TRAFICOM
Liikenne- ja viestintävirasto

Tietoturvan kehittämisen tuen arviointi

Arviointi

Heidi Uitto
Kimmo Halme
Vesa Salminen
Timo Kotilainen

Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar
Traficom Research Reports

07/2026

TRAFICOM
Liikenne- ja viestintävirasto

Julkaisupäivämäärä
3.6.2026

Julkaisun nimi
Tietoturvan kehittämisen tuen arviointi

Tekijät
Heidi Uitto, Kimmo Halme, Vesa Salminen & Timo Kotilainen

Toimeksiantaja ja asettamispäivämäärä
Liikenne- ja viestintävirasto Traficom 13.12.2024

Julkaisusarjan nimi ja numero
Traficomin tutkimuksia ja selvityksiä 7/2026
ISSN (verkkojulkaisu) 2669-8781
ISBN (verkkojulkaisu) 978-952-425-028-3

Avainsanat
Tieto- ja kyberturva, tietoturvan kehittämisen tuen arviointi, tietoturvaseteli

Tiivistelmä
Arvioinnissa tarkasteltiin vuosina 2022–2024 myönnetyn tietoturvan kehittämisen tuen suoria ja epäsuoria vaikutuksia. Tuen tarkoituksena oli edistää Suomessa toimivien yhteiskunnan toiminnan kannalta kriittisillä toimialoilla toimivien yritysten tietoturvallisuutta ja kykyä torjua, havaita ja selvittää tietoturvaloukkauksia. Arvioinnin keskeisiä menetelmiä ja tietolähteitä olivat hankeselvitysten ja rahoitusaineistojen analysointi, tuensaajille suunnattu kysely, yrityshaastatteluthaastattelut ja kirjallisuuskatsaus.

Tietoturvan kehittämisen tukea voidaan arviointiaineiston perusteella pitää pääosin oikeasuhtaisena ja tarkoituksenmukaisena välineenä edistää yllä mainittua tavoitetta. Tietoturvasetelin suorissa vaikutuksissa korostuu käytännönläheinen kehittäminen ja osaamisen vahvistaminen. Pitkällä aikavälillä suurimmat hyödyt liittyvät resilienssiin ja tehokkuuteen. Tuen lisäisyys oli pieniä hankkeita ajatellen selvästi kiihdyttävä. 91 % ilmoitti, ettei hanke olisi toteutunut lainkaan tai olisi toteutunut vain osittain ilman tukea. Suurissa hankkeissa vastaava vaikutus oli rajallisempi 16 % toimenpiteistä olisi tehty joka tapauksessa. Tietoturvan kehittämisen tuella voidaan havaita olleen joitain epäsuoria vaikutuksia markkinoihin, muihin yrityksiin ja koko yhteiskunnan kyberturvallisuuskyvykkyyteen, mutta sen rajallisesta koosta johtuen epäsuorat vaikutukset jäävät suhteellisen pieniksi. Tietoturvaseteli on lisännyt tietoturvatuotteiden ja palveluiden kysyntää. Rahoitetuissa hankkeissa toteutettiin hankintoja suoraan noin 7,4 miljoonalla eurolla. Tämän lisäksi tuki vivutti yrityksiltä omarahoitusta vähintään noin 3,3 miljoonaa euroa. Tuen tärkein epäsuora vaikutus liittyy sen yhteiskunnalliseen rooliin. Se on vahvistanut kriittisten alojen toimitusketjujen tietoturvaa ja lisännyt pk-yritysten valmiuksia toimia osana kansallisesti merkittäviä ekosysteemejä.

Arvioinnissa suositellaan, että tukea tulisi jatkaa osana kansallista kyberturvallisuuspolitiikkaa ja huoltovarmuusjärjestelmää, mutta sen ehtoja ja kohdentamista tulisi tarkentaa. Vaikuttavuutta voitaisiin lisätä mm. tarjoamalla neuvontaa ja verkostoja sekä ottamalla kunnalliset toimijat tuen piiriin.

Yhteyshenkilö
Markus Savolainen

Raportin kieli
Suomi

Luottamuksellisuus
Julkinen

Kokonaissivumäärä
55

Jakaja
Liikenne- ja viestintävirasto Traficom

Kustantaja
Liikenne- ja viestintävirasto Traficom

TRAFICOM
Transport- och kommunikationsverket

Utgivningsdatum
3.6.2026

Publikation
Utvärdering av stödet för utveckling av informationssäkerheten

Författare
Heidi Uitto, Kimmo Halme, Vesa Salminen & Timo Kotilainen

Tillsatt av och datum
Transport- och kommunikationsverket Traficom 13.12.2024

Publikationsseriens namn och nummer
Traficoms forskningsrapporter och utredningar 7/2026
ISSN (elektronisk publikation) 2669-8781
ISBN (elektronisk publikation) 978-952-425-028-3

Ämnesord
Stöd för utveckling av informationssäkerheten, informationssäkerhetssedel

Sammandrag
I utvärderingen granskades de direkta och indirekta effekterna av det stöd för utveckling av informationssäkerheten som beviljats under åren 2022–2024. Syftet med stödet var att främja informationssäkerheten hos företag inom branscher som är kritiska med tanke på samhällets funktion i Finland samt att stärka deras förmåga att förebygga, upptäcka och utreda informationssäkerhetsincidenter. De centrala metoderna och informationskällorna i utvärderingen var analys av projektrapporter och finansieringsmaterial, en enkät riktad till stödmottagarna, företagsintervjuer samt en litteraturöversikt.

Utifrån utvärderingsmaterialet kan stödet för utveckling av informationssäkerheten i huvudsak betraktas som ett proportionerligt och ändamålsenligt styrmedel för att främja det ovan nämnda målet. De direkta effekterna av informationssäkerhetssedeln handlar i första hand om praktiskt utvecklingsarbete och förstärkning av kompetensen. På längre sikt är de största nyttorna kopplade till ökad resiliens och effektivitet. Stödets additionalitet var tydligt påskyndande i fråga om mindre projekt: 91 procent av stödmottagarna uppgav att projektet inte skulle ha genomförts alls, eller endast delvis, utan stödet. I större projekt var motsvarande effekt mer begränsad: 16 procent av åtgärderna skulle ha genomförts oberoende av stödet.

Stödet för utveckling av informationssäkerheten har också haft vissa indirekta effekter på marknaden, på andra företag och på samhällets samlade informations- och cybersäkerhetsförmåga, men på grund av stödets begränsade omfattning förblir dessa indirekta effekter relativt små. Informationssäkerhetssedeln har ökat efterfrågan på produkter och tjänster inom informationssäkerhet. I de projekt som finansierats inom ramen för stödet genomfördes upphandlingar till ett belopp av cirka 7,4 miljoner euro. Utöver detta mobiliserade stödet minst cirka 3,3 miljoner euro i företagens egen finansiering. Den viktigaste indirekta effekten hänför sig till stödets samhälleliga roll: stödet har stärkt informationssäkerheten i leveranskedjor inom kritiska branscher och förbättrat små och medelstora företags beredskap att verka som en del av nationellt betydelsefulla ekosystem.

I utvärderingen rekommenderas att stödet fortsätter som en del av den nationella cybersäkerhetspolitiken och försörjningsberedskapssystemet, men att villkoren och inriktningen preciseras. Stödets genomslag kan förbättras bland annat genom att erbjuda rådgivning och möjligheter till nätverkande samt genom att utvidga kretsen av stödberättigade aktörer till att omfatta även kommunala aktörer.

Kontaktperson
Markus Savolainen

Språki
Finska

Sekretessgrad
Offentlig

Sidonantal
55

Distribution
Transport- och kommunikationsverket Traficom

Förlag
Transport- och kommunikationsverket Traficom

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
3rd of June 2026

Title of publication
Evaluation of the Support for the Development of Information Security

Author (s)
Heidi Uitto, Kimmo Halme, Vesa Salminen & Timo Kotilainen

Commissioned by, date
Finnish Transport and Communications Agency Traficom, 13th of December 2024

Publication series and number
Traficom Research Reports 7/2026
ISSN (e-publication) 2669-8781
ISBN (e-publication) 978-952-425-028-3

Keywords
The information security voucher, the support for the development of information security

Abstract
The evaluation examined the direct and indirect impacts of the support for the development of information security granted in 2022–2024. The purpose of the support was to promote the information security of companies operating in sectors critical to the functioning of society in Finland, and to strengthen their ability to prevent, detect and investigate information security breaches. The key methods and data sources used in the evaluation were the analysis of project reports and funding data, a survey addressed to support recipients, company interviews and a literature review.

Based on the evaluation data, support for the development of information security can be considered a mainly proportionate and appropriate instrument for promoting the above objective. The direct impacts of the information security voucher focus on practical development work and strengthening of competence. In the longer term, the greatest benefits relate to improved resilience and efficiency. The additionality of the support was clearly accelerating in the case of small projects: 91% of respondents stated that the project would not have been implemented at all or would only have been implemented in part without the support. For larger projects, the corresponding effect was more limited: 16% of the measures would have been carried out in any case.

The support for the development of information security has also had some indirect impacts on markets, other companies and the overall information security and cyber security capability of society, but due to the limited volume of the scheme these indirect impacts remain relatively modest. The information security voucher has increased demand for information security products and services. The projects funded under the scheme led to direct procurements of approximately EUR 7.4 million. In addition, the support leveraged at least approximately EUR 3.3 million in companies' own funding. The most important indirect impact relates to the societal role of the scheme: it has strengthened the information security of supply chains in critical sectors and improved the preparedness of SMEs to operate as part of nationally significant ecosystems.

The evaluation recommends that the support be continued as part of national cyber security policy and the security of supply system, while clarifying its conditions and targeting. The effectiveness of the scheme could be enhanced, for example, by providing advisory services and networking opportunities and by expanding the scope of eligible applicants to include municipal actors.

Contact-person
Markus Savolainen

Language
Finnish

Confidence status
Public

Pages, total
55

Distributed by
Finnish Transport and Communications Agency Traficom

Published by
Finnish Transport and Communications Agency Traficom

Sisällys

1 Johdanto

1.1 Arvioinnin tausta ja tavoitteet

Liikenne- ja viestintävirasto Traficom (jatkossa Traficom) on myöntänyt vuosina 2022-2024 Tietoturvan kehittämisen tukea (ns. tietoturvaseteli), jonka tavoitteena on ollut auttaa yhteiskunnan kannalta kriittisten alojen yrityksiä nostamaan nopeasti kyberturvallisuuden tasoaan ja tekemään kohdennettuja kyberturvallisuutta parantavia toimenpiteitä. Kyberturvallisuuden tason nostaminen organisaatioissa näkyy vastaavasti muun muassa parempana tietosuojana kansalaisille. Tuen tavoitteena on ollut myös vauhdittaa suomalaisen kyberturvallisuustoimialan ja -markkinan kehitystä sekä luoda uutta liiketoimintaa toimialle ja kyberturvallisuusosaamista Suomeen parantaen muun muassa Suomen kyberturvallisuuden omavaraisuutta. Tuki on suunnattu Suomessa toimiville yrityksille, erityisesti mikro- ja pk-yrityksille, jotka toimivat kriittisillä toimialoilla ja tuottavat yhteiskunnalle elintärkeitä palveluja. Tuen avulla yritykset ovat voineet toteuttaa esimerkiksi tietojärjestelmien tarkastus- ja arviointitoimia, henkilöstön tietoturvakoulutusta, tietoturvatasoa parantavia hankintoja tai teknisiä testauksia.

Traficom tilasi ulkopuolisen arvioinnin Tietoturvan kehittämisen tuesta. Tavoitteena on ollut arvioida tuen suoria ja välillisiä vaikutuksia, sekä tuen oikeasuhtaisuutta ja tarkoituksenmukaisuutta. Tarkemmat arviointikysymykset on esitetty Taulukossa 1.

Kilpailutuksen perusteella arvioinnin toteuttajaksi valittiin Forefront Oy. Arviointi on toteutettu syksyllä 2025 ja käsillä oleva raportti kokoaa yhteen arvioinnin tulokset.

Taulukko 1. Arviointikysymykset

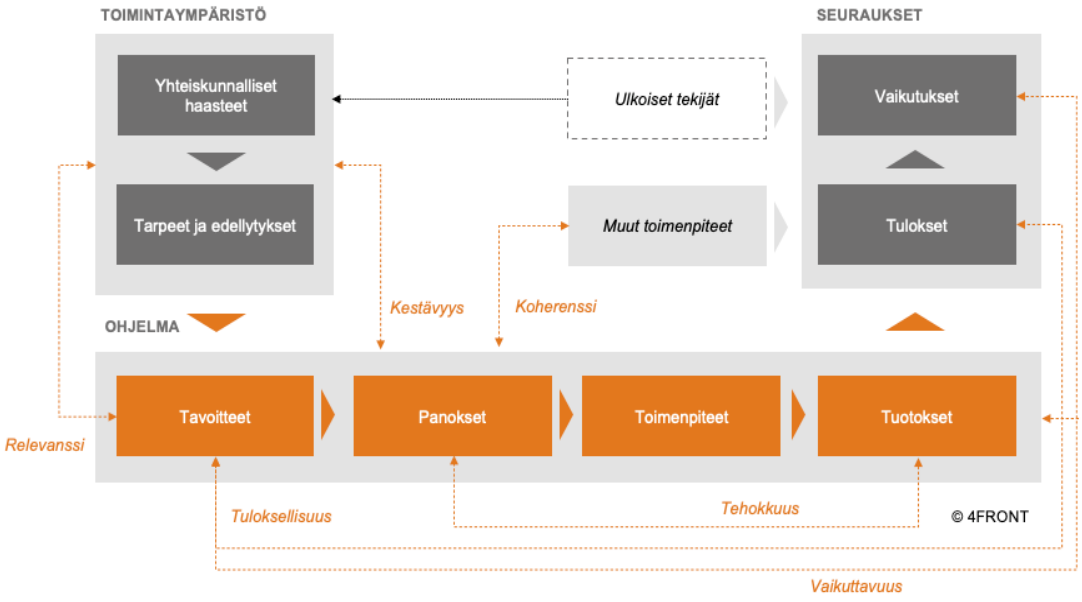
Kategoria	Arviointikysymykset
Suorat lyhyen ja pitkän ajan vaikutukset tuen saajiin	Miten tuki on vaikuttanut tuensaajien omaan tietoturvallisuuteen? Missä määrin tuki on edistänyt tuensaajien omaa tietoturvallisuutta parantavien toimenpiteiden toteuttamista (kannustava vaikutus)? Missä määrin toimenpiteet olisivat jääneet toteuttamatta ilman tukea? Missä määrin tuki on vastannut tuensaajien yritysten tarpeisiin? Missä määrin tuki on vaikuttanut tuensaajien kilpailukykyyn/kilpailutilanteeseen (kilpailuvaikutukset)? Missä määrin tuella on ollut odotetut vaikutukset? Miten tuki on vaikuttanut eri tuensaajiin yrityksen koon, sijainnin ja toimialan mukaan?
Lyhyen ja pitkän ajan välilliset vaikutukset	Miten tuki on vaikuttanut suomalaisten kyberturvallisuusalan yrityksiin ja niiden harjoittamaan liiketoimintaan? Miten tuki on vaikuttanut muihin yrityksiin? Miten tuki on vaikuttanut yhteiskunnan kyberturvallisuuskapasiteettiin?
Oikeasuhtaisuus ja tarkoituksenmukaisuus	Missä määrin tuki on ollut oikeassa suhteessa ratkaistaviin ongelmiin? Missä määrin sama vaikutus olisi voitu saada aikaan vähemmällä tuella tai erilaisella tukimuodolla? Missä määrin sama vaikutus olisi voitu saada aikaan muilla toimenpiteillä? Missä määrin valittu tukiväline oli tehokkain ja olisiko muut tukivälineet olleet tehokkaampia?

1.2 Arvioinnin menetelmät ja aineistot

1.2.1 Lähestymistapa ja viitekehys

Arvioinnin lähestymistapa perustuu kansainvälisten käytäntöjen ja kriteerien pohjalta kehitettyyn interventiologiikkaan ja muutosteoriaan (Kuvio 1). Arvioinnissa on tarkasteltu erityisesti seuraavia viitekehyksen mukaisia kriteereitä ja näkökulmia.

- **Relevanssi** eli tuen tarkoituksenmukaisuus suhteessa toimintaympäristön ja tuensaajien tarpeisiin.
- **Tehokkuus** eli tuen toimivuus ja kehitystarpeet suhteessa sen tuloksiin ja tavoitteisiin.
- **Tuloksellisuus** eli ohjelman saavuttamat lyhyen aikavälin vaikutukset tuensaajien tietoturvaan.
- **Vaikutukset** kuvastavat laajemmin tuen synnyttämää muutosta yhteiskunnassa (ml. mahdolliset negatiiviset ja ei-aiotut vaikutukset).



Kuva 1. Arvioinnin viitekehys.

Viitekehyksen pohjalta rakennettiin uusi sovellettu malli, joka tuen mallintaa rahoitustuen vaikuttavuuspolkuja (katso kuvio 2, sivu 20). Tätä mallia hyödynnettiin kyselyssä, aineiston keruussa sekä analyysissä.

1.2.2 Arvioinnin menetelmät ja aineistot

Arviointi toteutettiin monimenetelmällisesti ja siinä yhdistettiin sekä laadullisia että määrällisiä aineistoja tuen vaikutusten ja kohdentumisen arvioimiseksi. Aineistona hyödynnettiin Traficomin asiantuntijoiden taustahaastatteluja, avustustietoja, tuensaajien hakemuksia ja selvityksiä tuen

käytöstä, sekä kansallista ja kansainvälistä kirjallisuutta. Lisäksi toteutettiin laaja tuensaajien kysely, jonka avulla kerättiin tietoa hankkeiden toteutuksesta, tuloksista ja hyödyistä, sekä syventäviä yrityshaastatteluja, jotka valottivat yksityiskohtaisemmin tuen vaikutuksia eri toimialojen yritysten tietoturvakyvykkyyksiin ja käytäntöihin.

Taulukko 1. Menetelmät ja aineistot

Menetelmä	Kuvaus
Dokumenttianalyysi	Tuen valmisteluun liittyvät dokumentit ja lausunnot, tukea koskeva lainsäädäntö, rahoituspäätöksiin liittyvät dokumentit (hakemukset ja loppuraportit).
Kirjallisuuskatsaus	Kirjallisuuskatsaus tarkasteli kriittisten alojen kypsyyttä ja tarpeita liittyen tietoturvaan.
Tuensaajien kysely	Kysely lähetettiin kaikille tuensaajille ja analysoitiin erikseen molemmille tukiluokille.
Haastattelut	Arvioinnissa haastateltiin Traficomin henkilökuntaa ja asiantuntijoita, sekä tehtiin neljä syventävää yrityshaastattelua.

Rajoitukset

Arvioinnissa käytetyt menetelmät, kuten kysely ja haastattelut, tuottavat luonteeltaan laadullista ja kokemuksellista tietoa, eivätkä siten mahdollista kausaalivaikutusten todentamista. Kyselyn vastausprosentti oli 36 (n=114, N=313) mikä on yrityskyselyissä suhteellisen hyvä, mutta ei kuitenkaan täysin kattava. Rahoitustietoja ja tuensaajien selvityksiä koskevassa analyysissä on mukana 100 % tuensaajista, joten näiden osalta tulokset ovat kattavat.

Estetyistä kyberhyökkäyksistä ja tietoturvaloukkauksista ei myöskään ole mahdollista muodostaa täydellistä kokonaiskuvaa, koska monilla yrityksillä ei ole itsellääänkään käytössään järjestelmiä tai lokitietoja, jotka antaisivat siitä täsmällisen tiedon.

2 Tausta ja konteksti

2.1 Tietoturvan kehittämisen tuki

Tietoturvan kehittämisen tuki on valtionavustuksena myönnettävä määräaikainen rahoitusmuoto, jonka tavoitteena on parantaa suomalaisyritysten kyberturvallisuutta ja yhteiskunnan kriittisten toimintojen häiriönsietokykyä. Tuki on suunnattu yrityksille, jotka toimivat kriittisillä toimialoilla, kuten energiahuolto, elintarvikehuolto, finanssiala, jätehuolto, logistiikka, tietoyhteiskuntapalvelut, media-ala, sosiaali- ja terveydenhuolto (mukaan lukien lääkehuolto), vesihuolto, rakennusteollisuus ja teknologiateollisuus, ja tuottavat yhteiskunnalle elintärkeitä toimintoja. Näiden toimialojen turvaaminen on keskeinen osa Suomen huoltovarmuutta ja kokonaisturvallisuutta.

Tukea säätelee Valtioneuvoston asetus tietoturvan kehittämisen tuesta (860/2022), joka tuli voimaan 1.12.2022 ja on voimassa vuoden 2025 loppuun. Asetus nojaa valtionavustuslakiin (688/2001). Tukiohjelma rahoitetaan valtion talousarviossa osoitetusta 6 miljoonan euron määrärahasta, ja sen hallinnoinnista vastaa Traficom. Myöntämisperuste on hakemusten saapumisjärjestys ja tuen myöntämisen ehtojen täyttyminen, eikä hakemuksia pisteytetä tai kilpailuteta.

Tuki on osa Suomen kyberturvallisuusstrategian toimeenpanoa ja liittyy laajempaan valtion pyrkimykseen parantaa yritysten kykyä varautua kyberturvallisuusuhkiin, jotka ovat lisääntyneet nopeasti muun muassa Venäjän hyökkäyssodan ja digitaalisen toimintaympäristön monimutkaistumisen myötä. Tuen valmistelu käynnistettiin vuonna 2022 Liikenne- ja viestintäministeriön johdolla, ja se perusteltiin tarpeella kohdistaa tukea erityisesti kriittisten alojen yrityksille, joiden toiminnan häiriöt voisivat vaikuttaa laajasti yhteiskunnan turvallisuuteen, talouteen tai väestön hyvinvointiin.

Tukea voidaan myöntää kahdessa luokassa:

- enintään 15 000 euron tuki, jota voivat hakea pk-yritykset tietojärjestelmien tarkastus- ja arviointityöhön, tietoturvaparannuksiin, henkilöstön koulutukseen tai muuhun osaamisen kehittämiseen,
- enintään 100 000 euron tuki, joka on tarkoitettu hyökkäyksenestotestaukseen, tärkeimpien sähköisten palveluiden varautumistason testaamiseen tai muuhun vastaavaan välittömään toimenpiteeseen.

Suurimman tukiluokan osalta edellytetään vähintään 30 prosentin omarahoitusosuutta, ja enintään kolmasosa tietoturvan kehittämisen tuelle osoitetusta 6 miljoonan euron kokonaismäärärahasta voidaan käyttää tähän tukimuotoon. Tuki on ns. vähämerkityksellistä (de minimis) tukea ja yksittäinen yritys tai konserni voi saada kolmen verovuoden aikana yhteensä enintään 300 000 euroa tällaista tukea.

