TUTKIMUS

Suomalaisten organisaatioiden tietoturva 2023–2025

LOIHDE TRUST

CHECK POINT™

Tutkimuksen yhteenveto

Tutkimuksen tavoite oli tutkia tietoturvaan perehtyneiden yksityisen ja julkisen sektorin päättäjien ajatuksia ja mielipiteitä organisaatioiden kokonaisturvallisuuteen liittyvissä asioissa.

Tutkimukseen osallistui 87 suurten ja keskisuurten yritysten ja julkisyhteisöjen tietohallinnosta ja tietoturvasta vastaavaa päättäjää. Tutkimuksen tulokset piirtävät kuvan tarpeesta lisätä näkyvyyttä suomalaisten organisaatioiden tietoturvatyössä, kun toimintaympäristöt muuntuvat vauhdilla ja eri laitteet liittyvät verkkoon.

Organisaatioista 26 prosenttia oli tunnistanut liiketoimintaa haitanneen tietoturvatapahtuman viimeisten kahden vuoden aikana ja jopa 62 prosenttia uskoi joutuvansa kyberhyökkäyksen kohteeksi seuraavan kahden vuoden aikana. Määrä nousi 76 prosenttiin, kun tarkastellaan vain suuria, yli 100 milj. € liikevaihdon omaavia yrityksiä. Yleisimpiä liiketoimintaa haittaavia tietoturvatapahtumia olivat henkilörekistereihin liittyvät tietoturvahaastet (48 % vastaajista) ja tietovuoto (35 % vastaajista). Vaikka kyberhyökkäyksen kohteeksi joutumiseen uskotaankin vankasti, niin silti merkittäviä turvallisuusinvestointeja ei aina olla valmiita tekemään. Vastaajista 66 prosenttia tulee investoimaan tietoturvaan alle 250 tuhatta euroa seuraavien 3 vuoden aikana.

Merkittävimpinä kehityskohteina tietoturvassa seuraavina vuosina vastaajat näkivät digitalisoituvien turvajärjestelmien aiheuttamien tietoturvariskien hallinnan (90 % vastaajista), pilvipalveluiden yleistymisen ja niiden hallinnan (78 % vastaajista) sekä etätyön luomat tietoturvahaasteet (78 % vastaajista). Erilaisten turvajärjestelmien siirtyminen verkkoon pienentää toimitilaturvallisuuden ja tietoturvallisuuden kuilua ja niiden hallinta toisistaan erillään ei välttämättä enää ole optimaalista. Organisaatioista 44 prosenttia oli yhdistänyt turvallisuusorganisaation ja hallinnoivat yritysturvallisuutta yhden yksikön kautta.

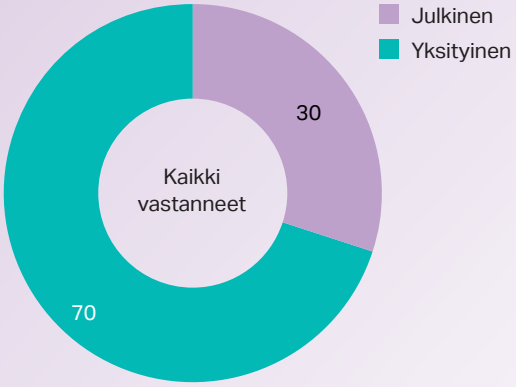
Suurimpina haasteina seuraavina vuosina tietoturvakehityksessä koettiin tiedon suojaaminen ja sen eheyden varmistaminen (66 % vastaajista) ja käyttäjätunnusten ja identiteettien suojaaminen (62 % vastaajista).

SOC (Security Operation Center) oli käytössä reilulla puolella organisaatioista. Organisaatioilla, joilla SOC oli käytössä, lisääntyi merkittävästi myös näkyvyys turvallisuustoiminnan vaikuttavuuteen. Tällaisista organisaatioista 60 prosenttia vastasi näkyvyyden olevan hyvä tai erittäin hyvä. Organisaatioista, joilla SOC ei ollut käytössä vastaava näkyvyys toiminnan vaikuttavuuteen oli vain 15 prosentilla.

