Jouko Voutilainen

# UHKA-ALTTIUDEN JA HYÖKKÄYSPINNAN HALLINTA OSANA YRITYSTEN TIETOTURVAA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

# TIIVISTELMÄ

Voutilainen, Jouko
Uhka-alttiuden ja hyökkäyspinnan hallinta osana yritysten tietoturvaa
Jyväskylä: Jyväskylän yliopisto, 2024, 72 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Tutkimuksessa selvitettiin mitä hyökkäyspinta ja uhka-alttius käsittää sekä miten yritykset kokevat perinteisen riskienhallinnan tarpeellisuuden, kun vertailukohdaksi asetetaan dynaamisempi ja automatisoidumpi prosessi. Lisäksi tarkoituksena oli selvittää, miten hyökkäyspinnan ja uhka-alttiuden hallinta ilmenee yritysten toiminnassa ja miten sitä voidaan hyödyntää.

Hyökkäyspinnan ja uhka-alttiuden aihealue tutkittiin kirjallisuuskatsauksena hyödyntämällä alaan liittyviä tutkimuksia, raportteja, artikkeleita, blogikirjoituksia, verkkosivuja ja kirjallisuutta. Kyselytutkimus toteutettiin kahdeksalle suomalaiselle IT-alan yritykselle, joiden tarkempi toimiala oli jaoteltu kolmeen kategoriaan. Yritysten koot vaihtelivat mikro- ja suuryritysten välillä. Kysely toteutettiin sähköpostin liitteenä olleella kyselylomakkeella, joka sisälsi niin määrällisiä, kuin laadullisiakin kysymyksiä. Vastausprosentti oli 57,1 %.

Vastausten analysointi tehtiin määrällisten vastausten osalta käsittelemällä tilastollisia tunnuslukuja. Muuttujien välisiä riippuvuuksia tulkittiin korrelaatiokertoimella. Kysymysten vastausfrekvenssien esittämiseen käytettiin taulukointia. Avointen kysymysten kohdalla käytettiin luokittelua, jolla tuettiin monivalintakysymysten analyysin tuloksia.

Perinteinen vaikutukseen ja todennäköisyyteen perustuva riskienhallinta koetaan suurelta osin tarpeelliseksi, mutta se sai osakseen myös kritiikkiä useilta vastaajilta ja muilta tutkijoilta. Tutkimuksessa havaittiin hyökkäyspinnan ja uhka-alttiuden nousevan selkeämmiksi trendeiksi vasta tulevaisuudessa, vaikka hyvinkin automatisoidut järjestelmät ovat jo saapuneet markkinoille. Erityisesti hyökkäyspinnan hallintaan keskittyvät sovellukset ja palvelut eivät ole kyselytutkimuksen perusteella suomalaisissa IT-yrityksissä juurikaan käytössä. Yritykset kokivat oman hyökkäyspintansa kasvaneen, mutta eivät kuitenkaan pääosin kokeneet tarvetta päivittää nykyisiä prosessejaan uusilla järjestelmillä tai palveluilla.

Tulosten perusteella voi päätellä, etteivät yritykset koe tarpeelliseksi yhä dynaamisempien tai automatisoidumpien järjestelmien integroimista omaan tietoturvan hallinnan prosessiinsa. Tähän vaikuttaa selkeästi yritysten itsevarmuus nykyisistä prosesseistaan ja järjestelmistään. On kuitenkin tunnistettava, että yritykset ovat pääosin kokeneet hyökkäyspintansa kasvaneen ja tätä myötä suojausmekanismien monimutkaistumiselle voi kuitenkin tulla tarve tulevaisuudessa.

Asiasanat: hyökkäyspinta, uhka-alttius, riskienhallinta, tietoturva, riskianalyysi

# ABSTRACT

Voutilainen, Jouko
Threat exposure and attack surface in enterprise information security management
Jyväskylä: University of Jyväskylä, 2024, 72 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

This research studied what attack surface and threat exposure entails and how companies experience the necessity of traditional risk management when it is compared against a more dynamic and automated process. In addition, the purpose was to understand how companies employ attack surface and threat exposure management and how it could be utilized.

Attack surface and threat exposure was studied as literature review by utilizing other research, reports, articles, blog posts, websites and other literature. An email-survey was conducted for eight Finnish IT-companies that varied from micro to large. The survey consisted of qualitative and quantitative questions. The response rate was 57,1 %.

The analysis was done by processing statistical key figures and correlation coefficient for the quantitative answers. Tabulation was used to summarize and present the responses. Open-ended questions were classified to facilitate analysis alongside the multiple-choice responses.

Traditional risk management which relies on the experience of impact and likelihood is seen to still be useful, but it did receive criticism. The trend towards managing attack surface and threat exposure was perceived as increasingly impactful in the future, even though there already is existing software and services on the market that market themselves as such. Attack surface management software isn't much used in the surveyed Finnish IT-companies. The companies felt that their own attack surface had increased, but mostly did not feel the need to update their current processes with new systems or services.

Based on the results, it can be concluded that companies do not find it necessary to integrate increasingly dynamic or automated systems into their own information security management processes. This is clearly influenced by companies' confidence in their current processes and systems. However, it is recognized that companies have mainly perceived an increase in their attack surface, and with this, there may be a need for the more complex protective mechanisms in the future.

Keywords: attack surface, threat exposure, risk management, information security, risk analysis

# KUVIOT



# TAULUKOT

# SISÄLLYS

# 1 JOHDANTO

Yrityksen tietoturvasäädösten suunnittelun alkuvaiheessa suoritetaan useasti riskienhallintaa, joka perustuu ymmärrykseen yrityksen kaikesta omaisuudesta ja tähän omaisuuteen kohdistuvien uhkien todennäköisyydestä ja vaikutuksesta (Raggad, 2010, s. 77). Tämän riskienhallinnan tarkoituksena on tunnistaa ja arvioida yritystoimintaan vaikuttavien riskien laajuus, jotta suuret riskit kyetään vähentämään täysin, kun taas pieniä riskejä saatetaan jättää kokonaan huomioimatta niiden aiheuttaessa vain pienimuotoista häiriötä yrityksen toiminnalle.

Gartner on todennut artikkeleissaan viime vuosien aikana digitalisaation, esineiden internetin ja varjo-IT:n kasvattaneen yritysten hyökkäyspintaa merkittävästi, sekä riskienhallinnan tuottaen huonoa kyberturvallisuutta (Schneider, Watts & Shoard, 2022; Walls, McMullen, Heiser & Gopal, 2023). Kasvua on jopa niin paljon, ettei kaikkea hyökkäyspintaa kyetä yrityksessä tunnistamaan, esimerkiksi työntekijöiden käyttäessä sovelluksia ja laitteita, joita yritys ei ole työntekijöilleen antanut lupaa käyttää. Samalla sovellukset monimutkaistuvat, lisäten haavoittuvuuksien todennäköisyyttä. Tähän yhdistettynä on yritysten jatkuvasti muuttuva ja kasvava hyökkäyspinta uusien ja tuntemattomien uhkien kohteena, uhkatoimijoiden kehittyessä yhä nopeammiksi, tehokkaammiksi ja enenevissä määrin näkymättömiksi. Kyberpoikkeama voi muodostua yhä useammin tuntematonta hyökkäyspintaa pitkin.

Näiden tutkimusten lisäksi myös Digiturvallisuuden riskikyselyn tuloksissa (Digi- ja väestötietovirasto, 2021) yritykset ovat nostaneet esille huolensa monimutkaisuuden hallittavuudesta ja resursoinnista. Toisessa DVV:n kyselyssä riskienhallintaan liittyen (Rousku, 2021), jossa julkisen hallinnon organisaatioiden riskienhallinnan toteuttamista tutkittiin, tunnistettiin myös vastaavia ongelmakohtia. Keskeistä on myös huomata, että organisaatioista vain noin puolet tekivät säännöllistä riskienarviointia, jossa uudet ilmiöt huomioitiin.

Tässä tutkimuksessa tutkitaan, miten perinteinen riskienhallinta tukee Gartnerin tutkimusten ajatusta tulevaisuuden mahdollisesta trendistä, jossa jatkuva uhka-alttiuden ja hyökkäyspinnan hallinta nostetaan riskienhallinnan keskiöön, ja jossa erityisesti riskien todennäköisyyden epätarkka arviointi on kritiikin kohteena. Tutkimuksen tavoitteena oli suomalaisiin IT-yrityksiin

kohdistetulla kyselyllä tunnistaa, miten yritykset kokevat oman hyökkäyspintansa kasvun sekä perinteisen riskienhallinnan ja onko esitetty kritiikki perinteistä riskienhallintaa kohtaan tarpeellista. Päämääränä oli myös tarkastella yritysten varmuutta omiin nykyisiin prosesseihinsa ja selvittää kuinka paljon hyökkäyspinnan hallintaan liittyvät sovellukset ovat yrityksissä jo nyt käytössä. Lopuksi tarkoituksena oli tunnistaa, miten hyökkäyspinnan ja uhka-alttiuden hallintaa voisi ja tulisi soveltaa perinteisen riskienhallinnan ohella.

Hyökkäyspinta ja hyökkäyspinnan hallinta ovat termeinä hyvin monisyisiä. Yksinkertaisimmillaan hyökkäyspinnalla tarkoitetaan teknisiä sovellushaavoittuvuuksia, jotka näkyvät julkisessa verkossa. Tällöin termin käyttäminen on pitkälti turhaa, sen tarkoittaessa jo suoraan sovellushaavoittuvuuksia. Toisaalta hyökkäyspinta käsitettiin hyvin laajana kyberfyysisenä kokonaisuutena, jossa yrityksen työntekijätkin voidaan mieltää hyökkäyspinnaksi esimerkiksi kalasteluhyökkäyksen näkökulmasta. Hyökkäyspinnasta tulisikin puhua laajassa mittakaavassa, sillä yrityksiin kohdistuvat uhat eivät pelkästään perustu verkkosovelluksiin ja niiden haavoittuvuuksiin tai virhekonfiguraatioihin, vaan uhkien luonne on paljon monipuolisempi, niiden kohdistuessa yrityksen hallinnolliseen, operatiiviseen ja tekniseen tasoon.

Hyökkäyspinnan hallintaan liittyen on esitetty kolme selkeää sovellus- tai palvelukokonaisuutta: Kyberassettien hyökkäyspinnan hallinta (engl. *Cyber Asset Attack Surface Management CAASM*), Ulkoisen hyökkäyspinnan hallinta (engl. *External Attack Surface Management EASM*) ja Digitaalisen riskin turvaamisen palvelut (engl. *Digital Rights Protection Services*). Näillä termeillä markkinoituja sovelluksia on jo markkinoilla, mutta niiden käyttöaste on hyvin vähäistä tämän tutkimuksen vastaajien osalta.

Yritykset eivät tyrmää perinteistä riskienhallintaa täysin, joskin kritiikkiä sitä kohtaan esiintyy. Kuitenkaan Gartnerin kuvailemaa hyökkäyspinnan hallintaa ei toisaalta koeta kriittiseksi kokonaisuudeksi, vaikka hyökkäyspinnan kasvu onkin useissa yrityksissä tunnistettu esimerkiksi pilvipalveluiden myötä. Yrityksillä on vahva usko omiin prosesseihinsa ja nykyisiin järjestelmiin, jotka vaikuttavat jo osaltaan siihen, ettei uusille sovelluksille ja palveluille ole tarvetta. Yrityksen koko vaikuttaa myös siihen, koetaanko näitä sovelluksia edes tarpeellisiksi.

Tutkimuksen johtopäätöksistä nousee esille kolme kokonaisuutta. 1. Hyökkäyspinnan tunnistaminen on keskeistä onnistuneessa tietoturvassa: Tunnistamatonta laitetta on mahdoton valvoa tai hallita, joten varjo-IT:n ja tuntemattoman hyökkäyspinnan syntyminen on kyettävä minimoimaan. 2. Perinteiselle riskienhallinnalle on edelleen tarve: Vaikka kritiikki vaikutuksen ja todennäköisyyden arvioimista kohtaan on osin aiheellista, koetaan riskienhallintaprosessi kuitenkin hyvin tärkeäksi osaksi tietoturvan hallintaa. 3. Tulevaisuudessa on todennäköistä, että uhkien torjumisen tulee olla yhä proaktiivisempaa. Uhkatoimijoiden ja hyökkäysmallien monimutkaistuessa ja kehittyessä yhä nopeammin, on hyvin tarpeellista siirtyä yhä dynaamisempaan ja automatisoidumpaan uhkienhallintaprosessiin. Tällä hetkellä hyökkäyspinnan hallinnan sovellukset eivät juurikaan ole käytössä, mutta niiden tarve kasvaa jatkuvasti.

# 2 TUTKIMUKSEN TOTEUTUS

## 2.1 Tutkimuksen lähtökohta ja tutkimuskysymykset

Organisaatiot ovat perinteisesti korostaneet riskienhallintaa kyberturvallisuuden toteuttamisessa. On kuitenkin väitetty (Walls, ym., 2023), etteivät nykyiset riskienhallinnan mallit ole välttämättä riittävän tehokkaita tämän päivän jatkuvasti muuttuvassa ja kasvavassa uhkaympäristössä. Tulevaisuuden trendeinä on tunnistettu, useita sovellus- ja palvelukokonaisuuksia, jotka mahdollistavat entistä monipuolisemman ja tehokkaamman riskien ja hyökkäyspinnan hallinnan (Schneider, ym. 2022). Näiden käytön tarpeesta ja käyttöasteesta ei kuitenkaan ole riittävästi tutkittu.

Tutkimus tarkastelee siis yritysten mieltymyksiä ja kokemuksia perinteisestä riskienhallinnasta sekä vertaa näitä havaintoja siihen tarpeeseen, joita muissa tutkimuksissa on nostettu esille. Lisäksi tulevaisuuden trendeiksi kuvailtujen, ja jo nyt markkinoilla olevien, sovellusten käyttöastetta ja käyttötarvetta tarkastellaan sekä sitä, miten hyökkäyspinnan ja uhka-alttiuden hallinnan periaatteita sovelletaan ja voidaan soveltaa perinteisen riskienhallinnan ohella.

Tutkimukselle määritettiin yksi päätutkimuskysymys:

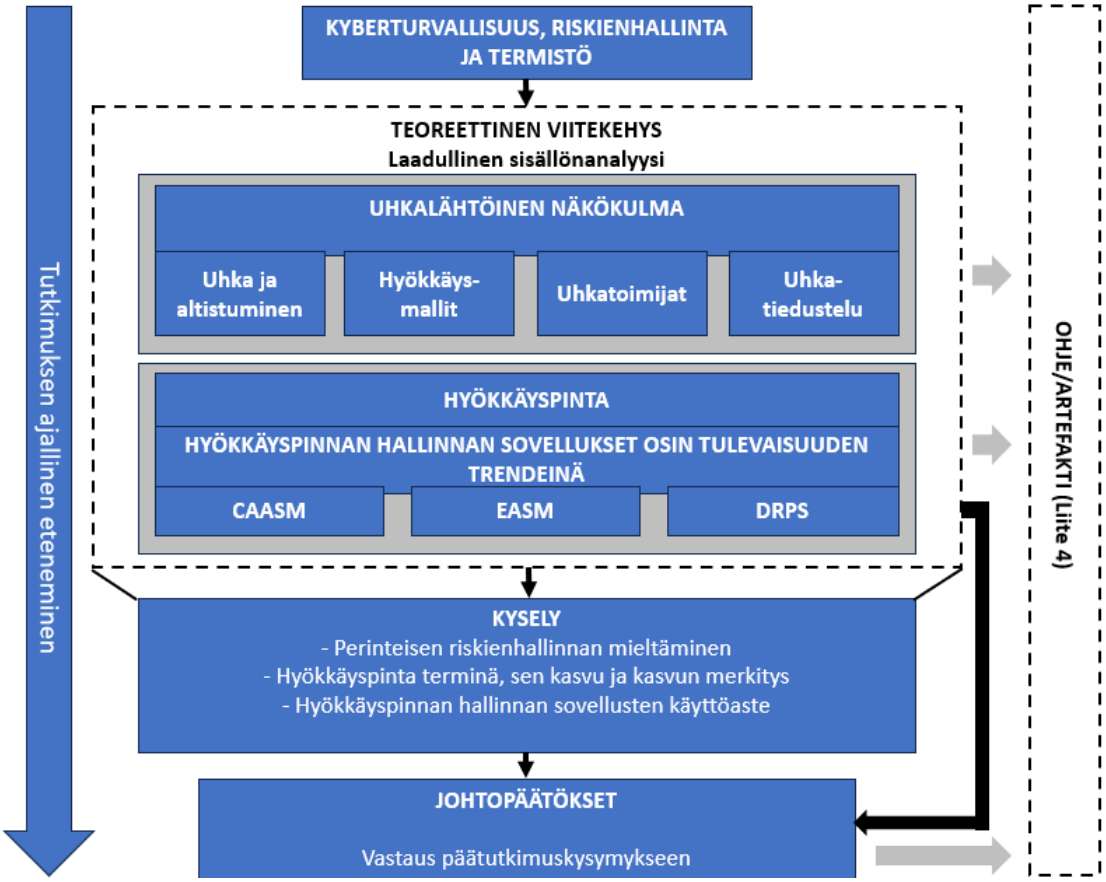
1. Miten uhka-alttiuden ja hyökkäyspinnan hallintaa voidaan soveltaa perinteisen riskienhallinnan ohella?

Tämän lisäksi päätutkimuskysymyksen tueksi määritettiin kolme alatutkimuskysymystä:

1. Mitä kyberturvallisuuden perinteinen riskienhallinta käsittää?
2. Mitä on uhkalähtöisyys sekä uhka-alttiuden ja hyökkäyspinnan hallinta?
3. Miten yritykset kokevat perinteisen riskienhallinnan ja hyökkäyspinnan hallinnan?

Tässä tutkimuksessa puhuttaessa yleisesti Gartnerin tutkimuksista tai Gartnerin artikkeleista, viitataan sillä neljään tälle tutkimukselle keskeiseen lähteeseen, jotka esittävät kritiikin perinteiseen riskienhallintaan ja kuvaavat hyökkäyspinnan ja uhka-alttiuden hallinnan periaatteita (Walls, ym., 2022; Schneider, ym., 2022; D'Hoinne, Shoard & Schneider, 2022; Zhang & Perkins, 2023).

Tutkimusprosessi on kuvattu alla olevassa kuvassa (KUVIO 1). Luku kolme on lyhyt yleiskatsaus perinteiseen riskienhallintaan liittyviin asiakokonaisuuksiin ja kyberturvallisuuden periaatteisiin ja termistöön. Kolmannen luvun tarkoituksena on antaa lukijalle riittävä pohjatieto siitä, mitä kyberturvallisuuden hallinta ja riskienhallinta tänä päivänä sisältää, ja mitkä asiat siihen vaikuttavat. Luku myös pyrkii tarjoamaan lukijalle ymmärryksen siitä, että kyberturvallisuuden hallinnassa on useita eri tapoja ja keinoja päästä samaan lopputulokseen hyödyntämällä eri kriteeristöjä ja muuta materiaalia. Kyberturvallisuuden hallinnassa ovat myös suuressa keskiössä kansainväliset säädökset ja lait.



KUVIO 1 Tutkimusprosessi

Kirjallisuusosion toisessa vaiheessa, eli uhkalähtöisessä näkökulmassa, käydään läpi uhkiin ja niiden tunnistamiseen ja hallintaan liittyvät asiakokonaisuudet. Hyökkäyspinta ja sen hallinta muodostivat kirjallisuusosion kolmannen vaiheen, jossa tunnistettiin kolme keskeistä sovelluskokonaisuutta, joita kuvaillaan myös tulevaisuuden trendeiksi.

Näiden vaiheiden jälkeen luotiin yhteenvedon pohjalta kyselyn, jolla vastattiin tutkimusongelmaan. Näiden osien yhteenvedon ja pohdinnan tuloksena vastattiin päätutkimuskysymykseen.

Tutkimuksen rinnakkaisena tuotoksena syntynyt ”Tarkistuslista ja ohje hyökkäyspinnan hallinnasta yritykselle” on esitetty liitteessä 4.

## 2.2 Tutkimusmenetelmät

### 2.2.1 Laadullinen tutkimus

Tutkimuksen kirjallisuusosiossa käytettiin laadullisia eli kvalitatiivisia tutkimusmenetelmiä. Hirsijärvi, Remes ja Sajavaara (2015) esittävät kirjassaan laadullisen tutkimuksen perustuvan todellisen elämän kuvaamiseen, kuitenkin tunnistaen sen, että kokonaisuutta on rajattava, jotta asioiden välille on mahdollista tunnistaa ja luoda suhteita. Kysymystä kuten ”Onko kirja jännittävä?”, ei voida määrällisesti mitata niin, että sen vastaus kuvaisi absoluuttisesti kirjan jännittävyyttä. Yksi tutkija voisi arvoasteikolla 1–10 todeta kirjan olevan tasolla 10, kun taas toinen tutkija tasolla 5. Tämän lisäksi on täysin subjektiivista, minkä takia henkilö kokee kirjan jännittäväksi. Laadullisessa tutkimuksessa on siis ominaista tarkastella käsiteltävänä olevaa asiaa mahdollisimman kokonaisvaltaisesti (Hirsijärvi ym., 2015, s. 161). Edellä esitetyn esimerkinkin myötä voi kuitenkin huomata, että kvantitatiivisen ja kvalitatiivisen tutkimuksen eroja voi olla vaikea välillä tunnistaa (Hirsijärvi ym., 2015, s. 136). Kirjan jännittävyyttä voidaan mitata esimerkiksi numeraalisesti, mutta sitä voidaan myös tukea avoimilla haastatteluilla. Tällöin nämä kaksi suuntausta täydentävät toisiaan, eikä voida puhua puhtaasti jommastakummasta.

Hirsijärvi ym. (2015) toteaa, että kvalitatiivinen käsittelee merkityksiä, ja kvantitatiivinen numeroita. Tämä tutkimus oli tällöin pohjimmiltaan kvalitatiivinen sen tutkimusongelman ja päätutkimuskysymyksen myötä. Kyseistä asiaa ei voida täysin kuvata numeerisesti, joskin mahdolliset kvantitatiiviset menetelmät voivatkin johtopäätöksiä tukea.

”(Laadullinen) tutkimus on luonteeltaan kokonaisvaltaista tiedon hankintaa, ja aineisto kootaan luonnollisissa, todellisissa tilanteissa” (Hirsijärvi ym., 2015, s. 164). Laadullisessa tutkimuksessa ominaista on induktiivinen analyysi, jossa hypoteesia ei välttämättä edes luoda, vaan aineiston monipuolinen tarkastelu johtaa odottamattomien asioiden paljastumiseen. Kohdejoukon määrittelyssä myös pyritään vahvaan tarkoituksenmukaiseen otantaan niin haastateltavien, kyselyjen kuin kirjoitetunkin materiaalin osalta. Tässä tutkimuksessa tarkoituksenmukainen otanta nousi esille kyselyä suunniteltaessa. Tutkimussuunnitelma myös usein tarkentuu tutkimuksen edetessä (Hirsijärvi ym., 2015, s. 164).

Lähdemateriaalin keräämisessä käytettiin aineistolähtöistä analyysiä. Laadullista materiaalia kerättäessä, ei lähdeaineisto välttämättä lopu koskaan

(Hirsijärvi ym., 2015, s. 18). Tästä syystä käytetyt lähteet pyrittiin keräämään niiden ajankohtaisuus huomioiden.

Laadullisessa tutkimuksessa on tunnistettava tutkimuksen subjektiivisuus (Saaranen-Kauppinen & Puusniekka, 2009, s. 7). Tutkijalla on suhteellisen vapaa asetelma tutkia käsiteltävää asiaa, joka vaatii tutkijalta vahvoja perusteluita ja selkeää viitekehystä johtopäätöksilleen.

Tutkimuksen pohjatiedon muodostamisen ja viitekehyksen tutkimiseen käytettiin sisällönanalyysiä systemaattisen kirjallisuuskatsauksen tukena. Tässä tutkimusmenetelmässä on ominaista syventää jo valmista ja tutkittua tietoa, eli tuottaa siis toisen asteen tutkimusta (Tuomi & Sarajärvi, 2018, s. 145). Jotta kyselyaineiston luominen oli laadukasta, oli tarpeen tutkia aiempaa aiheen ympärillä tehtyä tutkimusta. ”hyökkäyspinnan hallinta” ja ”uhka-alttiuden hallinta” ovat termeinä suhteellisen tuoreita. Jo tämän takia oli tarpeen tutkia, mitä näillä termeillä tarkoitetaan ja miten niitä käsitellään alan muussa tutkimuksessa. Kirjallisuuskatsausta tehdessä tunnistettiin kuitenkin kyseisen termistön hyvin niukka käyttö siinä muodossaan, missä sitä lähdettiin alun perin hakemaan. Eli hyökkäyspinnasta usein puhutaan muissa tutkimuksissa, mutta erityisesti ”hyökkäyspinnan hallinnasta” huomattavasti vähemmän.

Artikkelien hakemisessa, analysoinnissa ja valitsemisessa hyödynnettiin Levyn ja Ellisin (2006) esittämiä malleja ja ohjeistusta informaatioteknologian tutkimuskentän kirjallisuuskatsauksen systeemisestä lähestymistavasta. He toteavat tutkimuksessaan (2006), että informaatioteknologian tutkimuksessa aloittelevat tutkija saattaa herkästi löytää kirjallisuuskatsaukseensa vain pienen määrän valittuun aiheeseensa täydellisesti kohdistuvia tutkimuksia, sillä tällä alalla monitieteellisyys on hyvin yleistä. Tästä syystä lähestymistapa systemaattiseen kirjallisuuskatsaukseen voi erota muista tutkimusaloista. Tutkimuksen kirjallisuuskatsauksen osiota jatkettiin läpi tutkimuksen kuten on suotavaakin (Levy & Ellis, 2006, s. 192). Pääosa kirjallisuuskatsauksen lähdeaineistosta tulisi olla vertaisarvioituja tutkimusartikkeleita, mutta ei ole täysin poissuljettua käyttää muunkinlaista materiaalia (Levy & Ellis, 2006, s. 185). Tällöin tutkijan on kuitenkin tunnistettava kyseisen materiaalin subjektiivisuus. Tässä tutkimuksessa osin jo termistön nuoren iän vuoksi, oli tarpeen hyödyntää lähteinä kyberturvallisuuteen liittyvien yritysten kuten IBM:n ja Ciscon näkemyksiä aiheesta, eikä koko tutkimusta voinut, eikä kannattanutkaan perustaa pelkkien tutkimusartikkelien pohjalle.

Tutkimus sisälsi empiirisen tapaustutkimuksen ja kuvailevan tutkimuksen elementtejä. Empiirinen strategia tässä tutkimuksessa keskittyi yritysten havaintoihin, jotka kerättiin kyselyllä. Kuvaileva tutkimus taas esiintyy johtopäätöksissä, jossa yritysten kyselytuloksia käsiteltiin systemaattisen kirjallisuuskatsauksen pohjalta luodussa viitekehyksessä.

Kyseessä ei kuitenkaan ollut siis perinteinen tapaustutkimus, jossa yksittäistä tapahtumaa tai kohdetta käsiteltäisiin, vaan käsiteltäviä kohteita oli useita. Tätä tutkimusta kuitenkin voi siis kutsua tapaustutkimukseksi sen kyselyn luonteen myötä. Useimmiten tapaustutkimuksella ei ole pyrkimys saavuttaa yleistettävää tietoa, sen keskittyessä vain yhteen kohteeseen (Saaranen-Kauppinen &

Puusniekka, 2009, s. 43). Tässä tutkimuksessa, otannan ollessa enemmän kuin yksi yritys, voitiin yleistettävää tietoa kuitenkin saada. Kuitenkin Eskola ja Suoranta (1998, s. 57) esittävät ristiriitaisesti tapaustutkimuksesta, että sen taustalla kuitenkin on ajatus saada yleistettävää tietoa.

### 2.2.2 Kyselytutkimuksen toteuttaminen

Tutkimuksen systemaattisena kirjallisuuskatsauksena toteutettu ensimmäinen osa toimi pohjana kyselyn sisällön muodostamisessa.

