TUTKIMUS

Suomalaisten organisaatioiden turvallisuus 2025

LOIHDE

taloustutkimus

TUTKIMUKSEN YHTEENVETO

Tutkimuksen tavoitteena oli selvittää, miten suomalaiset organisaatiot kokevat kokonaisturvallisuuden nykytilan ja kehittämistarpeet vuonna 2025. Lisäksi kulmana oli tutkia missä määrin organisaatiot ovat onnistuneet siirtämään turvallisuuden strategiseksi osaksi toimintaansa ja miten ne varautuvat tekoälyn tuomiin uusiin riskeihin ja mahdollisuuksiin.

Tutkimukseen osallistui 65 suurten ja keskisuurten yritysten ja julkisyhteisöjen turvallisuudesta ja tietoturvasta vastaavaa päättäjää. Turvallisuus nähdään yhä vahvemmin osana liiketoiminnan jatkuvuutta ja kilpailukykyä. Tämä näkyy myös siinä, että useimmat organisaatiot pitävät turvallisuutta kriittisenä menestystekijänä – ei enää vain suojautumisen välineenä, vaan liiketoiminnan mahdollistajana.

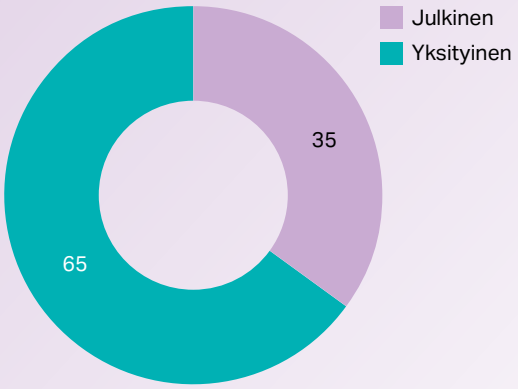
Organisaatioiden suurimmat turvallisuushaasteet liittyvät ennen kaikkea osaamisen ja resurssien riittävyyteen, reaaliaikaisten uhkien tunnistamiseen sekä tiedon suojaamiseen ja eheyden varmistamiseen tekoälyn aikakaudella. Julkisella sektorilla korostuu erityisesti osaamisen ja resurssien puute, kun taas yksityinen sektori painottaa enemmän kykyä hallita nopeasti kehittyviä teknologisia uhkia.

Noin kolmasosa vastaajista ilmoittaa omassa organisaatiossaan tapahtuneen liiketoimintaa haittaavan tietoturvapoikkeaman edellisen kahden vuoden aikana. Useimmiten kyseessä oli palvelunestohyökkäys tai henkilötietoihin liittyvä tietoturvahaaste. Neljällä viidestä organisaatiosta on tekoälytyökaluja koskevat hyväksytyn käytön politiikat. Julkisella sektorilla tekoälypolitiikat ovat käytössä useammin kuin yksityisellä sektorilla.

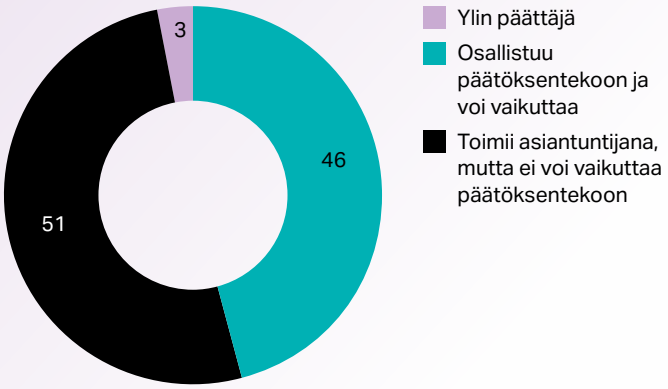
Seitsemän kymmenestä organisaatiosta käyttää SOC:ia, ja sen käyttö on yleistynyt erityisesti julkisella sektorilla vuodesta 2022 lähtien. Suurin osa vastaajista korostaa vastuunjakoa, suunnitelmallisuutta ja sisäistä osaamista turvallisuusuhkiin varautumisessa. Julkisella sektorilla painotetaan erityisesti vastuunjakoa sekä sisäisiin uhkiin varautumista harjoittelun ja skenaarioiden avulla. Seuraavien kahden vuoden aikana organisaatiot aikovat panostaa erityisesti käyttäjätunnusten ja identiteettien suojaamiseen sekä tekoälyn hyödyntämisen mahdollistamiseen henkilöstölle.