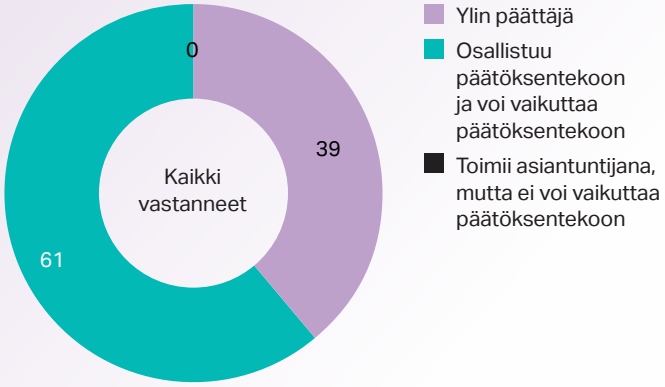
Taustatiedot

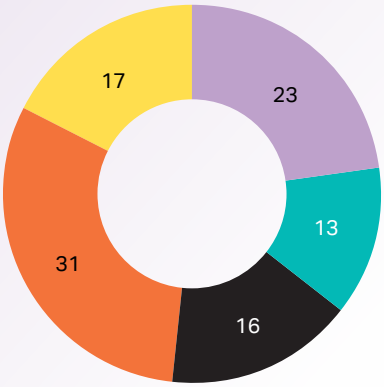
Kaikki vastaajat, n=87

SEKTORI



ASEMA ORGANISAATION TIETOTURVA- JA TIETOHALLINTOASIOISSA





YRITYKSEN LIIKEVAIHTO

- 30–49 miljoonaa euroa
- 50–99 miljoonaa euroa
- 100–149 miljoonaa euroa
- 150+ miljoonaa euroa
- Ei osaa sanoa (sis. julkista sektoria)

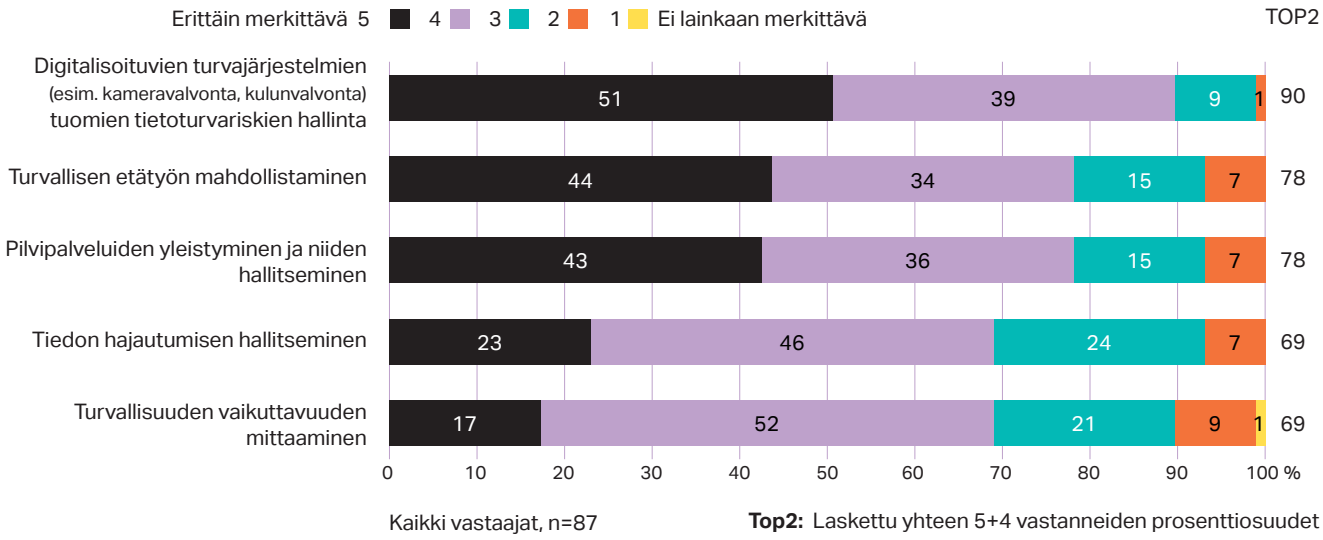
Tutkimuksen toteuttaja, tiedonkeruu ja ajankohta

Taloustutkimus Oy toteutti tämän tutkimuksen Loihde Trustin ja Check Pointin toimeksiannosta. Tiedonkeruumenetelmänä valittujen yritysten ja organisaatioiden tietoturvapäättäjien puhelinhaastattelut. Ajankohta 19.10.–2.12.2022. Yhden haastattelun keskimääräinen kesto oli 14 minuuttia. Puhelinhaastattelut teki kaksi Taloustutkimuksen koulutettua puhelinhaastattelijaa.

Kohderyhmä, otoskoko, tutkimuksen näyte ja puhelinhaastattelut

Pääasiallisesti suurten ja keskisuurten yritysten tietohallinnosta ja tietoturvasta vastaavat päättäjät, toissijaisesti valitut julkisen sektorin tietohallinnosta ja tietoturvasta vastaavat päättäjät. Lopullinen otoskoko n=87, otosta ei ole painotettu. Loihde Trust ja Check Point muodostivat tutkimusnäytteen yhdessä Taloustutkimuksen kanssa sovittujen poimintakriteerien perusteella. Tutkimukseen tehtiin ohjaavat vastaajakiintiöt yksityiselle ja julkiselle sektorille.

Miten merkittävänä koet seuraavat asiat yrityksesi tai organisaatiosi turvallisuuden kehittämisessä seuraavien kahden vuoden aikana?



