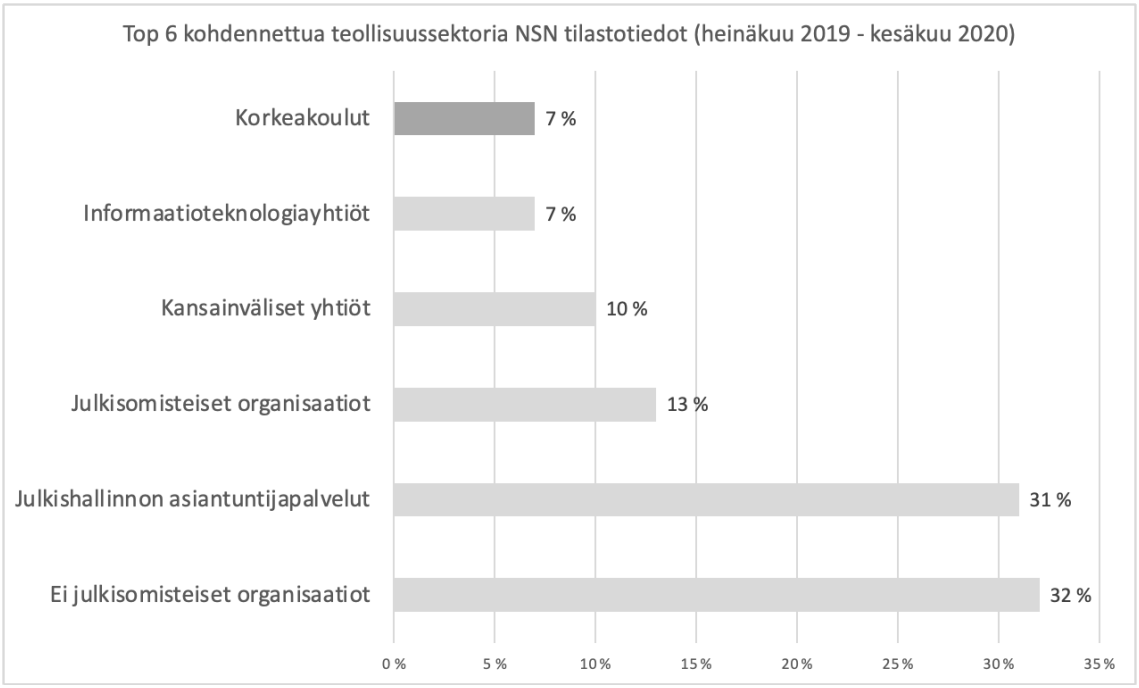
Kuvio 14: Kyberhyökkäysten motivaatiotekijä toimialoittain 2020 (mukaillen Passeri 2021)

Passeri (2021) on yhdistänyt toimialaan kohdistuneet hyökkäystavat (kuvio 15). Tilaston mukaan lähes 60 % opetustoimeen kohdistetuista kyberhyökkäyksistä tapahtuu käyttämällä jotain haittaohjelmaa.



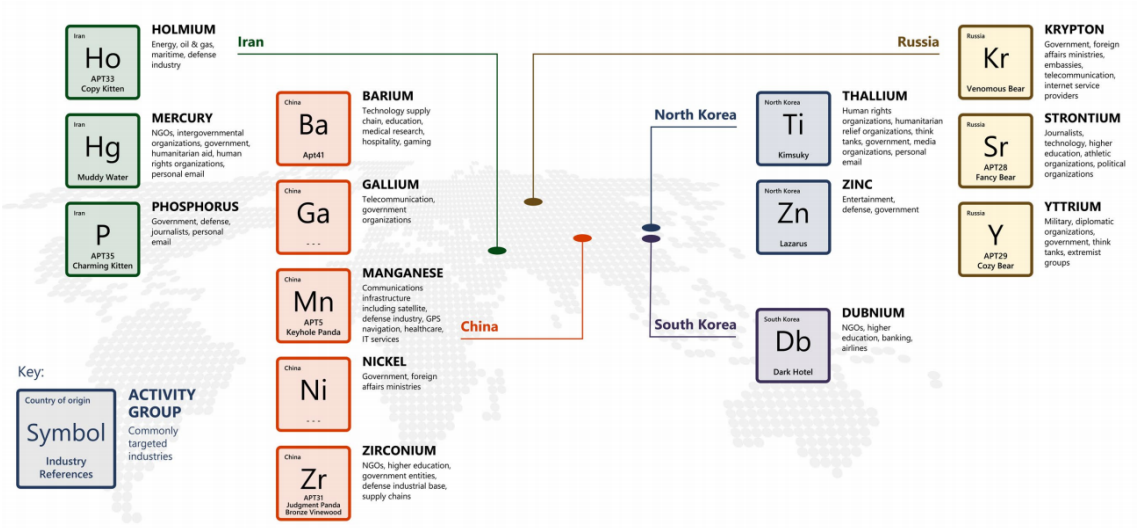
Kuvio 15: Kyberhyökkäysten toteutustapa toimialoittain 2020 (mukaillen Passeri 2021)

Microsoft seuraa asiakkaidensa pilvipalveluiden turvallisuutta ja tekee havaintojensa perusteella vuosittain Digital Defence raportin. Vuoden 2020 raportin mukaan korkeakouluopetukseen kohdistettiin maailman laajuisesti viidenneksi eniten kyberhyökkäyksiä eri teollisuuden aloilla (kuvio 16) ja usein taustalla oli kansallisen tason toimijoita. Rikollisia kiinnosti erityisesti korkeakoulut ja yliopistot, jotka tuottivat huippututkimusta. Microsoftin vastaavassa vuoden 2021 raportissa koulutuksen toimiala oli noussut vastaavassa toimialavertailussa jo neljännelle sijalle ja vuoden 2022 raportissa jo sijalle kolme. Huomioitavaa kuitenkin on, että Microsoft on käyttänyt eri vuosina hiukan erilaista toimialajaottelua. (Microsoft 2020, 41–47; Microsoft 2021, 53; Microsoft 2022, 35.)



Kuvio 16: Kuusi eniten kyberhyökkäyksiä kohdannutta teollisuussektoria (tiedot: Microsoft 2020, 47)

Microsoft kuvaa raportissaan erilaisia kybertoimijoita antamalla heille jalometalleja kuvaavan tunnisteen. Kuviossa 17 on Microsoft (2020) kuvannut erilaisten valtiollisten toimijoiden tyypillisimpiä kohteita. Kaikki raportissa mainitut toimijat kohdistavat kybertoimintaa hallinnon (government) alueille. Microsoftin (2020) mukaan näistä toimijoista korostuu erityisesti Venäläinen Strontium, joka oli raportin mukaan osallinen yli 63 %:ssa Microsoftin asiakkaisiin kohdistuneissa kyberhyökkäyksissä. Eniten opetustoimintaan ja koulutukseen kohdistuvia kyberpoikkeamia tunnistettiin tapahtuneen Venäjältä, Kiinasta ja Iranista. Vuoden 2022 raportille oli noussut myös Pohjois-Korea koulutukseen toimia kohdistaneiden kyberrikollisten joukkoon. (Microsoft 2020, 41–47; Microsoft 2022, 34.)



Kuvio 17: Sample of nation state actors and their activities (Microsoft 2020, 44)

Myös Microsoftin havaintojen perusteella koulutuksen toimiala on yksi eniten kiristyshaittaohjelmien kohteeksi joutunut toimiala. Microsoft (2022, 15) listaa koulutuksen, energian, finanssin ja valtiohallinnon toimialoiksi, joissa tapahtuu neljänneksi eniten kiristyshaittaohjelmien aiheuttamia häiriöitä.

StealthLabsin tutkimuksen mukaan Yhdysvalloissa opetukseen kohdistuu merkittävä määrä kyberturvallisuuteen liittyviä uhkia ja vahingontekoja. Heidän mukaansa yli 1.000 kouluun USA:ssa kohdistui kiristyshaittaohjelma vuonna 2019, käyttäjistä 30 % joutui tietojenkalastelun uhriksi ja tietoturvahäiriöistä 41 % liittyi sosiaalisen vaikuttamiseen kautta saatuihin tietoihin. Koulutuksen toimialalla todennäköisyys joutua tietojenkalastelun uhriksi oli yli kaksinkertainen verrattuna muihin aloihin. Raportin mukaan akateemisten koulutusalojen tiedosta (records) myös maksetaan rikollisilla markkinoilla (black markets) huomattavia summia ja niistä maksettavat summat olivat nousussa. StealthLabsin tutkimuksen päätelmien mukaan oppilaitoksiin kohdistuvat kyberturvallisuuden ongelmat nostivat vakavien taloudellisten ja maineeseen liittyvien vahinkojen todennäköisyyttä. (StealthLabs 2021.)

VMware selvitti vuosina 2016 ja 2018 kyselytutkimuksilla erityisesti UK:ssa toimivien yliopistojen kyberturvallisuuden tilaa. Vuonna 2016 VMware tutki, millaisia uhkia UK:n yliopistot kohtaavat ja miten ne voivat suojautua verkkohyökkäyksiltä sekä suojella aineetonta omaisuutta. Kysely suoritettiin haastattelemalla noin 50 yliopiston 75:ttä IT päättäjää. Tutkimuksen mukaan 87 % yliopistoista oli joutunut ainakin yhden onnistuneen kyberhyökkäyksen kohteeksi ja useampi kuin joka kolmas (36 %) yliopistoista oli havainnut vähintään yhden hyökkäysyrityksen joka tunti. Yliopistoista 83 % uskoi hyökkäysten määrän kasvavan tulevaisuudessa ja lähes kaksi kolmasosaa vastaajista (64 %) ei uskonut, että nykyiset IT kontrollit pystyisivät suojaamaan heitä kyberhyökkäyksiä vastaan seuraavien 12–18 kuukauden kuluessa. Yli neljäsosa (27 %) uskoi, että heidän tietokeskustensa turvallisuuden taso oli riittämätöntä ja se vaatisi

pikaista parantamista. Yliopistoista 85 % oli sitä mieltä, että IT:lle pitää osoittaa lisää taloudellisia resursseja, jotta se kykenee suojaamaan aineetonta omaisuutta. Tutkimuksen mukaan tietohyökkäysten uhka on kasvussa koko korkeakoulualalla ja IT-osastojen rooli tulee olemaan entistä tärkeämpi koulujen kasvun ja maineen suojaamisessa. (University Challenge: Cyber Attacks in Higher Education 2016, 5–6.)

VMwaren vuoden 2018 tutkimuksessa selvitettiin millaista tutkimustietoa hakkerit erityisesti haluavat. Heistä 54 % tavoittelee tieteellisen tutkimustyön tuloksia, 50 % kohdistaa mielenkiintonsa lääketieteeseen, 33 % turvallisuuteen ja puolustukseen ja 37 % talouteen. Kiinnostuksen kohteina saattaa olla muun muassa lääketieteen, ympäristöteknologian ja uusien valmistustekniikoiden sekä materiaaleja koskevat innovaatiot. UK:n yliopistoista 36 % uskoi, että tutkimustietojen päätyminen kyberrikollisille voi vaarantaa kansallisen turvallisuuden. Tutkimukseen osallistuneista yliopistoista 49 % kertoi, että heidän laitokseensa yritetään tehdä tietoverkkohyökkäys joko päivittäin tai useamman kerran viikossa ja vastaajista 97 % uskoi, että onnistunut kyberhyökkäys voi heikentää oppilaitosten mainetta. Tämä on hyvä huomioida varsinkin, kun oppilaitosten tulorahoituksesta yhä merkittävämpi osa tulee tutkimustyöstä elinkeinoelämälle. (University challenge: Protecting research in higher education 2018, 3–4.)

Kaupallisten yhtiöiden tutkimustöiden havaintojen lisäksi myös Dr John Chapman (2019) päätyy myös omassa artikkelissaan johtopäätökseen, että korkea-asteen koulutuksessa on välttämätöntä jatkuvasti arvioida ja parantaa tietoturvakyvykkyyksiä, jotta opiskelijat, henkilökunta ja arvokas tutkimustieto voidaan suojata kasvavalta hyökkäysuhalta (Chapman 2019, 6).

Suomessa Suojelupoliisi on esittänyt huolestumisensa korkeakouluissa tapahtuvasta vakoiluriskistä ja sen mukaan erityisesti Kiinaa koskeva riskitaso on kasvanut. Suurimman ulkomaalaisten opiskelijoiden ryhmän muodostaa kiinalaiset ja esimerkiksi jossain kouluissa myös opettajista lähes puolet tulevat kiinasta. Euroopassa onkin laajemmin herätty arvioimaan, millaisia uhkia ja riskejä Kiinan kanssa suoritettavaan korkeakouluissa ja yliopistoissa tehtävään tutkimustoimintaan liittyy. Tämän vuoksi esimerkiksi Suomessa ollaan laatimassa uutta toimintaohjetta turvallisuuden varmistamiseksi ja parantamiseksi. (Rantalainen 2021.)

3 Tietoturvavalvomo (SOC)

Tietoturvavalvomo (SOC) pääluku muodostaa tämän opinnäytetyön teoreettisen viitekehysten toisen, ja työn kannalta tärkeimmän osan. Kokonaisuutena teoria muodostaa viitekehyksen SOC:n perustamiseen ja käyttöönottoon. Jokaisen alaluvun alussa on lyhyt tiivistelmä luvun tarkoituksesta. Seuraavissa neljässä kappaleessa avataan lukijalle mikä SOC käsitteenä tarkoittaa ja mikä on sen keskeisin tehtävä, merkitys ja rooli tietoturvan suojaamisessa ja sen parantamisessa.

Suomenkielinen nimi SOC:lle on tietoturvavalvomo tai tietoturvahallintakeskus. SOC voidaan määritellä myös komentokeskukseksi, jossa kyberturvallisuuden ammattilaiset vastaavat liiketoiminnan kyberturvallisuuden monitoroinnista, analysoinnista ja suojaavat toimintaa kyberhyökkäyksiltä. (Kyberturvallisuuden sanasto 2018, 16.)

Nykyään SOC:sta näkee yleisesti käytettävän myös CSOC lyhennettä, joka tulee Cyber Security Operation Center. Erityistä virallista määritelmää CSOC:lle ei kuitenkaan vielä ole tehty. Tässä opinnäytetyössä käytetään vain SOC lyhennettä.

SOC:n keskeisin tehtävä on tuottaa turvallisuutta ja se on toiminto, joka on tarkoitettu kyberturvallisuuteen liittyvien hyökkäysten havainnointiin, torjuntaan ja raportointiin. Toimintona SOC on operaatiokeskus, joka sisältää sen toiminnan edellyttämät osaavat henkilöt, prosessit ja teknologiat turvallisuuspalveluiden tuottamiseksi. SOC:n voi perustaa joko yrityksen sisäisenä toimintona tai vaihtoehtoisesti ulkoistaa sen kokonaan tai osittain. SOC voidaan myös organisoida toimimaan osana yrityksen muuta organisaatiota. SOC voi valvoa yrityksen internetliikennettä, sisäistä verkkoa, palvelimia, tietokantoja, sovelluksia ja päätelaitteita kuten työasemia, mobiili- ja IoT laitteita. Usein kyberturvallisuuden valvontaa tehdään ympärivuorokautisella valvonnalla ja näin pyritään estämään mahdolliset organisaatiota uhkaavat kyberturvallisuuden ongelmat jo ennalta sekä tarvittaessa käynnistämään mahdollisimman nopeasti toimenpiteitä riskien mitigoimiseksi tai häiriöiden korjaamiseksi. SOC:lla tulee olla kyvykkyys käynnistää kaikki tarvittavat toimenpiteet uhkien torjumiseksi. SOC luo reaaliaikaisen tilannekuvan yrityksen tietoverkkojen toimintaan ja/tai toiminnan turvallisuuteen. SOC:n toimintamallin tulee perustua liiketoimintaan, jota se palvelee ja jolle se tuottaa palveluita. Liiketoiminnan koko ei määrittele tai rajaa tarvetta SOC:lle vaan jokaiseen liiketoimintaan kohdistuu erilaisia tietoturvauhkia kyberrikollisuudesta huonoihin IT:n toimintamalleihin. (Nathans 2021, 3; Muniz 2021, 2–3; van Os ym. 2017; Logpoint 2020; McAfee 2020.)

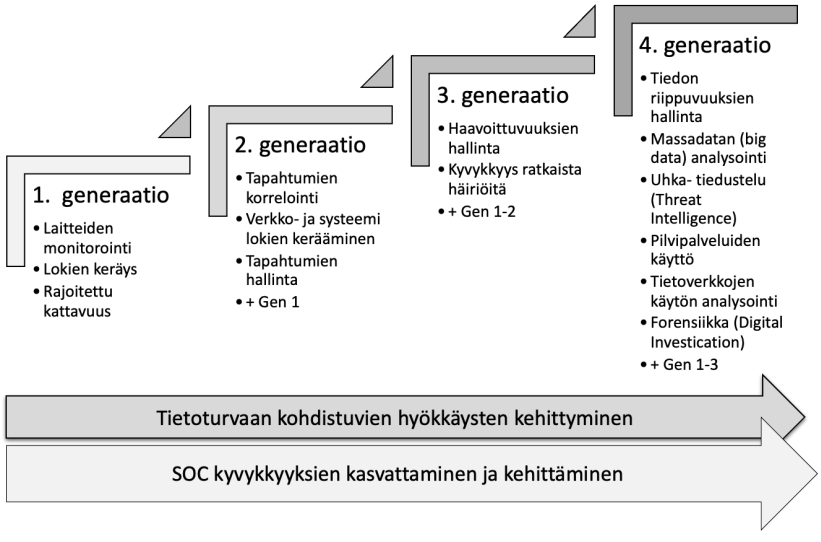
Toinen, edellistä määritelmää laajempi SOC:n kuvaus on määritellä sen tehtävä ja tarkoitus laajemmin toiminnoksi, jonka tehtävänä on suojata kaikkea sen vastuulle annettua omaisuutta. Omaisuus voi olla esimerkiksi materiaalia, aineettomia oikeuksia ja henkilöitä. Tämä lisäksi SOC:lle voidaan määritellä myös muita soveltuvia tehtäviä, kunhan sen perustehtävä,

turvallisuuden varmistaminen, ei vaarannu. Johtuen mahdollisuudesta käyttää SOC:a moniin, ensisijaisesti turvallisuuden, käyttötarkoituksiin onkin yrityksen panostettava erityisesti SOC:n vastuiden kuvaamiseen. IT ympäristöjen turvallisuuden valvonnan lisäksi SOC:a voidaan käyttää esimerkiksi kamera-, rikosilmoituslaitteiden, ilmastoinnin (HVAC), kulkuoikeuksien valvontaan, keskitettynä turvallisuuden yhteydenottopisteenä, kriisinhallintakeskuksena ja erilaisten turvallisuuden raporttien tuottajana. Tässä määritelmässä SOC:n turvallisuustoiminnan ulkopuolelle rajataan ainoastaan fyysinen turvallisuustyö kentällä, kuten vartiointi. (Jarpey & McCoy 2017, 11–12.)

3.1 Historia ja kehitysvaiheet

Tässä alaluvussa käsitellään SOC:n historiaa ja kehitysvaiheita, jotta lukija saa käsityksen, miten SOC toimintojen maturiteetti on kehittynyt ajassa. Eri maturiteettitasojen kautta lukija pyritään avaamaan SOC:a koskevan vaatimustason ja haasteiden kasvua eri vaiheissa. Maturiteettitasojen kautta lukija voi myös arvioida, millaisia palveluita SOC voi erimaturiteettitasoilla tuottaa ja millaista teknologiaa se tarvitsee palveluiden tuottamiseksi.

SOC konseptia on kehitetty yli 15-vuoden ajan ja sen kehitysversiot voidaan jakaa neljään eri evoluutiovaiheeseen, jossa seuraavaan vaiheeseen on aina lisätty edellisten vaiheiden opit ja kokemukset (kuvio 18). Kehittymisen taustalla on organisaatioiden liiketoiminnan tarpeiden muutos ja toiminnan yhä suurempi riippuvuus tiedosta sekä IT:stä. Vastaavasti erilaiset kyberturvallisuuden uhkakuvat ja rikollisten kyvykkyydet suorittaa tietoturvarikkomuksia ovat lisääntyneet ja kehittyneet. (Muniz, McIntyre & Alfardan 2016, 21–24.)



Kuvio 18: SOC neljä kehitysvaihetta (Muniz, McIntyre & Alfardan 2016, 21–24)

3.2 Toiminnan standardit, oppaat, viitekehykset ja kypsyysmallit

Tässä alaluvussa käydään läpi millaisia yleisiä tietoturvaan liittyviä standardeja, oppaita, viitekehyksiä ja kypsyysmalleja on olemassa. Nämä toimivat niin yleisen tietoturvan kuin SOC:a perustavankin teoreettisena tietoperustana ja hyvien käytäntöjen lähteenä.

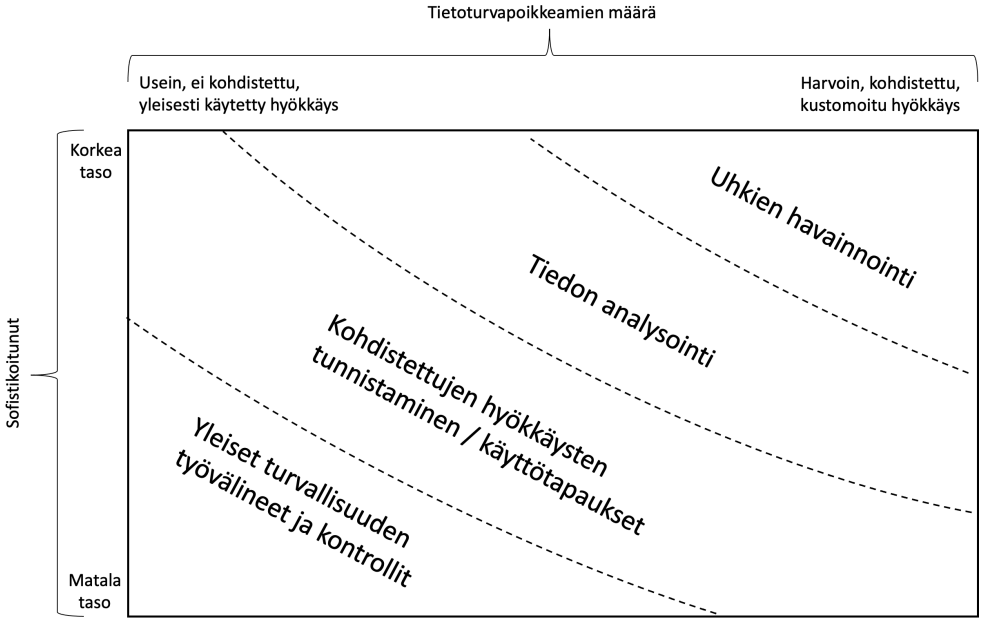
Tietoturvaa ja SOC toimintoja kehitettäessä voidaan hyödyntää erilaisia standardeja, oppaita ja viitekehyksiä. Yleisiä ja hyvä standardeja, ohjeita tai viitekehyksiä tietoturvapoikkeamien hallintaan löytyy esimerkiksi The National Institute of Standards and Technology (NIST) tekemä Cybersecurity Framework (CSF), FIRST.org tekemä viitekehys (FIRST Service Framework) ja International Organization for Standardization (ISO) organisaatiolta. Muita huomioitavia ohjeiden ja viitekehysten tuottajia ovat muun muassa SANS Intitute (SANS.org), Center for Internet Security (CIS) ja ISACA.org, jonka COBIT viitekehyksessä on useita tietoturvanhallintaan liittyviä suosituksia. Standardeja, oppaita ja viitekehyksiä kannattaa käyttää erityisesti silloin kun SOC:n kehitystyö aloitetaan tai halutaan nostaa nykyisen toiminnan maturiteettia. Käyttämällä valmiita malleja yritykset voivat saada etua, koska ne ovat tuotettu alan erityisasiantuntijoiden toimesta ja niiden toimivuus uhkien torjunnassa on testattu. Osa standardeista liittyy vahvasti johonkin toimialaan, kuten esimerkiksi PCI DSS (Payment Card Industry Data Security Standard), joka on tehty lisäämään maksukorttien käytön turvallisuutta. Toinen merkittävä etu mallien käytöstä on, että niitä käyttävien tahojen käsitteet ovat yhteneväisiä ja viestintä tehostuu. Usein malleja käytettäessä etua saadaan vaikka ne eivät olisikaan eri toimijoiden välillä samoja, koska erilaisten mallien välille on luotu valmiita oppaita niiden integroimiseksi. Haasteet ja ongelmat mallien käytössä liittyvät siihen, että ne päivittyvät melko hitaasti ja ne eivät ota riittävästi huomioon organisaatiokohtaisia erityispiirteitä ollen liian yleisellä tasolla kirjoitettuja suoraan käytettäväksi. Vahva suositus on, että malleja tulee käyttää mutta huolehtia myös omaan toimintaan liittyvien erityistarpeiden huomioimisesta. (Muniz 2021, 19–22.)