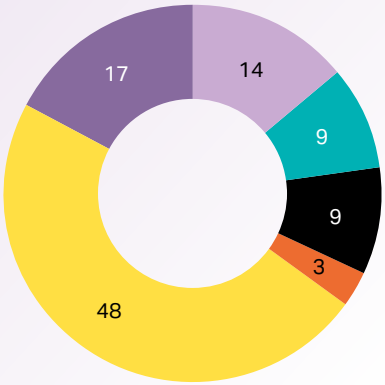
TAUSTATIEDOT

Vastaajan organisaatio



Vastaajan asema organisaation turvallisuus- ja tietohallintoasioissa





Organisaatioiden liikevaihto

- 10–29 miljoonaa euroa/v
- 30–49 miljoonaa euroa/v
- 50–99 miljoonaa euroa/v
- 100–149 miljoonaa euroa/v
- 150+ miljoonaa euroa/v
- Ei osaa sanoa

Kaikki vastaajat, n=65

Tutkimuksen toteuttaja, tiedonkeruu ja ajankohta

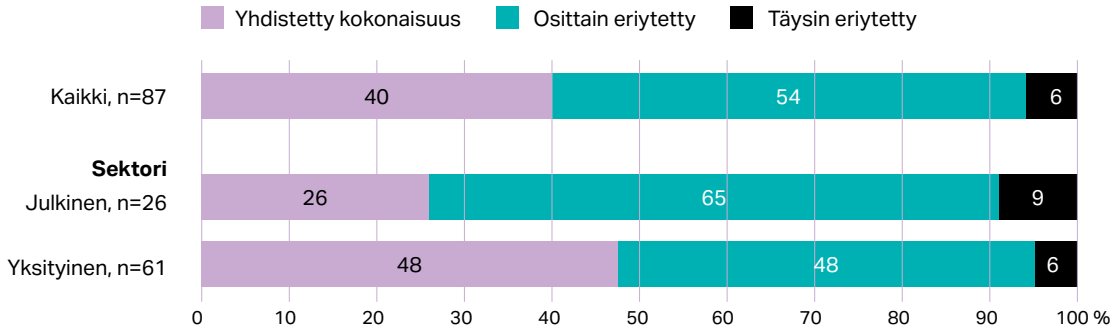
Taloustutkimus Oy toteutti tämän tutkimuksen Loihteen toimeksiannosta. Tiedonkeruumenetelmänä valittujen yritysten ja organisaatioiden turvallisuudesta ja tietoturvasta vastaavien puhelinhaastattelut. Ajankohta 15.9.–9.10.2025. Yhden haastattelun keskimääräinen kesto oli noin 14 minuuttia. Puhelinhaastattelut teki kaksi Taloustutkimuksen koulutettua puhelinhaastattelijaa.

Kohderyhmä, otoskoko, tutkimuksen näyte ja puhelinhaastattelut

Pääasiallisesti suurten ja keskisuurten yritysten turvallisuudesta ja tietoturvasta vastaavat päättäjät, toissijaisesti valitut julkisen sektorin turvallisuudesta ja tietoturvasta vastaavat päättäjät. Lopullinen otoskoko n=65, otosta ei ole painotettu. Loihde muodosti tutkimusnäytteen yhdessä Taloustutkimuksen kanssa sovittujen poimintakriteerien perusteella. Näytelähteenä Alma Insights päättäjätietokanta. Tutkimukseen tehtiin ohjaavat vastaajakiintiöt yksityiselle ja julkiselle sektorille.

Vain 6% vastaajista toimii täysin eriytetyillä turvallisuusorganisaatioilla.

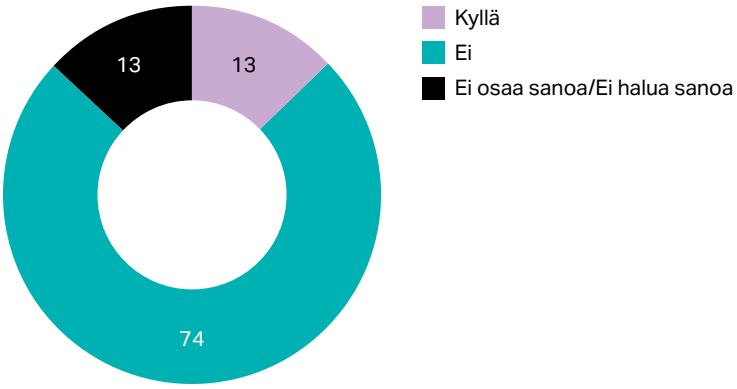
Mikä seuraavista kuvaa parhaiten organisaatiosi turvallisuusasioiden (esim. toimitila- & tietoturvallisuus) organisointia?



n=kaikki vastaajat

Lievä enemmistö (54 %) vastaajista kertoo, että heidän organisaatiossaan turvallisuusasiat, kuten toimitila- ja tietoturvallisuus, on osittain eriytetty. Kuitenkin vain 6 % vastaajista toimii täysin eriytetyillä turvallisuusorganisaatioilla. Yksityisellä puolella lähes 48 %:lla organisaatioista turvallisuus on yhdistetty kokonaisuus. Julkisella sektorilla tästä luvusta jäädään. Suurin osa eriytetyillä organisaatioilla toimivista ei suunnittele näiden yhdistämistä seuraavien kahden vuoden aikana.