Taulukko 3. Tukea koskevat perustiedot

Kansallisen koordinointikeskuksen tuki	
Tuen tavoite	Nostaa nopeasti yhteiskunnan toiminnan kannalta kriittisten alojen yritysten kyberturvallisuuden tasoa ja tehdä niissä kohdennettuja kyberturvallisuutta parantavia toimenpiteitä.
Kohderyhmä	Suomeen rekisteröidyt yhteiskunnan toiminnan kannalta kriittiset yritykset
Tukiluokat (kategoriat)	Enintään 15 000 euron tuki pk-yrityksille (ei omarahoitusosuutta) ja enintään 100 000 euron tuki kaikille yrityksille (omarahoitusosuus 30 %)

Tuen myöntämisajankohta	1.12.2022–31.12.2024
Myönnetyn tuen suuruus	Yhteensä 6 milj. euroa 371–15 000 euroa / hanke (15 000 euroa tuki) 19 504–100 000 euroa / hanke (100 000 euroa tuki)
Tukea saaneet yritykset (lkm)	313 kpl (hakemuksia 771 kpl)
Tuen käytön seuranta	Selvitys avustuksen käytöstä ja vaikutuksista yrityksen tietoturvaan (viim. 6 kk tuella katettavien kustannusten syntymisen jälkeen)

Hyväksyttäviä kustannuksia ovat muun muassa tietoturvaa parantavien välineiden, laitteiden ja lisenssien hankinnat, koulutukset ja osaamisen kehittäminen, tutkimus- ja kehitystyö, konsultointi, auditoinnit, penetraatiotestaukset sekä kotimaiset matkakulut ja materiaalihankinnat. Sen sijaan tuen hakemiseen liittyviä kustannuksia, konserni- tai intressiyhtiöiltä tehtyjä ostoja ja yrityksen omia palkkakuluja ei voida hyväksyä.

Valmistelun yhteydessä korostettiin erityisesti, että julkisen tuen tehtävänä ei ole korvata normaaleja liiketoimintakustannuksia vaan mahdollistaa sellaisia kehittämistoimia, joihin yrityksillä ei ilman tukea olisi ollut riittäviä resursseja. Asetus perusteltiin tarpeella nopeuttaa koko yhteiskunnan kyberturvallisuuden vahvistamista tilanteessa, jossa uhkataso on koholla ja monilla kriittisillä sektoreilla on merkittäviä osaamis- ja resurssivajeita.

Tuen hallinnointi keskitettiin Traficomin Kyberturvallisuuskeskukselle, joka mm. kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa kyberturvallisuuden tilannekuvaa. Tuen käyttöönotolla pyrittiin varmistamaan, että tuen myöntämisessä voidaan hyödyntää Kyberturvallisuuskeskuksen asiantuntemusta, tukea saavat yritykset voivat hyödyntää Kyberturvallisuuskeskuksen kansallisia ohjeita ja auditointimenetelmiä, ja että rahoitus tukee suoraan yhteiskunnan kokonaisturvallisuutta vahvistavia tavoitteita.

2.2 Kriittiset alat ja niiden maturiteetti Suomessa

Kyberturvallisuusympäristön haasteista huolimatta suomalaisen yrityskentän ja laajemmin koko yhteiskunnan kyberturvallisuus on ollut kansainvälisissä mittauksissa perinteisesti hyvä. Syitä tähän on ollut hyvä osaamistaso, toteuttavien tahojen välinen yhteistyö, teknologia- ja palveluntarjoajien korkea taso, kurinalaiset toimintaperiaatteet ja kielialueen pienuus. Tilanne on mahdollisesti muuttumassa ja etumatkamme kaventumassa.

Yhtenä vaikuttavana tekijänä on käytettävien teknologioiden globalistoituminen ja platformistuminen.

Digitalisaation ja teknisen kehittymisen myötä kyberturvallisuusuhkien merkitys koko yhteiskunnalle, yrityksille ja yksilöille kasvaa ja vielä kiihtyvästi. Kunkin toimijan ns. hyökkäyspinta laajenee ja monipuolistuu. Verkostoituneet toimintamallit lisäävät todennäköisyyksiä sille, että yhteen osaan kohdistuneet onnistuneet hyökkäykset vaikuttavat häiriöinä laajasti koko tuotanto- tai palveluketjussa. Tämä lisää varautumisen kompleksisuutta, teknologioiden moninaisuutta, osaamisvaatimuksia ja kustannuksia. Verkostoituneen toimintamallin riskit ovat kuitenkin hyvin tunnistettu ja EU-tasoinen NIS2-regulaatio[1] tuo, ainakin yhteiskunnan kriittisten toimijoiden osalta, tähän hyvän ja konkreettisen varautumismallin.

Suomen ja Euroopan kyberturvallisuuden toimintaympäristö on viime vuosina muuttunut nopeasti, mikä heijastuu suoraan myös tietoturvan kehittämisen tuen merkitykseen. Venäjän hyökkäys Ukrainaan, geopoliittinen jännite ja kriittisen infrastruktuurin kasvava digitalisoituminen ovat nostaneet kyberturvallisuuden keskeiseksi osaksi kansallista turvallisuus- ja elinkeinopolitiikkaa. *Traficomin vuoden 2023 katsauksen* mukaan Suomessa uhkataso pysyi koholla koko vuoden, ja yleisimmät uhat olivat palvelunesto-hyökkäykset, kiristyshaittaohjelmat, tietojenkalastelu ja valtiollinen vakoilu, joiden kohteena olivat erityisesti julkishallinnon, logistiikan ja terveydenhuollon palvelut. Tämä vahvistaa tarvetta tukea erityisesti kriittisiä sektoreita ja niiden alihankintaverkostoja, jotka ovat altteimpia hyökkäyksille ja joilla on suurimmat yhteiskunnalliset vaikutukset.

Huoltovarmuuskeskuksen toimialojen kyberkypsyyskartoitus[2] osoittaa, että Suomen kriittisten alojen keskimääräinen kypsyystaso on perustasoa (3,0/5), mutta vaihtelu alojen välillä ja yksittäisten alojen sisällä on huomattavaa. Kypsimpiä aloja ovat tele-, ICT- ja finanssiala, joilla on pitkään ollut sekä sääntelyä että omia turvallisuusstandardeja. Sen sijaan logistiikka, teollisuus, satamat, kauppa ja vesihuolto sijoittuvat alle perustason, mikä kertoo resurssien, osaamisen ja järjestelmällisen riskienhallinnan puutteista. Myös pk-yritykset, jotka ovat usein osa kriittisiä toimitusketjuja, jäävät keskimäärin selvästi suuria toimijoita heikommalle tasolle sekä teknisten ratkaisujen että riskienhallinnan kypsyydessä.

Yleisiä tunnistettuja pullonkauloja ovat osaajapula, toimitusketjujen hallinnan puutteet ja OT-ympäristöjen eriytynyt hallinta. Tämä osoittaa, että vaikka Suomessa on korkean kypsyyden osa-alueita, kokonaisuus on epätasapainossa.

[1] Euroopan unionin kyberturvallisuusdirektiiviin NIS2:een liittyvät kansalliset asetukset tulivat voimaan 18.10.2024 jolloin se korvasi aiemman NIS1 -direktiivin vuodelta
[2] Huoltovarmuuskeskus (2022). Toimialojen kyberkypsyyden selvitys 2022.

ENISAn NIS360-raportin[3]mukaan tilanne on samankaltainen koko EU:ssa. Unionin tasolla korkeimman kypsyystason sektorit ovat energia, sähköinen viestintä ja pankkiala, kun taas terveys, julkishallinto, ICT-palveluhallinta (MSP/MSSP), kaasu ja avaruus ovat niin sanotulla riskivyöhykkeellä — niiden kriittisyys on korkea, mutta kypsyys jää alle tavoitetason. Tämä korostaa, että Suomen haasteet eivät ole poikkeuksellisia, vaan osa laajempaa eurooppalaista ilmiötä, jossa erityisesti pk-yritykset ja infrastruktuurien alihankkijat muodostavat tietoturvan heikoimman lenkin.

Systeeminen varautuminen yhä tärkeämpää

Varautumisen kannalta ei enää riitä, että palveluita ja teknologioita hankitaan pistemäisesti ja lähiajan tarpeeseen. Huomioon on otettava kokonaisarkkitehtuureja ja systeemitasoisia kokonaisuuksia sekä ymmärrettävä suurien globaalien toimijoiden tarjonta, sen kehittyminen ja monasti monimutkainen hinnoittelu. Aiemmin esimerkiksi haittaohjelmien torjuntaan riitti hyvin irrallinen ja ehkä paikallisesti tuotettu ratkaisu. Nyt tällaisten ratkaisujen integrointi osaksi pilvestä tarjottavaa IT-kokonaisratkaisua on monasti järkevää ja ehkä jopa välttämätöntä, jotta se toimisi saumattomasti yhteen valitun kokonaisarkkitehtuurin ja teknologioiden kanssa.

Kuvattu kehitys ei ole, erityisesti pk-yritysten kannalta, ongelmaton. Toisaalta valitsemalla, ja käytännössä myös sitoutumalla, laajan globaalin toimijan kuten Microsoftin tarjontaan, saa asiakas varmuutta ja mahdollisuuden hyvinkin laajaan kyberturvatarjontaan ja -turvaan. Tällä on kuitenkin merkittävä hintalappu ja se voi olla liian kova monelle pk- ja jopa suuryritykselleki n. Microsoftin tyyppisten globaalien toimijoiden lisenssimaksut ovat mittavia ja asiakkaiden neuvotteluvoima hintakeskusteluissa vähintäänkin vaatimaton. Lisäksi tuoteroadmappien, -paketointien ja -hinnoittelun ymmärtäminen ja ennakointi vaatii myös hyvää perehtyneisyyttä ja ajallista panostusta. Tämäkin lisää kustannuksia. Vaakakupin toisella puolella ovat toimittajasta irtautumisen kustannukset. Ne voivat olla varsin merkittäviä ja ajallisesti pitkäkestoisia.

Yksittäinen yritys yhä useammin osana ketjua

Käyttötarpeiden ja järjestelmien moninaisuuden kasvu asettaa haasteita myös sille, miten yksi taho voi parantaa omaa kyberturvaansa. Yhä enenevässä määrin tarvittaville turvatasoille pääseminen vaatii systeemitason ja arkkitehtuurin muutoksia kuten Zero Trust -konseptin toteutusta. Siinä paikkaan ja sisäverkkoihin perustuvat suojausmallien sijaan oletetaan käyttäjällä olevan haitallisia tarkoitusperiä ja siksi käyttäjän identiteetti ja käyttövaltuudet tarkistetaan usein ja ennen pääsyä järjestelmään. Mallista on kiistatonta hyötyä käytettäessä pilvipalveluita lokaatiosta riippumattomasti

[3] ENISA (2024). ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors.

ja näin tuetaan esim. etätyötä ja sen turvallisuutta. Konseptin toteutus on kuitenkin raskasta ja vaatii tyypillisesti tietojärjestelmä- ja tietoturva-arkkitehtuureihin merkittäviä muutoksia ja investointeja. Näiden perusteleminen yhtiön johdolle ja mahdollisesti myös hallitukselle voi olla merkittävän vaikeaa verrattuna aiempiin pistemäisiin ja ehkä konkreettisempiin kyberturvainvestointeihin. Kyberturvallisuusinvestointien talousperusteinen perustelu on yleisestikin ottaen haastavaa. Kyseessä on vakuutustyyppinen investointi, jossa riskin toteutumisen todennäköisyys koetaan pieneksi sekä kokonaisvaikutusten arviointi vaikeaksi.

Tekoäly ja kvanttilaskenta ovat uusia ja hankalia vastuksia

Perinteinen kyberturvallisuusympäristö kehittyy edelleen haastavammaksi ja monipuolistuu. Voidaan kuitenkin ajatella, että balanssi perinteisten uhkien ja suojautumiskeinojen välillä on jossain määrin hallinnassa ja merkittävää muutosta ei ole odotettavissa. Tekoäly ja kvanttilaskenta muodostavat kuitenkin erikseen ja etenkin yhdessä uuden kyberturvan riskialueen, jonka kaikkia vaikutuksia on tällä hetkellä varsin vaikea arvioida. Tähän tulisi kuitenkin pyrkiä.

Tekoälyllä on laajat vaikutukset

Tekoälyn nopealla kehittymisellä on moninaisia vaikutuksia kyberturvaan. Se auttaa kehittämään tehokkaampia suojautumiskeinoja, mutta toisaalta myös hyökkäyksien tehokkuutta. Verkkotason suojautumisessa käytetyt algoritmit kehittyvät sen avulla aiempaa reaktiivisemmiksi ja havaitsevat yhä monimutkaisempia anomalioita. Toisaalta hyökkäysten tehokkuus kasvaa, koska tekoälyavusteisuus löytää tehokkaasti kohteiden haavoittuvuuksia ja kehittää näihin sopivia murtotyökaluja. Tämä asettaa yhä kiristyviä vaatimuksia suojaustoimenpiteiden nopeudelle. Kun aiemmin puhuttiin uuden kriittisen haavoittuvuuden korjausajoissa päivistä, nyt tunneista. Tämä asettaa merkittäviä paineita kansallisille kyberturvallisuusuhkien havainnoinnista ja koordinoinnista vastaavilla tahoille. Tiedottamisen ketju on oltava tehokas ja suojautumistoimenpiteiden nopeita. Ne organisaatiot, joilla resurssit, työvälineet ja osaaminen ovat puutteellisia, ovat yhä vakavamman uhan alla.

Generatiivinen tekoäly on oiva työkalu moneen ja myös luomaan uskottavia valeidentiteettejä, lainahakemuksia, vakuutuskorvaushakemuksia, perusteettomia laskuja, jne. Tämä on yksi tekijä, joka on kasvattanut kyberrikollisuuden sen nykyisiin mittapuitteisiin. Kyberrikollisuuden vaikutusten arvioidaan olevan globaalilla tasolla vuonna 2025 10,5 biljoonaa USD ja kasvavan vuositasolla 15%[4]. Identiteettihuijausyritykset ovat kasvaneet

[4] Cybercrime Magazine, Oct 25, 2023

Signicatin tekemän tutkimuksen mukaan vuosina 2021-2024 69% [5]. Sama tutkimus sanoo 22% yrityksistä kärsivän huijausten vaikutuksista liikevaihdossaan. Vastaavasti Global Anti-Scam Alliance arvioi kuluttajien kärsineen huijauksissa vuonna 2024 1,03 biljoonan dollarin tappion[6]. Tekoälyn avulla voidaan siis luoda yhä kehittyneempiä kalasteluviestejä, mutta myös laajoja ja syviä yritysten ja henkilöiden identiteettejä, jolloin huijausten tuottopotentiaali kasvaa merkittävästi. Tekoäly auttaa myös luomaan ajallisesti pitkäkestoisia ja toimitusketjussa laajasti vaikuttavia huijauksia. Pohjoismainen rahaliikenteen hyvin kehittynyt osapuolten tunnistautumismekanismit pienentävät riskiä täällä toimivilta yrityksiltä, mutta tilanne ei ole sama jo Keski- ja Etelä-Euroopan maissa toimiville yrityksille.

Kvanttilaskentaan liittyviä riskejä on vielä vaikea arvioida

Kvanttilaskentaan kykenevien tietokoneiden läpimurron ajankohtaa on vaikeaa arvioida. Kyseessä on erittäin monimutkainen ja vaativa teknologia. Olemme kuitenkin lähempänä toimivien kaupallisten järjestelmien käyttöönottoa kuin koskaan aiemmin. Nyt toteutetut koneet kykenevät jo muutamien kymmenien kubittien laskentatehoon. Tehon noustessa tuhansiin kubitteihin olemme jo se sellaisella tasolla, että laitteet tai niiden ohjelmistot kykenevät murtamaan tällä hetkellä laajasti käytössä olevat salausmekanismit.

Riittävän tehokas kvanttitietokone voisi tulevaisuudessa murtaa julkisen avaimen RSA salauksen tai elliptisiin käyriin perustuvan ECC-salauksen kaltaiset salausmenetelmät. Näillä suojataan kaikkea rahaliikenteestä valtionhallinnon tietoihin. Tällä hetkellä on jo kuitenkin ratkaisuja, jotka ovat ns. PQC eli kvanttikryptografian jälkeistä salausta ja nähdään turvallisina. Vaikka suuret, nykyisten salausmenetelmien murtamiseen kykenevät kvanttitietokoneet eivät ole vielä täysin toiminnallisia, ne saattavat olla sitä seuraavien 10–20 vuoden aikana. Tämän vuoksi asiaan on tärkeä valmistautua etukäteen, jotta salatut tiedot eivät altistuisi salauksen purkamiselle tulevaisuudessa. On olemassa tutkijoiden ja turvallisuusviranomaisten arvioita siitä, että suuret maat kuten Kiina harrastavat ”Harvest Now, Decrypt Later” -toimintaa. Eli massakeräävät dataa jonka salaus voidaan purkaa myöhemmin[7].

Olemme monilla tavoilla ja säädöksillä, kuten GDPR, pyrkineet suojaamaan henkilötietoja ja rahaliikennettä. Näihin ei kohdistu merkittävää kvanttilaskennan kehittymiseen liittyvää riskiä mm. koska kyseinen tieto vanhenee nopeasti. Yrityssalaisuudet ja kansallisiin turvallisuusratkaisuihin liittyvät

[5] ”The Battle in the Dark” -tutkimus Signicat 2025
[6] Global Anti-Scam Alliance, Nov 7, 2024
[7] ”The Quantum Apocalypse is Coming. Be very Afraid” Wired Mar 24 2025 sekä ”Why post-quantum cryptography tops the new cybersecurity agenda

tiedot ovat kuitenkin ajallisesti hyvinkin pitkäkestoisia salaisuuksia, joiden paljastuminen voi aiheuttaa erittäin merkittävää haittaa.

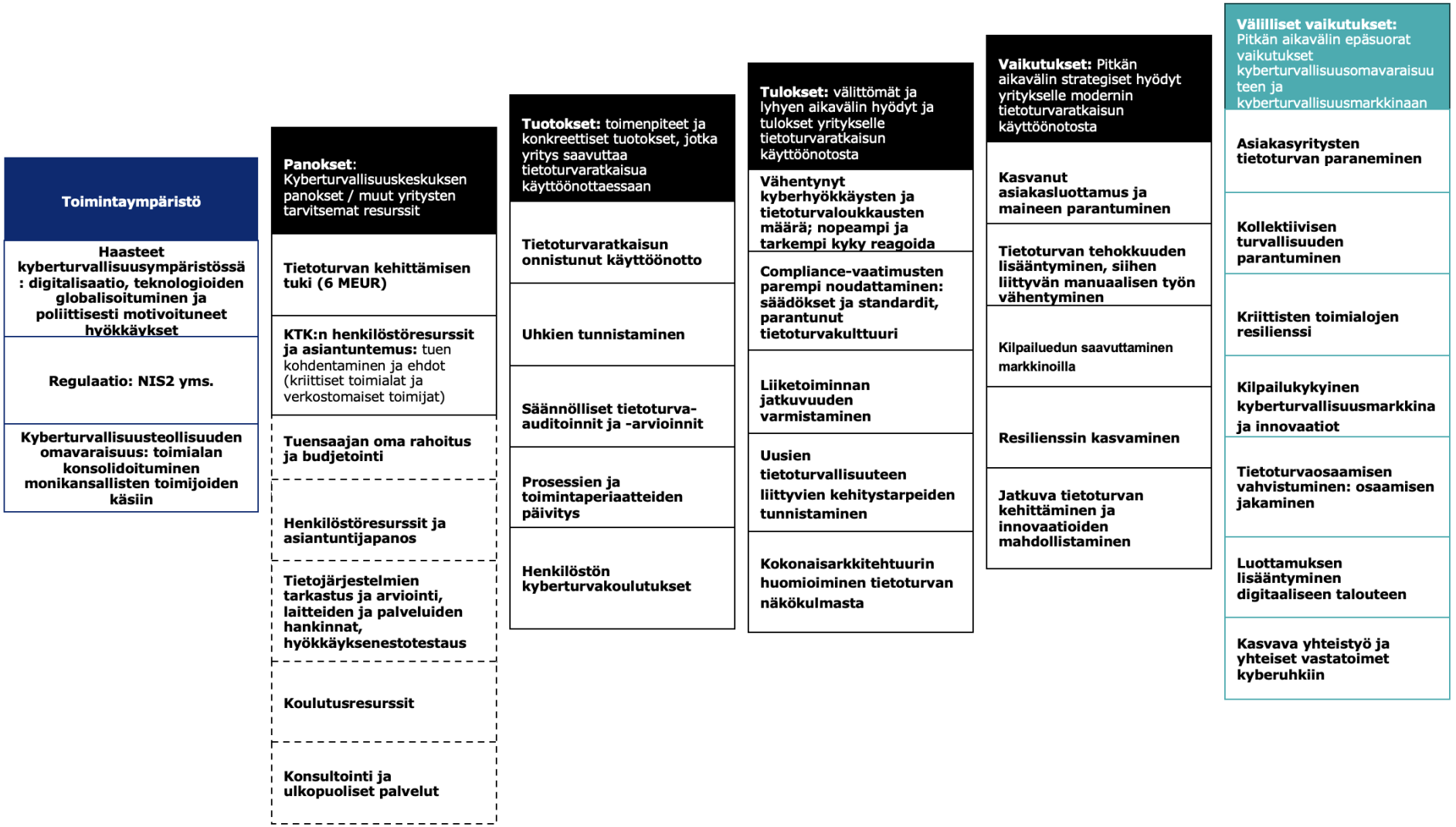
Ylläkuvattu toiminta tullee yrityskentässä kohdistumaan ensisijaisesti yhtiöihin, joilla on merkittävää T&K -toimintaa, kuten on lääkeyhtiöiden tapauksessa. Mutta myös pienempien toimijoiden, kuten insinööritoimistojen ja konepajayhtiöiden suunnitelmat ja innovaatiot ovat vaarassa. Nämä toimijat eivät välttämättä ole havainnoineet uhkaa ja heidän kyvykkyytensä varautua kyberuhkiin on tutkimusten mukaan keskimääräistä heikompaa. Kansalliset toimijat kuten Huoltovarmuuskeskus ovat omalla toiminnallaan pyrkineet nostamaan varautumisen tasoa[8].

