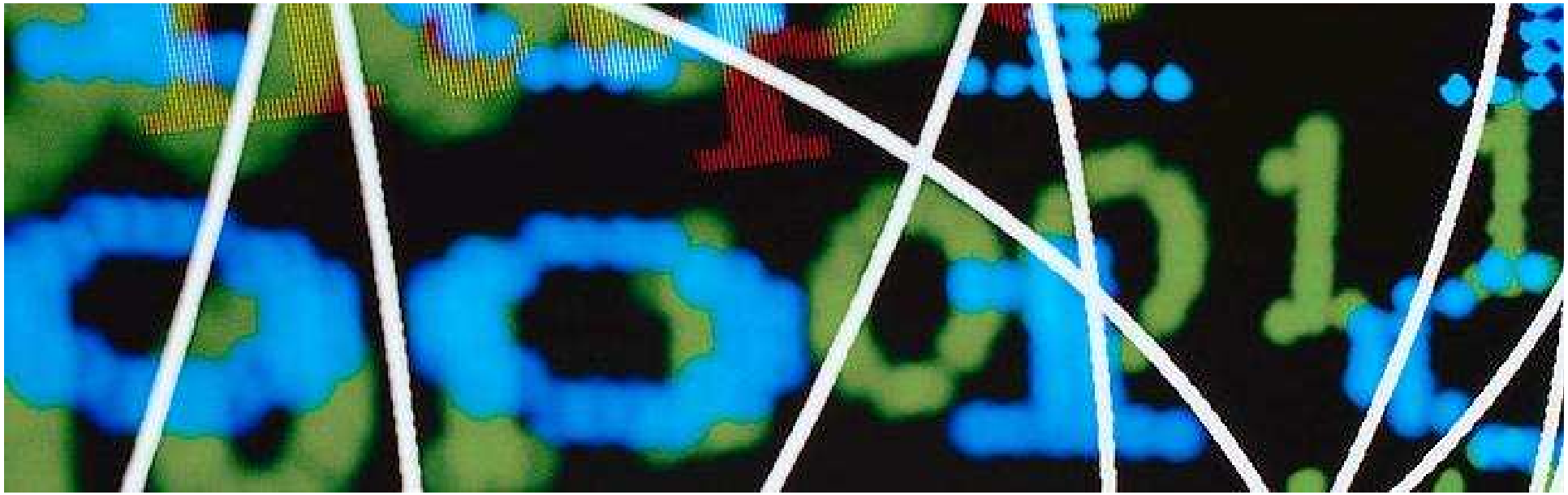


LOPPURAPORTTI [LUONNOS]

TIETOTURVA-ALAN ENNAKOINTISELVITYS

HELMIKUU 2013

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

Sisällys

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

1. SELVITYKSEN TAUSTA, TAVOITTEET JA TOTEUTUS

SELVITYKSEN TAUSTA

- Tietoturva-ala on vielä pieni, mutta se on **nopeassa kasvussa** (arvioitu kasvu noin 20-30%). Kasvun pullonkaulana pidetään **osaavan työvoiman puutetta.**

- Vuonna 2012 perustettiin **tietoturvaklusteri (FISC - Finnish Information Security Cluster)**, jonka tavoitteena mm. alan yhteisresursointi, koulutustarjonnan kehittäminen ja vienninedistäminen. Klusterin koko on tällä hetkellä noin 50 yritystä, jotka työllistävät arvioiden mukaan noin 2000 henkilöä (koko IT-ala noin 50 000).

- Alan kehitykseen liittyy myös vahva **kansallinen näkökulma**, jonka taustalla mm. ICT-alan rakennemuutos ja kyberturvallisuus (katso esim. ICT2015-työryhmän raportti (2013) ja Suomen kyberturvallisuusstrategia (2013).

- Tietoturva-alan osaamiskeskittymiä on Suomessa useampia (esim. Oulun tietoturvaklusteri), mutta **Uusimaa keskeinen alue**; alueella paljon alan yrityksiä ja osaajia.

- Tätä taustaa vasten Uudenmaan ELY-keskus ja Espoon kaupunki tilasivat syksyllä 2012 selvityksen **ennakointiselvityksen tietoturva-alan osaamis- ja palvelutarpeista.** Selvityksen tarkoituksena oli tukea tietoturvaklusterin toimintaa ja samaan aikaan käynnissä ollutta klusterin omaa selvitystyötä.

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

SELVITYSKYSYMYKSET

- Selvityksen tavoitteena oli vastata seuraaviin alan **kasvunäkymiä sekä osaamis- ja palvelutarpeita** koskeviin kysymyksiin:
  - Millaiset ovat **tietoturvaklusterin** yritysten kasvunäkymät ja osaamistarpeet tällä hetkellä ja 2-3 vuoden päästä? Mitkä tekijät mahdollistavat/hidastavat kasvua?
  - Millaiset ovat **tietoturvaintensiivisten alojen* (klusterin yritysten asiakkaiden / loppukäyttäjien)** tietoturvaan liittyvät palvelu- ja osaamistarpeet tällä hetkellä ja 2-3 vuoden päästä?
  - Miten tietoturva-alan **koulutus** vastaa alan tarpeisiin ja miten koulutusta voitaisiin kehittää? (erityisfokus Uudenmaan alueella)
  - Miten tietoturvaklusterin ja sen keskeisten sidosryhmien **yhteistyötä** voisi kehittää jatkossa työvoiman, koulutuksen ja osaamistarpeiden näkökulmasta? (erityisfokus Uudenmaan alueella)

* Tietoturvaintensiivisillä aloilla tarkoitetaan tietoturvatuotteiden ja palveluiden loppukäyttäjiä eli tietoturvaklusterin yritysten potentiaalisia asiakasryhmiä. Tässä selvityksessä mukaan valittiin seuraavat alat: 1) Rahoitus- ja vakuutusala, 2) Logistiikka-ala, 3) Energia-ala, 4) Televiestintä sekä 5) julkinen sektori (puolustusvoimat ja sosiaali- ja terveyspalvelut)

SELVITYKSEN TOTEUTUS

- Ramboll Management Consulting toteutti selvityksen marraskuussa 2012 – helmikuussa 2013. Selvitys oli luonteeltaan pienimuotoinen ja se toteutettiin nopealla aikataululla. Tarkoituksena oli useita tietolähteitä yhdistämällä koota yleiskuva keskeisten toimijoiden näkemyksiä tietoturva-alan osaamis- ja palvelutarpeista sekä laatia sen pohjalta johtopäätöksiä ja ideoita konkreettisiksi kehittämistoimenpiteiksi. **Selvityksen havainnot ja johtopäätökset ovat luonteeltaan suuntaa antavia.**

- **Selvityksen menetelmät ja työvaiheet:**

1. **Dokumenttianalyysi.** Aikaisempien selvitysten, raporttien ja muun kirjallisen materiaalin analyysi selvityksen taustaksi.
2. **Haastattelut** (27 henkilöä). Tietoturvaklusterin yritysten ja keskeisten sidosryhmien (asiakkaat, viranomaiset, oppilaitokset) edustajien haastattelut.
3. **Sähköinen kysely tietoturvaintensiivisille aloille** (n=100)
   - Kysely lähetettiin noin 3000 tietoturvaintensiivisten alojen (TOL 35, 4791, 49, 50, 51, 61, 64, 65, 66) yritysten päättäjille (toimitusjohtaja / tietoturvajohtaja tai –päällikkö).
4. **Sähköinen kysely tietoturvaklusterin yrityksille** (n=15)
   - Lähetetty avoimena linkkinä klusterin jakelulistalle (noin 50 yritystä)
5. **Työpaja** 5.2.2013 (osallistujiana 17 klusterin yritysten, loppukäyttäjäorganisaatioiden, oppilaitosten ja viranomaisten edustajaa)

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

MÄÄRITELMÄT

- Tietoturva-alalle ei ole olemassa yksiselitteistä määritelmää, minkä vuoksi puhe ”tietoturva-alasta” voi olla jopa harhaanjohtavaa. Suppeimmillaan termillä tarkoitetaan tietoturvatuotteita, palveluita ja konsultointia tarjoavat yrityksiä. Toisaalta tietoturva-alaan voidaan laskea mukaan myös esimerkiksi suuret konsultti- ja ICT-yritykset, joilla on sisäisiä tietoturvayksiköitä tai muiden toimialojen yrityksissä tai julkisella sektorilla toimivat tietoturvaosaajat.

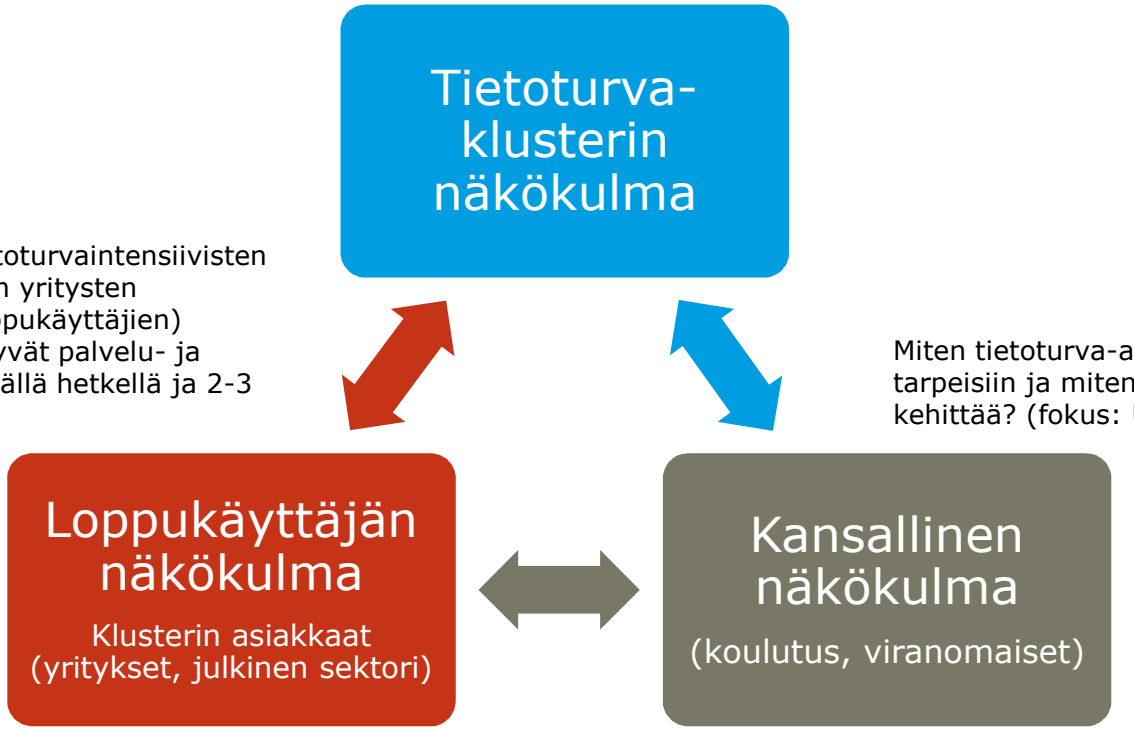
- Tietoturva ja siihen liittyvä osaaminen voidaan lisäksi jakaa hallinnolliseen, tekniseen ja fyysiseen tietoturvaan.

- Tässä selvityksessä **tietoturva-alan yrityksillä** tarkoitetaan tietoturvaklusteriin kuuluvia yrityksiä (n. 50).

- **Tietoturva-alan osaamisesta** puhuttaessa sen sijaan käytetään laajaa tietoturvan määritelmä, joka pitää sisällään sekä hallinnollisen, teknisen että fyysisen tietoturvaan liittyvän osaamisen kaikissa eri organisaatioissa (klusterin yritykset, loppukäyttäjät, julkinen sektori).

SELVITYKSEN VIITEKEHYS

Millaiset ovat **tietoturvaklusterin** yritysten kasvunäkymät ja osaamistarpeet tällä hetkellä ja 2-3 vuoden päästä? Mitkä tekijät mahdollistavat/hidastavat kasvua?



Millaiset ovat tietoturvaintensiivisten alojen* (klusterin yritysten asiakkaiden / loppukäyttäjien) tietoturvaan liittyvät palvelu- ja osaamistarpeet tällä hetkellä ja 2-3 vuoden päästä?