Etuna kyselyn tekemisessä on mahdollisuus saada suurelta määrältä vastaajia tietoa, joka on suhteellisen helppo jäsennellä tulkittavaan muotoon (Hirsijärvi ym., 2015). Heikkoutena kuitenkin on se, ettei kyselyn tuloksista näe kuinka tosissaan vastauksissa on oltu, tai kuinka hyvin kysymykset ja vastausvaihtoehdot ovat luotu. Lisäksi on mahdollista, ettei vastaaja välttämättä tiedä aihealueesta riittävästi antaakseen sellaista vastausta, josta tutkimuksessa olisi hyötyä.

Kysely kohdistettiin neljääntoista suomalaiseen yritykseen ja vastauksia pyydettiin erityisesti heidän tietoturvallisuutensa asiantuntijoilta. Yritysten toimialat ovat tietoteknisten laitteiden valmistusta, konsultointia ja/tai tietoturvatestausta. Yritysten koot vaihtelivat mikron, pienen, keskisuuren ja suuren välillä.

Vastaajat olivat siis valittu niin, että hyvin todennäköisesti heidän osaamisensa riittää kyselyyn vastaamiseen. Kysymyksien asettelussa on huomioitu vastaajien kompetenssi kysymysten vastaamiseen varmistamalla, että heillä on riittävät tiedot aihealueesta. On myös tarpeen tunnistaa, että kyselyihin vastaavat saattavat omata erilaisen osaamisen tason. Vastausten ja sitä myötä myös johtopäätösten yleistettävyyden kriteerinä onkin vastaajien mahdollisimman samanlainen kokemusmaailma (Eskola & Suoranta, 1998, s. 57). Erityisesti tämänkaltaisessa kyselyssä, jossa vastaajamäärä on pieni, on tarpeen valita vastaajat onnistuneesti, sillä jo muutama epäonnistunut vastaus voi hankaloittaa kyselyn analyysiä, ja täten heikentää mahdollisesti löydetyn yhteenvedon perusteltavuutta ja reliabiliteettia.

Avoimet kysymykset mahdollistavat vastaajien täydentää monivalintakysymystensä vastauksia, jolloin Hirsijärven (2015) esittämät heikkoudet saadaan suurelta osin vähintäänkin huomioitua. Tämän lisäksi avoimet kysymykset voivat sisältää hyviä ideoita, ja vastaajan ajatukset on mahdollista saada perusteellisesti selville (Valli & Aaltola, 2018). Kyselyssä hyödynnettiinkin paljon avoimia tekstikenttiä, joihin vastaajat saivat halutessaan täydentää monivalintakysymystensä vastauksia. Tutkija tunnisti myös riskin, että kysymykset voivat pahimmillaan olla liian ohjaavia tai liian ympäripyöreitä, jolloin vastausten todellinen käytettävyys tutkimuksessa oli mahdollista koitua ongelmaksi. Avoimia kysymyksiä kuitenkin voi arvioida tilastollisin menetelmin, kun ne määritellään tarkasti luokkiin vastausten mukaan (Valli & Aaltola 2018).

Tämänkaltainen pienelle ja kohdennetulle vastaajamäärälle kohdennettu kysely saa todennäköisemmin myös avoimiin kysymyksiin laadukkaita vastauksia, verrattuna tutkimukseen, jossa kohteena on satoja tai jopa tuhansia vastaajia.

Kyselyn muodostamista teemahaastattelun muotoon harkittiin, vastaajien määrän ollessa suhteellisen pieni. Perinteiseen kyselyyn kuitenkin päädyttiin

siitä syystä, että hyvin tehdyn kyselylomakkeen hyödyntäminen jatkotutkimuksissa olisi mahdollista. Jos tutkimusta päädytään myöhemmin laajentamaan suuremmalle vastaajamäärälle, on kyselylomake ja tämän tutkimuksen vastaukset hyödynnettävissä esimerkiksi väitöskirjaa tehtäessä. Jos tässä tutkimuksessa olisi käytetty haastattelumuotoista tiedonkeräysmenetelmää, ei vastaava menetelmä enää toimisi, jos vastaajia olisi useita kymmeniä. Kyselomake on jäsennelty kolmeen kategoriaan, jota käytetään myös hyödyksi vastausten analyysissä: 1. Riskienhallinnan toteutus ja taustatiedot, 2. Riskienhallinnan ja hyökkäyspinnan hallinnan mieltäminen ja 3. Hyökkäyspinnan hallintaan ja uhkametsästykseen liittyvien sovellusten ja palveluiden käyttö.

Kyselylomakkeen viimeinen kysymys, jossa tarkastellaan yrityksen riskienhallintaprosessin dynaamisuutta, on poikkeavasti sijoitettu kyselylomakkeen loppuun, eikä se kuulu kategoriaan 3, vaan on täysin oma kysymyksensä, joka osaltaan antaa vastauksia toteutukseen ja taustatietoihin. Kysymyksen sijoittelulla on pyritty siihen, että vastaaja on käsitellyt mielessään lomakkeen aiheita, ennen kuin antaa vastauksen näin laajaan kysymykseen. Jos kyseisen kysymys olisi jo lomakkeen alussa, olisi vastaus hyvin todennäköisesti erilainen.

Kyselylomakkeen ensimmäiseen versioon pyydettiin palautetta erään yrityksen vastaajalta jo ennen virallista kyselyn toteuttamista. Lisäksi palautetta lomakkeesta pyydettiin toiselta tutkijalta. Näin tunnistettiin päivitettäviä ja tarkennettavia kohtia kyselyssä, jotka korjattiin viimeistä kyselylomakkeen versiota varten. Valli (2018) toteaakin, että tutkimuslomakkeen huolellinen suunnittelu ja esitestaus takaavat onnistuneen tutkimuksen ja säästävät turhalta työltä myöhemmässä vaiheessa.

Kysymyslomakkeet lähetettiin sähköpostitse joulukuun 2023 puolessa välissä, ja vastauksia odotettiin viimeistään tammikuun toisella viikolla. Vastausaikaa pidennettiin heikon vastausprosentin myötä, ja lopulta vielä erillisillä puhelinsoitoilla varmistamalla saatiin muutamilta vastaajilta täytetyt lomakkeet. Kyselylomakkeen mukana ensimmäisellä sivulla lähetetty saateviesti on esitetty liitteessä 1. Kyselylomake on liitteessä 2.

### 2.2.3 Kyselyn aineiston analyysi

Tutkimustulosten analysointiin on hyödynnetty erityisesti kirjoja Ikkunoita tutkimusmetodeihin (Valli & Aaltola, 2018) ja Kyselytutkimuksen mittarit ja menetelmät (Vehkalahti, 2014). Tuloksia analysoitiin ja tulkittiin Microsoft Excel -ohjelmalla.

Kyselyn sisältäessä määrällisiä, kuten likert-asteikolla mitattavia kysymyksiä, sekä avoimia vastauksia, on vastauksia tulkittava määrällisen tulkinnan ohella myös laadullisesta näkökulmasta.

Laadullisen aineiston analyysi kuvataan Puusan ja Juutin teoksessa (2020) kolmivaiheisena. Ensimmäisessä vaiheessa on aineiston lukeminen. Toisessa vaiheessa raakateksti käsitellään kategorioiksi, löytämällä merkityksellisiä asiakokonaisuuksia, jotka tukevat tutkimusta teoreettisen ajattelun ja tutkimuskysymysten näkökulmasta. Kolmannessa vaiheessa kategoriat kääntyvät teemoiksi. Teemojen pohjalta kirjoitetaan lopulta tutkimuksen johtopäätökset. Laadullisten

(eli tässä tapauksessa avointen) vastausten kategorioiden avulla tuetaan tutkimuksen määrällisten vastausten tulkintaa.

Avointen vastausten analysointiin käytettiin siis luokittelua. Havaintojen luokittelu on ominainen laadullisen aineiston analyysin keino (Puusa & Juuti, 2020). Vastauksista tunnistettiin kategorioita ja yhtäläisyyksiä, joiden pohjalta vastaukset kyetään luokittelemaan samankaltaisuuksien pohjalta. Alakategorioiden pohjalta voidaan yhdistelemällä tunnistaa yläkategorioita. Puusa ja Juuti (2020) toteavat, että tämänkaltaista kategorioiden yhdistelyä ja muodostamista voidaan jatkaa niin kauan, kuin aineisto sen mahdollistaa.

Likert-asteikko on Vehkalahden (2014, s. 35) mukaan yleisin kyselytutkimusten mittausmenetelmä. Useimmiten sitä käytetään viisiportaisessa muodossaan, jossa keskimmäinen vaihtoehto on neutraali, kuten ”Ei samaa, eikä eri mieltä”. Tämän neutraalin vaihtoehdon voi kuitenkin nähdä aiheuttavan ongelman, jos vastaaja ei ole ymmärtänyt kysymystä tai hän on jo uupunut vastaamaan. Tämän tutkimuksen kyselylomakkeeseen ei ollut neutraalia vastausvaihtoehtoa, mutta kysymykset mahdollistavat avoimen kommentoinnin. Tämän pyrkimyksenä oli tunnistaa ne vivahteet vastauksista, jotka herkästi jäävät piiloon liian rajatun kyselylomakkeen myötä.

Määrällisten vastausten osalta käsiteltiin tunnuslukuja sekä sijaintilukuja kuten keskiarvoa. Näiden tarkoituksena on tiivistää suurienkin aineistojen tulkittavaa kokonaisuutta pienempään muotoon (Heikkilä, 2014). Tällöin osa informaatiosta häviää, mutta toisaalta tavoiteltaessa yleistettävää tietoa johtopäätöksiä varten, on tunnuslukujen hyödyntäminen tarpeellista. Vastaajamäärän ollessa tässä tutkimuksessa pieni, on vastauksia mahdollista tarkastella tarkemminkin. Muuttujien välisten riippuvuuksien selvittämiseen hyödynnettiin korrelaatiokerrointa (Liite 3). Tämän toimenpiteen yhtenä tarkoituksena on tunnistaa syy-seuraussuhteita vastauksista (Heikkilä, 2014). Keskeisten kysymysten osalta hyödynnettiin taulukointia.

Vastausten analysoinnissa toteutettiin siis kvantitatiivisia menetelmiä monivalintakysymyksissä ja luokittelua avoimissa kysymyksissä. Tämän lisäksi vastauksia tulkittiin vastaajakohtaisesti pyrkien tunnistamaan syy-seuraussuhteita vastauksissa. Kyselyn tulokset ja analysointi on esitetty luvussa 5.

Analyysissä esitetyt frekvenssitaulukot sisältävät sarakkeet 1, 2, 3 ja 4, jotka kysymyslomakkeessa tarkoittavat vaihtoehtoja ”Täysin eri mieltä”, Osittain eri mieltä”, ”Osittain samaa mieltä” ja ”Täysin samaa mieltä”. Poikkeuksena on kysymys 9, jossa vastausvaihtoehdot olivat “Ei jää tunnistamatta”, “Hyvin vähän”, “Jonkin verran” ja “Paljon”. Frekvenssitaulukoissa esitetyt kysymykset ovat typistettyjä versioita kyselylomakkeen kysymyksistä tiedon esittelyn selkeyttämiseksi. Kysymykset alkuperäisessä muodossaan löytyvät liitteestä 2.

## 2.3 Aikaisempi tutkimus ja lähdeaineiston esittely

Aikaisempaa tutkimusta aiheesta ei täysin tällaisenaan ole tehty, joskin riskienhallintaa on tutkittu kyselytutkimuksissa muun muassa Digi- ja väestötietoviraston kahdessa tutkimuksessa (Digi- ja väestötietovirasto, 2021) ja (Rousku, 2021).

Maverick Researchin ja Gartnerin julkaisemat artikkelit (D'Hoinne, Shoard & Schneider, 2022; Schneider, Watts & Shoard, 2022; Walls ym., 2023) käsittelevät aihetta kukin noin 10–20 sivun artikkeleissaan.

Google Scholarin haulla ”*Attack Surface Management*” tuottaa 94 hakutulosta.”*Threat Exposure Management*” tarjoaa 2 hakutulosta, mutta *”Threat exposure” cyber* kuitenkin 599. ResearchGaten sekä Google Scholarin hakuja tarkasteltaessa voi kuitenkin huomata, että ainakin otsikkotasolla hyvin harva hakutulos on suoraan käytännöllinen tähän tutkimukseen liittyen. Hyökkäyspinta ja uhka-alttius on siis tunnistettuja termejä, mutta lisättäessä termien perään ”hallinta”, muuttuu artikkelien määrä ja sisältö mittavasti. Useat yritykset kuten IBM (2023b), Mandiant (2023b) ja SANS (2023) ovat omilla verkkosivuillaan puhuneet hyökkäyspinnan hallinnasta lyhyesti, mutta niiden tapa käsitellä aihealueen termistöä eroaa hieman.

”*Threat Exposure Management*” esiintyy kuitenkin hakutuloksissa useiden yritysten omissa blogeissaan ja tietoiskuissaan markkinoidessaan omia palveluitaan ja tuotteitaan (Anomali, 2023; Breachlock, 2023; Picus Labs, 2023). Googlen hakutulosten pohjalta selviää, että kyseisiä blogijulkaisuja ja tietoiskuja on pääsääntöisesti julkaistu vuodesta 2022 lähtien. Termit ovat siis yleisesti käytössä yritysmaailmassa, mutta tutkimuskentässä niihin törmää suhteellisen vähän. ”*Threat Exposure Management*” (Google haku: 39 600 tulosta) on kuitenkin harvinaisempi termi verrattuna ”*Attack Surface Managementiin*” (Google haku: 449 000 tulosta) (Google, 2023).

Jyväskylän yliopistossa on viime vuosina tutkittu paljon eri kriteeristöjä sekä yritysten tietoturvan tasoa ja hallintaa. Nämä eivät kuitenkaan tarkennu erityisesti hyökkäyspintaan tai uhka-alttiuteen. Suoraan aiheeseen liittyviä Jyväskylän pro gradu –tutkielma löytyi yksi (Arponen, 2023), jossa tutkittiin ICT-organisaatioiden riskienhallinnan suunnittelun ja toteutuksen tapoja. Tämän lisäksi löytyi useita tutkimuksia, joissa eri organisaatioita ja toimijoita tutkittiin ja näiden kokemuksia tietoturvan ja kyberturvallisuuden hallinnasta, peilattiin kriteeristöihin kuten ISO 270001 ja KATAKRI.

Tämän tutkimuksen lähteinä käytettiin kirjoja, kriteeristöjä, verkkosivustoja ja artikkeleita. Tutkimukseen kerätyt artikkelit aihepiiriin liittyen olivat haettu sivuilta kuten ResearchGate, IEEEXplore, ProQuest ja ScienceDirect. Valittaessa viitattavia artikkeleita oli pyritty ajankohtaisuuteen ja tutkimuksen yleiseen laatuun. Osa tutkimuksista, joita hakuvaiheessa tunnistettiin merkittäviksi otsikon tai lyhennelmän perusteella, oli saatavilla vain kyseisen yliopiston tai laitoksen opiskelijoille tai henkilöstölle, josta syystä pieni määrä potentiaalisia artikkeleita jäi tähän tutkimukseen huomioimatta.

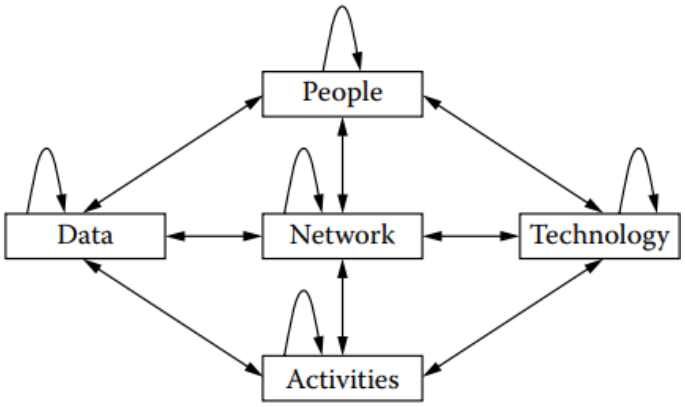
# 3 KYBERTURVALLISUUS JA RISKIENHALLINTA

## 3.1 Tietoturva

Sanastokeskus määrittää kyberturvallisuuden seuraavasti: "tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa, ja jossa sen toiminta turvataan" (Sanastokeskus, 2018, s. 22). Kyberturvallisuus on siis suhteellinen laaja käsite, eikä se pelkästään tarkoita teknisiä ratkaisuja kuten palomuurien oikeita asetuksia tai riittävän vahvoja salasanoja. Sanastokeskuksen määritys kuitenkin täsmentää, että kybertoimintaympäristön häiriintyminen kuitenkin usein johtuu tietoturvauhkasta, jonka keskiössä on tietoturva (Sanastokeskus, 2018, s. 22). Täten tietoturva ja informaatioturvallisuus on vahvasti linkittyneenä kyberturvaan käsitteellisesti.

Sanastokeskus (2018, s. 22) täsmentää kyber- ja tietoturvallisuuden eroa seuraavasti: "Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. "

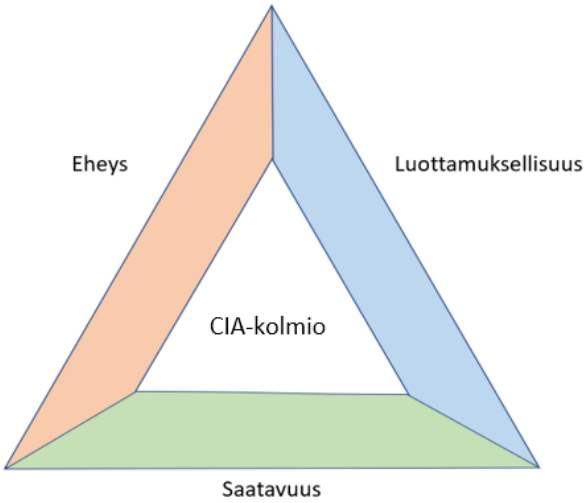
Kyberturvallisuuden voi nähdä olevan kokoelma turvallisuusjohtamista, fyysistä turvallisuutta ja teknistä tietoturvallisuutta, kuten se on jaoteltu suomalaisessa tietoturvallisuuden auditointityökalu Katakrissa (Ulkoministeriö, 2020). Yrityksen tietoturvaa ja kyberturvallisuutta käsiteltäessä on tärkeä tunnistaa kaikki osatekijät ja niiden väliset suhteet. Esimerkiksi riittävän hyvät teknisen tietoturvallisuuden päätökset eivät välttämättä auta mitään, jos työntekijöille ei ole ohjeistettu oikeanlaisten salasanojen käyttöä tai avaimista huolehtimista. Lisäksi, vaikka data olisi kuinka hyvin salattu, jos salausavain on helposti saatavilla, on tekninen suojaus täysin turhaa. Raggad esittää teoksessaan yksinkertaistetun esimerkin tietojenkäsittelyn osatekijöiden suhteesta (KUVIO 2) (Raggad, 2010, s. 4).




KUVIO 2 Tietojenkäsittely-ympäristön osatekijöiden suhteet (Raggad, 2010, s. 4)

Huomioitavat osatekijät ovat Raggadin (2010) jaottelulla ihmiset, verkko, teknologia, toiminnot ja data. Jokainen näistä osatekijöistä vaikuttaa myös itseensä. Esimerkiksi ihmiset vaikuttavat ihmisiin rekrytoinnin ja johtamisen kautta. Teknologia asettaa rajoitteita ja mahdollisuuksia ihmisille ja toiminnoille sekä vaikuttaa verkon käyttöön. Ihmiset ja toiminnot vaativat dataa tuottaakseen tulosta yritykselle. Myös eri toiminnot vaikuttavat toisiin toimintoihin ja yksittäinen datapiste vaikuttaa muuhun dataan (Raggad, 2010, s. 5).

CIA-kolmio (engl. *CIA-triad*) on yleisesti käytössä oleva määrittelytapa turvallisuustavoitteille (Raggad, 2010, s. 20). Esimerkiksi CVSS (Common Vulnerability Scoring System), jonka tarkoituksena on määritellä kuvaavat numeraaliset arvot löydetyille haavoittuvuuksille, hyödyntää CIA-kolmiota vaikutusten merkittävyyden tunnistamisessa (First, 2023). CIA-kolmio koostuu kolmesta osa-alueesta: luottamuksellisuus, eheys ja saatavuus (engl. *Confidentiality, integrity and availability*). Kyseinen malli kuvataan usein kolmiona (KUVIO 3), jonka periaatteena on näiden kolmen osa-alueen keskinäisriippuvuus tietoturvallisuuden keskiössä: Jos yksi kolmion reunoista puuttuu, sortuu kolmio, eikä tietoturvallisuus toteudu tarkoitetulla tavalla. Onnistuneen tietoturvan tarkoituksena on ylläpitää tiedon eheys, luottamuksellisuus ja saatavuus.




KUVIO 3 CIA-kolmio

Luottamuksellisuudella tarkoitetaan sitä, että tieto on nähtävissä ja käsiteltävissä vain niiden henkilöiden toimesta, joilla on tosiasiallinen tarkoitus siihen (Raggad, 2010, s. 20, 27). Esimerkiksi henkilökohtaisesti tunnistettava tieto kuten henkilötunnus tulisi olla salattuna ja turvattuna. Tähän kategoriaan kuuluu myös arkaluontoisen, fyysisessä muodossa olevan tiedon vääränlainen hävittäminen, joka voi esiintyä esimerkiksi paperiroskiksesta löytyvillä dokumenteilla. Hyökkäyskeinoja luottamuksellisuutta kohtaan ovat verkon vakoilu, tietojen kalastelu ja salasanojen varastaminen.

Eheys käsittää tiedon korruptoitumiseen liittyvät ilmiöt (Raggad, 2010, s. 20, 27). Tämä voi tarkoittaa siis tahallista tai tahatonta tiedon muuttumista. Esimerkiksi, jos opiskelija pääsisi muokkaamaan hänelle myönnettyjä arvosanoja, ei tiedon eheyteen voisi enää luottaa. Myös tiedonsiirron yhteydessä tapahtunut tiedon muuttuminen liittyy eheyteen. Eheyttä kohtaan voidaan hyökätä esimerkiksi viruksilla ja takaovilla.

Saatavuudella käsitetään palvelun tai tiedon täsmällinen ja tarkoituksenmukainen käsiteltävyys (Raggad, 2010, s. 20; First, 2023). Kriittisissä palveluissa kuten pankki ja terveydenhuolto, on erityisen tärkeää, että ne toimivat poikkeuksetta. Hyökkäykset, joissa vaikutetaan esimerkiksi verkkosivun verkkoyhteyden, prosessorin tai levyn kapasiteettiin, ovat hyökkäyksiä saatavuutta kohtaan. Saatavuus voi häiriintyä myös esimerkiksi luonnollisten laitteistorikkojen myötä, jotka voivat johtua säätilan muutoksista tai virtapiikeistä.

Raggad (2010, s. 21–23) esittää kirjassaan, että turvallisuustavoitteiden ja yrityksen tavoitteiden välille saattaa muodostua ristiriita, jossa CIA-kolmion osa-alueet haittaavat yrityksen toiminnallisuuksia. Täten on tunnistettava, että CIA-kolmiossa on omat heikkoutensa. Niin kutsuttu "Turvallisuustähti" (engl. *The Security Star*) on CIA-kolmion ohella toinen vaihtoehtoinen tapa tarkastella tietoturvallisuutta. Tähtimallissa mukaan tulevat todennus, kiistämättömyys ja riski. Kiistämättömyydellä pyritään siihen, että viestinnän molemmat osapuolet eivät voi kieltää olleensa osallisia tiedonvaihtoon. Tähän liittyen todennuksella kyetään tunnistamaan käyttäjä tosiasiassa siksi, kun hän väittääkin olevansa. Lopuksi riskienhallinta on koko turvallisuustähden keskiössä. Sillä on vaikutus kaikkiin muihin osa-alueisiin, ja onnistuneella riskienhallinnalla nämä pystytään turvaamaan riittävän hyvin, tunnistamalla mahdolliset uhkat ja kehittämällä niitä kohtaan vastatoimet (Raggad, 2010, s. 21–23).

## 3.2 Kyberturvallisuuden hallinnan osakokonaisuudet

Tietoturvan ja kyberturvallisuuden hallinnan osa-alueet voidaan kategorisoida usealla eri tavalla. Vertailemalla eri lähteitä ja auditointikriteeristöjä, on sisältö kuitenkin pitkälti samankaltaista, joskin jaotteluissa on eriäväisyyksiä. Pohjaymmärryksen luomiseksi kyberturvallisuuden hallinnasta, on tässä luvussa esitelty kolmiosainen jaottelu, joka esiintyy sellaisenaan muun muassa Kansallisen tietoturvan auditointikriteeristö KATAKRI:ssa (Ulkoministeriö, 2020). Jaottelu on seuraava: Turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen turvallisuus.

Kyseisen jaon voisi pilkkoa useampaankin osaan. Esimerkiksi turvallisuusjohtamisesta voisi irrottaa henkilöturvallisuuden omaan kategoriaansa ja teknisen turvallisuuden voisi jakaa esimerkiksi verkkoon, laitteisiin ja dataan. Kuitenkin kolmikantainen jaottelu antaa selkeän kuvan niistä kokonaisuuksista, mitä kyberturvallisuuden hallintaan kuuluu.

Turvallisuusjohtamisella tarkoitetaan erityisesti hallinnollisia toimenpiteitä, joilla yrityksen turvallisuus on taattu (Ulkoministeriö, 2020, s. 8). Tässä tutkimuksessa turvallisuusjohtamisessa käsitellään erityisesti turvallisuusjohtamista tietoteknisestä näkökulmasta. Tämän osa-alueen onnistuneella toteuttamisella johdon lähtökohdat, toteutustavat ja päämäärät ovat alaisillekin selkeät. Yksinkertaisimmillaan turvallisuusjohtaminen on vain onnistunutta yrityksen tietoturvaajatuksen jalkauttamista jokaiselle toimijalle. Käytännössä se voi esiintyä yksittäiselle työntekijälle esimerkiksi toistuvina tietoturvakoulutuksina ja salasanakäytäntöjen vaatimuksina. Organisaation tulee myös kyetä varmistamaan, että opetettuja asioita noudatetaan oikein (Ulkoministeriö, 2020, s. 8), eli pelkkä käskeminen ei riitä, vaan onnistunut turvallisuusjohtaminen vaatii myös riittävää valvontaa. Myöhemmin hyökkäyspinnan hallinnan luvussa varjo-IT näyttelee merkittävää roolia tässä osa-alueessa.

Turvallisuusjohtamisen alle asettuu menettelytapojen ja riskien arvioinnin dokumentointi (Ulkoministeriö, 2020, s. 8). Yleisesti kaikki johtamiseen ja turvallisuuteen liittyvät asiat tulee olla kirjattuna ylös, jotta epäkohtien sattuessa ongelmanratkaisu on sujuvampaa. Tämän tutkimuksen viitekehykseen liittyy ominaisesti turvallisuusjohtaminen ja yrityksen toteuttama riskienhallinta.

Henkilöstöturvallisuuden hallinnointiin kuuluu asiat kuten laadunvarmistus ja turvallisuusnäyttö (Raggad, 2010, s. 17). Eli palkatun henkilön tulee olla tosiasiassa riittävän osaava tehtävään, sekä hänen taustansa tulee olla selvillä, jotta sisäisen uhkan muodostuminen ei ole mahdollista. Pääsyoikeuksien säätäminen, niin fyysisten laitteiden kuin sähköisten sovellusten ja verkkolevyjen suhteen, kuuluu saman kategorian alle. Turvallisuuskoulutuksella pyritään siihen, että työntekijöillä on riittävä osaaminen, ja lisäksi salassapitosopimuksella varmistetaan lain silmissä tiedon vuotamiseen liittyvät asiakokonaisuudet. Riittävällä osaamisen- ja laadunvarmistamisella voidaan varmistua esimerkiksi siitä, ettei työntekijä vahingossa lataa verkkoon julkiseksi yrityksen käytössä olevia avaimia tai salasanoja, jotka pahimmassa tapauksessa vaikuttavat yrityksen tietojen luotettavuuteen ja eheyteen.

