TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kalastajatonttu

Loppuraportti

Tiivistelmä

- Kalastajatontussa kokeiltiin, millä tavoilla MS-ympäristöjen turvallisuutta voidaan parantaa helposti.
- Kokeilussa testattiin myös osallistujamäärän skaalausta.
- Tulokset olivat jälleen erittäin rohkaisevia:
  - Kokeiluun osallistui kolminkertainen määrä organisaatioita aiempaan verrattuna.
  - Osallistujat antoivat kokeilun helppoudesta ja hyödyllisyydestä loistavaa palautetta.
  - Kokeilun ansiosta kyselyyn vastanneista organisaatioista 43% korjasi kaksivaiheisen tunnistautumisen puutteita ja Internetille altistuneita ylimääräisiä palveluita.

Verkostot kasvavat ja kumppaneiden kypsyystaso nousee

Tonttu-kokeilut hyödyttävät sekä osallistujia, että Kyberturvallisuuskeskusta.

- *Yritykset* tunnistavat automaattisesti suojattavia kohteitaan ja vastaanottavat niille räätälöityjä tietoturvahavaintoja ja korjauksia.
- *Kyberturvallisuuskeskus* parantaa ymmärrystään suojattavista kohteista ja tuottaa ymmärryksen avulla kohdennettua tietoturvatietoa.

PASSIIVINEN YHTEISTYÖ

Otamme yhteyttä kun jotain on jo sattunut - jos tunnistamme teidät.

SATUNNAINEN YHTEISTYÖ

51 yhteistyöhön soveltuvaa kontaktia tavoitettu. Näistä **25** KTK:n verkostojen kautta, sekä **26** uutta kontaktia.

AUTOMATISOITU YHTEISTYÖ

71% kontaktoiduista tekee käytännön toimenpiteitä automatisoinnin mahdollistamiseksi, **54%** jakaa ajantasaiset tiedot pilvipalveluiden suojattavista kohteista Kyberturvallisuuskeskukselle ja **43%** osallistuu aktiivisesti kehittämiseen.

HAVARO 2

SOC-tilaus, järeät sensorit ja salaiset tunnisteet.

TRAFICOM

Kommentteja yhteistyöstä ja kokeiluista

- *Kokeilut ovat olleet erittäin hyviä. Konkreettisia tuloksia ja hyvä olla tällaisia työkaluja käytössä. Lisäksi helppo tapa pilotoida uusia teknologioita.*
- *Toivomme, että nämä eivät jäisi pelkäksi kokeiluksi, vaan niistä tulee myös jatkuvaa palvelua. Voimme jakaa tiedot melkein kaikista suojattavista kohteistamme Kyberturvallisuuskeskukselle.*
- *Yhteistyö tähän asti on toiminut hyvin. Nykyinen malli on hyvä.*
- *Kyberturvallisuuskeskus on hieno asia!*

Skaala ja vaikuttavuus löytyy perusasioista

- Kyberturvallisuutta voi parantaa helposti ja suuressa skaalassa, kunhan keskitytään kyberturvallisuuden perusasioihin.
- Perusasioihin myös kannattaa keskittyä - niistä löytyy korjattavaa ja korjaukset estävät myös hyökkäyksiä, joita emme osaa vielä ennakoida

Ajattele että yhteistyön toisella osapuolella on yhdeksän tehtävää hoidettavana tänään. Sinun asiasi on kymmenes. Miten varmistat, että asia hoituu?