Uusien syvällisten teknologioiden kehittäminen, kuten tekoälyn, vaatii hyvin mittavia resursseja. Tästä syystä niiden kehittäminen ja integroiminen osaksi tuote- ja palvelukokonaisuuksia on yhä enemmän suurten globaalien toimijoiden käsissä. Vaikka ajurit teknologioiden kehittämiselle, kuten generatiivinen tekoäly, eivät välttämättä suoranaisesti liity mitenkään kyberturvaan, on tälläkin kehitykselle merkitystä turvateknologioille. Niiden avulla voidaan luoda yhä kehittyneempiä ja nopeampia hyökkäyksiä, ja ne auttavat myös tällaisten hyökkäysten tunnistamisessa. Eli tekoälykehityksen elementtejä on siis lähes pakko soveltaa myös turva-alan tuotteisiin ja palveluihin, jotta aiemmat turvatasot voidaan edes pitää yllä. Verkkotasoisessa perinteisessä kyberturvassa on jo pitkään kehitetty ja käytetty tekoälytyyppisiä algoritmeja, joilla on pyritty tunnistamaan haitallisia anomalioita verkkoliikenteessä. Uusin tekoälykehitys luo mahdollisuuksia edelleen kehittää näitä järjestelmiä.

[8] ”Data Security Impacts of Quantum Computing – Preparedness Recommended” HVK 2024

3 Arvioinnin havainnot ja tulokset

Tässä luvussa esitellään arvioinnin tulokset. Tulokset on jaettu viiteen osioon. Ensimmäinen tarkastelee tuen valmistelua ja suhdetta kansallisiin ja EU-tason toimenpiteisiin ja regulaatioon, toinen tuen kohdentumista, kolmas tuensaajiin kohdistuvia suoria vaikutuksia, neljäs tuen tarvevastaavuutta ja viides sen epäsuoria vaikutuksia. Vaikutusten arviointi perustuu tukea varten kehitettyyn vaikutusmalliin (kuvio 2), joka on laajennettu versio muutosteorian viitekehyksestä (kuvio 1).



Kuva 2. Vaikuttavuusarvioinnissa käytetty viitekehys. Lähde: 4FRONT Oy.

3.1 Tuen valmistelu ja toteutus

Taustahaastattelujen mukaan tuen valmistelu tapahtui poikkeuksellisen nopeassa aikataulussa keväällä ja kesällä 2022, tilanteessa, jossa Ukrainan sodan ja kiristyneen turvallisuusympäristön vuoksi nähtiin tarve vahvistaa kriittisten alojen kyberturvallisuutta välittömästi. Asetus valmisteltiin muutamassa kuukaudessa ja tuki avattiin haettavaksi saman vuoden lopulla, mikä oli virkamiesvalmistelulle poikkeuksellisen nopea aikataulu. Kiire näkyi kuitenkin käytännön toimeenpanossa. Hakuehdoista viestintä ja ohjeistus jäivät osin epäselviksi, ja viranomaiset joutuivat jälkikäteen linjaamaan useita yksityiskohtia kuten kustannusten hyväksyttävyyttä. Kyseessä oli myös täysin uusi tukimuoto Suomessa. Vastaavaa ei ollut aiemmin toteutettu, eikä vertailukohtia löytynyt muualta Euroopastakaan. Tämä lisäsi epävarmuutta sekä viranomaisten että hakijoiden puolella, ja esimerkiksi tukikelpoisuuden arviointi sekä hakemusten käsittelyprosessi veivät huomattavasti odotettua enemmän työaikaa.

Valmistelun kiire ja uuden instrumentin luonne heijastuivat myös viestintään. Suunniteltuja koulutustilaisuuksia ja ohjeistuksia ei ehditty järjestää ennen kuin myönnettäväksi osoitettu kokonaismääräraha oli haettu kokonaan, ja tukea koskeva tieto levisi pääosin median ja alan toimijoiden omien verkostojen kautta. Tämä johti siihen, että osa hakijoista ei täysin ymmärtänyt tuen rajoituksia tai ehtoja, osa avustushakemuksista olivat osin puutteellisia ja osa yrityksistä joutui palauttamaan osan saadusta tuesta, kun kustannukset osoittautuivat tukikelvottomiksi. Lisäksi toisen tukiluokan tuen kohderajaus sulki pois julkisomisteiset toimijat. Esimerkiksi pääasiassa tukea hakeneet vesihuollosta vastaavat yritykset ja paikalliset energiayhtiöt, jotka muutoin olisivat olleet yhteiskunnan toiminnan kannalta kriittisiä, eivät juridisesti täyttäneet pk-yrityksen määritelmää. Tämä nähtiin valmistelijoidenkin keskuudessa puutteena, sillä juuri näillä sektoreilla kyberturvallisuuden perustaso oli monin paikoin matala ja tuen tarve ilmeinen.

3.1.1 Tuen valmisteluun liittyvät lausunnot

Tietoturvan kehittämisen tukea koskeva asetus (VN/18738/2022) herätti poikkeuksellisen laajaa kiinnostusta sen lausuntokierroksella kesällä 2022. Lausuntoja saapui useilta hallinnonaloilta, elinkeinoelämän järjestöiltä, viranomaisilta, tutkimusorganisaatioilta ja yrityksiltä. Lausuntopalautteessa tunnistettiin selvästi sekä tuen tarpeellisuus että sen käytännön toteutukseen liittyvät haasteet.

Yleinen linja lausunnoissa oli myönteinen. Useimmat tahot pitivät tietoturvaseteliä tervetulleena ja nopeasti vaikuttavana välineenä, joka voisi vahvistaa kriittisten toimialojen yritysten kyberturvallisuutta ja

huoltovarmuutta. Samalla kuitenkin toivottiin, että tukea ei rajattaisi vain kriittisiin sektoreihin, vaan että myös muut pk-yritykset voisivat hyötyä siitä. Useat elinkeinoelämän edustajat, kuten Suomen Yrittäjät ja Elinkeinoelämän keskusliitto, korostivat pienten yritysten merkitystä osana toimitusketjuja ja ehdottivat, että tuen piirissä tulisi olla laajempi joukko yrityksiä. Myös mahdollisuutta käyttää tukea pidempiaikaisiin kehitystoimiin ja ylläpitoon pidettiin tärkeänä, sillä asetuksen määrittelemä aikarajaus katsottiin liian kapeaksi.

Lausunnoissa nousi esiin myös hallinnollisia ja lainsäädännöllisiä huomioita. Työ- ja elinkeinoministeriö kiinnitti huomiota EU:n valtiontukisääntöjen ja de minimis -sääntelyn asianmukaiseen soveltamiseen, ja Valtiovarainministeriö painotti vaikutusten arvioinnin ja valvonnan selkeyttä. Kilpailu- ja kuluttajavirasto puolestaan nosti esiin mahdolliset kilpailuvaikutukset ja sen, että julkisen tuen tulisi kohdistua selvästi markkinapuutteiden korjaamiseen. Opetus- ja kulttuuriministeriö painotti osaamisen ja koulutuksen roolia osana kyberturvallisuuden kehittämistä, kun taas Huoltovarmuuskeskus ja Traficom näkivät tukimuodon vahvistavan koko yhteiskunnan kriittisiä toimintoja ja varautumiskykyä.

Lisäksi lausunnoissa esitettiin yksityiskohtaisia kehittämisehdotuksia. Ehdotettiin esimerkiksi tuen määrärahan kasvattamista, omavastuuosuuden tarkistamista, hallinnollisen taakan keventämistä ja hakuprosessin selkeyttämistä. Badrap Oy ja TIVIA ry nostivat esiin tarpeen kehittää myös palveluntarjoajien pätevyyskriteerejä ja pk-yritysten hankintaosaamista, jotta tuen vaikuttavuus olisi mahdollisimman suuri. Moni lausunnonantaja painotti, että tuki tulisi nähdä osana pitkäjänteistä kansallista kyberturvallisuuspolitiikkaa eikä vain kertaluonteisena toimenpiteenä.

3.1.2 Linkki EU-tason toimenpiteisiin

ECCC:n strateginen agenda (European Cybersecurity Competence Centre, 2023) määrittelee EU:n yhteiset painopisteet kyberturvallisuuden tutkimus-, innovaatio- ja teollisuusinvestoinneille. Sen tavoitteena on vahvistaa Euroopan kyberturvallisuusosaamista, teknologista omavaraisuutta ja kilpailukykyä sekä tukea unionin resilienssiä kyberuhkia vastaan. Agenda linjaa, että kyberturvallisuutta tulee kehittää kokonaisuutena – yhdistäen tutkimus, osaaminen, teollinen kehitys ja pk-yritysten tukeminen. Keskeisiä vaikutusalueita ovat pk-yritysten kyvykkyyksien vahvistaminen, osaavan työvoiman kouluttaminen ja sertifiointi, sekä tutkimus- ja innovaatiotoiminnan koordinointi EU:n ohjelmien (Digital Europe Programme ja Horizon Europe) puitteissa. ECCC korostaa myös synergioita siviili- ja puolustussektorin välillä sekä post-kvanttisalausta, tekoälypohjaisia turvallisuusratkaisuja ja toimitusketjujen kyberturvallisuutta. Strateginen agenda toimii ohjenuorana EU:n ja jäsenmaiden yhteisille investoinneille ja tukee jäsenvaltioiden kansallisia toimenpiteitä, kuten Suomen tietoturvan kehittämisen tukea, jolla

vahvistetaan erityisesti pk-yritysten ja kriittisten toimialojen perustason kyberturvallisuutta.

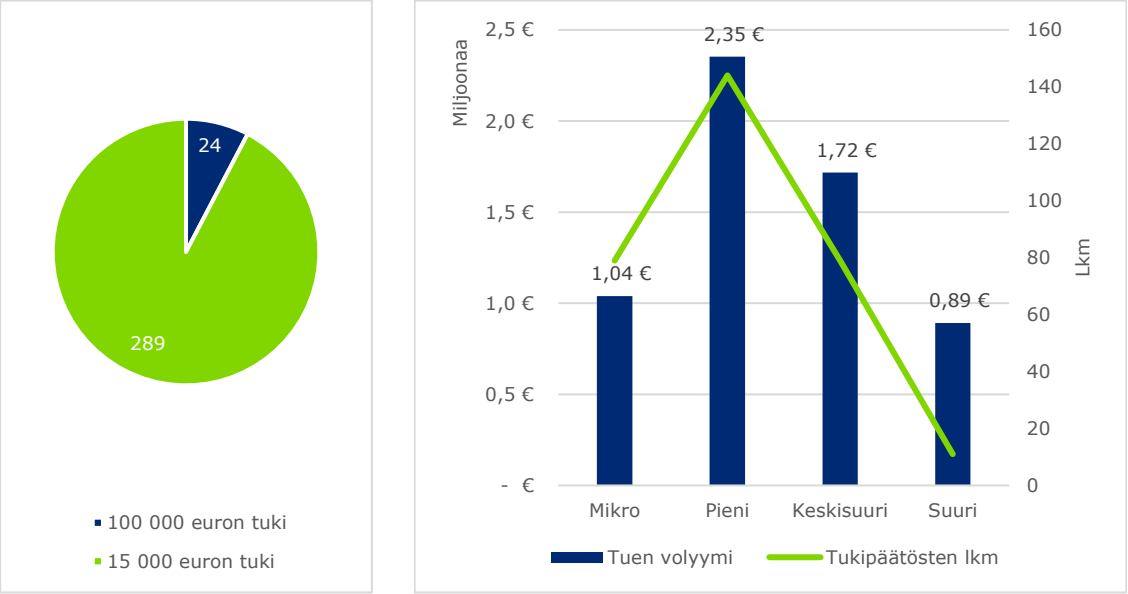
Niin sanottu NIS2-direktiivi (EU 2022/2555) muodostaa koko Euroopan unionia koskevan yhteisen oikeudellisen kehyksen verkko- ja tietojärjestelmien turvallisuuden vahvistamiseksi. Se korvasi aiemman NIS1-direktiivin ja nosti EU:n kyberturvallisuusvelvoitteiden kunnianhimon tasoa laajentamalla sääntelyn piiriin kuuluvien toimialojen määrää, selkeyttämällä sääntöjä ja tehostamalla valvontamekanismeja. Direktiivi kattaa yhteensä 18 kriittistä sektoria, mukaan lukien energia-, terveys-, rahoitus-, kuljetus-, vesi- ja jätehuolto, digitaaliset palvelut, julkinen hallinto sekä avaruussektori. Se velvoittaa jäsenvaltioita laatimaan kansalliset kyberturvallisuusstrategiat, ylläpitämään luetteloa yhteiskunnan kannalta välttämättömistä palveluista sekä varmistamaan, että näiden toimijoiden kyberturvallisuuden riskienhallinta, valvonta ja raportointi täyttävät EU-tason vaatimukset. Direktiivi asettaa myös yritysjohdolle selkeän vastuun kyberturvallisuuden riittävästä hallinnasta, mikä nostaa tietoturvan osaksi organisaatioiden strategista johtamista. NIS2-direktiivin mukaiset velvoitteet tulivat Suomessa voimaan 8.4.2025 uuden Kyberturvallisuuslain voimaan tullessa.

NIS2-direktiivi ja tietoturvan kehittämisen tuki liittyvät kiinteästi toisiinsa. Tuen avulla Suomi on pyrkinyt vahvistamaan juuri niitä kyberturvallisuusvalmiuksia, joita NIS2-direktiivi edellyttää kriittisiltä ja tärkeiltä toimijoilta. Asetuksella käynnistetty tuki tarjosi matalan kynnyksen rahoituskanavan erityisesti pk-yrityksille, joilla ei vielä ollut valmiuksia täyttää NIS2-direktiivin mukaista riskienhallinnan, raportoinnin ja varautumisen tasoa. Monilla tuen saajilla ei ollut aiemmin velvoitteita tai kokemusta systemaattisesta tietoturvan kehittämisestä, joten tuki auttoi luomaan perustaa tulevien NIS2-direktiivin vaatimusten täyttämiselle. Samalla tuen tavoitteena oli täydentää kansallista kyberturvallisuusstrategiaa ja huoltovarmuuden tavoitteita, auttaen Suomea rakentamaan yhtenäistä kyberturvallisuusvalmiutta EU:n yhteisen sääntelyn pohjalta. Käytännössä tietoturvan kehittämisen tuki toimi siirtymäkauden työkaluna, jolla madallettiin pk-yritysten kynnystä varautua direktiivin voimaantuloon ennen sen kansallista toimeenpanoa.

3.2 Tuen kohdentuminen

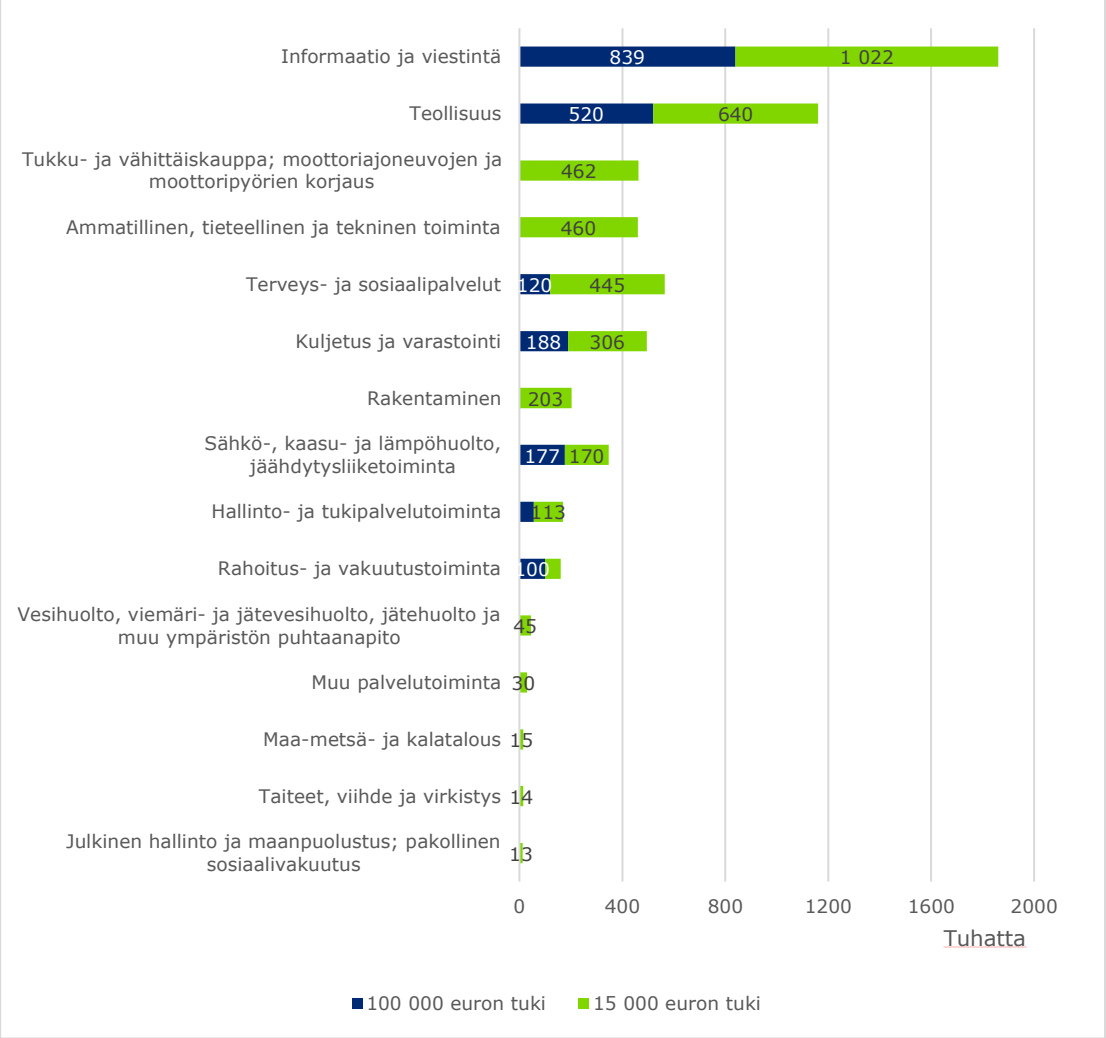
Tietoturvan kehittämisen tukea myönnettiin yhteensä 6 miljoonaa euroa 313 hankkeelle. Tukea myönnettiin kahdessa kategoriassa: enintään 15 000 euron luokassa ja enintään 100 000 euron luokassa. Molemmissa tukiluokissa tukea saatettiin kuitenkin myöntää vähemmän kuin maksimimäärä, perustuen ilmoitettuihin hyväksyttyihin kustannuksiin. Valtaosa, 92 % (289 kpl), tehdyistä tukipäätöksistä oli pienemmän tukiluokan hankkeita ja loput 8 % suuremman tukiluokan hankkeita (24 kpl). Valtaosa tuesta, eli reilu 5 miljoonaa euroa kohdentui pienille ja keskisuurille yrityksille.

Suuryrityksille kohdentui vajaa miljoona euroa. Nämä olivat keskimäärin suurempia (81 000 euroa) hankkeita.



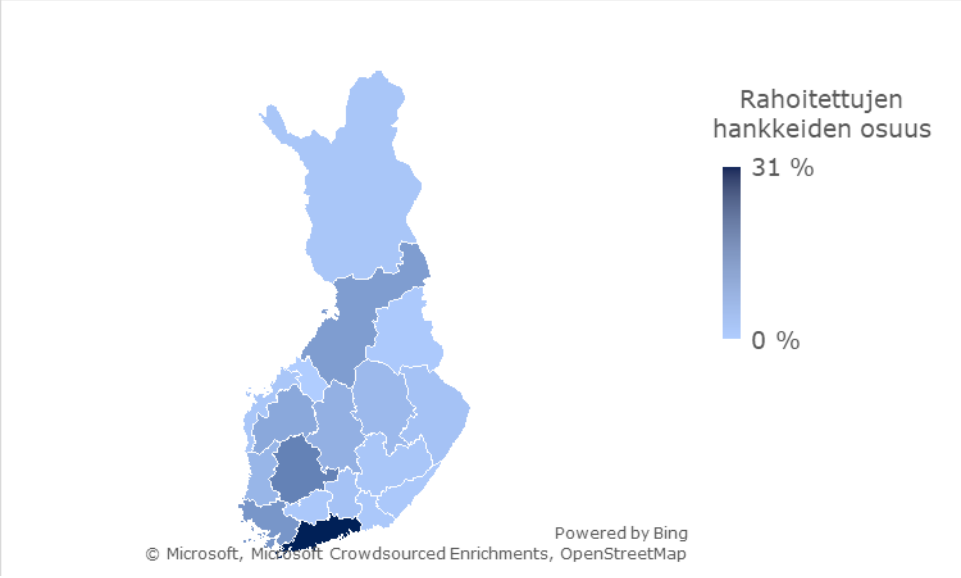
Kuva 3. Vasen: Tuen kohdentuminen eri tukiluokkiin (lukumäärä). Oikea: Tuen kohdentuminen eri kokoisille yrityksille. Lähde: Traficom.

Pienemmän tukiluokan hankkeissa rahoitus kohdistui erityisesti informaatio- ja viestintä alalle (26 %), teollisuuteen (16 %), tukku- ja vähittäiskauppaan (12 %), ammatilliseen, tieteelliseen ja tekniseen toimintaan (11 %) sekä terveys- ja sosiaalipalveluihin (11 %). Suuremmassa tukiluokassa rahoitus kohdistui erityisesti informaatio- ja viestintä alalle (42 %) ja teollisuuteen (26 %). TOL-toimialaluokitus ei kuitenkaan juuri kerro yritysten toiminnan sijoittumisesta kriittisille aloille. Kappaleessa 3.4.2 on kuvattu kyselyn perusteella toiminnan sijoittumista NIS2-direktiivin mukaisille kriittisille toimialoille.



Kuva 4. Tuen euromääräinen kohdentuminen toimialoittain (myönnetty avustus). Lähde: Traficom.

Valtaosa avustetuista hankkeista sijoittuu yrityksen toimipaikan mukaan Uudellemaalle (31 %), Pirkanmaalle (14 %) tai Varsinais-Suomeen (10 %).



Kuva 5. Avustettujen hankkeiden osuus maakunnittain. Lähde: Traficom.