Suunnitteleeko organisaatiosi turvallisuusorganisaatioiden yhdistämistä seuraavien kahden vuoden aikana?

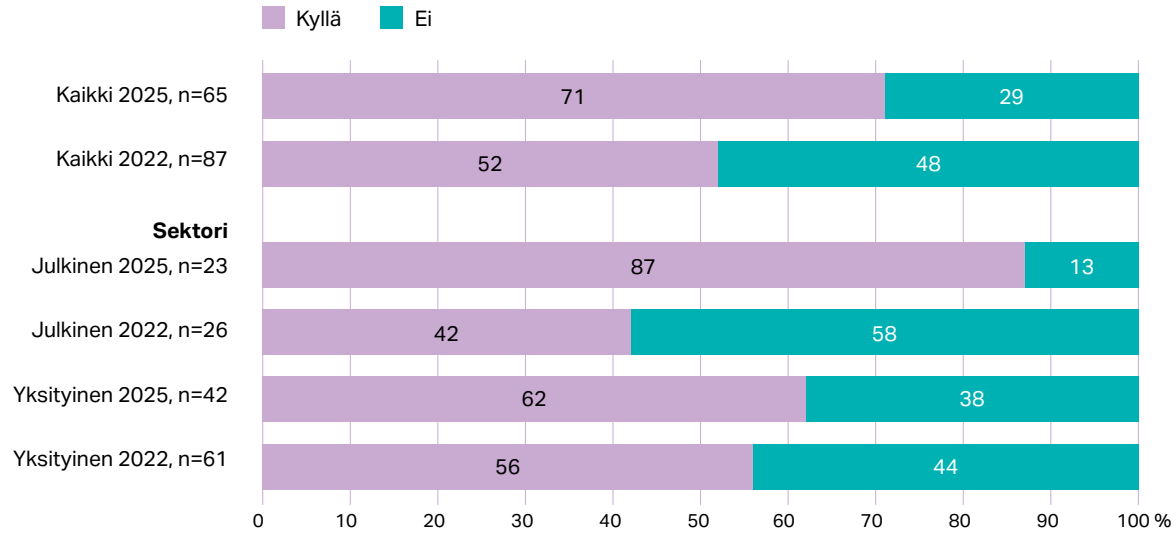


Täysin tai osittain eriytetty, n=39

Seitsemän kymmenestä organisaatiosta käyttää SOC:ia.

Onko organisaatiossasi käytössä SOC (=Security Operation Center)?

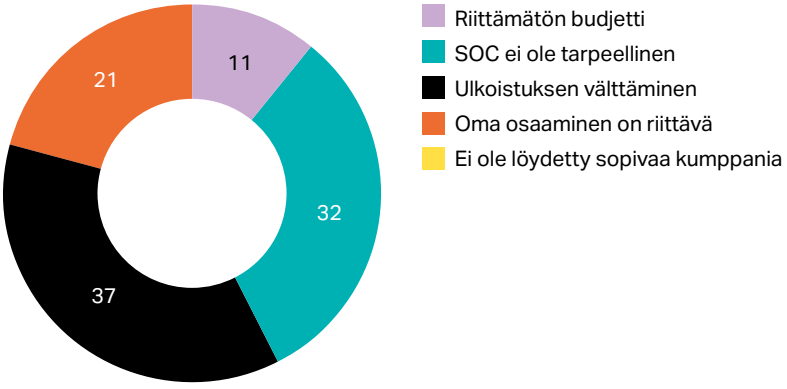
Tuloksia verrattu Loihteen vuoden 2022 tutkimukseen, jossa vastaajaryhmä oli hyvin samanlainen.



n=kaikki vastaajat

Seitsemän kymmenestä organisaatiosta käyttää SOC:ia, ja sen käyttö on yleistynyt erityisesti julkisella sektorilla vuodesta 2022 lähtien (edellinen teettämämme tutkimus). Pääsyiksi sille, ettei SOC:ia ole otettu käyttöön kerrottiin oman osaamisen riittävyyden tai sen ettei SOC:ia koeta tarpeelliseksi.

