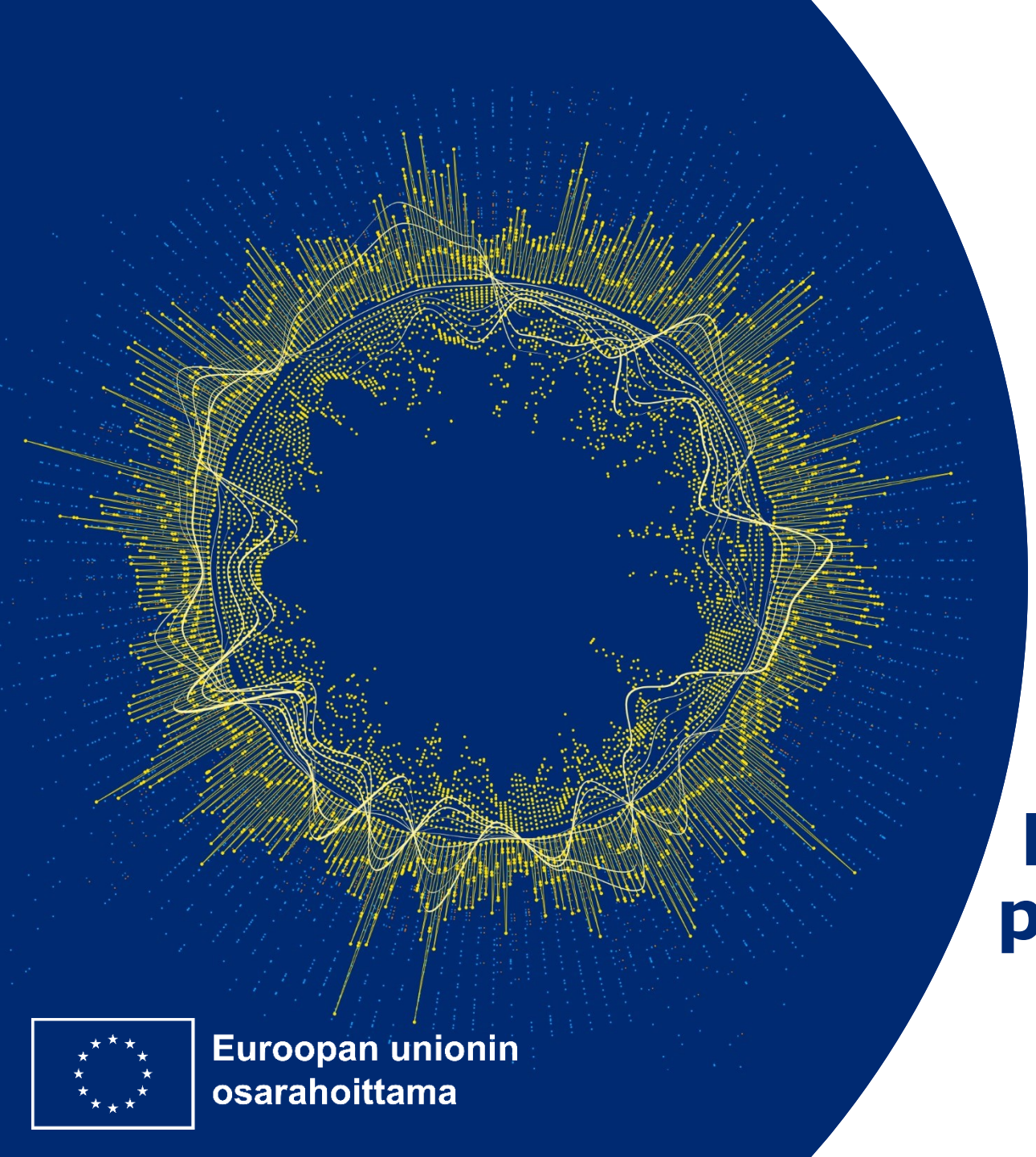


Euroopan unionin osarahoittama

TRAFICOM
Liikenne- ja viestintävirasto

NCC-FI
KYBERTURVALLISUUDEN KANSALLINEN KOORDINOINTIKESKUS

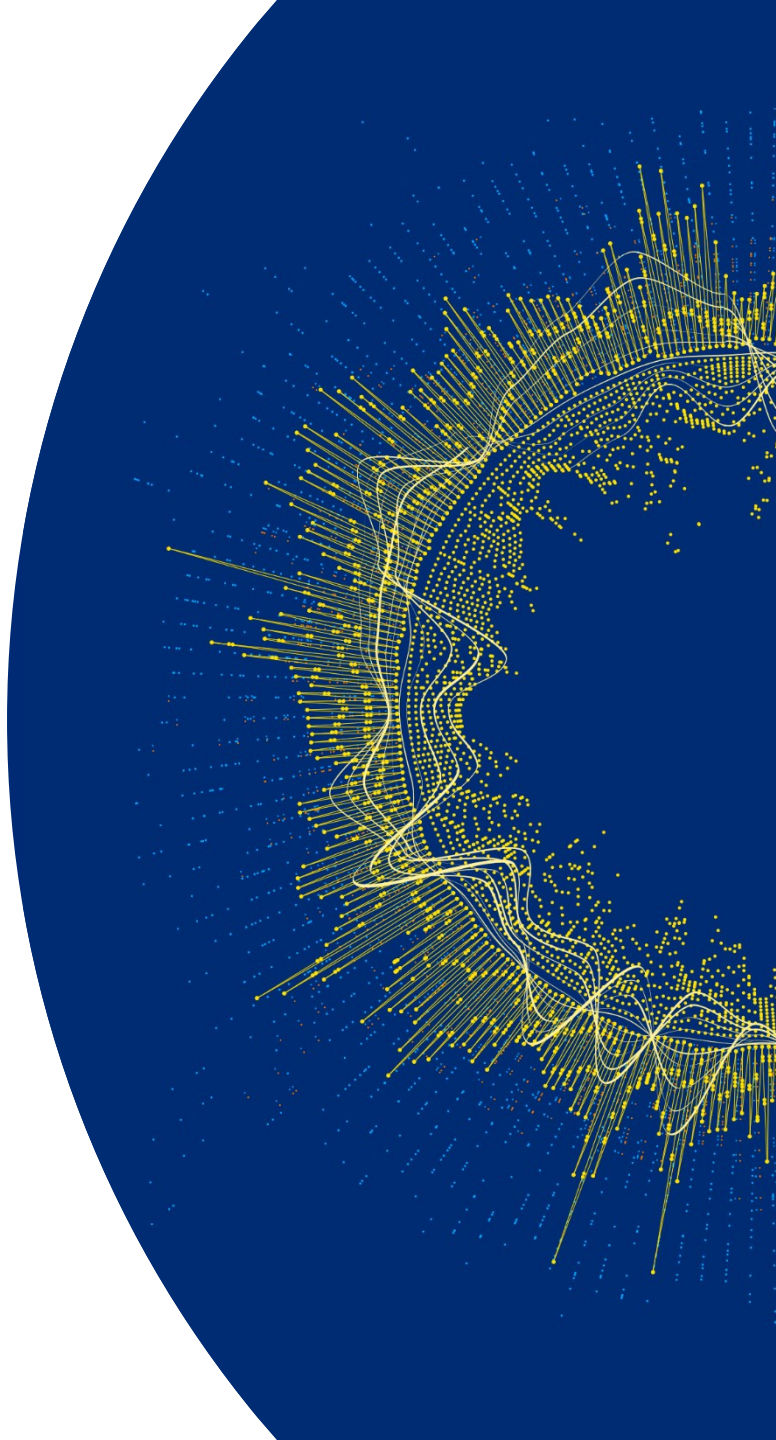
Kansallisen koordinointikeskuksen palvelut ja rahoitustuki