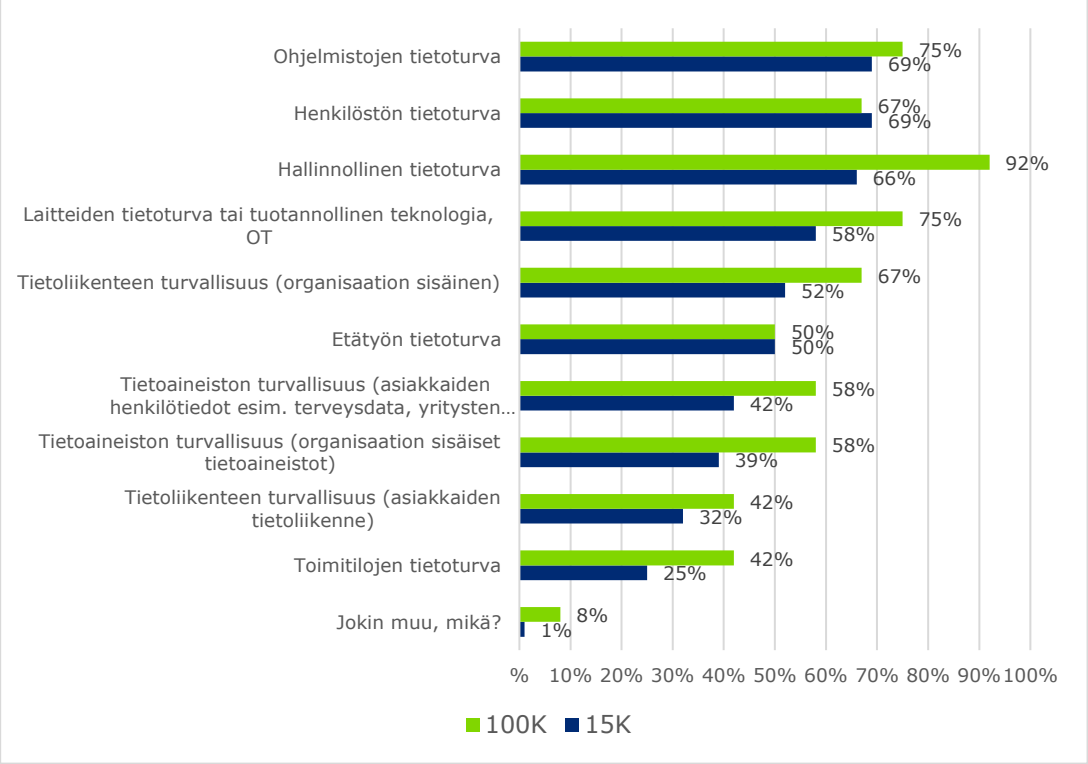
Tukea palautettiin ja takaisinperittiin yhteensä noin 430 000 euroa, eli noin 7 prosenttia myönnetystä tuesta. Tukea palautti ja sitä takaisinperittiin yhteensä 68 yritykseltä.

3.3 Suorat vaikutukset tuen saajiin

3.3.1 Tuen käyttö ja hankkeiden toteutus

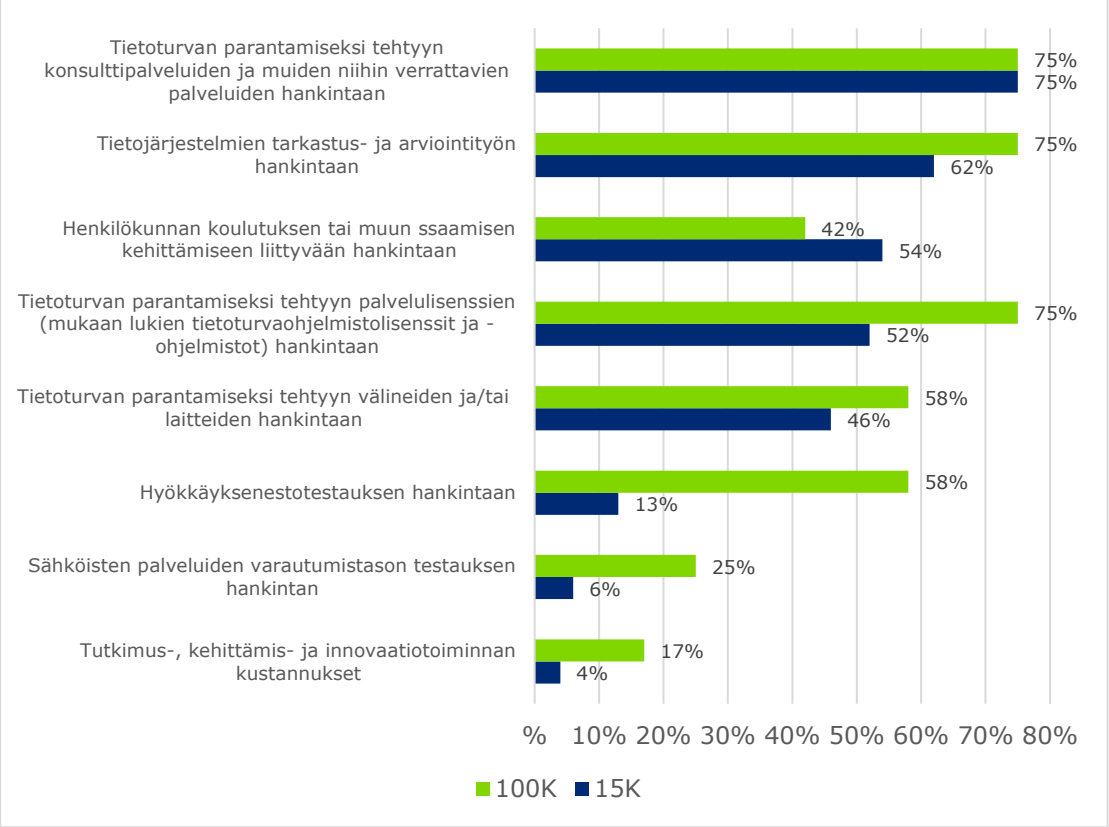
Hankkeissa toteutetut toimenpiteet kohdistuivat tyypillisesti useampaan toiminnan osa-alueeseen, joista selvästi eniten ohjelmistojen (75 % suurissa, 69 % pienissä hankkeissa) ja hallinnollisen tietoturvan kehittämiseen (92 % suurissa, 66 % pienissä hankkeissa). Myös henkilöstön tietoturvaosaamisen vahvistaminen oli keskeinen painopiste (67 % suurissa, 69 % pienissä hankkeissa). Laite- ja tuotantoteknologian tietoturvaa painotettiin suhteellisesti enemmän suuremmissa hankkeissa (75 % vs. 58 %). Sen sijaan asiakkaiden tietoliikenteen ja tietoaineistojen turvallisuuteen kohdistuvat toimet jäivät vähemmälle huomiolle, vaikka niissäkin oli havaittavissa kehitystä. Toimitilojen tietoturvaan panostettiin vain 25 prosentissa pienistä hankkeista. Kriittisten alojen maturiteettia mittaavissa selvityksissä[9] on todettu, että yleisiä pullonkauloja ovat mm. osaajapula, toimitusketjujen hallinnan puutteet ja OT-ympäristöjen eriytynyt hallinta. Näin olleen voidaan todeta, että avustetuissa hankkeissa on kehitetty oikeita asioita. Toimitusketjujen hallintaan ja tuotannollisen teknologian tietoturvaan tulisi kuitenkin keskittää vieläkin enemmän toimenpiteitä.

[9] HVK:n kypsyyskartoituksen mukaan (2022)



Kuva 6. Millaisiin toimintoihin hankkeessa toteutettu tietoturvan parantaminen kohdentuu (suoraan tai välillisesti asiakkaiden kautta)? Voit valita useamman. n=114. Lähde: Selvityksen osana toteutettu kysely (4FRONT Oy).

Hankkeet toteutettiin tyypillisesti hyödyntäen useampia eri kanavia, useimmiten hankkimalla konsulttipalveluita (75 % molemmissa tukiluokissa) ja tietojärjestelmien tarkastus ja arviontitöitä (75 % suuremmista ja 62 % pienemmistä). Noin puolet (52 %) pienemmistä hankkeista osti henkilöstön kouluttamiseen liittyviä palveluita. Tukea käytettiin myös tietoturvan parantamiseen liittyviin palvelulisensseihin ja välineisiin (75 %/58 % suuremmissa ja 52 %/46 % pienemmissä hankkeissa). Hyökkäyksenestotestauksia hankittiin lähinnä suuremmissa hankkeissa (58 %). Sähköisten palveluiden varmuustestaukset ja tutkimus- tai innovaatiokustannukset olivat selvästi harvinaisempia tuen käyttökohteita. Yleiskuva kertoo, että tuki ohjautui ennen kaikkea käytännönläheiseen kehittämiseen ja osaamisen vahvistamiseen, kun taas teknisesti vaativammat tai tutkimukselliset toimet jäivät marginaalisemmiksi.



Kuva 7. Mihin tietoturvan kehittämisen tuki käytettiin? Voit valita useamman. n=114. Lähde: Selvityksen osana toteutettu kysely (4FRONT Oy).

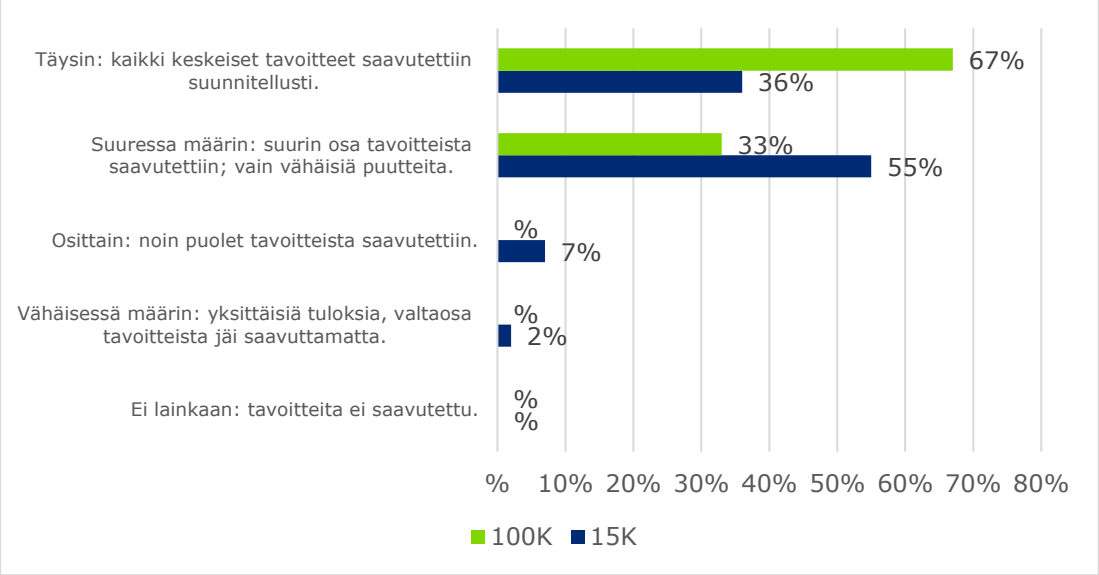
Hakemustekstien perusteella eri tukiluokissa tehtiin jossain määrin erilaisia toimenpiteitä. Enintään 100 000 euron tuet (24 hanketta) kohdistuivat organisaatioihin, jotka rakensivat pitkäjänteisesti omaa kyberturvakyvykkyyttään, kehittivät infrastruktuuriaan ja hallintamallejaan sekä yhdistivät toimenpiteissään teknologiaa, testausta ja koulutusta. Näissä hankkeissa oli usein kyse laajemmista, usean osa-alueen kokonaisuuksista tai jatkuvista kehitysohjelmista. Yleisiksi teemoiksi nousivat verkkoturva ja teknologia (esimerkiksi tietoturva-arkkitehtuurin rakentaminen, verkko- ja järjestelmäsuojausten parantaminen), hallinta ja kehittäminen (tietoturvan johtamismallit, prosessien ja strategioiden kehittäminen) sekä testaus ja koulutus (penetraatiotestaukset, haavoittuvuusanalyysit ja henkilöstön osaamisen vahvistaminen).

Enintään 15 000 euron tuet (290 hanketta) puolestaan kohdistuivat yritysten perustason tietoturvan ja riskienhallinnan vahvistamiseen. Toimenpiteet olivat luonteeltaan taktisempia ja rajatumpia, usein yksittäisiä teknisiä parannuksia tai koulutuksellisia panostuksia. Näissä hankkeissa yleisiä teemoja olivat verkkoturva (palomuurit, uhkien tunnistus, phishing-harjoitukset, monivaiheinen tunnistautuminen ja identiteetinhallinta), hallinta ja koulutus (perustoimintamallien kehittäminen, henkilöstön kouluttaminen ja tietoisuuden lisääminen), kehittäminen ja teknologia (pienimuotoiset

tietoturvaprojektit ja teknisten ratkaisujen käyttöönotto) sekä testaus (haavoittuvuuskartoitukset, ulkoiset testaukset ja auditoinnit).

Tavoitteiden saavuttaminen

Valtaosa hankkeista kertoi saavuttaneensa niille asetetut tavoitteet täysin tai suuressa määrin (100 % suurista ja 91 % pienistä hankkeista).



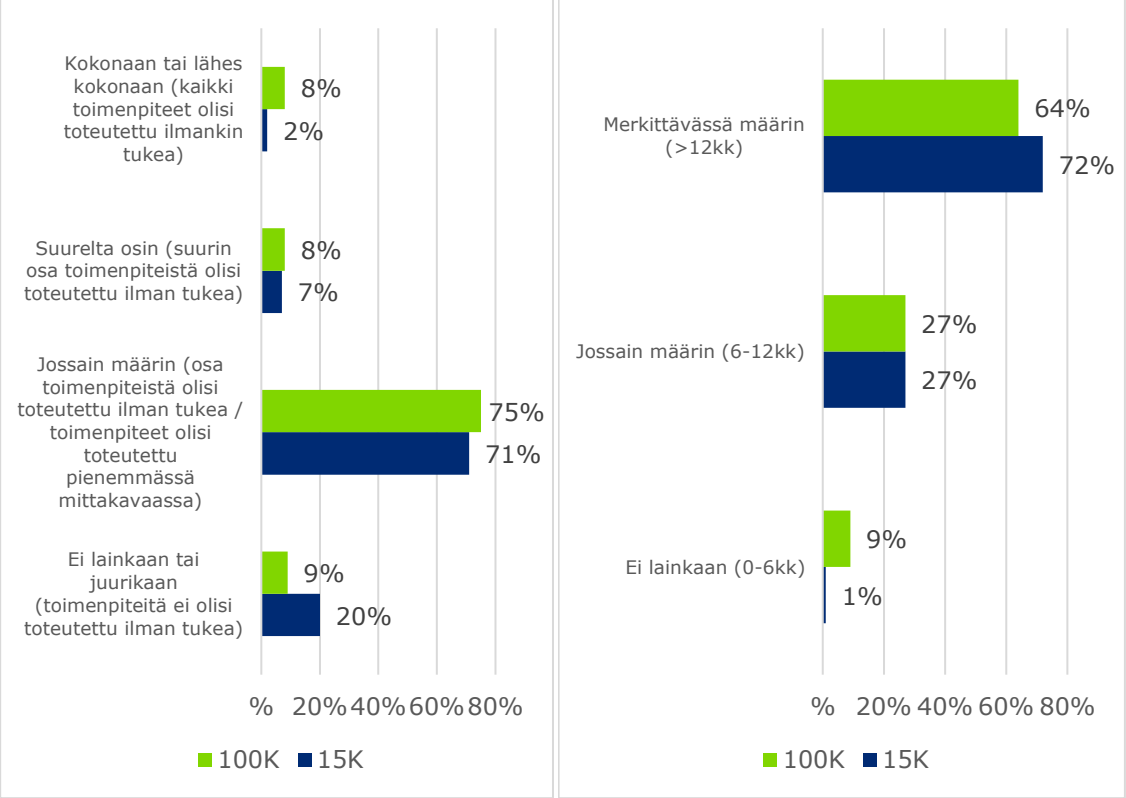
Kuva 8. Missä määrin yrityksenne saavutti hankkeella tavoitellut tulokset? n=114. Lähde: Forefront Oy:n kysely.

3.3.2 Tuen lisäisyys (additionaliteetti)

Tuen vaikutus pienemmän tukiluokan hankkeiden toteutukseen oli kiihdyttävä. 91 prosenttia kertoi, että hanketta ei olisi toteutettu lainkaan tai se olisi toteutunut vain osittain ilman tukea. Suuremmassa tukiluokassa lisäisyys oli kuitenkin rajallinen, 16 prosenttia kertoi, että hanke olisi toteutunut ilman tukea kokonaan tai suurelta osin – vaikkakin jossain määrin nopeammin. Näiltä osin tuki siis subventoi toimintaa, joka olisi toteutettu joka

tapauksessa. Ottaen huomioon, että tuki ei ollut kilpailtua, luku olisi voinut kuitenkin olla suurempi.

Niistä vastaajista, jotka kertoivat, että hanke ei olisi toteutunut ilman tukea, suurin osa kertoi, että se myös nopeutti toimenpiteiden toteuttamista merkittävästi (72 % pienistä ja 64 % suurista hankkeista).



Kuva 9. Vasen: Miltä osin hankkeissa toteutetut toimenpiteet olisivat toteutuneet ilman tukea? Oikea: Arvioi, missä määrin tuki nopeutti toimenpiteiden toteuttamista ajallisesti? n=114. Lähde: Forefront Oy:n kysely.

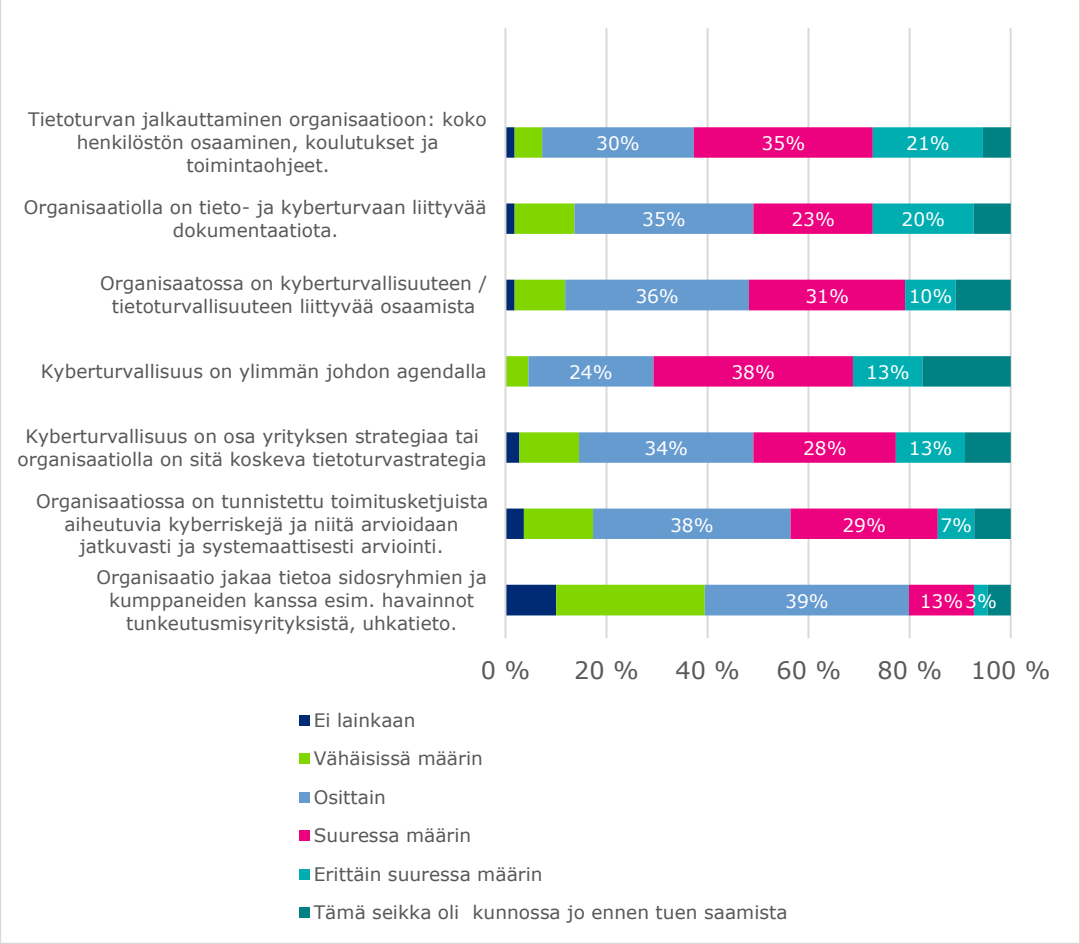
3.3.3 Vaikutukset tietoturvaan

Organisaation sisäiset muutokset

Tuella oli selvästi havaittava vaikutus organisaatioiden tietoturvakäytäntöihin ja osaamiseen. 86 prosenttia vastaajista arvioi tietoturvan jalkauttamisen henkilöstölle parantuneen vähintään osittain. Myös kyberturvallisuuden asema yritysjohdon agendalla vahvistui (75 % vähintään osittain), samoin dokumentointi (78 % vähintään osittain) ja tietoturvan rooli osana yrityksen strategiaa (73 % vähintään osittain). Sen sijaan toimitusketjuista tulevien riskien tunnistamisessa (18 % ei parannuksia) ja uhkatiedon jakamisessa verkostoille (40 % ei parannuksia) on vielä parantamisen varaa. Tulosten perusteella voidaan todeta, että suuret hankkeet loivat merkittävää rakennemuutosta yrityksiin. Tietoturva nousi johdon ja strategisen

päätöksenteon tasolle, ja organisaatioiden kyky ylläpitää ja arvioida tietoturvaa vahvistui selvästi.

Pienemmän ja suuremman tukiluokan välillä oli lähinnä pieniä eroja, jotka liittyivät vaikutusten intensiteettiin. Enintään 100 000 euron tukiluokassa useampi arvioi vaikutukset suuriksi tai erittäin suuriksi, kun pienemmässä tukiluokassa vaikutukset arvioitiin useimmin osittaisiksi.



Kuva 10. Missä määrin tuen avulla toteutettu hanke on parantanut tai edistänyt seuraavia seikkoja organisaatiossasi? n=112. Lähde: Forefront Oy:n kysely.