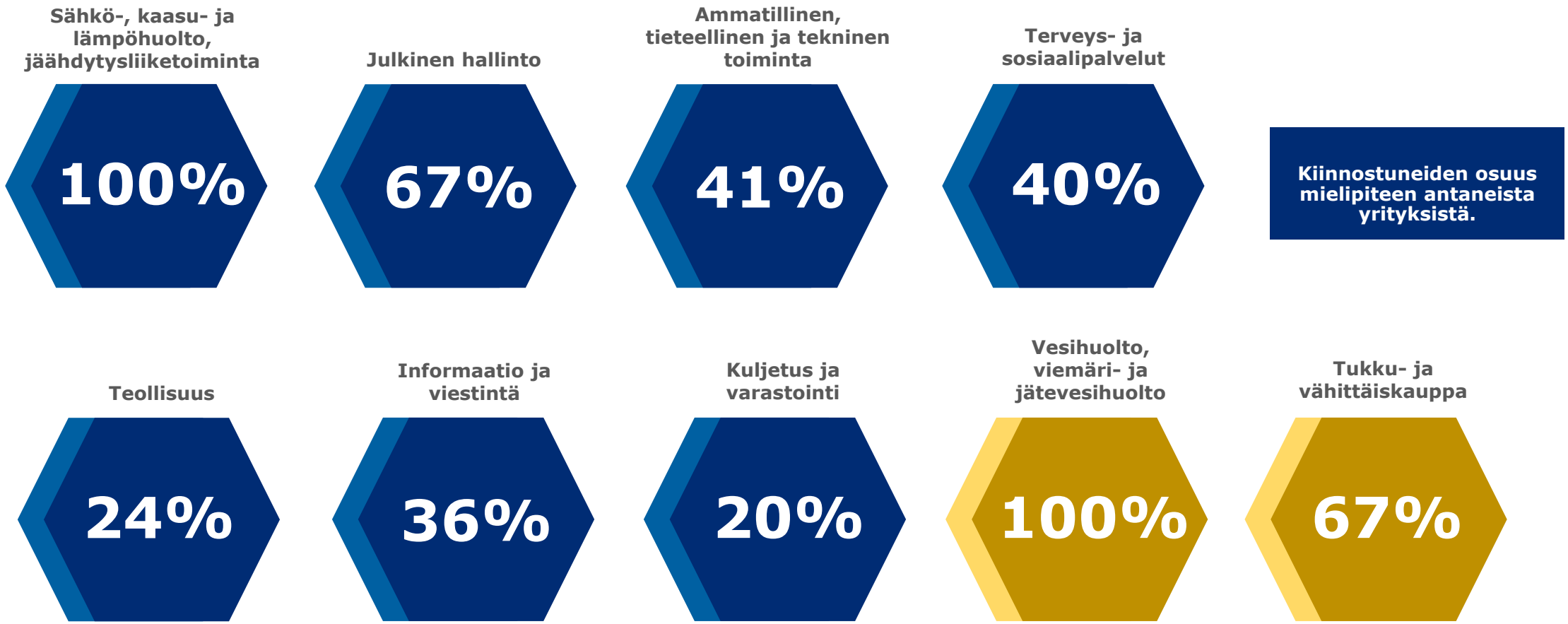
Skaalaus

Käytännön kokemukset osallistujamäärän kolminkertaistamisesta

Suorituksia monipuolisesti eri toimialoilta

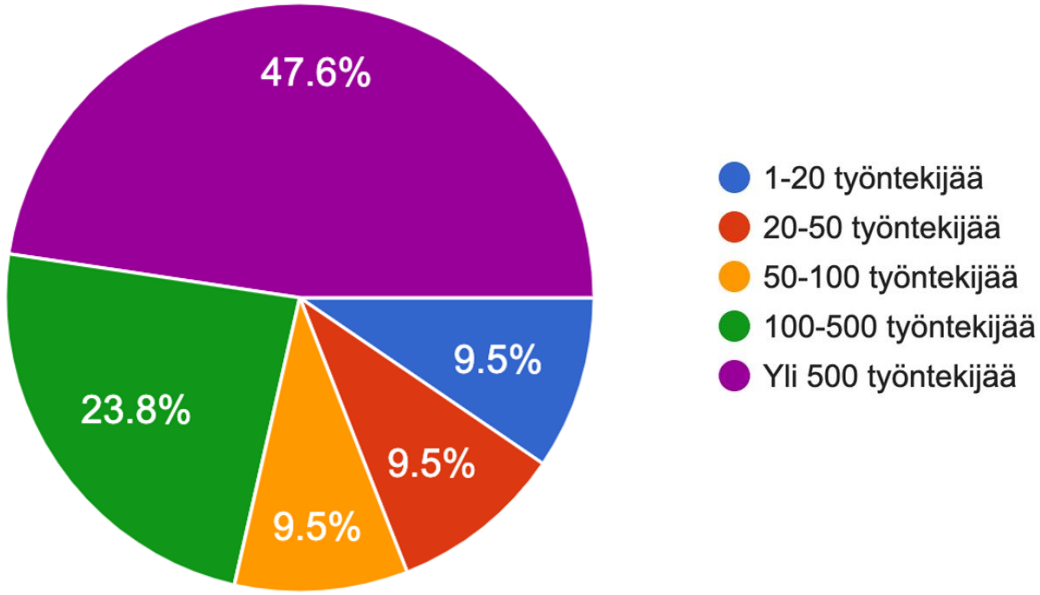
- Energiasektori on muita aktiivisempi.
- Aktiivisuuteen vaikuttaa kuitenkin monet tekijät, esimerkiksi yritysten koko.
- Merkittävä määrä suorituksia organisaatioista, jotka eivät kuulu nykyisiin sektoreihin.