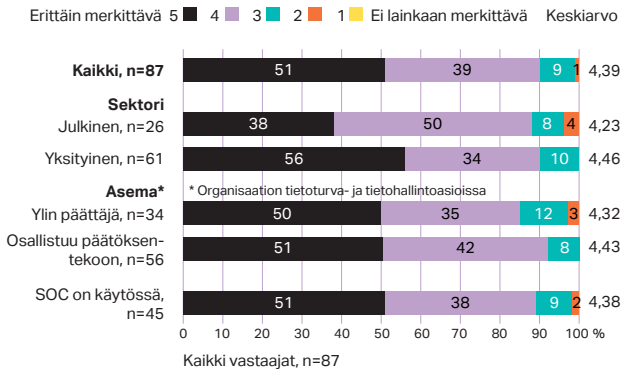
Kaikki vastaajat, n=87

Top2: Laskettu yhteen 5+4 vastanneiden prosenttiosuudet

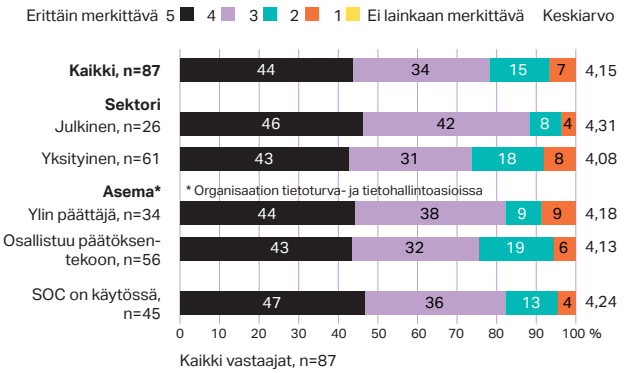
Seuraavien kahden vuoden aikana tietohallinto- ja tietoturvapäättäjien selkeä enemmistö pitää **merkittävimpänä** oman organisaatioiden turvallisuuden kehittämisessä **digitalisoituvien turvajärjestelmien aiheuttamaa tietoturvariskien hallintaa**. Myös **turvallisen etätyön mahdollistaminen ja pilvipalveluiden yleistymisen hallinta** koetaan hyvin merkittäviksi kehitettäviksi asioiksi seuraavien kahden vuoden aikana. Tutkituista asioista **vähemmän merkittäviksi** kehittämiskohteiksi koettiin **tiedon hajautumisen hallitseminen ja turvallisuuden vaikuttavuuden mittaaminen**.

Miten merkittävänä koet seuraavat asiat yrityksesi tai organisaatiosi turvallisuuden kehittämisessä seuraavien kahden vuoden aikana?

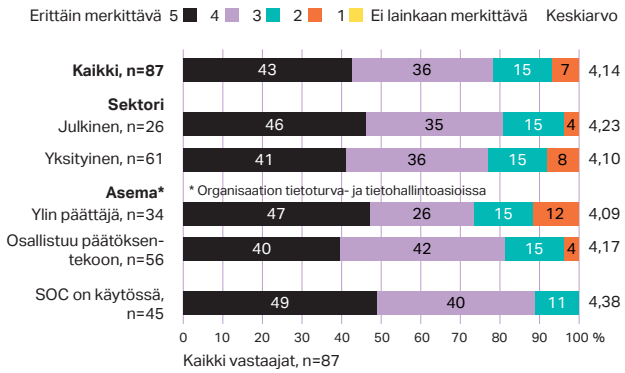
Digitalisoituvien turvajärjestelmien (esim. kameravalvonta, kulunvalvonta) tuomien tietoturvariskien hallinta



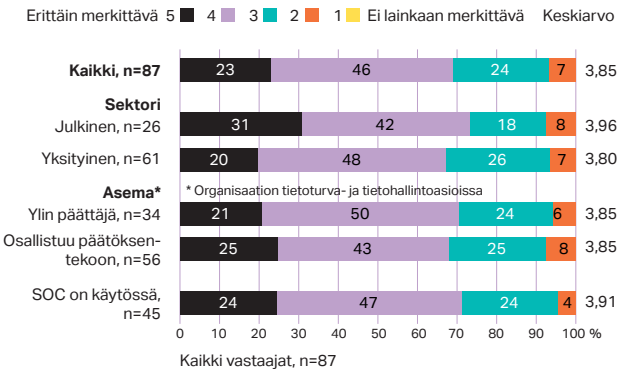
Turvallisen etätyön mahdollistaminen



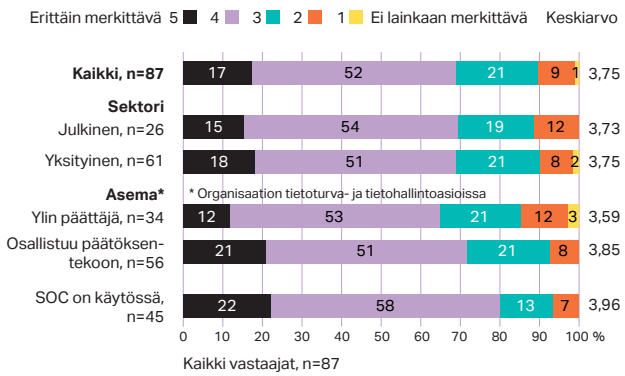
Pilvipalveluiden yleistyminen ja niiden hallitseminen