Välittömät hyödyt

Suurimmissa, enintään 100 000 euron hankkeissa suurimmat parannukset nähtiin reaktiokyvyn nopeutumisessa (73 % paljon tai erittäin paljon), ja digijärjestelmien parantuneessa tietoturvassa (73 % paljon tai erittäin paljon). Lisäksi valtaosa hankkeista tunnisti uusia kehitystarpeita (73 % paljon tai erittäin paljon). Sen sijaan fyysisen infrastruktuurin ja teollisuusautomaation (OT) tietoturva jäi heikommaksi, sen osalta tunnistettiin vain osittaisia parannuksia. Myös yhteistyö alan kumppaneiden, toimialaverkostojen tai viranomaisten kanssa vaatisi vielä parannettavaa valtaosalla yrityksistä. Tämä viittaa siihen, että isot hankkeet painottivat organisaation sisäisiä

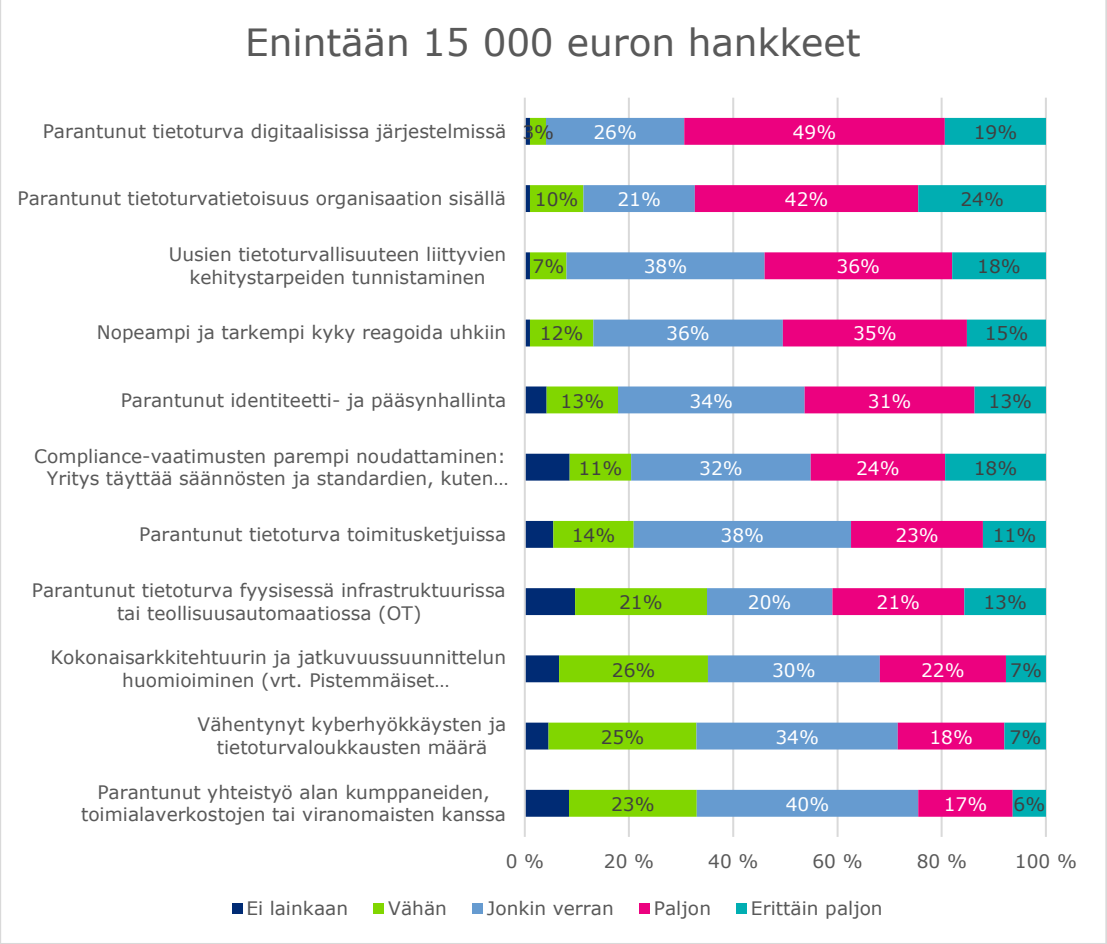
kyvykkyyksiä ja prosesseja enemmän kuin ulkoisia riippuvuuksia tai teknistä OT-ympäristöä.

Pienemmissä, enintään 15 000 euron hankkeissa suurimmat parannukset raportoitiin organisaation sisäisessä tietoturvatietoisuudessa (66 %: paljon tai erittäin paljon), digitaalisten järjestelmien tietoturvassa (68 % paljon tai erittäin paljon) sekä uhkien tunnistamisessa ja reagoinnissa (50 %). Lisäksi yli puolet hankkeista tunnisti uusia kehitystarpeita (54 % paljon tai erittäin paljon). Heikoimmat tulokset näkyivät vähäisenä yhteistyönä kumppaneiden kanssa (31 % ei lainkaan tai vain vähän), kyberhyökkäysten ja tietoturvaloukkausten määrän vähentämisessä (29 % ei lainkaan tai vain vähän) sekä kokonaisarkkitehtuurin ja jatkuvuussuunnittelun huomioimisessa (32 % ei lainkaan tai vain vähän).

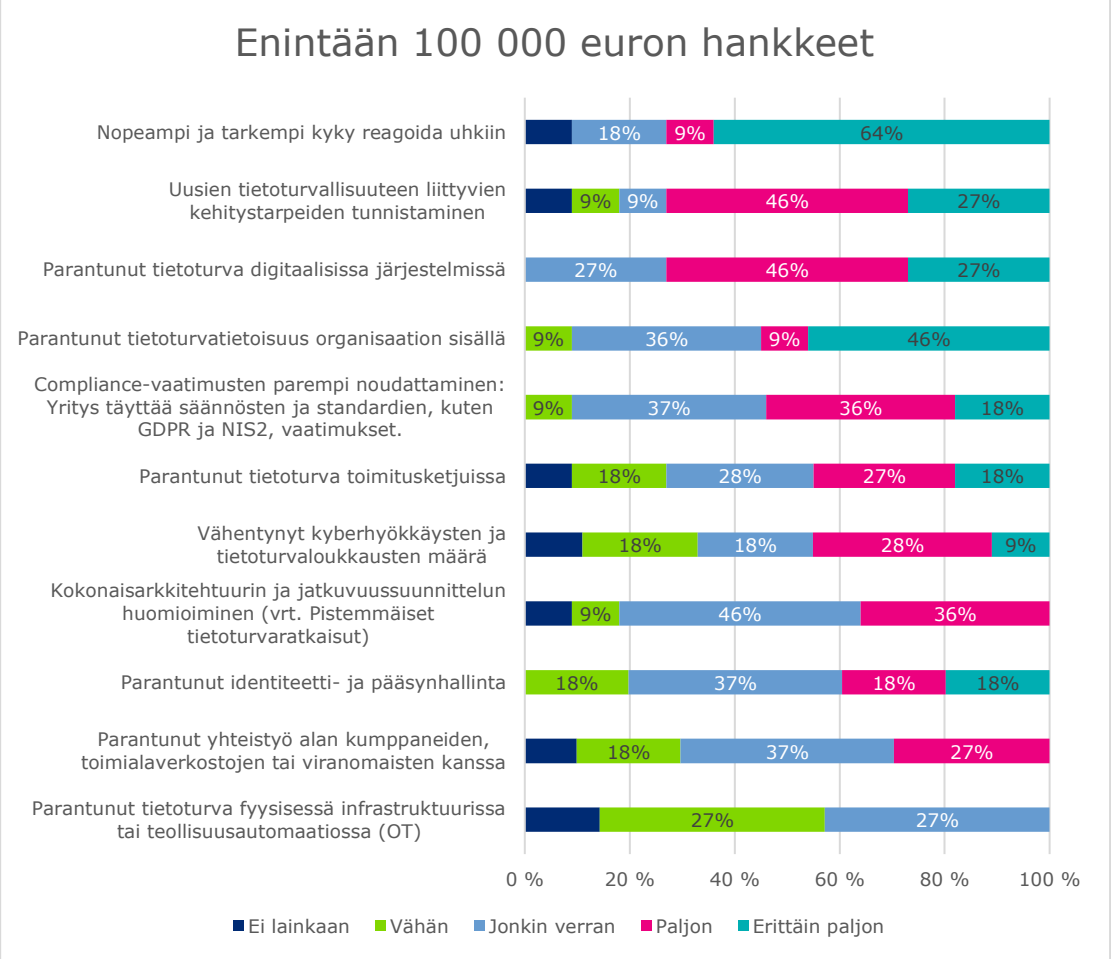
Suurista hankkeista 45 % (paljon tai erittäin paljon) paransi tietoturvan tasoa toimitusketjuissa, kun vastaava luku pienemmillä hankkeilla oli 34 % (paljon tai erittäin paljon).

Yleisesti voidaan todeta, että hankkeilla on onnistuttu edistämään laaja-alaisesti tietoturvaa. Suurimmat erot pienten ja suurien hankkeiden välillä liittyvät vaikutusten intensiteettiin. Suuremmissa hankkeissa vaikutukset koettiin useammin suuriksi tai erittäin suuriksi, kun taas pienemmissä hankkeissa raportoitiin useammin, että hankkeessa syntyi jonkin verran vaikutuksia. Suuret hankkeet myös tuottivat yleisemmin laaja-alaisempia ja syvempiä vaikutuksia erityisesti järjestelmien ja reagointikyvykkyyden osalta, kun taas pienet hankkeet keskittyivät henkilöstön osaamiseen ja tietoisuuden vahvistamiseen. Molemmissa tukiluokissa toimitusketjujen tietoturva ja teollisuusautomaation/OT-ympäristöjen suojaus jäivät selkeimmin kehittämisen varaan. Nämä ovat myös teemoja, jotka nousevat kriittisten alojen maturiteettia selvittävissä tutkimuksissa suurimmiksi pullonkauloiksi[10].

[10] HVK:n kypsyyskartoituksen mukaan (2022)



Kuva 11. Missä määrin organisaatiolle on syntynyt (tai odotetaan syntyvän pian hankkeen päätyttyä) seuraavia välittömiä ja lyhyen aikavälin hyötyjä ja tuloksia tuen ansiosta? n=101. Lähde: Forefront Oy:n kysely.



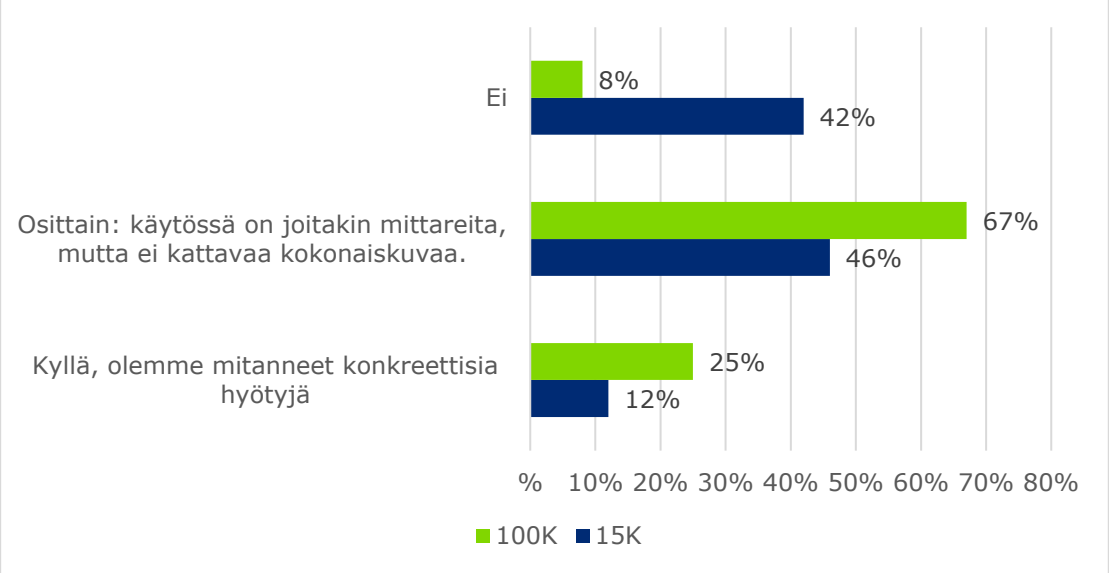
Kuva 12. Missä määrin organisaatiolle on syntynyt (tai odotetaan syntyvän hankkeen päätyttyä) seuraavia välittömiä ja lyhyen aikavälin hyötyjä ja tuloksia tuen ansiosta? n=12. Lähde: Forefront Oy:n kysely.

Vaikutusten mittaaminen

Yritykset keräävät mittaustietoa varsinkin suuremmissa hankkeissa. Valtaosa näistä kerää kuitenkin tietoa vain joistain mittareista ja harvempi niin laajasti, että niiden pohjalta voisi luoda selkeän kokonaiskuvan. Suuremmissa hankkeissa on yleisesti paremmat edellytykset ja resurssit mitata vaikutuksia systemaattisesti, mutta laajempi, yhtenäinen mittaristo puuttuu monesta organisaatiosta vielä molemmissa ryhmissä.

Avovastausten pohjalta mittarit liittyvät useammin organisaatiota koskeviin toimenpiteisiin tai laadullisiin mittareihin, esim. koulutetun henkilöstön määrään tai parantuneeseen valmiuteen. Vain harva kertoi keräävänsä tietoa poikkeamailmoituksista, hyökkäyksistä ja estetyistä hyökkäyksistä. Suurimmissa, enintään 100 000 euron hankkeissa tulokset olivat systemaattisempia ja monitasoisempia. Näissä hankkeissa saavutettiin selvästi mitattavia parannuksia, kuten poikkeamien havaitsemisajan lyheneminen, auditointien havaintojen väheneminen, automaattisen reagoinnin käyttöönotto ja henkilöstön laaja koulutus. Lisäksi useissa vastauksissa kuvattiin rakenteellista kehitystä, kuten SOC-palvelujen, Multi factor authentication-

palvelujen (MFA) ja penetraatiotestauksen käyttöönottoa sekä tietoturvapolitiikan ja vuosikellon luomista. Toisin sanoen suurempi tukiluokka mahdollisti kokonaisvaltaisen tietoturvajärjestelmän kehittämisen ja jatkuvan seurannan, kun taas pienemmissä hankkeissa painopiste oli yksittäisten kyvykkyyksien ja valmiuksien vahvistamisessa.

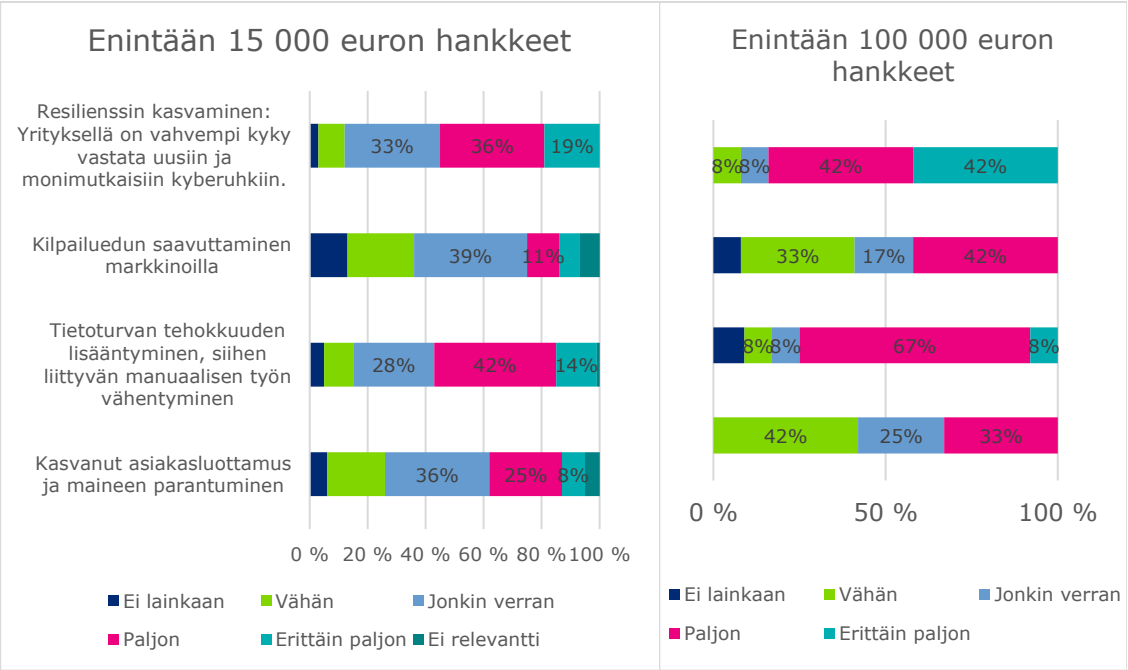


Kuva 13. Onko yrityksessänne saatavilla mitattavaa dataa tietoturvahankkeen hyödyistä? (esim. poikkeamailmoitukset, havaitsemisen kulunut aika, reagointiin kulunut aika, auditoinneissa havaitut puutokset, henkilöstökoulutettujen määrä, estettyjen hyökkäysten määrä). n=113. Lähde: Forefront Oy:n kysely.

Pidemmän aikavälin strategiset hyödyt

Yrityksiltä kysyttiin myös, missä määrin hanke on synnyttänyt heille pitkän aikavälin strategisia hyötyjä. Tietoturvaan liittyvän resilienssin kasvaminen koettiin suurimmaksi pitkän aikavälin hyödyksi (55 % pienistä ja 84 % suurista hankkeista vastasi paljon tai erittäin paljon). Toiseksi suurimmaksi pitkän aikavälin vaikutukseksi koettiin tietoturvan tehokkuuden lisääntyminen (56 % pienistä ja 75 % suurista hankkeista vastasi paljon tai erittäin paljon).

Osa yrityksistä koki myös, että hankkeen kautta se on pystynyt saavuttamaan kilpailuetua markkinoilla (18 % pienistä ja 42 % suurista hankkeista vastasi paljon tai erittäin paljon) ja kohottamaan asiakasluottamusta (33 % pienistä ja 33 % suurista hankkeista vastasi paljon tai erittäin paljon). Haastatellut yritykset totesivat, että asiakkaiden tietoturvatietoisuus on kasvanut viime vuosina niin paljon, että ilman hankkeessa tehtyjä parannuksia, markkinalla olisi todella vaikea toimia enään lainkaan. Tietoturvaparannukset nähtiin näin olen välttämättöminä myös liiketoiminnan jatkuvuuden kannalta.



Kuva 14. Missä määrin organisaatiolle on syntynyt tai odotetaan syntyvän seuraavia pitkän aikavälin strategisia hyötyjä tuen ansiosta? n=113. Lähde: Forefront Oy:n kysely.

3.3.4 Koetut riskit suhteessa tuen avulla tehtyihin parannuksiin

Suuremmissa hankkeissa suurimmiksi ja todennäköisimmiksi riskeiksi arviotiin järjestelmien ja infrastruktuurin haavoittuvuudet[11] ja toimitusketjuriskit.[12] Näissä molemmissa raportoitiin myös vähiten parannuksia hankkeiden aikana. Tätä selittänee se, että laitteiden ja teollisuusautomaation tietoturvan parantaminen on hyvin työlästä ja resurssi-intensiivistä. Näin ollen on ymmärrettävää, että varsinkin pienemmissä hankkeissa nämä jäävät vähemmälle huomiolle. Eräs haastateltu yritys kertoi, että vanhentuneet järjestelmät ovat tulleet vuosien saatossa useilta eri toimittajilta, ja niiden toiminta sekä toisiinsa kytkeminen on usein kuin musta laatikko, josta ei välttämättä ole olemassa dokumentaatiota. Tästä syystä järjestelmien päivittäminen tietoturvalliseksi on hyvin resurssi-intensiivistä. Toinen haastateltava taas kuvasi tilannetta niin, että tietoturva on usein laitekohtaista ja vanhemmissa laitteissa ei useinkaan ole tarvittavia järjestelmiä, joten olisi mahdotonta tietää, jos näissä olisi joku tietoturvariski. Molemmat näistä

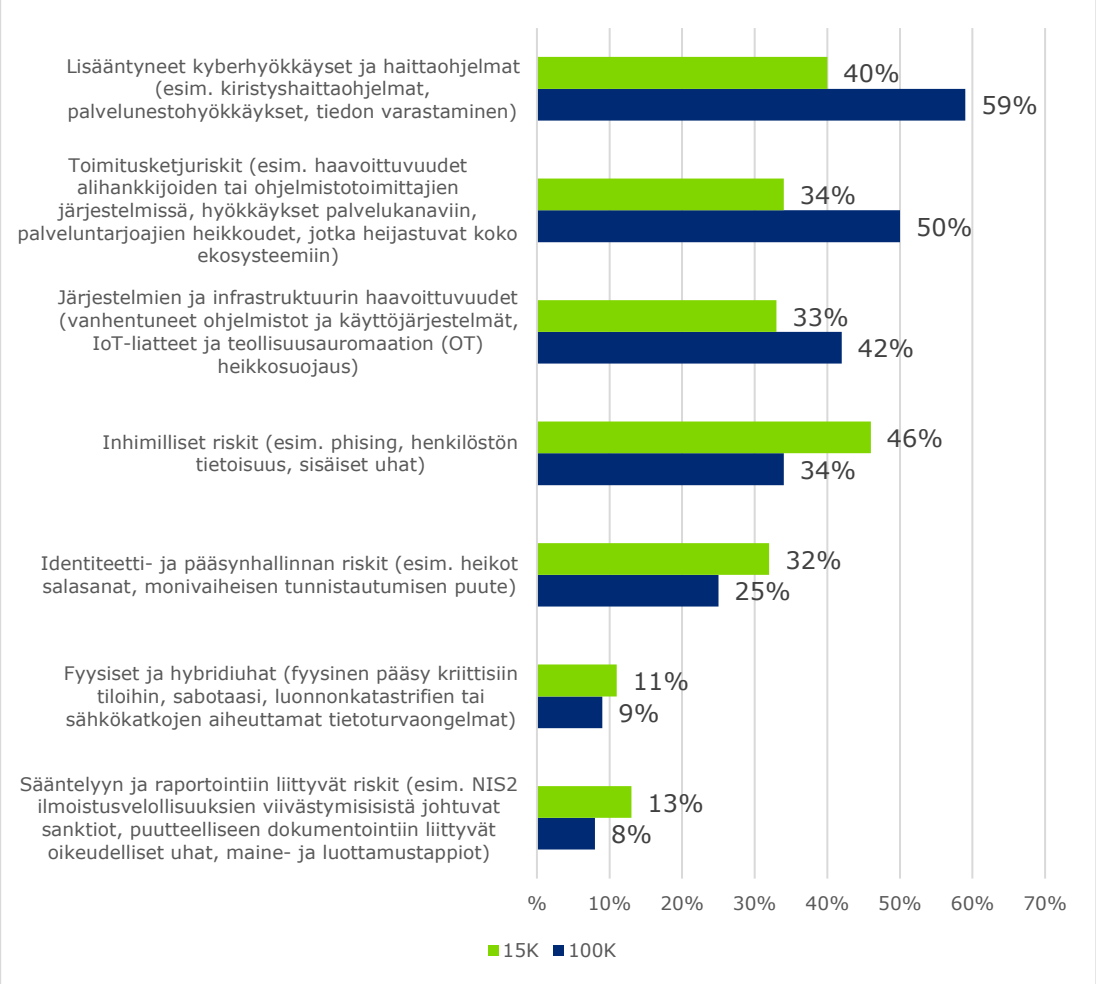
[11] Esim. vanhentuneet ohjelmistot ja käyttöjärjestelmät, IoT-laitteet ja teollisuusautomaation (OT) heikko suojaus
[12] Esim. haavoittuvuudet alihankkijoiden tai ohjelmistotoimittajien järjestelmissä, hyökkäykset palvelukanaviin, palveluntarjoajien heikkoudet, jotka heijastuvat koko ekosysteemiin

yrityksistä kuitenkin päivittivät tietoturvan kehittämisen tuella juuri näitä vanhempia järjestelmiä.