Osallistumisesta kiinnostuneiden osuus vs TOL 2008 pääluokka



Kyselyyn vastanneista yli puolet oli alle 500 hengen yrityksiä

- Kokeiluun osallistui ilahduttava määrä myös pieniä organisaatioita.
- Yli neljäsosa palautekyselyyn vastanneista oli alle sadan hengen yrityksiä.
- Melkein neljäsosa oli 100-500 hengen yrityksiä.



TRAFICOM

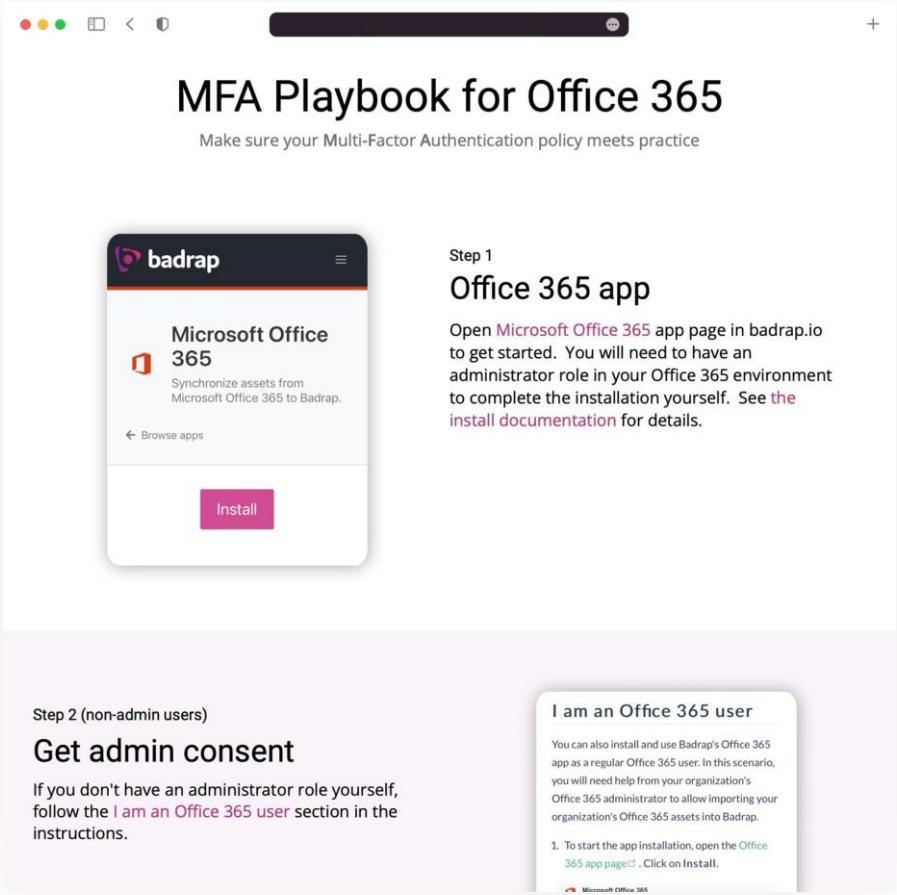
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Sisältö ja palaute