3.3 Käyttöönoton ja operoinnin viitekehyksiä

Tässä alaluvussa käydään läpi yleisellä tasolla millaisia SOC:n käyttöönottoon ja operointiin liittyviä viitekehyksiä on olemassa. SOC:n tehokkaaseen käyttöönottoon ja operointiin on kehitetty useita viitekehyksiä muun muassa Britannian The National Cyber Security Centre (NCSC), Gartnerin ja The Open Web Application Security Project (OWASP) toimesta.

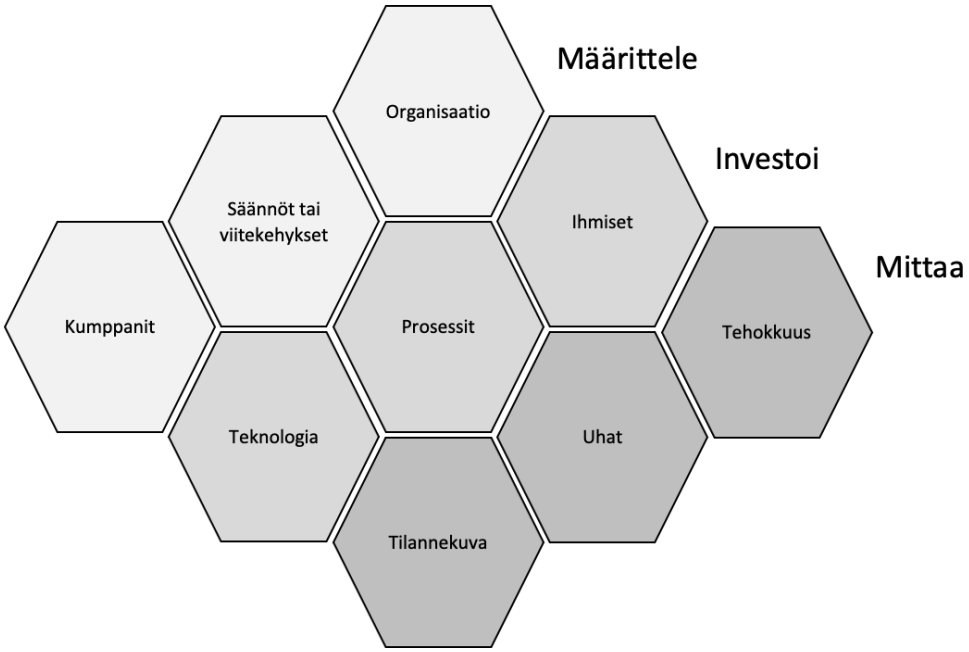
Britannian The National Cyber Security Centre (2022) opastaa, että SOC operointimalli tulisi jakaa kuuteen osa-alueeseen: (1) pilarit, joiden varaan SOC rakennetaan, (2) toimintoihin,

joita SOC tuottaa, (3) toimintamalliin miten SOC palveluita tuotetaan, (4) osaaviin resursseihin, (5) hallintomalliin ja (6) muihin huomioitaviin asioihin kuten jatkuvan kehityksen varmistamiseen, palvelutasoihin ja -aikoihin sekä SOC:n omaan turvallisuuden järjestämiseen. NCSC kuvaa oppaassaan myös, kuinka SOC:n operointiin tulevaa mallia tulisi kehittää. Kuviossa 19 kuvataan miten SOC:a perustava tai käyttöönottava taho voi arvioida millainen SOC:n kyvykkyystasotavoite olisi organisaatiolle asetettava verrattuna organisaation uhka-arvioon. (University challenge: Protecting research in higher education 2018.)



Kuvio 19: NCSC kykymatriisi (mukaillen The National Cyber Security Centre 2022)

Gartnerin SOC Target Operating Model Framework (SOCTOM) on erityisesti johdolle tarkoitettu työkalu SOC:n tavoitteiden asettamiseksi (Align), investoinnin määrittämiseksi (Invest) ja sen arvon mittaamiseksi (Measure). SOCTOM:a voi käyttää joko SOC:n rakentamiseksi tai sen jatkokehittämiseksi (kuvio 20). SOCTOM soveltaa Gartnerin toisen viitekehyksen, Gartner Information Security Function Operating Model (GISFOM) -käsitteitä ja siten sen kanssa yhdessä käytettynä tehostaa organisaation tietoturvan kehittämistä. (Collins 2021.)



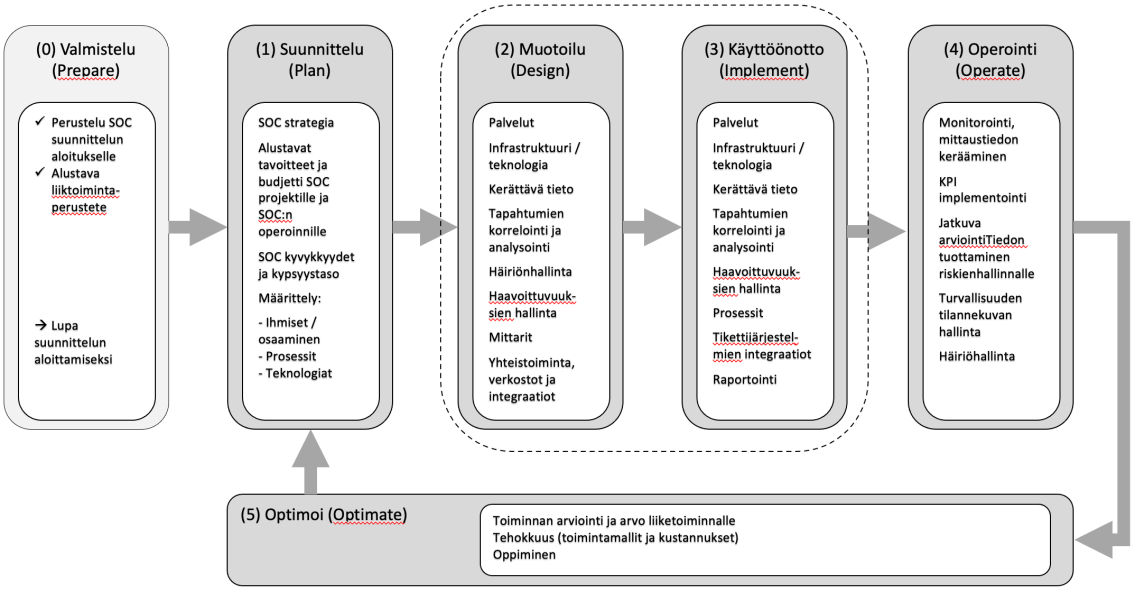
Kuvio 20: Gartnerin SOCTOM viitekehys (mukaillen Collins 2021)

Kolmas yleisesti SOC kehittämiseen käytetty viitekehys on The Open Web Application Security Project (OWASP) kehittämä malli. Se on viitekehys SOC strategian kehittämiseksi ja suunnittelemiseksi. Malli kattaa SOC:n perustamisen, käytön, johtamisen, hallinnan, parantamisen ja innovoinnin osa-alueet. Malli on saatavilla ilmaiseksi organisaatioiden käyttöön. Mallissa muun muassa verrataan erilaisten SOC toteutusstrategioiden etuja ja haasteita sekä kuvataan SOC palveluita. SOC:n perustamisstrategioita ovat keskitetty, hajautettu, itse tuotettu, kokonaan ulkoistettu, ulkoisen tiimin johtaminen tai näiden yhdistelmä eli hybridi. (OWASP 2019; SOC - Security Operations Centre Framework Project 2019, 3.)

3.4 Käyttöönoton metodologiat

Alaluvussa 3.5 kerrotaan lukijalle millaisia metodologeja SOC:n rakentamiseksi on olemassa. Metodologeja avaamalla pyritään avaamaan lukijalle, miten SOC:n voi käyttöönottaa.

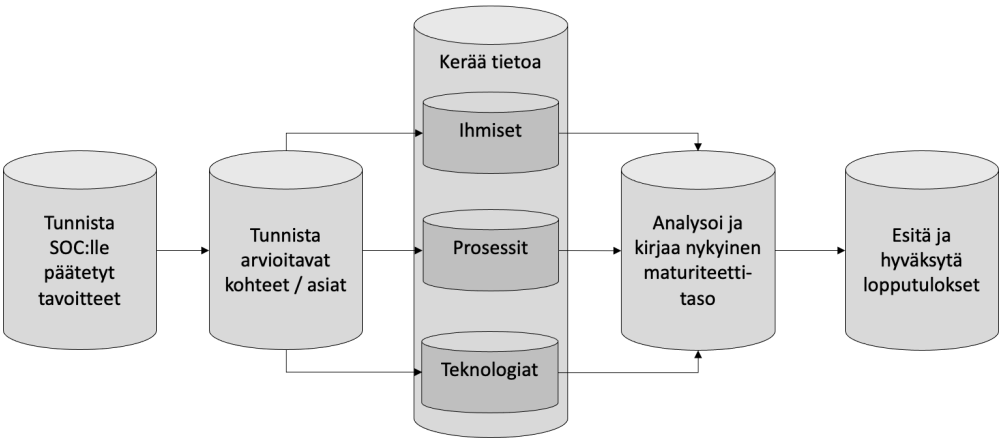
Cisco Systems Inc. asiantuntijat Muniz Joseph, McIntyre Gary ja AlFardan Nadhem kuvasivat vuonna 2016 julkaistussa kirjassaan Security Operation Center, Building, Operating, and Maintaining Your SOC, SOC:n käyttöönoton PPDIOO Lifecycle Approach to Network Design and Implementation metodologialla. Sen mukaan SOC käyttöönotto ja operointi voidaan jakaa viiteen vaiheeseen ja niitä edeltävään valmisteluun: (0) valmistelu, (1) suunnittelu, (2) palvelumuotoilu, (3) käyttöönotto, (4) operointi, (5) arviointi ja jatkuva kehittäminen (kuvio 21). PPDIOO tulee englanninkielisistä sanoista ”Prepare, Plan, Design, Implement, Operate, and Optimize”. (Muniz ym. 2016, II-VII; Cisco 2010.)



Kuvio 21: SOC:n rakentamisen vaiheet. (Mukaillen Cisco 2010; Muniz 2015; Muniz ym. 2016, 32)

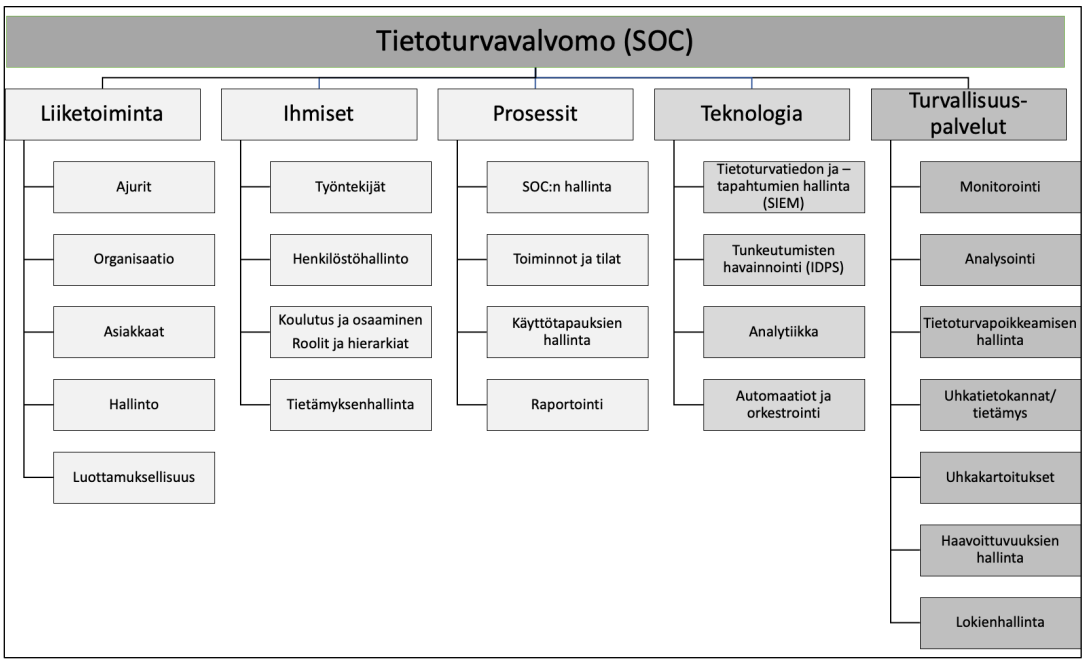
(0) Valmisteluvaiheessa perustellaan SOC:n arvo organisaation johdolle. Tämän vaiheen tavoitteena on ymmärryttää johdolle, millaisia uhkakuvia yrityksen toimintaan kohdistuu, perustella yrityksen johdolle miksi niiden proaktiiviseen torjuntaan kannattaa panostaa ja saada lupa tarkemman SOC suunnittelun aloittamiseksi. Yksi hyvä tapa on käyttää riskienarviointia, jonka avulla tietoturvauhkien vaikutusta ja niiden todennäköisyyttä voidaan käsitellä. Hyviä keskustelun aiheita voivat olla esimerkiksi millainen kyky organisaatiolla olisi nykytilassa havaita tietoturvapoikkeamia, ketkä havaintoja tekisivät ja miten niitä käsiteltäisiin, viestittäisiin sekä miten ne vaikuttaisivat yrityksen liiketoimintaan. (Muniz 2015.)

(1) Suunnitteluvaiheen tavoitteena on määritellä SOC:lle liiketoimintatavoitteet johdon näkökulmasta, tunnistaa organisaation olemassa kyvykkyydet, suorituskyky, hyväksyä seuraavaan vaiheen laajuus ja saada alustava hyväksyntä investoinnille. Suunnittelun ensimmäisessä vaiheessa tunnistetaan toiminnan ja IT tavoitteet SOC:lle. Organisaation turvallisuuden nykytila ja kyvykkyydet kartoitetaan, analysoidaan ja tiedon perusteella asetetaan vaatimustaso SOC:n tuottamalle turvallisuudelle. Vaiheen aikana kiinnitetään SOC:n liiketoiminta- ja IT-tavoitteet, tunnistetaan arvioitavat kohteet, kerätään tietoa yrityksen nykyisistä toimintamalleista (ihmiset, prosessit ja teknologia), analysoidaan kerätty tieto ja määritellään organisaation nykyiset valmiudet sekä esitetään vaiheen lopputulokset johdolle. Valmiuksien arviointiin tulee kiinnittää erityistä huomiota ja suorittaa se luotettavasti, sillä virheet tuottavat heikon SOC strategian. Kuviossa 22 on kuvattu Muniz prosessimalli valmiuksien arviointiin. (Muniz 2015; Muniz ym. 2016, 69–90.)



Kuvio 22: SOC maturiteetin arviointimetodologia (mukaillen Muniz ym. 2016, 70)

Oman SOC valmiuksien arviointiin voi myös käyttää esimerkiksi SOC-CMM:n julkaisemia itsearviointityökaluja. SOC-CMM luotiin pro gradu -tutkimusprojektina Luulajan teknillisen yliopiston (LTU) Master of Information Security -maisteriohjelmassa. Mallin luomisessa käytettiin Design Science Research -lähestymistapaa, jossa tieteellinen lähestymistapa yhdistetään käytännön testaukseen ja kokemuksiin käyttökelpoisen artefaktin, tässä tapauksessa kypsyyden arviointityökalun, luomiseksi. Mallissa SOC:n toimintaa arvioidaan liiketoiminnan, ihmisten, prosessien, teknologian ja SOC:n tuottamien palveluiden kautta (kuvio 23). Työkalua voi käyttää myös suunnitteluvaiheessa nykytilan määrittelemiseksi. (SOC-CMM 2021a; SOC-CMM 2021b.)



Kuvio 23: SOC-CMM itsearvioinnin työkalun viitekehys (mukaillen SOC-CMM 2021b)

Suunnittelun toisessa vaiheessa kuvataan myös turvallisuusasioiden johtaminen ja omistajuus organisaatiossa sekä laaditaan SOC strategia. Se muodostuu toiminta-ajatuksen (missio),

strategisten tavoitteiden, laajuuden, toimintamallin, palveluiden, valmiuksien kehittämisen tiekartan, keskeisten suorituskykyindikaattorien ja mittareiden kuvaamisesta. Strategian määrittely liittyy yhtiön tietoturvan johtamiseen ja on osa organisaatioiden hyvää hallintotapaa. SOC:n strategian kuvaaminen, hyväksyminen ja edistymisen seuraaminen ovat keskeinen osa hyvän hallintotavan mukaisten tietoturvan tavoitteiden saavuttamista ja kehittämistä. Toimintamallin osalta määritellään, tuotetaanko SOC erillisenä toimintona, virtuaalisesti vai hybridinä. Samoin määritellään miten SOC palveluita tuotetaan; sisäisesti vai ulkoisesti. Tarkemmalla tasolla muita SOC:n määrittelyyn liittyviä asioita ovat muun muassa tarvittavat teknologia-, metodologia-, infrastruktuurivalinnat, tapahtumien ja haavoittuvuuksien hallinta, ihmiset, prosessit, siirtyminen toiminnan käynnistämiseen, herätteiden ja häiriöiden käsittely sekä toiminnan jatkuva kehittäminen. Suunnitteluvaiheen lopputuloksia ovat SOC:n tehtävänkuvaus, strategiset tavoitteet, soveltamisala, toimintamalli, palvelut, valmiuksien kehittämisen tiekartta, keskeiset suorituskykyindikaattorit (KPI) ja mittarit. (Muniz ym. 2016, XX-XXI, 91–101; Muniz 2021, 164.)

(2–3) Muotoilu- ja rakennusvaiheet liittyvät lähes saumattomasti toisiinsa. Muotoiluvaiheessa alustavat suunnitelmat konkretisoidaan projektisuunnitelmaan, tavoitteiden saavuttamiseksi tarvittavat teknologiat valitaan ja rakennusvaiheessa suunniteltu projekti toteutetaan. SOC:n projektisuunnitelman tulee olla yhdenmukainen alkuperäisten liiketoimintavaatimusten kanssa määritettyjen laajuuden, kustannusten ja resurssiparametrien osalta, jotta ennalta päätetty validi liiketoimintaperuste SOC:lle on edelleen olemassa. Muotoilu- ja rakennusvaiheessa vaiheessa ratkaistavia asioita ovat muun muassa SOC:n tarvitseman teknologian käyttöönotto. Tyypillisesti tietoa kerätään SOC:n käyttöön erilaisista tietoturva- ja tapahtumahallintaratkaisuista kuten haittaohjelmien torjuntajärjestelmistä, palomuureilta ja tietojärjestelmien lokitapahtumista. Tieto kerätään ja käsitellään tietoturvatapahtumien hallintajärjestelmässä (SIEM). SIEM:n avulla SOC-analyytikot voivat korreloida ja arvioida tapahtumia ja saada suuremman kuvan organisaation nykyisestä suojaustilasta. Riippuen SOC:lle määrittelyvaiheissa kuvattujen tavoitteiden mukaisesti muotoilu- ja rakennusvaiheissa voidaan ottaa käyttöön myös muuta teknologiaa. Esimerkkejä SOC:n palveluista on haavoittuvuuksien hallinta ja tunkeutumisen havainnointi. Näihin molempiin on useita erilaisia järjestelmiä. (Muniz, J. 2015; Muniz ym. 2016, 85–93, 132–136.)

Muotoilu- ja rakennusvaiheissa ratkaistaan monta muutakin asiaa. SOC:ia perustavan työlistalla saattaa olla teknisten työkaluvalintojen ja käyttöönottojen lisäksi muun muassa SOC:ssa tarvittavien asiantuntijoiden palkkaus, fasiliteettien perustaminen, tietoturvapolitiikkojen, prosessein määrittely, olemassa olevan teknologia-arkkitehtuurien huomioiminen. SOC:n tulee ymmärtää esimerkiksi, miten identiteetinhallinnan järjestelmät, tietoverkot, järjestelmät ja tieto ovat segmentoitu. Työlistalla on myös SOC:n raportointi ja tietovarastojen tarpeiden ratkaiseminen. (Muniz, J. 2015; Muniz ym. 2016, 95–99, 101–113, 114–119, 126, 140–144.)

(4) Operointivaihe sisältää tietoturvan tilannekuvan ja turvallisuuden ylläpitämisen. SOC vastaanottaa tietoturvaan liittyviä tapahtumia, arvioi tapahtumiin liittyvää tietoa, monitoroi tietoturvan tilaa organisaatiossa ja käsittelee tapahtumia. Operointivaiheessa SOC käyttää suunnitteluvaiheessa luotuja ja käyttöönottoprojektissa testattuja erilaisia prosesseja, käyttötapauksia ja skenaarioita. Yksi skenaario voi olla esimerkiksi, miten SOC toimii tietyntyyppisen haittaohjelman havaitessaan. Operointivaiheessa SIEM:iin kerätään ja siellä korreloidaan tietoa muista tietoturvatyökaluista, kuten palomuureista, sisältösuodattimista, tunkeutumisen havaitsemis- / estojärjestelmistä ja muista lokilähteistä. Osa tapahtumista kirjataan varsinaisiksi liiketoimintaan negatiivisesti vaikuttaviksi tietoturvapoikkeamiksi eli häiriöiksi ja kirjataan häiriöraporteiksi. Operointivaiheessa SOC on implementoitu osaksi muuta organisaatiota ja sidosryhmiä, joita tietoturvaongelmien selvittämisessä ja hallinnassa tarvitaan. Näitä toimijoita voivat olla esimerkiksi tieto-omaisuuden (assets) omistajat ja käyttäjät, riskienhallinta, järjestelmien ja tietoverkkojen pääkäyttäjät, palvelupiste, päätelaitteiden pääkäyttäjät/ylläpitäjät, viestintä, HR, lakiasiat ja muut turvallisuustiimit. (Muniz ym. 2016, 347–363.)

Kun SOC on otettu käyttöön, viimeisessä vaiheessa (5) tarkastellaan SOC: n toiminnan onnistumista ja tunnistetaan parannettavia alueita. Tämä tapahtuu arvioimalla, kuinka hyvin SOC on täyttänyt sille asetetut tavoitteet ja onko se kyennyt tuottamaan sitä arvoa liiketoiminnalle, jota varten se on perustettu. Arviointia varten tulee määritellä arvioinnin laajuus, arviointiin osallistuvat henkilöt, menetelmä, jolla arviointi tehdään ja kuinka usein arviointi tehdään. Yksi tapa tehdä SOC:n toiminnan arviointia, on tehdä se välittömästi sen jälkeen, kun tietoturvapoikkeama on selvitetty. Näin varmistetaan, että asiat ovat kaikkien tuoreessa muistissa. Toimintaa tehostavat alueet tulee kirjata, priorisoida ja niiden toteutumista on seurattava. SOC:n suunnitteluvaiheessa asetettuja tavoitteita ja niiden etenemistä (KPI) tulee seurata säännöllisesti, esimerkiksi neljännesvuosittain. Mikäli tavoitteita ei saavuteta, se voi olla indikaatio resurssien puutteesta, toimimattomista prosesseista tai teknologiasta. (Muniz, J. 2015.; Muniz ym. 2016, 365–395.)