Toiminnallisuuksien hallinnassa tulee huomioida esimerkiksi yhteistyökumppaneiden kanssa toiminta. Eli miten, ja mitä tietoa saadaan jakaa ja siirtää järjestelmien välillä. Raggad esittää kyseisen osa-alueen kuitenkin hyvin suurpiirteisenä, joka tarkoittaa sitä, että tämä pätee myös täysin automatisoituihin ja sähköisiin järjestelmiin. Jo osatekijäkuvassa (KUVIO 2), esitettiinkin tietoturvallisuusjärjestelmän osatekijöiden keskinäisriippuvuus. Näiden keskinäisriippuvuuksien onnistunut hallinta vaatii säännöksiä, käytäntöjä, standardeja ja protokollia kaikkien osatekijöiden välille (Raggad, 2010, s. 17).

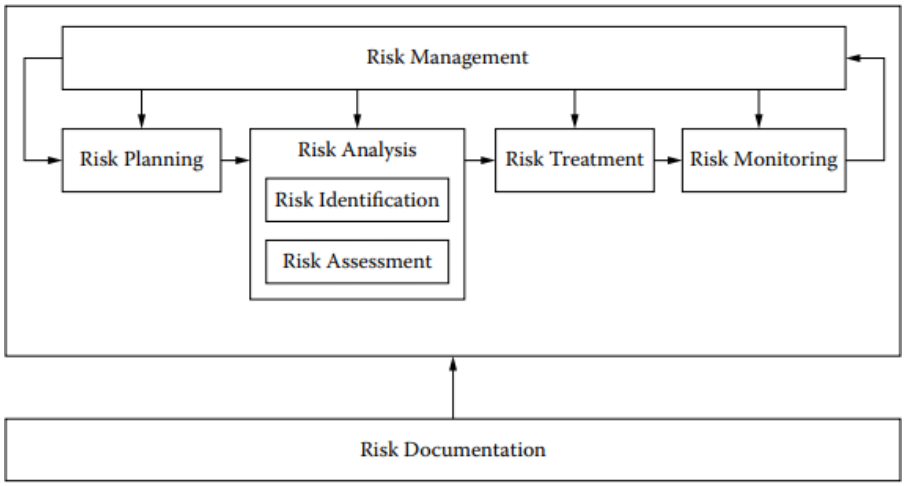
Turvallisuusjohtamiseen kuuluu olennaisesti riskienhallinta, joka on kaikkia tämän alaluvun kolmea osakokonaisuutta läpileikkaava elementti. Perinteinen riskienhallinta esitetään tarkemmin omassa alaluvussaan 3.3.

Fyysinen turvallisuus käsittää yleisesti tilaturvallisuuteen liittyvät asiat, jotka eivät välttämättä ole pelkästään tietoturvaan liittyviä asioita (Raggad, 2010, s. 508–509). Esimerkiksi pääsynvalvonta aitojen, valvontakameroiden ja vartijoiden toteuttamana turvaa tilan kaikelta asiaankuulumattomalta toiminnalta. Kyberturvallisuuden osalta tilaturvallisuuteen kuuluu laitekaappien sijoittelu ja niiden lukitseminen, ettei esimerkiksi haitallista ohjelmaa sisältävää muistitikkua päästä liittämään yrityksen järjestelmiin. Fyysisen turvallisuuden osalta on myös tärkeätä tunnistaa ne uhkatekijät ja riskit, jotka muodostuvat osin odottamattomasti ja reaalimaailmasta. Näitä ovat luonnonkatastrofit, tulipalot ja vesivahingot (Raggad, 2010, s. 508–509).

Tekninen tietoturvallisuus on se osa-alue, joka käsittää datan, järjestelmät, tietoverkot ja sovellukset sekä niiden toimintatavat teknisellä tasolla (Ulkoministeriö, 2020, s. 63–64). Huomioitavia asiakokonaisuuksia on esimerkiksi tiedonsiirron ja sen salauksen mekanismit sekä palomuurien ja tunkeutumisenhavaitsemis- ja estojärjestelmien toiminnan määrittäminen. Pääsyoikeuksien hallinnointi määritetään jo turvallisuusjohtamisen osa-alueella, mutta sen käytännön toteutus kuitenkin kuuluu teknisen tietoturvallisuuden alle (Ulkoministeriö, 2020, s. 76–77).

## 3.3 Perinteinen riskienhallinta

Riskien tunnistaminen ja niiden hallinta on usein keskeistä turvallisuuden hallinnassa. Raggad esittää riskienhallinnan elinkaaren alla olevan kuvion tavoin (KUVIO 4) (Raggad, 2010, s. 287). Kun riski on tunnistettu, voidaan sen todennäköisyyden ja vaikutuksen perusteella määrittää paras tapa poistaa tai vähentää riskin mahdollisesti aiheuttamaa vahinkoa. Tämän jälkeen riskin muutosta tulee kyetä seuraamaan, jotta myöhemmin suunnitelmaa voidaan päivittää. Kyseessä on siis iteratiivinen prosessi, josta tulee olla olemassa selkeä suunnitelma. Kyseinen malli toimii niin teknisiin riskeihin kuten sovelluksiin, mutta yhtä lailla myös ihmisiin ja prosesseihin (Raggad, 2010, s. 287).




KUVIO 4 Riskienhallinnan elinkaari (Raggad, 2010, s. 287)

Raggad (2010, s. 287) jakaa riskit kahteen eri kategoriaan: Omaisuusriski (engl. *Asset risk*), jossa riskin toteutumisen vaikutukset kohdistuvat luotettavuuteen, eheyteen tai saatavuuteen. Näitä riskejä voi luonnehtia jopa käsinkosketeltaviksi, kuten esimerkiksi "verkkosivu ei toimi" tai "varausjärjestelmä ei päivity". Yritysriskin (engl. *Enterprise Risk*) vaikutukset kohdistuvat suoraan yrityksen arvoon tai ei-rahalliseen arvoon kuten luotettavuuteen. Näiden kahden osa-alueen välillä on kuitenkin keskinäisriippuvuutta. Omaisuusriski voi aiheuttaa yritykselle myös arvonalenemaa, jos esimerkiksi verkkosivu on tarpeeksi kauan alhaalla. Toisaalta myös yrityksen johtoon kohdistunut realisoitunut riski, joka laskee yrityksen arvoa, voi suoraan vaikuttaa siihen, miten luotettavina käyttäjät näkevät yrityksen palvelut. (Raggad, 2010, s. 287)

Riskienhallinnassa tulee huomioida se, ettei riskiä välttämättä poisteta kokonaan. Riski voidaan tunnistaa eri vakavuusasteisiksi, jolloin kriittiset riskit halutaan todennäköisimmin poistaa kokonaan, keskitason riskit halutaan lieventää, ja matalan tason riskit jätetään jopa täysin huomioimatta. Esimerkiksi jos yritykselläsi on alle prosentin mahdollisuus, että sähkökatko katkaisee aamuyöllä verkkosivun minuutiksi, ei välttämättä satojen eurojen varavirtajärjestelmä ole kannattavaa. Tällöin riski on tunnistettu ja huomioitu, mutta sen vähäisen vaikutuksen vuoksi siihen ei ole katsottu tarpeelliseksi puuttua. Tämän takia riskienhallinnassa ei puhuta pelkästään riskin korjaamisesta tai poistamisesta, vaan sen hallinnasta.

Riskienhallinnassa pyritään arvioimaan menetettyä arvoa ja saatua hyötyä määrällisesti, jos vain tarkasteltava järjestelmä on riittävän helposti mitattavissa (Raggad, 2010, s. 301). Esimerkiksi verkkopalvelu, joka tuottaa yritykselle tasaisesti sata euroa tunnissa läpi vuoden, on helposti laskettavissa, että 24 tunnin mittainen aika, jonka järjestelmä on pois päältä, menettää yritys potentiaalisesta tuotostaan 0,27 % vuodessa. Rahassa mitattuna tämä on 2400 euroa. Tällöin on tarpeen tunnistaa, ettei esimerkiksi 10 000 euroa vuodessa maksavaa toimenpidettä ole välttämättä järkevää toteuttaa, tarkasteltaessa asiaa omaisuusriskin näkökulmasta. Raggad esittää kaksi eri tapaa laskea näitä: ALE (Annualized Loss

Expectancy) eli "Vuosittainen tappioennuste" ja ABLE (Asset-Based Loss Exposure) eli "Omaisuuteen perustuva menetysalttius" (Raggad, 2010, s. 301, 311).

Vaikka riskienhallinnassa on mahdollista käsitellä riskiä raakoina numeroina, ei riskin pienentäminen välttämättä ole numeraalisesti todennettavissa. Tästä syystä riskienhallinnassa vahvaa kontrollia onkin luonnehdittu pelkäksi illuusioksi (Walls, ym., 2019). Kriteeristöjen suuri painoarvo riskienhallinnassa voi johtaa siihen, että keskitytään arvioimaan sellaisia asioita, joiden tarkka arviointi todellisuudessa on mahdotonta. Tällöin päättäjillä ja suunnittelijoilla voi muodostua putkinäkö vain selkeästi tunnistettuja asioita ja järjestelmiä ja niiden riskejä kohtaan, kun tärkeämpi olisi painottaa ymmärryksen lisäämistä omaisuuden tunnistamiseen ja hyökkäyspinnan kokonaisuuteen.

Raggadin riskienhallinnan malli on kuitenkin vain yksi monista. Eri turvallisuuskehykset ja kriteeristöt kuvaavat omat riskienhallintamallinsa, sekä yksityisillä tietoturvayrityksillä voi olla omia prosessejaan. ENISAn (2023) laajassa raportissa riskienhallintamallien yhteentoimivuudesta todettiin johtopäätöksenä, että yleisimmin mallit sisältävät vähintäänkin riskien tunnistamiseen liittyen omaisuuden, uhkien ja haavoittuvuuksien tunnistamisen. Riskien arviointi käsittää jonkin asteisen laskennan ja arvioinnin. Raportissa tunnistettiin myös se, että useimmat mallit laskevat riskin arvon vaikutuksen ja todennäköisyyden kautta (Usein esitettynä *Likelyhood x Impact = Risk Score*). Tähän kaavaan on myös joissain malleissa lisätty esimerkiksi haavoittuvuuden taso tai mahdollisia muita muuttujia. Kokonaisuudessaan tarkasteltuna riskienhallintamallit noudattavat siis hyvin samankaltaisia periaatteita, joita jo Raggad kirjassaan esitti vuonna 2010.

Keskiöön riskienhallinnassa siis nousee yrityksen omaisuuden tunnistaminen ja niihin kohdistuvien riskien todennäköisyyden ja vaikutuksen tarkka arviointi. Riskien analyysiä voi NIST SP 800-30:n (NIST, 2012) mukaan toteuttaa kolmella eri tavalla: uhkalähtöinen, omaisuuslähtöinen ja haavoittuvuuslähtöinen. Uhkalähtöisessä mallissa uhkien tunnistaminen toimii pohjana skenaarioiden luomiselle, joka entisestään mahdollistaa haavoittuvuuksien ja vaikutuksen arvioinnin. Omaisuusperustaisessa mallissa kriittiset korkean riskin järjestelmät tunnistetaan, ja niiden osalta luodaan mahdolliset riskiskenaariot, jonka kautta arvioidaan mahdolliset uhkat. Haavoittuvuusperustainen malli taas tunnistaa olemassa olevat haavoittuvuudet, jonka pohjalta luodaan skenaariot ja sitä kautta tunnistetaan uhkat ja niiden vaikutukset.

Tutkimuksen lähtökohtana ja tutkimusongelmana esitetty Gartnerin kritiikki perinteiseen kyberturvallisuuden riskienhallintaan on jo tunnistettu Intian yliopiston tutkimusartikkelissa (Gandotra, Singhal & Bedi, 2012), jossa esitettiin malli proaktiivisesta uhkalähtöisestä riskienhallintamallista. Tämän mallin keskiössä oli uhkien tunnistamisen toteuttaminen hunajatunnusten (engl. *Honeytoken*) ja tilastollisten tekniikoiden avulla. Lähtökohtana tutkimuksessa oli, että tiedossa olevat sekä tiedostamattomat uhkat tulisi kyetä tunnistamaan. Artikkelin johtopäätöksissä tutkijat ovat todenneet jo vuonna 2012, että perinteiset riskienhallintatekniikat ovat tunnistettu riittämättömiksi, sillä ne perustuvat vain tunnistettuihin uhkiin. Gartnerin esitys jatkuvasta, uhkalähtöisestä ja

proaktiivisesta tavasta hallita hyökkäyspintaa tuottaisi parempia tuloksia kuin perinteinen riskienhallinta. Myöhemmissä luvuissa tarkastellaan tarkemmin uhkalähtöisen riskienhallinnan peruselementtejä kuten hyökkäysmallin ja uhkatoimijoiden ymmärrystä. Proaktiivisessa toiminnassa uhkien metsästys ja hyökkäyspinnan kokonaisvaltainen tulkinta on hyvinkin keskiöön nousevia kokonaisuuksia.

Arponen (2023) tunnisti pro gradu -tutkimuksessaan, että riskienhallintaan kohdistuva kritiikki kuitenkin on osin aiheetonta ja se voidaan perustella riskienhallintaa toteuttavan henkilöstön osaamattomuudella. Tärkeäksi koettiin myös se, että riskienhallintaprosessissa olisi mukana myös henkilöitä, joiden pääsubstanssi ei olisi itse riskienhallinta. Tutkimuksen haastatteluissa myös selvisi, että "laatikon ulkopuolelta ajattelu" koettiin positiiviseksi ja tärkeäksi asiaksi. Tulevaisuuden trendien tarkastelu ja omaksuminen sekä avoin lähtökohta riskienhallinnalle voisi siis olla avain onnistuneeseen riskienhallintaan.

Toisaalta digi- ja väestötietoviraston kyselyssä (Rousku, 2021) riskienhallinnan kehittämiskohteiksi nousi kyseisten prosessien kokonaisvaltainen kehittäminen ja ulottaminen erilaisiin toimijoihin. Vain kerran vuodessa tapahtuva ja liian staattinen prosessi tulisi päivittää tiheämpään tapahtuvaksi, joka tällöin tukee osaamisen kehittämistä, pienentää kuormitusta ja tukee tilannetietoisuutta. Kyselyyn vastanneista julkishallinnon organisaatioista vain noin puolet arvioivat riskejä säännöllisesti.

## 3.4 Lainsäädäntö ja kriteeristöt

Auditointikriteeristöjen, standardien ja ohjeiden tarkoituksena on tukea päätöksentekijöitä ja yrityksen johtoa luomaan ja ylläpitämään yrityksensä informaatiojärjestelmien turvallisuutta hallinnollisella, fyysisellä ja teknisellä tasolla. Kriteeristöt voivat tuottaa virallisen maksullisen sertifiointitodistuksen yritykselle (ISO, 2022) tai ne voivat olla puhtaasti ohjeistuksia ja suuntaviivoja (NIST, 2023a) onnistuneen tietoturvan toteuttamiseen. Lisäksi on kehitetty myös kansallisia kriteeristöjä, kuten suomalainen KATAKRI (Ulkoministeriö, 2020).

ISO/IEC 27001 (ISO, 2022) on tunnetuin tietoturvallisuuden hallintajärjestelmien standardi. Se on kriteeristö, jonka virallinen sertifiointi on yritykselle maksullinen prosessi. Tämänkaltainen sertifiointiprosessi on hyvä tapa näyttää asiakkaille, sidosryhmille ja osakkeenomistajille tietoturvan todellinen taso, eikä pelkästään luoda varmuutta sisäisesti omaan toimintaan, sillä kyseisen akkreditoinnin tekee täysin yrityksen ulkopuolinen toimija. ISO-standardisarjan voi kuitenkin myös implementoida toimintaansa ilman, että hakee sertifiointia. ISO 27002 on standardisarja, joka sisältää teknisellä tasolla tietoturvallisuuden hallintakeinot, kun taas 27001 asettaa vaatimuksia yrityksen ylemmällä tasolla (ISO, 2022). Suomessa esimerkiksi FiSMA Ry hoitaa ISO/IEC JTC1 SC7 standardin auditointeja ja siihen liittyvää työtä kuten koulutuksia ja tiedonantoa (FiSMA, 2023).

NIST on Yhdysvaltain kauppaministeriön kansallinen standardien ja teknologian instituutti. Toisin kuin ISO 27001, NIST Cybersecurity Framework

(NIST, 2023a) on ilmainen. On siis perusteltua etenkin aloitteleville, pienille tai keskisuurille yrityksille hyödyntää ilmaisia standardeja. NIST CSF on jaettu kuuteen osa-alueeseen. Näiden osakokonaisuuksien pohjalta yritys kykenee tarkastelemaan, kehittämään ja ylläpitämään omia tietoturvatoimenpiteitään. Koska NIST CSF:lle ei ole erikseen virallista auditoivaa elintä, tapahtuu auditointi joko yrityksen itsensä tai erikseen palkatun ulkoisen toimijan toimesta. Vaikka tämä parantaa yrityksen omaa ymmärrystä ja varmuutta toiminnastaan, se ei samaan tapaan kerro turvallisuuden tasosta ulkopuolisille kuin ISO-standardin virallinen sertifikaatti (NIST, 2023a).

Sisällöllisesti NIST CSF ja ISO 27001 ovat hyvin samankaltaisia, ja erot löytyvät lähinnä abstraktiotasojen käsittelyssä ja esittelyssä. Yllä esiteltyjen lisäksi standardeja, auditointikriteeristöjä ja turvallisuuskehyksiä (engl. *Security Framework*) löytyy useita, joista osa käsittelee aihetta laajemmin ja osa keskittyy tarkemmin yksittäisiin pienempiin osakokonaisuuksiin. SecurityFrame avasi blogissaan lyhyellä vertailulla näistä neljäätoista (Bonnie, 2024).

Päätettäessä turvallisuuskehyksen ja standardien käyttämisestä, on auditoijan ja yrityksen tunnistettava mahdollisuudet ja heikkoudet vähintäänkin tunnetuimpien kriteeristöjen kohdalla. Lisäksi vahva ymmärrys alaan liittyvästä lainsäädännöstä on tärkeää osata, jotta oikeaa kriteeristöä tulee käytettyä. Esimerkiksi terveyspalveluja koskeva HIPAA (Health Insurance Portability and Accountability Act) on tarpeen ottaa huomioon tietynlaisissa yrityksissä, jos liiketoimintaa tapahtuu EU:n lisäksi myös Yhdysvalloissa (ENISA, 1996).

Suuri osa tietoturvasta liittyy jo olemassa olevaan lainsäädäntöön, ja pyörää harvoin tarvitsee keksiä täysin uudelleen, kehitettäessä yrityksen kyberturvallisuuden suunnitelmaa. Katakri ja Julkri toimivat hyvinä reitteinä suomalaiseen lainsäädäntöön tutustuakseen. Näiden dokumenttien lähdeluettelosta löytyykin ajantasaisimmat ja merkittävimmät lait, joiden pohjalta kyseiset kaksi kriteeristöä on luotukin. Tämän lisäksi valtiovarainministeriö tarjoaa oppaita ja ohjeita esimerkiksi onnistuneeseen riskienhallintaan (Sääskilahti & Mustonen, 2023).

On kuitenkin tunnistettava kohdeyrityksen kansainvälisyys ja muiden kohdevaltioiden omat lainsäädännöt. Tämän lisäksi on aina huomioitava mahdollinen toimialakohtainen lainsäädäntö, jota löytyy esimerkiksi rikosoikeudellisissa, finanssialan ja lääketieteen asioissa. Tunnettuja ja merkittäviä kyberturvallisuuteen liitettäviä lakeja ja säädöksiä ovat muun muassa Yleinen tietosuoja-asetus (GDPR), Laki julkisen hallinnon tiedonhallinnasta (906/2019), Laki digitaalisten palvelujen tarjoamisesta (306/2019), Kansainvälisen turvallisuusluokitellun tiedon tietoturvan arviointi (588/2004) ja EU:n verkko ja tietoturvadirektiivi. Eroja löytyy julkishallinnon sekä yksityisten toimijoiden välillä. Lisäksi tietosuoja-asetus (GDPR) määrää asioita vain, kun se koskee tietynlaisen tiedon käsittelyä, eikä asetus täten koske automaattisesti kaikkia yrityksiä.

Hyökkäyspinnan ja uhka-alttiuden osalta lainsäädäntöä on määritelty jonkin verran, joskin se suurelta osin rivien välistä tulkittavana tekstinä riskienhallintaan liittyvissä tekstiosissa. Esimerkiksi Laki julkisen hallinnon tiedonhallinnasta (907/2022) määrittää tiedonhallintayksikön vastuulle selvittää "olennaiset

tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.”.

Euroopan unionin NIS2-asetuksessa (2022) riskienhallinta esiintyy useaan kertaan, joskin siihen ei aseteta järin tarkkoja vaatimuksia. Asetuksessa on tunnistettu hyökkäyspinnan jatkuva kasvu, jonka pohjalta asiakirjassa todetaankin uhkien todennäköisyyden yhä kasvavan (Euroopan unioni, 2022, s. 19). Asetus määrittää riskienhallinnan tavoitteet ja perustelee sen tarkoituksen, mutta riskienhallinnan vaatimukset ovat abstraktiotasoltaan suhteellisen korkeita. Ne eivät esitä tarkkoja teknisiä vaatimuksia tai niiden implementointikeinoja, vaan enemmänkin yleistason ohjenuoria, joissa käsitellään, mitä kaikkea riskienhallintaan liittyvää yrityksen tulisi toteuttaa. Näistä ovat esimerkkejä muun muassa hyvä kyberhygienia ja -koulutus, kybertapahtumien hallintakeinot ja toimitusketjun turvallisuus (Euroopan unioni, 2022, s. 48). Teknisenä vaatimuksena direktiivi esittää monivaiheisen tunnistautumisen ja jatkuvan tunnistautumisen ratkaisut kuvan, puheen ja tekstin välittämiseen tarvittavilta osin. Asetus antaa siis jokaiselle jäsenmaalle ja toimijalle hyvin vapaat kädet riskienhallinnan toteuttamiselle.

NIS2:n vaikutusta riskienhallinnan näkökulmasta on tutkittu ainakin Instan (2022) toimesta riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille. Tutkimus toteutettiin kyselytutkimuksena ja se pyrki tunnistamaan riskienhallintavelvoitteiden rahalliset kustannukset. Tutkimuksen tuloksissa todetaan, että riskienhallinnan rahallinen arviointi oli monista yrityksistä vaikeaa, eivätkä yritykset täten pystyneet esittämään arviotaan (Insta, 2022, s. 46). Instan tutkimus tukee siis ajatusta, että riskienhallinta sisältää epämääräisyyttä tulkittaessa uhkien vaikutusta. Yhteenvedossa todetaan, että yritykset tulevat tarvitsemaan ohjausta riskiperusteiseen lähestymistapaan, jotta toimenpiteet ovat suhteutettu oikein yrityksen kokoon nähden.

Soikkeli (2021) tutki lainsäädäntöä tieto- ja kyberturvallisuuden perustana, pro gradu –tutkielmassaan, jossa yhteenvedossa toteaa lainsäädännön olevan ristiriitaista riskienhallinnan osalta. Vaatimuksia asetetaan riskiperusteisesta arvioinnista, mutta todellisuudessa iso osa teknisistä ratkaisuista tapahtuvat palveluntarjoajan toimesta. Riskienhallinnan kokonaisvaltainen arviointi ja toteuttaminen voi siis olla yksittäiselle toimijalle hankalaa, jos yrityksellä on käytössään kolmannen osapuolen järjestelmiä ja palveluita. Peilaten tätä johtopäätöstä aiemmin esitettyyn Gartnerin väittämään, riskienhallinnan tuottamasta virheellisestä turvallisuuden tunteesta, olisi riskienhallinnan ohjeistuksessa lain ja valtiollisten ohjeiden näkökulmasta tarkentamisen varaa.

Lainsäädäntö tai direktiivit eivät siis suoranaisesti aseta tarkkoja vaateita tämän tutkimuksen viitekehykseen hyökkäyspinnasta tai uhka-alttiudesta, joskin nämä aiheet kulkevat käsi kädessä riskienhallinnanprosessien mukana.

# 4 UHKALÄHTÖISYYS JA HYÖKKÄYSPINTA

Tämä luku avaa lukijalle termit uhka-alttius (engl. *Threat Exposure*) ja hyökkäyspinta (engl. *Attack Surface)* sekä näiden hallinnan. Lisäksi uhkalähtöisen ajatteluumalliin ja uhkiin perustuvan riskienhallinnan osakokonaisuudet esitellään tässä luvussa. Luku käsittelee hyökkäysmalleja, uhkatoimijoita ja kyberuhkatiedustelun, jotta ymmärrys hyökkäyspintaan kohdistuvista konkreettista toimijoista, keinoista ja näiden tunnistamisesta avautuu lukijalle.

## 4.1 Hyökkäyspinta

Hyökkäyspinta ei ole täysin vakiintunut termi alalla, ja sen merkitys vaihtelee kirjoittajasta ja lähteestä riippuen. Kyberturvallisuuskeskus (2023) määrittää sen olevan julkisessa verkossa näkyviä sovellusten haavoittuvuuksia, joita hyökkääjä voi käyttää haitalliseen toimintaan.

IBM (2023b) kuvaa hyökkäyspinnan hallinnan olevan kyberturvallisuushaavoittuvuuksien jatkuvaa havaitsemista, analysoimista, korjaamista ja valvontaa. Tämän hallinnan pohjalta kyetään tunnistamaan yrityksen hyökkäyspinta. Hyökkäyspinnan hallinnassa on tarkoitus tarkastella organisaatiota täysin hyökkääjän silmin. IBM siis ymmärtää hyökkäyspinnan keskittyvän myös teknisiin haavoittuvuuksiin (IBM, 2023b)

Theisen, ym. (2018) tunnistivat systemaattisessa kirjallisuuskatsauksessaan, tutkittuaan 644 artikkelia, hyökkäyspinnalle 6 eri teemaa. Monet tutkimukset myös käyttivät termiä sen enempiä sitä avaamatta. Yleisesti teemoista voi tunnistaa sen, että monet käyttävät hyökkäyspintaa terminä, jolla kuvataan kokonaisvaltaisesti kaikkea mahdollista julkisessa verkossa näkyvää yrityksen toimintaa, jota hyökkääjän on mahdollista hyödyntää tehdäkseen tuhoa järjestelmään. Tällöin kyse on lähinnä digitaalisen näkökulman teknisistä asioista. Hyökkäyspinnalla voidaan tarkoittaa myös sovellusta, jossa mitään tiedossa olevia haavoittuvuuksia ei ole, mutta potentiaali haavoittuvuuden löytämiselle kuitenkin on olemassa. Haavoittuvuuksia voi kuitenkin myös löytyä ihmisistä, ja

esimerkiksi salakuuntelu voi tapahtua täysin ilman digitaalista ulottuvuutta. Hyökkäyspinta voidaan jakaa siis digitaaliseen ja fyysiseen hyökkäyspintaan.

Hyökkäyspinnalla voisi yleisesti tarkoittaa esimerkiksi yrityksen tiedossa ja tiedostamattomissa olevia sovelluksia, toimintamalleja ja järjestelmiä, joita hyökkääjä voi hyödyntää haitalliseen toimintaan. Hyökkääjän silmin tarkasteltuna tämä tarkoittaa kaikkia mahdollisia reittejä ja keinoja, joilla yrityksen tieto-omaisuuden luottamuksellisuuteen, eheyteen tai saatavuuteen kyetään vaikuttamaan. Käytettäessä toisaalta termiä ”tekninen hyökkäyspinta”, tarkoitettaisiin pelkästään teknisiä asioita kuten avoimia verkkosovellusten portteja ja haavoittuvaisia web-sovelluksia.

Randorin (2022, s. 6) tutkimuksen mukaan 67 % yrityksistä huomasivat oman hyökkäyspintansa kasvaneen viimeisen kahden vuoden aikana. Kasvuun vaikuttaneita tekijöitä olivat pilvisovellukset, SaaS-palvelu, kolmannen osapuolen tuottajat ja etätyöskentely. 69 % yrityksistä ovat kohdanneet kyberturvallisuuspoikkeaman tunnistamattoman, hallitsemattoman tai huonosti konfiguroidun sovelluksen tai järjestelmän takia. Randorin raportissa todetaankin näiden lukujen olevan jo riittävä todiste siitä, että yrityksen oman hyökkäyspinnan tunnistaminen on tärkeää.