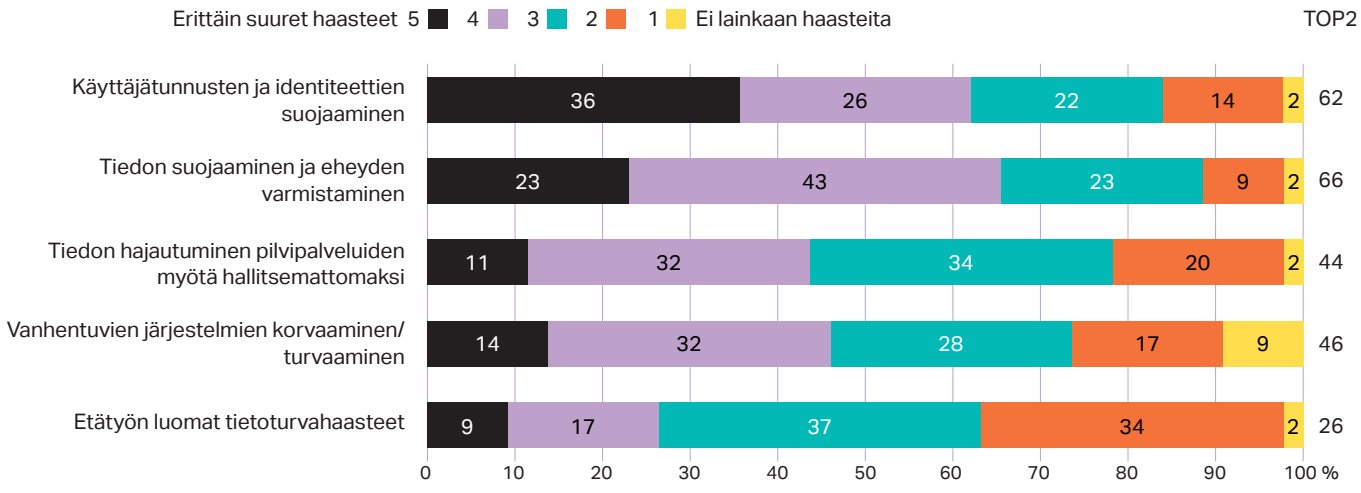
Tiedon hajautumisen hallitseminen



Turvallisuuden vaikuttavuuden mittaaminen



Millä seuraavilla osa-alueilla uskot suurimpien haasteiden syntyvän tietoturvallisuuden osalta seuraavien kahden vuoden aikana?

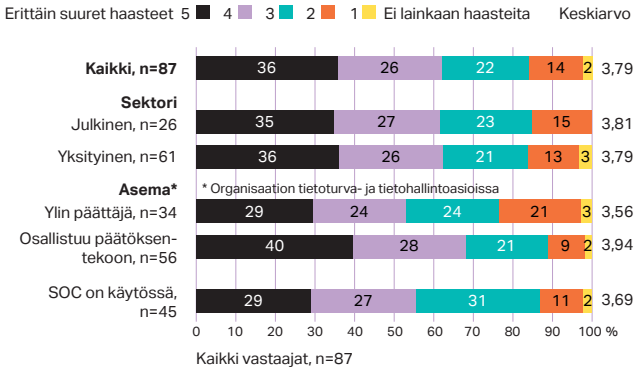


Top2: Laskettu yhteen 5+4 vastanneiden prosenttiosuudet

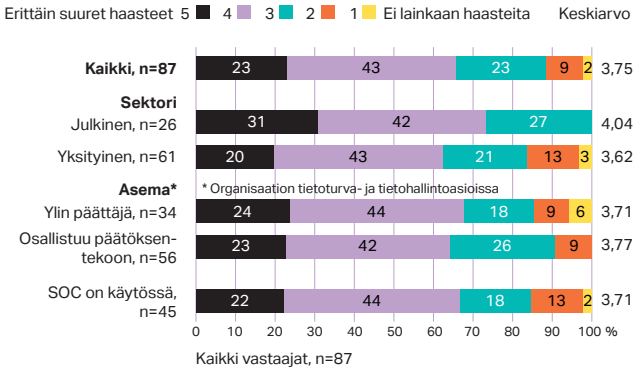
Seuraavien kahden vuoden aikana **suurimmiksi haasteiksi** tietoturvan suhteen koetaan **käyttäjätunnusten ja identiteettien suojaaminen yhdessä tiedon suojaamisen ja sen eheyden varmistamisen** ohella. Vastauksissa on jonkin verran eroja, sillä käyttäjätunnusten ja identiteettien suojaamista ei koettu aivan niin suuriksi haasteiksi ylimpien päättäjien keskuudessa ja niissä organisaatioissa, joissa SOC (=Security Operation Center) on käytössä. Toisaalta tiedon suojaaminen ja sen eheyden varmistaminen koettiin selvästi suurimmaksi haasteeksi erityisesti julkisella sektorilla. Kokonaistasolla selvästi **vähemmän haasteellisiksi** tuleviksi tietoturva-asioiksi koetaan **tiedon hajautuminen pilvessä, vanhentuvien järjestelmien korvaaminen/turvaaminen** ja **etätyön luomat tietoturvahaasteet**.