Nathans D on kuvannut kirjassaan SOC:n perustamisen ja kehittämisen mallin (kuvio 24), jolla SOC:n kasvu ja kyvykkyyksien kasvattaminen voidaan toteuttaa, riippumatta siitä onko se yrityksen sisäinen tai ulkoistettu, viiden vaiheen kautta: teknologia, organisaatio, politiikka, operointi ja tiedustelu. (Nathans 2021, 8–10.)

Kuvio 24: SOC kehitysvaiheet (mukaillen Nathans 2021, 8–10)

Teknologia -vaiheessa tunnistetaan millaisia turvallisuuden hallintaa liittyviä järjestelmiä ja resursseja yrityksellä on jo käytössään ja miten turvallisuuden osalta vastuut on määritelty. Tämän vaiheen pääasiallisena tarkoituksena on kuvata nykytilaa ja tehdä havaintoja mahdollisista uusista tarpeista halutun turvallisuustason saavuttamiseksi. (Nathans 2021, 8.)

Organisaatio -vaiheessa organisaation nykyiset turvallisuuden järjestelmät siirretään turvallisuusorganisaation vastuulle ja käyttöön sekä niiden käyttö koulutetaan. Tyypillisesti tämä on vaihe voi olla hyvin vaikea ja tunnepitoinen. Muutosvastarintaa esiintyy, koska osa henkilöstöstä saattaa kokea heidän omien vastuidensa vähenemisenä. Vaihe kannattaa suunnitella hyvin, jotta organisaation tuki uudelle perustettavalle SOC:lle varmistetaan. (Nathans 2021, 9.)

Politiikka -vaiheessa tehdään kaksi asiaa: katselmoidaan olemassa olevat turvallisuuspolitiikat ja siirretään politiikkojen kehitystyö SOC:lle määriteltyjen vastuiden mukaisesti. Politiikkojen katselmoinnin yhteydessä on suositeltavaa tehdä tarvittavat päivitykset niihin. Mikäli politiikkoja ei ole vielä tehty lainkaan voi mallia hakea esimerkiksi ISO/IEC 27002 standardista mutta myös muiden samalla alalla toimivien organisaatioiden politiikoista. Usein yritykset vaihtavat mielellään tämän tyyppistä tietoa keskenään. Yksi politiikka -vaiheen tärkeimmistä päivitettävistä politiikoista siihen liittyvine proseduureineen on viestintä. SOC tarvitsee selvät ohjeet, miten ja kenelle turvallisuuden häiriötilanteista tiedotetaan. Lopuksi politiikka -vaiheen lopputulokset tulee hyväksyttää yrityksen ylimmässä johdossa (senior management) ja tiedottaa ne sidosryhmille. (Nathans 2021, 9–10.)

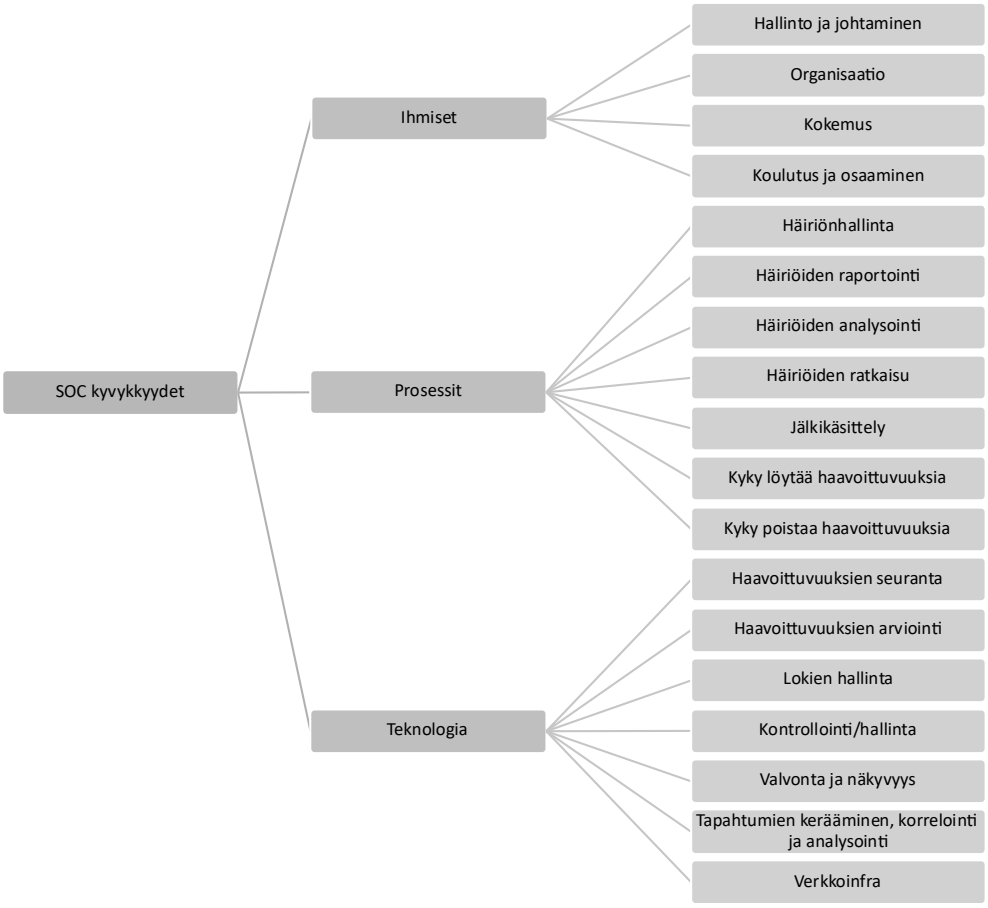
Operointi -vaiheessa SOC alkaa tuottamaan palveluitaan. Turvallisuuden järjestelmät on konfiguroitu, niitä ylläpidetään, prosessit ovat toiminnassa ja turvallisuutta valvotaan aktiivisesti. SOC:n vastuulle kuuluu myös alihankkijoiden turvallisuudenvalvonta, esimerkiksi turvallisuuteen liittyvien päivitysten suorittaminen palvelutasosopimusten mukaisesti. Tässä vaiheessa tyypillisesti myös eri toimijoiden väliset tiketöintijärjestelmät ja muut tilannekuvaa viestivät järjestelmät sekä prosessit integroidaan osaksi SOC:n työkaluvalikoimaa. (Nathans 2021, 10.)

Viimeisessä vaiheessa, jota voidaan kutsua tiedustelu- tai tiedonvaihtovaiheeksi, SOC pystyy käsittelemään ulkoisista tietolähteistä saatua informaatiota ja hyödyntämään sitä oman yrityksen tietoturvan tilannekuvan muodostamiseksi. Tavoitteena on saada yrityksen ulkopuolelta tietoa, jota analysoimalla estetään mahdolliset tietoturvapoikkeamat jo ennakolta. (Nathans 2021, 10–11.)

3.5 Kyvykkyydet

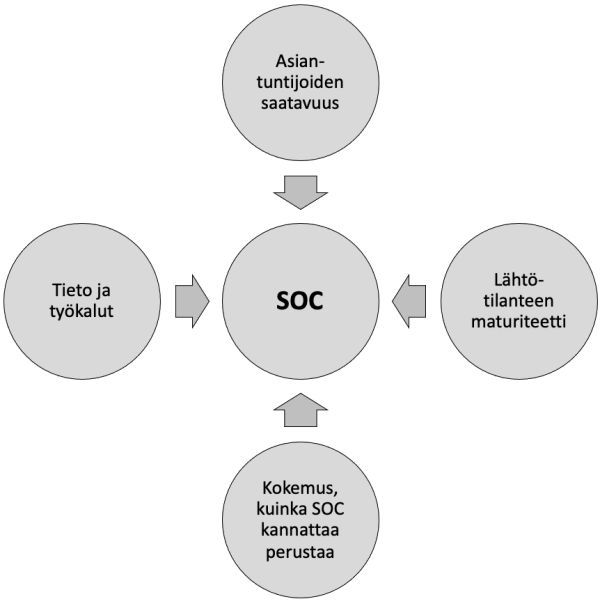
Tässä luvussa kerrotaan lukijalle millaisia kyvykkyyksiä SOC tarvitsee toimiakseen. Tavoitteena on avata lukijalle millaisia kyvykkyyksiä SOC:a käyttöönotettaessa joko tulee olla olemassa tai ne tulee kehittää käyttöönoton aikana.

Toimiakseen tehokkaasti SOC tarvitsee useita kyvykkyyksiä (kuvio 25). Niitä on useita ja SOC:n strategin kyvykkyyksien kehittämisen tiekartassa määritellään, miten niitä systemaattisesti lähdetään kasvattamaan SOC:n perustamisesta lähtien. (Muniz ym. 2016, 99–100.)



Kuvio 25: SOC kyvykkyydet (mukaillen Muniz ym. 2016, 100)

Perustettaessa SOC:a kohdataan tyypillisesti neljä haastetta (kuvio 26): (1) kyvykkyyksien ja asiantuntijoiden saavuus, (2) alhainen maturiteetti, (3) tiedon saamiseen liittyvät rajoitteet ja puutteet ja (4) kyky perustaa ja kehittää SOC palveluita (Muniz 2021, 152–154).



Kuvio 26: SOC käyttöönoton haasteet (Muniz 2021, 152–154)

Kyvykkyysien saatavuuden ratkaisu ja niiden kehittäminen on SOC:a käyttöönottavalle suuri haaste. Alkutilanteessa on puutteita osaavista resursseista, politiikkoja, toimintamalleja, prosesseja ja ohjeita ei joko ole tai ne tulee päivittää, pääsyä tietolähteisiin ei ole, työkaluja ei ole implementoitu ja kokemustakin, miten SOC kannattaa perustaa ei ole. Organisaatiossa uudet vastuut ja vanhoista luopuminen voi aiheuttaa muutosvastarintaa ja turvallisuuskulttuuriakin pitää kehittää. (Muniz 2021, 152–154.)

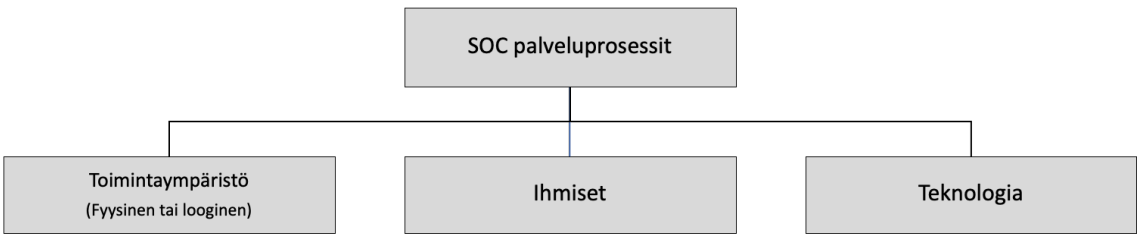
Ensimmäinen haaste, kyberturvallisuuden osaajien saatavuus, on (ISC)2 vuonna 2020 tekemän tutkimuksen mukaan globaali ongelma. Erityisesti osaajapulaa on SOC palveluiden tuottamiseksi vaadittavissa forensiikassa, haittaohjelmien analysoinnissa ja uhka-arvioiden teossa. SOC tarvitsee luotettavat ja osaavat ihmiset, joten taustaselvityksiin on kiinnitettävä erityistä huomiota. Rekrytoinneissa on varmistuttava palkattavien henkilöiden riittävästä osaamistasosta ja osaamisen laajuudesta. Samoin tulee ratkaistavasti normaaleja työsuhdekysymyksiä, kuten SOC:n henkilöjohtaminen, palkka-, työntekopaikka- ja aikakysymykset. ((ISC)² 2020, 14–17; Muniz 2021, 152–153, 155.)

Toinen haaste on, että SOC:n käynnistysvaiheessa sen maturiteetti on tyypillisesti alhainen. SOC tarvitsee osaavan henkilöstön lisäksi toimivia proaktiivisia ja reaktiivisia palveluita, prosesseja ja työtiloja. Vaarana on, että liiketoiminta ei saa SOC:sta riittävän nopeasti arvoa ja sen tehtävät annetaan organisaatiossa muualla hoidettavaksi. Tätä riskiä voi esimerkiksi pienentää testaamalla SOC:n toimintaa riittävästi ennen käyttöönottoa tai käyttämällä ulkoisia SOC toimittajia käyttöönoton valmistelussa ja oppimalla toimintaa heiltä. (Muniz 2021, 153.)

Kolmas haaste liittyy SOC:n mahdollisuuksiin saada tietoa ja puutteisiin työkaluissa, joilla se tietoa käsittelee. Ongelmana voi olla esimerkiksi, kuinka SOC saa tietoa prosesseista tai ongelmista tietoverkoissa. Ongelmana voi myös olla, että SOC:lla ei ole teknologiaa eristää haittaohjelmia (sandboxes), sovellus- ja käyttäjätietoisia palomuureja tai kykyä analysoida sovelluskerroksen (Layer 7) tason tietoa. Hyvä on kuitenkin muistaa, että jokaisella SOC:lla on puutteita tarvittavissa teknologioissa. Hyvä riskienhallinta auttaa valitsemaan ne työkalut, joista on suurin hyöty yritykselle. (Muniz 2021, 153.)

Neljäs haaste on SOC:a käyttöönottavien tahojen kokemuksen puute käynnistää ja kehittää SOC:n kyvykkyyksiä, erityisesti teknisiä. SOC tukipalvelua ei voi tuottaa ilman teknologiaa. SOC:lle on mahdollistettava itsenäinen pääsy turvallisuuspalveluiden tuottamisessa tarvittavaan tietoon ja järjestelmähallintaan. Suositus on, että SOC:n käyttämät teknologiat eriytetään niin fyysisellä kuin loogisella tasolla muun organisaation käyttämästä teknologiasta. Näin SOC pidetään toimintakykyisenä tilanteissa, joissa organisaatioon on kohdistunut kyberhyökkäys ja SOC kykenee sekä puolustamaan että suojelemaan sitä. (Nathans 2021, 158.) Markkinoilla on useita oppaita, kuinka rakentaa SOC:n tekniset palvelut mutta ne harvoin, jos ollenkaan käsittelevät ja vertailevat kaupallisia ja avoimen lähdekoodin (open source) vaihtoehtoja. SOC palvelua kehittävän on vaikea tehdä luotettavaa liiketoiminta-arviota (business case) siitä kumpaa mallia; ostamalla valmis kaupallinen tekninen ratkaisu vai kehittämällä omilla resursseilla oma ratkaisu, saavutetaan parempi lopputulos. Mikäli ei tiedä kuinka palvelu kannattaa rakentaa, suositus on käyttää suunnitteluun kyvykästä ulkoista toimittajaa. Toinen hyvä tapa on perehtyä asiaan erilaisissa kyberturvallisuuden seminaareissa kuten RSA, Blackhat, DEFCON, SecureWorld ja SANS. Hyviä tietolähteitä ovat myös FIRST Computer Security Incident Response Team (CIRT) Services Framework ja NIST Cybersecurity Framework (CSF). (Muniz 2021, 154.)

Alussa myös toimivien prosessien ja työtilojen puuttuminen on ongelma. SOC tietoturvapalveluita tuotetaan prosessilla, joita käyttävät osaavat ihmiset tietyssä toimintaympäristössä ja tietyillä teknologiolla (kuvio 25). Jokaisella näillä on erilaisia kyvykkyyksiä ja kyvykkyyksillä erilaisia kypsyys- eli maturiteettitasoja. Kyvykkyydet ja niiden maturiteettitasot vaikuttavat siihen, kuinka hyvin ja tehokkaasti SOC voi toimia. (Nathans 2021, 155.)



Kuvio 27: SOC tukipalveluiden rakenne (mukaillen Nathans 2021, 155)

Toimintaympäristöllä tarkoitetaan joko fyysistä tai loogista ympäristöä, jossa SOC toimii. SOC voidaan sijoittaa maantieteellisesti yhteen taikka useampaan lokaatioon, se voi sijaita organisaatiossa yhdessä tai useammassa tiimissä ja sen toimintamalli voi olla sisäinen, kokonaan ulkoistettu tai hybridi. Oleellista on, että SOC:n toimintakyky pitää turvata ja varmistaa silloin kun organisaatiota vastaan on kohdistunut kyberhyökkäys. Ratkaistavia asioita ovat esimerkiksi SOC:n tilojen riittävien turvatasojen määrittely ja sen oman toiminnan jatkuvuuteen varmistaminen esimerkiksi virransyötön häiriötilanteissa. SOC saattaa tarvita asiantuntijoilleen muusta toiminnasta eriytetyt työpisteet, tiimityötilat ja laitetilat. (Nathans 2021, 155.)

3.6 Palvelut

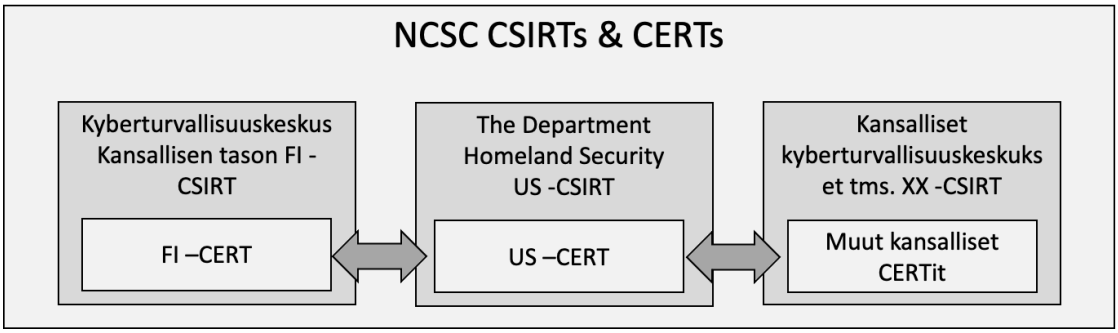
Tässä luvussa kerrotaan lukijalle millaisia palveluita SOC voi tuottaa. Tavoitteena on avata lukijalle, että eri SOC:t voivat tuottaa hyvinkin erilaisia palveluita ja myös eri lailla organisoituen. Palvelut ovat luvussa esitelty ryhmiteltynä palvelualueisiin ja jokaisen palvelualueen esittelyalussa on myös lyhyesti kerrottu palvelualueen keskeinen tarkoitus ja sisältö.

Muniz (2021) kuvaa SOC:n palveluiksi riskien, haavoittuvuuksien, poikkeamien (incidents), vaatimusten mukaisuuden hallinnan, tapahtumien analysoinnin, digitaalisen forensiikan, tilannekuvan ja tietoturvan tutkimuksen ja kehityksen. SOC palveluprosesseiksi OWASP:ssa listataan muun muassa kyberturvallisuustilanteen monitorointi ja tapahtumien havainnointi, poikkeamiin reagointi, uhkien ja haavoittuvuuksien hallinta ja laadun sekä jatkuvan kehityksen hallinta. (Muniz 2021, 162; SOC - Security Operations Centre Framework Project 2019, 12.)

Yleisesti SOC:n palvelut voidaan määritellä valikoimana niitä turvallisuuspalveluita, joilla se tuottaa arvoa organisaatiolle. Markkinoilta SOC palveluita on jo saatavilla usealla tuotantotavalla. Service as a Service (SaaS) tyyppisesti palveluita voi hankkia esimerkiksi lokien keräämiseksi, tietojärjestelmien muutosten valvomiseksi ja uhkien tai tapahtumien tiedottamiseksi asiakkaille. Organisaation SOC palveluiden tuottaminen voidaan myös jakaa useammalle toimittajalle. Tällöin esimerkiksi yksi tai useampi toimittaja voi tuottaa operatiivisia SOC palveluita ja toisten SOC toimittajien kanssa kehitetään palvelua. Eniten merkitsee se, kuinka SOC saavuttaa sille asetetut tavoitteet, ei se kuinka monessa paikassa palvelua tuotetaan tai kuinka monesta paikasta sitä ostetaan. Palvelut kannattaa hankkia sieltä, missä on paras maturiteetti tuottaa niitä – näin saavutetaan tehokkaasti toimiva SOC. (Muniz 2021, 150.)

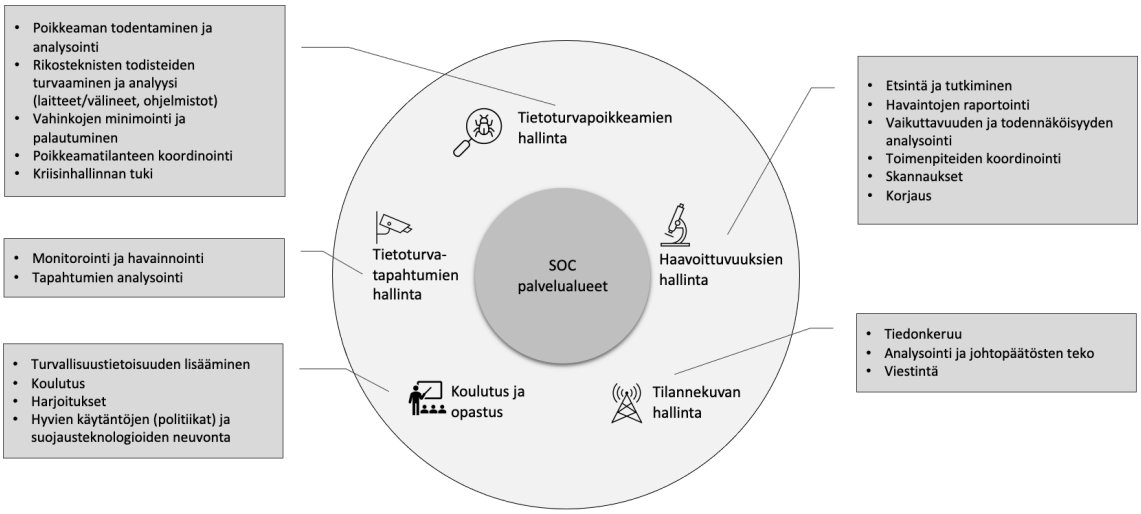
SOC:a perustettaessa ja markkinoilta SOC palveluita etsivä voi löytää myös käsitteet ja viitekehykset NCSC Computer Emergency Response Team (CERT), FIRST's Computer Security Incident Response Team (CSIRT) ja Gartner Cyber Incident Response Team (CIRT). CERT™ on myös Yhdysvaltalaisen Carnegie Mellon yliopiston rekisteröity tuotemerkki ja sen käyttö edellyttää erillistä lupaa. CERT™ rinnalle onkin muodostunut tuotemerkistä riippumaton tapa

käyttää CERT-käsitettä esimerkiksi maakohtaisen tunnuksen kanssa. Ensimmäisenä US-CERT tunnuksen otti käyttöön Yhdysvaltalainen The Department Homeland Securityn (DPS) ja myöhemmin nimeämistapa on otettu käyttöön yleisemminkin kansallisten kyberturvallisuusturvallisuuskeskuksien kyberturvallisuustiimejä nimettäessä. Muun muassa Traficomin kyberturvallisuuskeskus käyttää tunnisteena NCSC-FI CERT-muotoa. Vakiintuneen käytännön mukaan kansallisella tasolla organisaatiosta, jossa CERT tiimi toimii, käytetään nimitystä CSIRT (kuvio 28). CERT on CSIRT:iin kuuluva tietoturva-asiantuntijaryhmä, joka vastaa organisaatiossa kyberturvallisuushäiriöiltä suojaamisesta, niiden havaitsemisesta ja niihin reagoimisesta. CERT voi keskittyä tapausten, kuten tietomurtojen ja palvelunestohyökkäysten, ratkaisemiseen sekä hälytysten ja tapausten käsittelyohjeiden tarjoamiseen. CERTit myös järjestävät tiedotuskampanjoita ja osallistuvat tietoturvajärjestelmien parantamiseen tähtäävään tutkimukseen. Suomessa kyberturvallisuuskeskus kuvaa NCSC FI-CERT:n tehtäviksi muun muassa tietoturvaloukkauksien ehkäisemisen, havainnoinnin, tietoturva-asioista tiedottamisen ja yhteiskunnan elintärkeiden toimintojen turvaamisen. Riippumatta siitä, kutsutaanko tiimejä CERT-, CSIRT-, IRT- tai muulla vastaavalla nimillä, kaikkien niiden rooli on melko vertailukelpoinen. Kaikilla näillä tiimeillä on samat tavoitteet; niiden tehtävänä on reagoida tietoturvahäiriöihin, saada tilanne hallintaan, minimoida vahingot, auttaa palautumaan häiriötilanteista ja estää tietoturvahäiriöiden toistuminen. Myös yksityisten organisaatioiden on mahdollista nimetä oma CERT tehtäviä tuottava tiimi ”yritys-CERT” tyyppisenä toimijana ja siten selkeyttää tiimin tehtäviä ja käyttötarkoitusta niin organisaation sisällä kuin sen ulkopuolelle esimerkiksi toimiessaan muiden -IRT toimintoja tuottavien tahojen kanssa. Siinä missä -IRT voi organisaationa olla osa SOC:a, siitä täysin erillinen ja vain tarvittaessa perustettava erityisesti häiriöiden hallintaan keskittyvä tiimi, on SOC laajempi kokonaisuus. Esimerkiksi, jos tietoturvan seuranta on ensiarvoisen tärkeää ja organisaation rakenne mahdollistaa tietoturvan hallinnan keskittämisen yhteen fyysiseen tai loogiseen paikkaan, voi SOC:n luomisesta olla pelkkää -IRT luontia enemmän hyötyä. Keskittämällä tehtäviä SOC:lle voidaan saada esimerkiksi palveluiden tuottamiseen mittakaavaetuja tai yksinkertaistettua raportointihierarkiaa. Sitä vastoin, jos organisaatiorakenne on hajautetumpi tai ei muuten mahdollista valvonnan ja muiden turvallisuustoimintojen keskittämistä, CSIRT-ryhmän perustaminen voi olla järkevämpi toimenpide. (Sullivan 2021. Moyle 2021; Traficom 2021; Gartner 2021; US-CERT 2022; Kyberturvallisuuskeskus 2020.)