Osallistujista 21 antoi monipuolisesti palautetta kokeilun työkaluista ja pelikirjoista

Kokeilun sisältö

- Satunnaisen yhteistyön kypsyystaso:
  - Tiuku-skriptit MS-ympäristöjen auditoimiseksi
  - Webinaari: Sami Laihon ja Nestori Syynimaan vinkit MS-ympäristöjen turvaamiseksi
- Automatisoidun yhteistyön kypsyystaso:
  - Kaksi kyberturvallisuuden pelikirjaa badrap.io yhteistyö- ja itsepalvelualustan avulla:
  - MFA-tilanteen katselmointi
  - Joukkoistettu selkeytys Microsoftin MFA-avainlukujen tulkintaan
  - Osallistujalle räätälöidyn tietoturvatiedon hankkiminen KTK:n ja SensorFleet Oy:n tarjoamien sovellusten avulla.



Kokeilu edisti yhteistyötä eri kypsyystasoilla

1 SATUNNAINEN YHTEISTYÖ
Tiuku

Työkalut MS-ympäristöjen itsenäiseen auditointiin

43% vastaajista kokeili

- **24%** vastaajista koki työkalut melko tai todella hyödyllisiksi
- **5%** suhtautui neutraalisti
- **14%** ei kokenut työkaluja hyödyllisiksi

https://github.com/ncsc-fi/tiuku

2 AUTOMATISOITU YHTEISTYÖ
badrap.io

Tietoturvan ja yhteistyön itsepalvelualusta ja ohjaus

100% vastaajista kokeili

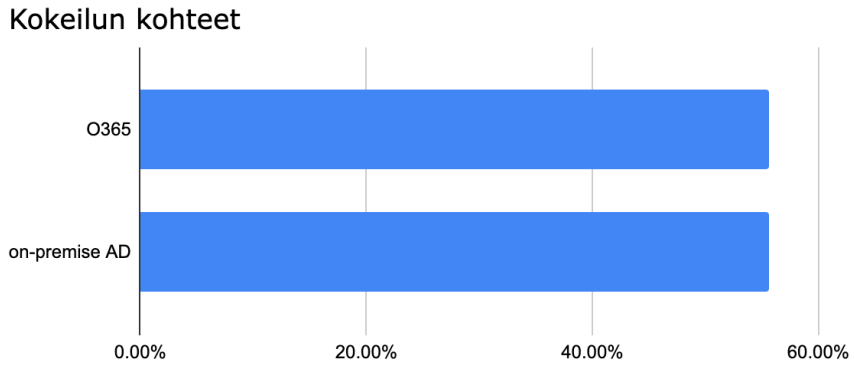
- **95%** kertoi, että ohjeiden mukaan toimiminen oli helppoa
- **5%** suhtautui neutraalisti
- **62%** korjasi suojattavia kohteitaan, esimerkiksi sulki KTK:n ilmoittamia avoimia palveluita tai ilmoitti käyttäjilleen kolmansien osapuolten tietovuodoista

https://badrap.io/

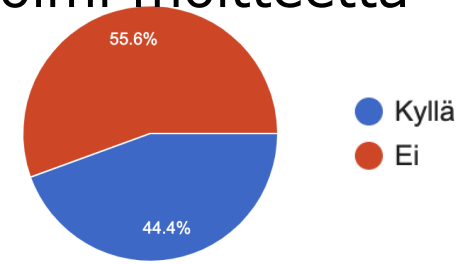
TRAFICOM

Satunnainen yhteistyö (Tiuku)