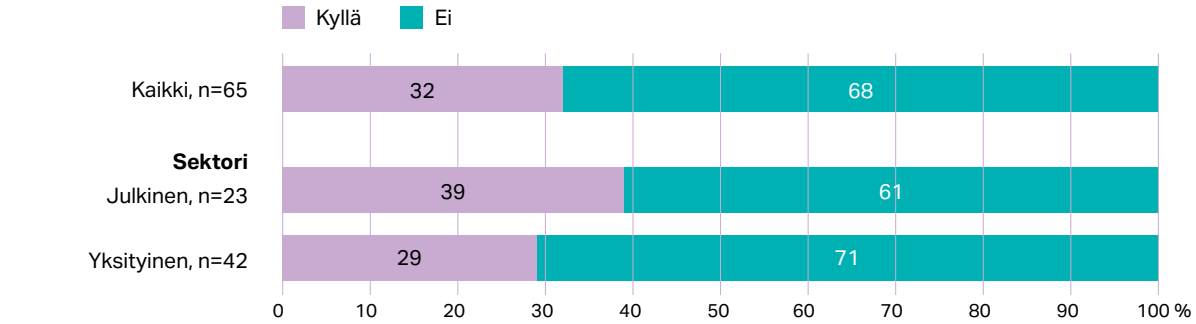
Mikä seuraavista kuvaa parhaiten syytä sille, että SOC ei ole organisaatiossasi käytössä?



Ei ole käytössä, n=19* *) Alhainen vastaajamäärä, tulos suuntaa-antava

Joka kolmannella organisaatiolla on tapahtunut liiketoimintaa haittaava tietoturvapoikkeama kahden vuoden sisällä.

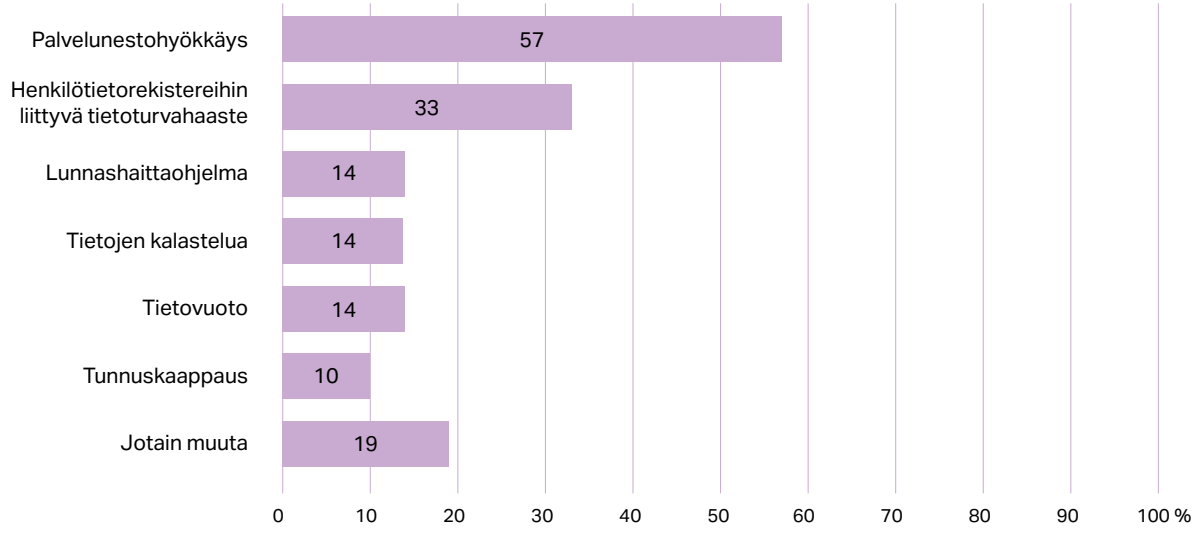
Onko organisaatiossasi tapahtunut liiketoimintaa haittaavaa tietoturvapoikkeamaa edellisen kahden vuoden aikana?