Millä seuraavilla osa-alueilla uskot suurimpien haasteiden syntyvän tietoturvallisuuden osalta seuraavien kahden vuoden aikana?

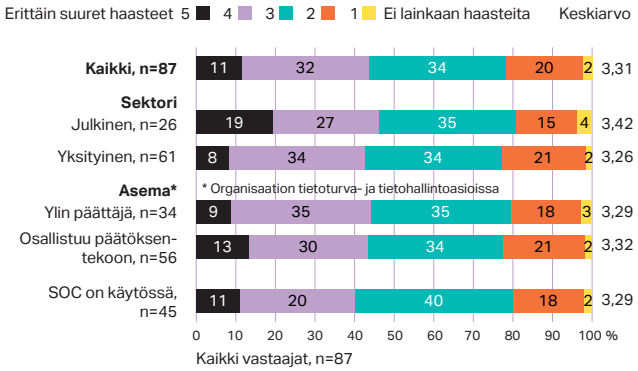
Käyttäjätunnusten ja identiteettien suojaaminen



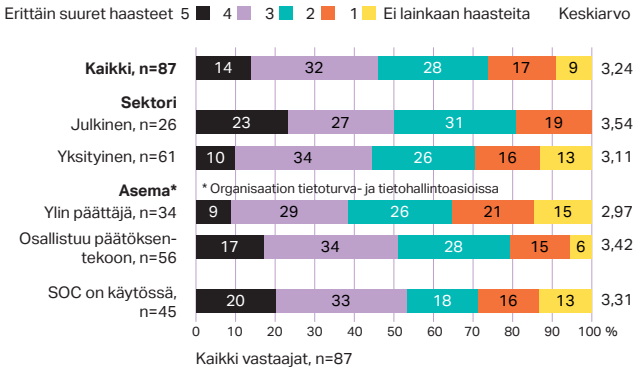
Tiedon suojaaminen ja eheyden varmistaminen



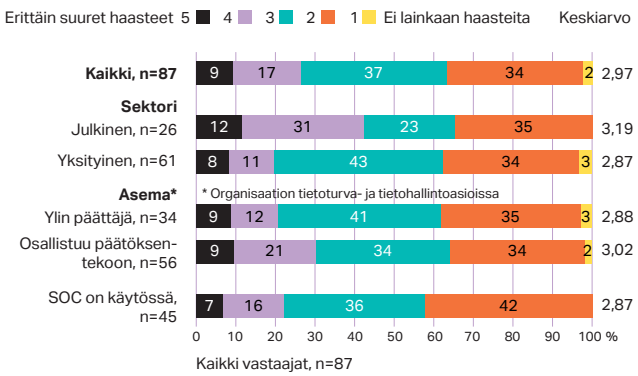
Tiedon hajautuminen pilvipalveluiden myötä hallitsemattomaksi



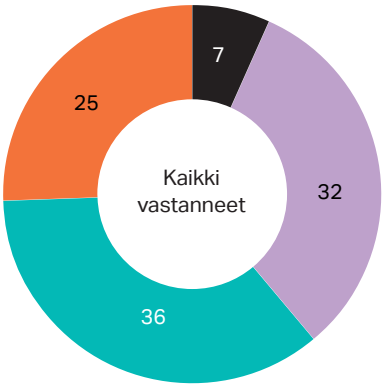
Vanhentuvien järjestelmien korvaaminen/turvaaminen