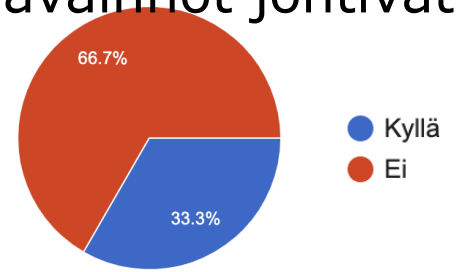
- Hieman alle puolet vastaajista kokeili KTK:n teettämiä avoimen lähdekoodin Powershell-työkaluja.
- Vastaajista viisi kokeili työkaluja O365-ympäristössään. Viisi kokeili työkaluja On-Premise AD –ympäristöissään.
- Hieman yli puolet vastaajista koki joitain työkaluihin liittyviä ongelmia tai virhetilanteita.
- Yli puolet koki myös työkalut erittäin hyödyllisiksi tai melko hyödyllisiksi.
- Kolmasosassa tapauksista työkalun tuottama tieto johti toimenpiteisiin.



Toimi moitteetta



Havainnot johtivat toimenpiteisiin



Automatisoidun yhteistyön aloitus

- Kaikki vastaajat kokeilivat badrap.io -yhteistyöalustaa
- Vastaajien mielestä kokeilun ohjaus oli selkeää ja ohjeiden mukaan toiminta oli helppoa
- Suurimmalle osalle vastaajista sähköpostiohjaus oli riittävä. Mutta moni toivoi että erikseen pyydettävä mahdollisuus henkilökohtaiseen ohjaukseen säilyisi myös jatkossa.