n=kaikki vastaajat

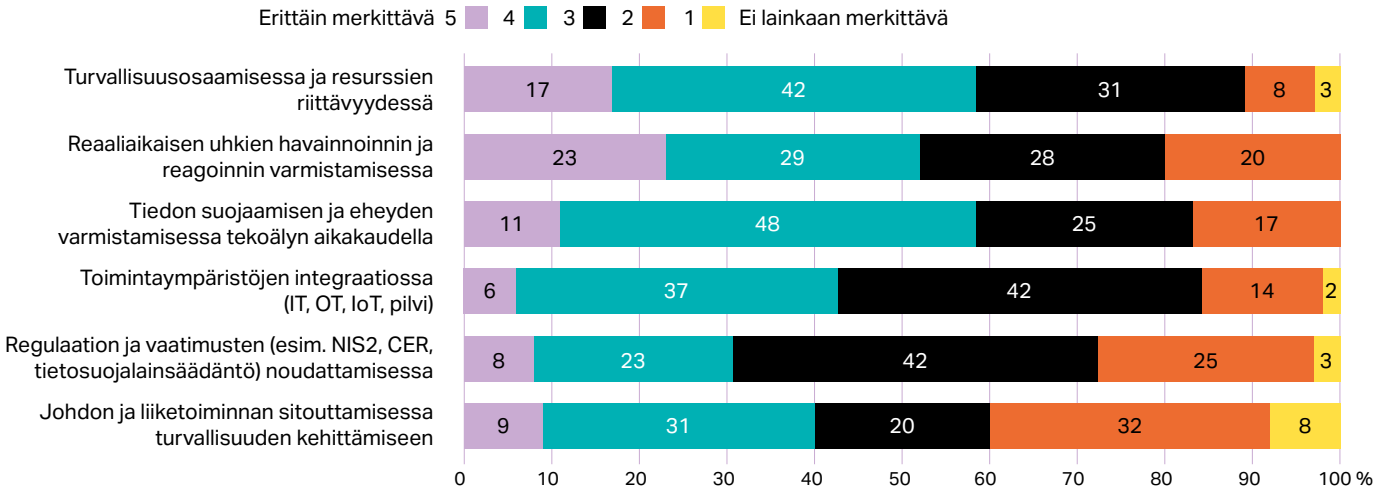
Noin kolmasosa vastaajista ilmoittaa omassa organisaatiossaan tapahtuneen liiketoimintaa haittaavan tietoturvapoikkeaman edellisen kahden vuoden aikana. Useimmiten kyseessä oli palvelunestohyökkäys tai henkilötietoihin liittyvä tietoturvahaaste.

Mikä seuraavista tieturvapoikkeamista?



On tapahtunut liiketoimintaa haittaavaa tietoturvapoikkeamaa edellisen kahden vuoden aikana, n=21

Minkä organisaatioihin vaikuttavista tekijöistä arvioit aiheuttavan suurimmat turvallisuushaasteet seuraavan kahden vuoden aikana?



Kaikki vastaajat, n=65

Keskiarvo 1–5 (1=ei lainkaan merkittävä...5=erittäin merkittävä)

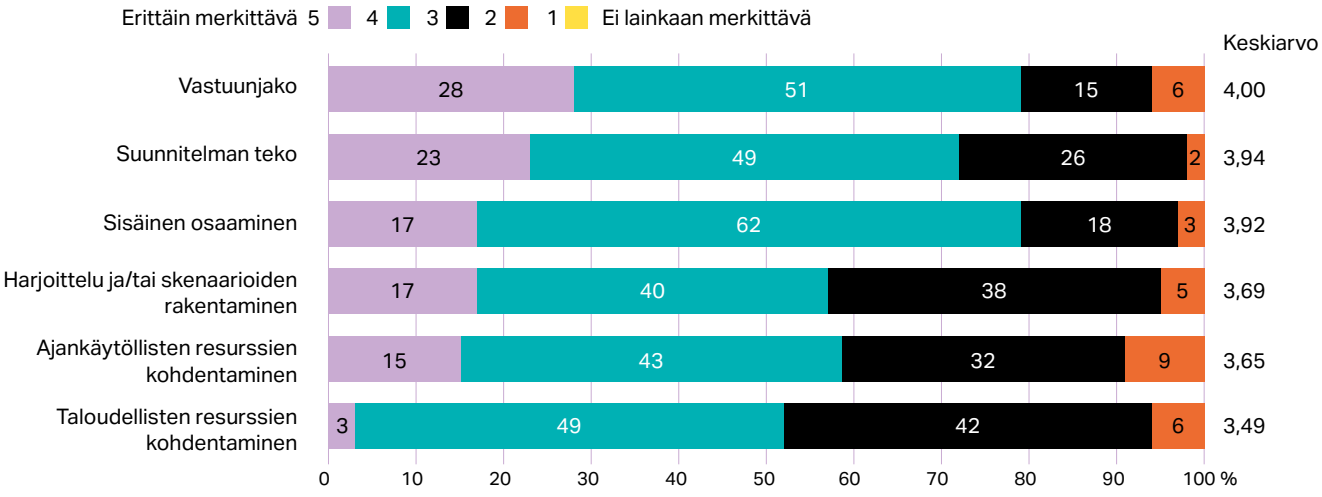
	Sektori		
	Kaikki, n=65	Julkinen, n=23	Yksityinen, n=42
Turvallisuusosaamisessa ja resurssien riittävyydessä	3,62	4,09	3,36
Reaaliaikaisen uhkien havainnoinnin ja reagoinnin varmistamisessa	3,55	3,70	3,48
Tiedon suojaamisen ja eheyden varmistamisessa tekoälyn aikakaudella	3,52	3,87	3,33
Toimintaympäristöjen integraatiossa (IT, OT, IoT, pilvi)	3,32	3,61	3,17
Regulaation ja vaatimusten (esim. NIS2, CER, tietosuojalainsäädäntö) noudattamisessa	3,08	3,26	2,98
Johdon ja liiketoiminnan sitouttamisessa turvallisuuden kehittämiseen	3,02	3,26	2,88