Noin 60 prosenttia suurista ja 40 prosenttia pienistä hankkeista arvioi, että lisääntyneet kyberhyökkäykset ja haittaohjelmat (esim. kiristyshaittaohjelmat, palvelunestohyökkäykset, tiedon varastaminen) muodostavat suuren tai erittäin suuren ja todennäköisen riskin. 37 prosenttia suurista ja 29 prosenttia pienistä hankkeista arvioi, että hankkeen avulla on onnistuttu vähentämään kyberhyökkäyksiä paljon tai erittäin paljon.

Pienemmistä hankkeista 46 prosenttia arvioi inhimilliset riskit (esim. phising, henkilöstön tietoisuus, sisäiset uhat) suureksi tai erittäin suureksi ja hyvin todennäköisiksi. Suuremmissa hankkeissa vastaava osuus oli 34 prosenttia. Hankkeissa suurimmat parannukset saavutettiin nimenomaan henkilöstön osaamista ja tietoisuutta parantamalla, joten hankkeilla onnistuttiin vastaamaan hyvin juuri tähän riskiin.

Sääntelyyn ja raportointiin liittyvät riskit sekä fyysiset ja hybridi uhat koettiin suhteellisen vähäisiksi sekä pienissä, että suurissa hankkeissa.



Kuva 15. Kuinka suureksi arvioisit seuraavat riskit yleisesti omalla toimialallasi? n=114. Lähde: Forefront Oy:n kysely.

3.3.5 Yhteenveto suorista vaikutuksista

Tietoturvan kehittämisen tuen avulla toteutetuissa toimenpiteissä korostuu käytännönläheinen kehittäminen ja osaamisen vahvistaminen. Toimenpiteet kohdistuivat eniten ohjelmistoihin ja hallinnolliseen tietoturvaan, sekä henkilöstön osaamiseen. Suuremmat hankkeet painottivat myös laite- ja tuotantoteknologian suojausta (75 % vs. 58 %). Hankkeet toteutettiin pääasiassa hankkimalla konsultointipalveluita, tarkastus- ja arviointitöitä sekä ostamalla koulutuksia. Suuremmat hankkeet rakensivat pitkäjänteisesti kyvykkyyksiä, kun taas pienemmät hankkeet vahvistivat perustasoa. Asiakkaiden tietoliikenteeseen ja tietoihin kohdistuvat toimet, toimitusketjujen ja OT-ympäristöjen tietoturva sekä toimitilaturva jäivät vähäisemmälle huomiolle.

Tuen lisäisyys oli pieniä hankkeita ajatellen selvästi kiihdyttävä. 91 % ilmoitti, ettei hanke olisi toteutunut lainkaan tai olisi toteutunut vain osittain ilman tukea. Suurissa hankkeissa vastaava vaikutus oli rajallisempi. 16 % yrityksistä olisi tehnyt toimenpiteiteet saman suurisina joka tapauksessa. Tavoitteet saavutettiin kuitenkin hyvin (100 % suurista ja 91 % pienistä suuressa tai erittäin suuressa määrin). Tuki paransi tietoturvan jalkauttamista, nosti teemaa johdon agendalle ja paransi dokumentointia. Vaikutusten intensiteetti oli suurissa hankkeissa useammin vahvempi, kun pienissä vaikutukset koettiin useammin osittaisiksi. Molemmissa tukiluokissa toimitusketjujen ja OT:n tietoturvan osalta vaikutukset jäivät matalemmiksi.

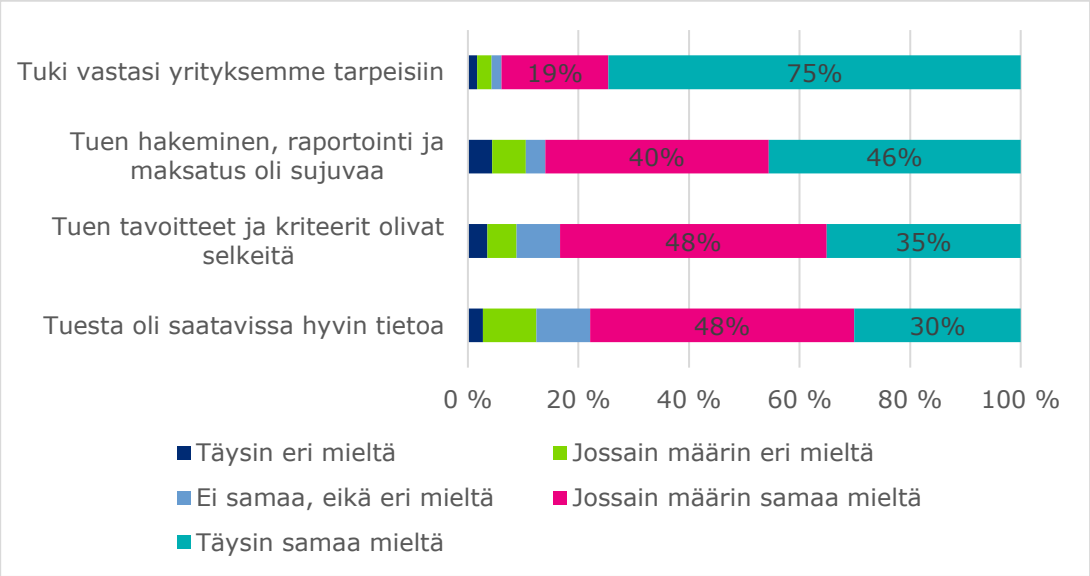
Pitkällä aikavälillä suurimmat hyödyt liittyvät resilienssin kasvattamiseen ja tehokkuuden parantamiseen. Osa raportoi myös kohonneesta kilpailuedusta ja asiakasluottamuksesta, mutta tämä oli huomattavasti yleisempää suuremmissa hankkeissa.

3.4 Tuen tarvevastaavuus

Kyselyn ja haastatteluiden perusteella tuki koettiin hyvin sopivana yrityksen tarpeisiin. Haastatteluiden pohjalta tuki koettiin myös hyvin oikea aikaisena, yritykset raportoivat nopeasta tietoturvaan liittyvästä tietoisuuden lisääntymisestä sekä johdon, että asiakkaiden parissa. Osittain tähän vaikuttaa julkisuudessakin esiintyneet haasteet, esim. Vastaamo-tapaus, jossa terveyspalvelun asiakkaiden tietoja vuoti julkisuuteen. Tällä nähtiin olevan kahdenlaisia vaikutuksia. Toisaalta asiakkaat ovat huomattavasti tietoisempia riskeistä ja vaativat toimittajiltaan parempaa tietoturvan tasoa. Toisaalta tämä on myös auttanut perustelemaan johdolle tietoturvainvestointeja.

Valtaosa tuensaajista oli tyytyväisiä myös tuen hakemiseen ja maksatukseen (85 %). Joillain oli kuitenkin yksittäisiä haasteita tuen hakemisen kanssa, jotka liittyivät ensi sijassa siihen, miten tuen ehdot ymmärrettiin, esim. mikä on tukikelpoista ja mikä ei. Osa myös raportoi, että tuesta ja

sen ehdoista olisi voinut tiedottaa paremmin. Haastatteluiden pohjalta voidaan todeta, että yritykset, joilla ei ollut entuudestaan kokemusta julkisen tuen hakemisesta, olivat niitä, joilla haasteita ilmeni. Ne yritykset, joilla oli jo kokemusta erilaisten julkisten tukien hakemisesta, kokivat tietoturvan kehittämisen tuen hakemisen suhteessa muihin tukiin hallinnollisesti kevyeksi ja helpoksi.



Kuva 16. Ota kantaa seuraaviin väittämiin. n=114. Lähde: Forefront Oy:n kysely.

Rahoituksen riittävyys

Kyselyssä kerättiin myös avovastauksia liittyen rahoituksen riittävyyteen. Pienemmän, enintään 15 000 euron tukiluokan hankkeissa rahoitus koettiin yleisesti hyödylliseksi mutta rajalliseksi. Tuki mahdollisti usein tärkeän ensiaskeleen tietoturvan kehittämisessä, kuten koulutusten, auditointien tai teknisten ratkaisujen käynnistämisen, mutta monissa vastauksissa korostui tarve jatkaa kehitystyötä omarahoitteisesti. Useat vastaajat mainitsivat, että rahoitus ei riittänyt laajempiin teknisiin investointeihin, kuten lokienhallintaan, automaatioon tai penetraatiotestaukseen. Moni piti summaa "pienenä mutta merkittävänä potkuna" ja toi esiin, että erityisesti koulutukseen ja jatkuvaan ylläpitoon olisi tarvittu lisää tukea. Pienemmässä tukiluokassa rahoitusta piti riittävänä noin puolet. Noin kolmannes sen sijaan koki sen riittämättömäksi tai toi esiin selkeitä rajoitteita, kuten sen, ettei testauksia, koulutuksia tai laajempia teknisiä investointeja voitu toteuttaa.

Suuremmassa, enintään 100 000 euron tukiluokassa rahoitus arvioitiin useimmiten riittäväksi suhteessa hankkeen laajuuteen. Useat vastaajat kokivat tuen kattaneen suunnitellut toimet hyvin, vaikka yksittäisiä rajauksia mainittiin. Esimerkkeinä näistä olivat aikataulun rajoitteet, testauksen laajuus ja tarve keskittyä vain tiettyyn osa-alueeseen. Osa kertoi käyttäneensä myös omaa rahoitusta tukemaan laajempaa kokonaisuutta. Näissä hankkeissa tuki mahdollisti merkittäviä investointeja, kuten SOC-

palveluiden, penetraatiotestauksen tai MFA-järjestelmien käyttöönoton, ja loi pysyvän pohjan jatkuvalle tietoturvakehitykselle.

Tuen palauttaminen

Tukea palautettiin ja takaisinperittiin yhteensä noin 430 000 euroa, eli noin 7 prosenttia myönnetystä tuesta. Tukea palautti ja sitä takaisinperittiin yhteensä 68 yritykseltä.

Kyselyssä tiedusteltiin syitä, jotka olivat johtaneet palautuksiin. Syyt liittyivät pääasiassa aikatauluhaasteisiin, kuten liian lyhyeen toteutusjaksoon, palveluntarjoajien ruuhkaan tai siihen, että osa hankkeista meni päällekkäin muiden projektien kanssa. Joissakin tapauksissa palautus johtui hallinnollisista syistä, esimerkiksi siitä, että kustannuksia ei hyväksytty tukikelpoisiksi, koska ne sijoittuivat tuen ulkopuoliselle ajanjaksolle tai tukiehtojen tulkinta muuttui maksatusvaiheessa. Joillain oli myös epäselvyyksiä hyväksyttävien toimenpiteiden kanssa.

Traficomin asiantuntijoiden haastatteluiden mukaan hakijoiden esiin nostamat haasteet näkyivät selvästi myös viranomaisen näkökulmasta. Asiantuntijat korostivat, että takaisinperintöjen ja palautusten määrä oli lopulta huomattavan suuri, mikä heidän arvionsa mukaan olisi osin voitu ehkäistä sillä, että tuki olisi maksettu vasta hankkeen päätyttyä toteutuneita kustannuksia vasten. Lisäksi monien tuen käyttöä koskevien selvitysten laatu muodostui ongelmaksi. Osassa raporteista hanketta oli kuvattu vain parilla lauseella, minkä vuoksi Traficomin oli pyydettävä lisätietoja ennen maksatusten hyväksymistä. Myös hylättyjen kustannusten taustalla oli selkeitä tulkintaeroja siitä, mitkä hankinnat kehittävät yrityksen tietoturvaa. Useissa hakemuksissa oli sisällytetty kustannuksiin esimerkiksi läppäreitä, tabletteja, printtereitä ja palvelimia, joita Traficom piti yleisen liiketoiminnan tukena eikä varsinaisina tietoturvan kehittämistoimina. Asiantuntijoiden mukaan osa näistä epäselvyyksistä olisi ehkä voitu välttää tarkemmalla ennakko-ohjeistuksella, mikä tarjoaa oppeja tulevien avustuskierrosten suunnitteluun.

Tukeen liittyvät haasteet

Kyselyssä pyydettiin avovastuksia tukeen liittyviin haasteisiin. Yleisimmät haasteet liittyivät hallinnollisiin ja aikataulullisiin kysymyksiin. Useat vastaajat kuvasivat tukiprosessin päätösten ja maksatusvaiheiden keston olleen liian pitkiä, mikä aiheutti epävarmuutta ja viivästytti hankkeiden käynnistystä tai toteutusta. Raportointia ja ohjeistuksia pidettiin osin raskaina ja epäselvinä, etenkin pienille yrityksille. Moni mainitsi myös, että tuen käyttöehtojen ja hyväksyttävien kustannusten tulkinta oli vaikeaa.

Hankkeiden toteuttamisessa ilmeni jotain haasteita erityisesti liittyen osaajien ja palveluntarjoajien saatavuuteen. Sopivia asiantuntijoita ei aina ollut

tarjolla, tai he keskittyivät vain suuriin yrityksiin. Joissakin hankkeissa aikataulut olivat liian tiukat, ja pienet yritykset kokivat resurssien riittämättömyyden rajoittavan toteutusta. Muutamat mainitsivat myös, että tietoturvakehittämisen jatkuva luonne tekee kertaluonteisesta tukimallista haastavan. Samalla kuitenkin useat vastaajat totesivat, ettei merkittäviä ongelmia ollut ja että tuki helpotti johdon sitoutumista tietoturvapanostuksiin, vaikka byrokratia ja aikarajat toivat lisätyötä.

Kyselyssä pyydettiin yrityksiä myös kertomaan, miten Traficom voisi parhaiten auttaa yrityksiä tietoturvan parantamisessa. Vastauksissa korostui erityisesti tarve selkeämmälle ja käytännönläheisemmälle ohjeistukselle sekä rahoitusinstrumenttien jatkamiselle ja kehittämiselle. Yritykset toivoivat yksinkertaistettuja, konkreettisia ohjeita eri tietoturvan osa-alueille, esimerkiksi hyökkäysten tunnistamiseen, NIS2-direktiivin vaatimuksiin ja passwordless-ratkaisuihin. Osa toivoi myös esimerkkimateriaalia, jota voisi hyödyntää suoraan johtoryhmien päätöksenteossa. Moni toivoi myös, että Traficom tuottaisi virallisia esittelyjä ja teknologiasuosituksia, joiden avulla yritykset voisivat perustella investointejaan uskottavammin. Pienemmille yrityksille kaivattiin kansankielistä tiedottamista, selkeämpää tukiehtojen viestintää ja mahdollisuutta sähköiseen asiointiin tukiprosessin hallinnoinnissa.

3.5 Tuen epäsuorat vaikutukset

3.5.1 Tietoturvaratkaisujen globalisaatio ja markkina

Globalisaatio ja suurten toimijoiden tarjonta tasaa pelikenttää, mutta palveluiden keskittyminen tuo uusia uhkia

Varautumisen kannalta ei enää riitä, että palveluita ja teknologioita hankitaan pistemäisesti ja lähiajan tarpeeseen. Huomioon on otettava kokonaisarkkitehtuureja ja systeemitasoisia kokonaisuuksia sekä ymmärrettävä suurien globaalien toimijoiden tarjonta, sen kehittyminen ja monasti monimutkainen hinnoittelu.

Kuvattu kehitys ei ole, erityisesti pk-yritysten kannalta, ongelmaton. Toisaalta valitsemalla, ja käytännössä myös sitoutumalla, laajan globaalin toimijan kuten Microsoftin tarjontaan, saa asiakas varmuutta ja mahdollisuuden hyvinkin laajaan kyberturvatarjontaan ja -turvaan. Tällä on kuitenkin merkittävä hintalappu ja se voi olla liian kova monelle pk-yrityksille, ja jopa suuryritykselleki n. Microsoftin tyyppisten globaalien toimijoiden lisenssimaksut ovat mittavia ja asiakkaiden neuvotteluvoima hintakeskusteluissa vähintäänkin vaatimaton. Lisäksi tuoteroadmappien, -paketointien ja -hinnoittelun ymmärtäminen ja ennakointi vaatii myös hyvää perehtyneisyyttä ja ajallista panostusta. Tämäkin lisää kustannuksia. Vaakakupin toisella puolella ovat toimittajasta irtautumisen kustannukset. Ne voivat olla varsin merkittäviä ja ajallisesti pitkäkestoisia.

Edellä kuvattu kehitys tarkoittaa myös sitä, että yritysten käyttämät ratkaisut standardoituvat ja kansalliset erot pienenevät. Jos aiemmin Suomessa oltiin ainakin Euroopan mittakaavassa edelläkävijöitä tietoturvateknologioiden kehittämisessä ja soveltamisessa, on tämä jatkossa varsin vaikeaa. Organisaatioissa ja niiden järjestelmissä on yhä enemmän samoja haavoittuvuuksia kuin muilla. Jos organisaatiolla on tavoitteita, osaamista ja rahallisia resursseja investoida ja kehittää turvaa verrokkejaan paremmaksi, ovat investointikohteet yhä enenevässä määrin muiden hallinnassa, kuten globaaleissa pilvipalveluissa. Asiakkaiden mahdollisuudet vaikuttaa pilvipalveluiden suojaustasoon, prosesseihin ja turvakontrolleihin ovat hyvin vaatimattomat.

Esimerkkinä tästä, vuonna 2025 Donald Trump allekirjoitti toimeenpanomääräyksen, jonka mukaan International Criminal Court (ICC) ei saa teknologista tai taloudellista tukea Yhdysvalloista tai sen liittolaisilta. Tämän seurauksena Microsoft keskeytti ICC:n pääsyä sähköpostipalveluihinsa. Tämä osoittaa, miten globaali teknologiatoimija voi joutua poliittisen painostuksen välineeksi. Tämä tapaus havainnollistaa sitä, että yrityksillä ei enää ole täyttä päätäntävaltaa omissa palveluissaan, kun ne ovat riippuvaisia suurten globaalien toimijoiden alustoista ja lainsäädännöllisistä vaikutuksista, jotka voivat leikata palveluvalintoja poliittisin perustein.

Kyberturvan kokonaismarkkina kasvaa voimakkaasti

Kyberturvatuotteiden ja palveluiden globaalin markkinan arvioitiin oleva vuonna 2023 160 miljardia euroa ja kasvavan vuoteen 2032 mennessä 523 miljardiin euroon. Tämä tarkoittaa merkittävää 14,3%:n vuotuista CAGR -kasvua. Palveluiden markkina kasvaa tuotemarkkinaa nopeammin 20,2 %:n CAGR-kasvulla 61,7 miljardiin euroon.[13]

Suomen kyberturvan kokonaismarkkinan on arvioitu olevan 1,3 miljardia euroa. [14] Kyberturvaan keskittyneitä yrityksiä on FISC ry:n jäsenkuntaan perustuvan arvion mukaan noin 50 kpl.[15] Yhä suurempi osa Suomessa toimivista yhtiöistä on palveluyhtiöitä, sillä aiemmin kuvatun kehityksen seurauksena suuret globaalit kyberturvaa tarjoavat tahot, kuten Palo Alto Networks, Fortinet, Cisco, Microsoft, CrowdStrike ovat tehneet paljon yritysostoja ja pyrkivät kasvamaan tavoitteenaan kattaa yhä suurempi osa ostajakunnan budjeteista. Tämä jättää vähemmän tilaa kapeille ja pienemmille toimijoille. Toisaalta kansallisten palvelutoimittajien kuten DNV Cyber, entinen Nixu Oyj, merkitys asiakkaiden kyberturvakokonaisuudessa saattaa kasvaa, koska tuotteiden integroiminen ja hallinta on yhä haastavampaa

[13] Fortune Business Insight https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
Last Updated: October 07, 2024 Report ID: FBI101165
[14] FISC ry, Finnish Information Security Cluster
[15] FISC ry, Finnish Information Security Cluster

digitalisaation laajetessa sekä kybertuotteiden ja palveluiden moninaistuessa.

Laajojen kyberturvaratkaisujen käyttöönotto koskee laajasti myös koko yritystä, esimerkiksi sen prosesseja, vastuiden määrittelyjä ja tiedon luokittelua. Jotta turvallisuus saavuttaa suunnitellun tason, on monen fundamentin oltava kunnossa. Esimerkiksi Zero Trust -konseptien käyttöönotto nojaa vahvasti siihen, että identiteettien ja käyttäjien hallinta on kunnossa. Tämä näkyy IAM[16] -palveluiden ja konsulttien kysynnässä. Suomessa on perinteisesti ollut laadukasta IAM-osaamista sekä omien tuotteiden, että palvelutarjonnan osalta.

3.5.2 Tuen vaikutukset muihin yrityksiin

Kokonaisuutena tuen markkinavaikutusten arvioidaan olevan rajalliset, sillä tuen kokonaisvolyymi on pieni suhteessa markkinoiden kokoon. Suomen koko kyberturvallisuusmarkkinan arvoksi on arvioitu noin 1,3 miljardia euroa.