24.9.2025

Annalotta Saarikoski

Esityksen sisältö

- Kansallinen koordinointikeskus ja sen palvelut
- Rahoitustuki kyberturvallisuuslain (124/2025) toimeenpanemisen tukemiseksi



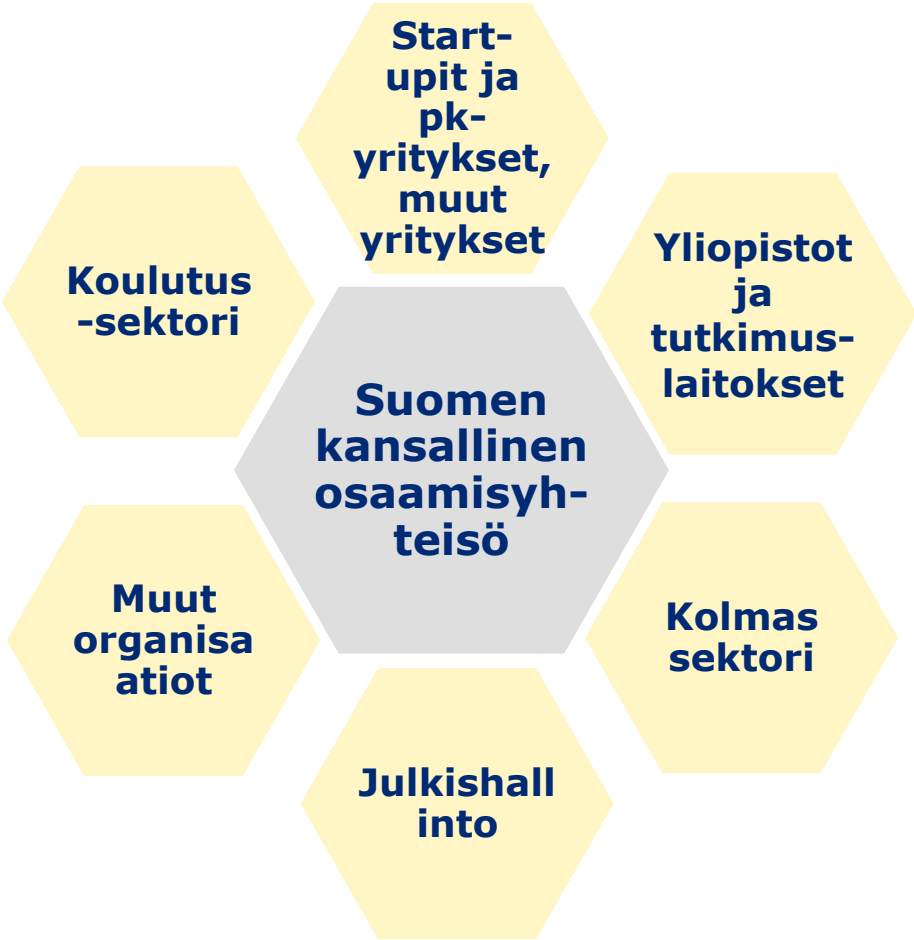
Kansallinen koordinointikeskus (NCC-FI)

Euroopan parlamentin ja neuvoston asetus (EU) 2021/887 Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta

- Koordinointikeskus sijaitsee Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksessa (KTK)
- Suomen kansallisen koordinointikeskuksen päämääränä on kasvattaa Suomen ja EU:n kyvykkyyksiä, kilpailukykyä ja strategista itsenäisyyttä kyberturvallisuuden alalla
- Käytännössä keskitymme tukemaan kansallisesti kyberturvallisuuskapasiteetin kasvattamista sekä kyberturvallisuuden tutkimusta, kehitystä ja innovointia

Koordinointikeskuksen keskeisimmät tehtävät

1. Tuetaan ja edistetään kansallisten toimijoiden osallistumista rajat ylittäviin EU-hankkeisiin ja muuhun yhteistyöhön
2. Kootaan ja kehitetään kansallista kyberturvallisuuden osaamisyhteisöä
3. Myönnetään rahoitustukea pk-yrityksille



Miten tuemme kyberturvallisuusalan EU-rahoituksen hakemisessa?

- Tiedotus avautuvista rahoitushauista ja tilaisuuksista Traficomin/KTK:n kanavissa
- Ohjeistus relevanttien kyberturvallisuusalan rahoitusmahdollisuuksien löytämiseen
- Tuki hallinnollisiin prosesseihin ja sopimusasioihin
- Koulutus ja tuki rahoitushakemusten valmisteluun
- Dokumenttien kuten lomakkeiden ja ohjeiden jakaminen
- Tuki partnereiden etsimiseen ja verkostoitumiseen
- Alustat kokemusten jakamiselle esim. hyvän hakemuksen valmistelusta ja hankekoordinaattorina toimimisesta

Kaikille toimijoille soveltuvat DEP-kyberrahoitushaut 2025

Dedicated action to reinforcing hospitals and healthcare providers (Sulkeutuu 7.10.2025)

- **support pilot projects**, which will bring together stakeholders such as regional and/or national clusters associations of hospitals and healthcare providers as well as cybersecurity service providers.

Transition to post-quantum Public Key Infrastructures (Sulkeutuu 7.10.2025)

- **design of digital signature combiners and key encapsulation mechanism combiners**
- **testing of deployment of certificates** in protocols that use those certificates
- the **development of novel protocols** for Automatic Certificate Management and revocation and of novel protocols for certificate-transparency
- the development of methods and tools that can be used by experts across various PKI domains, including **all aspects of key management of asymmetric systems**.

Deployment of a European testing infrastructure for the transition to PQC (Avautuu Q4/2025)

- **creating and maintaining a European PQC testing infrastructure**.
- The testing infrastructure should offer a **physical space for in-situ testing**. This **includes the possibility for providing remote testing** for different European stakeholders.
- **Proposals should build on results from ongoing activities in the EU.**

Cybersecure tools, technologies and services relying on AI (Avautuu Q4/2025)

- develop and deploy systems and tools for cybersecurity , **based on AI technologies** , addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing.

Uptake of innovative cybersecurity solutions for SMEs (Avautuu Q4/2025)

- improving industrial and market readiness for the **cybersecurity requirements set in the Cyber Resilience Act** bolstering cybersecurity rules to **ensure more secure hardware and software products**

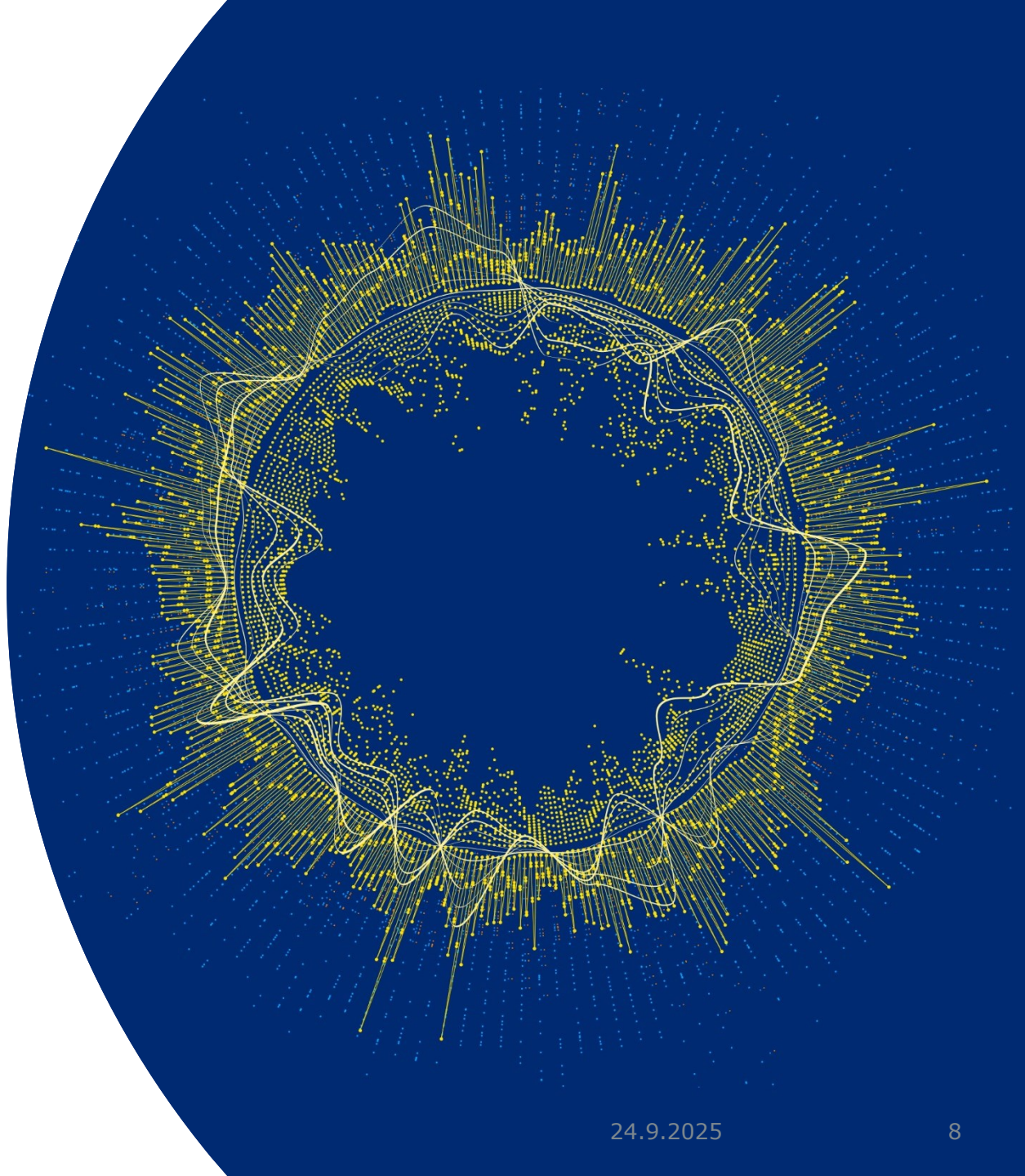
Horizon Europe CL 3 Cyber Rahoitushaut 2025

Alla olevat haut auki 12.6.-12.11.2025 EU Funding & Tenders portaalissa

Aihe	Kuvaus	Rahoitus
Generative AI for Cybersecurity Applications **(RIA)**	develop **technologies, tools, processes that reinforce cybersecurity using AI technological components**, in particular Generative AI, [...]. Proposals should address **at least one** of the following expected outcomes: a. Developing, training and testing of Generative AI models for monitoring, detection, response and self-healing capabilities in digital processes, and systems against cyberattacks, including adversarial AI attacks. b. Development of Generative AI tools and technologies for continuous monitoring, compliance and automated remediation. These should consider legal aspects of EU and national regulation as well as ethical and privacy aspects	40 M€ (14 M€ kpl)
New advanced tools and processes for Operational Cybersecurity **(IA)**	[...] **automated management of vulnerabilities** based on established standards like the Common Security Advisory Framework. [...] **increase the exchange of information** and improve our collective capabilities in order to **reduce drastically the time needed to detect cyber threats and mitigate**, before they can cause large-scale damage and costs. [...]**development of advanced frameworks, services tools, and processes**, in line with relevant EU legislation (NIS2, Cyber Resilience Act, Cyber Solidarity Act)	23,55 M€ (6 M€ kpl)
Privacy Enhancing Technologies **(RIA)**	**Protecting individuals' personal data** and **ensuring privacy** while **allowing for data processing and analysis**[...]. Privacy-enhancing technologies such as cryptographic anonymous credentials, differential privacy, secure multiparty computation, homomorphic encryption, advanced digital signatures, such as ring signatures, blind signatures and attribute-based credentials[...].	11 M€ (4M€ kpl)
Security evaluations of Post-Quantum Cryptography (PQC) primitives **(RIA)**	**Breakthroughs** in understanding the quantum hardness of various mathematical problem classes that underpin the security of current and future post-quantum cryptosystems; **New quantum algorithms, Improved implementation** of quantum algorithms, **testing the robustness** of cryptosystems, **AI-based approaches**, etc. [...] create a robust set of cryptographic building blocks for postquantum cybersecurity and design of post-quantum cryptosystems with improved security against quantum or AI-based attacks.	4 M€ (3 M€ kpl)
Security of implementations of Post-Quantum Cryptography algorithms **(RIA)**	Design and implementations of **Post-Quantum Cryptography algorithms** that are **resistant to side-channel and fault attacks**; **Optimized countermeasures**; **Recommendations on implementing countermeasures**; **Analysis of new attacks** or combinations of attack; **Design of automated security evaluations** for PQC implementations.	6 M€ (3 M€ kpl)
Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols **(RIA)**	**Design and implementations of at least one high-level post-quantum cryptography protocol**; Submission of these high-level protocols integrating PQC to standardization bodies and/or submission of the specification and implementation to the respective open source projects; Requirements analysis highlighting roadblocks and needs for development of PQC solutions.	6 M€ (3 M€ kpl)

Lisätietoa edellä mainituista?

- Tilaa uutiskirjeemme liittymällä kansalliseen osaamisyhteisöömme. Liittyminen ei sido mihinkään eikä ole maksullista.
- Liittymislomake löytyy osoitteesta www.koordinointikeskus.fi
- ncc-fi(at)traficom.fi



TRAFICOM
Liikenne- ja viestintävirasto

Rahoitustuki kyberturvallisuuslain (124/2025) soveltamisalaan kuuluville pienille ja keskisuurille organisaatioille

Kansallisen koordinointikeskuksen rahoitustuki kolmansille osapuolille

- Kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden kansallinen koordinointikeskus (NCC-FI) myöntää rahoitustukea kolmansille osapuolille ns. kaskadirahoituksena omasta EU-projektirahoituksesta
- EU-projektin aikana (2025–2029) tavoitteena on vahvistaa kansallista ja EU:n kyberturvallisuuskapasiteettia myöntämällä rahoitustukea modernien kyberturvallisuusratkaisujen käyttöönottoon ja levittämiseen etenkin pk-yrityksissä
- Auki olevista hauista viestitään: koordinointikeskus.fi, haeavustuksia.fi, EU Funding and Tenders Portal ja koordinointikeskuksen uutiskirje.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC-FI
KYBERTURVALLISUUDEN KANSALLINEN KOORDINOINTIKESKUS

Euroopan unionin osarahoittama

TRAFICOM

Kyberturvallisuuslain soveltamisala

- Oikeushenkilö tai luonnollinen henkilö (*toimija*), joka:
  - Harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on niissä tarkoitettu toimija JA
    - A) Täyttää tai ylittää keskisuuren toimijan määritelmän
    - B) Koosta riippumatta, jos toimija on
      - Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja
      - Luottamuspalvelun tarjoaja, aluetunnusrekisterin ylläpitäjä tai DNS-palveluntarjoaja
      - Yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain (310/2025) nojalla määritetty kriittinen toimija muulla kuin julkishallinnon toimialalla
      - Palvelun tarjoaja kuuluu erityisluokkiin, esim. toimija tarjoaa ainoana palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen.

Ks. tarkemmin:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_08042025.pdf

Energia

Liikenne

Pankkitoiminta

Finanssimarkkinoiden infrastruktuuri

Terveys

Juomavesi

Jätevesi

Digitaalinen infrastruktuuri

TVT-palvelujen hallinta (yritysten välinen)

Julkishallinto

Avaruus

Posti- ja kuriiripalvelut

Jätehuolto

Kemikaalien valmistus, tuotanto ja jakelu

Elintarvikkeiden tuotanto, jalostus ja jakelu

Valmistus

Digitaalisen palvelun tarjoajat

Tutkimustoiminta

NIS2-toimialat ja valvovat viranomaiset

Valvovat viranomaiset
Traficom
Energiavirasto
Finanssivalvonta
Valvira
Tukes
Fimea
Ruokavirasto
Etelä-Savon ELY-keskus

Ks. tarkemmin: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa?toggle=Valvovat%20viranomaiset%20vastuusektoreineen%20on%20listattu%20alla

Riskienhallinta

Toimijalla on oltava käytössään ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli, jossa

- Tunnistetaan verkko- ja tietojärjestelmiin kohdistuvia ennakoitavissa olevia riskejä
- Määritetään ja kuvataan toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan riskeiltä ja poikkeamilta (hallintatoimenpiteet).

Riskienhallintatoimenpiteet

- Toimija määrittää ja toteuttaa, valvova viranomainen valvoo.
- Kyberturvallisuuslain 9 §:ssä vähimmäisosa-alueet, jotka on huomioitava toimintamallissa ja hallintatoimenpiteissä.
- Suhteutettava toiminnan laatuun ja laajuuteen, poikkeamista kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeaman todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin ja ajantasaisiin teknisiin mahdollisuuksiin torjua uhka.

TRAFICOM

Rahoitustukihaku kyberturvallisuuslain (124/2025) toimeenpanemisen tukemiseksi

- Haku auennut 15.8. ja päättyy 16.10.2025 klo 16:15
- Rahoitustukea myönnetään yhteensä enintään 2 MEUR
- Rahoitustukea voidaan myöntää 1.1.–31.12.2026 syntyviin kustannuksiin.
- Rahoitustuki on de minimis -muotoista. Yksi yritys voi saada de minimis -tukea kuluvan kolmen vuoden aikana enintään 300 000 euroa.
- Enintään 100 000 euroa ja vähintään 10 000 euroa per hakija ja hanke.
- Omavastuuosuusvaatimus 50 % hankkeen kokonaiskustannuksista.

Hakukelpoisuus 1/2

- Rahoitustukea voivat hakea kyberturvallisuuslain 3 §:n mukaisesti lain soveltamisalaan kuuluvat mikrokokoiset, pienet ja keskisuuret oikeushenkilöt ja luonnolliset henkilöt (toimijat), jotka ovat ilmoittautuneet oman toimialansa valvovan viranomaisen ylläpitämään toimijaluetteloon.
  - Suuret yritykset, julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) piiriin kuuluvat organisaatiot ja toimijaluetteloon ilmoittautumatta jättäneet toimijat **eivät ole** hakukelpoisia.
- Hakijan koon määritelmässä sovelletaan mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitettä kyberturvallisuuslain tarkoittamalla tavalla
  - ”Mikroyritysten sekä pienten ja keskisuurten yritysten (pk-yritysten) luokka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa.”
  - Kuten kyberturvallisuuslaissa, suosituksen liitteen 3 artiklan 4 kohtaa ei sovelleta. Näin ollen myös julkisyhteisön tai -laitoksen omistuksessa olevat toimijat voivat olla hakijoina ja heidän osalta rahoitustuen hakijan koon määritelmässä huomioidaan vain kyberturvallisuuslain liitteessä tarkoitettu toiminta. Koon määrittelyssä ei tällöin huomioida julkisyhteisön tai -laitoksen, kuten kunnan henkilöstön määrää, liikevaihtoa ja tasetta (tai äänioikeudelle asetettuja rajoituksia).

Hakukelpoisuus 2/2

- Rahoitustukea hakeva harjoittaa toimintaansa Suomessa Suomeen rekisteröidyllä y-tunnuksella. Yksi hakija/y-tunnus voi jättää yhden hakemuksen hakukierrosta kohti.
- Tukea ei myönnetä yhteisesti usealle hakijalle, esimerkiksi konsortiolle tai konsernin yrityksille. Tukea ei myönnetä muiden kuin saajan itsensä käytettäväksi.
- Tukea ei myönnetä esim. jos
  - EU:n tai ETA:n ulkopuolella toimiva taho käyttää hakijaan suoraa tai epäsuoraa määräysvaltaa Kirjanpitolain (1336/1997) 5 §:ssä tarkoitetulla tavalla,
  - Hakijalla on suurempia kuin vähäisiä velkoja ulosotossa tai velkoja, jotka on palautettu ulosotosta varattomuusestetodistuksin
  - ... (kattava lista löytyy hakuilmoituksesta)

Käyttötarkoitus

- Rahoitustukea voidaan myöntää kyberturvallisuuslain 9 §:n vaatimuksia mukaileviin arviointi- ja kehittämistoimenpiteisiin.
- Toimenpiteillä on määrä arvioida ja kehittää tapoja, joilla toimija hallitsee riskejä ja estää tai minimoi haitallisia vaikutuksia, jotka kohdistuvat viestintäverkkojen ja tietojärjestelmien turvallisuuteen.
- Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Kyberturvallisuuslain 9 §:n vaatimuksia mukailevat arviointi- ja/tai kehittämistoimenpiteet

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuusosaaminen;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Hyväksyttävät kustannukset

- Palkkakustannukset
  - Lasketaan hakuilmoituksessa osoitetulla kaavalla
  - Loppuselvityksessä osoitettava, mikä on kunkin henkilön hankkeen aikana tehdyn työajanosuus kokonaistyöajasta
- Ostopalvelut
- Ostot
- Vuokrat ja lisenssit
- Sisäiseen viestintään liittyvät kustannukset
- Kohtuulliset matkakustannukset
- Hankkeen raportointiin liittyvät kustannukset
- Yleisiä kuluja 7 %

Muuta hyväksyttävistä kustannuksista

- Kustannukset hyväksytään ja maksetaan loppuselvityksessä raportoitujen toteutuneiden kustannusten perusteella.
- Hankkeen kustannusten täytyy syntyä ja kohdistua tukea myönnettävälle organisaatiolle niihin toimintoihin tai toimintayksikköihin, joihin kyberturvallisuuslain velvoitteet ulottuvat.
- Kustannukset hyväksytään lähtökohtaisesti arvonlisäverottomina.
- Intressiyrityksiltä ostetut palvelut eivät ole hyväksyttäviä kustannuksia.
- Ehdot koskevat myös omavastuuosuudella rahoitettavia kustannuksia.

Tukihakemus jätetään sähköisellä hakulomakkeella

- Lomakkeelle tunnistaudutaan vahvalla sähköisellä tunnistusvälineellä.
- Hakulomakkeen liitteenä toimitettava hankesuunnitelma tulee tehdä hakusivulla olevaan hankesuunnitelmapohjaan.
- Hakulomakkeen täyttävällä henkilöllä täytyy olla hakijaorganisaation puolesta perusrekisteriin, kuten kaupparekisteriin merkitty organisaation edustamiseen oikeuttava rooli tai Suomi.fi -valtuutus ('Tietoturvan kehittämisen tuen hakeminen') hakea rahoitustukea organisaation puolesta.

Rahoitustuki on harkinnanvaraista

- Rahoitustukea myönnetään hakukelpoisuuskriteerit täyttäville sekä parhaiten hakemusten arvioinnissa menestyville hakijoille.
- Hakemukset arvioidaan ensin hakukelpoisuuskriteerejä vasten. Kriteerit täyttävät hakemukset siirtyvät arviointivaiheeseen, jossa arvioidaan hankkeen tarkoituksenmukaisuutta, toimeenpantavuutta ja vaikuttavuutta.
- Arviointiin vaikuttavat esimerkiksi hakemuksessa annettujen tietojen riittävyys, ymmärrettävyys, selkeys, johdonmukaisuus ja uskottavuus.

Hakuprosessi ja aikataulu

Aika	Vaihe
16.10.2025 klo 16:15	Haun päättyminen
Q4/2025	Hakukelpoisuuden tarkistus ja arviointi
Q1/2026	Rahoitustukipäätösten antaminen, tuen 1. osan maksu ja tiedotus myönnetyistä rahoitustuista koordinointikeskuksen verkkosivuilla
Q1/2027	Loppuselvitysten jättäminen
Q1/2027	Toteutuneiden kustannusten hyväksyminen ja tuen loppuosan maksu
2027	Vaikuttavuuden arviointi

Tukea hankkeiden suunnitteluun

Suositus NIS2-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

- Suositukseen on koottu tietoa ja käytännön esimerkkejä siitä, millaisia toimenpiteitä laissa säädettyihin vaatimuksiin voi kuulua.
- Suositus voi tukea toimijoiden kyberturvallisuuden riskienhallinnan suunnittelua.
- Suosituksessa kuvataan myös erilaisia keinoja, joita valvova viranomainen voi harkintansa ja arvionsa mukaan käyttää ohjaus- ja valvontatehtävissään
- Suositus luettavissa Kyberturvallisuuskeskuksen sivuilla.

Suosituksen soveltamisesta

- Ei sido viranomaisia eikä toimijoita.
- Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää suosituksesta poikkeavia, tiukempia vaatimuksia.
  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.
  - Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

Suosituksen sisällöstä

- Toimijalle asetetaan **riskienhallintavelvoite** kyberturvallisuuslain 2 luvussa 7-10 §:ssä.
  - Suositus keskittyy lain 9 §:ssä säädettyihin **kyberturvallisuuden riskienhallinnan toimenpiteisiin**.
- Suositukseen on koottu yleisimmin käytetyt kyberturvallisuuden **riskienhallintakeinot**.
  - Esimerkkejä toteutuksista, joita valvova viranomainen saattaa kohdata valvonnan yhteydessä.
  - Esimerkkejä todennusmenetelmistä ja viittaukset yleisimpiin kansallisiin ja kansainvälisiin viitekehyksiin.

Esimerkki suosituksen kohdasta

10.3 Palautustestaus ja varmuuskopioiden suojaaminen

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Varmuuskopioiden palautusta ja varajärjestelmien toimivuutta tulisi testata säännöllisesti, ensisijaisesti automaattisesti. Testauksessa pitäisi tarkastaa myös varmuuskopioiden eheys. Varmuuskopioiden palautustestaus on tehtävä turvallisesti niin, ettei se vaaranna tuotantojärjestelmää.
- Varmuuskopioita on säilytettävä turvallisessa tilassa, joka on toimijan riskienhallinnan perusteella riittävän eriytettynä varmuuskopioitavasta järjestelmästä. Tämä voi tarkoittaa esimerkiksi muuta toimitilaa tai erillistä palotilaa. Varmuuskopioita voi säilyttää tarvittaessa useassa muodossa, joiden palautusnopeuksissa voi olla eroa, kuten levylle otetut varmistukset sekä erilliset pitkäaikaisarkistot.
- Varmuuskopioiden suojaamisessa voidaan ottaa huomioon niiden eheyden, saatavuuden ja luottamuksellisuuden tarpeet. Tämä tarkoittaa esimerkiksi riittävää fyysistä suojausta ja muita kontrolleja, kuten salausta.

Todennus

1. Valvova viranomainen todentaa, että toimija on mahdollisuuksien ja tarpeen mukaan määrittänyt toimenpiteet, joilla varmuuskopioiden ja varajärjestelmien toimivuutta testataan säännöllisesti, esimerkiksi kerran viikossa. Tämä voi olla automatisoitua tai manuaalista. Keskeistä on, että mekaanisen palautuksen lisäksi tarkastetaan myös se, että tieto saadaan palautettua eheänä ja käyttökelpoisena, sekä mahdollinen varajärjestelmä pystytettyä oikealla tiedolla. Valvovan viranomainen todentaa, että varmuuskopiot on suojattu riittävästi. Esimerkiksi arkkitehtuurikuvauksissa, järjestelmädokumentaatiossa tai vastaavassa pitäisi olla kuvattuna se, miten varmuuskopiojärjestelmä tai sen osa on eriytetty muusta järjestelmästä. Tämän pitäisi varmistaa se, että jos esimerkiksi viestintäverkkoon ja tietojärjestelmään pääsee hyökkääjä, ei tämä voi päästä käsiksi kaikkiin varmistuksiin.
2. Valvova viranomainen todentaa katselmoinneilla ja haastatteluilla, miten toimija testaa varmuuskopioiden toimivuutta mahdollisuuksien ja tarpeen mukaan. Tästä tulisi käydä ilmi esimerkiksi suoritetut toimenpiteet varmuuskopioiden eheyden varmistamiseksi sekä testauksen säännöllisyys. Valvova viranomainen voi tarvittaessa hyödyntää myös fyysisiä katselmointeja sen varmistamiseksi, että varmuuskopioita on eriytetty muusta järjestelmästä riittävästi. Katselmoinnissa tulisi varmistua esimerkiksi siitä, että uhkat kuten tulipalo, tulvat ja henkilöuhka, eivät koske sekä varmistettavaa järjestelmää että varmuuskopioita.
3. Jos kyseessä on fyysisen erottelun sijaan perusteltu looginen erottelu, voi valvova viranomainen hyödyntää esimerkiksi toimijan tekemiä skannauksia ja yhteydenottoyrityksiä sen varmistamiseksi, että eriytettyyn varmuuskopiointijärjestelmään ei pääse käsiksi varmistettavan viestintäverkon ja tietojärjestelmän puolelta.

Perustelut

Poikkeamatilanteista palautumisen yhteydessä tapahtuu liian usein niin, että palautus ei onnistu tai hyökkääjä onnistuu tuhoamaan sekä tietojärjestelmän että varmuuskopiot. Tämän vuoksi palautuksen kattava ja säännöllinen testaaminen sekä palautusjärjestelmän suojaaminen voivat olla toiminnan kannalta elintärkeitä.

Viitteet

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Työkalut

Julkri (TEK-20, VAR-09)

Kybermittari (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5)

Mitä suosituksen kohdat pitää sisällään?

- Toteutusesimerkissä kuvataan, millä tavoin taulukossa kuvattu suositus on voitu toteuttaa. Esimerkit eivät ole tyhjentäviä, koska toteutus voi vaihdella toimijaan koon ja toimialan mukaan.
- Todennuksessa on esimerkkejä siitä, miten valvova viranomainen voi todentaa toimijan kyberturvallisuuden riskienhallinnan toimenpiteiden toteutumista.
- Perusteluissa taustoitetaan sitä, miksi otsikon mukainen toimenpide on nostettu lainsäädäntöön ja sisällytetty suositukseen, sekä mihin sillä pyritään. Ne voivat sisältää esimerkiksi uhkanäkökulmia, jolta kyseisellä toimenpiteellä pyritään suojautumaan.
- Viitteissä on esimerkkejä yleisimmistä standardeista, viitekehyksistä ja ohjeistuksista, jotka liittyvät kyseiseen suositukseen.
- Työkaluissa on arviointivälineitä ja mittareita sekä työkaluja ja ohjelmistoja.

Lisätietoja

- Koordinointikeskus.fi
  - Hakuohjeet ja hakemuksen jättäminen
  - Usein kysytyt kysymykset ja vastaukset
- kyber.rahoitustuki(at)traficom.fi

- Huom! Hakemusten käsittelyn aikana hakemuksen tietoihin ilmenevistä muutoksista on viipymättä ilmoitettava kyber.rahoitustuki(at)traficom.fi