Moni yritys edelleen ylläpitää omaa ymmärrystään hyökkäyspinnastaan taulukkolaskentasovelluksessa, joka on riittämätön ratkaisu nykypäiväisessä yritysmaailmassa (Randori, 2022, s. 12). Tutkimus esittääkin kolme toimintoa, jotka parantaisivat hyökkäyspinnan hallintaa: Haavoittuvuusskannauksien tiheys, kyvykkyys tehdä riskiarviot uhkatiedustelun pohjalta ja koulutuksen lisääminen aiheesta turvallisuus- ja IT-henkilöstölle. Hyökkäyspinnan hallinnassa ei siis ole kyse mistään täysin uudesta ilmiöstä, vaan enemmänkin toimintojen uudesta priorisoinnista ja näkökulman vaihtamisesta.

Zhang ja Perkins (2019) toteavat riskienhallinnan kontrollin olevan illuusio, ennustettavuuden olevan tavoittamattomissa ja monimutkaisuuden olevan pysyvää. Näiden löydösten pohjalta raportti ei vielä vuonna 2019 esittänyt ajatusta hyökkäyspinnan hallinnasta, vaikkakin tekstissä esiintyy ymmärrys siitä, että perinteinen tapa hallita riskejä, vastaamalla tapahtumiin asettamalla erilaisia kontrolleja, ei välttämättä ole nopeasti kasvavassa ja muuttuvassa yrityksessä tehokkain tapa ylläpitää digitaalista turvallisuutta (Zhang & Perkins, 2019, s. 4). Adaptiivisella toiminnalla tutkimuksessa puhutaan automaattisesta, esimerkiksi tekoälyllä tuotetusta, järjestelmästä, joka kykenee valvomaan laitteistoja ja sovelluksia, ja jopa ennakoiden hälyttämään käynnistyvistä uhkista.

Hyökkäyspinta on oleellinen osa altistumista ja uhkia, sillä pelkkä haavoittuvuusanalyysi käsittää vain ne asiat, joita sen skannaukseen on konfiguroitu. Hyökkäyspinta-analyysi mahdollistaa niiden tietoaukkojen täydentämisen, joita haavoittuvuusanalyysi jättää avoimeksi (Schneider, ym., 2022, s. 1–2).

Hyökkäyspinnan tunnistaminen on kriittistä uhka-alttiuden muodostumisessa ja riskienhallinnassa. Tunnistamalla oman hyökkäyspintansa, kykenee yritys ymmärtämään hyökkääjän mahdollisuudet yhtenä kokonaisuutena. Yritys kykenee myös paremmin tunnistamaan, mitkä sovellukset ja toiminnot tarpeettomasti kasvattavat hyökkäyspintaa, ja ovat täten turhia (Gartner, 2022a).

Yhtenä keskeisenä hyökkäyspintaa kasvattavana, ja osin automatisoitujen haavoittuvuusskannereiden näkymättömiin jäävänä, ilmiönä on varjo-IT (engl. *Shadow IT*). Tällä tarkoitetaan yrityksen käytössä olevia järjestelmiä tai laitteita, joita ei ole alun perin tarkoitettu yrityksessä käytettäväksi. Tämä voi tarkoittaa esimerkiksi sovellusrajapintaa, jonka kehittäjä on päättänyt koodata sovellukseen ilman lupaa, jotta hänen työnsä olisi helpompaa. Varjo-IT voi tarkoittaa myös sovellusta, joka on ladattu koneelle, vaikkei sille ole saatu tietojärjestelmävastaavalta lupaa. Varjo-IT:tä ovat myös laitteet, joita ei ole hankittu normaalin hankintaprosessin kautta, kuten esimerkiksi luvaton langaton hiiri (Cisco, 2023b; Hart, Mingay & Topham, 2022).

Hyökkäyspinnan tunnistaminen on siis käytännössä haavoittuvuusskannausta laajempi tapa tunnistaa tietojärjestelmään kohdistuvat hyökkäysvektorit. Hyökkäyspinta on monesti osin näkymätön ja vaikeasti tunnistettava osa yrityksessä, joka kasvaa jatkuvasti ja täten mahdollistaa hyökkääjälle uusien hyökkäysreittien löytämisen, joista yritys ei ole tietoinen. Näitä reittejä yritys ei perinteisen riskienhallintamenettelyn kautta välttämättä tunnista, sillä se, mitä yritys on virallisesti dokumentteihinsa listannut omiksi järjestelmikseen ja laitteikseen, ei välttämättä vastaa sitä todellisuutta minkä hyökkääjä näkee.

Gartner oli vuonna 2018 arvioinut, että vuonna 2020 kolmasosa hyökkäyksistä tulisi tapahtumaan varjo-IT:n kautta (Goasduff, 2018). Osin tätä arviota tukee myöhemmin tullut data (Hart, ym., 2022), jonka mukaan noin 41 % yritysten henkilöstöstä ei ole IT-henkilöstöä, joka kuitenkin käyttää teknologiaa ja tuottaa siihen liittyvää dataa, ja täten voi olla riski varjo-IT:n kasvamiselle. Bombalin (2023) haastattelema ja Teslalle penetraatiotestausta suorittanut Jason Haddix totesi videohaastattelussa, että monet hänen asiakkaistaan eivät edes tienneet kaikkien omien palveluidensa ja verkko-osoitteiden olemassaolosta, joita Haddix esitteli yritykselle tiedusteluvaiheensa päätteeksi. Eli niinkin merkittävä yritys kuin Tesla ei ole tietoinen omasta hyökkäyspinnastaan, jonka osaava penetraatiotestaaja kuitenkin pystyi tunnistamaan.

Gartnerin tutkimuksissa kritisoidaan myös perinteisen riskienhallinnan tapaa mitata numeerisesti yrityksen potentiaalisia menetyksiä. Voiko kuitenkaan hyökkäyspintaan sen paremmin mitata? Hyökkäyspinnan mittaamista on tutkittu jonkin verran 2000-luvun puolella (Manadhata ym., 2005; Howard ym., 2005). Tutkimusten pohjalta on kuitenkin selkeää, että samankaltaista illuusiota kontrollista esiintyy, kun hyökkäyspintaa yritetään liian absoluuttisesti mitata. Mittaamalla on mahdollista arvioida esimerkiksi kahden sovelluksen hyökkäyspinnan kokoa yksinkertaisimmillaan tarkastelemalla, kummassa on enemmän portteja tai avoimia kenttiä, joihin syöttää tietoa. Tässä ei kuitenkaan saada vastausta siihen, onko hyökkäyspinta riittävän pieni, etteikö siihen kohdistuisi hyökkäyksiä. Siinä saadaan enemmänkin vastaus kysymykseen ”kumpi näistä sovelluksista olisi pienempi hyökkäyspinnan suhteen?” On kuitenkin myös todettava, että pelkkä absoluuttinen avoimien porttien määrä ei korreloi suoraan uhkalle altistumiseen, vaan tähän vaikuttaa myös, onko kyseinen portti hyväksikäytettävissä ja onko sovellukseen kohdistuva uhka luonteeltaan minkälainen.

Tämänkaltaisessa arvioinnissa auttaa aiemminkin mainittu CVSS-arviointitapa (First, 2023).

Howard, ym. (2005, s. 5) esittääkin tutkimuksessaan kattavan kolmikantaisen mallin, jolla teknisen hyökkäyspinnan mittaamisessa huomioidaan riittävästi osatekijöitä. Mallin kolme kohtaa ovat kohteet ja mahdollistajat, kanavat ja protokollat sekä pääsyoikeudet.

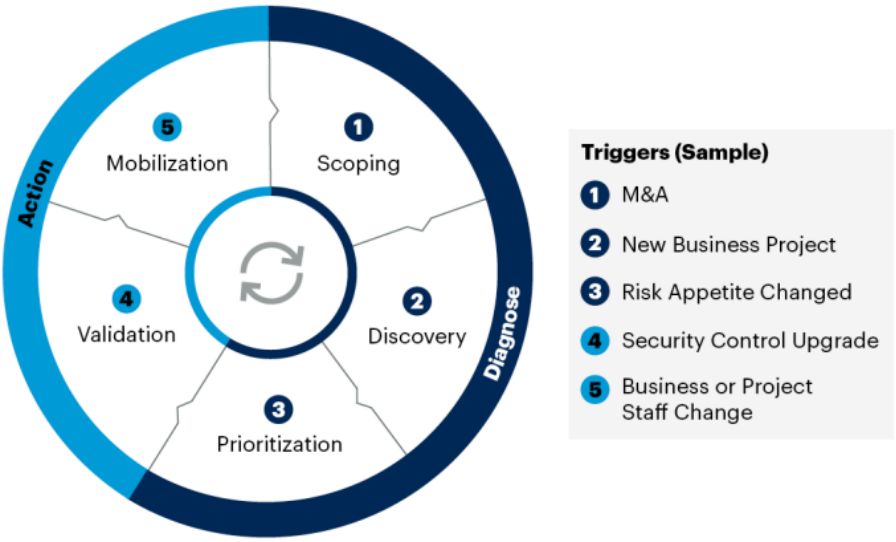
Hyökkäyspinnan hallinnassa on siis kolme keskeistä kokonaisuutta, joihin perinteinen riskienhallinta ei välttämättä vastaa täydellisesti: Ensimmäiseksi jatkuva ja kokoaikainen uhkien tunnistaminen, jota jatkuvasti kasvava hyökkäyspinta vaatii. Toiseksi hyökkäyspinnan laajuus ja näkymättömyys muun muassa varjo-IT:n ja yrityksen ulkoisten tietojen myötä. Kolmanneksi vaikutukseen ja todennäköisyyteen perustuva riskienhallinnan luoma illuusio kontrollista, johon hyökkäyspinnan ymmärrystä priorisoiva toimintamalli antaisi paremmat keinot hyökkäysten torjumiseen tai niiden tehon vähentämiseen. Näiden kolmen asian lisäksi keskustelu ja tutkimus käsitteellisesti hyökkäyspinnasta on rikkonaista. Hyökkäyspinta tulisikin nykyisessä vahvasti digitaalisen ja fyysisen maailman yhteen kasvaneessa kyberfyysisessä kokonaisuudessaan käsittää huomattavasti laajempana terminä, kuin vain hyökkäyspinnan teknisenä ulottuvuutena.

## 4.2 Uhka, altistuminen ja niiden hallinta

FIPS PUB 200 -standardi (NIST, 2023b) kuvailee kyberuhan olevan mikä tahansa olosuhde tai tapahtuma, jolla on potentiaali vaikuttaa yrityksen aineelliseen tai aineettomaan omaisuuteen liittyvään luvattomaan pääsyyn, tuhoamisen, paljastamiseen, muokkaamiseen tai käytön estämiseen.

D'Hoinne, Shoard ja Schneider (2022) kirjoittavat artikkelissaan, ettei mikään yritys pysty vastaamaan kaikkiin mahdollisiin kyberturvallisuustapahtumiin, vaan yrityksen tulisi ensisijaisesti pyrkiä minimoimaan altistuminen uhkille. Uhkille altistumisen minimointi voi sovellustasolla tarkoittaa yksinkertaisesti sitä, että yritys käyttäisi mahdollisimman pientä määrää erilaisia sovelluksia. Toisaalta minimointi voisi tarkoittaa myös yrityksen julkisen tiedottamisen minimointia tai työntekijöiden vähentämistä, joka hankaloittaisi hyökkääjän passiivista tiedustelua avointen lähteiden kautta. Tällöin kuitenkin yrityksen liiketoiminnan tavoitteet saattaisivat kärsiä. Altistumisella ei tule siis tarkoittaa haavoittuvuuksiin liittyvää uhkan realisoitumisen todennäköisyyttä. Altistumisessa kyse on kohteen näkyvyydestä uhkatoimijalle. Raggad (2010) konkretisoi altistumista esittämällä, miten hiiren on helpompi päästä juustoon käsiksi, jos juusto on sellaisenaan lattialla. Altistuminen on siis tällöin korkealla. Altistumista voi laskea, siirtämällä juusto laatikkoon ja jopa teippaamalla laatikon kansi kiinni.

Artikkeli (D'Hoinne, ym., 2022) esittää viisiportaisen mallin, jolla jatkuvaa uhka-alttiuden hallintaa (engl. *Continuous Threat Exposure Management*), myöhemmin CTEM voidaan toteuttaa (KUVIO 5).




KUVIO 5 Jatkuvan uhka-alttiuden hallinnan prosessivaiheet (D'Hoinne, ym., 2022)

Rajaus (engl. *Scoping*) vaiheessa yrityksen tulee tunnistaa omat ulkoisen hyökkäyspintansa rajat, johon sisältyy myös yleistymässä olevien tietoturvan palvelumallien (engl. *Security-as-a-Service (SaaS)*) toiminnallisuuksien tunnistaminen.

Toinen vaihe sisältää tunnistusprosessien laadinnan, jotta rajauksessa määritetty hyökkäyspinta on todellisuudessa tunnistettu (D'Hoinne, ym., 2022, s. 9). Ensimmäinen vaihe on äärimmäisen tärkeä, sillä vaikka toinen vaihe tehtäisiin kuinka hyvin, johtaa vaiheen yksi puutteet siihen, ettei koko hyökkäyspintaa ole todellisuudessa tunnistettu.

Kolmannessa vaiheessa priorisoidaan tunnistetut uhkat ja todennäköisyydet millä ne uhkat realisoituvat (D'Hoinne, ym., 2022, s. 9). On huomioitavaa, että tämänkaltaista mittausta ei välttämättä ole järkevä toteuttaa absoluuttisilla vaan ennemminkin suhteellisilla arvoilla samoin kuten hyökkäyspinnankin mittaamisessa (Manadhata, Wing, 2005; Howard, Pincus, Wing, 2020).

Neljännessä vaiheessa realisoituvien uhkien toteutumisen tapa ja vaikutus on tunnistettava (D'Hoinne, ym., 2022, s. 10). Esimerkiksi verkkosovellukseen kohdistuvan palvelunestohyökkäyksen tekotapa ja yrityksen oman palautumisen toimintamallien taso on arvioitava. Tässä vaiheessa on tärkeää ymmärtää hyökkäyksen toimintatapa ja kulku sekä mahdollisen hyökkääjän profiili, joka todennäköisesti yritystä kohtaan toimii. Näitä asiakokonaisuuksia tarkennetaan myöhemmissä alaluvuissa.

Viides vaihe on toiminnan jalkauttaminen siitä vastaaville toimijoille (D'Hoinne, ym., s. 11). Jatkuvaa uhka-alttiuden hallintaa pystytään automatisoimaan tiettyyn pisteeseen asti, mutta järjestelmistä vastaavien henkilöiden sekä päättävien henkilöiden tulee olla tietoisia toimintamallin mahdollisuuksista ja haasteista. Vaiheen tarkoituksena on poistaa tarpeettomat esteet toimintamallissa ja varmistua siitä, että koko prosessi toimii tarkoituksenmukaisesti.

Gartner arvioi, että vuonna 2026 yritykset, jotka käyttävät toiminnassaan jatkuvan uhka-alttiuden hallinnan ohjelmaa (CTEM) kärsivät kolme kertaa muita vähemmän tietomurroista (D'Hoinne, ym., 2022, s. 3).

Jatkuva uhka-alttiuden hallinta ei siis ole täysin uusi ilmiö tai trendi, vaan enemmänkin uusi näkökulma ja tapa käsitellä kyberturvallisuuden hallintaa, jossa keskeistä on se, miten hyökkääjä havainnoi yritystä ulkopuolelta hyökkäyspintaa kohden. Keskeistä on myös se, että perinteisen vuosikellon tavoin tehtävä riskienhallinta on hyvin staattinen prosessi ja CTEM:ssä taas on kyse alati jatkuvasta tarkastelusta. Kaikkiin uhkiin vastaaminen on lähes mahdotonta perinteisen riskienhallinnan keinoin, sillä uhkatoimijat kehittyvät ja muuttuvat jatkuvasti, eikä esimerkiksi tänä päivänä tehty riskien tunnistamisen prosessi välttämättä ole enää pätevä puolen vuoden päästä.

Walls, ym., (2023, s. 10) esittääkin perinteisen riskien arvioinnin sijasta käytettäväksi liiketoimintavaikutusten arviointia (engl. *Business Impact Assessment*), jossa tunnistamalla yrityksen järjestelmien kriittisyys ja niihin vaikuttavat liiketoimintaprosessit, on lähtökohta uhkien tunnistamiselle perinteistä mallia tarkempi. Tällöin periaatteena on, ettei kyberturvallisuudessa hallita riskejä, vaan uhkille altistumista.

## 4.3 Hyökkäysmallit

Hyökkäysmallien tarkoituksena on kuvata vihamielisen kybertoimijan prosessin osien ja niiden osien suhdetta helposti ymmärrettävällä mallilla (Stranger, 2020). Useimmat hyökkäysmallit sisältävät paljon samoja elementtejä kuten tiedustelu (engl. *Reconnaisance*), hyväksikäyttö (engl. *Exploitation*) ja tietojen varastaminen (engl. *Exfiltration*) (Lehto, 2022).

Yksinkertaisuudessaan eri hyökkäysmallit pilkkovat hyökkäysprosessin helpommin tarkasteltaviin osakokonaisuuksiin. Tämä mahdollistaa hyökkäyksen vaikutusten tarkastelun sekä suunniteltavien vastatoimenpiteiden järjestelmällisemmän ja helpomman suunnittelun ja toteutuksen. Esimerkiksi ymmärtäessämme, että tiedusteluvaihe saattaa sisältää huijauspuheluita, joiden tarkoituksena on kerätä yrityksestä sellaista tietoa, jota ei olisi tarkoitettu julkistettavaksi, voimme pyrkiä pysäyttämään hyökkääjän etenemisen jo tiedusteluvaiheessa. Sama pätee teknisellä tasolla esimerkiksi toteutettaessa tunkeutumisenestojärjestelmiä. Kun ymmärretään vastustajan toimintamalli, on siihen helpompi vastata.

Hyökkäysmalleilla usein kuvataan APT-ryhmien toimintaa. Edistynyt jatkuva uhka (engl. *Advanced Persistent Threat - APT*) on termi, jota käytetään kuvaamaan salaisesti toimivaa ja pitkäkestoista sekä sitkeää hyökkääjää, joka useimmiten on liitettynä sotilaallisesti ja/tai taloudellisesti valtioihin (Cisco, 2023a). Esimerkiksi APT-28, tunnetummin "Fancy Bear", on Venäläinen hakkeriryhmä, joka on aiheuttanut kaaosta tietoverkoissa muun muassa 2016 USA:n vaaleissa (Sayegh, 2023). APT:n kohteena on usein korkeatasoisesti ja tehokkaasti turvatut kohteet. Hyökkäysten tarkoituksena voi olla poliittisen, sotilaallisen tai taloudellisen hyödyn tavoitteleminen. APT hyökkäykset ovat usein vaikeita

tunnistaa ja havaita, jonka voi nähdä jo siitä, että useat APT-toimijat ovat olleet jopa vuosia organisaation tietoverkossa ennen niiden havaitsemista (Lehto, 2022).

Lehto esittelee artikkelissaan yleisen kyberhyökkäysmallin viiden eri hyökkäysmallin pohjalta, jotka ovat MITRE ATT&CK, Mandiant Attack Lifecycle Model, LM Cyber Kill Chain, Unified Kill Chain ja Hybrid Cyber Kill Chain (Lehto, 2022). CompTIA taas listaa yleisimpiä hyökkäysmalleja olevan Lockheed Martinin Cyber Kill Chain, The Diamond Model of Intrusion Analysis ja The Mitre ATT&CK Model (Stranger, 2020).

Lehto tunnistaa, että kaikista malleista löytyy paljon samankaltaisuuksia, joiden pohjalta voidaan luoda yksi yleinen malli, joka vastaa osittain kaikkia edellä mainittuja malleja.

Mitren ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) (MITRE, 2023) on 14-osainen malli, joka ei pelkästään listaa päällisin puolin hyökkäyksen vaiheita, vaan purkaa ne myös osakokonaisuuksiin teknisten toiminnallisuuksien osalta. Kyseinen hyökkäysmalli esittelee myös toiminnallisuuksien toteutustavan ja vaikutukset, sekä esittää keinoja niiden vaikutuksen estämiselle tai vähentämiselle. Malli esittää myös konkreettiset esimerkit APT-ryhmien tavoista toteuttaa mallissa esiteltyjä kokonaisuuksia (MITRE, 2023). Mitren mallin voi siis kuitenkin nähdä olevan jopa liian tarkka ja yksityiskohtainen, erityisesti sen teknisten esitystapojen myötä, verrattuna moniin muihin malleihin, joissa tekniselle tasolle ei mennä kovinkaan syvällisesti.

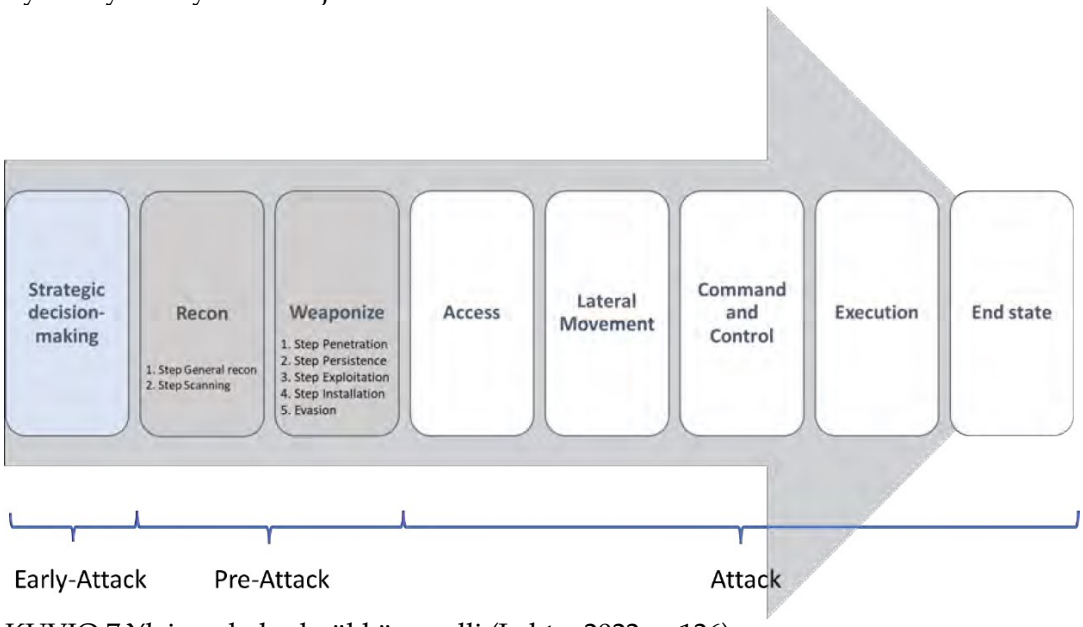
Vaihtoehtoisesti esimerkiksi Mandiantin Targeted Attack Lifecycle -malli on hieman yksinkertaisempi, sen esittäessä hyökkäys seitsemällä vaiheella (KUVIO 6) (Mandiant, 2023a)


KUVIO 6 Mandiant Targeted Attack Lifecycle (kuvaa muokattu) (Mandiant, 2023a)

Malleissa on siis niin esitystapa- kuin sisältöeroja. ATT&CK:sta ei esimerkiksi löydy yksinkertaistettua kaaviokuvaa, kuten monista muista malleista, sen ollessa lähinnä tekninen listaus tekniikoista ja taktiikoista, eikä niinkään kuvaus hyökkäysketjusta. Molemmille on kuitenkin paikkansa. ATT&CK on toimiva työkalu tekniselle asiantuntijalle, joka rakentaa käytännön keinoja toteuttaa yrityksessä vastatoimenpiteitä. Toisaalta Mandiantin malli on oiva tapa esittää esimerkiksi yrityksen toimitusjohtajalle, miten kyberhyökkäys voisi edetä. Täten sitä on hyvä käyttää korkean tason päätöksiä tehtäessä kuten säädöksien asettamisessa.

Lehdon malli (2022) lisää poikkeuksena yleisimpiin malleihin aikaisen hyökkäyksen (engl. *early-attack*) -vaiheen, joka sisältää strategisen päätöksenteon. Tämä vaihe kuvaa tilannetta, jossa esimerkiksi valtion päättäjät tekevät päätöksen kohteesta ja tavoitteista, sekä ylipäätään päättävät, että hyökkäys toteutetaan (Lehto, 2022, s. 126).

Tutkimuksen viitekehyksessä hyödynnetään Lehdon yleistä kyberhyökkäysmallia, joka on esitettynä alla (KUVIO 7) (Lehto, 2022, s. 126), sen yleisen käytettävyyden ja aikaisen hyökkäyksen vaiheen takia. Hyökkäyspintaan ja uhkille altistumiseen liittyen on yrityksen löydettävä ja tunnistettava yrityksensä koko hyökkäyspinta ja tätä myöten myös mahdolliset haavoittuvuudet yleisen kyberhyökkäysmallin jokaisessa vaiheessa.




KUVIO 7 Yleinen kyberhyökkäysmalli (Lehto, 2022, s. 126)

Jo hyökkäysmallin aikaisen hyökkäyksen -vaiheessa yrityksen tulee strategisessa päätöksenteossaan huomioida, miten hyökkääjä kykenee tarkastelemaan yritystä. Minkälaista kuvaa yritys antaa itsestään passiivisesti? Mitä tietoa hyökkääjä kykenee saamaan yrityksestä jo ennen kuin mitään konkreettisia hyökkäystoimia on käynnistetty? Onko yrityksestä valunut tietoja kolmannen osapuolen sivustoille, joita yritys ei tällä hetkellä valvo? Onko julkisessa palvelussa olevaan versionhallintaan ladattu vahingossa salaisia tietoja?

## 4.4 Uhkatoimijaprofiilit

Hyökkäysmallin tunnistamisen lisäksi yrityksen uhka-alttiuden hallinnassa on tunnistettava mahdolliset uhkatoimijat. Esimerkiksi valtion rahoittamilla hakkeriryhmillä on usein huomattavasti tehokkaammat työvälineet ja keinot kuin esimerkiksi verkkorikollisilla tai erityisesti harrastelijahakkerilla, jolla lähtökohtana hyökkäykselle on lähinnä mielenkiinto ja “seikkailun halu”. On tietysti suositeltavaa pyrkiä parhaaseen mahdolliseen tietoturvaan, mutta kuten on tunnistettu Raggadin teoksessa, ei matalan kustannustason tuotetta kannata turvata liian kalliilla toiminnallisuuksilla, sillä tällöin kyseinen tuote ei yritykselle tuota mitään (Raggad, 2010, s. 302–306). Turvallisuusjärjestelmä tulee suhteuttaa suojeltavaan kohteeseen.

Yritys voi jopa ajatella, että "kunhan omat järjestelmät ovat paremmin turvattu kuin naapurilla, niin rikollinen ei todennäköisesti murtaudu meille". Kuitenkin verkossa selkeitä naapureita ei ole siinä mielessä, kuten naapurustossa, jossa murtovarkaat saattavat katsoa kohteekseen mieluummin naapuriasunnon, jossa ei ole valvontalaitteistoja. Analogia on kuitenkin osittain kestävä myös kybermaailmassa. On myös huomioitava, että hyökkääjät voivat hyödyntää automatisoituja hyökkäyskeinoja, jotka eivät erottele kohdettaan, vaan valitsevat kohteensa massamaisesti ja summittaisesti.

Normaalielämässä saattaa huomata, että edullisen rivitaloasunnon pihassa ei välttämättä näy korkeita aitoja tai valvontakameroita samoissa määrin kuin rantaviivan läheisyydessä sijaitsevassa miljoonan arvoisessa omakotitalossa. Samalla tavalla voi todeta, että aloitteleva startup-yritys kokee todennäköisesti vähemmän korkean profiilin hyökkäyksiä, verrattuna miljardien arvoiseen yritykseen, pelkästään jo sen takia, että suuriresurssisten rikollisten motivaatio kohdistuu korkean profiilin toimijoihin. Tähän on kuitenkin poikkeuksia kuten seuraavaksi esiteltävissä uhkatoimijoissa voi nähdä.