Kuvio 28: NCSC CSIRT ja CERT toimintamalli (mukaillen Sullivan 2021; Kyberturvallisuuskeskus 2020)

FIRST organisaation Computer Security Incident Response Team (CSIRT) Services Framework (2019) viitekehyksessä on kuvattu millaisia palveluita SOC voi tarjota tukiessaan organisaation tietoturvatavoitteiden toteutumista (kuvio 29). Kehyksen ovat kehittäneet FIRST-yhteisön tunnetut asiantuntijat yhdessä CSIRT (TF-CSIRT) -yhteisön ja kansainvälisen televiestintäliiton (ITU) kanssa. Viitekehys on ylätason kuvaus, jossa kuvataan tietoturvapalveluiden ydinluokat eli palvelualueet, palvelut ja niiden keskeinen sisältö ja niissä käytettävät termit ja käsitteet. Viitekehys ei kuitenkaan tarkemmin kuvaa kuinka CSIRT tai SOC rakennetaan. Viitekehyksen mukaan CSIRT-ryhmä ja muut tapahtumien hallintaan liittyvät resurssit voivat tarjota näitä palveluita liiketoiminnan suojaamiseksi. CSIRT-palvelukehyksen tavoitteena on helpottaa CSIRT-toimintojen perustamista ja tukea uusien SOC palveluiden valintaa tai sen nykyisen palveluvalikoiman laajentamista tai parantamista. Viitekehys toimii perustana ja pohjana hyville käytännöille. Sen ideologia on modulaarinen, jatkuvasti toimintaa kehittävä ja se ei lähde oletuksesta, että kaikki siinä esitetyt palvelut ja toiminnot tulisi ottaa käyttöön heti vaan painottaa palveluiden valintaa liiketoiminnan tarpeiden mukaisesti. Kehyksessä on kuvattu myös CSIRT organisoitumista esimerkiksi konsernirakenteessa useamman CSIRTin toiminnalliseksi kokonaisuudeksi. Tällöin voi esimerkiksi organisaation sisällä ”Enterprise” CSIRT keskittyä organisaation infrastruktuurin muodostavien tietokonejärjestelmien ja -verkkojen turvallisuuteen, yksi koordinaatioon ja palvelemaan tiettyä henkilö- ja/tai organisaatiojoukkoa. (Computer Security Incident Response Team (CSIRT) Services Framework, version 2.1 2019, 6-8.)

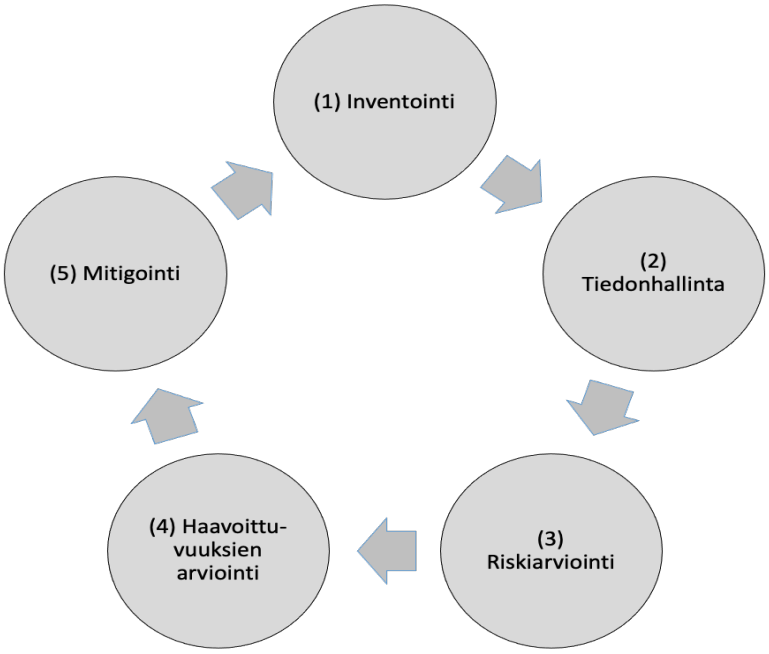


Kuvio 29: SOC:n palvelualueet FIRST's CSIRT viitekehyksen mukaisesti (mukaillen Muniz 2021, 161; Computer Security Incident Response Team (CSIRT) Services Framework 2019, 8)

Tietoturvatapahtumien hallinnan palvelualueella tarkoitetaan tietoturvaan liittyvän organisaation toimintoon tai sen tietojärjestelmään kohdistuneen tapahtuman monitorointia, analysointia ja tarvittaessa eskalointia. SFS-EN ISO/IEC 27000 (2020, 8) määrittelee tapahtuman tiettyjen olosuhteiden esiintymisenä tai muuttumisena. SFS-ISO/IEC 27035-1 (2016, 6) määrittelee tietoturvatapahtuman tapahtumaksi, jossa tietoturvallisuus tai sen hallintakeinot ovat mahdollisesti pettäneet. Tapahtuman seurauksena tietojen tai palveluiden tila on muuttunut tavalla, jolla saattaa olla vaikutusta tietoturvaan. (Kyberturvallisuuden sanasto 2018,16.)

Tietoturvapoikkeamien palvelualueen palveluita ovat todentaminen ja analysointi, rikosteknisten todisteiden turvaaminen ja analyysi (laitteet/välineet, ohjelmistot), vahinkojen minimointi ja palautuminen, poikkeamatilanteen koordinointi ja kriisinhallinnan tuki. Tietoturvapoikkeamien hallinnan tavoitteena on tunnistaa tietoturvahäiriöitä useiden eri tapahtuma- ja kontekstuaalisten tietolähteiden tietoturvatapahtumien korrelaatioiden, analyysien perusteella ja hallinnalla pyritään uhkan tai tapahtuneen poikkeaman vaikutuksien lieventämiseen tai poistamiseen. Tietoturvapoikkeaman hallintaa suorittava taho kerää ja arvioi tietoturvahäiriöraportteja, analysoi niitä tehden yksityiskohtaisen teknisen analyysin itse tapahtumasta ja käytetystä toimintatavasta. Analyysin perusteella tietoturvapoikkeaman hallintaa tekevä taho suosittelee toimenpiteitä tapahtumasta toipumiseksi tai haittojen lieventämiseksi. Suuremmissa organisaatioissa tämä palvelualue on joskus kokonaan tai osittain osoitettu SOC:lle, joka voi lisäksi suorittaa ensimmäisen tai jopa toisen tason tietoturvahäiriöiden hallintaa. Yleisesti poikkeamien hallinta edellyttää myös koordinointia ulkoisten tahojen, kuten vertais-CSIRT-ryhmien, muiden turvallisuusasiantuntijoiden ja toimittajien kanssa. (Computer Security Incident Response Team (CSIRT) Services Framework 2019, 9, 12; Cichonski ym. 2012, 60.)

Haavoittuvuuksien hallinnan palvelualue sisältää useita erillisiä palveluita, jotka liittyvät uusien tai aiemmin ilmoitettujen tietojärjestelmien tietoturva-aukkojen havaitsemiseen, analysointiin ja käsittelyyn. Alueen palveluita ovat haavoittuvuuksien etsintä, tutkiminen, raportointi, vaikuttavuuden ja todennäköisyyden analysointi, korjaus ja/tai korjaustoimenpiteiden koordinointi, haavoittuvuusskannaukset. Haavoittuvuuksien hallinnan tehtävänä on havaita, varmistaa, luokitella, priorisoida, arvioida, seurata tietoturvaan liittyviä haavoittuvuuksia tai niiden korjaamiseen liittyviä toimenpiteitä. Termiä "haavoittuvuuksien hallinta" käytetään myös joskus viittaamaan prosessiin, jolla yksinkertaisesti estetään tunnettujen haavoittuvuuksien hyödyntäminen (kuvio 30). Menetelmänä voidaan käyttää yleistä SANS viitekehystä. (Muniz ym. 2016, 59; Computer Security Incident Response Team (CSIRT) Services Framework 2019, 31.)



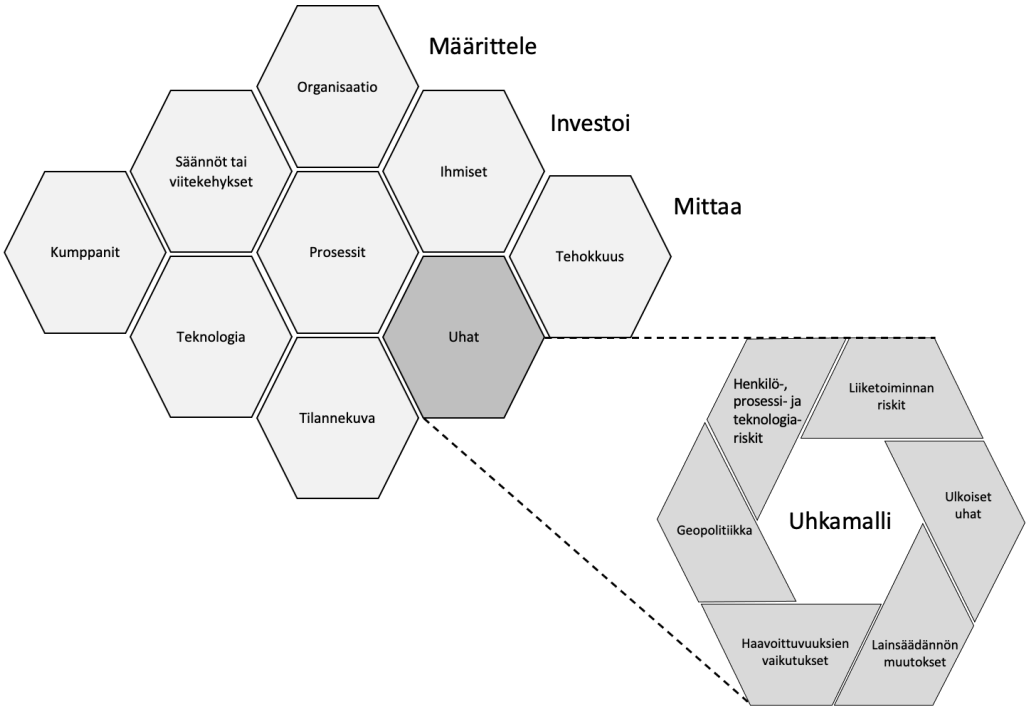
Kuvio 30: SANS Haavoittuvuuksien hallinnan malli (mukaillen Muniz ym. 2016, 58–59)

Tilannekuva -palvelualueen palveluita ovat tiedonkeruu, analysointi ja johtopäätösten teko ja viestintä. Palveluilla tuotetaan IT turvallisuusympäristön valvontaa, hallintaa ja kybertietoisuuden ylläpitoa. Tilannetietoisuus käsittää kyvyn tunnistaa, käsitellä, ymmärtää, viestiä palvelutuottajan vastuualueella ja sen ympäristössä tapahtuvat kriittiset osatekijät, jotka voivat vaikuttaa negatiivisesti asiakkaan toimintaan tai tehtävään. Tilannekuva muodostuu erilaisten tietojärjestelmien tietoturvaa valvovien järjestelmien keräämästä tiedosta, ulkoisesta informaatiosta, niiden käsittelyyn tarvittavista prosesseista ja asiantuntijuudesta. Tilannetietoisuutta tuottava palvelutoimittaja ei ole keskittynyt pelkästään tapauksiin reagoimiseen, vaan se tuottaa palvelua, joka varmistaa, että tiedot, analyysit ja toimet ovat muiden palveluiden, kuten tietoturvatapahtumien hallinnan, tapaustenhallinnan ja tiedonsiirron, saatavilla.

Palvelutuottaja myös varmistaa, että näiltä muilta palvelualueilta tulevat tiedot integroidaan asianmukaisesti yhteen ja toimitetaan takaisin asianosaisille oikea-aikaisesti. (Computer Security Incident Response Team (CSIRT) Services Framework 2019, 42.)

Koulutus ja opetus -palvelualueen palvelut tarjoavat tietoturvakoulutusta tietoturvatyöhön osallistuville ryhmille kehittäen ja ylläpitäen niiden tietoisuutta tietoturvasta. Tämä voi tapahtua esimerkiksi käsittelemällä erilaisia uhkakuvia ja niiden vaikutuksia. Yhtenä tavoitteena on myös parantaa tiedonvaihtoa eri toimijoiden välillä. Koulutuspalveluiden avulla voidaan kouluttaa tietoturvaan liittyvien työkalujen, prosessien ja menettelytapojen käyttöä. Koulutusohjelmaan voi sisältyä esimerkiksi menetelmiä uhkien havaitsemiseksi, ehkäisemiseksi tai niihin vastaamiseksi, työkaluja ja käytäntöjä kriittisen omaisuuden suojaamiseksi, tapaustenhallintaprosessin osaamiseksi ja avun saamiseksi. Lisäksi palveluihin voi kuulua esimerkiksi tarvittavien tietojen, taitojen ja kykyjen dokumentointia, koulutus- ja koulutusmateriaalien kehittämistä, sisällön toimittamista, mentorointia sekä ammatillisten taitojen kehittämistä. (Computer Security Incident Response Team (CSIRT) Services Framework 2019, 50.)

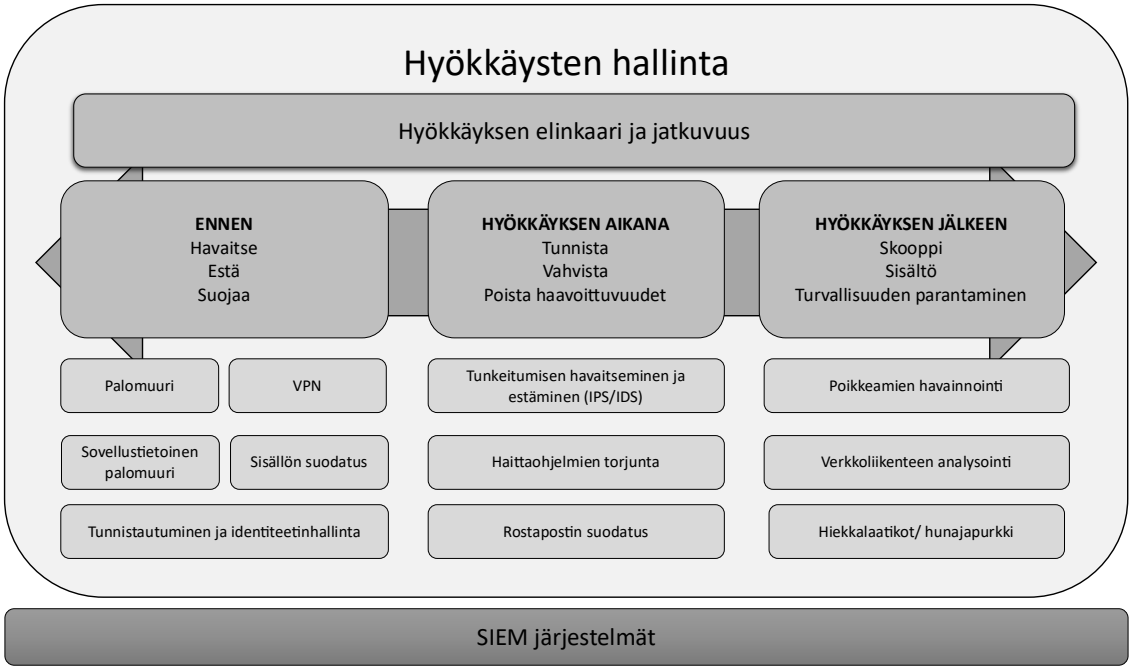
Gartner SOC Target Operating Model to Drive Success (SOCTOM) on ennen kaikkea malli, jolla organisaatio voi tunnistaa sitä koskevia todennäköisimpiä uhkia. Gartner nostaa SOCTOM mallissaan uhkamallinnuksen yhdeksi mahdolliseksi SOC:n palveluksi, joka usein liittyy ohjelmistokehitykseen ja järjestelmäarkkitehtuurin suunnitteluun (kuvio 31), kun taas CSIRT viitekehyksessä uhkamallinnus on vain osa tapahtumien hallintaa. Gartnerin mukaan mallinnuksessa tulisi kuitenkin käyttää uhkien tunnistamiseksi myös muita yleisiä ja testattuja malleja kuten ISO/IEC 27005:2018, CBEST Threat Modeling tai Mitre Threat Susceptibility Analysis -menetelmiä. (Collins 2021; Computer Security Incident Response Team (CSIRT) Services Framework 2019, 9.)



Kuvio 31: Gartnerin SOCTOM uhkamalli (mukaillen Collins 2021)

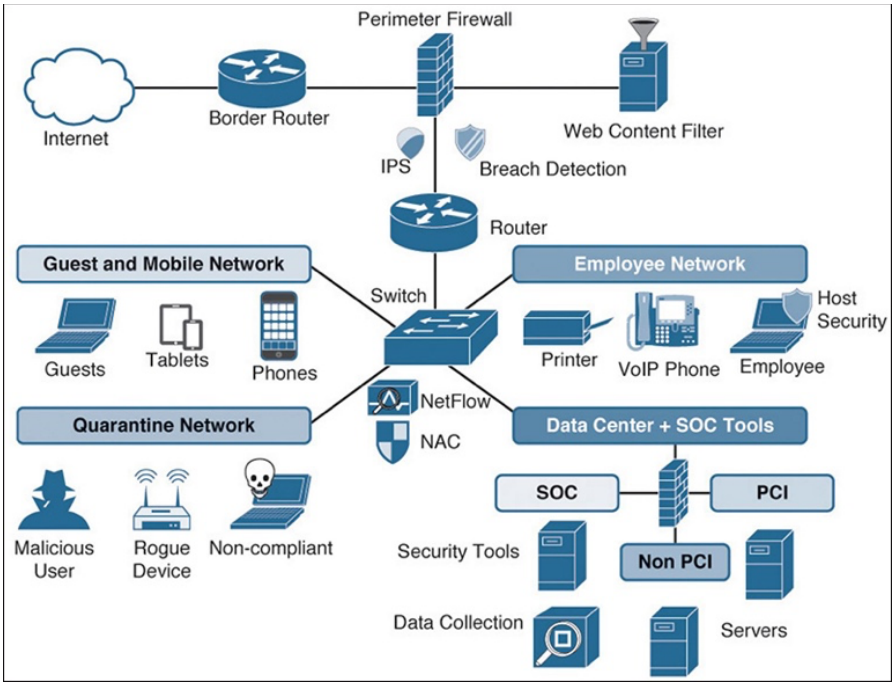
3.7 Teknologiat

Teknologiavalinnoillaan SOC tavoittelee kolmea asiaa: haavoittuvuudet kyetään tunnistamaan, ongelmat pystytään ehkäisemään ja/tai poikkeamat kyetään analysoimaan (kuvio 32). SOC:n käyttämien teknologiaratkaisujen tulee perustua kerroksellisuuteen ja turvallisuuden hallintaan tulisi olla useita järjestelmiä, joilla erilaisia tietoturvapoikkeamia voidaan havaita ja estää. Hyödyntämällä eri teknologioiden vahvuuksia voidaan hyökkääjän käytettävissä mahdollisuuksia rajoittaa, käytettävissä olevaa hyökkäyspinta-alaa supistaa tai poistaa se kokonaan. (Muniz ym. 2015.)



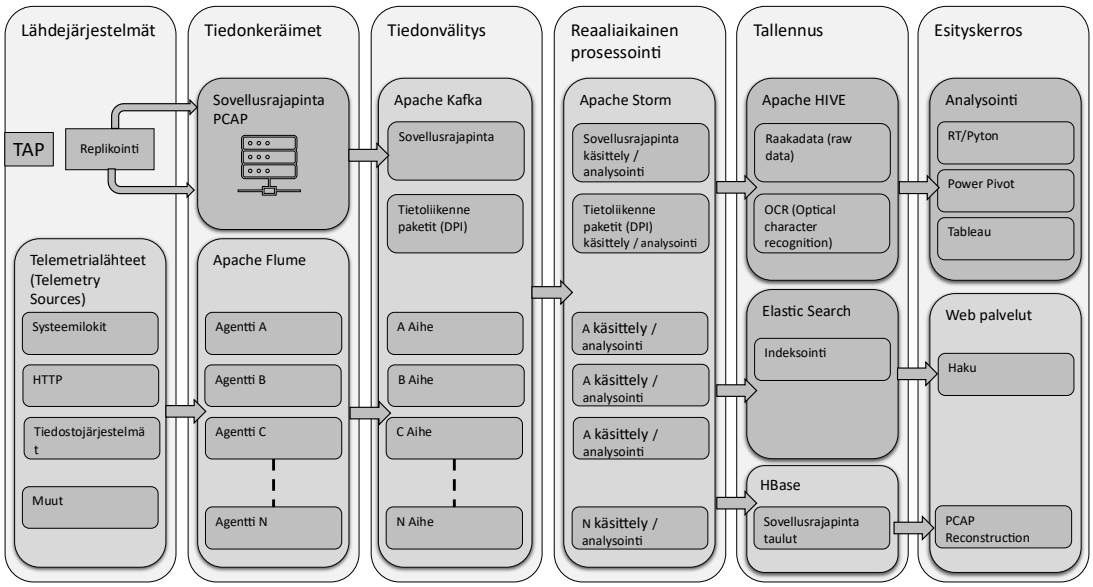
Kuvio 32: Hyökkäysten hallinta (mukaillen Muniz ym. 2015)

Organisaatioiden teknologiavalinnat poikkeavat paljon toisistaan ja sen vuoksi SOC:ien käyttämät teknologiat ovat organisaatiokohtaisia ja erilaisia variaatioita on paljon. Jotta SOC pystyy havaitsemaan ja ylläpitämään tilannekuvaa, sillä pitää olla mahdollisimman hyvä näkyvyys sen vastuulle määrätystä kokonaisuudesta (kuvio 33). SOC tarvitsee näkyvyyden yrityksen ICT järjestelmiin kuten tietoverkot, laskentakapasiteetti, tallennus ja päätelaitteet. (Muniz ym. 2016, 245–318.)



Kuvio 33: Example of a Mature SOC Architecture (Muniz ym. 2016, 315)

Cisco on julkaisut The Cisco OpenSOC platform arkkitehtuurin, jossa on kuvattu SOC:n teknologia-arkkitehtuuri perustuen avoimen lähdekoodin ratkaisuihin (kuvio 34). Arkkitehtuurimalli kuvaa SOC työvälineitä toimintalähtöisesti lähteiden käsittelystä aina lopputulosten analysointiin. (Muniz ym. 2016, 57–58.)