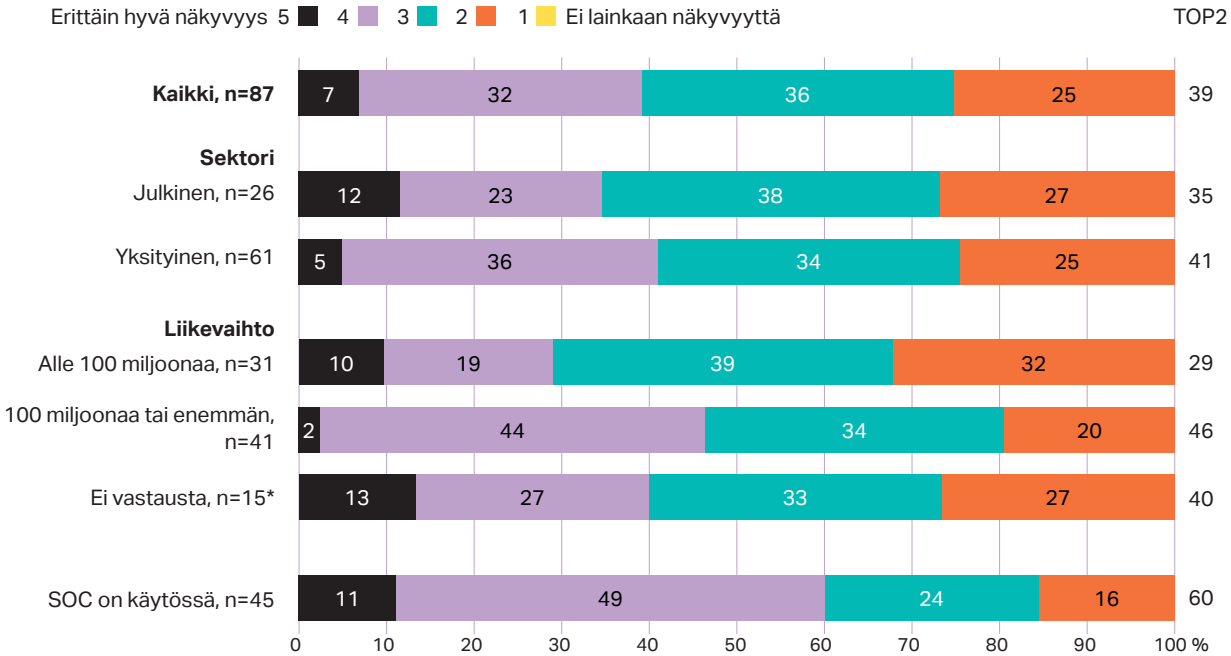


Etätyön luomat tietoturvahaasteet



Kuinka hyvin yrityksessäsi tai organisaatiossasi pystytään mittaamaan turvallisuustoiminnan vaikuttavuutta?



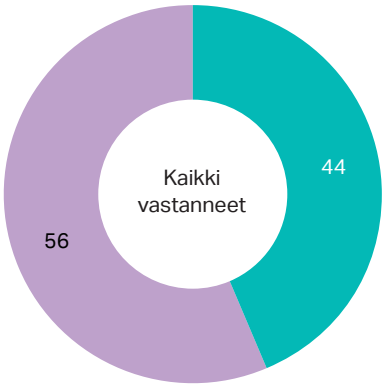


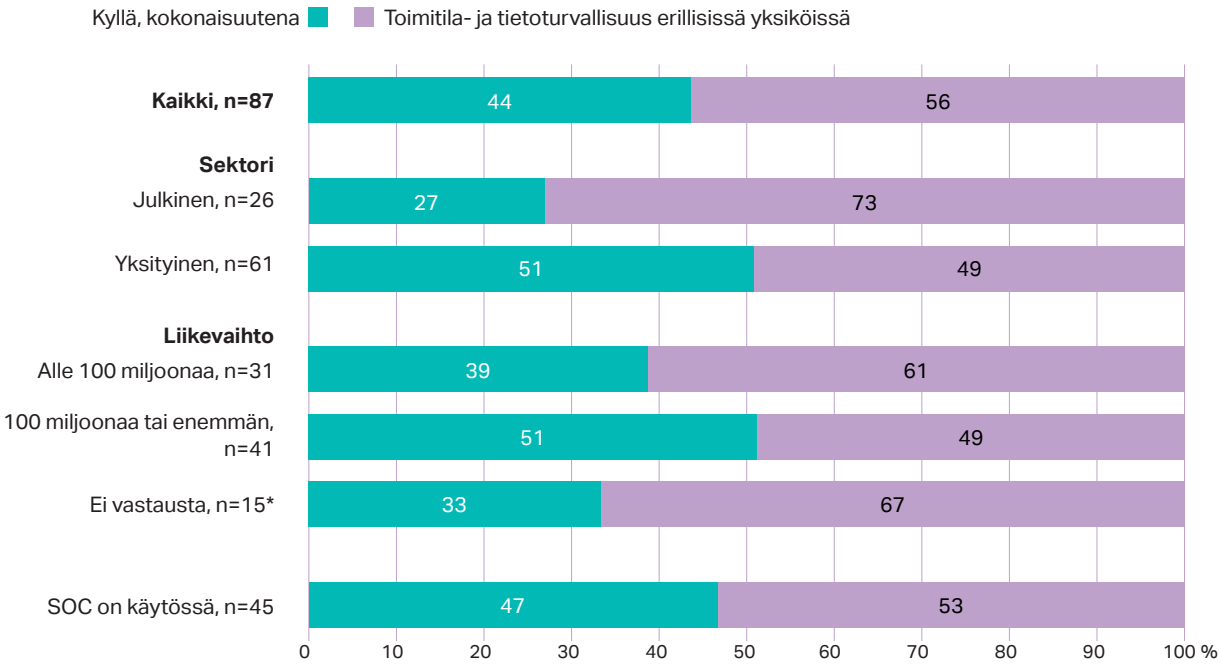
*) Pieni vastaajamäärä, tulos suuntaa-antava