Uhkatoimijaprofiileja listataan vaihtelevasti lähteestä riippuen. Kuitenkin keskeiset toimijat ovat poikkeuksetta esillä kaikissa artikkeleissa ja tutkimuksissa. Ablon (2018) listaa kyberrikolliset, valtiolliset toimijat, haktivistit ja kyberterroristit. Näiden lisäksi IBM listaa vielä jännityksen etsijät (muissa lähteissä käytetään myös termiä *script kiddie*, joka kääntyy suomeksi esimerkiksi koodipojuksi tai amatöörihakkeriksi) sekä sisäiset uhkatoimijat (engl. *Insider threat*) (IBM, 2023a).

**Kyberrikollisten** pyrkimyksenä on tavoitella taloudellista etua muun muassa kalasteluhuijauksilla ja kiristyshaittaohjelmilla (IBM, 2023a; Ablon, 2018). Kyberrikolliset myyvät ja ostavat valmiita haittaohjelmia pimeillä markkinoilla, joka tarkoittaa sitä, ettei välttämättä haittaohjelman kehittäjä, tilaaja ja käyttäjä ole edes sama toimija. Varastettu data voi olla puhtaasti rahaa, henkilötietoja tai yrityssalaisuuksia, joita rikolliset myyvät markkinoilla ja täten saavat itselleen taloudellista hyötyä. Kyberrikolliset kohdistavat toimiaan yrityksiin kuten pankkeihin, mutta myös yksittäisiin henkilöihin, esimerkiksi hankkien arkaluontoista materiaalia tai taloudellista hyötyä identiteettivarkausten tai laittomasti hankittujen luottokorttitietojen kautta (IBM, 2023a; Ablon, 2018).

Esimerkkinä tällaisesta ryhmästä on Revil Group, joka vuoden 2021 ensimmäisellä puolikkaalla vastasi 25 prosentista kiristyshaittaohjelmahyökkäyksiä (ThreatCop, 2021). Ryhmän kohteeksi joutui esimerkiksi maailman suurin lihanprosessointiyritys JBS sekä Taiwanilainen elektroniikka- ja tietokonevalmistaja Acer.

**Valtiolliset ja valtion tukemat toimijat** pyrkivät keräämään turvaluokiteltua ja arkaluontoista tietoa tai häiritsemään kohdevaltion hallintoa ja kriittistä infrastruktuuria (Ablon, 2018). Tämänkaltaisilla ryhmillä on usein takanaan suuri taloudellinen tuki valtiolta, josta syystä valtiollinen hakkeriryhmä on usein hankala tunnistaa tai sen toimintaa estää. Erona kyberrikollisiin on se, miten tietoa kerätään usein vain omaa jatkokäyttöä varten. Hyökkäysten tarkoituksena on

saavuttaa esimerkiksi poliittista hyötyä, vaikkapa vaikuttamalla kohdemaan vaaleihin (MITRE, 2017).

Esimerkiksi Sandworm on Venäläinen tuhoisa valtion tukema hakkeriryhmä, joka on ollut vastuussa useista tuhoisista hyökkäyksistä vuosina 2015–2019 (MITRE, 2017). Osan näiden hyökkäysten tavoitteina on ollut aiheuttaa tuhoa fyysisessä maailmassa esimerkiksi katkaisemalla sähköt.

On kuitenkin mahdollista, että taloudellista hyötyä tavoitellaan jatkotoiminnan mahdollistamiseksi. Esimerkiksi pohjoiskorealainen Lazarus (APT 38) on tehnyt kyberhyökkäyksiä valtion kassan kartuttamiseksi (Rapid7, 2023).

**Haktivistit** ovat hakkereita, jotka pyrkivät ajamaan omaa poliittista tai sosiaalista ideologiaansa eteenpäin, ottaen kohteekseen yrityksiä ja julkisuuden henkilöitä ja vuotaen tietoja näistä sananvapauden nimissä (Ablon, 2018). Hyökkäyskeinona voi olla myös palvelunestohyökkäys palveluun, jonka alasajo mielletään oikeelliseksi ja hyväksi asiaksi. Sananvapauden lisäksi myös tasa-arvoisuuden edistäminen ovat muun muassa Anonymous -haktivistiryhmän motivaation lähteitä (Coleman, 2014, s. 75).

**Kyberterroristeilla** on samat päämäärät kuin konventionaalisella terrorismilla: pelottelu, fyysinen vahinko sekä yleisöön ja poliittiseen päätöksentekoon vaikuttaminen (Ablon, 2018). Terroristien toiminnot näyttäytyvät helposti haktivismina, ja kyberympäristön käyttö onkin pitkälti rekrytointia, tiedonkeräämistä ja rahantekoa varten. Kyberterroristilla kuitenkin tarkoitetaan sellaista ryhmää, joka toteuttaa kyberhyökkäyksiä, eikä pelkästään terroristia, joka käyttää verkkoa apuvälineenä konventionaalisen terrorismin tukena.

Kyberterroristien tavoitteet ovat suhteellisen lähellä valtiollisten toimijoiden tavoitteita, mutta keinovalikoima on huomattavasti pienempi valtiollisen rahallisen tuen puuttuessa. Kyberterroristiryhmä kuitenkin voi olla samanaikaisesti valtion taloudellisesti tukema ryhmä (IBM, 2023a).

**Amatöörihakkerit** eli niin sanotut script kiddiet ovat toimijoita, jotka eivät välttämättä ymmärrä täysin tekojensa seurauksia (IBM, 2023a). Motivaationa hyökkäykselle voi olla mielenkiinto oppimiseen tai pelkkä huvin tavoittelu. Heidän tarkoituksenaan ei välttämättä ole aiheuttaa tuhoa tai vahinkoa, vaan pelkkä järjestelmään pääsy voi riittää heille. Termi "script kiddie" juontaa juurensa siitä, että kyseiset toimijat eivät ole teknisesti järin osaavia, jonka takia he käyttävät valmiita ohjelmia, työkaluja ja koodeja (engl. *Script*) hyökkäyksissään (IBM, 2023a).

Amatöörihakkerit saattavat vajaan ymmärryksensä myötä aiheuttaa vahingossa tuhoa kohteelleen käyttäessään liian aggressiivisia työkaluja, joka saattaa muokata tai poistaa kohteen tietoja haavoittuvuuden löydettyään (Abricto Security, 2020). Amatöörihakkereille on ominaista niiden toiminnan läpinäkyvyys ja selkeys. Tämän takia he usein jäävätkin suhteellisen nopeasti kiinni (Raggad, 2010, s. 436).

**Sisäinen uhka** on esitetty muun muassa Raggadin teoksessa (2010, s. 84, 436) sekä IBM:n listauksessa (IBM, 2023a). Sisäinen uhka voi olla tahallinen tai vahingollinen toimija. Tästä syystä sisäistä uhkaa ei pitäisi pelkästään mieltää yhdeksi uhkatoimijaksi muiden yllä esitettyjen rinnalla, vaan tiedostaa, että

teknisesti osaamattomampikin työntekijä voi olla sisäinen uhka yrityksen kyberturvallisuudelle.

Vahingollinen toiminta on esimerkiksi palomuurin porttien avaamista tai haitallisen ohjelman asentamista tietämättömyyteensä vedoten. Tahallinen toimija toisaalta voi tehdä täysin samat toimenpiteet. Vaarallisen tahallisesta sisäisestä uhkasta tekee sen mahdollisesti korkea ymmärrys sisäisen verkon rakenteesta, joka helpottaa hyökkäyksen toteuttamista (Raggad, 2010, s. 436).

Raggad (2010, s. 436) toteaa, että 80 % hakkereista ovat sisäisiä uhkia ja loput ovat ulkoisia toimijoita, joita yllä esiteltiin. On siis tärkeä ymmärtää kaikki mahdolliset kyberuhkatoimijat ja näiden tarkoitusperät ja toimintatavat yrityksen kyberturvallisuutta suunniteltaessa. Lisäksi prosessia tukee merkittävästi, jos yritys tunnistaa, miten eri toimijoiden motivaatiot voivat ilmetä kyseisen yrityksen toimintaan liittyen.

## 4.5 Hyökkäyspinnan hallinnan sovellukset

Hyökkäyspinnan alaluvun pohjalta kyseinen termi käsitetään siis usein enemmänkin trendinä tai suunnitteluprosessin osana, kuin valmiina sovelluksena, joka automaattisesti ilmoittaisi hyökkäyspinnan löydöksistä ja ehdottaisi näihin korjaustoimenpiteitä. Haavoittuvuusskannerit kuten Nessus (2023) tai OpenVAS (Greenbone, 2023) ovat jo sellaisenaan hyökkäyspinnan hallintaan liittyviä työkaluja. Nessus kuvaa sivuillaan lisäävänsä näkyvyyttä internetiä kohti näkyvään hyökkäyspintaan. Haavoittuvuusskanneri on kuitenkin siis lopulta vain sovellus, joka tarkistaa tunnistettujen sovellusten tietoturva-aukkoja kuten virheellisiä konfiguraatioita tai tarpeettomasti avoimia portteja, jotka altistavat verkon tietoturvauhkille.

Tämän tutkimuksen kehyksessä haavoittuvuusskanneria voisi siis luonnehtia hyökkäyspinnan valvonnan ja hallinnan sovellukseksi, mutta alkuperäiseen ongelmaan, eli hyökkäyspinnan minimoimiseen ja tuntemattomien sekä näkymättömien asioiden havainnointiin kuten varjo-IT:hen, vahingossa julkiseksi näkyviin jääneeseen lähdekoodiin, kalasteluyrityksiin tai tuotantoketjuhaavoittuvuuksiin ne eivät vastaa.

Hyökkäyspinnan ja uhka-alttiuden hallinnan sovelluksen tulisi siis kyetä vastaamaan useaan eri tasoiseen ja tyyppiseen uhkaan ja riskiin, jotka eivät välttämättä ole edes havaittavissa yrityksen sisältä käsin tehdyllä ulkoisen teknisen hyökkäyspinnan tarkastelulla. Pohjimmiltaan hyökkäyspintaa hallitsevan sovelluksen tulisi kyetä tunnistamaan miten yrityksen yksittäiset käyttäjät toimivat, jotta kalasteluun liittyvä hyökkäyspinta olisi tunnistettava. Mahdollisen hyökkäyspintaskannerin tulisi myös valvoa julkista internetiä hyvin laajalti, tunnistaen esimerkiksi pilvipalveluihin vahingossa julkisesti jääneitä hyökkäyksen mahdollistavia tietoja, kuten salasanoja tai verkko-osoitteita. Avainideana tämänkaltaisen sovelluksen tulisi siis olla hyvinkin holistinen.

Skybox Securityn artikkelissa (Friedman, 2016) esitettiin visuaalinen esimerkki hyökkäyspinnan hallinnan sovelluksesta Skybox Horizon –sovelluksen

muodossa. Artikkelin pohjaavana ajatuksena oli se, että suuressa yrityksessä hyökkäyspinta on niin suuri, ettei IT-osasto ehdi eikä kykene priorisoimaan ja hallinnoimaan kaikkia uhkia. Sovelluksen tulisi sisältää alttiuden indikaattoreita (engl. *Indicator of exposure*) ja vaarantumisen indikaattoreita (engl. *Indicator of compromise*) sidottuna niiden maantieteellisiin ja verkkotopologisiin sijainteihinsa.

Gartner (Schneider, ym., 2022) kuvaa kokonaisvaltaisen hyökkäyspinnan hallinnan vaativan seuraavia kolmea nousevan teknologiakentän innovaatiota: Kyberassettien hyökkäyspinnan hallinta (engl. *Cyber Asset Attack Surface Management CAASM*), Ulkoisen hyökkäyspinnan hallinta (engl. *External Attack Surface Management EASM*) ja Digitaalisen riskin turvaamisen palvelut (engl. *Digital Risk Protection Services DRPS)*. Artikkeli tarjoaa myös lyhyen listauksen yrityksistä, jotka tarjoavat hyökkäyspinta-analyysiä tuottavia palveluita.

CAASM:n toiminnan keskiössä on sen kyky tunnistaa ja ratkoa ongelmia, jotka kohdistuvat sekä sisäisiin, että ulkoisiin haavoittuvuuksiin. Se ylläpitää tietoa yrityksen tieto-omaisuudesta vähentäen manuaalisen käsittelyn tarvetta. Lisäksi sovelluksen tulee tunnistaa haavoittuvuuksien laatu ja laajuus sekä ymmärtää aukot sovellusten tietoturvassa (Schneider, ym., 2022). Kyseessä on siis haavoittuvuusskanneriin verrattava työkalu. Erona haavoittuvuusskanneriin on kuitenkin se, että CAASM on huomattavasti laajempi sekä sen tulisi kyetä tunnistamaan myös puutteita tietoturvassa eikä pelkkiä sovellusteknisiä haavoittuvuuksia. Lisäksi CAASM:n tarkoituksena on olla ohjelmistorajapintojen integraatiota hyödyntämällä toteutettu niin, että sillä voidaan valvoa yrityksen kaikkea teknologista omaisuutta reaaliaikaisesti.

EASM on kokoelma prosesseja, teknologioita ja palveluita, jotka havainnoivat ulkoisia yrityksen sovelluksia, yrittäen tunnistaa näistä poikkeamia, jotka voivat aiheuttaa uhkan yritykselle (Schneider, ym., 2022). Sovelluksen tulisi tunnistaa tietysti yrityksen omassa hallussaan olevat palvelut, järjestelmät ja sovellukset, mutta tämän lisäksi myös kolmannen osapuolen palveluissa olevat haavoittuvaiset tiedot, tai sellainen informaatio, joka voi mahdollistaa hyökkäyksen yritystä kohtaan. Tällaisia tietoja voisi olla esimerkiksi salasanat avoimen lähdekoodin säilytyspaikassa (engl. *repository*). Shodan (2023) on esimerkki yksittäisestä tällaisesta järjestelmästä. Se skannaa aktiivisesti koko IP-osoiteavaruutta ja tunnistaa esimerkiksi julkiseksi jääneitä valvontakameroita ja muita verkkolaitteita. Normaali haavoittuvuusskanneri kykenee tunnistamaan haavoittuvuuksia yrityksen tiedossa olevasta hyökkäyspinnasta, mutta Shodanin kaltaisella sovelluksella kyetään osin tunnistamaan myös tunnistamattomat sovellukset.

DRPS on palvelu, jolla julkisesta internetistä pyritään tunnistamaan sosiaalisen median kaappauksia tai brändin varastamista, yritykseen kohdistuvia kalasteluyrityksiä tai arkaluontoisen materiaalin vuotamista julkisuuteen. DRPS:n ytimessä on ajatus siitä, että se tarkastelee yrityksen brändiin ja julkisuuskuvaan kohdistuvia ilmiöitä julkisesta verkosta. (Hakluke, 2023; Schneider, ym., 2022)

Tarkastellaan lyhyesti neljää hyökkäyspinnan hallintaan keskittyvää yritystä. Group-IB:n Attack Surface Management SaaS-ratkaisu (Group-IB, 2023) toteuttaa pitkälti kaiken yllä kuvatun. Sovelluksen käyttämät teknologiat ovat

yrityksen patentoimia, joten kyseessä ei ole erilaisten haavoittuvuusskanneri-integraatioiden integraatio. Sovellus muun muassa skannaa koko IPv4-avaruutta tunnistaen yrityksen alttiita sertifikaatteja, domain-nimiä ja pilvivarantoja (engl. *bucket storage*). Tämän lisäksi sovelluksesta löytyy perinteisen haavoittuvuusskannerin toiminnot kuten haavoittuvuuksien löytämisen, vuotaneiden salasanojen ja heikkojen konfiguraatioiden tunnistamisen. Sovelluksen hälytykset ehdottavat korjaavia toimenpiteitä suoraan käyttöliittymässä tai tarvittaessa ne voidaan liittää rajapinnan avulla muihin tiketöinti- tai SIEM-järjestelmiin (Group-IB, 2023).

Argos Platform (Cyberint, 2023) on vastaava sovellus, joka mainostaa hakevansa tietoa myös pimeästä verkosta (engl. *dark web*). Lisäksi palvelu monitoroi sosiaalista mediaa turvatakseen yrityksen julkisuuskuvaa. Sovelluksesta löytyy myös ohjelmistorajapinta ja lisäosa verkkoselaimeen, joka turvaa yrityksen käyttäjiä.

Bitsight (2023) kuvailee hyökkäyspinnan analytiikan ratkaisunsa olevan osa laajempaa kokonaisuutta, jota he kuvailevat ”turvallisuuden tehokkuuden hallinnaksi”. Palvelu lupaa perinteisen haavoittuvuusskannerin toiminnallisuuksien lisäksi löytävänsä myös varjo-IT:n sekä hallinnoi yrityksen digitaalista jalanjälkeä. Bitsight tarjoaa myös yritykselle ilmaisena kokeiluna erikseen tehtyä raporttia (Bitsight, 2023).

Kyberturvallisuuskeskuksen (2023) luoma Hyöky on kansallinen hyökkäyspintakartoitus kunnille. Verkkosivu ei avaa ratkaisun teknisiä periaatteita tai käyttöliittymää yhtään, mutta sivusto kuvaa sen olevan helppokäyttöinen ja maksuton palvelu. Kyseessä on siis mitä luultavammin ulkoisesti tarjottava palvelu, joka analysoi julkisessa verkossa kunnan hyökkäyspintaa, tuottaen näin kunnalle raportin ja ymmärryksen omasta tietoturvansa tasosta hyökkääjän silmin nähtynä.

Näiden alustojen ja sovelluksen lisäksi verkosta löytyy suuri määrä vastaavia palveluita kuten hyvin laaja alusta SOCRadar (2023) ja pelkästään CAASM-toiminnallisuuteen perustuva Axonius (2023). Osa niistä tarjoaa valmista sovellusratkaisua ja osa ovat enemmänkin tilauspohjaisia palveluita, joissa yritykselle maksetaan raportin tuottamisesta. Tällöin tilaavan yrityksen ei itse tarvitse itse asentaa uusia sovelluksia ja opetella niiden käyttöä, mutta hyökkäyspinnan hallinta ei myöskään ole tällöin automatisoitua ja reaaliaikaista. Loppukädessä ihmisen toteuttama hyökkäyssimulaatio tai penetraatiotestaus ei ole mitenkään uusi juttu, mutta se mitä Gartner kuvaakin EASM-, CAASM- ja DRPS-sovelluksista on juuri niiden automaattisuus, jatkuvuus, reaaliaikaisuus ja holistisuus. Ajoittainen tilaustyönä tehty hyökkäyspintakartoitus on pienelle yritykselle todennäköisesti lopulta järkevämpi ratkaisu rahallisesti, kuin uuden sovelluksen ja siihen liittyvän henkilöstön integroiminen yrityksen nykyiseen kyberturvallisuuden hallintaprosessiin.

## 4.6 Kyberuhkatiedustelu- ja metsästys

Lähtökohtaisesti edellisten alalukujen pohjalta voi tunnistaa, että onnistunut uhkienhallinta vaatii ymmärryksen omaan hyökkäyspintaan kohdistuvista hyökkääjistä. Tutkimuksessa tunnistettiin tarve avata lyhyesti kyberuhkatiedustelun merkitystä hyökkäyspinnan ja uhka-alttiuden hallinnassa. Lehdon hyökkäysmallissa kuvatun aikaisen hyökkäyksen vaiheen merkitys kasvaa, käsiteltäessä edellisessä alaluvussa kuvattuja hyökkäyspinnan hallinnan sovellusten määrittämistä yrityksen käyttöön. Strateginen päätöksenteko vaikuttaa osaltaan jo siihen, miten ja minkälaiset uhkat kohdistavat hyökkäyksensä kyseiseen yritykseen.

Wang (2022) kuvasi laajassa kirjallisuuskatsauksessaan kyberuhkametsästyksen (engl. *Cyber Threat Hunting)* olevan jo vuonna 2016 kasvava trendi, jossa on pyrkimyksenä kehittää proaktiivisesti puolustuskeinoja kyberuhkia vastaan. Uhkien tunnistamisella tarkoitetaan tilannetta, jossa jo vaikuttanut uhka kyetään havaitsemaan (Miazi, ym. 2017, s. 3).

Kyberuhkatiedustelu (engl. *Cyber Threat Intelligence*) on kyberuhkametsästykseen liitetty analyyttinen prosessi, jossa kootaan laaja-alaisesti hyökkäys- ja uhkatietoja kuten tunkeutumisenhavaitsemisjärjestelmien ja hunajapurkkien hälytyksiä ja lokitietoja, joiden pohjalta voidaan tuottaa analysoitua tietoa hyökkääjien toiminnasta (Miazi, ym., 2017). Uhkametsästykseen liittyvät taidot käsittävät data-analyysiin ja analytiikkaan liittyvän osaamisen lisäksi myös koodin analysointia, penetraatiotestausta ja haavoittuvuusanalyysiä (Miazi, ym., 2017). 2017 75 % tutkimukseen vastanneista yrityksistä totesivat kyberuhkametsästyksen vaikuttaneen toimenpiteisiin, joilla pienennettiin yrityksen hyökkäyspintaa.

Gao ym. (2021) pohti tutkimuksessaan avointen lähteiden uhkatiedustelun vaativan tehokasta koneoppivaa kielimallia, joka kykenee poimimaan ajankohtaisimpia tietoja esimerkiksi blogeista ja turvallisuusalan nettisivuilta. Suurena ongelmana muodostuukin suuren datamäärän käsittely ja koneoppivan mallin tarkkuus.

SANS:n teettämässä uhkatiedusteluun liittyvässä kyselytutkimuksessa (Brown & Lee, 2019, s. 5) vastaajista 18 % esitti tärkeimmäksi digitaalisen jalanjäljen tai hyökkäyspinnan tunnistamisen, kun 40,6 % laittoi hyökkäyksen indikaattorin (engl. *Indicator of Compromise*). Hyökkäyspinnan hallintaa ei siis ainakaan vuonna 2019 asetettu kovin korkeaan arvoon verrattaessa muita vaikuttavia tekijöitä. Samassa tutkimuksessa tunnistettiin, että monet yritykset keräävät tietoa, jotka tuottavat proaktiivisesti havaintoja mahdollisista uhkista. Tietojen keräämisen prosessia peilaten, on se osin epäjärjestelmällistä, josta syystä tietoaukkoja syntyy, eikä yritys välttämättä itse tunnista näitä syntyneitä turvallisuusaukkoja.

Brown & Lee (2019, s. 11) toteavatkin lopulta uhkatiedustelun kypsyneen muutamien edellisten vuosien aikana. Sen kautta kerätty tieto ei enää pelkästään tunnista merkkejä hyökkäyksistä, vaan tämän lisäksi sen avulla on mahdollisuus kehittää ymmärrystä tekniikoista, taktiikoista ja prosesseista (engl. *Techniques,*

*tactics and procedures TTP*), uhkien käyttäytymisestä, hyökkäyspinnasta ja strategisesta arvioinnista ja päätöksenteosta.

37 % kyselyyn vastanneista toteuttivat uhkatiedustelun kokonaisuudessaan sisäisesti, kun toisaalta 54 % hyödynsivät ulkoisia ja sisäisiä resursseja (Brown & Lee, 2019, s. 8). Yrityksen pohtiessa hyökkäyspintansa ymmärryksen lisäämistä ja jatkuvaa uhkille altistumisen hallintaa, on tarpeen huomioida yrityksen kyky toteuttaa uhkatiedustelutoimintaa sisäisesti niin henkilöstö-, kuin muidenkin resurssien suhteen.

Uhkatiedustelun kautta hyökkäyspinnan hallintaa voi siis kehittää tunnistamalla todennäköisimpiä, tuntemattomia tai kehittyviä uhkia, joiden perusteella hyökkäyspintaa päätettäisiin pienentää. Tämän kuitenkin tunnistetaan vaativan hyvin laajaa osaamista, jossa automaatio ja koneoppivat mallit ovat keskiössä. Onnistunut ja oikein toteutettu kyberuhkatiedustelu tuottaa lähtökohtaisesti kokonaisvaltaista kyberturvallisuuden tilannekuvaa yritykselle, jossa sillä on vaikutusta niin hyökkäyspinnan hallinnalle, jatkuvalle uhka-altistumisen hallinnalle, riskien hallinnalle, kyberturvallisuusosaamiselle ja priorisointitoimille niin budjetin, kuin tietoturvankin osalta. Uhkien metsästystä voidaan toteuttaa yrityksen itsensä toimesta, mutta myös sen ulkoistaminen mahdollistaa pienemmille yrityksille kattavan uhkien hallinnan.

## 4.7 Yhteenveto

Riskienhallinnassa uhkien tunnistaminen esiintyy yhtenä tärkeänä osa-alueena, mutta suurimpana ongelmana koko prosessissa on se, miten tuntemattoman tai näkymättömän uhkan pystyy tunnistamaan ja lopulta torjumaan. Kyberuhkatiedustelu, jatkuvan uhka-alttiuden hallinnan prosessi sekä uhkatoimijoiden ja uhkamallien osaaminen on keskiössä siinä, miten tietoturvan ammattilaiset tulkitsevat hyökkääjiä ja kykenevät ennustamaan mahdollisia tulevaisuuden trendejä uusissa ja tuntemattomissa hyökkäyskeinoissa. Onnistunut kyberuhkatiedustelu mahdollistaa hyökkäyspinnan hallinnan jo Gartnerin artikkelien kuvailemalla tavalla.

Uhkatoimijat eritellään hieman eri tavalla riippuen kirjoittajasta, mutta eri uhkatoimijoiden kokonaisvaltainen ymmärtäminen mahdollistaa oman hyökkäyspinnan tulkinnan riittävän monipuolisesti. Yritykseen voi kohdistua esimerkiksi rikollinen tai aktivisti, joka ei välttämättä ole yrityksen ulkopuolelta tullut uhka. Toisaalta hyökkäystoimijoiden lisäksi tulee tunnistaa, että osa riskeistä voi muodostua vahinkojen ja erehdyksien kautta. Tästä syystä uhkien tunnistamisen tulee olla sisäistä sekä ulkoista. Lisäksi sen tulee myös kohdistua ei-yrityksen omistamiin palveluihin kuten sosiaaliseen mediaan, pimeään verkkoon ja versionhallintaan keskittyviin alustoihin. Uhkatoimijoiden käyttäytymismallien ymmärtämisellä voidaan jo osaltaan ennakoida tulevien hyökkäysten toteutustapoja.

Hyökkäysmalli on tärkeä osa uhkien tunnistamista, sillä sen avulla voidaan pilkkoa hyökkääjän toimintaa paremmin pieniin tarkasteltaviin osiin, joissa jokaisessa vaiheessa on mahdollista vaikuttaa riskin toteutumiseen. Parhaassa

tapauksessa riskin muodostumiseen voidaan vaikuttaa jo silloin, kun uhkatoimija suunnittelee hyökkäystä, eli jo ennen tiedusteluvaihetta. Tässä tärkeäksi teemaksi nousee hyökkäyspinnan ja uhkille altistumisen minimointi.

Gartnerin tutkimukset ja artikkelit kuvaavat hyökkäyspinnan hallinnan olevan uhkaorientoitunut, automatisoitu ja proaktiivinen tapa vähentää riskejä ja niiden vaikutuksia, mallin painottuessa erityisesti tuntemattomien uhkien välttämiseen ja väistämiseen.

Hyökkäyspinta on terminä kuitenkin hyvin moniulotteinen, sen tarkoittaessa usein pelkkää teknistä hyökkäyspintaa, jolloin sillä viitataan lähinnä verkkosovelluksen avoimiin portteihin ja virhekonfiguraatioihin. Hyökkäyspinnan hallinnasta puhuttaessa tulisikin sen ymmärtää sisältävän paljon laajempi kokonaisuus kuten yrityksen työntekijät ja muut ei-tekniset hyökkäysvektorit ja mahdollisia haavoittuvuuksia sisältävät elementit.