Kuvio 34: Mukaillen Cisco OpenSOC alusta-arkkitehtuuri (mukaillen Muniz ym. 2016, 58)

3.8 Palveluiden hankinta ja kilpailutus

Erilaisia toteutusvaihtoehtoja hankkia SOC ja siihen liittyviä palveluita on useita. SOC voidaan toteuttaa joko tehden palvelu kokonaan itse, hybridimallina tai ulkoistamalla palvelu kokonaan palvelutoimittajalle. Palveluissa käyttävät henkilöresurssit, teknologiat, prosessit ml. immateriaalioikeudet voivat olla joko omia tai ulkoa hankittuja. Se millaisen mallin yrityksen pitäisi itselleen valita, tulee perustua liiketoimintatarkasteluun ja -päätökseen (business case). Valittavaa toimintamallia ohjaa yrityksen kulttuuri, strategia, omien resurssien määrä, oma osaaminen ja taloudellinen kannattavuus. Hankittava palvelu voidaan määritellä ja hankkia prosessina eli työnä mitä palvelutoimittajan halutaan tekevän, lopputuotoksena, joka tulee saavuttaa tai mitä ostettavalla palvelulla halutaan laajemmin saavuttaa esimerkiksi parempi tietoturvan taso (kokonaisuutena). (Muniz ym. 2016, 245–246; Lehikoinen & Töyrylä 2013, 21–26.)

4 Toteutus

Tässä pääluvussa käydään läpi prosessi, miten opinnäytetyö tehtiin, peruste tutkimusongelman esitystavalle ja valitulle tutkimusstrategialle, kuvataan haastatteluiden suunnittelu ja toteutus sekä avataan, miten tuloksia analysoitiin.

Opinnäytetyöprosessi voidaan jakaa neljään eri vaiheeseen: orientaatioon, suunnitteluun, toteutukseen ja työn julkaisuun. Opinnäytetyön orientaatiovaihe aloitetaan työhön tarvittavan kokonaisprosessin hahmottamisesta ja työtä varten tarvittavan alustavan suunnittelun tekemisestä. Alustavaan suunnitelmaan kirjataan tehtävän työn aiheen hahmottelua. Myös toimeksiantajan etsintä suoritetaan orientaation vaiheen aikana. Suunnitteluvaiheessa orientaatiovaihetta tarkennetaan ja aiheanalyysi sekä opinnäytetyönsuunnitelma palautetaan. Suunnitelma myös esitetään seminaarissa. Suunnitelma vaiheessa tehdään varsinainen toimeksiantosopimus, tehdään tarvittaessa tutkimusluvat, salassapitosopimukset, määritellään aikataulu, ohjaaja tutkimukselle ja arvosanatavoitteet. Toteutusvaiheessa aloitetaan varsinaisen tutkimuksen työstö. Aiheeseen perehdytään tarkemmin ja aineisto kerätään ja analysoidaan. Työtä tehdään työn väliversioita iteroiden työlle määritellyn ohjaajan ja tilaajan kanssa. Julkaisuvaiheessa työ esitellään, tehdään kypsyysnäyte, englanninkielinen tiivistelmä ja julkaistaan työ. (Opinnäytetyö AMK-tutkinnossa 2021.)

Tämän opinnäytetyön tekeminen aloitettiin vuonna 2021, jolloin sen alustava toteutussuunnitelma laadittiin. Suunnitteluvaiheessa tehtiin aiheanalyysi, varsinainen suunnitelma ja Laurea ammattikorkeakoulu Oy:n kanssa sopimus tehtävästä työstä sekä erillinen salassapitosopimus. Suunnitelma myös esiteltiin Laurean järjestämässä seminaarissa. Sen jälkeen työ jatkui kartoittamalla markkinoilta löytyvää materiaalia ja perehtymällä siihen tarkemmin. Suurin osa opinnäytetyössä käytetystä lähdemateriaalista hankittiin vuonna 2021. Osa opinnäytetyössä käytetyistä tilastoista päivitettiin syksyllä 2022 ja alkuvuodesta 2023 sekä varsinaiset henkilöhaastattelut pidettiin 12/2022–3/2023 välisenä aikana. Opinnäytetyötä varten tehtiin neljä henkilöhaastattelua. Toteutusvaiheen aikana tekijä piti tilaajan kanssa kolme ja ohjaajan kanssa neljä tapaamista. Näiden lisäksi opinnäytetyöstä toimitettiin sähköpostilla molemmille osapuolille useita versioita tarkasteltavaksi.

Metsämuuronen (2006, 38–40) mukaan tutkimusongelma voidaan kuvata joko ongelmaa kuvailevana, kysymysmuotoisena tai hypoteesina. Mikäli tutkittavavalta alueelta ei ole saatavilla juurikaan aiempaa tietoa, on suositeltavaa käyttää kuvailevaa tutkimuskysymyksen asettelua. Mikäli tutkittavalta alueelta on saatavilla kohtuullisen verran tietoa, voidaan käyttää kysymysmuotoa. Hypoteesimuotoista tutkimusongelmaa käytetään, kun halutaan testata, onko esitetty väite paikkansapitävä. (Metsämuuronen 2006, 38–40.) Tämän opinnäytetyön tutkimusongelma kuvataan kysymysmuotoisena, koska esiselvityksen perusteella oli tiedossa, että käytössä oli jo jonkin verran käyttöönotettuja SOC:ja ja sitä kautta tietoa niiden

käyttöönottoihin liittyneistä haasteista. Tutkimusongelman pohjalta suunniteltiin asiantuntijahaastatteluissa esitettävät kysymykset tutkimusaineiston saamiseksi. Asiantuntijahaastatteluin pyrittiin selvittämään keskeisiä SOC palveluiden käyttöönottoon liittyviä haasteita.

4.1 Tutkimusmenetelmä

Tapaustutkimus, josta käytetään myös nimeä case study, on yksi empiirisen tutkimuksen menetelmä. Sen avulla tutkitaan toimintaa, tapahtumaa, ihmistä tai kokonaista järjestelmää (ihmiset, prosessit, teknologia) nykytoiminnassa ja ympäristössä. Tapaustutkimuksen etuja on, että se muun muassa sallii yleistykset, havaitsee sosiaalisten totuuksien monimutkaisuuksia, luo arkiston, josta voidaan tehdä erilaisia tulkintoja. Tapaustutkimusten näkökulma on usein toiminnallinen ja niiden tuloksia voidaan soveltaa käytännössä. (Metsämuuronen 2000, 16–17.)

Tämän opinnäytetyön tutkimusstrategiaksi valittiin kvalitatiivisen tiedonhankinnan tapaustutkimusstrategia. Yksi keskeinen peruste valinnalle oli, että opinnäytetyössä haluttiin selvittää SOC asiantuntijoiden konkreettisia ja omakohtaisia kokemuksia SOC:n perustamiseen liittyvistä haasteista. Toinen peruste valinnalle oli SOC:ien rajallinen lukumäärä Suomessa. SOC:in lukumäärän takia, kvantitatiivisin menetelmillä tuotetulle tiedolle ei todennäköisesti olisi saatu riittävää luotettavuutta.

Tässä opinnäytetyössä klassista tapaustutkimuksen strategiaa sovelletaan paremmin tähän opinnäytetyöhön soveltuvaksi. Tässä opinnäytetyössä Laurean tarvetta SOC:lle selvitetään vain tavoitteena ottaa sellainen käyttöön tietoturvariskien pienentämiseksi. Opinnäytetyön tekijällä ei ollut käytössään Laurean tietoturvan riskirekisteriä, joka olisi ollut edellytys etsiä klassisen tapaustutkimuksen keinoin esimerkiksi vastauksia rekisterissä oleviin konkreettisiin Laurean ongelmiin. Laajentamalla tämän opinnäytetyön tiedonhankintaa Laurean ulkopuolelle, haluttiin selvittää mitä Laurean tulisi yleisellä tasolla ottaa huomioon SOC:n käyttöönotossa.

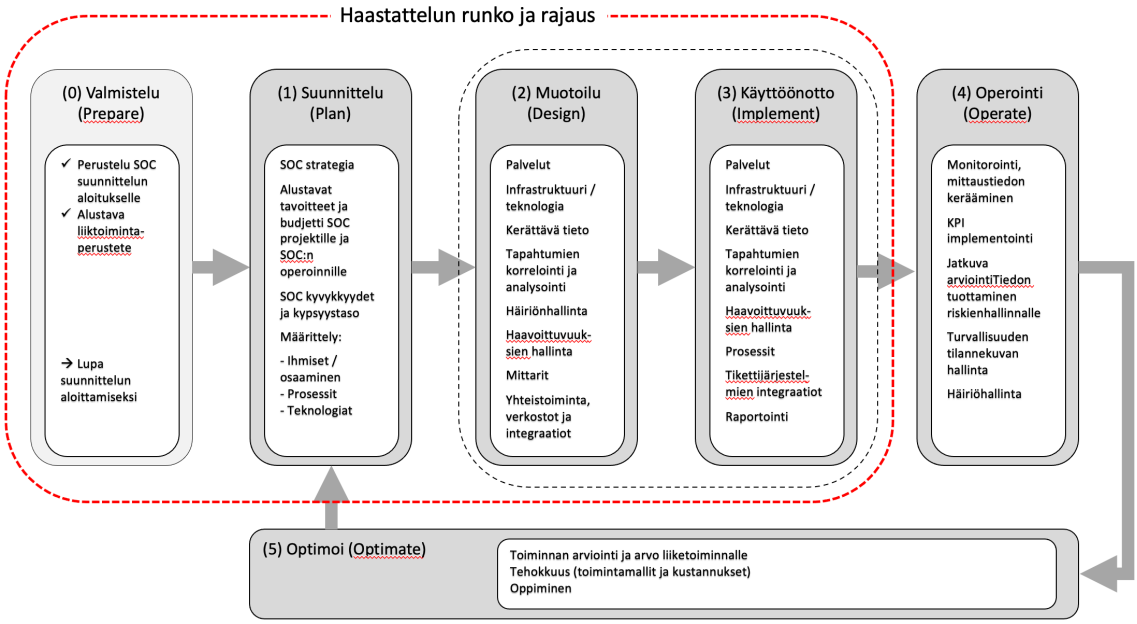
Hirsjärvi & Hurme (2008, 41, 43–44) mukaan haastattelun tavoitteena on tuoda haastateltavan ajatukset, käsitykset, kokemukset ja tunteet osaksi tutkimusta. Tapoja suorittaa tutkimushaastatteluja on useita ja valikoima on kirjava ja osin jopa sekava. Erot haastatteluiden välillä syntyvät pääsääntöisesti sen mukaan kuinka strukturoituja ne ovat. Haastattelu voi olla hyvin tiukasti ennalta määritelty, kiinteisiin kysymyksiin perustuva tai toteutustavaltaan vapaampi, jossa haastelu tehdään avoimien kysymysten varaan ja haastattelija syventää saatuja vastauksia sekä rakentaa haastattelun jatkoa saatujen vastausten perusteella. (Hirsjärvi & Hurme 2008, 41, 43–44.)

Tiedon hankkimisen metodologiaksi tähän opinnäytetyöhön valittiin haastattelut. Tämä toteutustapa valittiin, koska halutiin saada kokemusperäistä tietoa asiantuntijoilta SOC:n

käyttöönottoon liittyen. Haastateltaviksi haluttiin kokeneita johtavissa tehtävissä olevia tietoturva-ammattilaisia, joilla kaikilla oli kokemusta vähintään yhden SOC:n käyttöönotosta ja palveluiden tuottamisesta useamman vuoden ajalta.

Hirsjärvi ym. (2008, 41, 47–48) mukaan puolistrukturoidulla haastattelulla tarkoitetaan haastattelua, jossa kaikille haastateltaville esitetään samat kysymykset mutta niiden järjestys voi olla erilainen. Myöskään valmiita vastausvaihtoehtoja ei haastateltaville anneta vaan haastateltavat vastaavat kysymyksiin omin sanoin. Myös kysymysten sanamuodot voivat vaihdella. Varsinaista määritelmää ei puolistrukturoidulle haastattelulle kuitenkaan ole olemassa. Puolistrukturoitua haastattelua kutsuaan myös teemahaastatteluksi johtuen siitä, että puolistrukturoidussa haastattelussa keskustelu kohdistetaan tyypillisesti johonkin teemaan tai teemoihin. Englannin kielessä tästä haastattelutyypistä käytetään myös nimeä ”The focused interview”. (Hirsjärvi ym. 2008, 41, 47–48.)

Haastattelut suunniteltiin SOC:n käyttöönoton haasteita koskettavaksi puolistrukturoiduksi teemahaastatteluksi ja niiden runkona käytettiin yhtä opinnäytetyössä esiteltyä SOC:n käyttöönottoon soveltuvaa mallia (kuvio 35). Näin toimittiin, koska haastatteluun haluttiin tuoda systemaattinen viitekehys SOC:n valmistelusta sen rakentamiseen. Näin myös haastatteluiden aikana voitiin kysymyksiä kohdistaa oikea-aikaisemmin kehyksen eri vaiheisiin. Haastatteluja varten haastateltaville laadittiin valmiit kysymykset. Kysymyksiä ei esitetty haastateltaville kronologisesti samassa järjestyksessä ja niihin annettuja vastauksia tarpeen mukaan tarkennettiin lisäkysymyksin.



Kuvio 35 : Haastattelun runko ja rajaus

4.2 Haastatteluiden toteutus

Tätä opinnäytetyötä varten tehtiin yhteensä neljä puolistrukturoitua yksilöhaastattelua. Ennen haastattelua haastateltaville lähetettiin kutsun yhteydessä haastattelun aihe, lyhyt kuvaus sen tavoitteista ja selvitys miten haastattelussa saatavaa aineistoa tullaan käsittelemään. Kaikki haastatellut henkilöt olivat kyberturvallisuuden parissa jo useamman vuoden töitä tehneitä alan ammattilaisia, ja he kaikki olivat olleet käyttöönottamassa vähintään yhden SOC:n, osa haastatelluista jopa useamman. Heillä kaikilla oli kyberturvallisuuteen liittyvää konsultointitaustaa ja heillä kaikilla oli työkokemusta sekä palveluja toimittavien työnantajien palveluksessa, että palveluita ostavien palveluksessa. Kaikki haastatellut toimivat organisaatioissaan joko johtaja- tai päällikkötehtävissä ja heidän edustamansa organisaatiot edustivat valtiohallinnon tai yksityisen sektorin suuria kansainvälisiä organisaatioita. Haastateltujen henkilöiden organisaatioista yhdellä on oma SOC, yksi hankkii SOC palveluita kaupalliselta toimijalta ja kaksi ovat kaupallisia toimijoita, jotka tarjoavat SOC palveluita. Haastattelemalla kokeneita tietoturva-ammattilaisia tuotiin opinnäytetyöhön tietoa, millaisia käytännön elämän haasteita SOC:n käyttöönottoon yleisesti liittyy.

Haastattelut tehtiin Microsoft Teamsilla yksilöhaastatteluina kuviossa 35 olevan haastattelurungon (vaiheet 0–3) mukaisesti ja ennalta laadittuihin kysymyksiin perustuen. Haastatteluiden kesto vaihteli 45 minuutista yhteen tuntiin. Haastattelutilanteen alussa haastateltavalle pohjustettiin opinnäytetyön taustaa, kerrottiin opinnäytetyössä selvitettävä aihe, opinnäytetyössä käytetyn käsitteen ”SOC käyttöönotto” laajuus, rajaukset ja tutkimuskysymykset. Näin toimien haastattelija halusi varmistaa, että käyttöönoton kaikki vaiheet tulevat kattavasti käsitellyksi ja laajuus oikein ymmärretyksi. Haastattelun alussa ja sen aikana haastateltavalle korostettiin, että hänellä on mahdollisuus vapaasti nostaa omien kokemustensa kautta myös muita tutkimusongelman kannalta keskeisiä tekijöitä kuin haastattelussa kysyttiin.

Haastattelut tallennettiin digitaaliseen Windows Media Audio (WMA) formaattiin, jonka jälkeen jokaisesta haastattelusta muodostettiin koneellisesti oma erillinen Microsoft Word formaatissa oleva litterointi. Tämän jälkeen litteroinnin tulos tarkistettiin kuuntelemalla tallenne ja samalla tarvittaessa litterointia korjattiin tallennetta vastaavaksi. Haastattelut tehtiin joulukuu 2022 ja maaliskuu 2023 välisenä aikana. Opinnäytetyön valmistumisen jälkeen haastatteluissa saatu tieto tuhottiin tietoturvallisesti.

4.3 Tulosten analysointi ja tulkinta

Tutkimuksen ydinasia on, miten kerätty aineisto analysoidaan ja tulkitaan. Analysointivaiheessa etsitään aineistosta vastaukset tutkimusongelmaan ja analysointia voidaan tehdä monin tavoin. Oleellista on valita sellainen analyysitapa, jolla saadaan vastaus ongelmaan tai tutkimustehtävään. Laadullista aineistoa on myös mahdollista käsitellä tilastollisten tekniikoiden avulla. Analysoinnin perusteella saadut tulokset on tulkittava. Tulkinnan avulla

opinnäytetyön tekijä pohtii ja tekee oman tulkintansa analyysin tuloksista. Huomioitavaa on, että tutkimuksen tekijän lisäksi tutkielmaan sisältyy tulkintaa myös haastateltavilta ja tutkielmaa lukevilta. (Hirsjärvi ym. 2009, 221–224, 229.)

Haastatteluaineistosta pyrittiin tunnistamaan SOC käyttöönoton haasteisiin liittyvää tietoa. Haastatteluiden perustella muodostettua litteroitua aineistoa analysoitiin ensin muodostamalla yleiskuva lukemalla. Sen jälkeen tehtiin havaintoja eri haastatteluissa saadun tiedon samankaltaisuuksista, eroavaisuuksista sekä löytämällä selkeitä lähdeaineiston tietoon liittyviä poikkeamia. Havainnoista muodostettiin muistiinpanoja, joiden perusteella muodostettiin hakusanoja. Sen jälkeen haastatteluaineisto kooditettiin hakusanojen perusteella. Tekstistä etsittiin ongelmia, haasteita tai tarkoittavia ilmaisuja. Sen jälkeen näihin liittyvää tietoa yhdisteltiin laajemmiksi kokonaisuuksiksi, jossa samantyyppiset ongelmat teemoitettiin loogisiksi kokonaisuuksiksi. Nämä kokonaisuudet muodostuivat käyttöönoton perustelusta, käyttöönottomallista, kyvykkyyksien arvioinnista, odotuksiin SOC:n roolista, vastuisista ja sen toiminnan organisoinnista sekä johtamisesta, teknologian merkityksestä ja palveluiden hankintaan liittyvistä haasteista.

5 Tulokset

Opinnäytetyöni tavoitteena on selvittää millaisia haasteita tietoturvavalvomon (SOC) käyttöönottoon liittyy. Haastatteluista saatujen tulosten ja kirjallisten lähteiden perusteella käyttöönottoon liittyy lukuisia erilaisia haasteita. SOC käyttöönottoa suunnittelevan on ne hyvä tunnistaa jo siinä vaiheessa, kun vasta harkitaan SOC:n käyttöönottoa.

Opinnäytetyöni kvalitatiiviset tulokset perustuvat neljän kokeneen ja johtavissa tehtävissä olevan tietoturva-ammattilaisen henkilöhaastatteluihin. Lisää syvyyttä ja näkökulmaa sain tuloksiini, koska haastatellut asiantuntijat edustivat sisäisiä SOC palveluita itse tuottavia, palveluita ulkoa hankkivia ja palveluita tarjoavia toimijoita. Heillä kaikilla oli laaja-alaista kokemusta SOC:n käyttöönotoista ja palveluiden tuottamisesta. Haastattelut tehtiin yksilöhaastatteluina.

Ensimmäiseni ja primääri tutkimuskysymykseni on: ”Millaisia haasteita yleisesti on tai voi olla SOC käyttöönotossa?”. Toinen ja sekundaarinen tutkimuskysymykseni on: ”Millaisia vaikutuksia olisi päätöksellä eriyttää tietoturvan SIEM hallintajärjestelmän hankinta SOC:n käyttöönotosta?”

Tämän opinnäytetyön tulokset esitetään haastatteluaineistoista muodostettujen teemojen mukaisesti. Teemoja ovat (1) miten SOC käyttöönoton tarve perustellaan organisaatiolle, (2) haastattelussa käytetyn käyttöönottomallin mukaisesti eri vaiheisiin liittyvät haasteet, (3) kyvykkyyksien arviointi, joita SOC tarvitsee toimiakseen, (4) SOC:n rooli, vastuut, toiminnan

organisointi ja johtaminen, (5) teknologian merkitys SOC:lle ja (6) SOC:n hankkiminen palveluna. Tuloksia kuvaavien alalukujen alussa kuvatut kysymykset myös mukailevat haastatteluissa käytettyjä kysymyksiä.

5.1 Käyttöönottoon perustelu

Ensimmäinen haastatteluista saatu tulos vastaa kysymykseen, millaisia haasteita SOC:n käyttöönoton suunnittelun aloittamiseen liittyy.

Kartoitettaessa syitä miten tarve uudelle SOC:lle perustellaan johdolle, haastatellut asiantuntijat toivat esille kolme näkökulmaa. Yleisin peruste SOC:n käyttöönotolle on kyberuhkien jatkuva kasvu, jonka vuoksi tietoturvaan liittyviä riskejä haluttaan vähentää. Toinen tarve SOC käyttöönotolle tulee johonkin asetukseen tai lakiin perustuvan tarpeen tai vaatimuksen kautta havaita aikaisempaa tehokkaammin tietoturvaan- tai suojaan liittyviä ongelmia. Kolmas peruste oli organisaation tekemään sopimukseen perustuva vaatimus ottaa käyttöön jokin tietoturvaan tai -suojaan liittyvä yhteinen viitekehys, esimerkiksi ISO 27001 standardi, ja sen seurauksena tarve perustaa SOC.

Käyttöönoton perustelemiseen liittyvinä haasteina asiantuntijat kertoivat, että liiketoiminta ei välttämättä tunne organisaatioon kohdistuvia tietoturvavaatimuksia. Organisaation koskevat tietoturvavaatimukset voivat sisältyä asiakassopimuksiin tai olla yleisiä regulaatioon perustuvia vaatimuksia, esimerkiksi EU:n tietosuoja-asetuksen tai uuden NIS2 -direktiivin yrityksen kautta toiminnalle kohdistettuja velvoitteita. Yksi haastateltavista korosti, että lait saattavat myös rajoittaa tietoturvan valvontaa ja että asia on hyvä huomioida jo mahdollisimman aikaisessa vaiheessa, kun käyttöönottoa vasta valmistellaan. Kaksi haastatelluista kertoi, että harkittaessa SOC:n perustamista kannattaa teemaa lähestyä niin päin, että perustamista suunnittelevat ensiksi miettivät miten organisaatio jo nykytilassa hoitaa tietoturvan ja miksi SOC:a ei jo ole käyttöönotettu. Tämä ajattelutapa auttaa paremmin hahmottamaan uhkia ja viestimään liiketoiminnalle niistä aiheutuvia riskejä sekä tuomaan esille SOC:n organisaatiolle tuomia hyötyjä.

Haastatteluiden perusteella selvisi, että SOC:n käyttöönoton perustelu ja päätös käyttöönotosta syntyy vain harvoin tietoturvariskien arvioinnin perusteella. Osa haastateltavista totesi, että tarve SOC:n käyttöönottoon on jo niin ilmeisiä johdollekin, että juurikaan systemaattista riskienarviointia ei ole SOC:n perustamisen suunnittelulupaa varten tarvinnut tehdä. Yksi haastateltavista myös totesi, että mikäli riskienhallintaa yrityksessä systemaattisesti tehdään niin se voi olla hyvinkin SOC:n käyttöönoton päätöksentekoa ohjaava tekijä.