Myönnetyn tuen kokonaismäärä oli kahden vuoden aikana noin 6 miljoonaa euroa, pois lukien tuensaajien omat investoinnit. Selvitysten analyysin perusteella tuki vivutti yrityksiltä omarahoitusta vähintään[17] noin 3,3 miljoonaa euroa (1,3 miljoonaa suuremmissa ja 2 miljoonaa pienemmissä hankkeissa). Suuremmat hankkeet laittoivat keskimäärin 60 000 euroa omaa rahaa ja pienemmät hankkeet noin 8 000 euroa hankeen toteuttamiseen.[18]

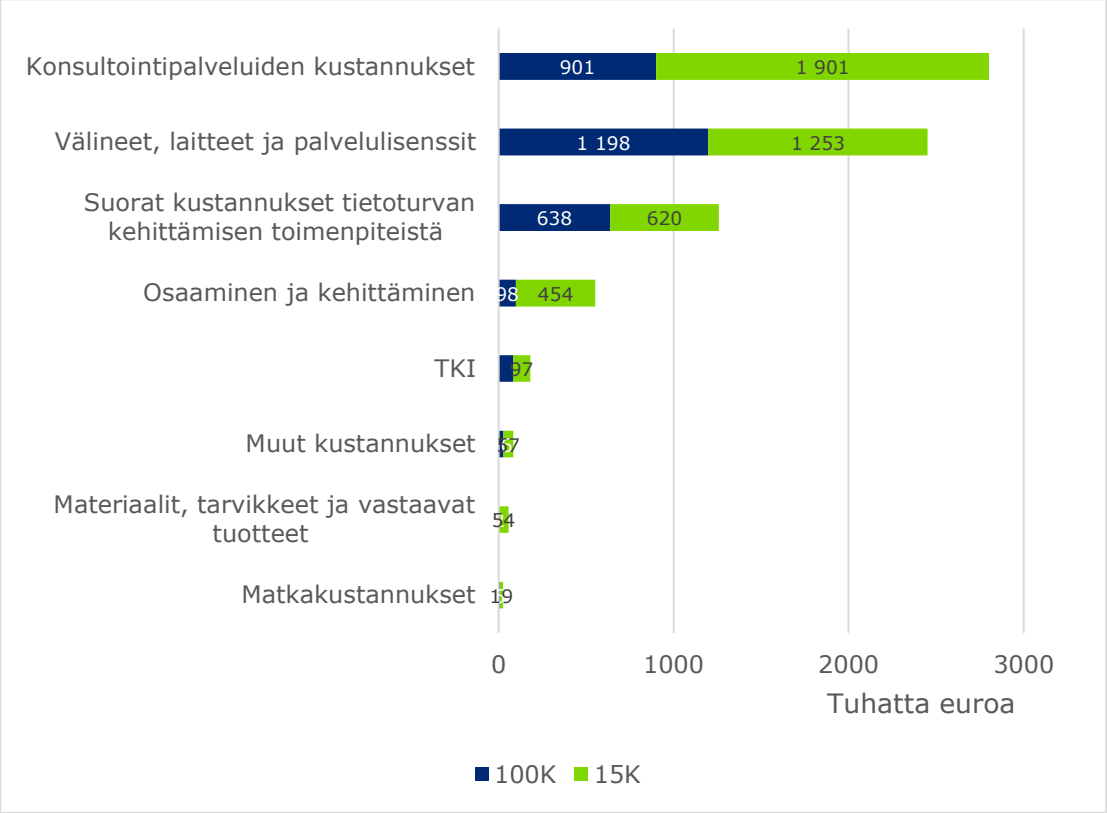
Hankkeissa palvelu- ja muihin ostoihin käytettiin rahaa noin 7,4 miljoonaa euroa. Tukirahoituksella ja omalla rahoituksella katettiin erityisesti konsultointipalveluihin liittyviä kustannuksia (n. 0,9 milj. euroa suurissa ja n. 1,9 milj. euroa pienemmissä hankkeissa), välineiden ja laitteiden ostoja sekä palvelulisenssien kustannuksia (n. 1,2 milj. euroa suurissa ja n. 1,3 milj. euroa pienissä hankkeissa) sekä muita suoria toimenpiteisiin liittyviä kustannuksia (n. 0,6 milj. euroa suurissa, että pienissä hankkeissa). Osaamisen kehittämiseen liittyviä palveluita ostettiin yhteensä noin 0,6 miljoonalla eurolla. Tutkimus-, kehittämis- ja innovaatiotoimintaan käytettiin alle 0,1 miljoonaa euroa.

Arvioinnin puitteissa ei ole mahdollista tarkasti eritellä, missä määrin palvelut ja muut hankinnat kohdentuivat suomalaisille toimittajille. Vaikuttaa kuitenkin siltä, että valtaosa palveluista on ostettu suomalaisilta toimittajilta, kun taas välineet, laitteet ja palvelulisenssit kohdentuivat suurissa

[16] IAM, Identity and Access Management
[17] Jos yritys toteutti suuren tietoturvahankkeen, jonka osana oli myös 15 tuhannen euron tietoturvan parantamisen avustus, Traficom ei vaatinut yritystä kuvaamaan selvityksessä hanketta kokonaisuudessaan, vaan vähintään käytetyn valtionavustuksen osalta.
[18] Luvut perustuvat arvioon. Osa selvityksistä oli täytetty epätäydellisesti, mistä syystä luku ei ole täydellinen.

määrin monikansallisille toimijoille (esim. Microsoft). Selvitysten laadullisen analyysin pohjalta voidaan myös todeta, että osa monikansallisille toimijoille kohdentuvista lisenssimaksuista menee myös suoraan konsulttipalveluiden kautta, sillä ne on joissain tapauksissa sisällytetty konsulttipalveluihin.

Kuten aiemmissa luvuissa on todettu, kyberturvallisuusratkaisujen markkinassa on käynnissä globaali kehitys, jossa markkinoita keskittyy suurille monikansallisille yrityksille. Tämä kehitys tarjoaa useita mahdollisuuksia, mutta luo samalla uhkia kansalliselle omavaraisuudelle. Suomalaisten kyberturvallisuusyritysten joukossa on kansainvälisesti kilpailukykyisiä ratkaisuja, mutta alan keskittyminen haastaa tätä asemaa. Yhä suurempi osa suomalaisista kyberturvallisuusyrityksistä toimii nykyisin palveluntarjoajina sen sijaan, että ne kehittäisivät omia ratkaisujaan.



Kuva 17. Tukirahoituksella katettavat tukikelpoiset menot niiden kohteiden mukaan. Lähde: rahoitusselvitykset, Traficom.

3.5.3 Tuen vaikutukset yhteiskuntaan

Yhteiskunnan kannalta kriittiset yritykset muodostavat yhteiskunnan toimintakyvyn selkärangan. Näiden yritysten kyberturvallisuus vaikuttaa suoraan yhteiskunnan häiriönsietokykyyn ja toimitusketjujen luotettavuuteen. Pienet ja keskisuuret yritykset voivat olla usein myös kytköksissä muihin yhteiskunnan kannalta kriittisiin organisaatioihin asiakkuuksien tai

toimitusketjujensa kautta. Jos yrityksen asiakkaat toimivat kriittisillä aloilla, asiakkaiden tietoturva on välillisesti riippuvainen kumppaniyritysten tietoturvan tasosta. Siksi tietoturvan perustason varmistaminen yhteiskunnan kannalta kriittisissä pk-yrityksissä vahvistaa merkittävästi koko kansallista kyberturvallisuuskyvykkyyttä.

On myönteistä, että tuki on suunnattu ensisijaisesti yhteiskunnan kannalta kriittisille sektoreille ja yrityksille, sillä juuri näillä aloilla ja näihin kohdistuviin yrityksiin tietoturvaloukkauksilla voi olla laajimmat vaikutukset yhteiskunnan toimintaan. Suomessa kriittistä infrastruktuuria ja toimintaa on kuitenkin paljon myös kunnallisella sektorilla ja kuntien omistamissa yhtiöissä – esimerkiksi energia-, vesi-, liikenne- ja sosiaali- ja terveyspalveluissa – mutta kuntaorganisaatiot oli rajattu tuen ulkopuolelle. Tämä rajaus tarkoittaa, että osa yhteiskunnan keskeisistä toimijoista jäi tuen ulkopuolelle, vaikka niiden kyberturvallisuuden vahvistaminen olisi yhteiskunnan kokonaisturvallisuuden kannalta perusteltua.

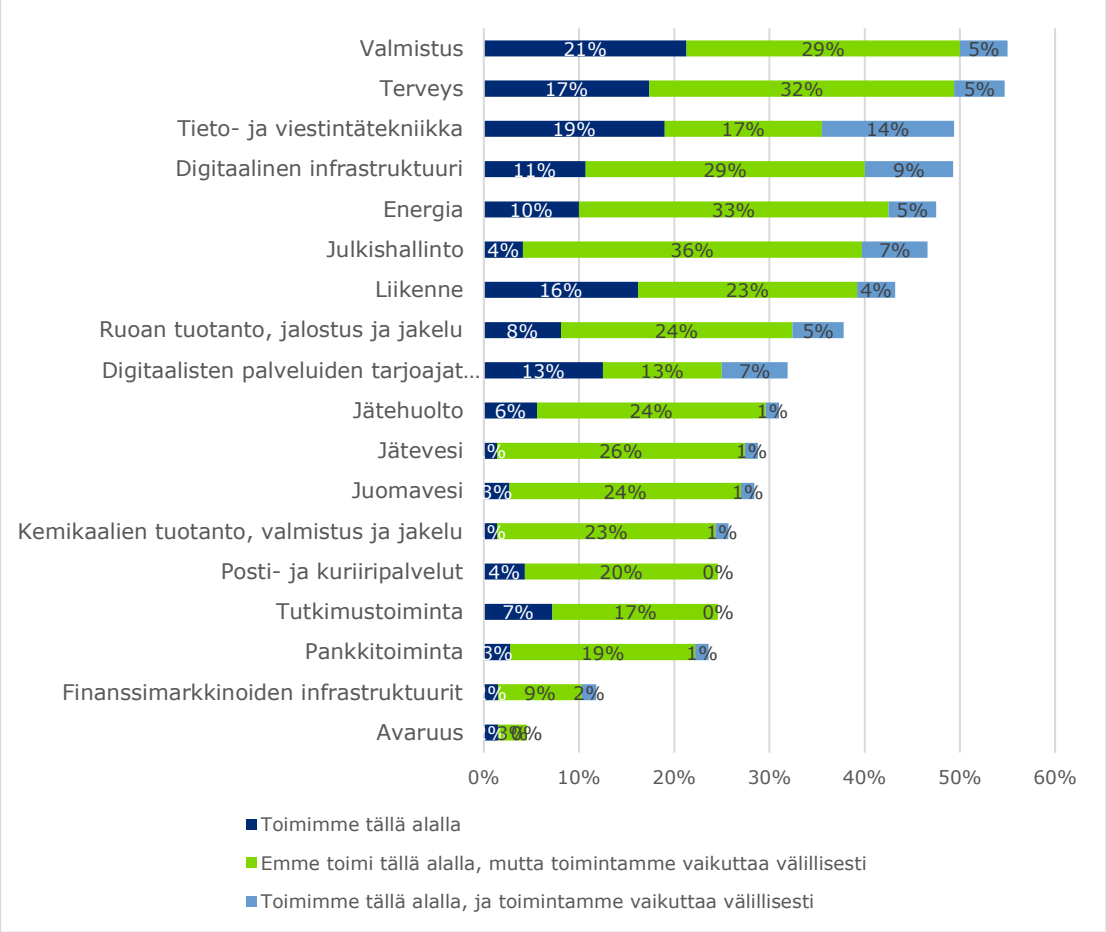
Huoltovarmuuskeskuksen (HVK) toimialojen kyberkypsyyskartoituksen (2022) mukaan kypsimpiä aloja ovat tele-, ICT- ja finanssiala, joilla on pitkään ollut sekä sääntelyä että omia turvallisuusstandardeja. Sen sijaan satamat, kauppa ja vesihuolto sijoittuvat alle perustason, mikä kertoo resurssien, osaamisen ja järjestelmällisen riskienhallinnan puutteista.

Tuensaajille suunnatussa kyselyssä tiedusteltiin mille kriittisille sektoreille heidän toimintansa sijoittuu suoraan sekä heidän asiakasyritystensä tai toimitusketjujen kautta. Yritykset toimivat laajasti kriittisillä ja yhteiskunnan toiminnan kannalta merkittävillä aloilla tai ovat niihin vahvasti kytkeytyneitä toimitusketjujen ja asiakassuhteiden kautta. Suoraan kriittisillä sektoreilla toimivista korostuvat valmistavateollisuus (26 %), tieto- ja viestintätekniikka (33 %) terveys (22 %) ja liikenne (20 %).

Välillisesti asiakkaidensa kautta tuensaajat vaikuttivat erityisesti julkishallintoon (36 %), energia-alalle (33 %), terveyteen (32 %).

Tuki kohdentui huomattavasti vähemmissä määrin suoraan esimerkiksi jäte- ja juomaveteen (2-4%), finanssimarkkinoiden infrastruktuuriin ja pankkisektorille (4 %), postiin (4 %) sekä jätehuoltoon (6 %). Tuen vaikutukset oletettavasti kohdentuivat kuitenkin epäsuorasti tuensaajien asiakkaiden kautta myös näille sektoreille suhteellisen laajasti.

Tulokset osoittavat, että tuki on tavoittanut yrityksiä, joiden toiminta vaikuttaa laajasti kriittisen infrastruktuurin turvallisuuteen, vaikka osa aloista – kuten julkishallinto ja kunnalliset toimijat – oli virallisesti rajattu tuen ulkopuolelle. Käytännössä tuki on siis vahvistanut kriittisten sektorien kyberturvallisuutta suoraan ja välillisesti toimitusketjujen ja palveluntuottajien kautta, mikä lisää koko yhteiskunnan häiriönsietokykyä.



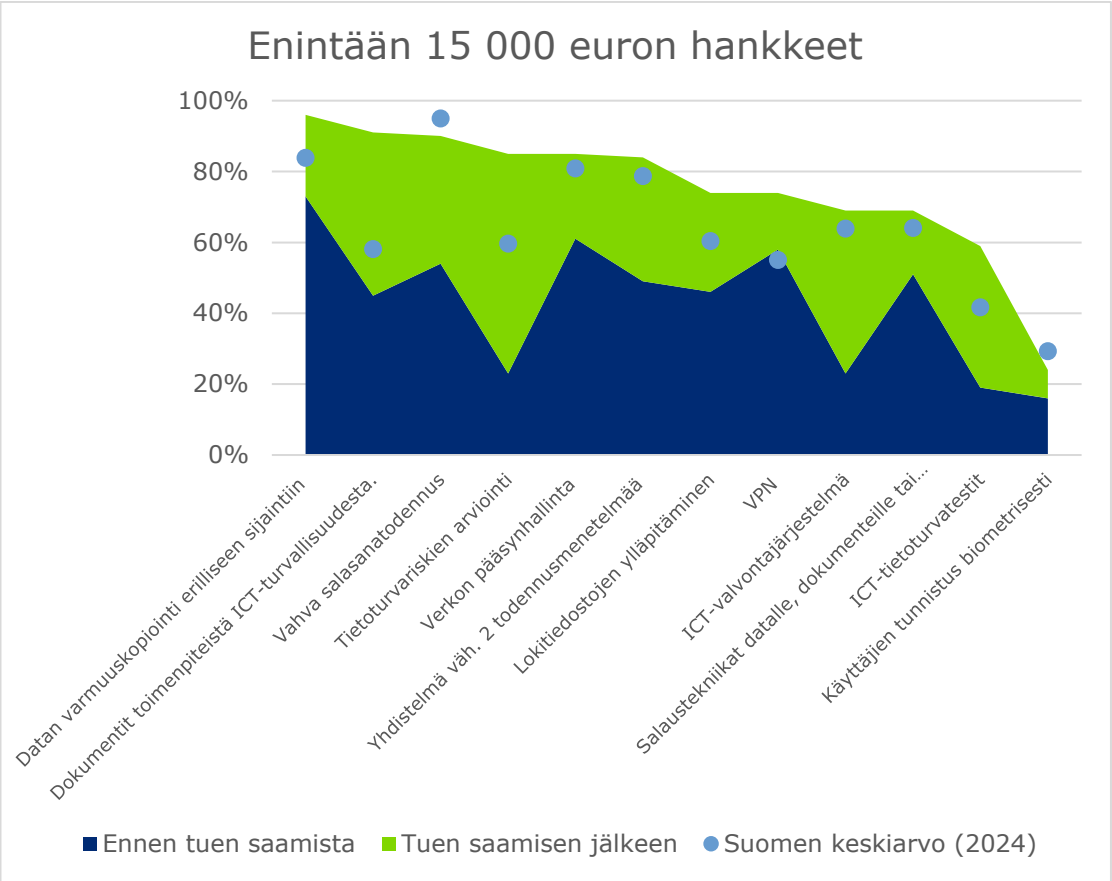
Kuva 18. Millä seuraavista yhteiskunnan kannalta kriittisistä toimialaloista organisaationne toimii (NIS2-direktiivin määritelmä) tai vaikuttaako toimintanne välillisesti niiden toimialojen tietoturvaan (esim. asiakkaat)? n=113. Luokittelu perustuu NIS2-direktiiviin. Lähde: Forefront Oy:n kysely.

3.5.4 Tuen kohdentuminen matalamman kypsyystason yrityksiin

Kansallisen ja EU-tasoisen kyberturvallisuusosaamisen näkökulmasta on ratkaisevan tärkeää, että tietoturvaa parannetaan kaikissa yrityksissä, ei vain edelläkävijöissä. Suomessa yritysten valmiuksissa on suuria eroja, ja yhteiskunnan kokonaiskyvykkyys edellyttää, että kaikki, varsinkin kriittisillä toimialoilla toimivat yritykset kehittävät tietoturvaansa. Tästä syystä on hyvin perusteltua, että tuki kohdistettiin mikroyrityksille ja pk-yrityksille, joilla on usein investointi- ja osaamisesteitä uusien tietoturvaratkaisujen käyttöönotossa. Koska yritysten toiminta on keskenään linkittynyttä, perässä olevien yritysten tukeminen parantaa paitsi yksittäisten yritysten myös koko yhteiskunnan turvallisuutta. Se lisää yhteiskunnan resilienssiä, vahvistaa ekosysteemien turvallisuutta, vahvistaa kriittisiä infrastruktuureja ja vähentää sekä taloudellisia että yhteiskunnallisia riskejä. Lisäksi kansallisen kyberturvallisuuden vahvistaminen parantaa Suomen mainetta turvallisena ja luotettavana maana kansainvälisesti, mikä tukee myös investointeja ja taloudellista houkuttelevuutta.

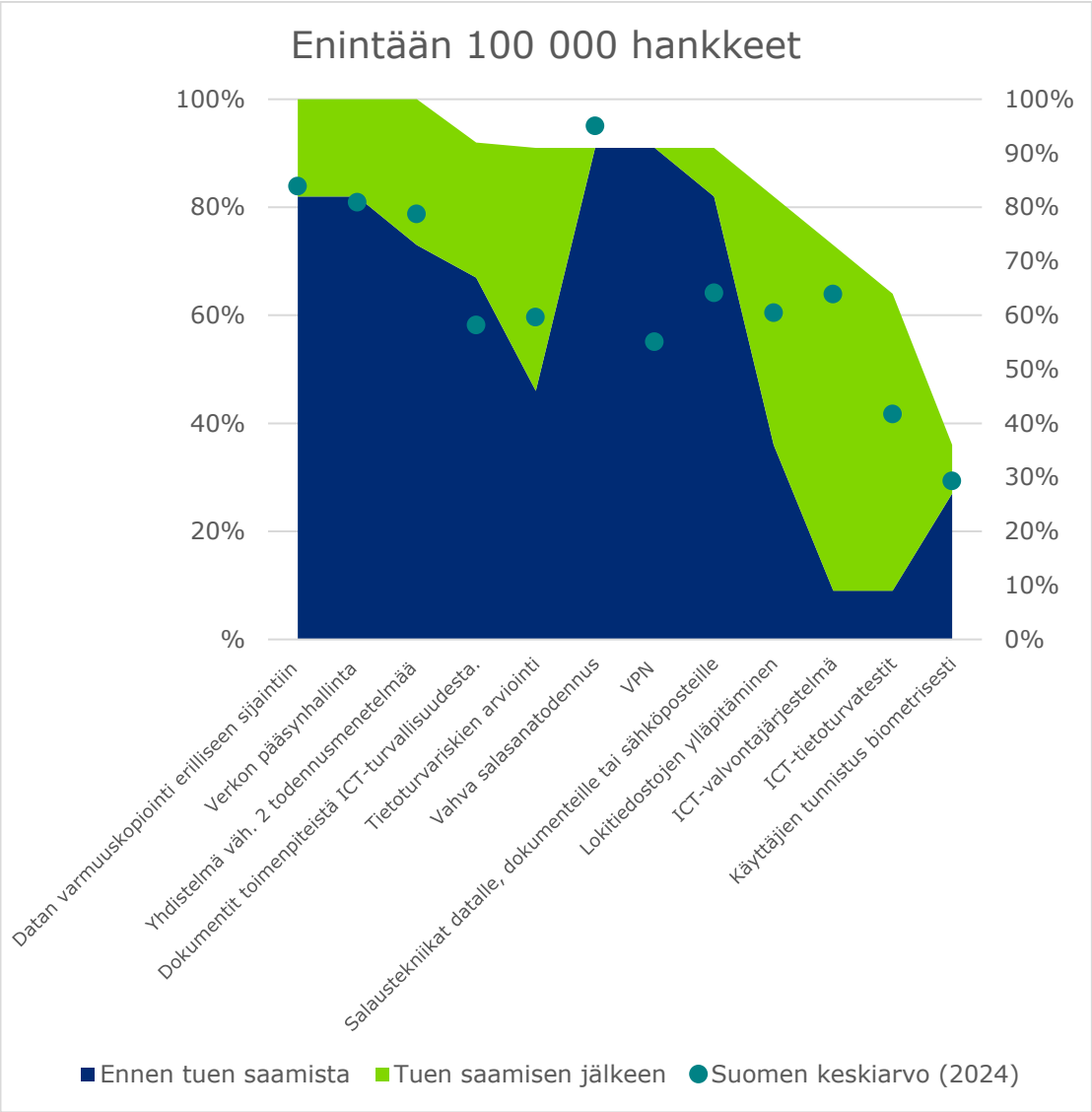
Arvioinnissa verrattiin tuensaajien kyselyvastauksia Eurostatin tietoihin suomalaisten yritysten ICT-tietoturvakäytännöistä. Kyselyn tulokset osoittavat, että erityisesti pienemmät, enintään 15 000 eurona tukea saaneet yritykset olivat ennen tuen saamista selvästi Suomen yritysten keskiarvoyritystä jäljessä lähes kaikilla tietoturvan osa-alueilla. Tämä on linjassa tuen alkuperäisen tavoitteen kanssa, jonka tarkoituksena oli tukea yrityksiä, jotka olivat vasta kehittämässä tietoturvavalmiuksiaan ja tarvitsivat tukea perusasioiden vahvistamiseen. Hankkeiden aikana nämä yritykset ottivat käyttöön useita sellaisia tietoturvatoimenpiteitä, joita niillä ei aiemmin ollut. Suurimmat parannukset nähtiin säännöllisissä tietoturvariskien arvioinnissa, ICT-tietoturvatesteissä ja valvontajärjestelmien käyttöönotossa. Tulokset viittaavat siihen, että hankkeiden päätyttyä pienemmät tuensaajat ovat jo Suomen keskiarvoyritysten yläpuolella useimmilla mittareilla, mikä kertoo merkittävästä kehitysloikasta ja hyvin kohdentuneesta tuesta.