Hyökkäyspinnan mittaaminen tai analysoiminen antaa viitteitä samanlaisesta ongelmasta, jota perinteisessäkin riskienhallinnassa esiintyy, jos sitä käsitellään vain määrällisillä mittareilla. Hyökkäyspintaa kannattaakin ensisijaisesti mitata laadullisesti ja hyvin kontekstisidonnaisesti, jotta sillä kyetään saamaan todenmukaisia tuloksia.

Hyökkäyspinnan hallinnan sovelluksia kuvattiin Gartnerin artikkeleissa tulevaisuuden trendeiksi, mutta hyökkäyspinnan hallinnan ja jatkuvan uhka-alttiuden termeillä itseään markkinoivat yritykset olivat jo ennen vuotta 2024 tuottaneet vastaavia sovelluksia ja palveluita. CAASM on käytännössä haavoittuvuusskannerien ja sitä vastaavien työkalujen muodostama järjestelmä, joka kerää dataa useasta laitteesta ja palvelusta tunnistaen virheitä ja ehdottaen korjausvaihtoehtoja reaaliaikaisesti. EASM on ulkoista hyökkäyspintaa valvova sovellus, jonka tulisi tunnistaa myös esimerkiksi varjo-IT tai verkossa avoimena ohjelmakoodi, joka sisältää julkisena sellaista tietoa, jonka tulisi olla piilotettu. DRPS on palvelu tai sovellus, joka tunnistaa hyökkäyksiä, jotka eivät kohdistu suoraan yritykseen. Tällainen toiminto voi olla esimerkiksi verkkosivun kopiointi kirjautumistietojen varastamisen toivossa.

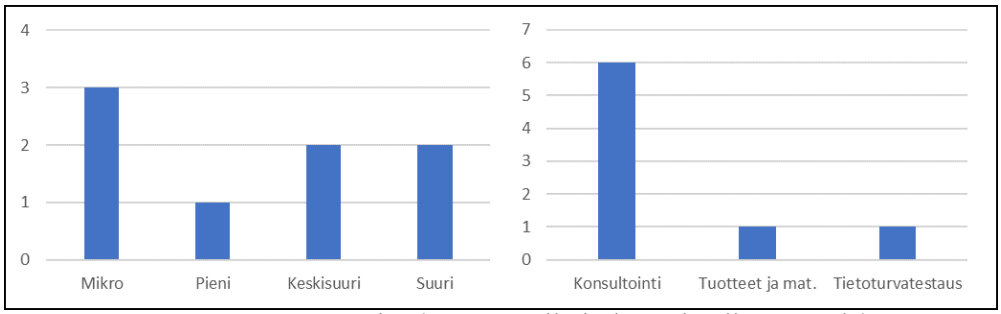
Kyberuhkatiedustelu ja uhkien metsästäminen on suhteellisen suuri kokonaisuus toimintoja, joilla pyritään ennakoimaan uhkia ja vastaamaan niihin jo osin ennen uhkien syntymistä. Tämän toiminnallisuuden merkitys on tunnistettu hyvinkin tarpeelliseksi, mutta sen vaatiessa suhteellisen paljon resursseja, on mahdollisesti pienempien yritysten vaikeaa toteuttaa sitä yrityksessä sisäisesti. Ulkoiset palveluntarjoajat kuitenkin tarjoavat palveluitaan valmiina sovelluksina sekä palvelumuotoisina tuotteina (SaaS). Tämä tietoturvaprosessien ulkoistaminen voi kuitenkin johtaa virheelliseen turvallisuuden tunteeseen, jossa yritys sinisilmäisesti luottaa ja uskoo ulkoistetun palvelun ylivertaisuuteen. Yrityksen suunnitellessa hyökkäyspinnan hallinnan sovellusten hankintaa on yrityksen pohdittava siis resurssien ja todennetun turvallisuuden tasapainoa.

# 5 TULOKSET JA ANALYYSI

## 5.1 Vastaajien taustatiedot

Kysely lähetettiin neljääntoista yritykseen, joista kahdeksalta saatiin vastaus. Alla (KUVIO 8) on kuvattu vastanneiden yritysten koko (vasemmalla) ja toimiala (oikealla). Vastaajien taustatiedot, kuten yrityksen koko ja toimiala, eivät olleet osana vastauslomaketta, vaan ne kerättiin julkisista lähteistä kuten kyseisten yritysten kotisivuilta ja vainu.io:sta (Vainu, 2024).

Yhteensä vastauksia saatiin kolmelta mikro- (37,5 %), yhdeltä pieneltä (12,5 %), kahdelta keskisuurelta (25 %) ja kahdelta suurelta yritykseltä (25 %). Yritykset jakautuivat toimialaltaan kolmeen yleistettyyn kategoriaan seuraavasti: 12,5 % tuotteet ja materiaalit (1 kpl), 12,5 % tietoturvatestaus (1 kpl) ja 75 % konsultointi (6 kpl).




KUVIO 8 Vastaajien taustatiedot (vasemmalla koko, oikealla toimiala)

Yksi vastaajista vastasi osaan kysymyksistä itse lisäämällään merkinnällä “en osaa sanoa”, joten tietyissä kysymyksissä tämän yrityksen vastaukset on jätetty analyysistä pois. Vastausten määrä kysymystä kohden on oletuksena kahdeksan. Poikkeavissa vastausmäärissä vastaajien määrä on merkitty frekvenssitaulukoissa kysymyksen perään (esim. N=7).

## 5.2 Riskienhallinnan toteutus ja varmuus hyökkäyspinnasta

Kyselyn ensimmäinen osio keräsi tietoa yrityksen riskienhallinnan toimintamallista ja prosessista sekä kohdistuneista ja tunnistetuista uhkista. Lisäksi vastauksissa tunnistetaan yritysten kokemus omasta varmuudestaan tunnistaa hyökkäyspintaansa.

Viisi vastaajaa (62,5 %) ilmoitti käyttävänsä ISO-sertifointeja kuten 27001:tä ja 31000:aa riskienhallinnan tukena. Yksittäinen vastaaja mainitsi myös käyttävänsä IRAM2:ta (Information Risk Assessment Methodology). Yksi mikroyritys totesi myös, etteivät noudata mitään erityistä standardia.

62,5 % yrityksistä totesivat olevansa täysin samaa mieltä teknisen hyökkäyspintansa merkittävästä kasvusta viimeisen viiden vuoden aikana. Toisaalta vastausten keskiarvo oli kuitenkin 3,25, sillä yksittäiset pienet ja mikroyritykset ovat olleet väittämästä täysin tai osittain eri mieltä. Yksi suurista yrityksistä mainitsi palvelujen digitalisoinnin ja pilvipalvelujen käytön kasvun kasvattaneen hyökkäyspintaa. Lisäksi suuren henkilöstömäärän koettiin kasvattavan riskiä käyttäjälähtöisiin virheisiin. Täten on tarpeen varmistaa tuon henkilöstön osaaminen ja toteuttaa asianmukainen reagointi poikkeamien varalle. Tämän kysymyksen vastaukset ovat hyvin linjassa Randorin raportin (2022) kanssa. Taulukossa 1 on esitetty ensimmäisten kysymysten frekvenssit.

TAULUKKO 1 Hyökkäyspinnan kasvun ja tietoisuuden kysymysten frekvenssit

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 2. Yrityksemme tekninen hyökkäyspinta on kasvanut merkittävästi viimeisen 5 vuoden aikana | 12,5 | 12,5 | 12,5 | 62,5 |
| 6. Koemme yrityksessä olevamme täysin tietoisia koko hyökkäyspinnastamme (N=7) | 0,0 | 0,0 | 85,7 | 14,3 |

Vastauksissa näkyi, että suuremmat yritykset kokivat poikkeuksetta hyökkäyspintansa kasvaneen, kun taas keskisuurten ja mikroyritysten vastauksissa oli enemmän hajontaa.

Vastanneisiin yrityksiin on kohdistunut hyvin vähän tietoturvapoikkeamia. Keskiarvo viiden vuoden vuosittaiselle keskiarvolle on vain 1,08 (N=5). Kolme vastaajista ilmoitti kohdanneensa muun muassa yhden APT-hyökkäyksen, tilimurtoja, haittaohjelmatartunnan, verkkosivun hakkeroinnin ja yhden nollapäivähaavoittuvuuden hyväksikäytön. Vastauksena todettiin myös se, että on huomioitava, ettei yritys, joka käyttää SaaS-palveluja ole täysin vastuussa palvelunsa tietoturvasta, vaan se kuuluu palveluntarjoajalle. Yksi pienyritys totesikin vastauksessaan tämän huomion lisäksi myös sen, että omien ”havaittujen tietoturvapoikkeamien määrä on 0. Se montako oikeasti on tapahtunut, on eri asia.” (Vastaaja 2)

Varjo-IT:tä on tunnistettu 37,5 prosentissa, eli kolmessa, kyselyyn vastanneista yrityksistä. Esille nostettiin se, miten virallista Sharepoint-

pilvitallennustilaa vältetään, käyttääkseen vanhaa Google Driveä. Lisäksi laajat admin-oikeudet johtavat osaltaan varjo-IT:n muodostumiseen. Suuri yritys kuitenkin totesi, että heillä on varjo-IT:tä, vaikkakin ohjelmistojen hallinnointi on toteutettu keskitetysti ja hankintaprosessit ovat selkeitä. Prosesseja varjo-IT:n rajoittamiselle siis on olemassa, mutta ongelma ilmeneekin siinä, miten niitä prosesseja ja ohjeistuksia noudatetaan ja kyetään valvomaan yrityksissä. Alla (TAULUKKO 2) on esitetty näiden kysymysten vastausfrekvenssit.

TAULUKKO 2 Varjo-IT-kysymysten vastausten frekvenssit

| | Ei | Kyllä |
|---|---|---|
| 4. Yritykseemme on kohdistunut kyberpoikkeama aiemmin täysin tuntematonta hyökkäyspintaa pitkin (N=7) | 85,7 | 14,3 |
| 5. Yrityksessämme on tunnistettu varjo-IT:tä | 62,5 | 37,5 |

Yritykset kokevat pääsääntöisesti olevansa varmoja hyökkäyspinnastaan: 85,7 % ollessa osin samaa mieltä ja 14,3 % täysin samaa mieltä väittämästä (TAULUKKO 2TAULUKKO 2, kysymys 6). Yksi vastaajista kuitenkin kritisoi yleisesti yritysten todellista käsitystä omasta hyökkäyspinnasta:

> ”Omakohtaisen kokemuksen kautta yritykset usein liioittelevat oman tilannetietoisuutensa. Samoin viitekehysten käyttö on kirjavaa. Osalle viitekehys merkitsee rastia tarkistuslistaan, vaikka todellisuudessa viitekehystä ei ole viety aidosti käytäntöön.” (Vastaaja 4)

Toinen vastaajista tunnisti osittain saman ilmiön huomauttaessaan, että täyden tietoisuuden saaminen voi olla vaativaa:

> ”Hyökkäyspinta-ala muuttuu jatkuvasti. Vaikka teemme paljon toimia tämän hallitsemiseen niin varmuutta ”täydestä tietoisuudesta” on hankala saada.” (Vastaaja 6)

Yhteenvetona ensimmäisen kategorian kysymyksissä näkyy, että vastauksissa esiintyy suhteellisen korkea itsevarmuus omaan prosessiin, oli se standardin tai viitekehyksen mukainen tai ei. Tätä tukee myös suhteellisen pieni määrä tunnistettuja kyberpoikkeamia. Suurissa yrityksissä hyökkäyspinnan kasvu on näkynyt selkeimmin. Varjo-IT on suhteellisen yleinen ongelma aikaisempien tutkimusten valossa, ja on mahdollista, että vaikka vastaaja ilmoittaa, ettei varjo-IT:tä ole tunnistettu, ei se tarkoita sitä, etteikö sellaista olisi olemassa.

## 5.3 Perinteisen riskienhallinnan mieltäminen

Sillä hyökkäyspinta on terminä moninainen eikä sille ole pelkästään yhtä kuvausta, pyrittiin toisen kategorian kysymyksillä tunnistamaan vastaajien käsitykset termistöstä hyökkäyspintaan liittyen. Lisäksi havainnoitiin miten suomalaisessa yrityskentässä Gartnerin tutkimusten kyselyiden tulokset ovat peilattavissa ja toisinnettavissa; Eli onko näiden tutkimusten kritiikki perinteisen riskienhallinnan epäselvyyttä kohtaan tarpeellisesta? Ja jos näin on, onko tähän olemassa selkeää ratkaisua? Alla (TAULUKKO 3) on esitettynä toisen kategorian kysymysten vastausten frekvenssit prosentteina.

TAULUKKO 3 Riskienhallinnan ja hyökkäyspinnan mieltämisen kysymysten frekvenssit

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 7. ”Hyökkäyspinnan pienentämisellä” voi mielestäni tarkoittaa vaikkapa henkilöstön vähentämistä | 0,0 | 25,0 | 62,5 | 12,5 |
| 8. Jatkuva hyökkäyspinnan kasvu haittaa merkittävästi kyberturvallisuuden riskienhallinnan onnistunutta toteuttamista. | 0,0 | 50,0 | 37,5 | 12,5 |
| 9. Uskon, että riskienhallintaprosessia läpikäydessämme, yritykseemme kohdistuvia mahdollisia uhkia jää varmasti tunnistamatta. | 0,0 | 37,5 | 62,5 | 0,0 |
| 10. Riskienhallinnan prosessi tuottaa mielestäni vain suuntaa antavan kuvan yritykseen kohdistuvista uhkista ja riskeistä | 0,0 | 25,0 | 50,0 | 25,0 |
| 11. Koen perinteisten riskienhallintamallien olevan lähinnä välttämätön paha, jota säädökset ja yritysmaailma vaativat | 37,5 | 50,0 | 12,5 | 0,0 |

Kysymyksessä 7 on väittämä, jolla tarkastellaan vastaajien tapaa käsitellä hyökkäyspintaa terminä: “Hyökkäyspintaa ei sopisi mieltää pelkästään teknisinä asioina, vaan se pohjimmiltaan hyökkäyspinnan pienentämistä tapahtuu myös henkilöstöä vähentämällä”. Vastaukset ovat suhteellisen yhtäläiset: ”Täysin eri mieltä” vastauksia ei ole ja hajonta vastauksissa on pientä ($\sigma$=0,60). 62,5 % vastasi osin samaa mieltä, 25 % osin eri mieltä, ja yksi vastaajista (12,5 %) oli täysin samaa mieltä väittämän kanssa. Hyökkäyspinta terminä on siis tulkinnanvarainen, eivätkä yritykset koe, että se pelkästään tarkoittaisi esimerkiksi sovellushaavoittuvuuksia, jolla tavoin se usein kuvataan teksteissä. Pääosin hyökkäyspinta tulisi siis mieltää hyvinkin laajana kokonaisuutena.

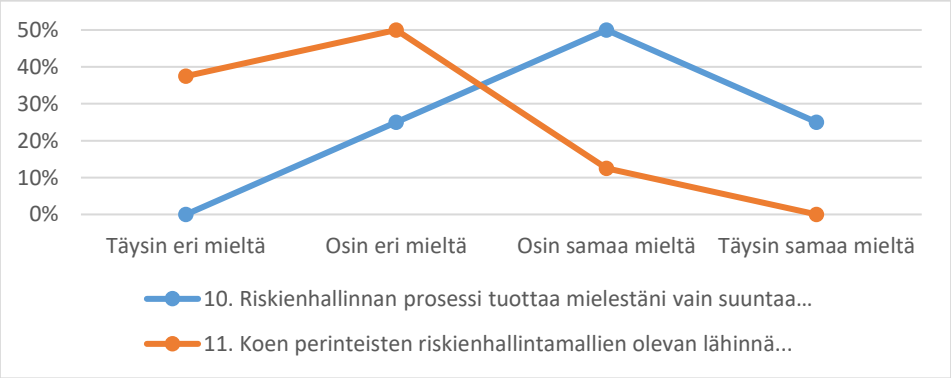
> ”Henkilöstön vähentäminen ei ole minusta keino hallita hyökkäyspinta-alaa. Toki jos sille on liiketoiminnalliset perustelut niin silloin voi ajatella tuota kautta.” (Vastaaja 6)

Ensimmäisen kategorian kysymyksissä monet yritykset totesivat hyökkäyspintansa kasvaneen, mutta tuo kasvu ei kuitenkaan siis vastausten valossa haittaa

merkittävästi kyberturvallisuuden toteutumista (Kysymys 8). Vastauksissa kuitenkin esiintyy jonkin verran hajontaa ($\sigma$=0,70). 12,5 % ovat täysin samaa mieltä, 37,5 % osin samaa mieltä ja loput (50 %) ovat osin eri mieltä. Korrelaation tämän kysymyksen sekä hyökkäyspinnan kasvun (kysymys 2) välillä jää vähäiseksi, joskin korrelaatio on joka tapauksessa positiivinen ($r_s$=0,288). Liitteessä 3 on esitetty kysymysten keskinäiset korrelaatiokertoimet tarkemmin taulukkomuodossa.

Vastaajista 62,5 % ovat osin samaa mieltä, että nykyistä riskienhallintaprosessiaan toteuttaessaan osa riskeistä jää huomioimatta. Vain 37,5 % vastasi ”Hyvin vähän”. Kuitenkaan yksikään vastaajista ei kokenut, että kaikki riskit tunnistettaisiin tai tunnistamattomia olisi liiaksi. Kysymykseen 10, jossa väitetään riskienhallinnan antavan lähinnä suuntaa antavia tuloksista, vastattiin hyvin vaihtelevasti. Vain 25 % on täysin samaa mieltä, 50 % osin samaa mieltä ja 25 % osin eri mieltä. Näiden kahden kysymyksen (Kysymykset 9 & 10) välillä ei kuitenkaan ole tunnistettu korrelaatiota tämän tutkimuksen valossa ($r_s$=0,000, N=8).

Kuitenkin tarkastellessa kysymystä 11, jossa väitetään riskienhallinnan olevan välttämätön paha, jota vain täytyy tehdä, on vastausten keskiarvo (1,75) enemmän ”eri mieltä” -suunnassa. Eli vaikka riskienhallintaa kritisoidaan vastausten valossa, ja sen ei koeta antavan välttämättä riittävän hyvää näkyvyyttä yrityksen uhkakenttään, koetaan perinteinen riskienhallinta kuitenkin pääosin tärkeäksi osaksi turvallisuudenhallintaa. Ainoastaan yksi vastaaja oli osin samaa mieltä väittämän kanssa. Riskienhallinnan prosessin epätarkkuuden (kysymys 10) ja kritisoinnin (kysymys 11) välillä ilmenee pieni positiivinen korrelaatio ($r_s$=0,267). Alla (KUVIO 9), on esitettynä näiden kysymysten vastausten jakauma.




KUVIO 9 Riskienhallinnan kritiikin kysymysten vastaukset

Selkeää positiivista korrelaatiota kategorian 2 kysymyksissä ilmeneekin kysymysten 6 ja 11 välillä ($r_s$=0,750). Tämä viittaa siihen, että yrityksen ollessa hyvin itsevarma omasta kyvystään tunnistaa uhkia, koetaan perinteisen riskienhallinnan prosessi lähinnä pakollisena standardien ja kriteeristöjen vaatimana toimenpiteenä. Vastaavasti yritys, joka kokee hyökkäyspintansa kasvaneen (kysymys 2) kritisoi riskienhallinnan prosessia (kysymys 10) selkeästi vähemmän ($r_s$= -0,811). Toisaalta yritykset, jotka eivät koe hyökkäyspintansa kasvaneen esittävät suurempaa kritiikkiä perinteistä riskienhallintaa kohtaan. Sama ilmiö toistuu tarkasteltaessa yrityksen kokoa ja kysymystä 10, korrelaation ollessa vahvasti

negatiivinen ($r_s$=-0,580). Yrityksen koon ollessa pieni, oli kritiikki riskienhallintaa kohtaan keskimääräistä suurempi. Toisaalta koon ollessa keskisuuri tai suuri, oli kritiikki pientä. Vastausten valossa ilmeni kuitenkin poikkeuksiakin. On nähtävillä, että pienissä yrityksissä kyberturvallisuuden hallintaprosessien kehittämiselle on pienempi tarve kuin suuremmissa yrityksissä.

Sanallisissa vastauksissa esiintyy kuitenkin huomioita siitä, että vaikka hyökkäyspinta kasvaakin merkittävästi, ei se välttämättä muutu vaikeammaksi hallita. Sen vain koetaan vaativan enemmän resursseja. Toisaalta hyökkäyspinta voi kasvaa huomaamatta esimerkiksi pilvipalveluiden käytön myötä (Vastaaja 4). Hyökkäyspinnan havainnoinnin uskotaan myös olevan asia, jota ei koskaan pystytä täysin tunnistamaan ja ymmärtämään, sillä siihen vaikuttaa esimerkiksi ulkopuolelta tuleva tekninen kehitys ja ulkopuolisen infrastruktuurin tekijät (Vastaaja 3).

## 5.4 Hyökkäyspinnan hallinnan sovellukset ja palvelut

Kategorian 3 kysymyksillä pyrittiin tunnistamaan, kuinka paljon yrityksillä on käytössään EASM-, DRPS- ja CAASM-palveluita tai -sovelluksia, ja miten niitä hyödynnetään. Gartnerin artikkeleissa ratkaisujen todettiin olevan tulevaisuuden trendi, mutta kirjallisuuskatsauksena tarkasteltuna näitä palveluita kuitenkin löytyy markkinoilta jo suhteellisen paljon. Kuvailut järjestelmistä myös mahdollistavat sen, että yksittäinen uhkametsästykseen liitettävä sovellus tai työkalu asettuisi jonkin näistä kategorian alle.

Vastauksissa näkyy selkeästi, etteivät kyseiset trendit ole vielä nostaneet päätään yrityksissä merkittävästi. Vain 1 yrityksistä vastasi käyttävänsä EASM- ja CAASM-sovelluksia. Tämän lisäksi yksi vastasi avoimessa kysymyksessä ulkoistavansa vastaavia palveluita. Kyseessä olivat suuri ja keskisuuri yritys. Avoimissa vastauksissa ilmenee, että yritykset toteuttavat näitä toiminnallisuuksia osin tai korvattuna esimerkiksi ulkoisella kartoituksella tai skannauksella. Alla (TAULUKKO 4) on esitetty kyseisen kategorian vastausfrekvenssit prosentteina.

TAULUKKO 4 Hyökkäyspinnan hallinnan sovellusten kysymysten frekvenssit

| | Ei | Kyllä |
|---|---|---|
| 12. Käytämme EASM-sovellusta tai -palvelua | 85,7 | 14,3 |
| 13. Käytämme DRPS-sovellusta tai -palvelua | 100,0 | 0,0 |
| 14. Käytämme CAASM-sovellusta tai -palvelua | 85,7 | 14,3 |

Yksi vastaajista (6) myös uskoo, ettei identiteettivarkauksilta voisi suojautua minkään sovelluksen avulla. Heidän yrityksensä kuitenkin seuraa lähinnä pimeää verkkoa vuotaneiden tunnusten varalta. Yksi keskisuuri yritys mainitsee käyttävänsä SIEM (Security Information and Event Management) ja SOAR

(Security Orchestration, Automation and Response) -järjestelmiä ja niihin liitettyjä uhkatietoja todeten seuraavaa:

> ”(…) SOAR on pystynyt automatisoimaan reagointia. Tämä ei kuitenkaan vastaa automaattista haavoittuvuuksien hallintaa. Osalle infrasta (esim. tietyt palvelimet ja päätelaitteet) on tehty automaattisia päivityksiä, samoin haavoittuvuusskannaukset on automatisoitu ja tulokset viety SIEM järjestelmään.” (Vastaaja 4)

Hyökkäyspinnan hallinnan tulevaisuuden trendeiksi kuvailtuja palveluita ei siis juurikaan ole käytössä, mutta suurempien yritysten voidaan nähdä toteuttavan jo osia sellaisista sovelluksista. Näiden kokonaisintegraatio ja automaatio ei kuitenkaan ole vielä hetkeen tapahtumassa, joka näkyy myös viimeisessä kysymyksessä, jonka vastausfrekvenssit on esitetty alla (TAULUKKO 5).

TAULUKKO 5 Riskienhallinnan jatkuvuuden luonteen kysymyksen frekvenssit

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 15. Arvioi riskienhallintaprosessinne ajallista luonnetta, staattisuutta ja dynaamisuutta asteikolla 1–5 | 0,0 | 25,0 | 25,0 | 50,0 | 0,0 |

Aiempien kategorioiden kysymysten pohjalta voitiin tunnistaa ymmärrys hyökkäyspinnasta ja kokemukset omista prosesseista, jotka viestivät jo siitä, että päivitetyille toimintamalleille tai sovelluksille ei ollut tarvetta. Tämä näkyi myös tämän kategorian kysymyksissä, yritysten pääsääntöisesti vastatessa kieltävästi siihen, käyttävätkö tämänkaltaisia hyökkäyspinnan hallinnan sovelluksia.

Riskienhallinnan jatkuvuuden luonteen kysymyksellä pyrittiin tunnistamaan kuinka automatisoiduksi yritykset tällä hetkellä kokevat prosessinsa ja järjestelmänsä asteikolla 1–5, jossa 1 tarkoittaa ”Riskienhallintaprosessimme tehtiin aikanaan ja se on pysynyt sellaisenaan jo vuosia” ja 5 tarkoittaa ”Prosessimme on täysin reaaliaikainen, jota tukee kokonaisvaltaiset ja automatisoidut järjestelmät”. Ideaalitilanteessa yrityksen hyökkäyspinta olisi automaattisesti valvottuna ja tarvittavat palvelut, sensorit ja työkalut olisivat integroituna ohjelmistorajapinnoin keskeiseen ilmoitus- ja hallintajärjestelmään (esimerkiksi CAASM-järjestelmän avulla). Vastausten valossa tämä ei kuitenkaan ole vielä nykypäivää, joskin viitteitä tästä suunnasta on nähtävillä kirjallisuuskatsauksen sekä kysymysten tulkinnasta.

Suuremmat yritykset toteuttavat automaatiota enemmän kuin pienet, joskin pieniä poikkeuksia löytyi. Konsultointia tekevä yritys totesi, että he tietävät kuitenkin asiakkaidensa käyttävän tällaisia. Toisaalta yritys, jonka toiminnot toimivat pääsääntöisesti ilman verkkoyhteyksiä, ei kokenut tällaisia tarpeelliseksi. Esille nousi myös maininta SaaS-palvelusta. Tällöin yritys ei itse ole vastuussa täysin omasta teknisestä hyökkäyspinnastaan, vaan osa tietoturvan toteutumisesta jää palveluntarjoajalle.

Kaksi yrityksistä ilmoitti tekevänsä muutostöitä ja päivittäen riskienhallintaprosessiaan aina, kun tulee muutos uhkakenttään tai saadaan uutta tietoa

tapahtuneista poikkeamista. Toinen näistä totesi myös, ettei täysin kokonaisvaltaista järjestelmää taida vielä olla olemassakaan.

Automaatio riskien- ja hyökkäyspinnan hallinnassa on siis suhteellisen pienimuotoista, eikä CAASM-, EASM- ja DRPS-tasoisia palveluita olla vielä juurikaan integroitu yritysten turvallisuustoimintaan. Suuremmat yritykset hyödyntävät automaatiota enemmän kuin pienet, joka onkin jotakuinkin itsestäänselvyys suuremman yrityksen suuremman hyökkäyspinnan myötä. Selkeästi osa yrityksistä ei koe tämänkaltaista kokonaisvaltaista automaatiota tarpeelliseksi, mutta vastauksissa tätä päätöstä ei perusteltu sen enempää.

# 6 KESKUSTELU JA JOHTOPÄÄTÖKSET

## 6.1 Pohdinta

### 6.1.1 Hyökkäyspinnan tunnistaminen

Hyökkäyspinta käsitetään hyvin eri tavalla riippuen esittäjästä ja tekstin luonteesta ja viitekehyksestä. Useissa tilanteissa hyökkäyspinnalla tarkoitetaan internetiin näkyvää haavoittuvaista tietoverkkokokonaisuutta, joka voi tarkoittaa esimerkiksi avointa porttia tai IP-osoitetta, jonka kuviteltiin olevan poistettu käytöstä. Mahdollisuuden hyökkäykselle voi kuitenkin löytää täysin toiselta sivulta, kuten varmuuskopiointipalvelusta, hakukoneesta tai pimeästä verkosta. Termiä käytetään myös paljon kokonaisvaltaisemmin, eikä se tällöin pelkästään käsitä yrityksen hallinnassa olevia palveluita. Hyökkäyspinnan voidaan jopa määrittää käsittävän digitaalisen ja fyysisen kokonaisuuden.