Haastattelujen mukaan haasteena on, että SOC perustamisen suunnittelu lähtee usein IT:n vetämänä. Ongelmina nostettiin IT:n puutteellinen kyky tunnistaa liiketoiminnan uhkia ja riskejä sekä IT:n osaamisen puute esittää SOC:n hyödyt liiketoimintalähtöisesti. Yksi

haastateltavista kertoi, että ”keskeisin haaste on miten saa liiketoiminnan ymmärtämään IT riskien vaikutukset liiketoiminnalle”. Haastatteluissa asiantuntijat kertoivat, että usein liiketoiminta ei ole tunnistanut millaisia riskejä tietoturvaongelmat voivat aiheuttaa IT järjestelmien toiminnalle ja sen vuoksi myöskään tarvetta SOC:lle ei ole tunnistettu.

Haastatelluissa asiantuntijat korostivat olemassa olevista kyvykkyyksistä, mittareista ja käyttöönottoprojektin rajauksista keskustelun tärkeyttä. Näillä vaikutetaan SOC:n käyttöönottoon liittyvien odotusten hallintaan ja budjetointiin. SOC:n käyttöönottoprojekti usein kilpailee muiden hankkeiden kanssa organisaation osaajista ja taloudellisista resursseista. Asiantuntijat kertoivat, että tarve perustella resurssien käyttöä SOC:n käyttöönoton valmisteluun ja suunnitteluun vaihtelee organisaatioissa. He kertoivat, että mittareiden ja raportoinnin avulla voi havainnollistaa SOC:n organisaatiolle tuomia hyötyjä. Mittareiden määrittelyn kerrottiin selkeyttävän dialogia johdon ja SOC:n käyttöönottoa ehdottavan välillä. Yksi haastateltavista sanoi: ”*mittareiden ja raportoinnin kautta voidaan johdon kanssa käydä keskusteluja ja varmistaa mitä palveluita SOC:n tulee tuottaa ja tehdä*”. Kolmas haastateltavista painotti organisaatiossa erilaisten ryhmien kanssa käytävän keskustelun merkitystä, jotta oikeat mittarit löytyvät. Alkuvaiheessa oman osaamisen puute vaikeuttaa oikeiden mittareiden määrittelyä. Niiden tulisi olla riittävän ylätasolla ja kuvata mieluiten liiketoiminnalle tulevia hyötyjä, jotta niistä on hyötyä päätöksentekovaiheessa.

Käyttötapauksien määrittely nostettiin SOC:n arvoa ja sen käytön laajuutta selkeyttävänä asiana. Käyttötapauksella tarkoitetaan ennalta tehtyä määrittelyä, jolla voidaan havaita, tunnistaa ja hallita tietoturvaan tai -suojaan liittyvää erityistä tapahtumaa. Yksi esimerkki käyttötapauksesta voisi olla, miten organisaatiossa havaitaan identiteettiväärinkäyttö ja miten sen jälkeen toimitaan. SOC:n suunnitteluvaiheessa käyttötapausten määrittelyssä on haasteena erityisesti niiden määrittelyyn tarvittavan liiketoimintaosaamisen puuttuminen. Haastatteluissa asiantuntijat toivat esille, että käyttötapausten määrittelyssä yhdistyvät erilaiset kyvykkyyden osa-alueet; ihmiset, prosessit ja teknologia ja näiden maturiteettitaso. Kartoittaessa, miten haastateltavien mielestä toimiala vaikuttaa käyttötapauksien määrittelyyn, he kertoivat, että suuri osa peruskäyttötapauksista ovat kaikille samanlaisia mutta toimialakohtaista vaihtelua on myös paljon. Yksi haastateltavista nosti esille, että erityisesti tietosuojaan liittyvät asiat tulisi huomioida, koska tarve henkilötietojen käsittelyyn ja tietojen luokitteluun voi organisaatioiden välillä vaihdella paljonkin. Käyttötapausten määrittelyllä saadaan myös tietoa, millaisia asioita tulee huomioida ja vaatia SOC:n hankintavaiheessa.

5.2 Käyttöönottomalli

Toinen haastatteluista saatu tulos vastaa kysymykseen, millaisia haasteita SOC käyttöönottomalliin tai -prosessiin liittyy. Tätä tulosta tarkastellaan haastatteluissa käytetyn PPDIOO

käyttöönottomallin näkökulmasta. Sen tässä opinnäytetyössä käytettyjä vaiheita olivat valmistelun, suunnittelun, muotoilun ja rakentamisen -vaiheet.

Yksi haastateltavista kommentoi, että käyttöönottoa helpottaisi, jos *"SOC:ien perustamiseen, kyvykkyyksien ja käyttötapausten määrittelyssä käyttäisi siihen soveltuvia malleja- ja viitekehyksiä"*.

Kaikki haasteltavat painottivat haastattelussa esitellyn valmisteluvaiheen merkitystä ja nostivat sen vaiheeksi, johon usein käytetään liian vähän aikaa ja resursseja. Jo tässä vaiheessa pitäisi tunnistaa SOC:n käyttöönotossa tarvittavat kyvykkyydet, alustavat käyttötapaukset ja mittarit, joilla SOC:n hyötyä arvioidaan. Haastatteluissa saadun tiedon mukaan haasteena on, että valmisteluvaiheessa käytössä on usein liian vähän aikaa, resursseja ja osaamista. Suurin osa haastateltavista nosti valmisteluvaiheen myös kaikkein vaikeimpana tehdä. Vaiheen keskeisimmiksi tekemisiksi nostettiin olemassa olevien kyvykkyyksien tunnistaminen ja liiketoimintaperusteen mittareiden määrittely johdolle. Myös käyttötapausten määrittelyä tässä vaiheessa korostettiin. Yksi haastateltavista kommentoi vaihetta: *"valmisteluvaihe on monille Akilleen-kantapää"*.

Suunnittelu -vaiheen tuloksissa haastatellut asiantuntijat nostivat paljon samoja asioita kuin valmisteluvaiheessakin. Haastatteluiden perusteella tässä vaiheessa kaikkia valmisteluvaiheen asioita tulee käsitellä ja tarkentaa. Erityisesti mittareiden osalta nostettiin tarve niiden konkretisointiin tarkemmalla tasolla.

Haastateltavien mukaan muotoilun ja käyttöönoton vaiheet ovat haasteltujen mukaan toisiinsa tiiviisti limittyviä ja niiden läpiviennin osalta haasteltavat eivät nostaneet esille erityisiä haasteita. Muotoilu- ja rakentamisvaiheen osalta kuitenkin nostettiin tärkeäksi määritellä toimintaprosessit, jotta SOC voisi toimia verkostossa.

5.3 Kyvykkyyksien arviointi

Kolmas haastatteluista saatu tulos liittyy kyvykkyyksien arvioinnin haasteisiin. Haastatteluissa asiantuntijat kertoivat, että SOC:n käyttöönottoa suunniteltaessa erityisesti olemassa olevien omien kyvykkyyksien realistiseen arviointiin tulisi kiinnittää erityistä huomioita. Asiantuntijoiden mukaan panostamalla omien kyvykkyyksien kartoitukseen saa realistisemman kehityspolun SOC:n käyttöönotolle. Organisaatioiden haasteena on, että niillä on harvoin entuudestaan omaa osaamista SOC toiminnassa tarvittavien kyvykkyyksien määrittelemiseksi. Yksi haastateltavista nosti haasteena, että *"tyypillisesti organisaatiolla itsellään ei ole riittävää osaamista arvioida omia kyvykkyyksiään oikein"*. Haastateltavan kertoman mukaan tämä voi näkyä esimerkiksi siten, että organisaatio ei itse ymmärrä puutteita sen omissa teknisissä valmiuksissa tai prosesseissa. Virhearviot oman nykytilan arvioinnissa näkyvät SOC:lle kohdistettavina epärealistisina arvon tuotto-odotuksina ja toimintatavoitteina. Laadukkaan kyvykkyyksien

kartoitustyön lopputuloksen varmistamiseksi kaikki haastatellut asiantuntijat suosittelivat käyttämään osaamista, jolla on myös käytännön kokemusta SOC:n tarvitsemien kyvykkyyksien kartoitustyöstä. Yksi haastatelluista kertoi omasta kyvykkyyksien kartoitukseen liittyvästä positiivisesta kokemuksestaan ja suositteli käyttämään kyvykkyysien arvioinnissa Espoon kaupungin kehittämää kyvykkyyksien johtamisen käsikirjaa. (Kyvykkyyksien johtamisen käsikirja. 2018.)

Haastatelluissa tyypillisenä ongelmana nostettiin kerralla liian suuresta käyttöönottokokonaisuudesta päättäminen. Osa haastateltavista kertoi tähän olevan syynä, että tyypillisesti omat kyvykkyydet arvioidaan usein paremmiksi kuin ne todellisuudessa ovatkaan. Haastatteluiden mukaan virhearvioinnit kyvykkyyksien määrittelyssä johtavat liian laajaan SOC käyttöönottoprojektiin ja sitä kautta projektin pitkittymiseen ja ennakoimattomiin kustannuksiin. Kaikki haastatellut asiantuntijat suosittelivat SOC:n käyttöönottoa ja siihen liittyvien hankintojen tekoa riittävän pienissä osissa.

Haastatteluissa asiantuntijat toivat esille, että SOC toiminnan edellyttämien kyvykkyyksien kehittäminen on nähtävä SOC:n käyttöönottoprojektiin kuuluvana tekemisenä. He nostivat SOC:n perustamiseen liittyvinä erityisinä kehittämishaasteina organisaation oman osaamisen tason ja kokemuksen tasonnoston, kehittämistarpeen yrityksen hallintoon ja johtamiseen liittyvien vastuiden sekä prosessien osalta, olemassa olevien ulkoisten palveluiden kattavuuden ja palveluihin liittyvien verkostojen rakentamisen.

Haastatteluissa nousi esille myös haaste, miten tulisi perustella johdolle SOC toimintaan liittyvä erilainen tietoturvan osaamistarve. Haasteena on, että johto ei ymmärrä miksi tietoturvavalvonta tarvitsee omat erityisosaajansa ja miksi IT:n nykyiset taidot eivät siihen riitä. Yksi haastateltavista korosti, että ”*tietoturvan valvonta edellyttää erityyppistä osaamiskokonaisuutta kuin IT-valvonta*”. Ennakkoasenteena johdolla saattaa olla käsitys, että jo olemassa olevat tekniset IT taidot ja palvelut riittävät. Asiantuntijat painottivat, että SOC palveluiden tuottamiseen tarvitaan tietoturvaan liittyvää erityistä osaamista, jota tyypillisesti teknisillä IT asiantuntijoilla ei ole.

5.4 SOC:n rooli, vastuut, toiminnan organisointi ja johtaminen

Neljäs kokonaisuus koskee SOC:n rooliin, vastuisiin, sen toiminnan organisointiin ja johtamiseen liittyviä haasteita. Haastatellut asiantuntijat kertoivat, että usein SOC:n rooli ymmärretään väärin. He kertoivat, että virheellinen kuva SOC:n ja olemassa olevien IT palvelutoimittajien tosiallisista rooleista, vastuista ja palveluista voi tuottaa kokonaisuuden, joka ei toimi tai sen toimintaan saaminen voi vielä ennakoitua enemmän sekä aikaa että resursseja. He myös painottivat, että SOC ei ole se toiminto, joka korjaa tietojärjestelmiä vaan korjausvastuun tulee olla joko sisäisellä tai ulkoisella ICT palvelutoimittajalla. SOC:n tehtävänä on havaita kyberongelmia ja IT toimittajien vastuulla on korjata ne. Yksi haastateltavista nosti

esille, että ”*vaikka SOC kyvykkyys olisikin olemassa niin, jos muu organisaatio, resurssit ja prosessit eivät tue SOC:a niin ei se vaan toimi. Haasteeksi nousee eritoimijoiden välillä sovitut prosessit sekä niihin liittyvät työ- ja/tai palveluajat ja palvelutasot*”. Toinen haastateltava kertoi, että ”isoissa toimintaympäristöissä SOC ei voi olla se, joka tunteen jokaisen järjestelmän”.

Erityisesti valmisteluvaiheeseen liittyvänä SOC:n haasteena haastatellut asiantuntijat kertoivat, että yrityksessä voidaan olla tilanteessa, jossa kyberturvallisuuden vastuista ja poikkeamien käsittelystä yrityksen sisällä ei olla vielä sovittu konkreettisesti lainkaan. Yksi haastateltavista painotti, että jo SOC:n suunnitteluvaiheessa on määriteltävä sen rooli, vastuut ja erityisesti kyberturvallisuuden poikkeamien käsittelyyn liittyvä päätöksentekokyky on kuvattava. Yrityksen johdolla voi olla kokonaan virheellinen odotusarvo SOC:n palveluista, vastuista ja tekemisestä. Erityisesti ongelmalliseksi tilanteeksi nostettiin, jossa yrityksen omalla organisaatiolla ei ole valmiuksia tehdä kyberturvallisuuteen liittyviä päätöksiä. Yrityksen johto voi kuvitella hankkimalla SOC:n saavansa myös kyberongelmien hoitamiseen liittyvää päätöksentekokykyä. Kaikki haastatellut asiantuntijat pitivät tätä virheellisenä johtopäätelmänä. Yksi haastateltavista kiteytti asian: ”se on niin kuin aina - vastuuta ei voi ulkoistaa”.

SOC toiminnan haasteina haastattelussa nousi esille usein SOC:n toiminnalta vaadittava 24/7/365 palveluaika. Haastateltujen asiantuntijoiden mukaan olemassa olevien toimijoiden vastuut, palveluajat ja -tasojen pitää yhteensovittaa SOC:n palveluihin. Ongelmia tuottaa erityisesti olemassa olevat IT toimittajien palvelusopimukset ja niiden vastuumatriisit, joissa SOC:n roolia ei ole määritelty. Eräs haastateltavista kuvasi asiaa näin: ”*tietoturvavalvonnan ja ensireaktion verkostovastuu pitäisi olla SOC:lla. Se ei kuitenkaan pysty toimimaan, mikäli sillä ei ole hyviä rajapintoja muihin toimijoihin*”. SOC:n käyttöönoton näkökulmasta haasteena pidettiin, että verkostot pitää tunnistaa, niiden väliset prosessit pitää sopia ja kuvata sekä saada systeemi toimimaan. 24/7/365 palvelun tuottaminen vaatii paljon henkilöresursseja. SOC palveluita tuottavien osalta huomioida myös olemassa olevat työsopimukset ja jatkuva osaamisen saatavuus.

Haastatteluissa asiantuntijat kertoivat, että mikäli SOC:n palveluajaksi määritellään 24/7/365, niin sen toiminnasta aiheutuu myös merkittäviä uusia tuotantokustannuksia. Erityisenä haasteena osa haastateltavista mainitsi riskin työvoimakustannusten noususta. Haasteena on, että SOC:n kaikki henkilökapasiteetti tulisi mitoittaa vaaditun palveluajan osalta siten, että se selviää aina myös yllättävien poikkeamien käsittelystä. Myös yrityksen päätöksentekokykyistä henkilöstöä tulee olla aina saatavilla. Työvoiman saatavuuteen liittyvät vaatimukset voivat vaikuttaa henkilöiden työehtosopimuksiin. Mikäli SOC tuotetaan kokonaan itse, pitää myös sen työntekijöiden työehtosopimukset olla halutun palveluaikavaatimusten mukaisia eli yleisesti 24/7/365 sopimuksia. Yksi haastateltavista nosti SOC:n organisointiin liittyvän

päätöksen: *”keskeinen päätös on, halutaanko SOC:a tehdä itse vai ostetaanko se palveluna yrityksen ulkopuolelta*”.

5.5 Teknologia

Viides haastatteluista saatu tulos liittyy kysymykseen, millaisia haasteita teknologia aiheuttaa SOC:n käyttöönotolle? Kaikki haastatellut asiantuntijat nostivat teknologian yhtenä kyvykkyyden osa-alueena ja haasteena SOC:a käyttöönottavalle. Useampi haastateltavista kertoi, että toimiakseen SOC tarvitsee oikeanlaista teknologiaa mutta teknologialle annetaan usein liian suuri painoarvo. Yksi haastateltavista halusi painottaa tätä näkemystä sanomalla: *”teknologialla itsessään ei ratkaista tässä yhtälössä yhtään mitään”*. Haastatellut asiantuntijat kertoivat, että teknologiavalintojen uskotaan usein ratkaisevan asioita, joita tosiasiallisesti ei voi teknologialla ratkaista. He totesivat, että SOC:a perustettaessa organisaatioilla on jo tyypillisesti ennestään runsaasti tietoturvapoikkeamien havainnointiin liittyvää teknologiaa ja niiden integrointi SOC:n työkaluihin osataan jo aika hyvin. Suurempana ongelmana pidettiin, että jos SOC:a ei ole perustettu, organisaatio itse ei välttämättä käytä olemassa olevaa tietoturvateknologiaa tehokkaasti hyväkseen. Käyttöönottamalla SOC:n, organisaatio pystyy hyödyntämään jo tehtyjä investointeja tehokkaammin.

5.6 Palveluiden hankinta

Kuudes haastatteluista saatu tulos liittyy kysymykseen, millaisia haasteita SOC palveluiden hankintaan liittyy. Haastatteluissa asiantuntijat kertoivat, että Suomessa haasteena ei ole erilaisten SOC palveluiden saatavuus. Kaikki SOC toimijat pystyvät tarjoamaan ja tuottamaan SOC:n peruspalvelut kuten tietoturvatapahtumien, -poikkeamien ja haavoittuvuuksien hallinnan. Kaikki haastatellut korostivat SOC:n hankinnassa organisaation tarkan tarveharkinnan merkitystä, jotta SOC:n palveluiden käyttöönotot voidaan suorittaa pienemmissä kokonaisuuksissa. Keskeisenä haasteena asiantuntijat pitivät palveluita hankkivan riittävän osaamisen ja kokemuksen puutetta. Yksi haastateltavista muotoili asian näin: *”Riskinä on, että asiakas kilpailuttaa oman, mutta puutteellisen näkemyksen mukaisen ratkaisun*”. Kolme neljästä haastateltavasta nostivat ongelmaksi, että SOC palveluita kilpailutetaan kuten ICT palveluita. Tarjouspyynnöissä toimittajia pyydetään sitoutumaan sellaisiin palvelutasomittareihin, jotka ovat ICT palveluiden osalta yleisesti käytettyjä mutta eivät juurikaan sovellu SOC:n palveluiden toimittamiseen. Erityisen ongelmallisina esimerkkeinä nostettiin yleisesti ServiceDesk kilpailutuksissa käytettävät vaatimukset SOC:n palvelutasovaatimuksina. Esimerkkeinä nostettiin, että SOC:lta vaaditaan usein häiriöhallinnan nopeita ratkaisuaikoja, kun sen sijaan tärkeämpää olisi tehdä ongelmanhallintaa, raportoida tietoturvapoikkeamista regulaatiovaatimusten mukaisesti, tuottaa tietoturvaa parantavia kehitysehdotuksia ja toimia proaktiivisesti. Yksi SOC palveluita toimittava asiantuntija nosti konkreettisena esimerkkinä tietojärjestelmien

palauttamiseen liittyneen aikaisemman tapauksen. Siinä tietomurron ajankohtaa ei ollut voitu tarkasti määritellä ja sen vuoksi SOC:n asiantuntijat joutuivat etsimään turvallista varmistusta pitkän aikaa.

Palveluita hankkivien näkemys oli, että palvelutuottajat tarjoavat asiakkailleen bulkkipalveluita ja valmius tehdä asiakaskohtaisia ratkaisuja on puutteellinen. Erityinen ongelma on SIEM teknologian sopivuus asiakkaan toimintaan ja arkkitehtuuriin. Yhden haastateltavan näkemyksen mukaan aikaisemmin teknologiaa hankittiin usein osana muita SOC palveluita, koska se oli helppoa. Nyt haastateltavan mukaan trendi on muuttumassa. Syynä tähän on se, että asiakkaiden kokemusten mukaan SIEM teknologia ei ole asiakkaan toiminnan tarpeisiin optimoitua ja riittävän nykyaikaista. Ongelmana haastateltava nosti, että osana muita SOC palveluita tarjottavalla teknologialla ei pysty ratkaisemaan kaikkia asiakkaan käyttötapauksista johdettuja tarpeita tai se ei ole asiakkaan näkökulmasta kustannustehokasta. Itse hankittuna SIEM sopii paremmin omaan arkkitehtuuriin ja sillä voidaan hoitaa kaikki asiakkaan haluamat käyttötapaukset. Omaan käyttöön tehdyt käyttötapaukset myös jäävät itselle käyttöön, mikäli palvelutoimittaja vaihtuu. Haastateltavan kertoikin, että *”me ollaan vähän palaamassa 10-vuotta taaksepäin ja haluamme itse omistaa SIEM teknologian”*. Toinen haastateltava nosti havaintona, että *”SIEM järjestelmän hankkija ostaa järjestelmän lisäksi myös käyttötapauksia eli sen mitä järjestelmällä pystytään valvomaan”*. Myös puute sopia palveluiden jatkuvasta kehittämisestä koettiin haastavaksi. Yksi palveluita hankkivista korosti, että on valmis maksamaan enemmän proaktiivisista palveluista (esimerkiksi edistyneiden uhkien metsästys eng. threat hunting) kuin reaktiivisista palveluista.

Toimittajien puolella työtä tekevät asiantuntijat painottivat haastatteluissa hankinnan valmisteluvaiheessa hankintaosaamiseen panostamista. Tämä tulisi näkyä siten, että hankintaprosessin aikana olisi enemmän mahdollisuuksia keskustella asiakkaan todellisista tarpeista ja tarjota asiakkaalle paremmin tarpeisiin soveltuvia toimittajakohtaisia ratkaisuja. Palveluita tarjoavien näkemyksen mukaan tarjouksissa usein pyydetään asioita, joita asiakas ei välttämättä tarvitse tai ne sisältävät elementtejä, joiden hinnoitteluun sisältyy toimittajan kannalta merkittäviä riskejä. Tarjouspyyntöjen kerrottiin olevan usein liian tarkalle tasolle vietyjä ja estävän toimittajia tarjoamasta asiakkaalle heidän mielestään asiakkaalle sopivampia ratkaisuja. Esimerkkeinä nostettiin erilaisen SOC:n tarvitseman teknologioiden kapasiteettitarpeet kuten tarvittava levytila tiedon tallennukseen tai lokien säilytysaika. Yksi haastateltavista kuvasi ongelmaa näin: *”Asiakas voi itse tahtomattaan ja tietämättään muodostaa kilpailutuksen vaatimuksista kokonaisuuden, joka ei olisi tavoitetilan näkökulmasta ihan tarpeellista tai se voitaisiin toteuttaa muulla tavoin ja sitä kautta asiakas joutuu maksamaan turhasta”*.

Palveluita tuottavat asiantuntijat kertoivat haastatteluissa, että toimittajien haasteena on asiakkaiden tapa kopioida toisten asiakkaiden kilpailutusten määrityksiä. Silloin samat SOC

kilpailutuksia koskevat ongelmat toistuvat kilpailutuksesta toiseen. Myös toimittajien edustajien mukaan palveluiden jatkuvasta kehittämisestä sopiminen koettiin haastavana. Hankittavaan palveluun tulisi sisällyttää vahvasti tietoturvakonsultoinnin käytön mahdollisuus, jotta asiakkaan tietoturvan jatkuva kehittyminen turvataan. Yksi haastateltavista toi esille, että SOC hankinnan budjetoinnissa on huomioitava myös sen sidosryhmien toimintaan vaikuttavat muutokset. Haastateltava kertoi, että niiden palveluihin tehtävät muutokset usein maksavat yhtä paljon kuin pelkän SOC:n käyttöönottokin.

SOC palveluita tarjoavien yhtiöiden edustajat kertoivat, että kaupallisia SOC palveluita tarjoavat haluavat usein käyttää itse valitsemaansa teknologiaa, jotta niiden oma toiminta olisi kustannustehokasta. Näitä järjestelmiä ovat esimerkiksi SIEM, SOAR ja erilaiset tiketöintijärjestelmät. SOC:n työkalut vaativat usein erityisosaamista ja yksi SOC ei pysty osaamaan ja hallitsemaan kerralla useita samantyyppiseen käyttötarkoitukseen tehtyjä työvälineitä tai ainakaan se ei olisi kovin kustannustehokasta. Yksi haastateltavista kertoi, että vaatimus käyttää asiakkaan omia SOC työkaluja ovat myös estäneet asiakkaille tarjouksien jättämisen.