4,5–5,0
4,0–4,5
3,5–4,0
3,0–3,5
2,5–3,0
2,0–2,5
1,5–2,0
1,0–1,5

n=kaikki vastaajat

Organisaatioiden suurimmat turvallisuushaasteet liittyvät tällä hetkellä osaamisen ja resurssien riittävyyteen, reaaliaikaisten uhkien tunnistamiseen sekä tiedon suojaamiseen ja eheyden varmistamiseen tekoälyn aikakaudella. Julkisella sektorilla erityisesti turvallisuusosaamisen ja resurssien riittävyys koetaan merkittäväksi haasteeksi. Yksityisellä sektorilla reaaliaikaisten uhkien tunnistaminen nousee hieman merkittävämmäksi. Etenkään yksityisellä sektorilla regulaatioiden ja vaatimusten (esim. NIS2, CER, GDPR) noudattamisen sekä johdon ja liiketoiminnan sitouttamisen turvallisuuden kehittämiseen ei nähty tuottavan merkittäviä haasteita seuraavan kahden vuoden aikana.

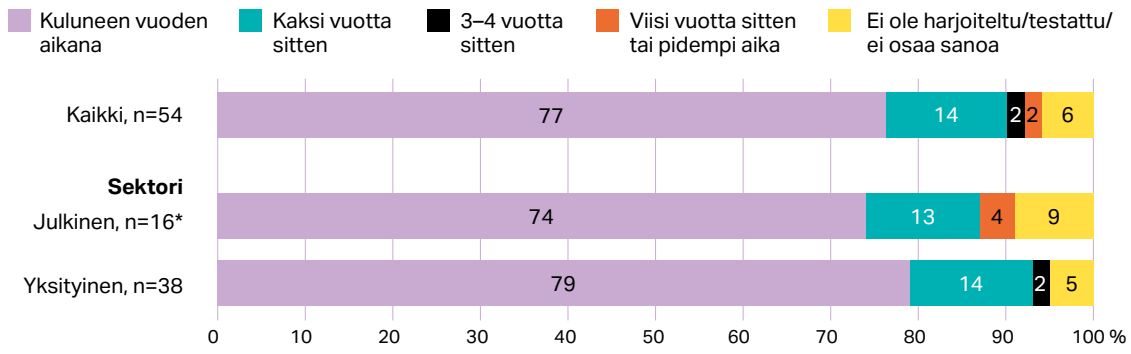
Miten arvioit seuraavien tekijöiden merkittävyyttä turvallisuusuhkiin varautumisen näkökulmasta?



Kaikki vastaajat, n=65

Vastuunjako nähdään kaikkein tärkeimpänä tekijänä turvallisuusuhkiin varautumisen kannalta. Lisäksi suunnitelmallisuus ja sisäinen osaaminen nousevat top 3 -listalle. Julkisella sektorilla painotetaan erityisesti vastuunjakoa sekä uhkiin varautumista harjoittelun ja skenaarioiden avulla. Kaikista vastaajista 77 % on harjoitellut tai testannut varautumissuunnitelmaansa kuluneen vuoden aikana ja 14 % kuluneen kahden vuoden aikana.

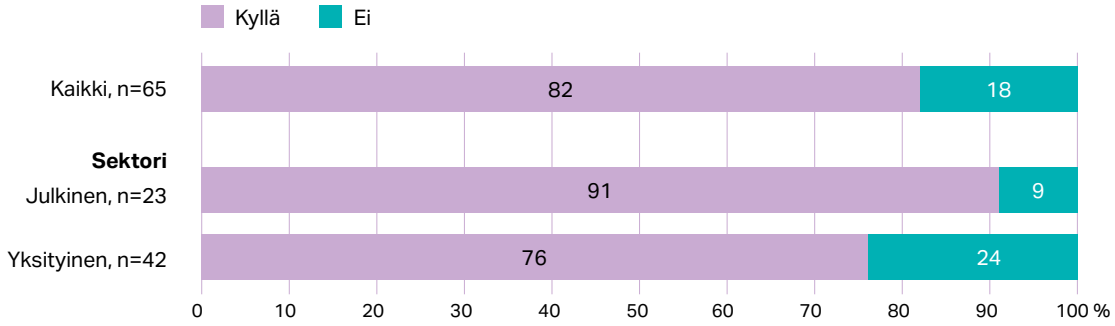
Milloin organisaatiosi on viimeksi harjoitellut / testannut turvallisuusuhkiin liittyvää varautumissuunnitelmaa?



n=kaikki vastaajat

Neljällä viidestä on hyväksytyn käytön politiikat tekoälytyökaluihin liittyen.

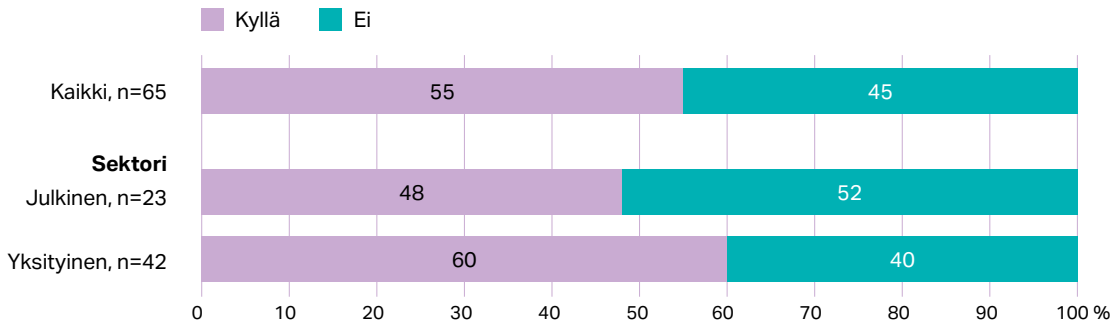
Onko organisaatiosi määrittänyt tekoälytyökaluihin liittyvät hyväksytyn käytön politiikat?



n=kaikki vastaajat

Hyväksytyn käytön politiikat tekoälytyökaluihin liittyen on neljällä viidestä. Julkisella sektorilla tekoälypolitiikat ovat käytössä useammin (91 %) kuin yksityisellä sektorilla (76 %).

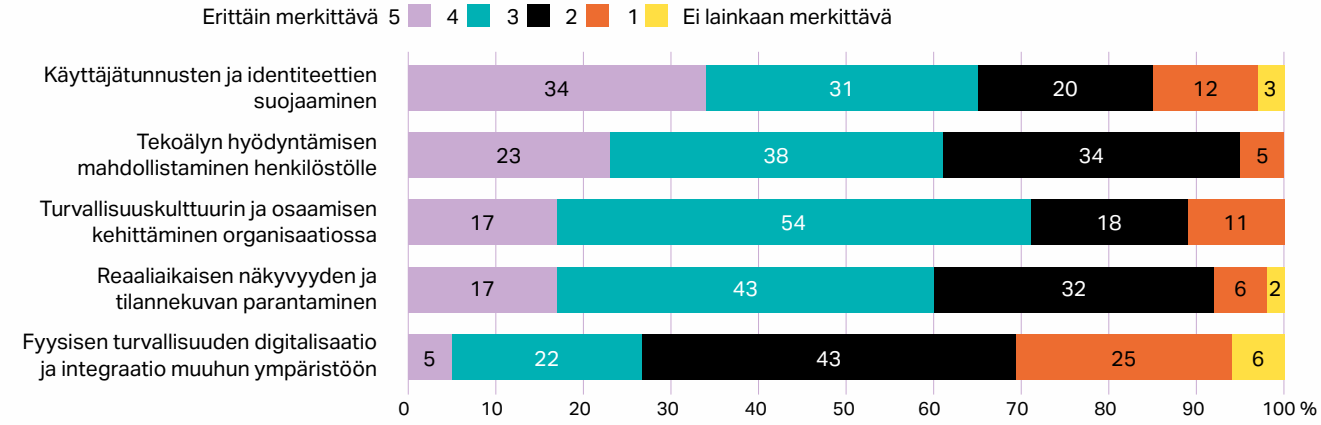
Valvotaanko teillä konkreettisesti tekoälytyökalujen käyttöä tai hyväksytyn politiikan noudattamista?



n=kaikki vastaajat

Vastaajista 55 % myös valvoo konkreettisesti tekoälytyökalujen käyttöä tai politiikan noudattamista. Yksityisellä sektorilla konkreettista valvontaa harjoitetaan enemmän (60 %) kuin julkisella (48 %).