Tärkeää on siis suunnata keskustelu asioihin, mitkä kasvattavat ja pienentävät hyökkäyspintaa, eikä siitä mitä hyökkäyspinta tosiasiassa on. Esimerkiksi ihmisten käyttäytyminen ja varjo-IT vaikuttavat hyökkäyspinnan kasvuun. Yksinkertaisesti voi ajatella, että 10 hengen yrityksessä on vähemmän mahdollisuuksia kalasteluyrityksen onnistumiselle kuin 1000 hengen yrityksessä. Onko perusteltua siis vähentää työntekijöiden määrää, jotta hyökkäyspinta pienenisi? Hyökkäyspinnan hallinta tulee siis käsittää yritystä läpileikkaavana prosessina, ja eräänlaisena kattokäsitteenä, joka on vahvasti linkittyneenä yrityksen liiketoimintaan. Hyökkäyspinnan hallinta voi olla osa haavoittuvuuksienhallintaa, mutta samalla myös haavoittuvuuksienhallinta voidaan nähdä osana hyökkäyspinnan hallintaa. Kyseessä on siis hyvin monisyinen termi, joka tutkimuksissa käsitellään hyvin eri tavalla kontekstin mukaan. Kyselyn vastauksissakin ilmeni vaihtelua siinä, miten yritykset haluavat termiä käsiteltävän.

Hyökkäyspinta ei siis monestikaan kuvaa tarkasti sitä mitä sillä yritetään tarkoittaa. Olisi soveltuvampaa puhua esimerkiksi teknisestä hyökkäyspinnasta suunniteltaessa teknisiä toimenpiteitä, mutta riskienhallintaprosessin osana

hyökkäyspinnan tulisi käsittää kyberfyysinen kokonaisuus sekä yrityksen muu hallinto. Muutoin keskustelussa herkästi ajaudutaan epäselviin tilanteisiin. Keskeisenä lähtökohtana onkin ymmärtää mitkä asiat vaikuttavat tuntemattoman hyökkäyspinnan kasvuun, ja miten näitä näkymättömiä ja tuntemattomia asioita voidaan tunnistaa ja hallita.

### 6.1.2 Perinteisen riskienhallinnan tarve

Tutkimuksen alussa oli oletuksena, että uhka-alttiuden ja hyökkäyspinnan hallinta eroaisi rajustikin perinteisestä riskienhallinnasta. Tämä ei kuitenkaan täysin pidä paikkansa. Riskienhallinta ja hyökkäyspinnan hallinta eivät ole toisiaan poissulkevia asioita, vaikka Gartnerin tutkimuksissa ilmenikin tällaista retoriikkaa.

Ongelmana on lähinnä perinteisen riskienhallinnan subjektiivisuus ja illuusio kontrollista, joka perustuu vaikuttavuuteen ja todennäköisyyteen. Tämä voi helposti johtaa tietoturvasta päättävät henkilöt virheelliseen turvallisuudentunteeseen. Vaikutuksen ja todennäköisyyden arviot ovat monesti siis vain valistuneita arvauksia. Tätä arviota on verrattu jopa säätilan ennustamiseen, sen sisältäessä liikaa muuttujia, jotta tulokset olisivat täysin tarkkoja. Pohja-ajatuksena uhka-alttiuden hallinnan ja yllä kuvatun riskienhallinnan mallien vastakkainasettelussa on siis lähtökohtatiedon ja tunnistamattomien muuttujien merkittävyys. Vaikutukset ja todennäköisyydet ovat valistuneita ja kokemusperäisiä arvauksia. Toisaalta kyberuhkatiedustelun tuottama tieto hyökkäyspinnan pienentämiseksi taas on dataan perustuvaa analyysiä.

Lainsäädäntö riskienhallinnan osalta on suhteellisen avointa, ja se jättää paljon yrityksen itsensä vastuulle. Hyökkäyspinta tai uhka-alttius eivät termeinä juuri ilmene lainsäädännöissä tai kriteeristöissä, joskin niitä käsitellään lyhyesti riskienhallinnan ohella. Lainsäädäntö ja kriteeristöt tukevat riskienhallinnan toteuttamista, mutta hyvin korkealla abstraktiotasolla. Tutkimuksissakin on huomattu, että yritysten voi olla vaikea arvioida riskejä perinteisin menetelmin, sillä kuten Gartnerin artikkelitkin väittävät, on todennäköisyyden ja vaikutuksen arviointi hyvin haastava, ja jopa mahdotonta.

Keskeistä alati kasvavan hyökkäyspinnan turvaamisessa on siis jatkuva toiminta. Automatisoidut ja koneoppivat mallit tukevat kyberuhkatiedustelussa ja kerätyn tiedon analyysissä, jotta yrityksessä olisi tehokkaammat päätöksentekoprosessit hyökkäyspinnan pienentämiseen ja järjestelmien turvaamiseen. Vuosikellon mukaisesti vaikutuksen ja todennäköisyyden kautta tehty riskienhallinta ei siis riitä nopeudessaan, kun vertailukohdaksi asetetaan laajempi ja automatisoitu järjestelmä.

Uhkalähtöisen ajattelun lähtökohdat eivät siis myöskään katoa mihinkään, vaikka hyökkäyspinnan hallinta muuttuisikin entistä automatisoidummaksi ja proaktiivisemmaksi. Hyökkäysmallin ymmärtäminen on edelleen tärkeää hyökkäysvaiheiden erittelyn ja mahdollisten haavoittuvuuksien löytämisessä. Uhkatoimijoiden piirteiden erottaminen toisistaan on vaatimus sille, että yritys kykenee resursoimaan suojaustoimensa oikein. Kyselyssäkin tunnistettiin se, ettei kaikki yritykset, etenkin pienet, edes kokeneet tarpeelliseksi hankkia

monimutkaisia suojausjärjestelmiä. Kyse on siis loppujen lopuksi perinteisen riskienhallinnan kustannusperiaatteen ajatuksesta: Harva yritys haluaa maksaa tuhatta euroa, suojatakseen kymmenen euron arvoista järjestelmää. Tilannetta kuitenkin hankaloittaa kustannusten arvioinnin vaikeus, joka on tunnistettu muun muassa Instan (2022, s. 46) kyselytutkimuksessa NIS2-direktiiviin liittyen.

### 6.1.3 Proaktiivisempi tulevaisuus

Gartner kuvaili hyökkäyspinnan hallinnan sovelluksia tulevaisuuden trendeiksi ja tämä tutkimus tunnistikin niiden olevan jo osin arkipäivää. Kuitenkin lopulliseen tavoitteeseemme pääsemiseksi, näiden järjestelmien tulisi olla keskenään yhteensopivia ja perustua mahdollisimman reaaliaikaiseen dataan. Parhaassa tapauksessa niiden toimintaa tukisi koneoppiva algoritmi, joka osaisi ennakoida mahdollisia uusia hyökkäysmalleja tai haittaohjelmia, jopa ennen niiden syntymistä.

Tällä hetkellä SIEM- ja SOAR-järjestelmät jo toteuttavat koostetun tiedon pohjalta aktiivista uhkienhallintaa, mutta useat uhkat eivät välttämättä ole täysin tavoitettavissa yrityksen omin keinoin. Pimeän verkon, koko IP-osoiteavaruuden tai Github-arkistojen skannaaminen vaatii omat resurssinsa ja sovelluksensa, jotta esimerkiksi hyökkäyksen valmistelu, vuotaneet salasanat tai avoimet portit tunnistettaisiin ajoissa. Yksittäisenä esimerkkinä Shodan (2024) on jo oiva esimerkki siitä osakokonaisuudesta, miltä tulevaisuuden hyökkäyspinnan hallinta tulee näyttämään.

Useisiin eri tarkoituksiin ja eri hyökkäysvektoreihin kohdistuvat skannerit tulisivat jatkuvasti keräämään tietoa koneluettavaan muotoon, jonka yritys voi kerätä omaan hallintajärjestelmäänsä, jossa automaattiset järjestelmät luovat johtopäätöksiä ja antavat hälytyksiä tarpeen mukaan. Tällaisten palveluiden yleistyessä, tulisi niiden kustannukset laskemaan, jolloin yritys kokee palveluiden käyttämisen yhtä yksinkertaisena päätöksenä kuin oikein konfiguroidun palomuurin.

### 6.1.4 Tarkistuslista yrityksille

Tutkimuksen tuloksena syntyi tarkistuslista ja ohje, joka on esitetty liitteessä 4. Ohjeen tarkoituksena on tuottaa yritykselle 12 kohdan tarkistuslista, joka arvioi yrityksen tarvetta integroida hyökkäyspinnan hallintaa vahvemmin omaan toimintaansa. Sen sisältö rakentui kirjallisuuskatsauksessa tunnistettujen asiakokonaisuuksien sekä kyselytutkimuksen analyysin ja pohdinnan tuloksena.

Listan 12 kohtaa ovat kysymyksiä ja väittämiä kuten ”Onko varjo-IT:tä on tunnistettu?” tai ”Onko yrityksen imagoa tai brändiä kopioitu tai tahrattu verkossa?”. Vastaajan saadessa vähintään puolet ”Kyllä” vastauksia, ohjeistetaan lukijaa tutustumaan hyökkäyspinnan hallintaan tarkemmin liitteen toisella sivulla. Toisella sivulla on selostus hyökkäyspinnan minimoimisen periaatteesta, kolmesta sovelluskokonaisuudesta ja proaktiivisesta uhkien tunnistamisen periaatteesta.

Tarkistuslista on muodostettu lyhyesti ja ytimekkäästi sellaiseen muotoon, että se pystytään tulostamaan yhdelle paperille kaksipuoleisena helpon käytettävyyden maksimoimiseksi. Sen tarkoituksena ei ole antaa absoluuttisia vastauksia, vaan saattaa päättävät henkilöt pohtimaan ja tarkastelemaan omia prosessejaan kriittisesti. Se antaa riittävät eväät aiheen tarkemmalle syventymiselle ja uhkalähtöisen ajattelun ja hyökkäyspinnan hallinnan periaatteille.

## 6.2 Johtopäätökset

Yritykset ovat hyvin varmoja omasta tietoturvastaan ja käytössään olevista järjestelmistään ja prosesseistaan. Täysin automaattista ja niin laajasti uhkia havaitsevaa järjestelmää, kuin tutkimuksessa esitetyt sovellukset olivat, ei koettu tarpeelliseksi. Yritykset kuitenkin pääsääntöisesti ovat tunnistaneet teknisen hyökkäyspintansa kasvaneen muun muassa pilvipalveluiden ja pienissä määrin myös varjo-IT:n myötä. On siis nykypäivää, että yritysten järjestelmät monipuolistuvat, laajenevat ja kasvavat. Tätä myötä täysin tuntemattomien hyökkäysvektoreiden syntyminen voi aikanaan olla hyvinkin arkipäivää jopa pienillekin yrityksille.

Uhka-alttiuden ja hyökkäyspinnan hallintaa sovelletaan perinteisen riskienhallinnan ohella hyvin vähän. Vain suuremmissa yrityksissä näkyy merkkejä yhä automatisoidumman ja uhkalähtöisemmän hyökkäyspinnan hallinnasta. Perinteinen riskienhallinta koetaan edelleen tarpeelliseksi, eikä se saanut vastaajilta yhtä suurta kritiikkiä kuin Gartnerin artikkeleissa. Vastauksissa kuitenkin näkyi, ettei perinteiseen riskienhallintaan sovi täysin luottaa, vaan vaikutuksen ja todennäköisyyden arviointi koetaan enemmänkin suuntaa antavaksi prosessiksi eikä niitä tulisi mieltää absoluuttisena totuutena.

EASM-, CAASM- ja DRPS-palveluiden ja -sovellusten käyttöaste on todella vähäistä, vaikka näitä sovelluksia markkinoilla onkin jo jonkin verran. Näiden vähäiseen käyttöasteeseen vaikuttaa vahvasti yritysten usko omiin nykyisiin prosesseihinsa ja palveluihinsa. Yrityksen varallisuus ja koko vaikuttavat myös vahvasti siihen, nähdäänkö edes tarpeelliseksi ostaa lisäturvaa tällaisista sovelluksista, joita ei tosiasiassa koeta kriittisiksi yritykselle.

Päätutkimuskysymykseen löydettiin siis kolme keskeistä vastausta:

(1) Yritykset eivät juurikaan sovella hyökkäyspinnan hallintaa perinteisen riskienhallinnan ohella. Tähän vaikuttaa varmasti tutkimuksessa esitettyjen teknologioiden suhteellisen nuori ikä, sekä yritysten keskimääräinen varmuus omista prosesseistaan ja pieni tietoturvapoikkeamien määrä.
(2) Hyökkäyspinnan hallintaa voi soveltaa perinteisen riskienhallinnan ohella suhteellisen vaivattomasti, mutta sen vaikuttavuutta on vaikea todentaa ilman tarkempaa tutkimusta. Loppujen lopuksi kyse on uusien periaatteiden ja toimintamallien sisäistämisestä, joita tukevat uudet sovellukset ja palvelut. Perinteinen riskienhallinta ei ole katoamassa

mihinkään, eikä sitä ja hyökkäyspinnan hallintaa sovikaan vertailla vastakkaisina ilmiöinä, vaan pohjimmiltaan toisiaan tukevina asioina.

(3) Hyökkäyspinnan hallintaa sovelletaan todennäköisesti tulevaisuudessa hyvinkin automatisoitujen yhteen liitettyjen osatoimintoja toteuttavien sovellusten toimesta, jossa reaaliaikaisen tiedon merkityksellä ja tarkkuudella tulee olemaan suuri merkitys. Jatkuva ja tarkka näkyvyys omasta hyökkäyspinnasta sekä proaktiivinen uhkatiedustelu mahdollistavat uhkiin reagoimisen jo ennen niiden realisoitumista.

## 6.3 Tutkimuksen luotettavuus

Kirjallisuuskatsausta voisi pohjimmiltaan luonnehtia yhtä luotettavaksi kuin sen viitteet. Tämän tutkimuksen luotettavuutta tukee sen pohjana käytetyt lähteet, jotka olivat ajantasaisia ja monipuolisia. Tämä jo osaltaan tuki kirjallisuuskatsauksen onnistumista, joka toimi pohjana kyselyn muodostamiselle. Pääosa viitteistä kohdistuu alan tutkimusartikkeleihin, joskin osa lähteistä on myös valmistajien verkkosivuja. Yritysten verkkosivuja käytettäessä lähteinä on aina arvioitava tiedon oikeellisuus ja erotettava perusteltavasta tiedosta ylimalkainen markkinointiteksti.

EASM, CAASM ja DRPS –sovellusten ollessa osin vasta tulevaisuuden trendejä, oli jo tutkimusta tehdessä arvioitava ja tunnistettava näiden sovellusten ja palveluiden mahdollinen todellinen käyttöaste. Tutkimus tarkastelikin jo olemassa olevia sovelluksia ja tarkasteli niiden kypsyysastetta. Tulevaisuuden tutkimuksen keinoihin ei kuitenkaan menty, sillä tarkoitus oli lähtökohtaisesti tutkia tämänhetkistä tilannetta, eikä arvioida tulevaisuuden trendien toteutumista.

Kyselyn toteutus oli siis yleisesti tuotettu hyvällä tietopohjalla kirjallisuuskatsauksen avulla. Kyselyn vastaajamäärä kuitenkin jäi suhteellisen vähäiseksi. Tämänkaltaisen vastaajamäärän valossa tutkimuksen luotettavuutta vähentäisi vastaajien kompetenssin puuttuminen tai pelkät määrälliset kysymykset. Nämä kaksi keskeistä ongelmakohtaa tunnistettiin ja huomioitiin jo tutkimuksen alkuvaiheessa. Vastaajien taito vastata asiantuntevasti ja laajasti oli varmistettu ennen kyselylomakkeen lähettämistä. Vastaajien mielenkiinto aiheeseen mahdollisti myös laadukkaiden avointen vastausten saamisen, joka parhaimmillaan täydensi määrällisten tulkintojen pohdintoja.

Usein tämänkaltaisen kyselyn tarkoituksena on saada yleistettävää tietoa. Kuitenkin tämän tutkimuksen valossa, otannan ollessa pieni, ei välttämättä voida analysoituja johtopäätöksiä luonnehtia täysin yleistettäviksi. Yritysten toimialat olivat suhteellisen lähellä toisiaan, ja ainakin tietoturvakonsultoinnin toimialaa kohden johtopäätösten kuitenkin voi todeta olevan yleistettävää tietoa. Tutkimuksen luotettavuutta lisää se, että tuloksissa on samankaltaisuuksia muihin vastaaviin tutkimuksiin. Esimerkiksi digiturvallisuuden riskikysely (Digi- ja väestötietovirasto, 2021), organisaation digiturvakysely (Rousku, 2021) ja Randori (2022) tunnistavat kehityskohteita uhkakentän tunnistamiseen ja

prosesseihin liittyen. Lisäksi eri kokoisten vastaajaluokkien vastauksissa tunnistetaan eroja, jotka voivat perustuvat pitkälti yrityksen resursseihin.

## 6.4 Jatkotutkimusehdotukset

Kyberuhkatiedustelu tunnistettiin tutkimuksessa merkittäväksi vaikuttajaksi onnistuneiden EASM-, CAASM- ja DRPS-palveluiden tuottamisessa. On siis tarpeen tutkia näiden kahden integraatiota: Miten kyberuhkatiedustelun keräämä tieto saadaan konemuodossa hyökkäyspinnan hallinnan sovellusten tarkasteltavaksi. Tällöin esimerkiksi DRPS-sovelluksen ei tarvitsisi tehdä muuta kuin itse analyysi sille syötetystä datasta. Toisaalta on hyvä myös pohtia, kannattaako uhkatiedustelua täysin erottaa näistä palveluista vai integroida ne jo sellaisenaan palveluun.

Tämän tutkimuksen kysely oli kohdistettu IT-alan yrityksiin, joissa tietoturvan oletettiin olevan keskimääräistä yritystä paremmalla tasolla. Tämä myös mahdollisti sen, että vastaajilla oli riittävä kompetenssi vastata asiantuntevasti kysymyksiin. Tämänkaltaisen kyselyn laajentaminen myös IT-alan ulkopuolelle voi tarjota jatkotutkimukselle tarvetta. Esimerkiksi kunnille tehtävä kyselytutkimus voisi valottaa kansallisen hyökkäyspinnan hallinnan tilaa. Tällöin tutkimusta tehdessä tulee kuitenkin harkita tiedonkeruun toteuttamista ennemmin haastatteluna, jotta epäselvyydet vastauksissa voi korjata jo haastattelun aikana.

Tutkimuksessa tunnistettiin, että yritys useimmiten vastaa olevansa tietoinen yrityksensä hyökkäyspinnasta. On kuitenkin tunnistettava, että yritys saattaa olla tietämättään hyökkäyksen kohteena pitkäänkin, ennen kuin hyökkäys tunnistetaan ja toivottavasti torjutaan. Hyökkäyspinnan tuntemuksen tutkimus olisi siis hyvä yhdistää esimerkiksi penetraatiotestaukseen tai jopa yksinkertaisimmillaan yrityksen tiedossa olevan IP-osoiteavaruuden porttiskannaukseen. Näin saadaan varmempi ymmärrys yrityksen kyvystä tunnistaa omat haavoittuvuutensa. Tämänkaltaisella tutkimuksella voidaan tunnistaa heikot prosessit ja palvelut sekä tietoturvavastaavien todellinen kyky havainnoida tietoturvaan liittyviä ongelmia.

Tutkimuksessa kuvattujen hyökkäyspinnan hallinnan sovellusten ollessa vielä kypsymisvaiheessa, on niihin mahdollista kohdistaa tulevaisuuden tutkimuksena toteutettu tutkimus. Trendien tarkastelu ja tulevaisuuden skenaarioiden luominen ja arviointi lisäisi ymmärrystä muun muassa niihin vaikuttavien tulevaisuuden teknologioiden kuten tekoälyn ja kvanttilaskennan vaikutuksesta.

Varjo-IT:n käyttämistä ja tietoturvasäädösten noudattamatta jättämistä on tutkittu jo jonkin verran, mutta tämän aiheen liittämistä hyökkäyspinnan hallinnan viitekehykseen sopii harkita.

# 7 YHTEENVETO

Tutkimuksella lähdettiin selvittämään pääkysymyksenä ”Miten uhka-alttiuden ja hyökkäyspinnan hallintaa voidaan soveltaa perinteisen riskienhallinnan ohella?” Tämän lisäksi kolme alakysymystä ohjasivat tutkimusta:

1. Mitä kyberturvallisuuden perinteinen riskienhallinta käsittää?
2. Mitä on uhkalähtöisyys sekä uhka-alttiuden ja hyökkäyspinnan hallinta?
3. Miten yritykset kokevat perinteisen riskienhallinnan ja hyökkäyspinnan hallinnan?

Perinteinen riskienhallinta perustuu usein vaikutukseen ja todennäköisyyteen, jotka perustuvat asiantuntijoiden arvioihin. Riskienhallinnassa pyritään tunnistamaan kaikki mahdolliset näkyvät ja näkymättömät uhkat ja arvioimaan niiden vaikutusta omalle yritykselle.

Uhkalähtöisyys, uhka-alttius ja hyökkäyspinnan hallinta ovat termeinä monisyisiä. Yleisenä periaatteena kuitenkin on, että yrityksen hyökkäyspinta on monesti hyvinkin tuntematonta varjo-IT:n, jatkuvan digitalisaation ja pilvipalveluiden myötä. Hyökkäyspinnan hallinnan periaatteena onkin tuottaa täydellinen näkyvyys omiin palveluihin ja järjestelmiin, jotta uhkiin vastaaminen ei perustuisi pelkästään haavoittuvuuksien metsästämiseen, vaan muun muassa hyökkäyspinnan minimoimiseen. Esimerkiksi yritys ei välttämättä tarvitse kaikkia käytössään olevia sovelluksia, jos pienemmälläkin määrällä saisi tehtävät täytettyä. Tällöin uhkia ei suoranaisesti ole torjuttu, mutta niiden todennäköisyyttä vaikuttaa yritykseen on huomattavasti laskettu.

Yritykset kokevat perinteisen riskienhallinnan vaihtelevasti. Se ei saa osakseen niin suurta kritiikkiä kuin kirjallisuuskatsauksessa tarkastelluissa artikkeleissa, joskin monet kokevat, ettei perinteinen riskienhallinta tuota täysin sitä tietoturvan tasoa, mitä sillä haluttaisiin. Hyökkäyspinnan hallinta koetaan osin haastavaksi. Yritykset eivät koe olevansa täysin tietoisia omasta hyökkäyspinnastaan, mutta ne eivät kuitenkaan juuri hyödynnä tutkimuksessa esitettyjä hyökkäyspinnan hallinnan sovelluksia.

Hyökkäyspinnan ja uhka-alttiuden hallinta tässä tutkimuksessa kuvatulla tavalla on suhteellisen vaivatonta toteuttaa, sillä markkinoilla on jo olemassa sovelluksia ja palveluita tähän tarpeeseen. On kuitenkin todennäköistä, että tämä trendi nousee suurempaan rooliin vasta tulevaisuudessa. Tämän trendin kasvuun voivat vaikuttaa sovellusten helppokäyttöisyys ja matala hinta sekä tekoälyn ja uhkametsästyksen riittävä kehittyminen.

# LÄHTEET


Ablon, L. (2018). *Data Thieves – The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*. 15.3.2018, Yhdysvallat. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Abricto Security. (2020). *SQLmap Cheatsheet and Examples*. https://abrictosecurity.com/sqlmap-cheatsheet-and-examples/

Anomali. (2023). *What is Threat Exposure Management?* https://www.anomali.com/resources/understanding-threat-exposure-management

Arponen, L-P. (2023). *Riskienhallinnan suunnittelu ja toteutus ICT-organisaatioissa pro gradu -tutkielma.* Jyväskylän yliopisto. http://urn.fi/URN:NBN:fi:jyu-202305112954

Axonius. (2023) *Axonius – Control Complexity -verkkosivu*. https://www.axonius.com/

Bitsight. (2023). *Attack Surface Monitoring*. https://www.bitsight.com/glossary/attack-surface-monitoring

Bombal, D. (2023). *Real World Hacking Tools Tutorial (Target: Tesla).* Youtube video, 1:22:27, 30.7.2023. https://www.youtube.com/watch?v=-jLbRnmGYaA

Bonnie, E. (3.1.2024). *Essential Guide to Security Frameworks & 14 examples*. SecureFrame. https://secureframe.com/blog/security-frameworks

Breachlock. (15.6.2023). *What is a Continuous Threat Exposure Management Program?* https://www.breachlock.com/resources/blog/what-is-continuous-threat-exposure-management-program/

Brown, R. & Lee, R.M. (2.2019). *The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey*. IntSight. https://a51.nl/sites/default/files/pdf/Survey_CTI-2019_IntSights.pdf

Cisco. (2023). *What is an Advanced Persistent Threat (APT)?* https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html

Cisco. (2023). *What Is Shadow IT?* https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous*. Versobooks.

Cyberint. (2023). *Argos Platform*. https://cyberint.com/platform/

Digi- ja väestötietovirasto. (2021). *Digiturvallisuuden riskikyselyn tuloksia, syksy 2021*. https://dvv.fi/documents/16079645/0/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf/32f991cd-1b0e-9275-fadb-2d5166c2102c/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf?t=1639476332261

D'Hoinne, J., Shoard, P. & Schneider, M. (2022). *Implement a Continuous Threat Exposure Management (CTEM) Program*. Gartner.

ENISA. (1996). *Health Insurance Portability and Accountability Act*. https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/data-protection-privacy/health-insurance-portability-and-accountability-act

ENISA. (8.11.2023). *Compendium of Risk Management Frameworks with Potential Interoperability*. https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

Euroopan unioni. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555

Eskola, J. & Suoranta, J. (1998).*Johdatus laadulliseen tutkimukseen*. Vastapaino, Tampere.

First (2023). *Common Vulnerability Scoring System v3.1: Specification Document*. https://www.first.org/cvss/v3.1/specification-document

FiSMA. (2023). Etusivu – FiSMA Ry. https://www.fisma.fi/

Friedman, J. (3.2016). *Attack Your Attack Surface – How to reduce your exposure to cyberattacks with an attack surface visualization solution*. Skybox Security. http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/attack-your-attack-surface-reduce-cyberattacks-attack-surface-visualization-pdf-1-w-2753.pdf

Gandotra, V., Singhal, A. & Bedi, P. (2012). Threat-Oriented Security Framework: A Proactive Approach in Threat Management. Teoksessa *Procedia Technology 4* (s. 487 – 494). University of Delhi, India. https://doi.org/10.1016/j.protcy.2012.05.078

Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z. & Xu, F. (2021). Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence. Teoksessa *2021 IEEE 37th International Conference on Data Engineering* (s. 193-204). http://dx.doi.org/10.1109/ICDE51399.2021.00024

Goasduff, L. (14.2.2018). *Protect Your Organization From Cyber and Ransomware Attacks*. Gartner. https://www.gartner.com/smarterwithgartner/protect-your-organization-from-cyber-and-ransomware-attacks

Google. (2023). *Google-haku hakusanoilla "Attack Surface Management" ja "Threat Exposure Management"*. https://www.google.com/

Greenbone. (2023). *Greenbone OpenVAS – Open Vulnerability Assessment Scanner*. https://www.tenable.com/products/nessus

Group-IB. (2023). *Attack Surface Management.* https://go.group-ib.com/hubfs/whitepaper/group-ib-asm-white-paper-2022-en.pdf

Hakluke. (8.3.2023). *How does EASM differ from CAASM and DRPS*. Detectify. https://blog.detectify.com/best-practices/how-does-easm-differ-from-caasm-and-drps/

Hart, N., Mingay, S. & Topham, D. (2022). *Quick Answer: The Difference Between Shadow and Business-Led IT, and Why It Matters*. Gartner. https://www.gartner.com/document/4008014

Heikkilä, T. (2014). *Tilastollinen tutkimus*. Edita Publishing Oy.