Top2: Laskettu yhteen 5+4 vastanneiden prosenttiosuudet

Turvallisuustoiminnan vaikuttavuuden mittaamisessa näkyvyys on parasta yrityksillä, joilla on SOC käytössä. Näissä yrityksissä yli puolet vastaajista arvioi turvallisuustoiminnan vaikuttavuuden näkyvyyden melko hyväksi. Kokonaistasolla vaikuttavuuden näkyvyyden arvioidaan olevan vain tyydyttävällä tasolla.

Hallitaanko yrityksessäsi tai organisaatiossasi turvallisuutta kokonaisuutena vai ovatko esim. toimitilaturvallisuus ja tietoturvallisuus erillisissä yksiköissä?

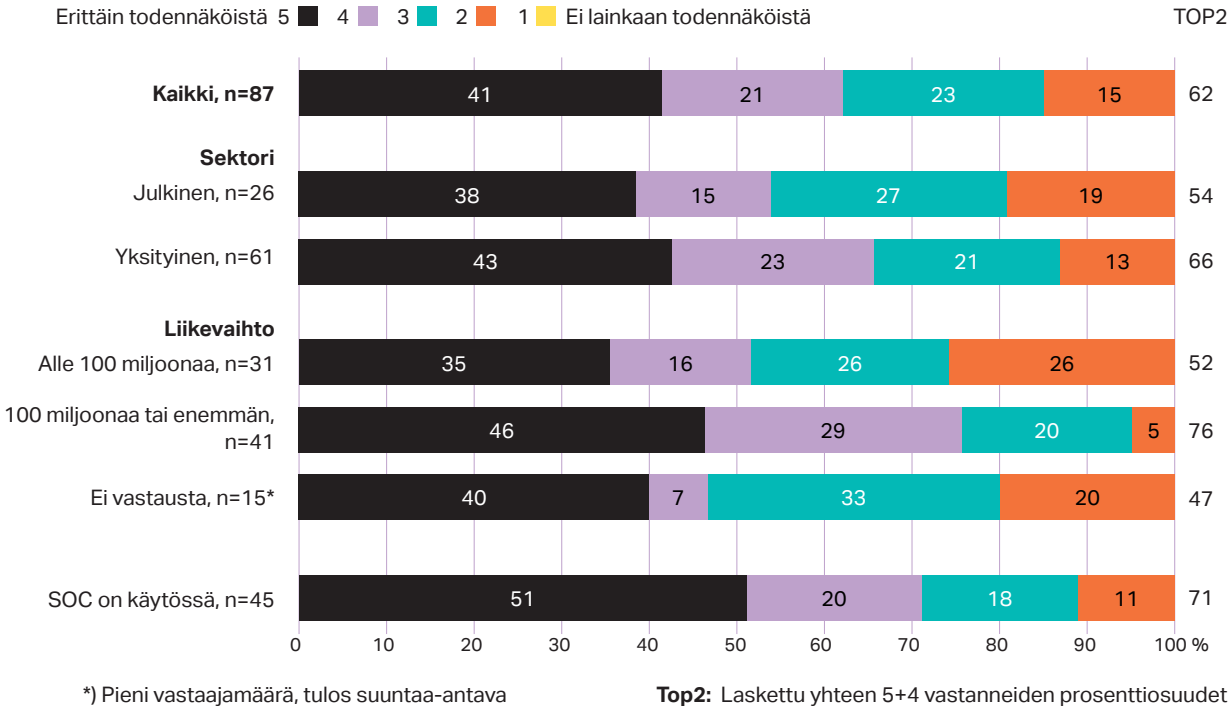




*) Pieni vastaajamäärä, tulos suuntaa-antava

Enemmistöllä tutkituista organisaatioista toimitila- ja tietoturvallisuus ovat erillisissä yksiköissä. Turvallisuutta hallitaan kokonaisuutena todennäköisimmin yksityisellä sektorilla ja suurissa vähintään 100 miljoonaa vuodessa vaihtavissa yrityksissä. Noin neljäsosa niistä organisaatioista, joilla toimitila- ja tietoturvallisuus on erillisenä yksikkönä harkitsee niiden yhdistämistä seuraavien kahden vuoden aikana.