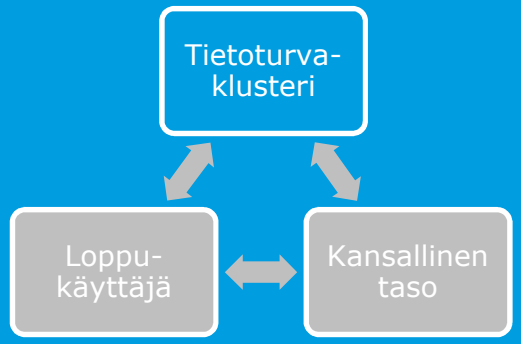
Miten tietoturva-alan **koulutus** vastaa alan tarpeisiin ja miten koulutusta voitaisiin kehittää? (fokus: Uusimaa)

Miten tietoturvaklusterin ja sen keskeisten sidosryhmien **yhteistyötä** voisi kehittää jatkossa työvoiman, koulutuksen ja osaamistarpeiden näkökulmasta? (fokus: Uusimaa)

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto



2. SELVITYKSEN HAVAINNOT

2.1 TIETOTURVAKLUSTERIN NÄKÖKULMA

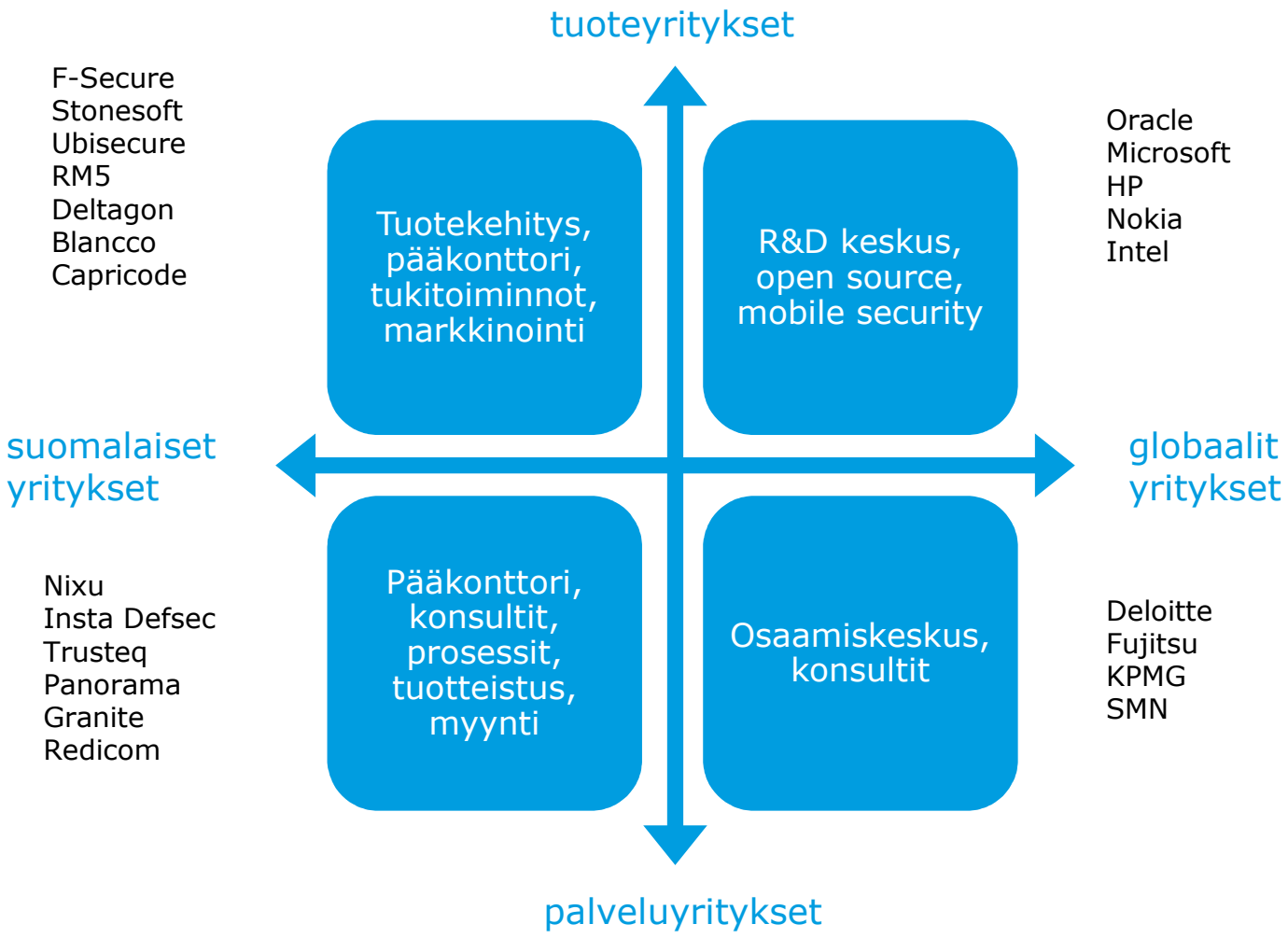
ALAN YLEISET TULEVAISUUDENNÄKYMÄT

- Haastatteluiden perusteella tunnistetut kolme alan kehitykseen vaikuttavaa keskeistä trendiä:
    1. **Regulaatio.** Lainsäädännön, direktiivien, asetusten etc. myötä tulevat mahdolliset muuttuvat vaatimukset loppukäyttäjäorganisaatioille (esim. pankit, julkinen sektori) voivat lisätä merkittävästi tietoturvatuotteiden ja –palveluiden kysyntää.
    2. **Kyberturvallisuuden ”diskurssi”.** Kyberturvallisuusasioiden nostaminen esiin kansallisella tasolla sekä lisääntyvät kyberrikollisuus, tietovuodot jne. lisäävät tietoisuutta tietoturvan merkityksestä ja riskeistä ja siten nostavat tietoturvan prioriteettia organisaatioissa.
    3. **Digitalisoituminen.** Tietojen, palveluiden, kommunikaation jne. siirtyminen enenevässä määrin verkkoon ja sähköiseen muotoon (ml. pilvipalvelut) lisäävät entisestään riippuvuutta sähköisistä tietojärjestelmistä ja siten myös tietoturvasta.
- **Tämän hetken taloudellinen tilanne** vaikuttaa myös olennaisesti kasvunäkymiin ja osaamistarpeisiin: arviot välittömistä osaamistarpeista tällä hetkellä selvästi maltillisemmat (noin 50%) kuin esimerkiksi viime keväänä. Pidemmällä aikavälillä kuitenkin selvää kasvua.
- **Tietoturva-alan** (cyber security) kansainvälinen kasvuvauhti on nopeaa. Markkinoiden nykyiseksi kooksi on arvioitu noin 60 miljardia dollaria ja markkinan koon on arvioitu jopa kaksinkertaistuvan viidessä vuodessa (120 miljardia dollaria vuonna 2017). Eri markkinatutkimuslaitosten ennusteissa on kuitenkin suuria eroja.

KLUSTERIN YRITYSTEN PROFIILI

- Klusterissa **hyvin erilaisia yrityksiä**. Alalle leimallista kapea huippuosaaminen **fragmentoituneena** kymmeniin pk-yrityksiin. Toisaalta myös **isoja kv-toimijoita**.
  - Hieman yli 70% klusterin yrityksistä omistajapohjaltaan suomalaisia, mutta huomattava osuus myös suuria globaaleja yrityksiä (esim. Deloitte, KPMG).
  - Noin 40%:lla yrityksistä on henkilöstöä vain Suomessa, toisaalta noin 20%:lla yrityksistä Suomessa vain alle 10% henkilöstöstä.
  - Yritysten liikevaihto vaihtelee muutamasta sadasta tuhannesta kymmeniin miljooniin euroihin.
  - Noin 70% yrityksistä tietoturva-alan substanssiosaajia on alle 25% henkilöstöstä.
  - Yritykset saavat tietoturva-alan tuotteista keskimäärin noin 17% liikevaihdosta (vaihteluväli 0-75%, mediaani 10%) ja tietoturva-alan palveluista/konsultoinnista noin 24% liikevaihdosta (vaihteluväli 0-95%, mediaani 10%)

ESIMERKKI KLUSTERIN YRITYSTEN LUOKITTELUSTA (KIMMO RASILA, 12.6.2012)



KLUSTERIN YRITYSTEN OSAAMISTARPEET

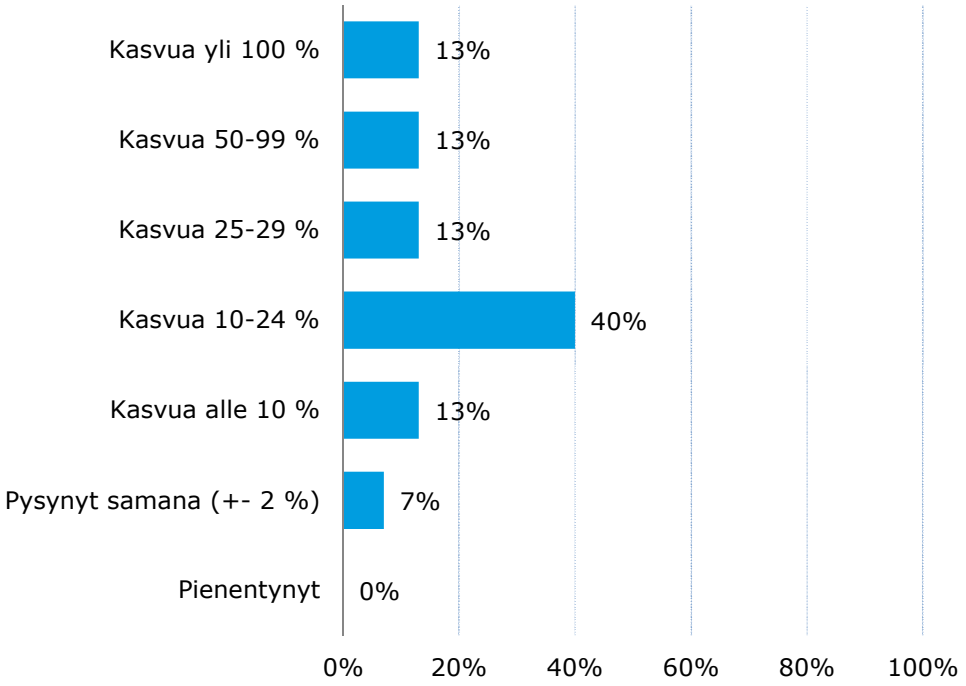
- Pidemmällä aikavälillä (2-3 vuotta) nähdään **selvää kasvua (noin 20%)**

  → myös osaamistarpeen kysyntä kasvaa.

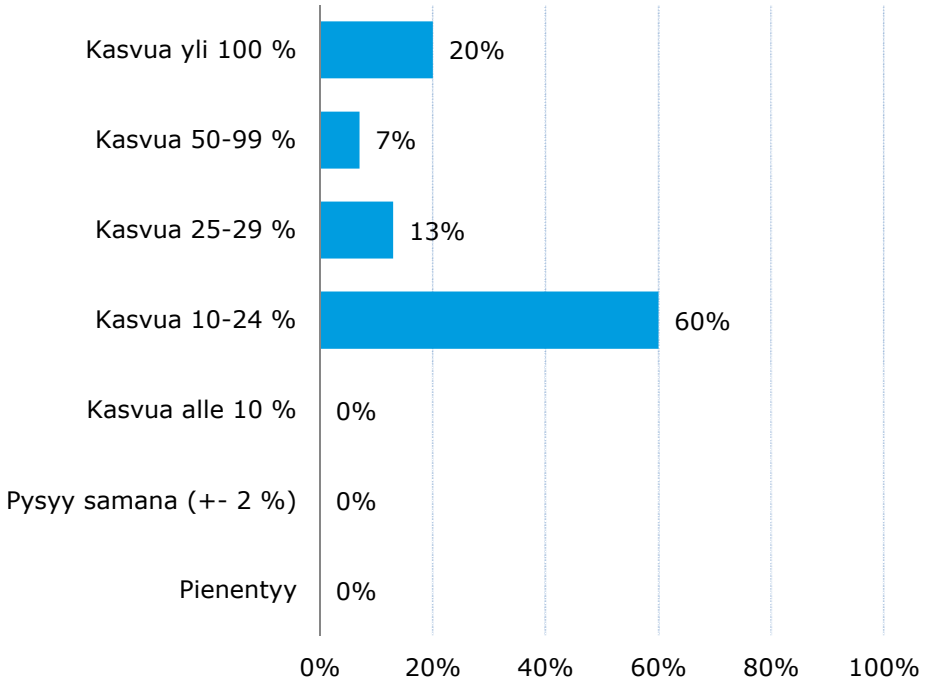
  - Tällä hetkellä **paikoittaista osaamisvajetta**, joka näkyy joissain tapauksissa myös asiakkaille (esim. ei mahdollisuutta osallistua tarjouskilpailuihin, koska pätevä osaaminen jo varattu)
- Kaikkien yritysten osaamistarpeissa (yrityksen kasvun kannalta) painottuu vahvasti **liiketoimintaosaaminen** (ml. asiakasymmärrys-, vienti-, markkinointi-, tuotteistamis- ja projektiosaaminen / ”horisontaalinen osaaminen”)
- Palveluyrityksissä **substanssiosaamisen** tarve korostuu tuoteyrityksiä enemmän liiketoimintaosaamisen ohella kasvun edellytyksenä
- Suomen **korkea palkkataso** merkittävä haaste; monet (tuote)yritykset pyrkivät toteuttamaan työt halvemman työvoiman maissa mahdollisuuksien mukaan
- **ICT-rakennemuutoksen myötä vapautuneet osaajat harvoin vastaavat yritysten tarpeisiin** (korkea palkkataso suhteessa kokemukseen tietoturva-alalta). Nokialta vapautuneet ovat tosin työllistyneet hyvin muualle.
- Globaalien yritysten **merkittävät lisäinvestoinnit (esim. tutkimuskeskukset) Suomeen epätodennäköisiä**, koska markkinat Suomessa pienet ja huippuosaamisen kärki kapea.

KASVU JA KASVUNÄKYMÄT

Liiketoiminnan kasvu kahden edellisen vuoden aikana keskimäärin (n=15)



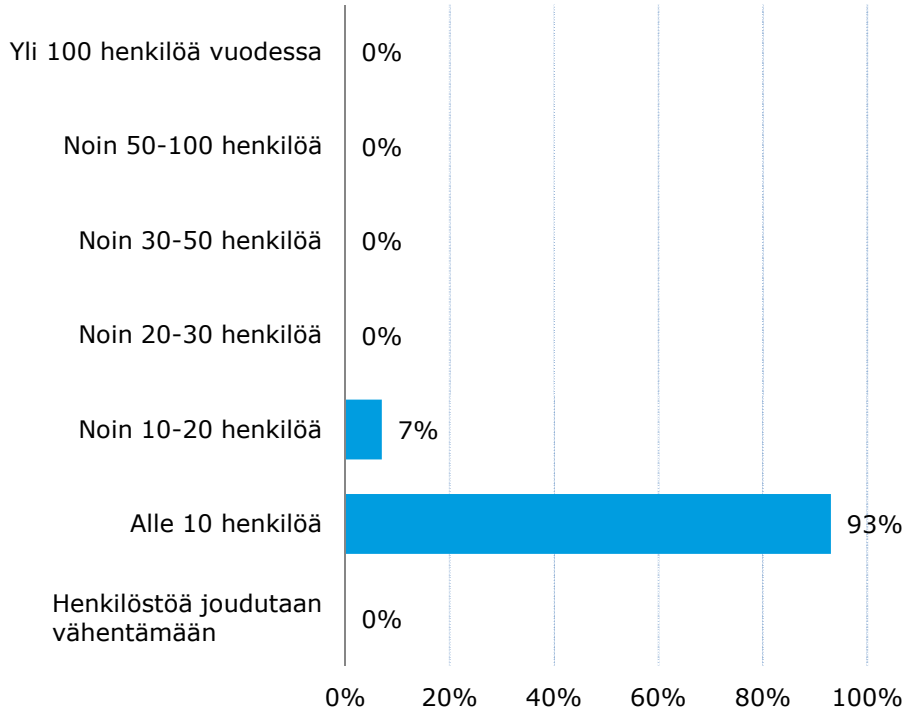
Odotettu liiketoiminnan kasvu 2-3 vuoden aikana (n=15)



Suurin osa yrityksistä kasvanut edellisenä vuonna merkittävästi. Kasvun odotetaan pysyvän vähintään samana tulevina vuosina. Noin 80% arvioi kasvun tapahtuvan vain tai pääosin Suomessa.

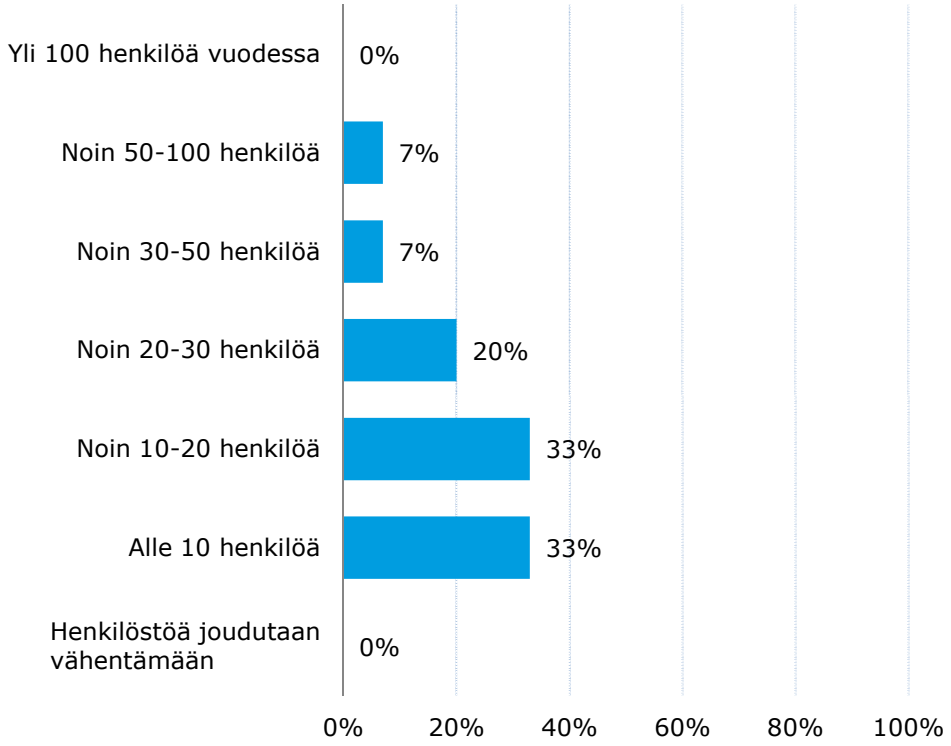
REKRYTOINTITARPEET

Klusterin yritysten tietoturvaosaajien rekrytointitarpeet tällä hetkellä (n=15)



Tällä hetkellä rekrytointitarve klusterin yrityksissä yhteensä noin 50-100 henkilöä.

Klusterin yritysten tietoturvaosaajien rekrytointitarpeet 2-3 vuoden sisällä (n=15)



Vastaajayritykset arvioivat rekrytointitarpeeksi 2-3 vuoden sisällä yhteensä noin 200 henkilöä. Jos tulos laajennetaan koko klusteriin rekrytointitarve olisi noin 550-1000 henkilöä.

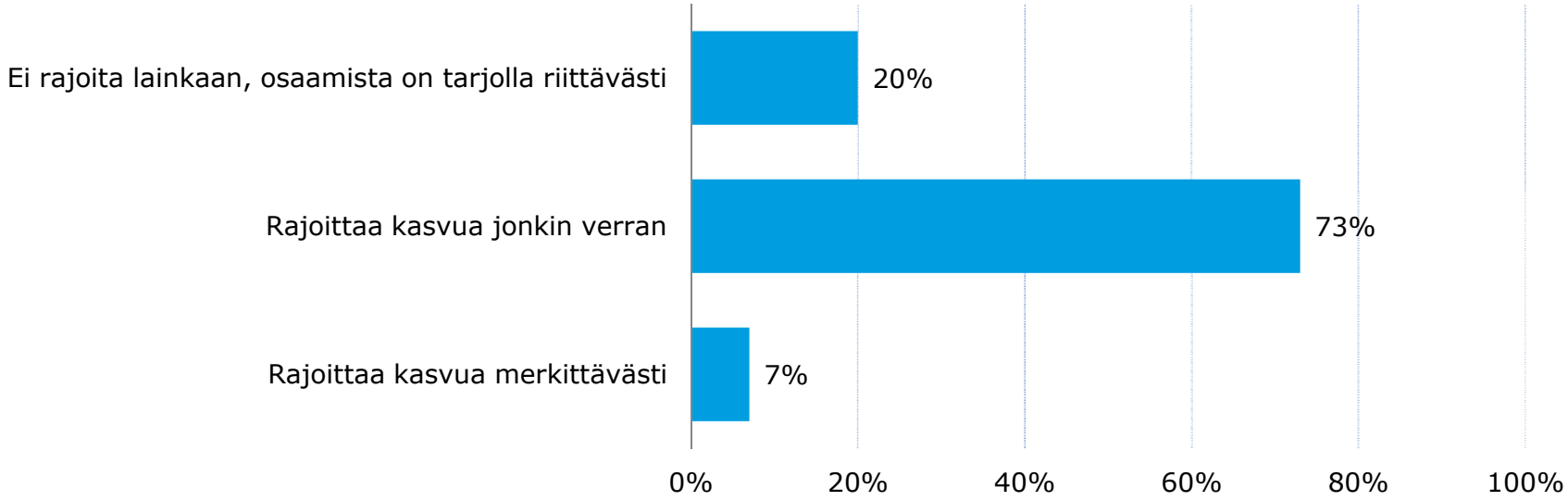
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

TYÖVOIMAN SAATAVUUDEN ASETTAMAT RAJOITTEET

Miten saatavilla olevan, ja yrityksenne tarpeisiin sopivan, osaavan työvoiman saatavuus vaikuttaa yrityksenne kasvunäkymiin? (n=15, klusterin yritykset)



Osaavan työvoiman saatavuus rajoittaa kasvua 80% yrityksiä!

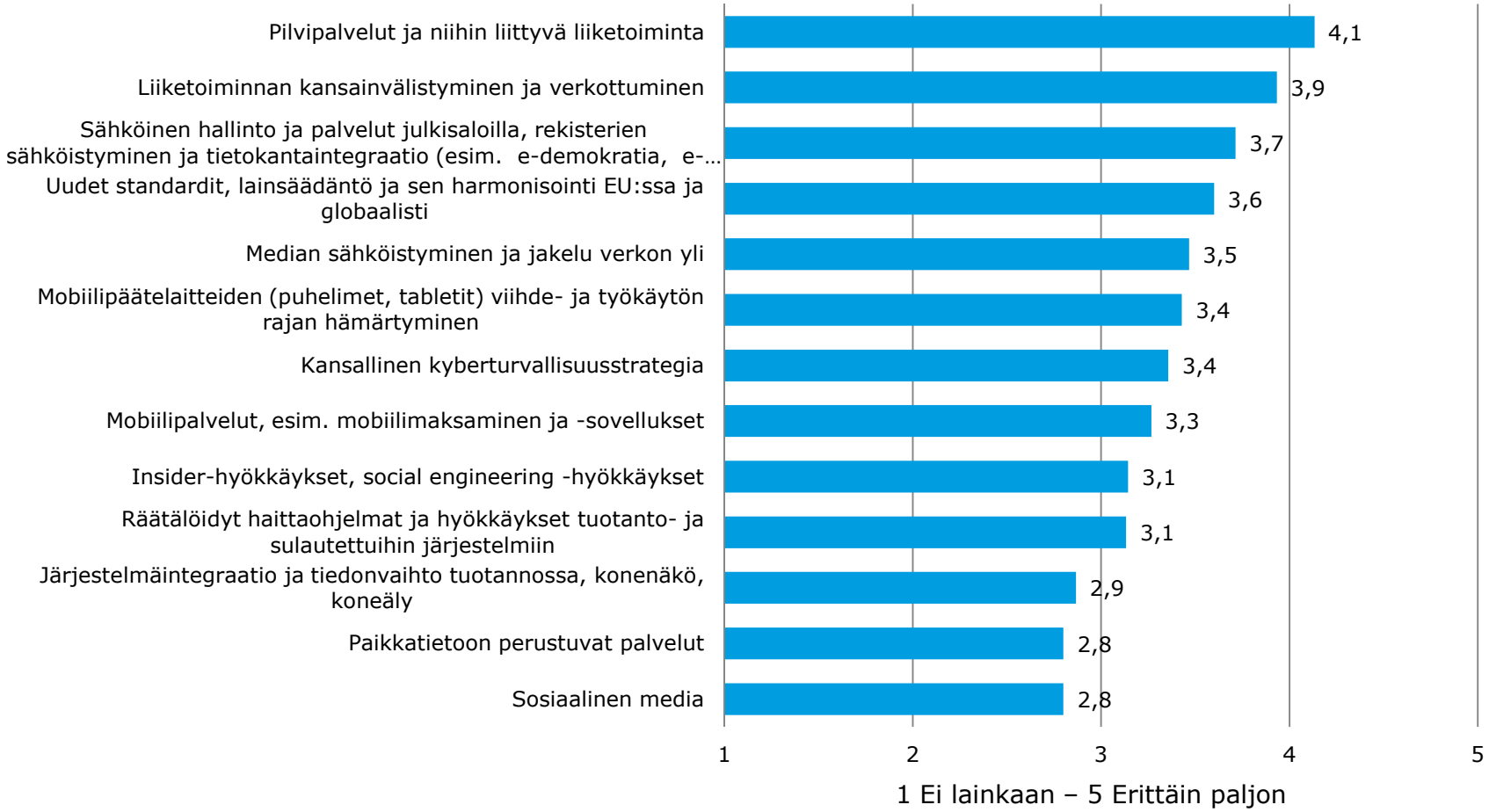
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

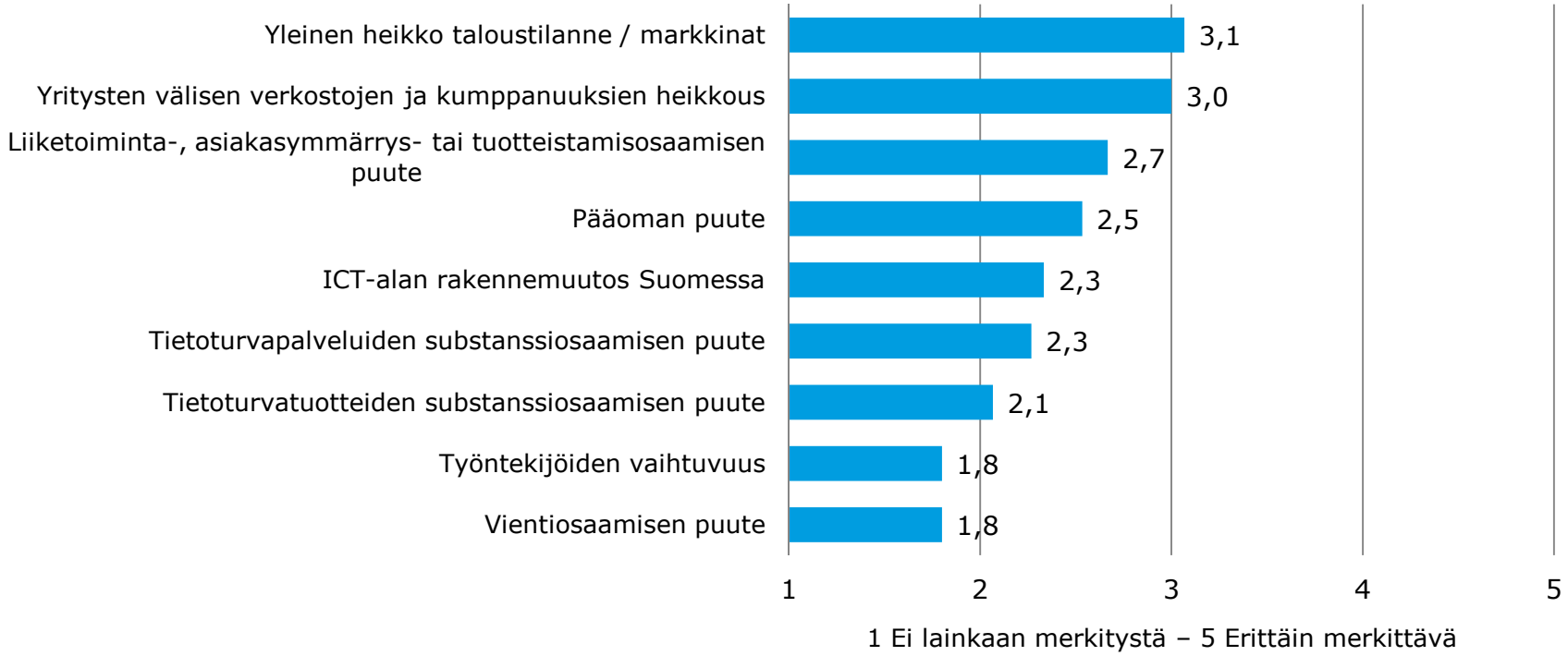
LIIKETOIMINTAMAHDOLLISUUKSIA LUOVAT TRENDIT

Mitkä seuraavista kehityssuunnista luovat suoraan tai välillisesti liiketoimintamahdollisuuksia yrityksellenne seuraavien 2-3 vuoden aikana? (n=15, klusterin yritykset)



KASVUN ESTEET

Miten merkittäviä seuraavat tekijät ovat yrityksenne kasvun esteinä tällä hetkellä? (n=15, klusterin yritykset)



Yleinen taloustilanne, verkostojen puute ja liiketoimintaosaamisen puute rajoittavat kasvua tietoturvan substanssiosaamista enemmän.

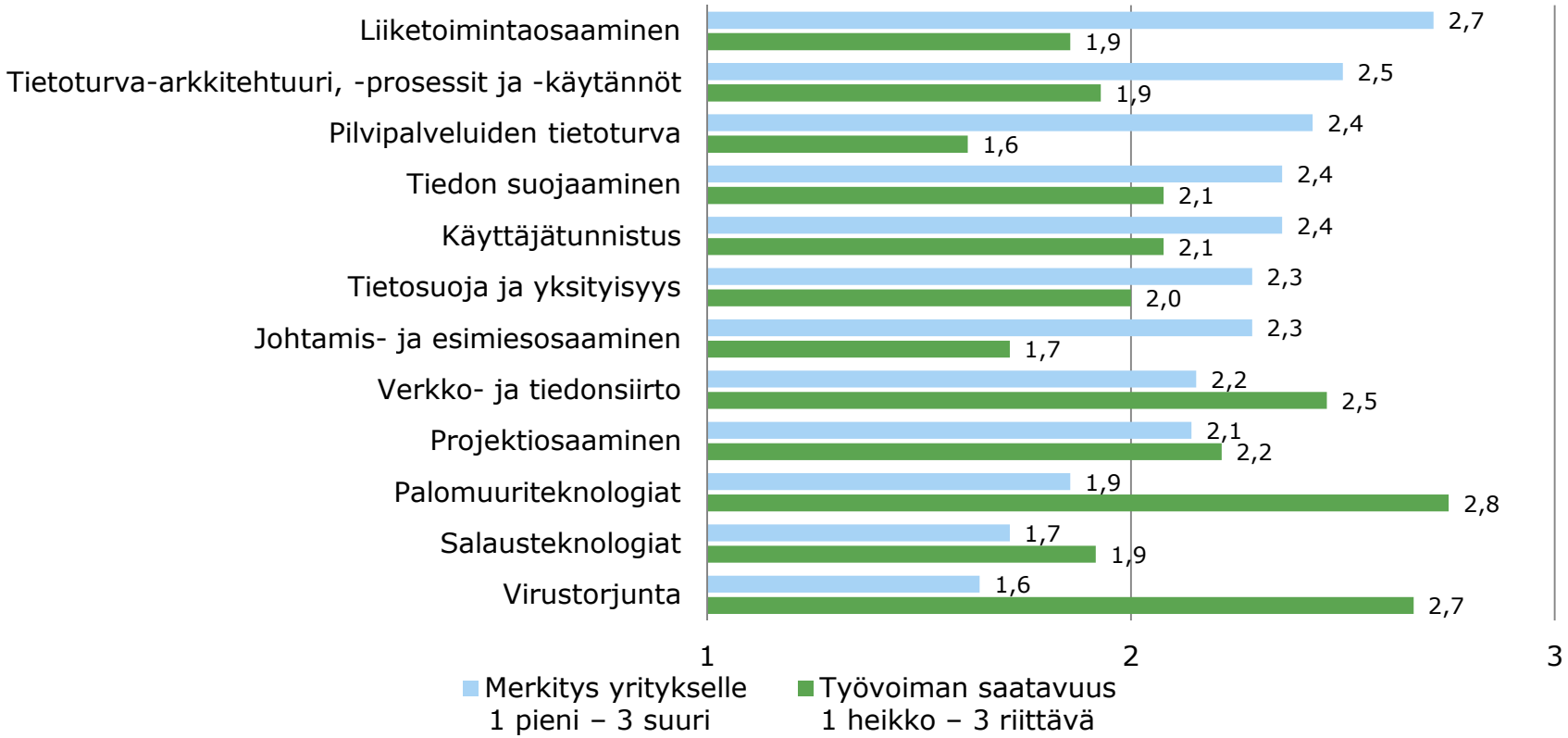
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

TYÖVOIMAN SAATAVUUS JA MERKITYS

Arvioi eri osa-alueiden osaavan työvoiman nykyistä saatavuutta ja ko. osaamisen merkitystä yrityksesi kilpailukyvyn kannalta (n=15, klusterin yritykset)

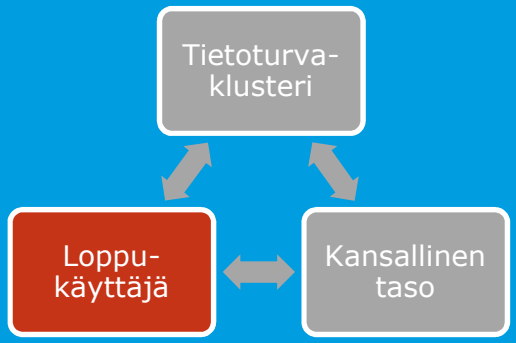


Mm. liiketoimintaosaamiselle ja pilvipalveluihin liittyvälle tietoturvaosaamiselle paljon kysyntää, mutta vähän tarjontaa.

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto



2. SELVITYKSEN HAVAINNOT

2.2 LOPPUKÄYTTÄJIEN NÄKÖKULMA

TIETOTURVA LOPPUKÄYTTÄJÄORGANISAATIOISSA

- Keskeisiä tietoturvan loppukäyttäjiä julkisella sektorilla ovat sosiaali- ja terveyspalvelut sekä turvallisuusviranomaiset ja puolustusvoimat; yksityisellä puolella keskeisiä aloja mm. rahoitus- ja vakuutusala, logistiikka-ala, energia-ala ja televiestintä. Yrityksiä näillä aloilla on Suomessa yhteensä noin 2500.

- Tietoturvapalvelut tuotetaan **ostopalveluna**, jolloin **keskeistä tietoturvajohtaminen ja tilaajaosaaminen** (erityisesti riskien tunnistaminen): Mitkä ovat organisaation tietoturvariskit ja niiden vaikutukset? Mitä tietoja pitäisi suojata? Mitä palveluita/tuotteita siihen tarvitaan?

    - → kun ymmärrys riskeistä lisääntyy, myös tietoturvapalveluiden kysyntä kasvaa. Tehtävä klusterin yrityksille: **miten saadaan johto ymmärtämään riippuvuus tietoturvasta?**

- Yleisesti **resursointi vähäistä** ja tietoturva vain pieni osa loppukäyttäjien IT-palveluita. Tietoturva-asiantuntijat loppukäyttäjäorganisaatioissa usein ”generalisteja”, joilla ei välttämättä syvää tietoturvaosaamista tai alaan liittyvää korkeakoulututkintoa (AMK tai YO)

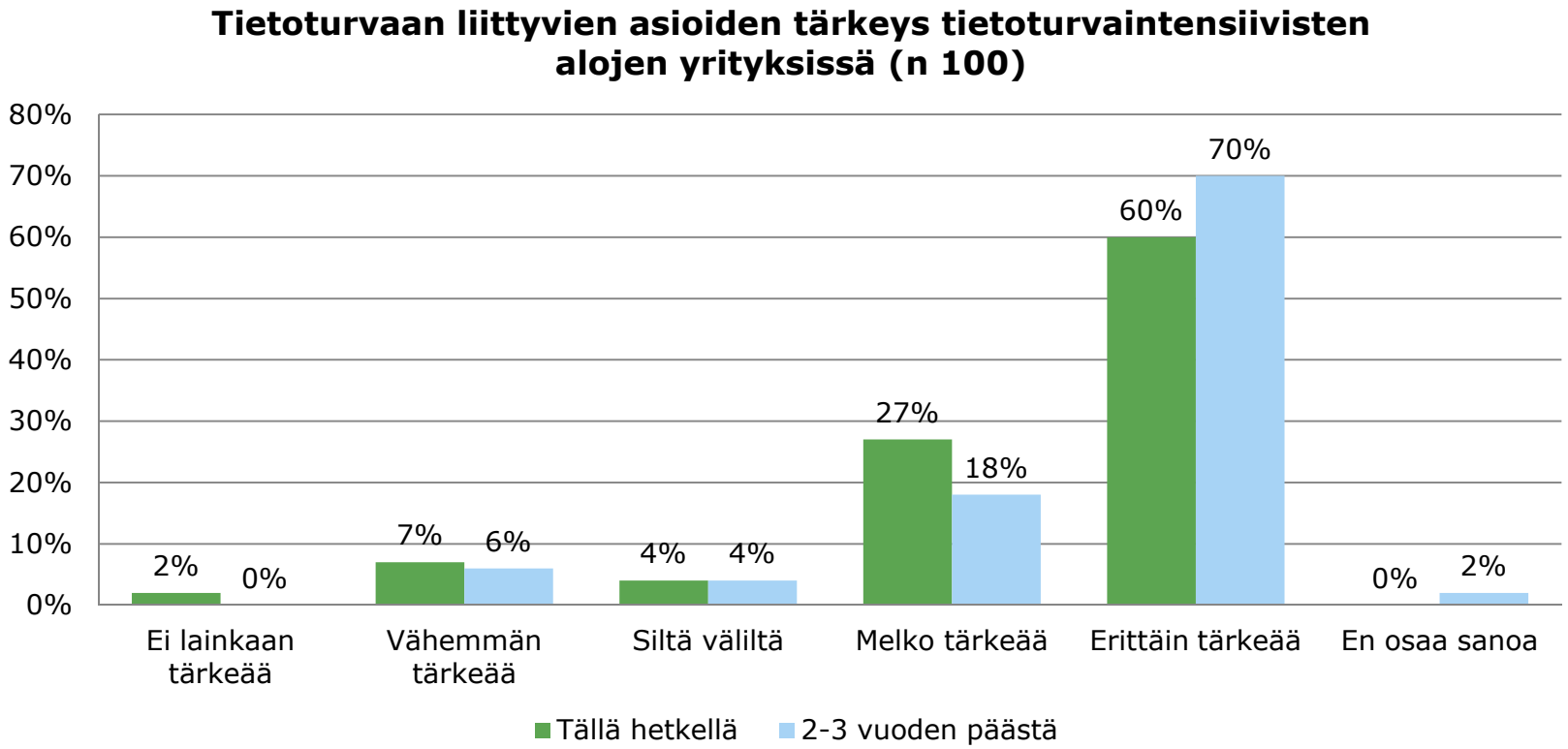
    - Poikkeuksena suuret **huoltovarmuuskriittiset organisaatiot** (esim. pankit), joiden toimintaa säännelty laissa ja joilla myös omaa teknistä tietoturvaosaamista.

    - **Kuntien** tietoturvaosaaminen (erit. hallinnollinen) nähdään varsin puutteellisena ja paikoittaisena. Suurimmissa kunnissa tilanne kohtalainen, mutta varsinkin pienissä kunnissa puutteet merkittäviä.

TULEVAISUUDENNÄKYMÄT JA TARPEET

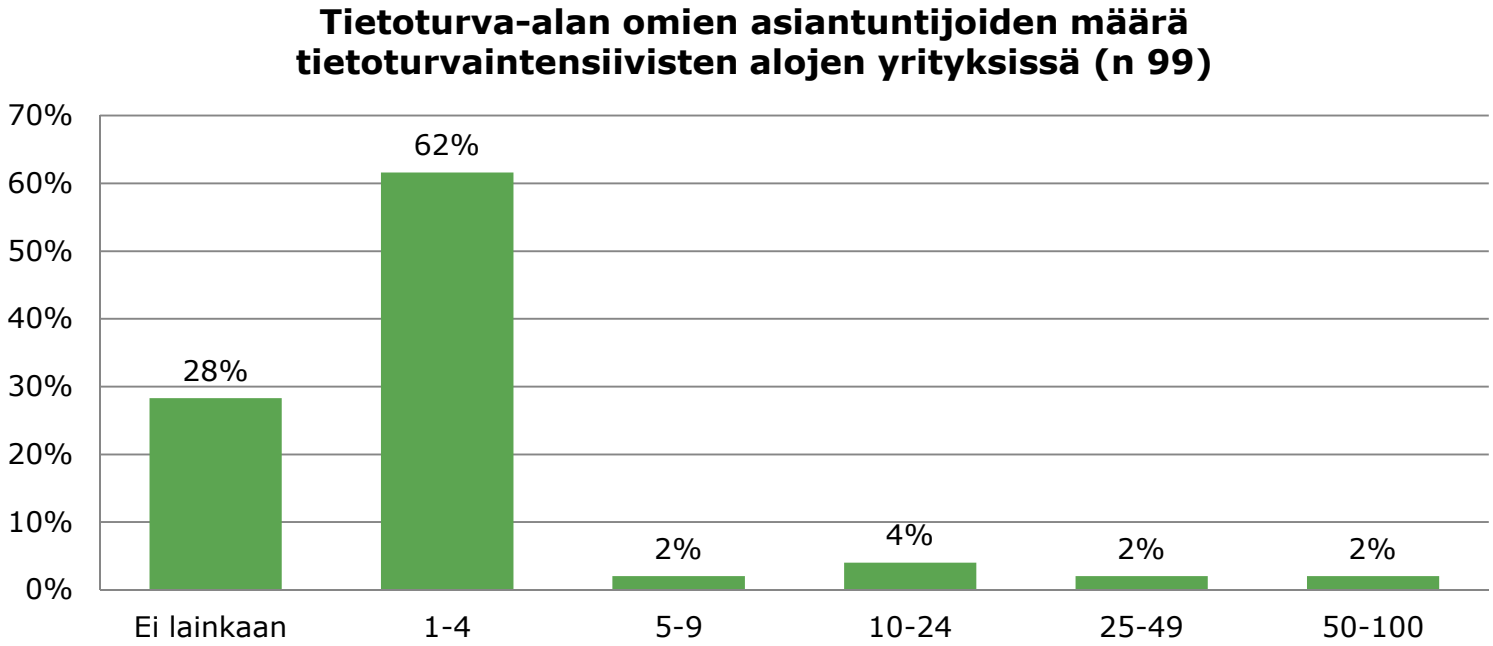
- Tulevaisuuden osaamis- ja palvelutarpeisiin vaikuttaa ensisijaisesti **johdon sitoutuneisuus** tietoturvan edistämiseen ja **tietoturvan prioriteetti** organisaatiossa → vaikutus tietoturvaan kohdennettaviin resursseihin (koskee sekä julkista sektoria että yrityksiä)
    - Prioriteettiin vaikuttaa a) **sääntelyn** asettamat velvoitteet (esim. lainsäädäntö ja EU:n tietosuoja-asetukset) ja b) **tietoisuus** tietoturvaan liittyvistä riskeistä
    - Hyvin **suuret erot yritysten välillä** tietoturvan priorisoinnissa: osalle tietoturva hyvin keskeistä, osa ei näe lainkaan merkittävänä. Haasteellisimpina nähty pienet pilvipalveluita tuottavat ICT-alan yritykset, joiden asiakkaat eivät välttämättä osaa vaatia palveluihin riittävää tietoturvaa.
- Osaamis- ja palvelutarpeet **voivat muuttua verraten nopeastikin,** esim. regulaation myötä tulevien mahdollisten uusien velvoitteiden kautta
- Tietoturvayrityksiltä kaivataan erityisesti **asiakasymmärrystä:** asiakkaan tarpeiden ja vaatimusten (myös heidän tuotteiden/ palveluiden loppukäyttäjien näkökulman) yhdistäminen tekniseen toteutukseen

TIETOTURVAN MERKITYS



Tietoturva nähdään tärkeänä tai erittäin tärkeänä. Tietoturvan merkitys korostuu entisestään lähitulevaisuudessa

TIETOTURVA-ASIANTUNTIJAT ASIAKASYRITYKSISSÄ



Useimmissa (61%) tietoturvaintensiivisten alojen yrityksissä on 1-4 tietoturva-asiantuntijaa. Yhteensä kyselyyn vastanneissa yrityksissä (100) työskentelee noin 280-550 asiantuntijaa. Jos tämä kyselyn suuntaa antava tulos skaalataan koskemaan ko. aloja kokonaisuudessaan (noin 2500 yritystä), on aloilla tämän hyvin karkean arvion mukaan noin 7000 – 14000 tietoturva-asiantuntijaa, joista suurin osa vastaajayritysten profiilista päätellen Suomessa.

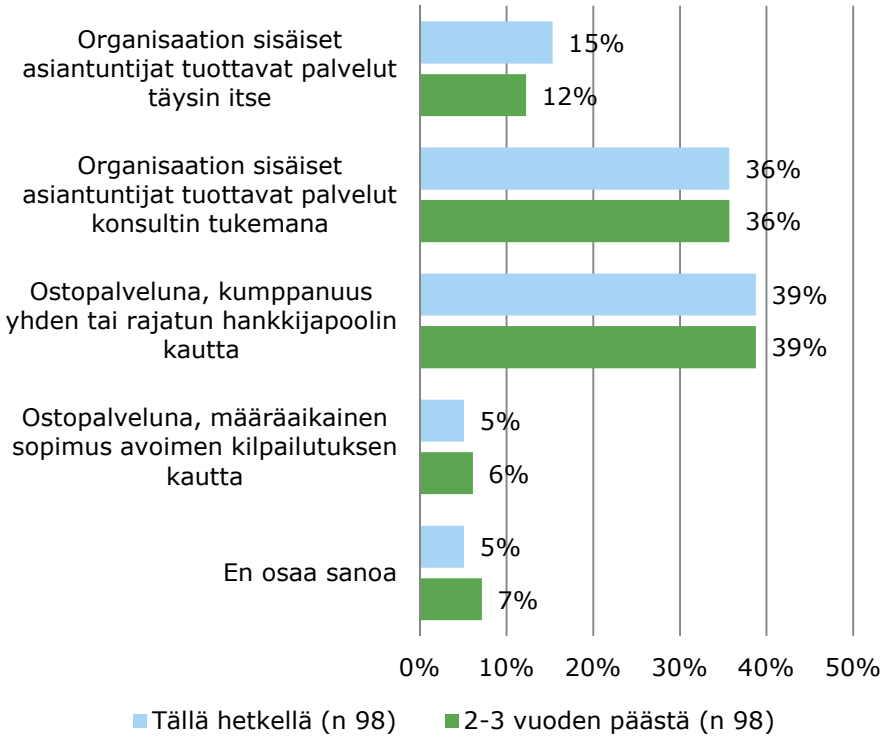
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

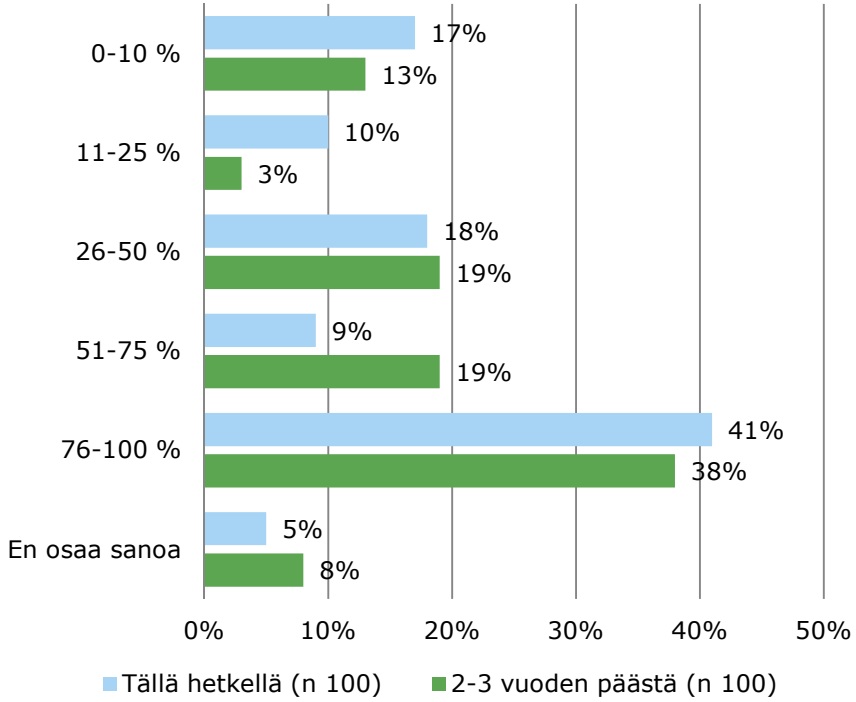
Euroopan unioni
Euroopan sosiaalirahasto

TIETOTURVAN HANKINTA

Tietoturvan hankintatapa tietoturvaintensiivisten alojen yrityksissä



Ostopalveluiden osuus tietoturvaintensiivisten alojen yritysten tietoturvainvestoinneista (%)



Tietoturva tuotetaan suurimmaksi osaksi kokonaan ostopalveluna tai konsultin tukemana. Myös 2-3 vuoden kuluttua.

RAMBØLL

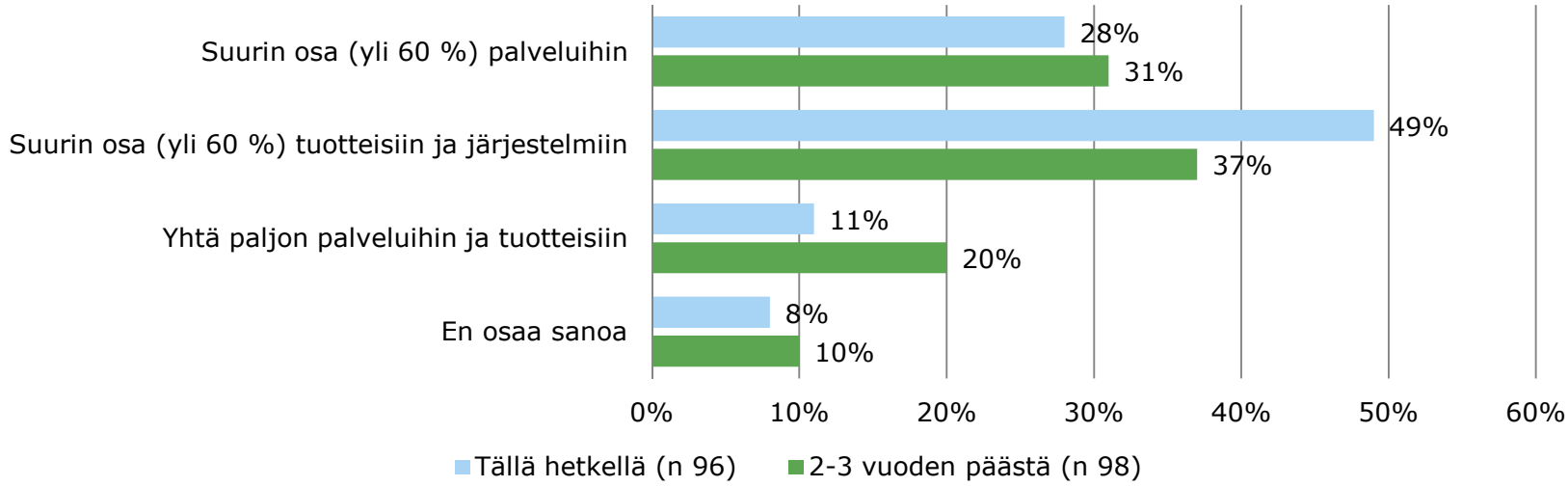
Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

TIETOTURVAINVESTOINNIT

- Vastaajayritysten arvioidut tämän hetken tietoturvainvestoinnit vuositasolla vaihtelevat 0 – 10 000 000 € välillä (mediaani 10 000 €). **2-3 vuoden päästä vuositason tietoturvainvestointien uskotaan olevaan nykyistä suuremmat** (mediaani 17 500 €)

Tietoturvaintensiivisten alojen yritysten tietoturvainvestointien jakautuminen palveluiden ja tuotteiden välillä (%)



Palveluiden osuus investoinneista suhteessa tuotteisiin ja järjestelmiin kasvaa jonkin verran 2-3 vuoden päästä

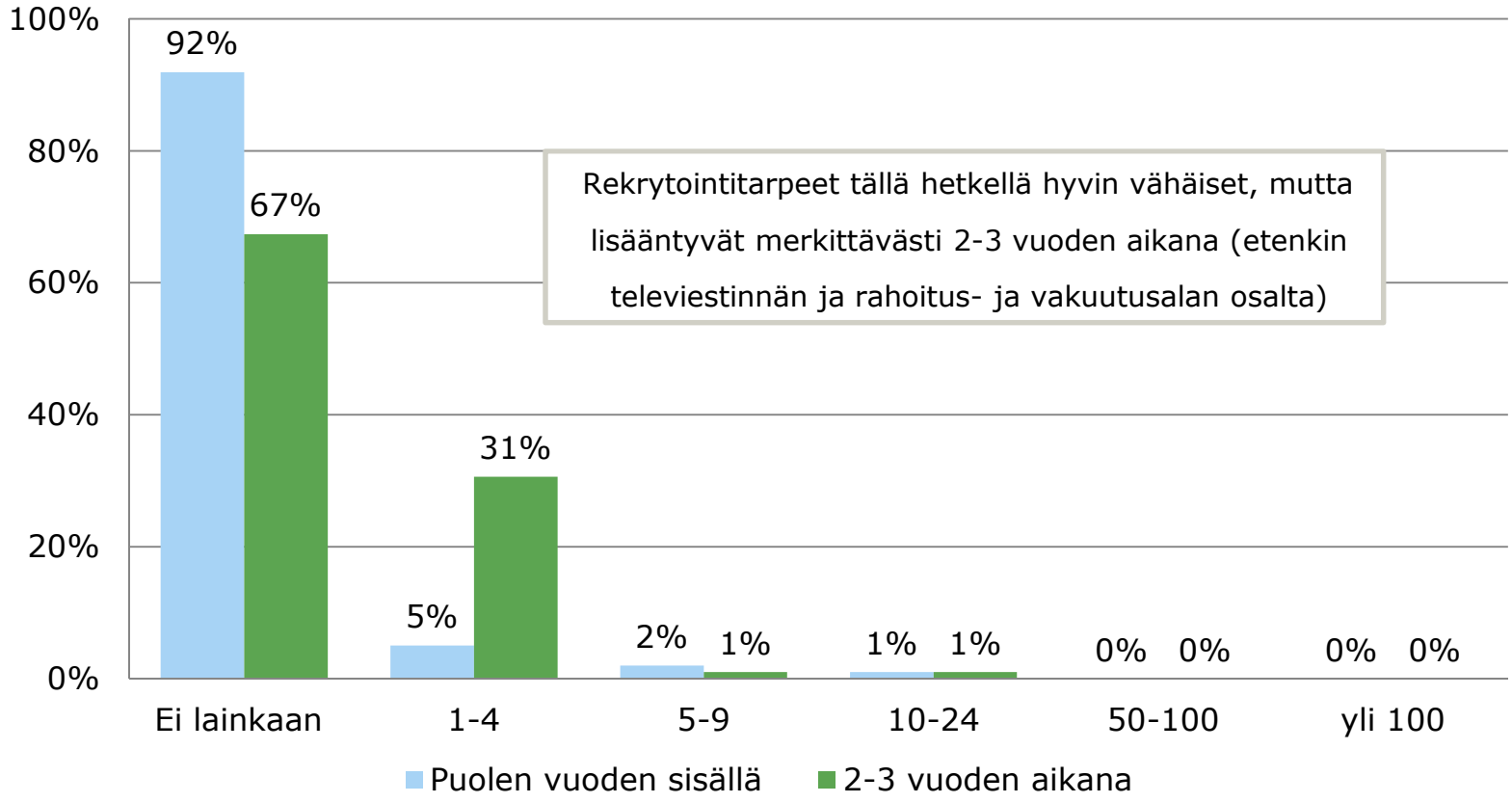
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

REKRYTOINTITARPEET

Rekrytoitavien asiantuntijoiden määrä tietoturvaintensiivisten alojen yrityksissä (n 99)



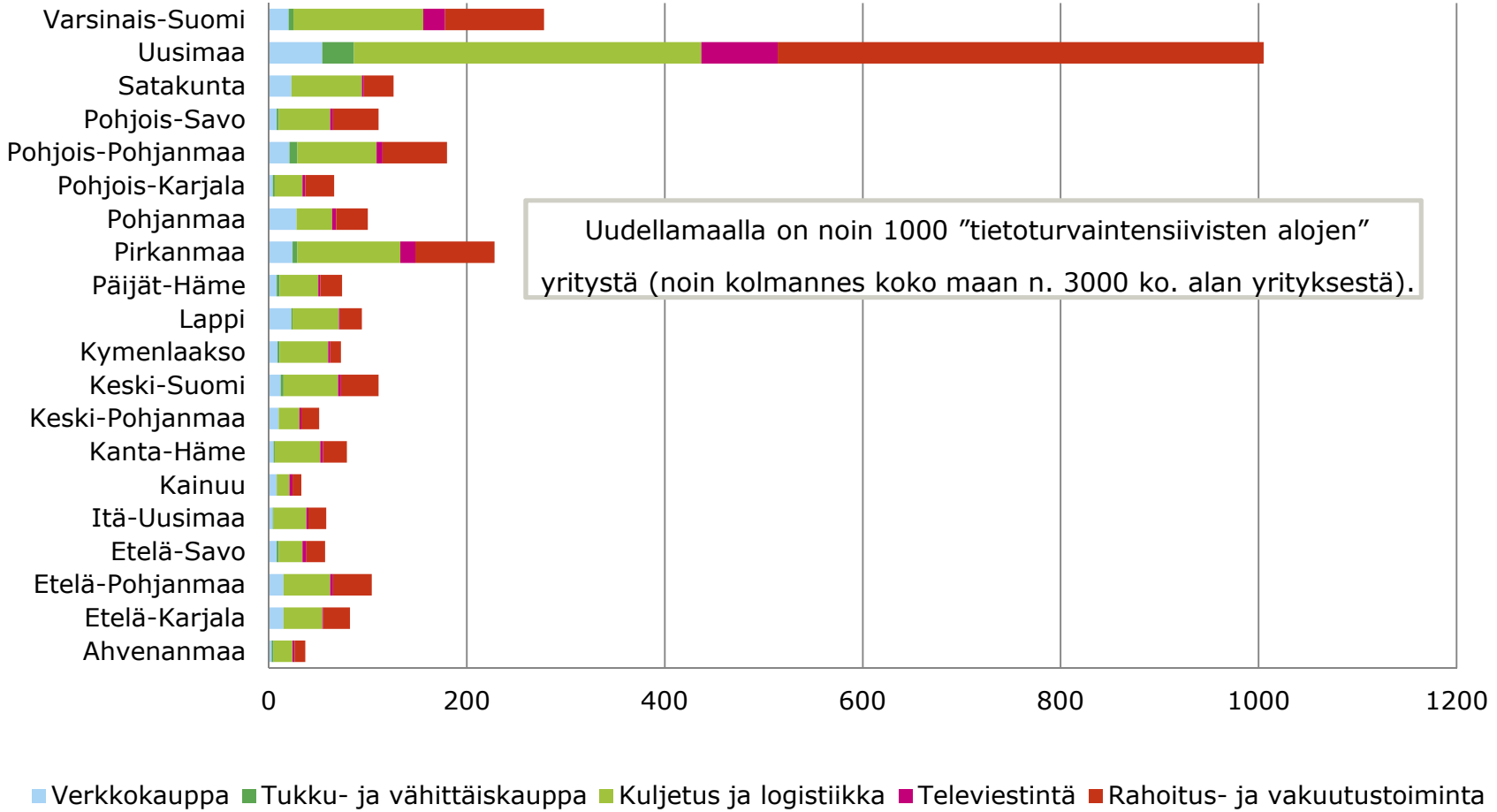
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

UUSIMAA TIETOTURVA-ALAN KESKUKSENA?

Tietoturvaintensiivisten alojen yritysten alueellinen jakautuminen



(Lähde: Fonecta)

UUSIMAA TIETOTURVA-ALAN KESKUKSENA?

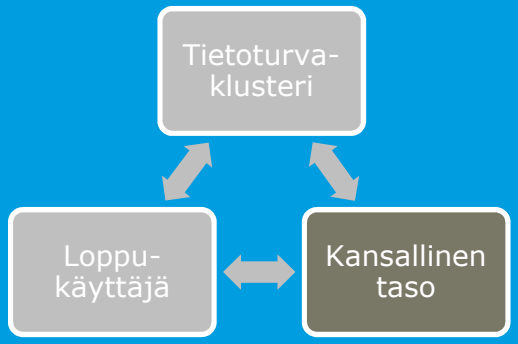
Katso myös: Hallikas, Huvinen, Kontio, Köninki, Mutanen, Nevalainen, Peltonen (2013). Kasvua ja kilpailukykyä ICT:stä – Pääkaupunkiseudusta Suomen innovaatio- ja kasvuyrityskeskittymä. Aalto PRO julkaisusarja 4/2013. http://lib.tkk.fi/CROSSOVER/2013/isbn9789526050140.pdf

- Kansainvälisesti merkittävä osaamiskeskittymä tarvitsee
  - Kriittistä massaa, vetäviä kotimarkkinoita
  - Verkostoitumista ja alustoja
  - Rahoitusta
  - Saavutettavuutta
- Etuina mm.
  - yrittäjien vertaistuki, komplementtipalvelut ja kumppanuusmahdollisuudet, sosiaalistuminen ja yhteistoiminta, helpompi maali sijoittajille
  - Vrt. San Fransisco Bay Area (Piilaakso), CA, USA; Bangalore (International Tech Park), IN; Shanghai (Zhangjiang Hi-Tech Park), CN; Dublin, IR
  - Synteettisen klusterin synnyttäminen on kallista ja hidasta vrt. Skolkovo, RU

UUSIMAA TIETOTURVA-ALAN KESKUKSENA?

Katso myös: Hallikas, Huvinen, Kontio, Köninki, Mutanen, Nevalainen, Peltonen (2013). Kasvua ja kilpailukykyä ICT:stä – Pääkaupunkiseudusta Suomen innovaatio- ja kasvuyrityskeskittymä. Aalto PRO julkaisusarja 4/2013. http://lib.tkk.fi/CROSSOVER/2013/isbn9789526050140.pdf

- Uudellamaalla toimii jo vahva ohjelmistoklusteri
  - Verkosto: Suomen ohjelmistopalveluyrityksien työpaikoista puolet ovat nyt jo Uudellamaalla ja 1/3 yksin pääkaupunkiseudun kunnissa
- Uudenmaan edellytykset muodostua klusteriksi ovat maan parhaat
  - Vahva markkina: Suomen yritysten liikevaihdosta ja kansantuotteesta jopa 40% syntyy Uudellamaalla, koko maan työllisistä uudenmaan osuus on yli 30%. Yksityisen sektorin investoinnista 30% tehdään Uudellamaalla (vrt. asiakasyritysten alueellinen jakauma edellä)
  - Kehitysalustat: Useita, esim. Aalto Entrepreneurship Society, Centre for Entrepreneurship, Spinno, TIVIT Oy ja TIVIT FORGE
  - Rahoitus: Rahoittajien verkosto tiivis ja parhaiten saavutettavissa
  - Saavutettavuus: Suomen ainut merkittävä kansainvälinen lentokenttä on pääkaupunkiseudulla



2. SELVITYKSEN HAVAINNOT

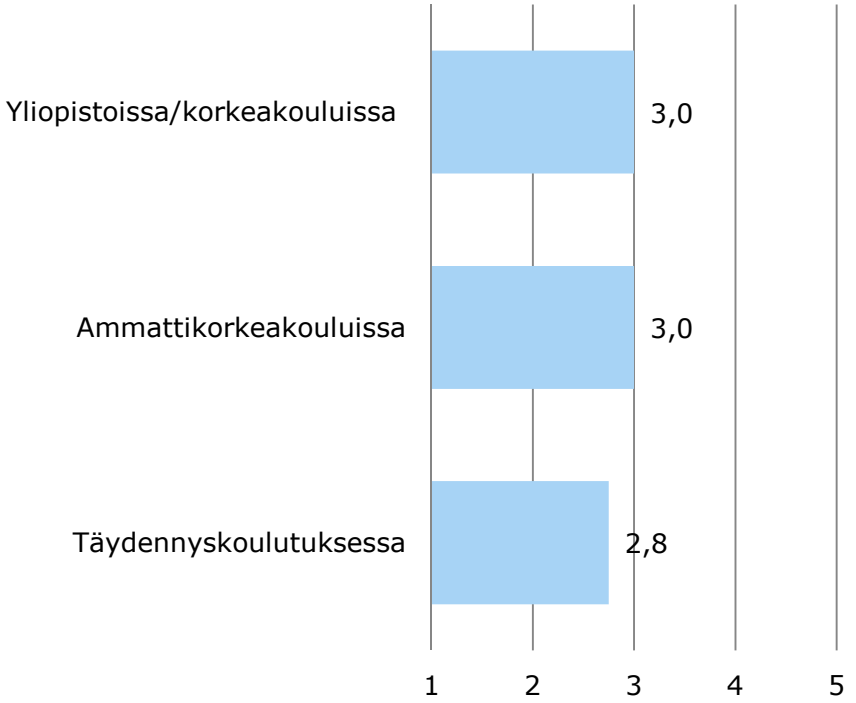
2.3 KANSALLINEN NÄKÖKULMA

TIETOTURVA-ALAN KOULUTUS (FOKUS: UUSIMAA)

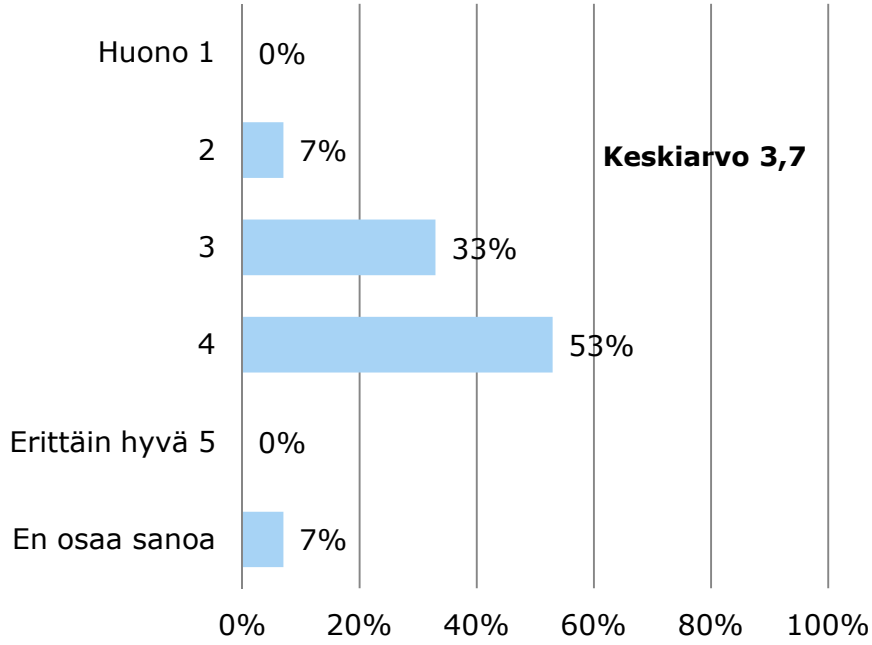
- **Aalto-yliopisto:** tietoturva mukana osana monia eri kursseja / koulutusohjelmia. Osa tietotekniikan kandiopintoja. DI tasolla ei mahdollista erikoistua pelkästään tietoturvaan (vain tietoliikenteen pääaineen kautta).
  - Vuosittain noin 10 opiskelijaa tekee diplomityön tietoturvasta (yhteensä tietoliikenteen pääaineesta valmistuu noin 30 / vuosi). Erikoistuminen tietoturva-alalle diplomitöiden kautta.
  - Kryptologian professuuri loppumassa
- **Laurea:** tietoturvallisuusopintoja osana tietojenkäsittelykoulutusta (noin 30 opiskelijaa otetaan vuosittain). Lisäksi turvallisuuspuolen koulutus kytkeytyy osin tietoturvaan. Koulutus keskittyy hallinnolliseen tietoturvaan (organisaatioiden tietoturva-asiantuntijat), ei tekniseen ”syväosaamiseen”.
  - Erikoistuminen tietoturvaan opinnäytetöiden kautta
  - Tulevaisuudessa tietoturvaa tarkoitus painottaa nykyistä enemmän (tietojenkäsittelytieteisiin tietoturvan suuntautumisvaihtoehto)
- **Aalto Pro (täydennyskoulutus):** tällä hetkellä käynnissä yksi tietoturva-alan täydennyskoulutus. Mahdollisuus järjestää lisää koulutusta nopeallakin aikataululla, jos rahoitus löytyy.

KOULUTUKSEN VASTAAVUUS TARPEISIIN

Miten nykyinen tietoturva-alan koulutus vastaa mielestäsi tietoturva-alan osaamistarpeisiin? (n=15, klusterin yritykset)



Mikä on mielestäsi saatavilla olevan suomalaisen työvoiman tietoturvaosaamisen nykytaso verrattuna kansainväliseen huipputasoon? (n=15, klusterin yritykset)



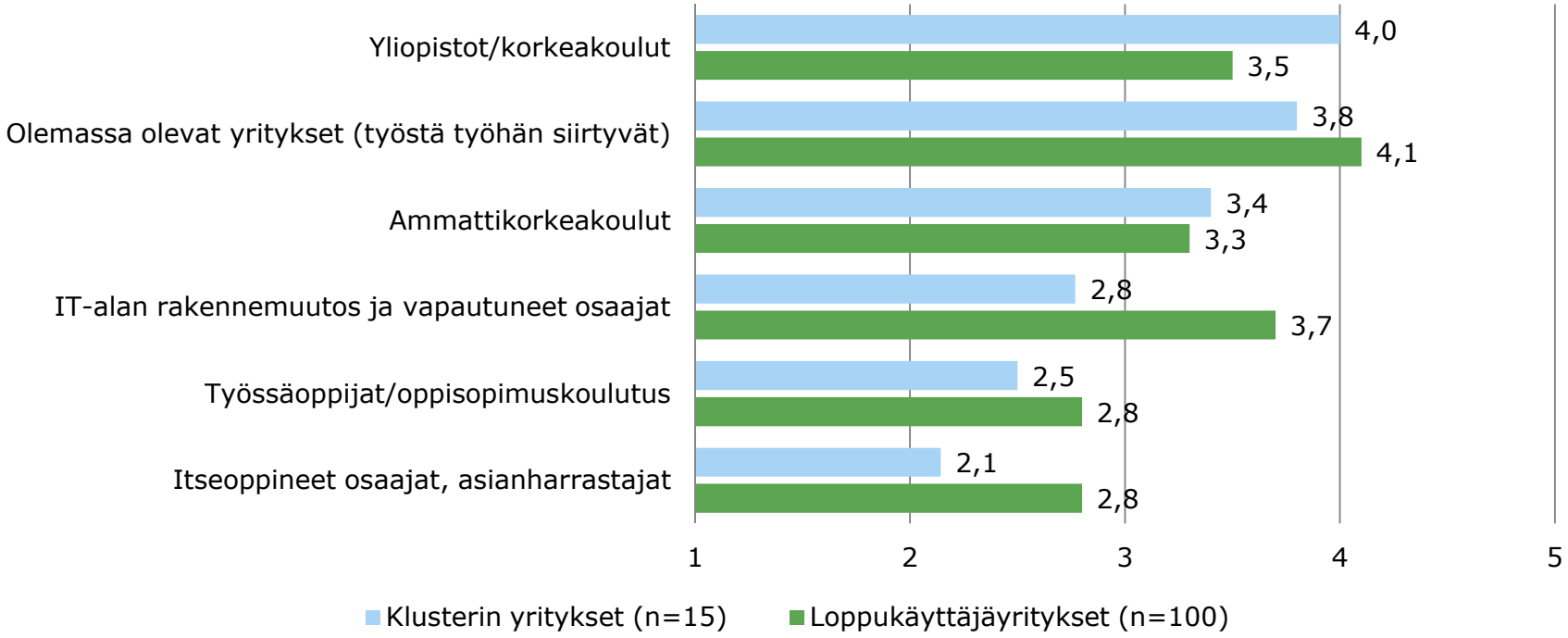
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

REKRYTOINTIKANAVAT

Miten todennäköisesti yrityksen tulevat rekrytoinnit kohdistuvat seuraaviin ryhmiin?



1 Ei lainkaan merkitystä – 5 Erittäin merkittävä

Yliopistot, muut yritykset sekä ammattikorkeakoulut potentiaalisimpia rekrytointikanavia. IT-rakennemuutoksen myötä vapautuneet houkuttelevimpia loppukäyttäjille kuin klusterin yrityksille.

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

NÄKEMYKSET KOULUTUKSEN KEHITTÄMISESTÄ 1/2

- Erityisenä haasteena koulutusjärjestelmän **hajanaisuus** ja selkeän profiloitumisen / ”veturin” puuttuminen
- Yksinomaan tietoturvaan keskittyvän koulutuksen sijaan keskeistä **tietoturvan integroiminen sovellusaloihin** (esim. mobiili-, tietoliikenneverkot ym). Koulutuksessa tärkeää tarjota **valmiudet ja pohja**; yritysten kannalta varsinainen erikoistuminen järkevintä interaktiossa yritysten kanssa
- Myös koulutuksen osalta pidetään tärkeänä **liiketoimintaosaamisen, asiakasymmärryksen ja riskien tunnistamisen ja hallinnan näkökulmaa**
- Täydennyskoulutuksen osalta selvät rakenteet ja yhteistyömallit olemassa (FEC-yritysyhteistyömalli)
- Yrityksissä jo työskentelevien osalta (johto + henkilökunta) tiiviitä koulutusohjelmia pidetään hyvänä ja kysyntä niille kasvanee jatkossa

NÄKEMYKSET KOULUTUKSEN KEHITTÄMISESTÄ 2/2

- Laajasti jaettu näkemys siitä, että Suomen **nostaminen tietoturvan huippumaaksi edellyttää panostusta huipputason tieteelliseen tutkimukseen ja opetukseen**, **erityisesti kryptologiaan**, johon liittyvä matemaattinen osaaminen nähdään tietoturvatutkimuksen perustana sekä keskeisenä myös kansallisen turvallisuuden kannalta.

- **Suurin osa haastatelluista pitää hallinnollisen tietoturvakoulutuksen laatua ja määrää riittävänä tällä hetkellä**. Teknisen huippuosaamisen osalta nähdään aukkoja, erityisesti jos Suomi haluaa jatkossa profiloitua tietoturva-alan huippumaana. Alan kasvun uskotaan lisäävän koulutustarvetta erityisesti hallinnollisen tietoturvan osalta loppukäyttäjäorganisaatioissa.

YRITYSTEN JA OPPILAITOSTEN YHTEISTYÖ

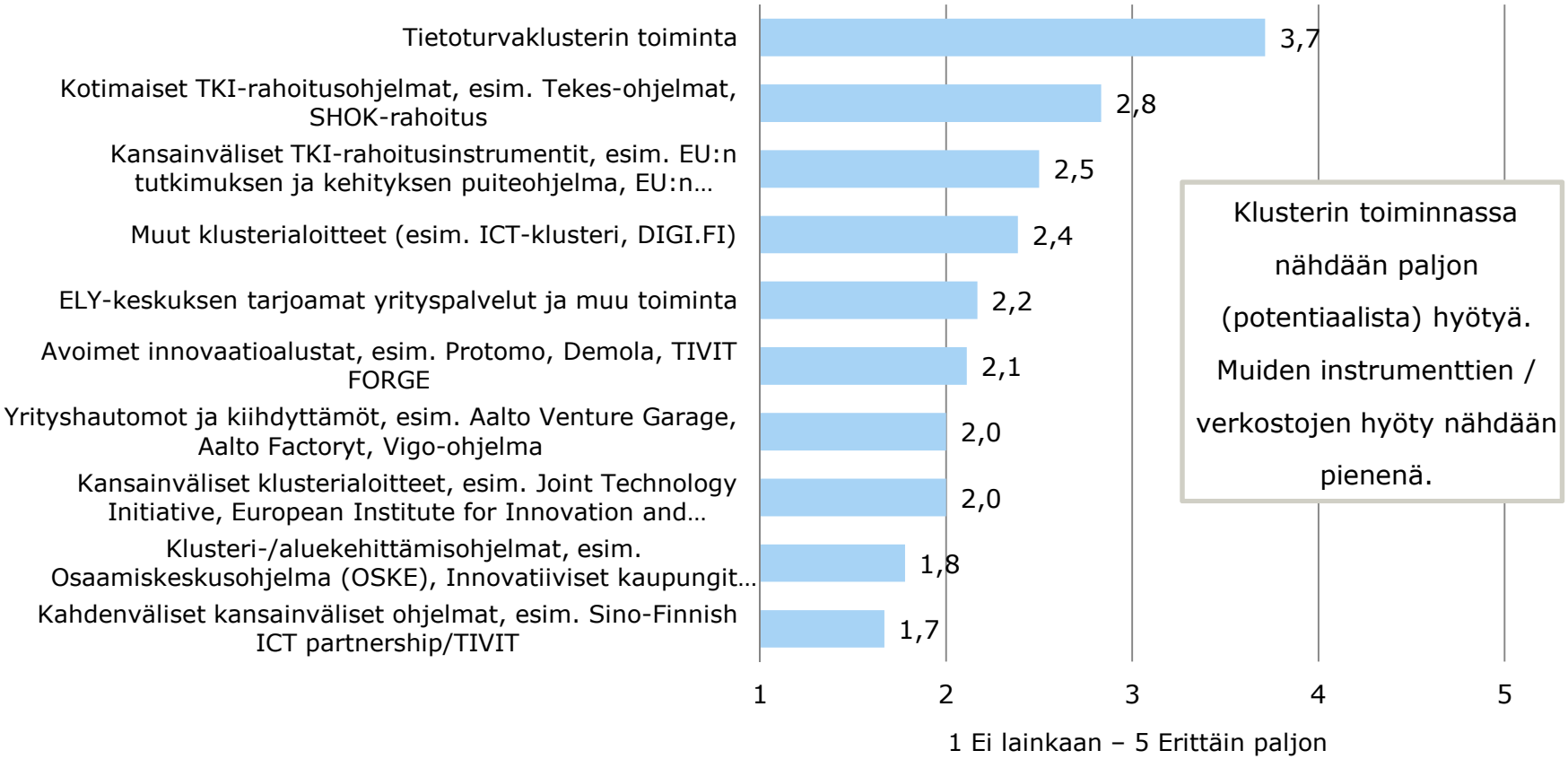
- **Yhteistyötä jo olemassa** (esim. Laurean ja klusterin yritysten auditointikoulutukset, Aalto-yo:n ja F-Securen yhteistyö) ja niistä **kokemukset erittäin myönteisiä**. Haasteena se, että tietoturva-alan yritykset ovat yhä useammin pienempiä kuin aiemmin eikä pienillä yrityksillä ole resursseja yhteistyöhön oppilaitosten kanssa.
- **Sekä klusterin yrityksissä että oppilaitoksissa tarvetta ja kiinnostusta yhteistyömallien kehittämiselle / yhteistyön tiivistämiselle**
    - Win-win-win: yritykset voivat hyödyntää opiskelijoiden osaamista ja käyttää yhteistyötä rekrytointikanavana / perehdytyksenä; opiskelijat saavat työkokemusta; oppilaitokset voivat kehittää opetustarjontaansa
- Konkreettisia ehdotuksia haastatteluista:
    - Harjoitteluohjelmien / projektiyhteistyön kehittäminen; ”crowdsourcing”
    - Yritysten osallistuminen sisältöjen suunnitteluun ja kurssien toteutukseen
    - Kesätyöpaikat suomalaisille opiskelijoille; klusterin yhteinen kesätyöpaikkailmoitus
    - Stipendien rahoittaminen kv-huippuosaajien saamiseksi Suomeen. Jos stipendin lisäksi tarjottaisiin esim. kesätyöpaikka ja diplomityön rahoitus niin todennäköisyys Suomeen jäämiseksi kasvaisi.

VIRANOMAISNÄKÖKULMA

- Yhteistyötä yritysten ja viranomaisten välillä pidetään riittävänä ja toimivana (Huoltovarmuuskeskus, Cert-FI). Ei noussut esiin tarvetta uusille yhteistyömalleille viranomaisten ja yritysten välillä
- Lainsäädäntöä tietoturvaan/tietosuojaan liittyen paljon olemassa, mutta suuri ero lainsäädännön vaatimusten ja tietoturvan käytännön toteutuksen välillä: **ymmärrys lainsäädännön vaatimusten merkityksestä käytännön toteutukselle puutteellista**

KLUSTERIN YRITYSTEN KOKEMA HYÖTY ERI INSTRUMENTEISTA/VERKOSTOISTA

Arvioi seuraavien rakenteiden ja palveluiden tuomaa lisäarvoa edustamasi yrityksen kannalta (n=15, klusterin yritykset)



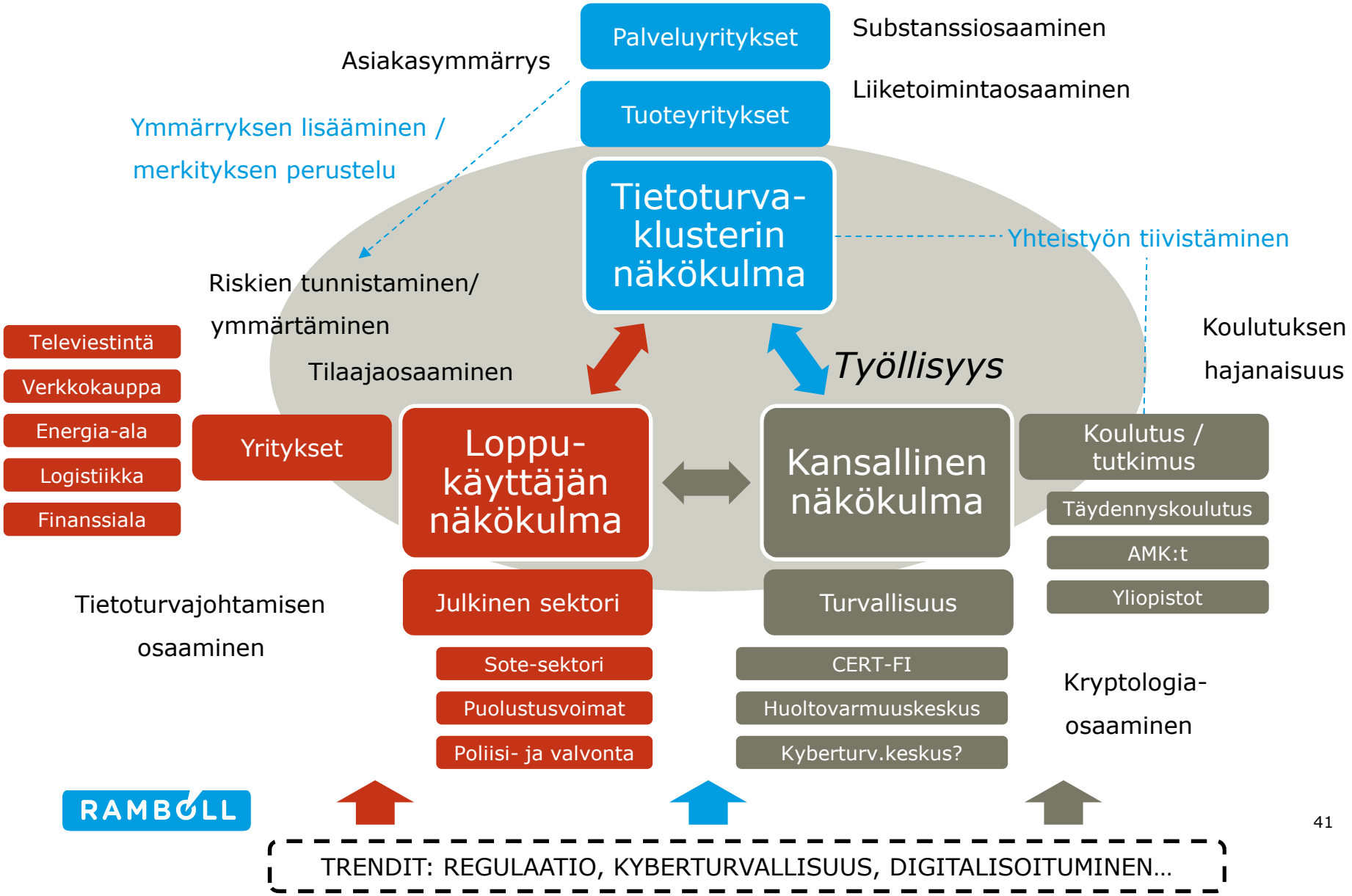
RAMBØLL

Vipuvoimaa EU:lta 2007–2013

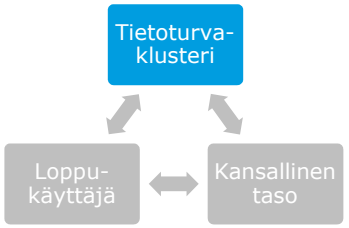
Euroopan unioni
Euroopan sosiaalirahasto

3. JOHTOPÄÄTÖKSET

YHTEENVETO: NÄKÖKULMAT TIETOTURVA-ALAAN



JOHTOPÄÄTÖKSET KLUSTERIN NÄKÖKULMA



- Yleinen huono taloustilanne heijastuu alan näkymiin ja rekrytointitarpeeseen. **2-3 vuoden perspektiivillä odotetaan kuitenkin selvää kasvua** (kesimäärin noin 20 % tai enemmän). Yleisen toimintaympäristön kehityksen (regulaatio, kyberturvallisuuden ”diskurssi”, digitalisoituminen) nähdään tukevan kasvua laajasti eri toimijoiden keskuudessa.
    - Karkea arvio klusterin rekrytointitarpeesta 2-3 vuoden perspektiivillä on noin 550-1000 henkilöä (mahd. uudet yritykset eivät mukana)
- Noin 80%:ssa klusterin yrityksistä **pula osaavasta työvoimasta rajoittaa kasvua** ainakin jonkin verran. Tuoteyrityksissä kasvun pullonkaulana korostuu asiakasymmärrys- ja liiketoimintaosaaminen, palveluyrityksissä lisäksi tietoturva-alan substanssiasiantuntemus.
- Suomen **vahvuuksina nähdään hyvä maine, vakaus, vahva peruskoulutuksen taso, yhteistyö eri toimijoiden kesken sekä vahva ja monipuolinen yrityspohja**.
- Merkittävimpänä **pullonkaulana kasvulle nähdään ”huippuasiantuntijakärjen” kapeus** ja **korkea palkkataso** (tuoteyrityksissä) yhdistettynä alan kansainväliseen luonteeseen.

JOHTOPÄÄTÖKSET LOPPUKÄYTTÄJIEN NÄKÖKULMA

- Klusterin yritysten asiakkaiden keskuudessa tietoturvaan liittyvä **tietoisuus, ymmärrys ja johdon sitoutuminen hyvin paikoittaista**
    - Kuitenkin myös asiakkaiden keskuudessa tietoturvan **merkitys tunnistetaan ja sen nähdään kasvavan** lähitulevaisuudessa (88 % vastaajista pitää tietoturvaa melko tärkeänä tai erittäin tärkeänä 2-3 vuoden päästä)
- **Regulaatio avainasemassa** (erityisesti julkisella sektorilla): keskeinen johdon sitoutumisen ja resurssien kohdentamisen kannalta
- **Suurin osa tietoturvaosaajista hallinnollisella puolella**. Lähitulevaisuudessa jonkin verran rekrytointitarvetta erityisesti hallinnolliselle osaamiselle.
    - Suurin osa palveluista ostetaan ulkoa. Erityisenä haasteena **tilaajaosaaminen**
- Klusterin yrityksiltä toivotaan erityisesti vahvempaa **asiakasymmärrystä**, teknisen toteutuksen sitomista muihin prosesseihin ja konsultointiapua organisaation **tietoturvariskien tunnistamiseen**

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

JOHTOPÄÄTÖKSET
KANSALLINEN NÄKÖKULMA

- Tietoturva-alan **koulutuksen osalta keskeinen haaste hajanaisuus ja selkeän profiilin puuttuminen**. Huippututkimuksen osalta **kryptologian osaamisen turvaaminen** nähdään kriittisenä.
- Klusterin ja oppilaitosten välillä **vahva motivaatio ja tilaus yhteistyön tiivistämiselle**
- **Uudenmaan alueella mahdollisuus profiloitua tietoturva-alan koulutuksen keskuksena** (tietoturva- ja loppukäyttäjäyritysten sekä osaajien suuri määrä)
- **Suomen haasteena kärjen kapeus ja pienet markkinat** (+ korkea palkkataso). Suomen mahdollisuus profiloitua tietoturvaosaamisen keskuksena edellyttää vahvaa **verkostoitumista** kansainvälisten huippuosaajien kanssa. Roolina kansainvälisten verkostojen fasilitointi ja siten huippuosaamisen kartoittaminen ja profiloituminen?
- Yritysten ja viranomaisten välinen yhteistyö riittävää ja toimivaa.

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

4. EHDOTUKSIA TIETOTURVA-ALAN KASVUN TUKEMISEKSI

Seuraavassa on esitetty jatkokeskustelujen pohjaksi selvityksen tekijöiden ehdotuksia tietoturva-alan kasvun tukemiseksi ja eri toimijoiden yhteistyön kehittämiseksi.

RAMBØLL

EHDOTUKSIA TIETOTURVA-ALAN KASVUN TUKEMISEKSI 1/3

1. **Tietoturvaklusteri ja oppilaitokset tiivistävät yhteistyötä** keskitetysti klusterin kautta, tavoitteena rekrytointien helpottaminen ja valmistuvien opiskelijoiden valmiuksien vahvistaminen (vastuu: klusteri, oppilaitokset).

    - Konkreettisia alkuvaiheen toimenpide-ehdotuksia esim. klusterin yhteiset kesätyöpaikkailmoitukset, yritysten ottaminen enenevässä määrin mukaan koulutuksen suunnitteluun ja toteuttamiseen sekä harjoittelu- ja stipendiohjelmien rakentaminen.

    - Erityishuomiota tulisi kiinnittää opiskelijoiden liiketoimintaosaamisen vahvistamiseen yritysten osaamistarpeiden näkökulmasta (asiakasymmärrys, projektiosaaminen, toimintaympäristön tuntemus jne.)

EHDOTUKSIA TIETOTURVA-ALAN KASVUN TUKEMISEKSI 2/3

2. Lisätään tietoturvaan liittyviä **yritysyhteistyömallin mukaisia täydennyskoulutusohjelmia**. Ohjelma(t) painottuisi erityisesti koulutettavien osaamisprofiilin täydentämiseen tietoturvan substanssiosaamisella liiketoimintaosaamisen ja asiakasymmärryksen näkökulmasta. Suunnittelussa konsultoitaisiin klusterin yrityksiä. (vastuu: oppilaitokset ja rahoittajat; klusteri)

3. Oppilaitokset ja klusterin yritykset yhteistyössä järjestävät **koulutuksia/seminaareja loppukäyttäjäorganisaatioiden johdolle** tietoturvan merkityksestä, riskien tunnistamisesta ja tilaajaosaamisesta. Koulutuksia tuettaisiin/rahoitettaisiin ELY-keskuksen kautta (esim. rakennerahastotuki).

EHDOTUKSIA TIETOTURVA-ALAN KASVUN TUKEMISEKSI 3/3

4. Selvitetään edellytykset ja mahdollisuudet suomalaisen tietoturvan **huippuosaamisen turvaamiseksi** ja vahvistamiseksi. (vastuu: kaikki, laaja vaikuttaminen sidosryhmissä)

   - Selvitetään edellytykset ja mahdollisuudet **kryptologian professuurin** ja tutkimusryhmän (”tutkimuksen kriittisen massan”) perustamiseksi. Selvityksessä tulee huomioida laajasti kansalliset näkökulmat ja kokonaisuus.

   - Vahvistetaan kryptologian ja muun teknisen tietoturvan osaamista eri koulutusohjelmissa (vastuu: oppilaitokset, konsultoiden klusteria)

   - Selvitetään edellytykset ja vaadittavat toimenpiteet, joiden avulla Suomesta saataisiin kansainvälinen tietoturva-alan huippututkimuksen **solmukohta** (esim. kv-tietoturvatutkimuksen konferenssit)

   - Selvitetään yhteistyömahdollisuudet **TIVIT-SHOK:n** kanssa

RAMBØLL

Vipuvoimaa EU:lta 2007–2013

Euroopan unioni
Euroopan sosiaalirahasto

Lisätietoja:

Vesa Salminen
vesa.salminen@r-m.com
www.ramboll-management.fi