Howard, M., Pincus, J. & Wing, J.M. (2005). Measuring Relative Attack Surfaces. Teoksessa Teoksessa Lee, D.T., Shieh, S.P., Tygar, J.D. (eds) *Computer Security in the 21st Century* (s. 109-137). Springer, Boston, MA. http://dx.doi.org/10.1007/0-387-24006-3_8

IBM. (2023). *What is a threat actor*? https://www.ibm.com/topics/threat-actor

IBM. (2023). *What is attack surface management?* https://www.ibm.com/topics/attack-surface-management

Insta. (2022). *Selvitys kyberturvallisuusdirektiivin (NIS2- direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille –loppuraportti.* Liikenne- ja viestintäministeriö. https://api.hankeikkuna.fi/asiakirjat/34beb41e-515a-4fcd-a824-5136fd497329/310cde7e-950a-43f3-8429-2340a5d525b9/KIRJE_20230614065803.PDF

ISO. (2022). *ISO/IEC 27001 Information security management systems*. https://www.iso.org/standard/27001

Kyberturvallisuuskeskus. (2023). *Hyöky.* TRAFICOM. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky

Laki julkisen hallinnon tiedonhallinnasta 906/2019. https://www.finlex.fi/fi/laki/alkup/2019/20190906

Lehto, M. (2022). Cyber-attack Modelling: Building a General Model. Teoksessa *Proceedings of the 17th International Conference on Information Warfare and Security*. Jyväskylän yliopisto.

https://www.researchgate.net/publication/359038788_APT_Cyber-attack_Modelling_Building_a_General_Model

Levy, Y. & Ellis, T. (2006). *A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research.* Nova Southeastern University, Florida, USA.

Manadhata, P.K. & Wing, J.M. (2011). An Attack Surface Metric. Teoksessa *IEEE Transactions of Software Engineering Volume 37 , Issue 3* (s. 371-386) https://doi.org/10.1109/TSE.2010.60

Mandiant. (2023). *Targeted Attack Lifecycle*. https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

Mandiant. (2023). *Attack Surface Management*. https://www.mandiant.com/advantage/attack-surface-management

MITRE. (2017). *Sandwork Team*. https://attack.mitre.org/groups/G0034/

MITRE. (2023). *ATT&CK.* https://attack.mitre.org/

Miazi, N.S., Pritom, M.A., Shehab, M., Chu, B. & Wei, J. (2017). The Design of Cyber Threat Hunting Games: A Case Study. Teoksessa *2017 26th International Conference on Computer Communication and Networks* (s. 1-6). Vancouver, BC, Kanada. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8038527

National Institute of Standards and Technology NIST. (2023). *Public Draft: The NIST Cybersecurity Framework 2.0.* Yhdysvaltain kauppaministeriö. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

National Institute of Standards and Technology NIST. (2023). *FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems*. Yhdysvaltain kauppaministeriö. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

National Institute of Standards and Technology NIST. (2012). *Guide for Conducting Risk Assessment*. Yhdysvaltain kauppaministeriö. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Nessus. (2023). *Tenable Nessus – The Global Gold Standard in Vulnerability Assessment Built for the Modern Attack Surface*. Tenable. https://www.tenable.com/products/nessus

Picus Labs. (2.6.2023) . *What is Continuous Threat Exposure Management (CTEM)?* https://www.picussecurity.com/resource/glossary/what-is-continuous-threat-exposure-management-ctem

Puusa, A. & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeaus Oy.

Raggad, B. (2010). *Information Security Management – Concepts and Practice*. CRC Press, Taylor & Francis Group.

Randori. (2022). *The State of Attack Surface Management*. https://info.randori.com/hubfs/State%20of%20ASM%20Report.pdf

Rapid7. (2023). *Lazarus Group*. https://docs.rapid7.com/insightidr/lazarus-group/

Rousku, K. (2021). *Organisaation Digiturvakysely – Raportti ja kehittämiskohteet*. Digi- ja väestötietovirasto, VAHTI. https://dvv.fi/documents/16079645/17634906/Raportti+ja+kehitt%C3%A4miskohteet+-+Organisaation+Digiturvakysely,+18.8.2021.pdf/418e549f-45f5-4778-055d-e8692a46b17a/Raportti+ja+kehitt%C3%A4miskohteet+-+Organisaation+Digiturvakysely,+18.8.2021.pdf?t=1630305518554

Saaranen-Kauppinen, A. & Puusniekka, A. (2009). *Menetelmäopetuksen tietovaranto KvaliMOTV - Kvalitatiivisten menetelmien verkko-oppikirja*. Yhteiskuntatieteellinen tietoarkisto Tampereen yliopisto, Tampere.

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto*. Helsinki. ISSN: 1795-6323. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Sayegh, E. (28.2.2023). *APT28 Aka Fancy Bear: A Familiar Foe By Many Names*. Forbes. https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/?sh=4b56faa759ad

Schneider, M. Watts, J. & Shoard, P. (2022). *Innovation Insight for Attack Surface Management*. Gartner. https://www.gartner.com/document/4012816?ref=solrAll&refval=398019701&

Shodan. (2023). *Shodan - Search Engine for the Internet of Everything*. https://www.shodan.io/

SOCRadar. (2023). *Socradar – Extended Threat Intelligence -verkkosivu*. https://socradar.io/extended-threat-intelligence/

Soikkeli, M. (2021). *Lainsäädäntö tieto- ja kyberturvallisuuden perustana – valtionhallinnon viranomaisen näkökulma pro gradu -tutkielma*. Jyväskylän yliopisto. http://urn.fi/URN:NBN:fi:jyu-202105303303

Stranger, J. (26.6.2020). *Popular Cybersecurity Models*. CompTIA. https://www.comptia.org/blog/think-like-a-hacker-3-cybersecurity-models-used-to-investigate-intrusions

Sääskilahti, T & Mustonen, E. (2023). *Riskienhallinnan käsikirja valtionhallinnon toimijoille*. Hallintopolitiikka, Valtiovarainministeriön julkaisuja – 2023:54, Helsinki. http://urn.fi/URN:ISBN:978-952-367-633-6

Theisen, C., Munaiah, N., Al-Zyoud, M., Carver J.C., Meneely, A. & Williams, L. (2018). Attack Surface Definitions: A Systematic Literature Review. Teoksessa *Information and Software Technology Volume 104, December 2018* (s. 94-103). https://doi.org/10.1016/j.infsof.2018.07.008

ThreatCop. (2021). *Revil Group: Notorious Ransomware*. https://threatcop.com/blog/revil-group/

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi.

Ulkoministeriö. (2020). *Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaisille*. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Vainu. (2024). *Vainun yritystietokanta -internetsivu*. Vainu.Io Software Oy. https://vainu.io

Valli, R. & Aaltola, J. (2018). *Ikkunoita tutkimusmetodeihin 1*. (5. painos). PS-Kustannus, Jyväskylä.

Vehkalahti, K. (2014). *Kyselytutkimuksen mittarit ja menetelmät*. Finn Lectura.

Walls, A., McMullen, L., Heiser, J. & Gopal, D. (2023). *Maverick Research: Risk Management Produces Bad Cybersecurity*. Gartner. https://www.gartner.com/document/4327099?ref=solrAll&refval=398019825&

Wang, Z. (2022). *A Systematic Literature Review on Cyber Threat Hunting*. University of Guelph, Ontario. https://arxiv.org/pdf/2212.05310.pdf

Zhang, J. & Perkins, E. (2019). *Maverick Research: Don't Care Too Much About Cyber Risk*. Gartner. https://www.gartner.com/document/3942062?ref=solrAll&refval=398019947&

# LIITE 1 KYSELYN SAATEVIESTI

**POHJUSTUS**

Tämä kysely liittyy pro gradu -tutkimukseen, jossa pyritään tunnistamaan yritysten mielipiteitä ja havaintoja perinteisestä informaatioturvallisuuden riskienhallinnasta, jonka keskiössä on vaikutuksen ja todennäköisyyden arviot riskien laajuuden tunnistamisessa. Lisäksi pyritään tunnistamaan trendejä yritysten toimintamalleista hyökkäyspinnan ja uhka-alttiuden hallintaan liittyvistä sovelluksista, palveluista ja toimintamalleista. Vastausaika kyselyyn on noin 30–60 minuuttia. Merkitse monivalintakysymyksissä valitsemasi vastausvaihtoehtosi vasemmalle puolelle X tai lihavoi kyseinen vastausvaihtoehto. Avoimissa kysymyksissä voit tarvittaessa kasvattaa laatikon kokoa. Kategorioiden lopussa on avoin laatikko, johon voi täydentää vastauksiaan tai antaa palautetta kyselyn kyseisestä osiosta.

Lähetäthän täytetyn vastauslomakkeen osoitteeseen [MUOKATTU]

Kiitos vastaamisesta jo etukäteen!

**TUTKIMUKSEN TAUSTAA**

Gartner on useissa tutkimuksissaan (Schneider, M. Watts, J. & Shoard, P, 2022; Walls, A., McMullen, L., Heiser, J. & Gopal, D., 2023; Zhang, J. & Perkins, E, 2019) tunnistanut viime vuosien aikana digitalisaation, esineiden internetin ja varjo-IT:n kasvattaneen yritysten hyökkäyspintaa merkittävästi. Kasvua on jopa niin paljon, ettei kaikkea hyökkäyspintaa kyetä yrityksessä tunnistamaan, muun muassa työntekijöiden käyttäessä sovelluksia ja laitteita, joita yritys ei ole työntekijöilleen antanut lupaa käyttää. Samalla sovellukset monimutkaistuvat ja niiden keskinäisintegraatio lisääntyy, kasvattaen samalla haavoittuvuuksien todennäköisyyttä. Tähän yhdistettynä uhkatoimijoiden kehittyminen yhä nopeammiksi, tehokkaammiksi ja enenevissä määrin näkymättömiksi, on yritysten jatkuvasti muuttuva ja kasvava hyökkäyspinta uusien ja tuntemattomien uhkien kohteena. Riski voi muodostua yhä useammin tuntematonta hyökkäyspintaa pitkin yritykseen, johon liian staattinen ja joidenkin tutkijoiden mielestä ”perinteiseksi” mielletty informaatioturvallisuuden riskienhallinta välttämättä riitä.

Kyselyssä tietoturvapoikkeamalla tarkoitetaan seuraavaa: ”yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti” (Turvallisuuskomitea, 2018). Eli tässä tulee huomioida prosessi- ja konfiguraatiovirheiden ja vahinkojen takia tapahtuneet poikkeamat, mutta lisäksi myös henkilöön kohdistuneet toimet kuten kalastelu.

**VASTAUSTEN KÄYTTÖ**

Vastaukset anonymisoidaan lopullisessa tutkimuksessa, joskin vastaajia ryhmitellään mahdollisiin kategorioihin yrityksen koon tai toimialan pohjalta kuten ”*keskisuuret yritykset*” tai ”*tietoturva-auditointeja tekevät yritykset*”. Vastauslomakkeita säilytetään tutkimuksen valmistumisen jälkeen pseudonymisoidussa muodossa vielä 6 kuukautta, jonka jälkeen ne tuhotaan. Tämä ajankohta on arviolta marraskuussa 2024.

# LIITE 2 KYSELYLOMAKE

**KATEGORIA 1. Riskienhallinnan toteutus ja taustatiedot**

1. Toteutamme kyberturvallisuuden riskienhallinnan prosessia seuraavasti:

   (Voit vastata standardin tai viitekehyksen nimellä. Jos prosessinne poikkeaa suuresti alan yleisimmistä malleista, niin avaisitteko asiaa lyhyesti.)

2. Yrityksemme tekninen hyökkäyspinta on kasvanut merkittävästi viimeisen 5 vuoden aikana (IoT, lisääntyvä laitekanta, verkon laajennukset)
   __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

3. Yritykseemme on viimeisen 5 vuoden aikana vuosittaisena keskiarvona tarkasteltuna kohdistunut tietoturvapoikkeamia määrällisesti seuraavasti (Vastaa luvulla):

   ____

   Kuvaa lyhyesti yllä olevaa vastaustasi poikkeamien kriittisyyden, laajuuden ja vaikutuksen kautta.

4. Yritykseemme on kohdistunut kyberpoikkeama aiemmin täysin tuntematonta hyökkäyspintaa pitkin (huomioi esimerkiksi varjo-IT)
   __ Kyllä __ Ei

5. Yrityksessämme on tunnistettu varjo-IT:tä. Jos vastasit ”Kyllä” avaathan vastaustasi
   __ Kyllä __ Ei

6. Koemme yrityksessä olevamme täysin tietoisia koko hyökkäyspinnastamme
   __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

Avoin kommentointi ja palaute 1. kategorian kysymyksiin:

**KATEGORIA 2. Riskienhallinnan ja hyökkäyspinnan hallinnan mieltäminen**

7. ”*Hyökkäyspinnan pienentämisellä*” voi mielestäni tarkoittaa vaikkapa henkilöstön vähentämistä, sillä tällöin onnistuneen massakalasteluyrityksen mahdollisuudet heikkenevät. Hyökkäyspintaa ei siis sovi mieltää pelkästään teknisinä asioina kuten sovellushaavoittuvuuksina.
   __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

8. Jatkuva hyökkäyspinnan kasvu haittaa merkittävästi kyberturvallisuuden riskienhallinnan onnistunutta toteuttamista.
   __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

9. Uskon, että riskienhallintaprosessia läpikäydessämme, yritykseemme kohdistuvia mahdollisia uhkia jää varmasti tunnistamatta.
   __ Ei jää tunnistamatta __ Hyvin vähän __ Jonkin verran __ Paljon

10. Riskienhallinnan prosessi tuottaa mielestäni vain suuntaa antavan kuvan yritykseen kohdistuvista uhkista ja riskeistä. (Mieti asioita kuten uhkan todennäköisyyden ja vaikutuksen arvioinnin realistisuus. Jos tiedät realisoituja uhkia, niin kuinka hyvin ennustetut arviot vaikutuksesta ja todennäköisyydestä vastasivat todellisuutta? Onko hyvin todennäköiseksi arvioitu uhka jäänyt realisoitumatta tai onko matalan vaikutuksen uhka tehnytkin arvioitua suurempaa tuhoa?)
    __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

11. Koen perinteisten riskienhallintamallien olevan lähinnä välttämätön paha, jota säädökset ja yritysmaailma vaativat.
    __ Täysin eri mieltä __ Osittain eri mieltä __ Osittain samaa mieltä __ Täysin samaa mieltä

Avoin kommentointi ja palaute 2. kategorian kysymyksiin:

**KATEGORIA 3. Hyökkäyspinnan hallintaan ja uhkametsästykseen liittyvien sovellusten ja palveluiden käyttö**

Jos koet, että vastauksesi on laajempi kuin ”Kyllä” tai ”Ei”, täydennäthän vastaustasi kysymysten alla oleviin laatikoihin. Alla olevia toiminnallisuuksia on usein yrityksissä täysin ulkoistettu, jolloin pyrithän vastaamaan niin tarkasti kuin tiedät. Myös ulkoistetun palvelun tarjoavan yrityksen nimi on hyvä tieto.

12. EASM (*External Attack Surface Management*) on sovellus tai palvelu, joka tunnistaa yrityksen hallussa olevat ja julkiseen internetiin näkyvät sovellukset, mutta tämän lisäksi myös kolmannen osapuolen palveluissa olevat haavoittuvaiset tiedot ja palvelut tai sellainen informaatio, joka voi mahdollistaa hyökkäyksen yritystä kohtaan. (Esim. Group-IB tai Bitsight). Käytämme tällaista sovellusta tai palvelua.
    __ Kyllä __ Ei

13. DRPS (Digital Rights Protection Service) on sovellus tai palvelu, jolla julkisesta internetistä pyritään tunnistamaan sosiaalisen median kaappauksia, brändin varastamista, yritykseen kohdistuvia kalasteluyrityksiä tai arkaluontoisen materiaalin vuotamista julkisuuteen (Esim. SOCRadar tai Cyberint). Käytämme tällaista sovellusta tai palvelua.
    __ Kyllä __ Ei

14. CAASM (Cyber Asset Attack Surface Management) on sovellus, joka on ohjelmistorajapintojen avulla kokonaisvaltaisesti yrityksen kaikkeen kyberomaisuuteen integroitu järjestelmä, joka valvoo sisäisiä sekä ulkoisia uhkia ja hallinnoi mahdollisia haavoittuvuuksia (Esim. Axonius). Käytämme tällaista sovellusta tai palvelua.
    __ Kyllä __ Ei

15. Arvioi riskienhallintaprosessinne ajallista luonnetta, staattisuutta ja dynaamisuutta asteikolla **1–5 (vastaa yhdellä luvulla)**:
    **1**: Riskienhallintaprosessimme tehtiin aikanaan ja se on pysynyt sellaisenaan jo vuosia.
    **2:** Jotain 1 ja 3 väliltä
    **3**: Prosessimme on tasaisin väliajoin ja lähes täysin ihmisten toimesta toteutettu prosessi eikä sitä voi kuvailla reaaliaikaiseksi.
    **4**: Jotain 3 ja 5 väliltä
    **5**: Prosessimme on täysin reaaliaikainen, jota tukee kokonaisvaltaiset ja automatisoidut järjestelmät.

Avoin kommentointi, täydennykset ja palaute 3. kategorian kysymyksiin:

# LIITE 3 KYSYMYSTEN KORRELAATIOTAULUKKO

| | Koko | Toimiala | 2. | 6. | 7. | 8. | 9. | 10. | 11. | 12. | 13. | 14. | 15. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. Yrityksemme tekninen hyökkäyspinta on kasvanut merkittävästi viimeisen 5 vuoden aikana | 0,306 | -0,618 | - | | | | | | | | | | |
| 6. Koemme yrityksessä olevamme täysin tietoisia koko hyökkäyspinnastamme | -0,052 | 0,881 | -0,778 | - | | | | | | | | | |
| 7. "Hyökkäyspinnan pienentämisellä" voi mielestäni tarkoittaa vaikkapa henkilöstön vähentämistä | 0,235 | -0,187 | -0,335 | 0,091 | - | | | | | | | | |
| 8. Jatkuva hyökkäyspinnan kasvu haittaa merkittävästi kyberturvallisuuden riskienhallinnan onnistunutta toteuttamista. | -0,129 | -0,226 | 0,288 | -0,417 | -0,112 | - | | | | | | | |
| 9. Uskon, että riskienhallintaprosessia läpikäydessämme, yritykseemme kohdistuvia mahdollisia uhkia jää varmasti tunnistamatta. | 0,450 | 0,046 | -0,296 | 0,354 | -0,162 | -0,046 | - | | | | | | |
| 10. Riskienhallinnan prosessi tuottaa mielestäni vain suuntaa antavan kuvan yritykseen kohdistuvista uhkista ja riskeistä | -0,580 | 0,508 | -0,811 | 0,540 | 0,295 | -0,254 | 0,000 | - | | | | | |
| 11. Koen perinteisten riskienhallintamallien olevan lähinnä välttämätön paha, jota säädökset ja yritysmaailma vaativat | 0,271 | 0,475 | -0,434 | 0,750 | 0,552 | -0,204 | 0,098 | 0,267 | - | | | | |
| 12. Käytämme EASM-sovellusta tai -palvelua | 0,311 | -0,240 | 0,311 | -0,167 | -0,548 | -0,417 | 0,354 | -0,540 | -0,417 | - | | | |
| 13. Käytämme DRPS-sovellusta tai -palvelua | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | - | | |
| 14. Käytämme CAASM-sovellusta tai -palvelua | 0,311 | -0,240 | 0,311 | -0,167 | -0,548 | -0,417 | 0,354 | -0,540 | -0,417 | 1,000 | 0,000 | - | |
| 15. Arvioi riskienhallintaprosessinne ajallista luonnetta, staattisuutta ja dynaamisuutta asteikolla 1–5 | 0,526 | -0,379 | -0,208 | -0,070 | 0,314 | -0,487 | 0,545 | 0,000 | -0,114 | 0,420 | 0,000 | 0,420 | - |

# LIITE 4 TARKISTUSLISTA JA OHJE HYÖKKÄYSPINNAN HALLINNASTA YRITYKSELLE

Ohjeen tarkoituksena on esittää johdattelevia kysymyksiä ja väittämiä yritykselle, luoden lukijalle selkeän kuvan siitä, onko heidän tarpeen harkita hyökkäyspinnan ja uhka-alttiuden hallinnan toimintamalliensa päivittämistä esimerkiksi EASM-, CAASM- ja/tai DRPS-sovelluksia tai -palveluita hyödyntämällä. Riittävä kyllä-vastausten määrä viittaa siihen, että yrityksen kannattaa harkita kyseisiä sovelluksia.

Ohjeen toisella sivulla on tarkennukset jatkotoimenpiteitä varten.

| | | Kyllä | Ei |
|---|---|---|---|
| 1 | Onko yrityksen hyökkäyspinta kasvanut lähivuosina esimerkiksi digitalisaation, pilvipalveluiden myötä? Tämä kasvu tulee todennäköisesti jatkumaan, jolloin hyökkäyspinnan hallinta monimutkaistuu, ja vaatii entistä enemmän automatisointia. | | |
| 2 | Jos yritys on julkisesti merkittävä, hyökkääjien kiinnostus sitä kohtaan voi olla normaalia korkeampaa helpon avointen lähteiden tiedustelun myötä. Onko yritys julkisesti merkittävä? | | |
| 3 | Jos yrityksessä on aikaisemmin tunnistettu varjo-IT:tä, on sitä mahdollisesti edelleenkin käytössä. Tämän varjo-IT:n tunnistaminen suuressa yrityksessä voi olla hyvin hankalaa. Onko varjo-IT:tä on tunnistettu? | | |
| 4 | Onko samaa toimenpidettä tai hyvin samaa tarkoitusta varten olevia sovelluksia useita? | | |
| 5 | Julkiset ja kaupalliset versionhallintapalvelut kuten Github vastaavat muun muassa varmuuskopioinnista. Näihin valuu aika ajoin julkista tietoa yritykseltä, joka olisi pitänyt pitää salassa. Salasanat ja avaimet ovat esimerkkejä näistä tiedoista. Käytetäänkö varmuuskopiointiin julkisia repositoryjä? | | |
| 6 | Riskienhallinnan perusteet tulisivat muuttua uhkakentän muuttuessa. Uhkakenttä päivittyy jatkuvasti. Onko yrityksen riskienhallintaprosessi hyvinkin staattinen? | | |
| 7 | Onko yrityksen imagoa tai brändiä kopioitu tai tahrattu verkossa, esimerkiksi käyttämällä yrityksen logoja tai muuta brändiin liittyvää tieto-omaisuutta? | | |
| 8 | Onko jokin ulkoinen toimija lähetellyt kalasteluviestejä tai muuta haitallista verkkoliikennettä yrityksen nimissä? | | |
| 9 | Kokeeko yritys olevansa edes osin epävarma omasta hyökkäyspinnastaan? | | |
| 10 | Kokeeko yritys, että perinteinen vaikutukseen ja todennäköisyyteen perustuva riskienhallinta ei välttämättä anna kaikkea turvaa, joka siltä haluttaisiin? | | |
| 11 | Onko yritys kohdannut tietoturvapoikkeamia viime vuosina? | | |
| 12 | Yrityksen käytössä ei ole uhkametsästykseen liittyviä palveluita. | | |

Jos vastasit yli puoleen vastauksista "Kyllä" on hyvin todennäköistä, että yrityksenne kannattaa tutustua EASM-, CAASM- ja DRPS-palveluihin ja -sovelluksiin, tai muihin keinoihin hallita hyökkäyspintaa. Kyseiset sovelluskategoriat ovat vielä kehityksen alkuvaiheessa, ja ne eivät ole markkinoillaan nostaneet päätään merkittävästi vuoden 2024 alussa.

**EASM (External Attack Surface Management)** on kokoelma prosesseja, teknologioita ja palveluita, jotka havainnoivat ulkoisia yrityksen sovelluksia, yrittäen tunnistaa näistä poikkeamia, jotka voivat aiheuttaa uhkan yritykselle. Sovelluksen tulisi tunnistaa tietysti yrityksen omassa hallussaan olevat palvelut, järjestelmät ja sovellukset, mutta tämän lisäksi myös kolmannen osapuolen palveluissa olevat haavoittuvaiset tiedot, tai sellainen informaatio, joka voi mahdollistaa hyökkäyksen yritystä kohtaan.

**CAASM (Cyber Asset Attack Surface Management)** on sovellus, jonka tarkoituksena on tuottaa näkyvyys yrityksen kaikesta ulkoisista ja sisäisistä kyber-asseteista ohjelmistorajapintoja hyödyntäen. CAASM toimii automaattisen haavoittuvuusskannerin tavoin, mutta huomattavasti monipuolisemmin. Se tunnistaa haavoittuvuudet, ilmoittaa niistä, ja jatkuvasti analysoi ja priorisoi uhkia sekä esittää ongelmilla korjausehdotuksia.

**DRPS (Digital Rights Protection Services)** on palvelu, jolla julkisesta internetistä pyritään tunnistamaan imagoon ja brändiin liittyviä uhkia kuten brändin varastamista, sosiaalisen median kaappauksia, kalasteluyrityksiä tai arkaluonteisen materiaalin vuotamista julkisuuteen. Se valvoisi esimerkiksi pimeää verkkoa ja antaa hälytyksen poikkeaman ilmetessä. Toisaalta se myös huomaisi ajoissa, jos esimerkiksi Facebookiin yritetään tehdä valetiliä yrityksen nimellä.

**Hyökkäyspinnan minimoinnin** periaatteena on se, että kaikkia uhkia ei pystytä koskaan torjumaan, mutta mahdollisia hyökkäyksiä voidaan vähentää minimoimalla uhkatoimijan mahdollisuudet vaikuttaa järjestelmiin. Tämä tarkoittaa sitä, ettei käytetä useita samankaltaisia sovelluksia tai avoimia portteja. Lisäksi hyökkäyspinnan minimoimisessa yritykselle on tärkeätä ymmärtää mitä kaikkea omaan hyökkäyspintaan kuuluu. Sovellusten, palveluiden, järjestelmien ja toimintamallien tarkka listaus on siis hyökkäyspinnan minimoinnin keskiössä. Kaikkia näitä toiminnallisuuksia ei välttämättä kyetä omin keinoin edes tunnistamaan, jolloin ulkoinen penetraatiotestaus tai yllä esitetyt sovellukset tukevat tämän tiedonkeräämisen toteuttamisessa.

**Proaktiivinen ja jatkuva hallinta** mahdollistaa uhkiin reagoimisen ennen kuin uhka on kohdistunut omaan yritykseen. Tämä tarkoittaa sitä, että mahdolliset vuotaneet salasanat onnistutaan tunnistamaan, ennen kuin kukaan asiaankuulumaton on niillä päässyt kirjautumaan yrityksen palveluihin. Uhkakentän kehittyessä hyvin nopeaan tahtiin ovat myös uudet haavoittuvuudet, hyökkäysvektorit ja toimintamallit muuttumassa jatkuvasti. Liian staattinen ja hidas prosessi riskien tunnistamisessa ja arvioinnissa voi johtaa siihen, että yritys saa uhkasta tiedon vasta liian myöhään.

**Illuusio turvallisuudesta** on periaate, jota voi välillä kuulla puhuttaessa tietoturvasta. Yritys, joka ei ole tunnistanut varjo-IT:tä tai tietoturvapoikkeamia, ei välttämättä ole kuitenkaan turvassa niiltä. Monikaan hyökkäys ei paljastu heti tekohetkellä, vaan voi mennä jopa viikkoja, ennen kuin hyökkäys tunnistetaan ja sen torjuntatoimet aloitetaan. Tietoturvasta päättävän henkilön on siis kriittisesti arvioitava omaa käsitystä yrityksen tietoturvasta, eikä tuudittautua siihen turvallisuudentunteeseen, jota palveluntarjoajille ulkoistetut palvelut tarjoavat. Hyökkäyspinnan hallinnassa alleviivaavana periaatteena onkin täyden näkyvyyden saaminen koko hyökkäyspintaan.