Suurissa, enintään 100 000 euron hankkeissa yritykset olivat jo ennen tukea useimmilla mittareilla Suomen keskiarvon tasolla tai sen yläpuolella, ja tuen avulla ne nousivat keskiarvoa huomattavasti paremmalle tasolle. Poikkeuksena kuitenkin muutamat tekniset osa-alueet, joissa myös suuremmat yritykset olivat lähtötilanteessa keskiarvon alapuolella: lokitiedostojen ylläpito ja analysointi poikkeamien jälkeen, valvontajärjestelmien puutteet, sekä ICT-tietoturvatestien toteuttaminen. Nämä osa-alueet edustavat tyypillisesti kehittyneempiä teknisiä käytäntöjä, joiden käyttöönotto vaatii erityisosaamista ja resursseja – ja siten ne jäävät usein jälkeen jopa edistyneemmissä organisaatioissa. Suurempien hankkeiden osalta voidaan todeta, että tuen avulla on myös tehty suuria parannuksia tietoturvaan, mutta se ei varsinaisesti ole kohdentunut sellaisille yrityksille, jotka olisivat vasta kehittämässä perusvalmiuksiaan.



Kuva 19. Mitä seuraavista tietoturvaa lisäävistä toimenpiteistä oli käytössä a) ennen tuen saamista, b) hankkeen päätyttyä tai pian sen jälkeen? Huom. Vaihtoehtojen tarkemmat kuvaukset alaviitteessä.[19] Suomen keskiarvo perustuu Eurostatin tilastoon Security policy, measures, risks and staff awareness by size class of enterprise [isoc_cisce_ra__custom_18677288] ja se sisältää yritykset, joissa on 10-249 työntekijää. n=101. Lähde: Forefront Oy:n kysely.

[19] * Vaihtoehtojen tarkemmat kuvaukset: *Yhdistelmä vähintään kahta todennusmenetelmää, Datan varmuuskopiointi erilliseen sijaintiin (mukaan lukien pilvivarmuuskopiointi), Verkon pääsynhallinta (laitteiden ja käyttäjien pääsyn hallinta yrityksen verkkoon), Yrityksellä on dokumentteja toimenpiteistä, käytännöistä tai menettelytavoista ICT-turvallisuudesta, Tietoturvariskien arviointi, eli säännöllinen arviointi tietoturvapoikkeamien todennäköisyydestä ja seurauksista, Vahva salasanatodennus, VPN (Virtuaalinen yksityisverkko, joka laajentaa yksityisverkon julkisen verkon yli mahdollistaen turvallisen tiedonvaihdon julkisessa verkossa), Salaustekniikat datalle, dokumenteille tai sähköposteille, Lokitiedostojen ylläpitäminen analysointia varten tietoturvapoikkeamien jälkeen, Valvontajärjestelmä, joka havaitsee epäilyttävää toimintaa ICT-järjestelmissä ja varoittaa siitä yritystä, lukuun ottamatta erillistä virustorjuntaohjelmistoa, ICT-tietoturvatestit, Käyttäjien tunnistus ja todennus yrityksen käyttämillä biometrisillä menetelmillä*



Kuva 20. Mitä seuraavista tietoturvaa lisäävistä toimenpiteistä oli käytössä a) ennen tuen saamista, b) hankkeen päätyttyä tai pian sen jälkeen? Suomen keskiarvo perustuu Eurostatin tilastoon “Security policy, measures, risks and staff awareness by size class of enterprise [isoc_cisce_ra__custom_18677288]” ja se sisältää yritykset, joissa on 10-249 työntekijää. n=12. Lähde: Forefront Oy:n kysely.

3.5.5 Yhteenveto epäsuorista vaikutuksista

Tietoturvan kehittämisen tuella on ollut useita epäsuoria vaikutuksia sekä markkinoihin, muihin yrityksiin että koko yhteiskunnan kyberturvallisuuskyvykkyyteen.

Globaalilla tasolla kyberturvaratkaisujen tuotanto keskittyy yhä harvemmille monikansallisille toimijoille. Tämä kehitys on johtanut siihen, että yritysten omat vaikutusmahdollisuudet käyttämiensä järjestelmien ja palveluiden tietoturvaan ovat kaventuneet. Esimerkiksi Donald Trumpin vuonna 2025 tekemä päätös evätä International Criminal Courtin pääsy Microsoftin palveluihin osoitti, kuinka yritysten riippuvuus globaaleista

teknologiatoimijoista voi altistaa ne geopoliittisille päätöksille, joihin ne eivät itse voi vaikuttaa. Tämä korostaa tarvetta vahvistaa kansallista ja eurooppalaista kyberturvallisuuden omavaraisuutta sekä osaamis- ja palvelupohjaa.

Maailmanlaajuisesti kyberturvamarkkina kasvaa nopeasti: sen arvioidaan nousevan 160 miljardista eurosta vuonna 2023 yli 520 miljardiin euroon vuoteen 2032 mennessä. Palveluiden kysyntä kasvaa tuotemarkkinoita nopeammin. Suomessa kyberturvatoimiala on noin 1,3 miljardin euron kokoinen, ja sen painopiste on siirtynyt ratkaisukehityksestä palvelutuotantoon ja palveluiden integroimiseen ja hallintaan. Tietoturvaseteli on lisännyt tätä kysyntää edelleen, erityisesti auditointi-, koulutus- ja tietojärjestelmäpalveluissa. Hankkeissa palvelu- ja muihin ostoihin käytettiin noin 7,4 miljoonaa euroa, josta noin 2,8 miljoonaa euroa kohdentui konsulttipalveluihin ja noin 2,5 miljoonaa välineiden ja laitteiden ostoihin ja palveluiden lisenssikustannuksiin. Selvitysten analyysin perusteella tuki vivutti yrityksiltä omarahoitusta yhteensä noin 3,3 miljoonaa euroa (1,3 miljoonaa suuremmissa ja 2 miljoonaa pienemmissä hankkeissa).

Toisaalta tuen avulla on hankittu myös lisenssejä monikansallisilta yrityksiltä. Vaikka nämä toki parantavat tietoturvaa, liittyy niihin myös edellä mainittuja geopoliittisia riskejä. Rahoitustuen kokonaismarkkinavaikutukset ovat kuitenkin rajallisia, sillä sen volyymi – noin kuusi miljoonaa euroa kahdessa vuodessa – on pieni suhteessa markkinoiden kokoon.

Tuen tärkein epäsuora vaikutus liittyy sen yhteiskunnalliseen rooliin. Se on vahvistanut kriittisten alojen toimitusketjujen tietoturvaa ja lisännyt pk-yritysten valmiuksia toimia osana kansallisesti merkittäviä ekosysteemejä. Vaikka kunnalliset toimijat jäivät virallisesti tuen ulkopuolelle, tuki on välillisesti vahvistanut myös niiden toimintaympäristöä, koska monet yksityiset toimijat toimittavat palveluita juuri energia-, vesi- ja terveydenhuollon kaltaisille aloille. Näin ollen tuki on lisännyt koko yhteiskunnan kyberresilienssiä, vahvistanut kriittisten verkostojen turvallisuutta ja tukenut Suomen asemaa luotettavana digitaalisena toimintaympäristönä.

Lisäksi tuki on erityisesti pienempien, enintään 15 000 euron hankkeiden osalta kohdentunut yrityksille, joiden tietoturvakypsyys oli keskimääräistä matalampi – juuri näille toimijoille suunnattu rahoitus on ollut keskeistä koko yhteiskunnan kokonaisturvallisuuden kannalta, sillä se on vahvistanut peruskyvykkyyksiä ja kaventanut eroa edelläkävijöiden ja perässä tulijoiden välillä.

4 Johtopäätökset ja suositukset

4.1 Johtopäätökset

Oikeasuhtaisuus ja tarkoituksenmukaisuus

Tuen tarkoituksena oli edistää Suomessa toimivien yhteiskunnan toiminnan kannalta kriittisillä toimialoilla toimivien yritysten tietoturvallisuutta ja kykyä torjua, havaita ja selvittää tietoturvaloukkauksia. Lisäksi tavoite on laajemmin osa kansallista huoltovarmuutta ja kokonaisturvallisuutta. Tuen tarkoituksena on parantaa yhteiskunnan kriittisten toimintojen jatkuvuutta ja varautumista, vähentää kyberturvallisuusuhista aiheutuvia häiriöitä ja lisätä erityisesti pk-yritysten tietoturvan perustasoa.

Tietoturvan kehittämisen tukea voidaan arviointiaineiston perusteella pitää pääosin oikeasuhtaisena ja tarkoituksenmukaisena välineenä edistää yllämainittua tavoitetta. Sen suunnittelu, kohdentaminen ja toimeenpano ovat vastanneet selvästi havaittuun yhteiskunnalliseen tarpeeseen, vaikka tuki oli volyymiltaan rajallinen. Määräraha (6 MEUR) ja pienemmän tukimuodon enimmäissumma olivat pienet suhteessa tarpeeseen. Tuki on ollut hyvin suosittu, hakemuksia tuli runsaasti, mutta moni jäi ilman tukea, mikä kertoo instrumentin kysynnästä ja tarpeellisuudesta.

On myös hyvin perusteltua kohdentaa tukea pk-yrityksille, sillä kokonaisturvallisuus vaatii, että verkoston kaikilla toimijoilla on tietoturvaan liittyvät seikat kunnossa ja pk-yrityksillä on useimmiten vähemmän resursseja ja osaamista liittyen tietoturvaan.

Tuen oikeasuhtaisuutta voidaan perustella sen kohderajauksella ja kaksiportaisella rakenteella. Pienempi, 15 000 euron tukiluokka toimi tehokkaasti matalan kypsyystason pk-yritysten "ensiapuna" ja madalsi kynnystä lähteä kehittämään perustason tietoturvaa. Arvioinnin tulokset osoittavat, että juuri näillä yrityksillä tuki toi suurimmat suhteelliset parannukset, ja että niiden tietoturva nousi jopa Suomen yritysten keskiarvotason yläpuolelle tietoturvatoimenpiteiden käyttöönoton määrässä mitattuna hankkeiden päätyttyä. Tämä vastaa hyvin tuen tavoitetta tukea perässä tulijoita ja vahvistaa kokonaisturvallisuutta toimitusketjujen kautta. Suurempi, 100 000 euron tukiluokka puolestaan mahdollisti strategisemmat ja pitkäjänteisemmät kehitystoimet niille yrityksille, joilla oli jo perustaso kunnossa. Näin rakenne tuki sekä perustason vahvistamista että syvempää kyvykkyyden rakentamista. On kuitenkin jotain viitteitä siitä, että tuki subventoi sellaisia toimijoita, jotka olisivat toteuttaneet hankkeet joka tapauksessa. 16 prosenttia suuremman tukiluokan yrityksistä vastasi kyselyssä, että olisi toteuttanut toimenpiteet samassa mittakaavassa myös ilman tukea. Myös, kun näiden yritysten tietoturvan tasoa verrataan Suomen yritysten

keskiarvoon, huomataan, että useilla mittareilla nämä yritykset olivat edelläkävijöitä.

Tarkoituksenmukaisuuden osalta tuki onnistui kytkeytymään sekä kansallisiin että EU-tason tavoitteisiin. Se täydensi NIS2-direktiivin toimeenpanoa vahvistamalla kyberturvallisuuskyvykkyyksiä niissä yrityksissä, jotka ovat jatkossa velvoitettuja riskienhallinta- ja raportointivaatimuksiin. Samalla se toteutti Huoltovarmuuskeskuksen kyberkypsyyskartoituksen (2022) osoittamaa tarvetta tasoittaa alojen välisiä eroja – erityisesti niillä sektoreilla, joilla resilienssi oli matalampi (vesihuolto, kauppa, teollisuus). Tukimuoto vastasi myös ENISAn NIS360-raportissa (2024) tunnistettuihin EU:n painopisteisiin: pk-yritysten tukemiseen, osaamisen vahvistamiseen ja toimitusketjujen resilienssin parantamiseen.

Tuen suhteellista kokoa arvioitaessa voidaan todeta, että noin 6 miljoonan euron kokonaisrahoitus oli pienessä maassa kohtuullinen kokeilu – mutta se ei ollut riittävä pysyvän muutoksen aikaansaamiseksi. Markkinavaikutukset jäivät rajallisiksi suhteessa 1,3 miljardin euron kansalliseen kyberturvamarkkinaan, mutta vaikutukset yritysten valmiuksiin ja tietoisuuteen olivat selvästi havaittavia. Instrumentti toimi joustavasti ja hallinnollisesti kevyesti, mikä lisäsi sen käytettävyyttä. Haasteita syntyi lähinnä aikataulujen tiukkuudesta ja ohjeistuksen tulkinnasta, mutta nämä liittyivät enemmän toimeenpanoon kuin instrumentin peruslogiikkaan.

Kokemukset muista arvioinneista viittaavat siihen, että avustus on tehokkainta, kun sitä täydennetään ei-rahallisilla keinoilla, kuten teknisellä tuella ja asiantuntijaohjauksella – tämä olisi perusteltu lisä myös kyberturvan kehittämisen yhteydessä, jossa teknologiset ratkaisut ja niiden valinnat ovat keskeisessä asemassa.

Suorat ja lyhyen aikavälin vaikutukset

Tuki on täyttänyt hyvin tarkoituksensa, ja sen suorat vaikutukset tuensaajiin voidaan arvioida selvityksen havaintojen perusteella merkittäviksi. Tietoturvasetelin suorissa vaikutuksissa korostuu käytännönläheinen kehittäminen ja osaamisen vahvistaminen. Toimenpiteet kohdistuivat eniten ohjelmistoihin ja hallinnolliseen tietoturvaan, sekä henkilöstön osaamiseen. Suuremmat hankkeet painottivat myös laite- ja tuotantoteknologian suojausta. Asiakkaiden tietoliikenteeseen ja tietoihin kohdistuvat toimet, toimitusketjujen ja OT-ympäristöjen tietoturva sekä toimitilaturva jäivät kuitenkin vähäisemmälle huomiolle.

Pitkällä aikavälillä suurimmat hyödyt liittyvät resilienssiin ja tehokkuuteen. Osa raportoi myös kohonneesta kilpailuedusta ja asiakasluottamuksesta, mutta tämä oli huomattavasti yleisempää suuremmissa hankkeissa.

Tuen lisäisyys oli pieniä hankkeita ajatellen selvästi kiihdyttävä. 91 % ilmoitti, ettei hanke olisi toteutunut lainkaan tai olisi toteutunut vain osittain ilman tukea. Suurissa hankkeissa vastaava vaikutus oli rajallisempi 16 % toimenpiteistä olisi tehty joka tapauksessa.

Lyhyen ja pitkän aikavälin epäsuorat vaikutukset

Tietoturvan kehittämisen tuella voidaan havaita olleen joitain epäsuoria vaikutuksia markkinoihin, muihin yrityksiin ja koko yhteiskunnan kyberturvallisuuskyvykkyyteen, mutta sen rajallisesta koosta johtuen epäsuorat vaikutukset jäävät suhteellisen pieniksi.

Suomessa kyberturvallisuustoimiala on noin 1,3 miljardin euron kokoinen, ja sen painopiste on siirtynyt ratkaisukehityksestä palvelutuotantoon ja palveluiden integroimiseen ja hallintaan. Tietoturvaseteli on lisännyt tätä kysyntää edelleen, erityisesti auditointi-, koulutus- ja tietojärjestelmäpalveluissa. Hankkeissa palvelu- ja muihin ostoihin käytettiin noin 7,4 miljoonaa euroa, josta noin 2,8 miljoonaa euroa kohdentui konsulttipalveluihin ja noin 2,3 miljoonaa välineiden ja laitteiden ostoihin ja palveluiden lisenssikustannuksiin. Selvitysten analyysin perusteella tuki vivutti yrityksiltä omarahoitusta vähintään noin 3,3 miljoonaa euroa (1,3 miljoonaa suuremmissa ja 2 miljoonaa pienemmissä hankkeissa).

Tuen avulla on hankittu myös lisenssejä monikansallisilta yrityksiltä. Vaikka nämä toki parantavat tietoturvaa, liittyy niihin myös geopoliittisia riskejä. Rahoitustuen kokonaismarkkinavaikutukset ovat kuitenkin rajallisia, sillä sen volyymi – reilu 7 miljoonaa euroa kahdessa vuodessa – on pieni suhteessa markkinoiden kokoon.

Tuen tärkein epäsuora vaikutus liittyy sen yhteiskunnalliseen rooliin. Se on vahvistanut kriittisten alojen toimitusketjujen tietoturvaa ja lisännyt pk-yritysten valmiuksia toimia osana kansallisesti merkittäviä ekosysteemejä. Vaikka kunnalliset toimijat jäivät virallisesti tuen ulkopuolelle, tuki on välillisesti vahvistanut myös niiden toimintaympäristöä, koska monet yksityiset toimijat toimittavat palveluita juuri energia-, vesi- ja terveydenhuollon kaltaisille aloille. Näin ollen tuki on lisännyt koko yhteiskunnan kyberresilienssiä, vahvistanut kriittisten verkostojen turvallisuutta ja tukenut Suomen asemaa luotettavana digitaalisena toimintaympäristönä.

Lisäksi tuki on erityisesti pienempien, enintään 15 000 euron hankkeiden osalta kohdentunut yrityksille, joiden tietoturvakypsyys oli keskimääräistä matalampi – juuri näille toimijoille suunnattu rahoitus on ollut keskeistä koko yhteiskunnan kokonaisturvallisuuden kannalta, sillä se on vahvistanut peruskyvykkyyksiä ja kaventanut eroa edelläkävijöiden ja perässä tulijoiden välillä.

4.2 Suositukset

1. **Tukea tulisi jatkaa osana kansallista kyberturvallisuuspolitiikkaa ja huoltovarmuusjärjestelmää**. Tarve kriittisten alojen yritysten tietoturvan parantamiseen on yhä olemassa ja muutokset toimintaympäristössä korostavat sen tarvetta. Arvioinnin havaintojen perusteella tukea on perusteltua jatkaa toistaiseksi, vaikka syitä jatkuvaan tukeen ei kuitenkaan nähdä. Traficomin tulisi jatkaa tätä työtä ja hakea tarkoitukseen soveltuvaa rahoitusta sekä eurooppalaisista että kansallisista lähteistä.

2. **Tuen kohdentamista ja ehtoja tulisi tarkentaa.** Tuen kohdentaminen ilman laatupisteitä on perusteltua erityisesti pienemmän tuen kohdalla, jotta tuki tavoittaa myös ne yritykset, joilla on eniten kehitettävää tietoturvassa. Suuremman tukimuodon kohdalla olisi kuitenkin perusteltua kohdentaa tukea kilpaillusti. Rahoitusehdoissa tulisi myös varmistaa, että tuella tehdään toimenpiteitä, jotka eivät ilman tukea tapahtuisi. Tuen vaikuttavuutta voitaisiin lisätä esimerkiksi kohdentamalla sitä vuosittaisiin teemahakuihin (esim. OT-ympäristöt tai toimitusketjujen riskin hallinta). Myös omarahoitusosuuden sisällyttäminen ehtoihin on ollut perusteltua. Varsinkin suuremman tuen kohdalla monet hankkeista olisi toteutuneet ilmankin tukea. Näissä tapauksissa tuen ehtojen muuttaminen rajaavammaksi tai omarahoitusosuuden nostaminen voisi olla perusteltua.

3. **Kunnalliset toimijat tulisi ottaa mukaan tuen piiriin**. Tuen vaikuttavuutta voitaisiin todennäköisesti lisätä ottamalla mukaan kunnalliset toimijat. Kunnissa on paljon kriittistä infrastruktuuria, jonka parantunut tietoturva vaikuttaa suuresti kansalliseen kokonaisturvallisuuteen.

4. **Rahoitustuen ohella tulisi tarjota aktiivisesti palveluita sekä verkostoja**. Tuen vaikuttavuutta voitaisiin lisätä tarjoamalla sen ohella eirahallisia palveluita, kuten neuvontaa ja verkostoitumistilaisuuksia. Erityisesti pienemmillä yrityksillä on vielä haasteita esimerkiksi hankintaosaamisessa. Monet yritykset myös hyötyisivät vertaisoppimisesta ja kokemusten vaihtamisesta muiden yritysten kanssa.

5. **Ohjeistusta ja viestintää tulisi selkeyttää**. Osittain johtuen tuen valmisteluun liittyneestä kiireestä, tuen ehtoja koskeva ohjeistus ja viestintä jäi toivottua matalammalle tasolle. Tukimuoto on ollut hallinnollisesti kevyt, mutta ottaen huomioon, että monet yritykset hakevat julkista tukea ensimmäistä kertaa, hakuehtojen, aikarajojen ja tukikelpoisten kustannusten tulkinta aiheutti epäselvyyksiä. Tämä aiheutti hallinnollista taakkaa myös Traficomille.

6. **Vaikutusten seurantaa tulee kehittää**. Kysely osoitti, että yritykset eivät systemaattisesti mittaa tietoturvapoikkeamia eikä niihin

reagointia. Traficomin tulisi kehittää yhtenäinen seuranta- ja mittarikehikko, jonka mukaisesti yritykset raportoivat esimerkiksi tietoturvapoikkeamien määrän, reagointiajan kehityksen, henkilöstön koulutustason, ja auditointitulosten parannukset. Tämä mahdollistaisi vaikuttavuuden vertailun ja tiedon hyödyntämisen seuraavien rahoituskierrosten suunnittelussa.

Lähteet

ECCC (2023). European Cybersecurity Competence Centre – Strategic Agenda for Cybersecurity Research, Innovation and Industrial Policy.

ENISA (2024). NIS360 – Maturity Assessment and Criticality Mapping of EU Sectors. European Union Agency for Cybersecurity.

Huoltovarmuuskeskus (2022). Toimialojen kyberkypsyyden selvitys 2022.

Liikenne- ja viestintävirasto Traficom (2023). Tietoturvan vuosi 2023 – Kyberturvallisuuden tilannekuva ja kehityssuunnat Suomessa.

Liikenne- ja viestintäministeriö (2022). Muistio valtioneuvoston asetuksesta tietoturvan kehittämisen tuesta (860/2022).

Valtioneuvoston asetus tietoturvan kehittämisen tuesta (860/2022). Annettu 13.10.2022.

Valtionavustuslaki (688/2001).

4FRONT (2025). Tietoturvan kehittämisen tuen vaikuttavuusarviointi – kysely ja haastatteluaineisto.

Traficom (2025). Tietoturvasetelin hakemus- ja raportointiaineisto.

Lausuntoaineisto tietoturvan kehittämisen tuesta (VN/18738/2022), lausunnot mm. EK, Suomen Yrittäjät, KKV, OKM, TEM, VM, HVK, Traficom, TIVIA ry, Elisa Oyj, Ammattiliitto Pro, Badrap Oy (2022).

Euroopan komissio (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978-952-311–000–0
ISSN 2669-8781 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto