

Kyseessä on x Lausuntopyyntö		☐ Tiedoksianto	Päiväys 2.8.2022
Tuen nimi Tietoturvan kehittämisen tuki			
Komission tukinumero (SA xxxx)		Tuen voimassaoloaika 1.10.2022-31.12.2024	
Tukiviranomainen Liikenne- ja viestintävirasto		EU-valtiontukisäännös tuki perustuu de minimis -asetus	
Lausunnon pyytävä ministeriö liikenne- ja viestintäministeriö		Yhteyshenkilön tiedot Mari Marttila, 0504732933, @gov.fi	

Kyseessä on x Uusi tukiohjelma	
☐ Tukiohjelman muuttaminen ☐ Tukiohjelman mukainen yksittäinen tukipäätös ☐ Tukiohjelman ulkopuolinen yksittäinen tukipäätös tai tukipäätöksen muuttaminen ☐ Tuen voimassaoloajan jatkaminen	

Lain 3–5 §:ien edellytykset	
Lausuntoa pyytävä viranomainen täyttää. (Huom. Kenttään kirjoitettavan tekstin pituutta ei ole rajattu.) Tämän liitesivuilla on esitetty ohjaavia kysymyksiä helpottamaan kunkin kuvauksen kirjoittamista.	YRITYSTUKINEUVOTTELUKUNNAN LAUSUNTO 31.8.2022 Esittelijä: Anne Rothovius

1. Selkeä taloudellinen tai yhteiskunnallinen tavoite, joka perustuu hallitusohjelmaan tai politiikatavoitteeseen	☒ x  ☐  ☐ 
Kybertoimintaympäristö on muuttunut merkittävästi turvallisuusympäristön ja koronapandemian myötä. Koronapandemian seurauksena koko digitaalinen toimintaympäristö ajautui murrokseen uusien teknologioiden käytön ja teknologisen kehityksen vuoksi. Venäjän hyökkäyssota Ukrainaan on lisännyt kyberhyökkäyksiä maailmalla, ja hyökkäyksiä on suunnattu niin valtio- ja kuntatason toimijoita kuin elinkeinoelämää kohtaan myös Suomessa. Tietoturvan kehittämisen tuen avulla yrityksillä ja yhdistyksillä olisi mahdollisuus nopeasti nostaa kyberturvallisuuden tasoa organisaatioissa ja tehdä kohdennettuja kyberturvallisuutta parantavia toimenpiteitä. Kyberturvallisuuden tason nostaminen organisaatioissa näkyy vastaavasti muun muassa parempana tietosuojana kansalaisille. Tietoturvan kehittämistuella myös vauhditettaisiin suomalaisen kyberturvallisuustoimialan ja -markkinan kehitystä sekä luodaan uutta liiketoimintaa toimialle ja kyberturvallisuusosaamista Suomeen parantaen muun muassa Suomen kyberturvallisuuden omavaraisuutta.	Tuen päätavoite on yhteiskunnallinen: Tavoitteena on lisätä yhteiskunnan ja kansalaisten turvallisuutta sekä huoltovarmuutta nopeasti muuttuneessa turvallisuusympäristössä. Tuki edistää taloudellisia tavoitteita luoden uutta suomalaista liiketoimintaa toimialalle ja kehittää toimialan markkinaa. Tuen myötä taloudellisen toiminnan edellytykset vahvistuvat osaamisen vahvistuessa, mistä seuraa myös positiivisia ulkoisvaikutuksia. Tuelle tulisi määritellä tulosindikaattorit valmisteluvaiheessa erikseen asetussuunnitelman 3 §:n 1 momentin 1 ja 2 kohdista, jotta varmistetaan datan keruu yrityksistä myöhempää seurantaan ja arviointia varten.
2. Markkinapuutteen korjaaminen ja ulkoisvaikutukset	☒ x  ☐  ☐ 
Suomalaisen yhteiskunnan kyberturvallisuus mukaan lukien kyky suojautua hybridiuhkilta on suurelta osin riippuvainen yhteiskunnan eri sektoreilla toimivien organisaatioiden kyvystä havainnoida, ennalta ehkäistä, estää ja rajoittaa kyberturvallisuusloukkauksia sekä toipua niistä kuin myös suojata eri järjestelmiin ja palveluihin tallennettua tietoa. Muuttuneen turvallisuusympäristön kehityksen myötä on entistä keskeisempää kiinnittää huomioita laaja-alaisesti yhteiskunnan kyberturvallisuuteen ja varmistaa kyberturvallisuuden korkea taso yhteiskunnan kaikilla sektoreilla siten, että eri sektoreilla toimivat organisaatiot ovat varautuneet kyberturvallisuushyökkäyksiin ja -loukkauksiin. Etenkin pienten ja keskisuurten yritysten sekä yhdistysten osalta on havaittu tarve parantaa niiden varautumista kyberturvallisuushyökkäyksiin ja -loukkauksiin ja kehittää niiden toimintaa, tietojärjestelmiä, sähköisiä palveluja kuin myös	Tuen markkinapuutteena on negatiivisten ulkoisvaikutusten ehkäiseminen koskien turvallisuutta ja huoltovarmuutta. Markkinat eivät kykene hinnoittelemaan yhteiskunnalle syntyvää negatiivista ulkoisvaikutusta. Negatiivinen ulkoisvaikutus on taloudellisesta toimimattomuudesta seuraava haitallinen vaikutus kansantalouteen / yhteiskuntaan, joka jäisi muutoin ottamatta huomioon. Yrityksillä ei välttämättä ole riittäviä kannusteita ylläpitää kyberturvallisuutta, koska yritysten kyberturvallisuuden ylläpidon hyödyt koituvat koko yhteiskunnalle ja kansalaisille

kyberturvallisuusosaamista. Myös suurten yritysten varautumisessa kyberturvallisuushkiin ja -loukkauksiin on edelleen parannettavaa. Kyberturvallisuuden ylläpito ja kehittäminen vaativat jatkuvaa työtä. Suomessa kriittinen infrastruktuuri on valtaosin yritysten hallussa, joten yritysten rooli ja toimet ovat Suomen kyberympäristön turvaamisessa avainasemassa. Yhteiskunnan toiminnan kannalta kriittisten alojen yrityksen ja yhdistyksen tietoturvan kehittäminen parantaa myös huoltovarmuutta ja vahvistaa resilienssiä.	turvallisuuden paranemisena kyberuhkien varalta eikä se välttämättä näy suoraan tuloksessa. Kyberturvallisuuteen varautuminen on osa yrityksen yhteiskuntavastuuta, josta yritys vastaa asiakkaille, omistajille ja sidosryhmille. Tuella voidaan luoda edellytyksiä uusille tai nykyistä monipuolisemmille markkinoille, jolla aikaansaadaan uudenlaista kysyntää. Tähän liittyen tulee seurata milloin markkinoilta tulisi poistua eli milloin markkinamekanismi alkaa toimia ilman julkista tukea. On huomioitava, että yritykset noudattavat normaali- ja kriisiaikana tietoturvallisuudesta annettuja säädöksiä, mutta kyberturvallisuus korostuu erityisesti turvallisuustilanteen heikentyessä. Tukea puoltaa kyberturvallisuuden parantamisen nopeuttaminen.
3. Tarkoituksenmukainen keino tavoitteen saavuttamiseksi Tietoturvasetelin käyttöönotto vahvistaisi konkreettisesti kansalaisten tietosuojaa ja parantaisi pienten, keskisuurten ja myös suurten toimijoiden sekä järjestöjen tietoturvaa oikeasuhtaisella tavalla. Yleisen kybervarautumistason nostaminen eniten tukea tarvitsevilla sektoreilla parantaisi yhteiskunnan kykyä suojautua muun muassa hybridiuhkilta. Investoinnilla olisi välittömiä, positiivisia vaikutuksia myös kyberturvallisuusalan tuotteiden ja palveluiden kehittämiseen.	☐ ☒ ☐ x ☐ ☒ ☐ ☒ Kuvauksesta ei käy ilmi miksi on valittu juuri tuki politiikkatoimeksi muiden politiikkakeinojen sijaan (sääntely, palvelu tai muu ohjauskeino). Kuvauksesta ei käy esimerkiksi ilmi mikä on tietoturvalainsäädännön rooli politiikkatoimena. Koska yritysten tietoturvaratkaisut yleisesti yrityksissä ovat ostopalveluita tai oman henkilöstön osaamisen parantamista esim. koulutuksella, palveluseteli mahdollistaa yritykselle pienempien ostopalveluiden hankinnan.
4. Kustannustehokkuus ja hallinnollinen rasitus tuen saajalle Tukea haettaisiin Liikenne- ja viestintävirastolta, jolla on kokemusta erilaisten tukien myöntämisestä. Liikenne- ja viestintävirasto myöntäisi tuen ensi sijassa hakemuksessa ilmoitettujen tietojen perusteella. Hakijan olisi esitettävä hakemuksessaan tuen myöntämiseksi ja maksamiseksi välttämättömät tiedot sekä yksilöity suunnitelma tai kuvaus tietoturvan kehittämisen hankkeesta sekä ilmoitettava tämän haettavan tuen määrä. Taloudellista toimintaa harjoittavan hakijan olisi lisäksi tukea koskevassa hakemuksessa annettava riittävä selvitys saamastaan muusta julkisesta tuesta tai avustuksesta. Tuen hakijan tulisi toimittaa selvitys tukiviranomaiselle sen saamista muista de minimis –tuista tukihakemuksen yhteydessä, jotta tukiviranomainen eli Liikenne- ja viestintävirasto pystyisi varmista-maan, ettei kiellettyä tukikumulaatiota tapahtuisi. Tuensaajan tulee toimittaa Liikenne- ja viestintävirastolle selvitys avustuksen tuen käytöstä ja vaikutuksista toimijan tietoturvaan viimeistään kuuden kuukauden kuluttua tuella katettujen kustannusten syntymisestä. Esityksestä aiheutuisi Liikenne- ja viestintävirastolle uusia resursoitavia tehtäviä 3-3,5 htv:tä sekä tietojärjestelmämuutosten kuluja noin 400 000 euroa.	☐ ☒ ☐ x ☐ ☒ ☐ ☒ Liikenne- ja viestintävirastolla on vakiintuneet prosessit tuen sähköiseen myöntämiseen. Tukisäännöt ovat kaavamaisia tuen määrän osalta, mikä vähentää hallinnollista rasitusta. Palveluseteli on kustannustehokas tukiväline, jos tuen saajia on paljon ja tukisummat ovat pieniä. Huomiota kiinnitetään kuitenkin siihen, että hallinnolliset kustannukset ovat melko suuret noin 11 % (tukiohjelman suuruus 6 M€ 1.10.2022 – 31.12.2024 ja kustannukset ovat arviolta 0,7 M€). Tukisääntöjen, tuen myöntämisen ja avustuksen käytöstä raportoinnin tulisi siksi olla mahdollisimman kaavamaisia ja tietojärjestelmän tukemia. Väärinkäytöksiä voidaan ennaltaehkäistä tuomalla hakuohjeissa esille esimerkiksi otantaan perustuvat jälkitarkastukset. Tuen valmisteluvaiheessa olisi hyvä benchmarkata tukimenettelyt ja säännöt Business Finlandin innovaatioasetelin

	kanssa, jossa hallinnollinen rasitus on minimoitu. Saaajan selvitys tuen käytöstä ja vaikutuksista (mm. lkm tiedot, kohdentuminen, vaikutukset, johtiko jatkohankkeeseen) voisi myös olla teknisesti tuettu hallinnollisen rasituksen minimoimiseksi ja vaikuttavuuden arvioinnin tukemiseksi.
5. Vaikutukset kilpailuun Tuki kanavoidaan toimijoiden tietoturvallisuuden kehittämiseen. Koska tietoturvariskien voidaan katsoa kuuluvan tavanomaisiin yritystoiminnan riskeihin, esitetty julkinen tuki voi antaa tuen saajalle edun, joka saattaa vääristää kilpailua. Tukea voitaisiin myöntää niin kauan kuin tuen maksamista varten osoitettu määräraha riittää. Sen vuoksi on erityisen tärkeää, että asetuksen tultua voimaan kyseessä olevasta tukimahdollisuudesta tiedotetaan kattavasti, jotta kohderyhmään kuuluvilla yrityksillä ja yhdistyksillä olisi yhdenvertaiset mahdollisuudet hakea tukea.	☒ x ● ☐ ● ☐ ● Tuella voi olla välillisiä vaikutuksia kansainväliseen kilpailukykyyn, kun suomalaisten yritysten toimintaedellytykset kyberturvallisuuden osalta paranevat. Kuvauksesta ei ilmene kilpailuvaikutukset kyberturvallisuustoimialan yrityksissä. Tuen saaja käyttää palvelusetelin valitsemaansa yritykseen, joten kyberturvallisuusyritysten valinta tapahtuu markkinoilla eikä kilpailu siten paikallisesti tai alueellisesti vääristy tuen johdosta.
6. Määräaikaisuus Tuki perustuu kesän 2022 lisätalousarviossa myönnettyyn 6 miljoonan euron määrärahaan, joten se on määräaikainen. Tukea voidaan maksaa viimeistään 31.12.2024 syntyneihin kustannuksiin.	☒ x ● ☐ ● ☐ ● Tuki on määräaikainen.
7. Kannustava vaikutus Tietoturvan kehittämisen tukea myönnettäisiin vain kustannuksiin, jotka syntyvät myöntöpäätöksen jälkeen Tuen on tarkoitus olla toimijakohtainen käynnistys tietoturvan kehittämiseksi. Helmikuussa 2022 toteutetun Yrittäjägallup – tietoturvatutkimuksen perusteella on epätodennäköistä, että pk-yrityksillä olisi mahdollisuuksia ylläpitää omaa, yrityksen sisäistä tietoturvaosaamista. Saman tutkimuksen mukaan, tietoturvallisuuden kustannusten arvioidaan olevan toiseksi merkittävin este tarvittavien toimenpiteiden toteuttamiselle. Yhdistettynä osaamisen puutteisiin yritykset kaipaavat apua erityisesti hankintaosaamiseen ja konsultointiin, jotta hankinnat olisivat tarkoituksenmukaisia. Määräaikaisen tietoturvasetelin avulla organisaatiot voisivat hankkia tarkastuksen ja arvion uhkamallinnuksesta järjestelmiensä tietoturvasasta markkinaehtoisilta toimijoilta sekä ryhtyä tulosten perusteella parantamaan järjestelmiensä tietoturvaa ja tietoturvaosaamistaan määrätietoisesti.	☒ x ● ☐ ● ☐ ● Kuvauksesta poiketen asetusluonnoksen 2 §:ssä todetaan, että tukea voidaan myöntää vain kustannuksiin, jotka syntyvät tukihakemuksen jättämisen jälkeen. Kannustava vaikutus toteutuu silloin kun tuettava hanke tai toiminta aloitetaan vasta tukipäätöksen jälkeen. Tehokas tuki luo riittävän kannusteen sen kohteena oleville yrityksille muuttua toimintaansa tuen perimmäisten tavoitteiden suuntaisesti. Kuvauksen mukaan palvelusetelin arvioidaan toimivan useimmiten alkusysäyksenä varsinaiselle hankinnalle, mutta sitä voidaan käyttää myös oman osaamisen lisäämiseen. Tavoitteena lieene nopeuttaa toimintaa kyberturvallisuuden parantamiseksi. Tuelle esitetty tuki-intensiteetti oli erittäin korkea, 70 % 3 § 1 mom. 2 kohdassa. Julkisen rahoituksen osuus yrityksen kokonaisrahoituksesta ei saa nousta kohtuuttoman korkeaksi, vaikka hankkeeseen sinänsä voitaisiin myöntää tukea EU valtiontukisääntöjen mukaan. Korkeaa tuki-intensiteettiä puoltaa tuen yhteiskunnallinen tavoite ja negatiivisten ulkoisvaikutusten ehkäiseminen nopeammassa aikataulussa. Tuki voi myös nopeuttaa tietoturvallisuuden parantamista, jos yritys

	on jo tehnyt testauksen mutta välitön toimi on jäänyt tekemättä. Toisaalta voidaan pohtia tuen kannustavaa vaikutusta eli tekisikö yritys toimenpiteen joka tapauksessa, jos on jo tehnyt testauksen.
8. Vaikuttavuus Tuensaajan tulee toimittaa Liikenne- ja viestintävirastolle selvitys avustuksen tuen käytöstä ja vaikutuksista toimijan tietoturvaan viimeistään kuuden kuukauden kuluttua tuella katettujen kustannusten syntymisestä. Näiden selvitysten perusteella tukiviranomainen voi tehdä analyysia esimerkiksi siitä, millaisiin toimiin tuki tarkalleen on kohdentunut ja millaisia vaikutuksia sillä arvioidaan olevan.	☐ ☒ ☐ ☐ ☒ ☐ ☐ ☐ ☒ ☐ ☐ ☐ ☒ Tuen vaikuttavuutta tulee arvioida ulkopuolisen tahon toimesta ja laatia arviointisuunnitelma valmisteluvaiheessa. Vaikuttavuuden arvioinnissa tulisi kiinnittää huomiota siihen, onko palveluseteli johtanut myöhemmin varsinaiseen kehittämistyöhön ja onko tämä seurausta juuri palvelusetelin käytöstä. Koska tuen saajia on paljon ja tukisummat pieniä, tukiohjelma soveltuisi hyvin satunnaistamiskokeeksi. Tuen vaikuttavuutta voitaisiin arvioida verrokkiryhmään perustuvalla menetelmällä (ovatko yritykset parantaneet kyberturvallisuutta myös ilman tukea). Tuen vaikutusta yrityksen käyttäytymiseen tulisi tutkia jälkikäteen.
9. Yksittäiset tukipäätökset Liikenne- ja viestintävirasto voisi myöntää tukea hakijalle, jos asetuksessa säädetyt edellytykset täyttyvät. Tuen myöntäminen ei olisi harkinnanvaraista, vaan Liikenne- ja viestintävirasto myöntäisi tuen, jos edellä mainitut edellytykset täyttyisivät ja tukeen varattua määrärahaa olisi edelleen jäljellä niin, että tuki voitaisiin myöntää. Hakemusten käsittelyssä pyritäisiin näin mahdollisimman pieniin hallinnollisiin kuluihin. Liikenne- ja viestintävirasto maksaisi tietoturvan kehittämisen tukea tuensaajalle myönteisen tukipäätöksen perusteella.	
9 a Tukikumulaatio Tuen hakijaa pyydetään hakemuksen yhteydessä ilmoittamaan, onko se saanut de minimis -tukea verovuonna ja kahtena edellisessä verovuotena. Lisäksi tukipäätöksessä mainitaan, että myönnetty tuki on de minimis –tukea.	☒ ☒ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Julkisen rahoituksen osuus yrityksen kokonaisrahoituksesta ei saa nousta kohtuuttoman korkeaksi, vaikka hankkeeseen sinänsä voitaisiin myöntää tukea EU valtiontukisääntöjen mukaan. Tuen myöntämistä ja maksamista koskevat tiedot tulee tallettaa yritystukirekisteriin (799/2021, 7a§).
9 b Vaikutukset kilpailuun paikallisesti Suomessa ja EU-alueella Tuki kanavoidaan toimijoiden tietoturvallisuuden kehittämiseen. Koska tietoturvariskien voidaan katsoa kuuluvan tavanomaisiin yritystoiminnan riskeihin, esitetty julkinen tuki voi antaa tuen saajalle edun, joka saattaa vääristää kilpailua.	☒ ☒ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Ks. edellä.
9 c Edellytykset kannattavaan toimintaan, arviointi Hakijan tulee hakemuksessaan vakuuttaa, että se täyttää tuensaajan kriteerit.	☐ ☒ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☒ ☐ Kuvaukseen ja asetusluonnokseen ei sisälly kannattavan toiminnan edellytysten arviointia. Tukea ei saa myöntää vaikeuksissa olevalle yritykselle. Yrityksen julkiset maksut tulee olla maksettu ja verovelosta tulee esittää Verohallinnon hyväksymä maksusuunnitelma. Lisäksi voidaan ottaa huomioon yrityksen luottokelpoisuus ja maksuviiveet. Näiden tulisi olla edellytyksenä tuen myöntämiselle.