6 Johtopäätökset

Lähdeaineiston perusteella SOC:n käyttöönotossa voidaan käyttää systemaattista käyttöönottomallia. Sitä käyttämällä käyttöönoton haasteet tunnistetaan oikea-aikaisesti ja SOC:a käyttöönotettavassa organisaatiossa syntyy yhteinen tavoitetila. Muniz (2021) esitti omassa kirjassaan, että SOC:n perustamiseen tai sen operointiin kannattaa käyttää joitain yleisiä standardeja, ohjeita tai viitekehyksiä. Näin toimien etuna on, että niitä käyttävien käsitteet ovat yhteneväisiä ja viestintä tehostuu. Käytin haastatteluiden pohjana opinnäytetyössäni esittelemääni PPDIOO viitekehystä ja sen vaiheisiin perustuvia kysymyksiä. Mallin vaiheet olivat (0) valmistelu, (1) suunnittelu, (2) palvelumuotoilu, (3) käyttöönotto, (4) operointi, (5) arviointi ja jatkuva kehittäminen. Vaiheet 4–5 rajattiin haastattelujen ulkopuolelle, koska ne eivät liittyneet käyttöönottoon. Haastatteluideni aikana tein kolme havaintoa. Ensimmäinen oli, että kukaan haastateltavista ei tuonut esille, että olisi aiemmin käyttänyt tätä tai muutakaan viitekehystä SOC:n käyttöönottoprojekteissa. Havainnon osalta on kuitenkin huomioitava, että en haastatteluissa kysynyt suoraan olivatko haastateltavat käyttäneet jotain tiettyä mallia aikaisemmin. Toinen havainto oli, että haastateltujen asiantuntijoiden näkemykset kussakin vaiheessa tarvittavista toimenpiteistä erosivat melko paljon haastattelussa käytetystä viitekehyksestä. Mallissa olevat asiat olevat asiat olivat lähes samoja mutta asiantuntijat painottivat omiin kokemuksiinsa perustuen pääsääntöisesti niiden suorittamista jo aiemmin kuin PPDIOO mallissa ne oli kuvattu. Kolmas havainto oli, että asiantuntijat pitivät yleisellä tasolla palvelumuotoilun ja rakentamisen vaiheita melko ongelmattomina, mikäli valmistelu- ja suunnitteluvaiheet ovat hyvin suoritettuja.

Opinnäytetyöni lähdeaineiston perusteella SOC:n arvontuotto-odotuksille ja sen käyttöönotolle pitäisi olla riskienhallinnan kautta johdetut mitattavat perusteet. Kirjallisten lähteiden ja haastatteluiden perusteella SOC:n käyttöönottoa suunniteltaessa tavoitteena on ymmärryttää johdolle, millaisia uhkakuvia yrityksen toimintaan kohdistuu, perustella yrityksen johdolle miksi niiden proaktiiviseen torjuntaan kannattaa panostaa ja saada lupa tarkemman SOC suunnittelun aloittamiseksi. SOC:lle asetettavia odotusarvoja saadaan selkeytettyä valmistelu- ja suunnitteluvaiheessa yhdessä sovittujen mittareiden kautta. Haastatteluiden perusteella käytännössä käyttöönoton valmistelun aloituspäätökseen ei liity suuria haasteita. Päätökseen riittää yleisesti johdon ja valmistelun aloittamista ehdottavien ”yleinen tietoisuus” SOC:n tarpeellisuudesta eli yleinen tietoisuus yrityksiä uhkaavista kyberuhista. Haastatteluissa pidettiin yleisellä tasolla ongelmana liiketoimintojen osaamisen tasoa niitä velvoittavien tietoturvaan liittyvien lakien, asetusten, asiakassopimusten vaatimusten osalta.

Kirjallisten lähteiden ja haastatteluiden perusteella toimiakseen tehokkaasti organisaation on määriteltävä SOC:n rooli, vastuut, järjestettävä toiminnan organisointi ja johtaminen. SOC tarvitsee tietoturva-asiantuntijoiden lisäksi myös liiketoiminnasta päättäviä ja ICT toimittajia. Perustettaessa organisaatioon uusi SOC toiminto, käyttöönottoon liittyvinä haasteina ovat organisaation olemassa olevan tietoturvan osaamisen, tekemisen ja vastuiden nykytilan tunnistaminen sekä olemassa olevan palveluorganisaation yhteensovittaminen. Verkostoitunut SOC myös tuo organisaatiolle tietoa muilta kyberturvallisuuden toimijoilta. Ilman SOC:a tämä luottamuksellinen tieto voi jäädä organisaatiolta kokonaan saamatta. Haastatteluiden perusteella olemassa olevien vastuiden, roolien ja ICT palveluiden selvittämistarpeet ja niiden muutostarpeet nousivat vahvasti SOC:n käyttöönottoon liittyvinä konkreettisina haasteina esille. Erityisenä organisaation sisäisenä haasteena saattaa olla se, että tietoturvavastuista ei olla vielä lainkaan sovittu organisaatiossa. Haastatteluissa korostui olemassa olevien toimijoiden vastuiden, palveluaikojen ja -tasojen yhteensovittaminen SOC:n palveluihin. Tämän opinnäytetyön lähdeaineistossa nämä asiat eivät tulleet esille. Haastatteluiden mukaan ongelmia tuottaa erityisesti olemassa olevat IT toimittajien palvelusopimukset ja niiden vastuumatriisit, joissa SOC:n roolia ei ole määritelty.

Lähdeaineiston ja haastatteluiden perusteella SOC palveluita tuotetaan usein 24/7/365 periaatteella ja tämän seurauksena siitä seuraa merkittäviä tuotantokustannuksia. Palveluaikavaade tuo myös haasteita työntekijöiden työehdoista sopimiseen. Palveluiden organisointimallina tuotiin esille itse tekeminen, SOC palvelun ulkoiselta palvelutoimittajalta hankkiminen ja hybridimalli. Lähdeaineiston mukaan, mahdollisimman varhaisessa vaiheessa ja käyttöönottoa vasta suunniteltaessa, erilaisten tuotantotapojen vertailuun kannattaa käyttää aikaa ja omien henkilöresurssien käytön arviointiin tulisi ottaa mukaan henkilöstöhallinnon osaamista. Tämä vertailu ei kuitenkaan noussut haastatteluissa lainkaan esille.

Opinnäytetyöni lähdeaineiston mukaan SOC:n kyvykkyydet jaetaan kolmeen osa-alueeseen; ihmiset, prosessit ja teknologiat. Opinnäytetyöni lähteiden ja haastatteluiden perusteella tunnistetuilla ja oikein arvioiduilla kyvykkyyksillä käyttöönottoprojektille annetaan vankka pohja niin aikataulun, kustannusten kuin projektin lopputuloksen eli perustetun SOC:n arvon odotuksen osalta. Tarvittavien kyvykkyyksien tunnistaminen ja saatavuus ovat erityisesti SOC:n käyttöönoton valmistelu- ja suunnitteluvaiheen ongelmia. Alussa organisaatiolla ei tyypillisesti ole riittävää osaamista tehdä SOC:n kyvykkyysien arviointia, aikaisempaa kokemusta SOC:n käyttöönotoista tai osaamisen laatu ei ole muutoin riittävää. Tällä ei tarkoiteta pelkästään SOC asiantuntijaosaamisen puuttumista, vaan myös esimerkiksi taitoa tunnistaa liiketoiminnan tietoturvatarpeita SOC:lle. Haastatteluissa oman organisaation SOC:n käyttöönoton kannalta merkityksellisten kyvykkyyksien kartoitus ja kypsyystasoista saatava oikea arvio nousi erityisen tärkeäksi jo heti käyttöönoton valmistelun alkuvaiheessa. Haastatteluissa korostui erityisesti ihmisiin ja prosesseihin liittyvät haasteet ja teknologiaan liittyvien haasteiden ratkaisua pidettiin helpompana.

Teknologia on SOC:lle sekä opinnäytetyöni lähdeaineiston että haastatteluiden perusteella hyvin merkityksellinen. Molempien tietolähteiden perusteella SOC palveluita ei voi tuottaa ilman teknologiaa ja se on SOC:n yksi keskeinen kyvykkyyden osa-alue. Lähdeaineisto korostaa teknologiaa arkkitehtuurin, käyttötarpeen ja valitun ratkaisun toteutuksen näkökulmasta. Esimerkkeinä tästä ovat muun muassa opinnäytetyössäni viittaukset teknologiaan, joita käytetään kyberhyökkäysten havainnointiin, torjuntaan ja jälkikäteen tehtävään analysointiin. Haastatteluissa, joissa asiaa tarkasteltiin erityisesti haasteiden näkökulmasta, painottui että teknologilta usein odotetaan enemmän kuin sitä käyttämällä saadaan. Haastatteluissa korostettiin, teknologia ei yksistään ratkaise mitään ja että osaavat ihmiset, hyvin johdettu organisaatio hyvin mietittyine prosesseineen ovat käytetyn teknologian rinnalla usein tärkeämpiä kuin teknologiset valinnat. Haastatteluiden perusteella haasteena pidettiin, että usein jo hankittua tietoturvateknologiaa ei käytetä ilman SOC:a tehokkaasti ja odotusarvo teknologialle kyberongelmien ratkaisussa ylimitoitetaan. Tästä tietoa ei lähdemateriaalissa ollut.

Lähdeaineiston perusteella opinnäytetyössäni palvelut ovat ryhmitelty palvelualueisiin ja niiden sisältämiin palveluihin. Aineisto ei suoraan kerro, missä järjestyksessä tai mitkä palvelut tulisi ensiksi ottaa käyttöön. Aineisto korostaa riskien arviointiin perustuvaa SOC palveluiden valintaa. Haastatteluissa SOC:n palvelut tunnistettiin ja niiden käyttöönottoa ei pidetty erityisen haasteellisina, kunhan valmistelu ja suunnitteluvaiheet ovat suoritettu hyvin ja laadukkaasti. Haastatteluiden perusteella tuotiin kuitenkin esille, että tietoturvatapahtumien ja -poikkeamien palvelut ovat käytännössä ne, joiden käyttöönottamisella yleisimmin lähdetään liikkeelle.

SOC:n hankkiminen palveluna oli teema, jossa lähdeaineisto ja haastatteluissa saatu tieto poikkesivat toisistaan eniten. Hankintaan liittyviä haasteita käsiteltiin julkisissa

lähdemateriaaleissa ylipäätään hyvin vähän ja lisäksi haastatteluissa SOC:n käyttöönottoon liittyvät hankinnan haasteet polarisoituvat sekä niitä ostavien tai itse tekevien ja palveluita tarjoavien välillä. Lähdeaineiston mukaan erilaisia toteutusvaihtoehtoja hankkia SOC ja siihen liittyviä palveluita on useita. SOC voidaan toteuttaa tehden palvelu kokonaan itse, hybridimallina tai ulkoistamalla palvelu kokonaan palvelutoimittajalle. Palveluissa käyttävät henkilöresurssit, teknologiat, prosessit ml. immateriaalioikeudet voivat olla joko omia tai ulkoa hankittuja. Organisaation tulee valita itselleen sopivin malli ja valinnan tulee perustua liiketoimintatarkasteluun sekä -päätökseen. Valittavaa toimintamallia ohjaa organisaation kulttuuri, strategia, omien resurssien määrä, oma osaaminen ja taloudellinen kannattavuus.

Lähdeaineiston ja haastatteluiden perusteella SOC:n hankintaan liittyviä haasteita käsitellään pitkälti SOC:n verkostoitumiseen ja eri toimijoiden keskinäiseen työnjakoon sekä palvelusopimuksiin liittyvinä haasteina, että ennakko-odotuksina. Yksi keskeinen hankintaan liittyvä käyttöönoton onnistumisen kriteeri on, miten hyvin saavutetaan hyvin toimiva ja saumaton yhteistoiminta eri toimijoiden välillä.

Lähdeaineiston ja haastatteluiden perusteella SOC:t tarvitsevat toimiakseen teknologiaa ja SOC:n käyttämien tietojärjestelmien pitää soveltua niitä käyttäjälle organisaatiolle. Johtuen organisaatioiden erilaisista teknologiavalinnoista, SOC:lle optimaalinen teknologinen ratkaisu voi olla eri organisaatioissa hyvinkin erilainen. Haastatteluissa palveluita ostavat tai niitä itse tekevät perustelivat työkalujen valintaa ja niiden omistamiseen liittyviä etuja. Erityisesti SIEM järjestelmien osalta omistajuus nähtiin tärkeänä. Lähdeaineistosta ei löytynyt tietoa, millaisia vaikutuksia sillä on, hankitaanko SIEM järjestelmät itse tai esimerkiksi osana SOC palvelutoimitusta. Haastateltujen asiantuntijoiden mukaan, kun järjestelmä valitaan ja hankitaan itse, voidaan saada parhaiten juuri omaan käyttötarkoitukseen sopiva ratkaisu. Työkaluihin tehdyn kehitystyön säilyminen organisaatiossa nähtiin myös etuna. Palveluita tarjoavat kokivat työkalujen eriyttämisen palveluhankinnasta heikentävän palveluiden tuottamisen kustannustehokkuutta ja vaikeuttavan heidän työkalujen osaamisen hallintaa, ja tätä kautta se näkyy myös asiakkaille negatiivisena. Toimittajien edustajat nostivat esille asiakashyötyjä, mikäli hankintaprosessissa annetaan toimittajille enemmän liikkumatilaa ratkaisuehdotusten tekemiseksi. Julkisen sektorin toimijoiden osalta tämä edellyttää hyvää lain julkisista hankinnoista ja käyttöoikeussopimuksista osaamista ja sen soveltamista.

7 Pohdinta

Tässä pääluvussa ja sen alaluvuissa käyn läpi omia ajatuksiani, päätelmiäni ja ideoita opinnäytetyöni aihealueeseen peilaten.

Opinnäytetyön kirjoittajana itselläkin on kokemusta SOC:n käyttöönotosta ja useamman vuoden SOC palveluiden johtamisesta. Tietoaineistoon perehtyessäni ja myöhemmin tekemissäni haastatteluissa välittyi usein samat reaalielämässä kokemani SOC:in liittyvät haasteet, joita olen itsekin kokenut. Haastatteluissa kuulemani havainnot käyttöönottoon liittyvistä haasteista olivat asiantuntijoiden välillä hyvin yhteneväisiä, vaikka erojakin oli. Yhtenäiseen tulokseen todennäköisesti vaikutti se, että haastateltavilla oli sekä osaamista että käytännön kokemusta joko useamman SOC:n perustamisesta tai niiden käyttöönottoihin liittyvästä konsultoinnista.

7.1 Miten SOC perustellaan?

Uskon, että organisaatiokulttuuri vaikuttaa paljon siihen miten uusiin ideoihin suhtaudutaan ja kuinka helppoa tai vaikeaa niiden eteenpäin vieminen voi organisaatiossa olla. Myös organisaation oma asenne tietoturvallisuuteen, oman toimialan tai sen asiakkaiden tietoturvavaatimukset ja miten turvallisuutta ylipäätään kehitetään omassa organisaatiossa vaikuttaa SOC:n käyttöönottoon. Näihin liittyvät tavoitteet näkyvät usein organisaation visiossa, strategiassa ja asiakassopimuksissa. Niihin tutustuminen luo hyvän pohjan SOC:n käyttöönottoa suunnittelevalle.

Organisaatioilla on usein kehityssalkussaan paljon erilaisia kehitysideoita ja käynnissä olevia projekteja, jotka kilpailevat samoista resursseista. Osa tekemisestä perustuu lainsäädännön vaatimuksiin, osa suoraan asiakassopimuksiin tai mahdollisuuksiin saada uusia asiakkaita, osa tehostaa toimintaa ja osa varmistaa toiminnan jatkuvuuden. Yksi tapa priorisoida tekemistä, on kehittää kokonaisvaltaista riskienhallintaa. Sen tarkoitus on varmistaa, että organisaatio saavuttaa itselleen asettamansa strategiset, myös turvallisuuteen liittyvät, tavoitteet. Tietoturvaan liittyvä riskienarviointi ja erityisesti siihen liittyvä liiketoiminnan häiriöiden vaikutuksen arviointi kannattaa tehdä huolella. Hyvin tehty analyysi antaa hyvän pohjan keskusteluihin johdon kanssa, onko SOC tarpeellinen ja paljonko siihen kannattaa sijoittaa. Samalla voi saada hyviä onnistumisen seurannan mittareita ja perusteen SOC toiminnan jatkuvuudelle.

Hetki, jolloin SOC:n hankintaa vasta harkitaan ja valmistellaan, on organisaatiolle tärkeä mutta myös haastava vaihe. Todennäköisesti SOC:iin liittyvät käsitteet ja asiat ovat organisaatiossa suurelle osalle uusia. SOC:n roolia ja sen tuomia hyötyjä on vaikea hahmottaa. Erilaiset ennakkokäsitykset myös saattavat vaikeuttaa päätöksentekoa ja SOC:n käyttöönotto projekti saattaa joutua kilpailemaan muiden yritykselle tärkeiden hankkeiden kanssa. SOC:n hyötyjen esille tuomiseksi on löydettävä yrityksessä yhteinen, liiketoiminnan ymmärtämä, kieli. Käyttöönoton hyötyjä voi perustella erilaisten käyttötapausten avulla. Niillä johdolle konkretisoidaan SOC:n hyötyjä sekä mittarien avulla. Alkuvaiheessa haasteena kuitenkin on, että organisaatiossa usein ei ole riittävää omaa osaamista käyttötapausten määrittelemiseksi.

7.2 Miten SOC käyttöönotetaan?

SOC:n käyttöönottoon liittyy paljon saman kaltaisia haasteita kuin minkä tahansa uuden toiminnon tai palvelun käyttöönottoon. Verrattuna ICT palveluiden tuottamiseen, SOC palveluita on maailmalla tuotettu vielä melko vähän aikaa, ja pidempiaikaisia kokemuksia SOC palveluiden käyttöönotoista on kertynyt vielä melko vähän.

Muniz (2021) mukaan perustettaessa SOC:a kohdataan tyypillisesti neljä haastetta: (1) kyvykkyyksien ja asiantuntijoiden saavuus, (2) alhainen maturiteetti, (3) tiedon saamiseen liittyvät rajoitteet ja puutteet ja (4) kyky perustaa ja kehittää SOC palveluita. Näiden haasteiden ratkaiseminen olisi todennäköisesti tehokkaampaa, jos panostetaan systemaattisen käyttöönottomallin käyttöön. Tarjolla on, opinnäytetyössänikin mainitun PPDIOO lisäksi, useita muitakin viitekehyksiä ja oppaita tietoturvan kehittämiseksi ja jotkin niistä soveltuvat myös SOC:n palveluiden käyttöönottoon. Hyödyntämällä näitä valmiita malleja käyttöönottoon liittyvät asiat tulevat oikea-aikaisesti päätettäväksi ja varmistetaan, että tärkeät asiat eivät unohdu. Myös odotus SOC:n hyödystä organisaatiolle kirkastuu. Tässä opinnäytetyössä käytetyssä PPDIOO mallin palvelusuunnitteluvaiheessa systemaattisen palvelunmuotoilun menetelmien käytöstä voisi olla paljonkin hyötyä ja siten tehostaa SOC:n tuottamisen palveluiden suunnittelua. Ojasalo, Koskelo & Nousiainen (2015) ovat omassa artikkelissaan kuvanneet yhden mallin palvelusuunnitteluun.

Haasteellisuus on käsite, joka kuvaa tehtävän, tilanteen tai ongelman vaikeusastetta tai vaativuutta. Se heijastaa sitä, kuinka haastavaa tai vaikeaa jokin asia on suhteessa yksilön tai organisaation kykyihin, taitoihin tai resursseihin. Lähdemateriaalissa SOC käyttöönottoon liittyvät asiat esitetään pääosin siihen kuuluvina tehtävinä ja niihin liittyviä erityisiä haasteita käsitellään vähemmän. Tehtävien haasteellisuus ei avaudu lukijalle välttämättä samalla tavoin merkittävinä haasteita kuin ne haastateltavien kertomana esitettiin. Haasteellisuus käsitteenä sisältää myös subjektiivisen näkemyksen. Se mikä toiselle on hyvinkin haasteellista, voi olla toiselle hyvinkin helppoa.

Onko tehokkain tapa tehdä SOC palvelut itse, ostaa kokonaan ulkoa vai rakentaa jonkinlainen hybridimalli? Tähän kysymykseen ei ole olemassa yhtä vastausta ja valintaan vaikuttaa usea tekijä. Kyky ja halu investoida omaan tietoturvaorganisaatioon, tietoturvan merkitys organisaation liiketoiminnalle, organisaation koko, olemassa olevat kyvykkyydet ovat joitain päätöksentekoon vaikuttavia kriteereitä.

SOC:n käyttöönotossa pätee sama sanonta kuin muussakin uuden tekemisessä: ”hyvin suunniteltu on puoliksi tehty”. Valmistelu-, määrittely- ja suunnitteluvaiheet ovat tyypillisesti vaiheita, joissa korostuu organisaation omat tarpeet ja vaatimukset. Palveluiden tekniseen käyttöönottoon ei liity merkittäviä haasteita, jos nämä vaiheet ovat huolellisesti tehty. Myös

käyttöönottoprojektiin liittyvien ulkoisten toimijoiden on helpompi tuoda mukaan oma osaamisensa, kun vaatimukset lopputulokselle ovat selkeitä.

7.3 Kyvykkyyksien määrittely

Kuinka hyvin ja realistisesti omia kyvykkyyksiä osataan arvioida? Ja miten arviointi tulisi tehdä erityisesti silloin kun ollaan tilanteessa, jolloin ollaan tekemässä jotain uutta? Teorian, haastatteluiden ja kokemukseni perusteella johtopäätökseni on, että reaalielämässä omien kyvykkyyksien selvittämiseen panostetaan usein liian vähän. Kyvykkyysarviointien tekoon kannattaa kuitenkin panostaa. Niiden lopputulosten perusteella saa hyvän lähtökohdan omalle muutosmatkalleen. Välitavoitteet matkalle löytyvät usein asiaan soveltuvista viitekehyksistä, oppaista ja asiantuntijaverkostosta. Kyvykkyyksien määrittelyssä tulee käyttää riittävää substanssiosaamista. Muutoin on usein vaarana omien kyvykkyyksien yli- tai aliarviointi. Yliarviointi on näistä ongelmallisempi. Mikäli esimerkiksi SOC:n tarvitsemia kyvykkyyksiä ei kartoiteta riittävän hyvin, ongelmat näkyvät SOC:n käyttöönottoprojektissa kustannusten kasvuna, käyttöönoton aikatauongelmina sekä myöhemmin jatkuvina ongelmina SOC:sta saatavan arvo-odotuksen saavuttamisessa.

7.4 SOC toiminnan organisointi ja johtaminen

Harkittaessa SOC:n käyttöönottoa saatetaan olla tilanteessa, jossa kyberturvallisuuden vastuista ja poikkeamien käsittelystä ei olla organisaatiossa kattavasti sovittu tai SOC johtaminen edellyttäisi asian uudelleen arviointia. Kokemukseni mukaan, jota tekemäni haastattelutkin tukivat, organisaatio yliarvioi sekä SOC:n roolia, että kykyä ratkaista teknologialla kyberongelmia. Tilanteissa, jolloin organisaatio havaitsee kyberpoikkeaman ja joka edellyttää tietotekniikan käytön rajoittamista, otetaan kantaa myös yrityksen liiketoiminnan jatkuvuuteen. Mikäli SOC palveluita tuotetaan ulkoisen palvelutoimittajan toimesta niin tämä tarkoittaisi, että rajoittamiseen liittyvä liiketoimintapäätöskin olisi delegoitu ulkoiselle toimijalle. Tämän tyyppistä päätöksentekovaltaa harva organisaatio haluaa antaa ulos ja harva ulkoinen toimija haluaa ottaa vastuulleen.

SOC palveluita pitää jatkuvasti kehittää ja palvelun jatkuvan kehittämisen pelisäännöistä tulee sopia jo varhaisessa vaiheessa. Mikäli SOC palveluita ei aiota tuottaa itse, on jo kilpailutusvaiheessa mietittävä, miten SOC palveluita kehitetään. Operatiivisia palveluita tuottavalla ulkoisella palvelutoimijalla ei välttämättä ole intressejä kehittää palveluita suuntaan, jossa palveluiden tuotto vähenee. Tämä saattaa olla täysin vastakkainen intressi asiakkaan näkökulmasta, joka haluaa parempia palveluita edullisemmin.

Kyberrikollisilla ei ole palveluaikaa vaan ne toimivat jatkuvasti ja riski kyberhyökkäyksille on jatkuva. Sen vuoksi SOC:n palveluaikaan liittyy usein vaatimus saada palvelua 24/7/365, joka tarkoittaa ympärivuorokautista ja ympäri vuoden tapahtuvaa keskeytyksetöntä toimintaa.

Oman toiminnan tuottamiseen 24/7365 periaatteella liittyy kuitenkin paljon tyypillisiä jatkuvan vuorotyön haasteita. Ylläpitääkseen jatkuvaa toimintaa työnantajan on varmistettava, että henkilöstöä on riittävästi eri vuorokauden aikoina ja pyhinä. Työnantajan on myös suunniteltava ja toteutettava työvuorosuunnittelu, joka huomioi henkilökunnan työaikatoiveet ja -tarpeet. Tarve voi vaihdella eri aikoina. Myös viestintä on 24/7/365 toimintamallissa paljon haastavampi järjestää kuin käytettäessä normaalia työaikamallia. Haasteet viestinnän ja tiedonvälityksen osalta ovat moninaisia. Miten esimerkiksi tiimipalaverit ja vuoronvaihtojen yhteydessä tiedon vaihto toteutetaan?

On hyvin tärkeää sopia SOC:n vastuista ja roolista ICT palveluissa ja niiden prosesseissa. Haasteena on usein toimittajien välisestä yhteistyöstä ja tavoitteista sopiminen. Joitain vuosia sitten tutustuin palveluiden integrointi ja hallinta (Service Integration and Management, SIAM) viitekehykseen. Sen mukaista toimintaa ei ole helppo tuoda osaksi olemassa olevaa toimittajasopimuskokonaisuutta, mutta suosittelen siihen tutustumista, kun toimittajien välistä yhteistoimintaa kehitetään.

7.5 Hankinnan haasteet

Hyviä käytäntöjä ja esimerkkejä SOC palveluiden hankkimiseksi löytämissäni tietolähteissä oli hyvin vähän. Haasteet kulminoituvat siihen, miten osataan määritellä juuri omalle organisaatiolle paras ratkaisu, miten palvelun tuottamista mitattaan ja miten sitä jatkuvasti kehitetään. Mikäli omassa organisaatiossa ei ole kokemusta SOC:ien käyttöönotoista, suunnitteluun ja kilpailutukseen kannattaa käyttää konsultointia. SOC palveluita hankkivien ja niitä toimittavien käsitykset SOC:n hankinnasta polarisoituvat erityisesti SOC:n käyttämän teknologian hankinnan osalta. Siinä missä SOC:n palvelu- ja teknologiakehittämisen eriyttäminen voidaan nähdä SOC:n operoinnin näkökulmasta hankalana ja kustannustehottomana niin se voidaan nähdä myös mahdollisuutena hankkia juuri omalle organisaatiolle sopivaa teknologiaa. Teknologian omistaminen voi myös varmistaa jo tehtyjen kehitysinvestointien pysyminen omassa organisaatiossa. Kääntöpuolena tulee yleiset omistamisen haasteet, kuten valintaan liittyvät riskit ja teknologian ylläpitoon saatavan osaamisen saatavuus.

Haastatteluiden jälkeen jäi itseäni mietityttämään, mikä on hankinnan haasteiden juurisyy. Vaikka taustalla saattaa olla kaupallisiakin tekijöitä niin en kuitenkaan usko, että ne selittävät asian kokonaan. Itse uskon, että asiaan vaikuttaa moni asia. Yksi merkittävä tekijä on erityisesti SOC palveluiden hankkimiseen tarvittavan osaamisen ja kokemuksen saatavuus. Opinnäytetyön hankintaa koskevat tärkeimmät ratkaisuehdotukseni ovat: panosta hankintaosaamiseen jo valmistelu- ja määrittelyvaiheessa, tee oma tietoturvan riskienarviointi ja varmista liiketoiminnan tarpeiden ymmärtäminen tekemällä riittävän kattava liiketoiminnan vaikutusten arviointi.

7.6 Oikean teknologian valinta?

SOC tarvitsee toimiakseen teknologiaa ja usein ensimmäiseksi hankintavaksi tulee SIEM järjestelmä. SIEM järjestelmällä tulisi kyetä käsittelemään kaikki oleelliset yrityksen kyberturvallisuuden käyttötapaukset. SOC:n työkaluihin liittyvät tarpeet tulee kartoittaa ja sopia erityisen hyvin etenkin silloin, kun SOC:n tietoturvatapahtumien tai poikkeamien hallinnan aiotaan hankkia ulkopuoliselta toimittajalta. Mikäli järjestelmä päätetään hankkia itse, toimintamalli sisältää useita haasteita ja riskejä. Ensimmäinen riski on, että resursseja tai osaamista käyttötapausten määrittelyyn ja sitä kautta järjestelmävalintaan ei ole riittävästi ja valitaan vääränlainen järjestelmä. Toinen riski on, että kilpailutettaessa SOC:n palvelutuottajaa, ei omaan käyttöön valitulle SIEM järjestelmälle ei löydy montaa osaajaa. Tämä saattaa karsia tarjoajia tai vähäinen tarjonta nostaa hintoja. Kolmas riski on, että palvelutuottaja ei osaa käyttää järjestelmää tehokkaasti tai se integroituu huonosti palvelutuottajan muuhun palveluympäristöön. Tämä taas voi aiheuttaa puutteita tietoturvapoikkeamien havainnointikyvyssä tai nostaa palvelun hintaa.

Tekoälyn käyttö laajenee nopeasti ja siihen liittyvät teknologiat ja sovellukset ovat tulleet yhä näkyvämmiksi ja helpommin saataville. Tekoälyn kehittyminen tietoturvapoikkeamien analysointiin, voi tuoda aivan uusia mahdollisuuksia sitä käyttävien organisaatioiden käyttöön. On todennäköistä, että tekoälystä muodostuu eräänlainen virtuaalinen SOC. Tekoälyn käyttö anomalioiden tunnistamiseen kasvaa varmasti ja tämä kyvykkyys tulee yhä enemmän osaksi SIEM ja/tai SOAR työkaluja.

7.7 Reflektointi opinnäytetyömatkastani

Oman osaamisen kasvattamisen lisäksi halusin työni teoriaosuudessa avata myös lukijalle SOC:iin liittyvää aihetta laajasti, tuoden tietoa riskienhallinnasta, kyberuhkista ja SOC:sta kokonaisuutena. Tällä tavoittelin, että lukija voi itsekin paremmin arvioida näiden asioiden keskinäisriippuvuuden merkitystä myös empiirisessä osassa saatujen tulosten osalta. En myöskään voinut ennen haastatteluita olla varma, millaisia haasteita haastateltavat haastatteluissa toisivat esille, joten päädyin sen vuoksi kartoittamaan SOC aihetta laajasti.

Työni tilaajana toimi Laurea ammattikorkeakoulu, jonka vuoksi toin työhöni koulutuksen toimialaan tietoturvaan liittyviä regulaatiovaatimuksia ja kyberuhkia syvällisemmin. Opinnäytetyöni lähti prosessina liikkeelle Laurean tarpeesta käyttöönottaa SOC. Ensimmäinen suunta opinnäytetyölle rakentui ”Laurean SOC:n käyttöönotto ja kustannukset” teeman alle. Ensimmäisen vedoksen perusteella, ja opinnäytetyön ohjaajan pyynnöstä, otimme työhöni mukaan enemmän riskienhallinnan näkökulmaa. Tavoitteena oli käsitellä ja verrata riskienhallinnan keinoin erilaisten SOC:n palveluiden käyttöönottoa (hyödyt, riskit, hinta) Laurealle. Parin vedoksen ja ymmärryksen lisääntymisen jälkeen havaitsin, että sellaisenaan opinnäytetyötä oli mahdotonta toteuttaa. En tiennyt todellisia Laurean tietoturvariskejä. Havainnon jälkeen

opinnäytetyöni tutkimuskysymystä muutettiin enemmän yleisempään SOC:n käyttöönoton haasteiden tunnistamiseen suuntaan. Myöhemmin, kun haastatteluidenkin kautta vahvistui käyttöönoton haasteiden melko vähäiset toimialakohtaiset erot, tämä osoittautui oikeaksi päätökseksi. Tämä ei kuitenkaan tarkoita, etteikö SOC:a käyttöönotettaessa toimialakohtaiset erityishaasteetkin olisi arvioitava organisaation riskienhallinnassa ja tuotava sitä kautta osaksi omaa SOC:n käyttöönoton suunnittelua.

Tietoturvauhkien määrä on koko ajan kasvussa ja tietoturvahäiriöiden toteutuminen saattaa keskeyttää yrityksen koko liiketoiminnan. Tässä opinnäytetyössä tarkastelin asiaa erityisesti koulutuksen toimialan kautta, mutta myös muut toimialat ovat jatkuvien kyberhyökkäyksien kohteena. Suuremmat yritykset voivat usein panostaa pieniä yrityksiä paremmin tietoturvaan. Opinnäytetyötä tehdessäni pohdin, miten pienten yritysten tietoturvapalvelut, mukaan lukien SOC palvelut, saadaan toteutettua kustannustehokkaasti. Pienten yritysten ottaessa käyttöön julkisia pilvipalveluita, näihin palveluihin ”sisäänrakennetut” tietoturvapalvelut ja -kontrollit mahdollistavat myös pienille yrityksille tehokkaiden ja aikaisemmin vain suurille yrityksille mahdollisten tietoturvaratkaisujen käyttöönoton.

7.8 Ehdotukset jatkotutkimusaiheiksi

Tämän opinnäytetyön jatkotutkimusaiheina voisi toteuttaa SOC:n perustamisen tässä opinnäytetyössä mainitun käyttöönottomallin mukaisesti. Käyttöönottomallin käytön arvioinnin osalta olisi kiinnostavaa tietää selkeyttääkö ja tehostaako se organisaation mielestä käyttöönottoa?

Yrityksen omien SOC kyvykkyyksien tai jonkin kyvykkyyden (ihmiset, prosessit, teknologia) konkreettisen kehitystyön toteuttaminen voisi tuottaa arvokasta tietoa muille SOC palveluiden käyttöönottoa harkitseville.

Konkreettinen SOC palveluiden kilpailutus valmisteluineen voisi myös olla mielenkiintoinen aihe. Kilpailutukseen liittyvän työn näkökulma voisi olla esimerkiksi, miten palveluiden ja teknologian eriyttäminen käytännössä tehtiin.

SOC:n toiminnan edellyttämän ICT palvelutoimittajien yhteystyömallin kehittämisestä voisi myös saada mielenkiintoisen työn. Työssä voisi olla näkökulmana, miten eri ICT toimittajien rooleista ja vastuista tulee sopia sekä miten käyttöönotto mahdollistetaan.

Lähteet

Painetut

Ilmonen, I., Kallio J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. 1. lisäpainos. Helsinki: Kustannusosakeyhtiö Tammi.

Jarpey, G. & Mccoy, S. 2017. Security Operations Center Guidebook: A Practical Guide for a Successful SOC.

Leppänen J. 2006. Yritysturvallisuus käytännössä. Helsinki: Talentum.

Metsämuuronen, J. 2006. Laadullisen tutkimuksen käsikirja. 1. painos. Jyväskylä: Gummerus Kirjapaino Oy.

Muniz, J. McIntyre G & Alfardan N. 2016. Security Operation Center. U.S. Indianapolis: Cisco Press.

Muniz, J. 2021. The Modern Security Operations Center. 1st edition. U.S.: Addison-Wesley Professional.

Nathans, D. 2014. Designing and Building Security Operations Center. 1st Edition. U.S.: Syngress Media.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. 3.–4. painos. Helsinki: Sanoma Pro Oy.

Parker, D. 1998. Fighting Computer Crime: A New Framework for Protecting Information. Wiley.

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet. Helsinki: Suomen standardoimisliitto.

SFS-EN ISO/IEC 27000. 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen standardoimisliitto.

SFS-ISO/IEC 27005. 2018. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta. Helsinki: Suomen standardoimisliitto.

SFS-ISO/IEC 27035-1. 2016. Helsinki: Suomen standardoimisliitto.

SFS-opas 73. 2011. Riskienhallinta. Sanasto. Helsinki: Suomen standardoimisliitto.

The CRISC Review Manual 7th Edition. 2021. ISACA.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Kustannusosakeyhtiö Tammi.

Sähköiset

(ISC)². 2020. Cybersecurity Professionals Stand Up to a Pandemic. Viitattu 27.7.2021. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDriven-WhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

Ammattikorkeakoululaki 932/2014. https://www.finlex.fi/fi/laki/ajantasa/2014/20140932#P25

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999. Viitattu 24.7.2021. https://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Campbell, S. 2021. Cybersecurity in Higher Education: Problems and Solutions. Viitattu 31.10.2021. https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

Cichonski, P., Millar, T., Grance, T. & Scarfone, K. 2012. Computer Security Incident Handling Guide. 7.11.2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cisco. 2010. PPDIOO Lifecycle Approach to Network Design and Implementation. Viitattu 28.7.2021. https://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3

Collins, J. 2021. Create an SOC Target Operating Model to Drive Success. Viitattu 21.10.2021. https://www.gartner.com/doc/reprints?id=1-279ZG8HN&ct=210824&st=sb

Computer Security Incident Response Team (CSIRT) Services Framework, version 2.1. 2019. FIRST. Viitattu 15.8.2021. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Viitattu 31.10.2021. https://www.researchgate.net/publication/326309769_Defining_Cybersecurity

CyberEdge Group. 2021 Cyberthreat Defense Report. Viitattu: 30.6.2022. https://cyberedge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf

Department of Defense Dictionary of Military and Associated Terms 2001. Department of the army United States of America. Viitattu 22.7.2021. https://fas.org/irp/doddir/dod/jp1_02-april2010.pdf

Euroopan kyberturvallisuuden verkosto ja osaamiskeskus. 2021. Viitattu 23.4.2023. https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=LEGISSUM%3A4532506)

F-Secure 2021. F-Securen tietoturvanäkymät vuoteen 2021. Viitattu 22.10.2021. https://www.f-secure.com/fi/press/p/f-securen-tietoturvaturvanaekymaet-vuoteen-2021

Forsberg, J. 2022. Measuring the technical performance of a security operations center. Viitattu 21.5.2023. https://jyx.jyu.fi/handle/123456789/84367

Gartner 2021. CIRT (Cyber Incident Response Team). Viitattu 7.11.2021. https://www.gartner.com/en/information-technology/glossary/cirt-cyber-incident-response-team

Kauppi, J. 2022. 3 yleisintä tietoturvariskiä ja asiantuntijoiden vinkit niiden välttämi-seen. Viitattu 12.10.2022. https://www.asiakastieto.fi/web/fi/asiakastieto-media/blogit/3-yleisinta-tietoturvariskia-ja-asiantuntijoiden-vinkit-niiden-valttamiseen.html

Keltanen, P 2019. Measuring outsourced Cyber Security Operations Center. Viitattu 21.5.2023. http://www.theseus.fi/handle/10024/265393

Kokonaisturvallisuuden sanasto. 2017. Turvallisuuskomitea. Viitattu: 22.10.2021. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Kybersää Helmikuu 2023. Traficom.Viitattu 8.4.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20helmikuu%202023.pdf

Kybersää Tammikuu 2023. Traficom. Viitattu 8.4.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20tammikuu%202023_0.pdf

Kyberturvallisuuden sanasto 2018. Turvallisuuskomitea. Viitattu 31.10.2021. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Kyberturvallisuus ja yrityksen hallituksen vastuu 2020. Traficom. Viitattu 23.4.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskus 2020. RFC 2350. Viitattu 12.11.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert/rfc-2350

Kyvykkyyksien johtamisen käsikirja 2018. Espoon kaupunki. Viitattu 25.3.2023. https://6aika.fi/wp-content/uploads/2019/06/Kyvykkyyksien-johtamisen-ka%CC%88sikirja.pdf

Laki viranomaisten toiminnan julkisuudesta 621/1999. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Lanne, M & Heikkilä, J. 2016. Uutta riskien arviointiin!. Viitattu 22.10.2021. https://helda.helsinki.fi/bitstream/handle/10138/224445/114469-loppuraportti_A.pdf?sequence=1&isAllowed=y

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Viitattu 25.9.2021. https://www.vttresearch.com/sites/default/files/pdf/publications/2007/P632.pdf

Lindström, O. 2028. Next Generation Security Operations Center. Viitattu 21.5.2023. http://www.theseus.fi/handle/10024/157357

Logpoint 2020. What is a Security Operations Center (SOC)?. Viitattu 28.7.2021. https://www.logpoint.com/en/blog/security-operations-center/

Lubna, A, Baber, A & Umar, K. 2015. Security Operations Center – A Need for an Aca-demic Environment. Viitattu 31.10.2021. https://ieeexplore.ieee.org/abstract/document/7368297

McAfee 2020. What Is a Security Operations Center (SOC). Viitattu: 28.7.2021. https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html

Microsoft 2020. Microsoft Digital Defense Report. Viitattu 31.10.2021. https://go.microsoft.com/fwlink/p/?LinkID=2154950&clcid=0x40b&culture=fi-fi&country=FI

Microsoft 2021. Microsoft Digital Defense Report. Viitattu 29.10.2022. https://go.microsoft.com/fwlink/p/?LinkID=2154950&clcid=0x40b&culture=fi-fi&country=FI

Microsoft 2022. Microsoft Digital Defense Report. Viitattu 5.11.2022. https://go.microsoft.com/fwlink/p/?LinkID=2154950&clcid=0x40b&culture=fi-fi&country=FI

Moyle, E. 2021. CERT vs. CSIRT vs. SOC: What's the difference?. Viitattu 7.11.2021. https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Muniz, J. 2015. 5 Steps to Building and Operating an Effective Security Operations Center (SOC). Viitattu 31.10.2021. https://www.ciscopress.com/articles/printerfriendly/2460771

Ojasalo, K., Koskelo, M. & Nousiainen, A. K. 2015. Foresight and Service Design Boosting Dynamic Capabilities in Service Innovation. Viitattu 1.6.2023. https://www.academia.edu/download/38878030/Ojasalo_Koskelo_Nousiainen_chapter_HOSI_2015.pdf

Opetushallitus 2021. Tietoturva ja -suoja koulussa. Viitattu: 27.7.2021. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa

Opinnäytetyö AMK-tutkinnossa 2021. Laurea ammattikorkeakoulu Oy. Viitattu 2.5.2021. https://laureauas.sharepoint.com/sites/studentFin_opinnaytetyojavalmistuminen/SitePages/Opinnäytetyö.aspx#arviointi-ja-työelämän-palaute

OWASP. 2019. OWASP Security Operations Center (SOC) Framework Project. Viitattu 7.11.2021. https://wiki.owasp.org/index.php/OWASP_Security_Operations_Center_(SOC)_Framework_Project

Passeri, P. 2020. Monthly Attacks (2020 vs. 2019 vs 2018). Viitattu 31.10.2021. https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/

Passeri, P. 2021. Monthly Attacks (2021 vs. 2020 vs. 2019 vs 2018). Viitattu 30.1.2022. https://www.hackmageddon.com/2022/01/13/2021-cyber-attacks-statistics/

Povejsil, E. 2021. 10 Concerning Stats About Cybersecurity in Higher Ed. Viitattu 31.10.2021. https://collegiseducation.com/news/technology/10-concerning-stats-about-cybersecurity-in-higher-ed/

Rantalainen, E. 2021. Supo huolestui vakoiluriskistä korkeakouluissa – kiinalaisista tuli isoin ulkomaalaisten opiskelijoiden ryhmä eri yliopistoissa. Viitattu 7.11.2021. https://yle.fi/uutiset/3-12155872

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot - Onnettomuudet, kulttuuri ja johtaminen. Viitattu: 22.10.2021. https://www.researchgate.net/publication/322577981_Turvallisuuskriittiset_organisaatiot_-_onnettomuudet_kulttuuri_ja_johtaminen

Roger, G. & Ashford, T. 2015. Mitigating Higher Ed Cyber Attacks. Viitattu: 31.10.2021. https://files.eric.ed.gov/fulltext/ED571277.pdf

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Viitattu: 22.10.2021. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf

SOC - Security Operations Centre Framework Project. 2019. OWASP Foundation, Inc. Viitattu 7.11.2021. https://owasp.org/www-pdf-archi-ve/OWASP_Security_Operations_Centre_(SOC)_Framework_Project_Presentation.pdf

SOC-CMM 2021a. About the SOC-CMM. Viitattu 28.7.2021. https://www.soc-cmm.com/about/

SOC-CMM. 2021b. SOC-CMM basic assessment tool. Viitattu 28.7.2021. https://www.soc-cmm.com/downloads/latest/

StealthLabs. 2021. Cybersecurity in Education: 10 Important Facts and Statistics 2021. Viitattu 30.6.2022. https://www.stealthlabs.com/blog/cybersecurity-in-education-10-important-facts-and-statistics/

Sullivan, P. Computer Emergency Response Team (CERT). 2021. Viitattu 12.11.2022. https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team

The National Cyber Security Centre 2022. Designing an Operating Model. Viitattu 1.10.2022. https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/operating-model/designing-an-operating-model/

Tietosuoja 2021. Tietosuojavaltuutetun toimisto. Viitattu: 22.10.2021. https://tietosuoja.fi/tietosuoja

Tietosuojalaki 1050/2018. Viitattu 22.10.2022. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Traficom 2021. CERT. Viitattu 7.11.2021. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert

Turvallisuusjohtaminen. 2010. Aluehallintovirasto. Viitattu 26.9.2021. https://www.tyosuojelu.fi/documents/14660/2426906/Turvallisuusjohtaminen_TSO_35.pdf/ef0c3554-4593-49d6-9530-64c28f404cb0

University Challenge: Cyber Attacks in Higher Education. 2016. VMware, Inc. Viitattu 22.10.2021. https://www.nextgensecurityforeducation.com/wp-content/uploads/VMWare-UK-University-Challenge-Cyber-Security.pdf

University challenge: Protecting research in higher education. 2018. VMware, Inc. Viitattu: 22.10.2021. https://www.vmware.com/content/dam/learn/en/emea/fy20/50590_Higher_Education_report.pdf

US-CERT. 2022. Viitattu 12.11.2022. The Department Homeland Security. https://www.cisa.gov/uscert/sites/default/files/publications/infosheet_US-CERT_v2.pdf

Valtionhallinnon tietoturvasanasto. 2008. Digi ja viestintävirasto. Viitattu 22.10.2021. https://dvv.fi/documents/2252790/13063677/2008_VAHTI_ohje_tietoturvasanasto.pdf/0cd599d4-e8c5-3e82-8f06-ae76cae7dd8a/2008_VAHTI_ohje_tietoturvasanasto.pdf

van Os, R. & ym. 2017. MaGMa: a framework and tool for use case management. Viitattu: 28.7.2021. https://www.betaalvereniging.nl/wp-content/uploads/FI-ISAC-use-case-framework-verkorte-versie.pdf

Vehkamäki, P. Lahtinen, M. & Vanttaja, U. 2018. Julkisuus ja tiedonhallinta opetustoimessa. Viitattu 24.7.2021. https://www.oph.fi/sites/default/files/documents/julkisuus_ja_tiedonhallinta_opetustoimessa.pdf

Yhteiskunnan turvallisuusstrategia. 2017. Turvallisuuskomitea. Viitattu: 28.7.2021. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Kuviot