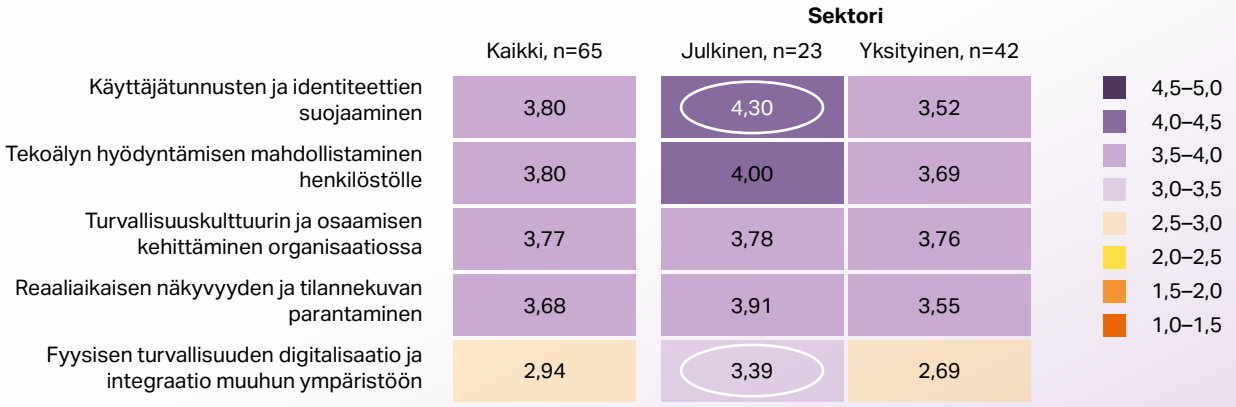
Miten merkittävinä koet seuraavat asiat organisaatiosi turvallisuuden kehittämisessä seuraavien kahden vuoden aikana?



Kaikki vastaajat, n=65

Merkittävimmiksi kehityskohteiksi omassa organisaatioissa seuraavan kahden vuoden aikana koettiin käyttäjätunnusten ja identiteettien suojaaminen, tekoälyn hyödyntämisen mahdollistaminen henkilöstölle ja turvallisuuskulttuurin ja osaamisen kehittäminen organisaatiossa. Julkisen sektorin päättäjät korostavat käyttäjätunnusten ja identiteettien suojaamista selvästi useammin kuin yksityisellä sektorilla. Toisena panostuksena julkisella puolella korostuu selvästi tekoälyn hyödyntämisen mahdollistaminen. Yksityisellä puollella oli tasaisempaa merkittävimmiksi koetuissa asioissa organisaation turvallisuuden kehittämisessä. Suurimmiksi haasteiksikin koetut turvallisuuskulttuuri ja osaaminen, tekoälyn mahdollistaminen sekä reaaliaikaisen näkyvyyden parantaminen nostivat kuitenkin päätään yksityisellä puolella.

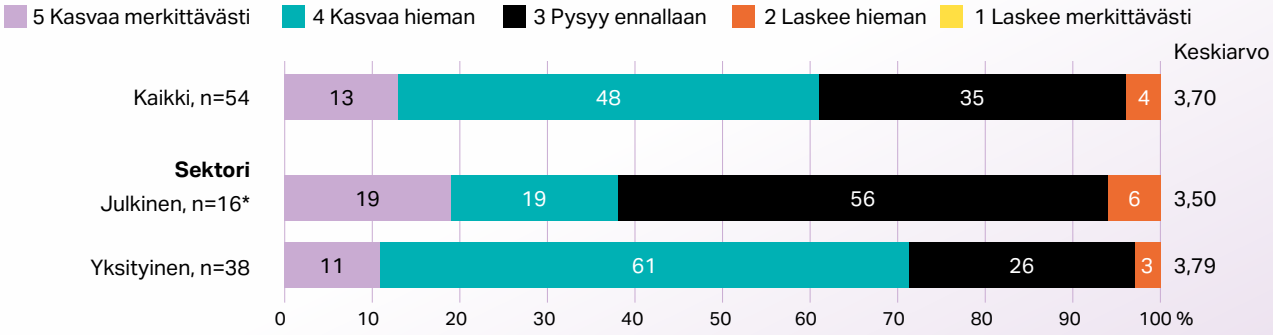
Keskiarvo 1–5 (1=ei lainkaan merkittävä...5=erittäin merkittävä)



n=kaikki vastaajat

Vain 38 % julkisista organisaatioista uskoo turvallisuusbudjetin kasvavan seuraavina kahtena vuotena vs. Yksityinen 72 %

Kuinka arvioit turvallisuusbudjetin kehittyvän seuraavan kahden vuoden aikana?



n=on erillinen turvallisuusbudjetti: *) Alhainen vastaajamäärä, tulos suuntaa-antava

Loihde on liiketoiminnan jatkuvuuden mahdollistaja. Autamme asiakkaitamme luomaan kestävää kilpailukykyä datan, tekoälyn ja digitalisaation avulla, hyötymään pilven mahdollisuuksista ja suojautumaan sekä fyysisen että verkkomaailman uhilta. Näiden osaamistemme yhdistäminen tekee Loihteesta ainutlaatuisen ja kokonaisvaltaisen kumppanin. Asiantuntijoita meillä on noin 760, ja Loihteen liikevaihto vuonna 2024 oli 140 miljoonaa euroa.

loihde.com

LOIHDE