Miten todennäköisenä pidät sitä, että yritykseesi tai organisaatioosi kohdistuu kyberhyökkäys seuraavan kahden vuoden aikana?

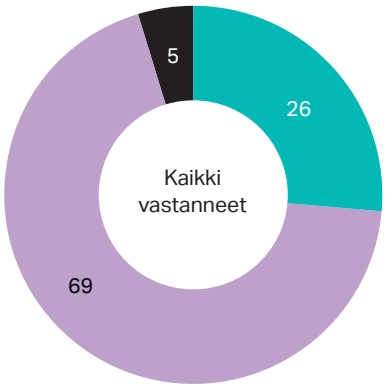


*) Pieni vastaajamäärä, tulos suuntaa-antava

Top2: Laskettu yhteen 5+4 vastanneiden prosenttiosuudet

Kokonaistasolla vastaajat pitävät hyvin todennäköisenä, että omaan organisaatioon kohdistuu kyberhyökkäys seuraavien kahden vuoden aikana. Hyökkäykset koetaan hyvin todennäköisiksi suurissa vähintään 100 miljoonaa vaihtavissa yrityksissä ja niissä organisaatioissa, joilla on SOC käytössä.

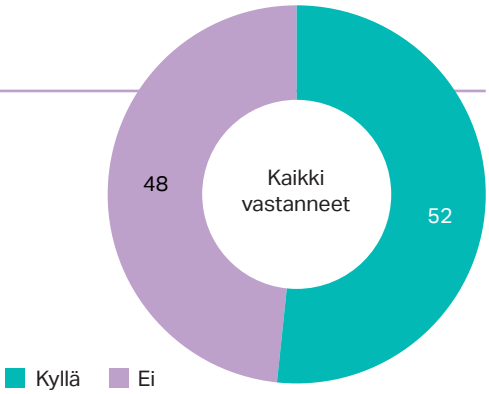
Onko yrityksessäsi tai organisaatiossasi tapahtunut liiketoimintaa haittaavaa tietoturvatapahtumaa viimeisten kahden vuoden aikana?



26 % vastaajista on kohdistunut liiketoimintaa haittaava tietoturvatapahtuma viimeisen kahden vuoden aikana. Yleisimmät haittaa aiheuttaneista tietoturvatapahtumista ovat olleet henkilörekistereihin liittyvät tietoturvahaastet (48 %) ja tietovuoto (35 %).

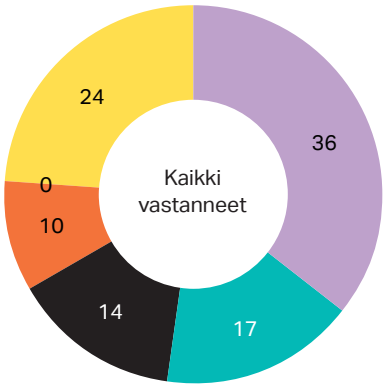
Kyllä Ei Ei halua vastata

Onko yrityksessäsi/ organisaatiossasi SOC (=Security Operation Center) käytössä?



SOC on käytössä hieman yli puolella tutkituista organisaatioista. SOC:in käyttö korostuu yksityisellä sektorilla ja suuremmissa yrityksissä. Pääsyy sille, että SOC:ia ei ole otettu käyttöön on se, että organisaation oma osaaminen on riittävällä tasolla.

Mikä seuraavista kuvaa parhaiten syytä sille, että yrityksessäsi/ organisaatiossasi ei ole SOC (=Security Operation Center) käytössä?



- Yrityksen oma osaaminen on riittävä
- Ei ole löydetty sopivaa kumppania
- Riittämätön budjetti
- SOC ei ole tarpeellinen
- Ulkoistuksen välttäminen
- Joku muu

Loihde Trust (loihdetrust.com) on kokonaisvaltainen yritysturvallisuuden kumppani, joka turvaa liiketoiminnan jatkuvuuden fyysisen ja digitaalisen maailman uhkia vastaan. Teemme tämän suojaamalla tiedon, ihmiset ja omaisuuden 22 toimipisteen ja lähes 500 ammattilaisen voimin kaikkialla Suomessa. Uskomme siihen, että turvallisuus ei saa olla rajoite, vaan käyttäjien arkea tukeva ja mahdollistava tekijä. Ymmärtämällä kokonaisuuden ja sen osien vaikutukset, voidaan luoda ympäristö, jossa turvallisuus on käytettävää ja liiketoiminta kehittyy. Tätä on Yksi turvallisuus®.

Loihde Trust on osa Loihde-konsernia. Loihde on liiketoiminnan jatkuvuuden mahdollistaja. Autamme asiakkaitamme luomaan kasvua ja kilpailukykyä digitalisaation avulla sekä suojautumaan fyysisen ja verkkomaailman uhilta.

Check Point Software Technologies Ltd. (www.checkpoint.com) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla.

Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.