Vastaanottamani ohjeet olivat selkeitä

4.5/5

Ohjeiden mukaan toimiminen oli helppoa

4.4/5

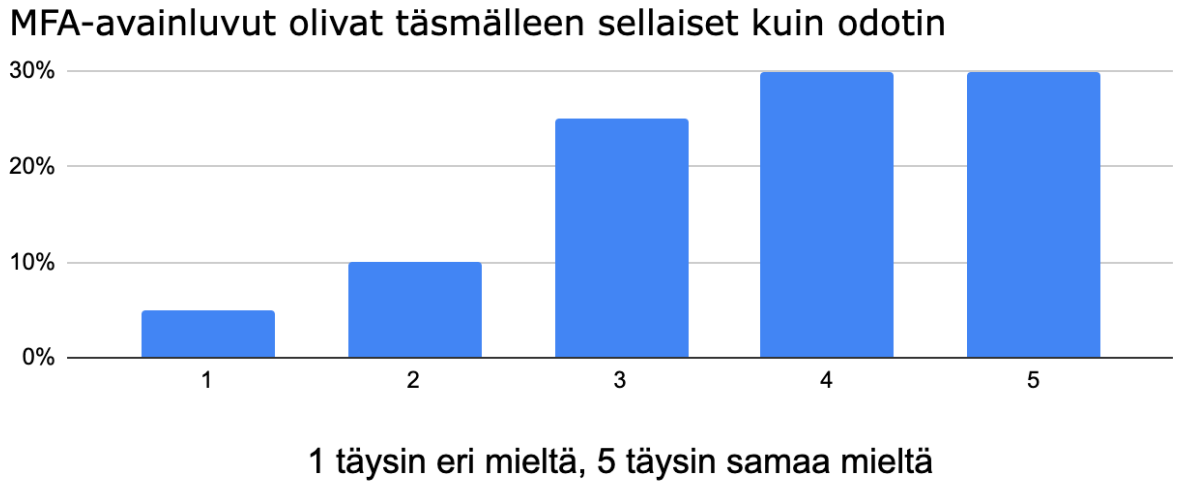
TRAFICOM

Kommentteja automatisoidusta yhteistyöstä

- *Kaikki mitä tehdään automaattisesti on parhautta.*
- *IT-infra on sen verran laaja, että aina tulee jotain yllätyksiä esille. Aika on tiukassa, automatiikka nopeuttaa asioita.*
- *Nykytilanteessa automatisointi ja havainnointikyvyn parantaminen on tärkeää. Käsin ei ehdi eikä aika riittäisikään.*
- *Kohdennettu tieto tärkeää - ylimääräinen tieto ja erikseen etsittävä ei.*
- *Tieto yksin ei auta, pitää pystyä prosessoimaan. Pitää saada paras hyöty siitä tiedosta mitä on jo saatavilla.*

MFA-pelikirja

- Monivaiheinen tunnistautuminen on toistaiseksi tehokas tapa estää kalastelu ja tilien haltuunotto.
- Osallistujat arvioivat kaksivaiheisen tunnistautumisen tilannetta badrap.io:n MFA-pelikirjan ja O365-integraation avulla.
- Vaikka vastaajista 70% koki MFA-tilanteensa hyväksi ennen kokeilua, 45% teki silti korjauksia havaintojensa perusteella.



Kommentteja MFA-pelikirjaan liittyen

- *Admin-tilien vajavainen MFA-peitto yllätti.*
- *Admin-tunnusten määrä aiheutti selvitystoimenpiteitä*
- *Oma hanke oli myös käynnissä, 90% havainnoista tiedettiin, mutta löytyi myös uusia havaintoja.*
- *Tiesimme lukemat ennestään, koska niihin liittyvää työtä on tehty ennenkin.*
- *Olemme tehneet jo paljon asiaan liittyvää työtä. Kokonaisuus on kuitenkin yllättävän haastava. MFA-video oli hyvä.*
- *[Microsoftin] MFA-luokitteluissa on epäjohdonmukaisuuksia, samaan kysymykseen saa eri vastauksen, riippuen siitä mistä portaalista asiaa katsoo. Selkeää vastausta kysymykseen "kuka pääsee ilman MFA:ta kirjautumaan" ei ole.*

Altistuneet verkkopalvelut -pelikirja

- Tämän pelikirjan suorittaneet aloittivat pilvipalveluiden suojattavien kohteiden reaaliaikaisen seurannan.
- Jakoivat automaattisesti tiedot suojattavista kohteistaan Kyberturvallisuuskeskukselle räätälöidyn tietoturvasisällön vastaanottamiseksi.
- Aloittivat ylimääräisten avointen palveluiden seurannan alustan SensorFleet-sovelluksella.
- Sulkivat ylimääräisiä hyökkäyksille alttiita verkkopalveluita KTK:n ja SensorFleet-sovelluksen varoitusten perusteella

ALTISTUNEITA VERKKOPALVELUITA

Kyberturvallisuuskeskus ja SensorFleet löysivät altistuneita verkkopalveluita 29%:lla vastaajista.

TEKI KORJAUSTOIMENPITEITÄ

100% varoituksen vastaanottaneista organisaatioista teki havaintojen perusteella korjaustoimenpiteitä.

Johtopäätökset

- **Kokeilun tulokset osoittavat, että turvallisuutta voi parantaa helposti ja suuressa mittakaavassa, kunhan keskitymme perusasioihin.**
- Perusasioihin keskittyminen kannattaa:
  - Perusasioiden korjaaminen on helpompaa
  - Tulosten perusteella korjattavaa on
  - Kunnossa olevat perusasiat suojaavat tuntemattomia ja tulevaisuuden uhkia vastaan

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus