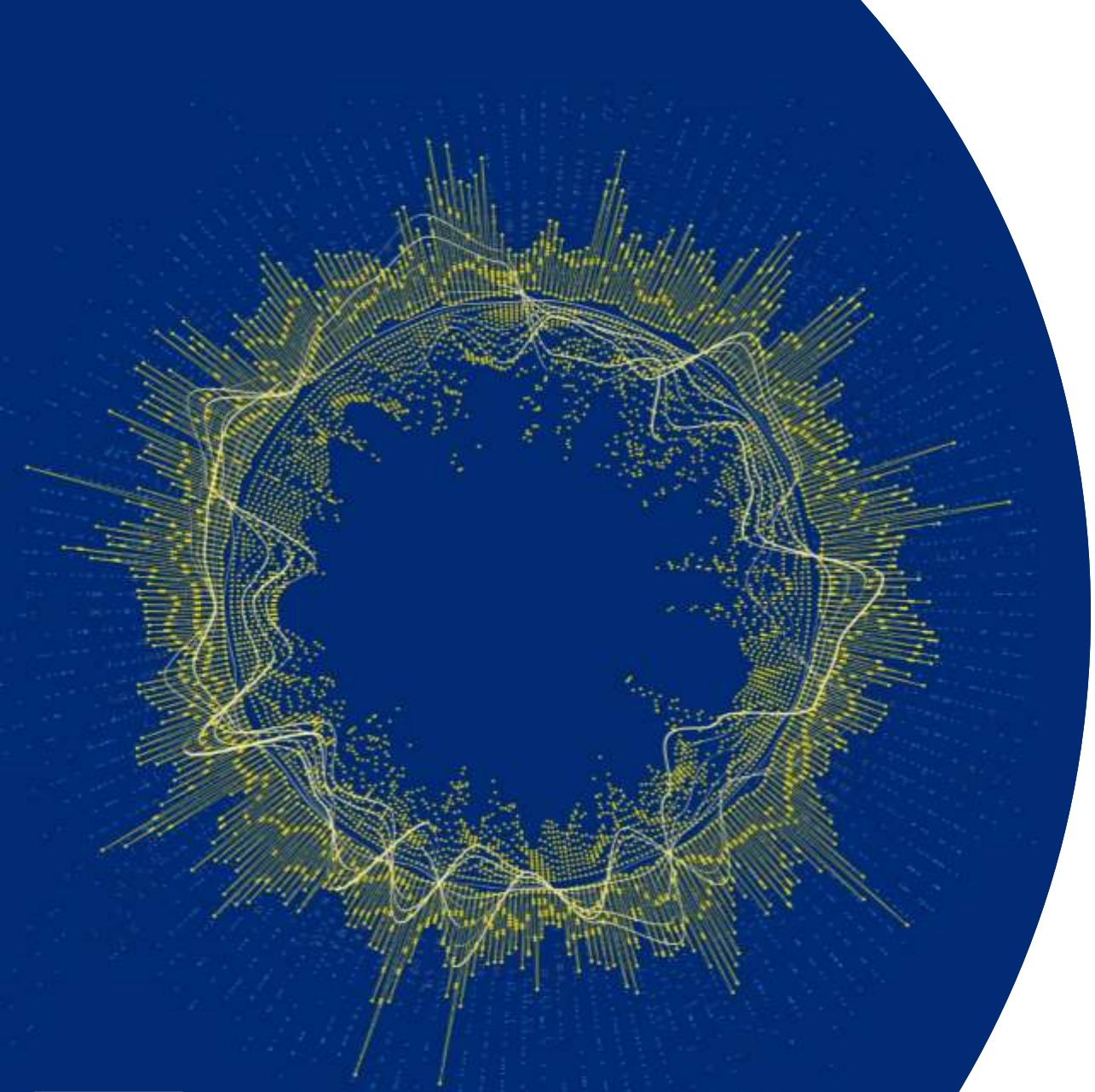


Co-funded by
the European Union

TRAFICOM
Liikenne- ja viestintävirasto

NCC-FI
FINLAND NATIONAL COORDINATION CENTRE FOR CYBERSECURITY

Yritysturvallisuusvartti

EU:n tarjoamat rahoitusmahdollisuudet kyberturvallisuuden kehittämiseen

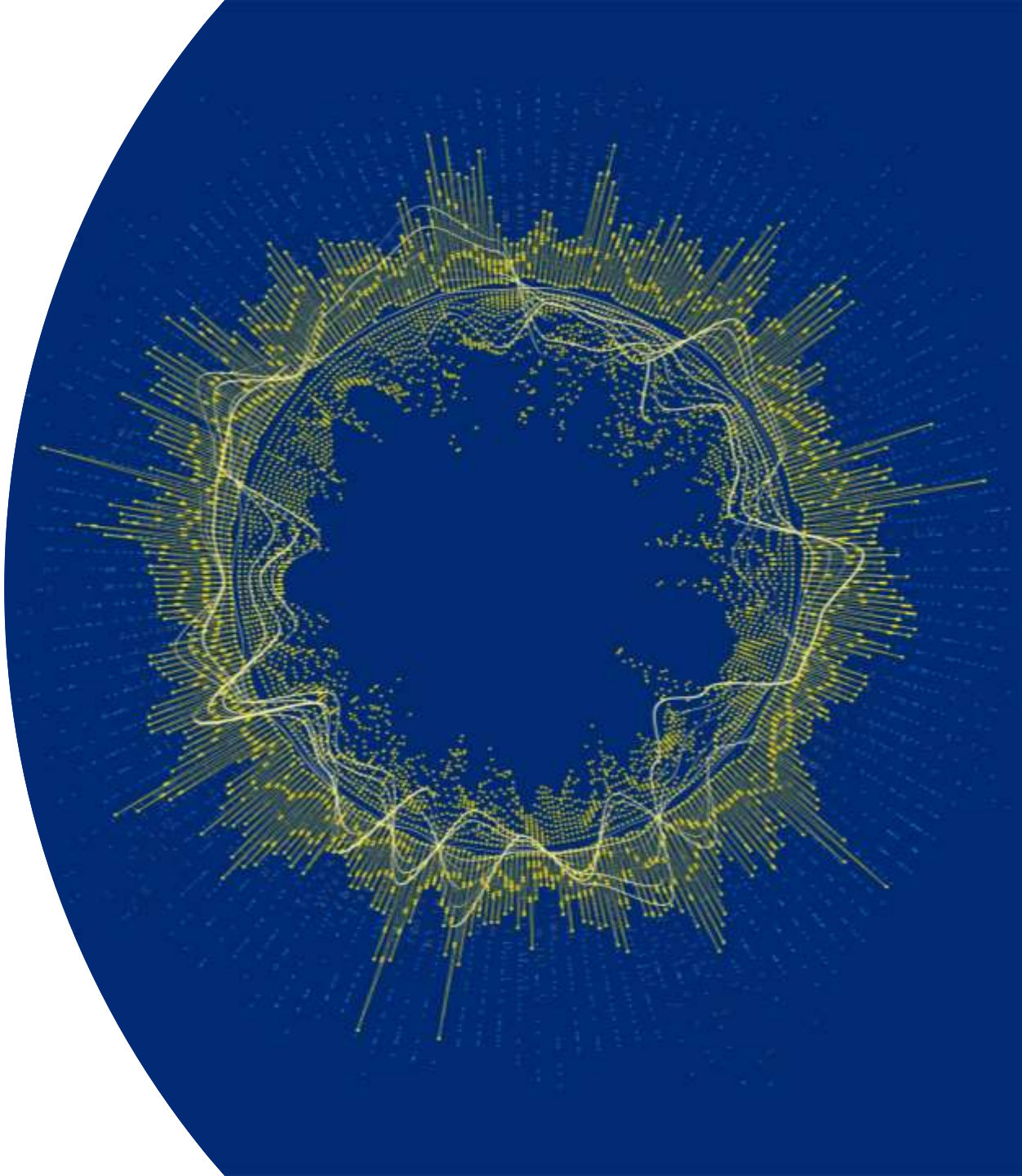
21.01.2026

Ohjelma

- Kansallisen koordinointikeskuksen palvelut
- EU-rahoituksen perusteet
- Kyberturvallisuuden rahoitus
  - Horisontti Eurooppa
  - Digitalainen Eurooppa
- Digitaalinen Eurooppa –CYBER-09 rahoitushaut
  - Cybersecure tools, technologies and services relying on AI
  - Uptake of innovative cybersecurity solutions for SMEs
  - Coordinated preparedness testing
  - Regional Cable Hubs
- Kysymykset ja vastaukset
- Tilaisuuden päättäminen

TRAFICOM

Kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden kansallisen koordinointikeskuksen (NCC-FI) palvelut



TRAFICOM

Kansallisen koordinointikeskuksen tavoitteena on

- Tukea Euroopan Kyberturvallisuuden Kompetenssikeskuksen (ECCC) toimintaa sekä edistää unionin kilpailukykyä, johtajuutta ja strategista itsenäisyyttä kyberturvallisuusalalla
  - Tukea kansallisesti kyberturvallisuuden tutkimusta, kehitystä ja innovointia
  - Kasvattaa kansallista kyberturvallisuuskapasiteettia ja valmiuksia suojautua kyberuhilta
    - Mm. myöntämällä kaskadirahoitusta
  - Vastata kyberturvallisuusalan osaajapulaan
  - Koota kyberturvallisuusalan toimijat osaamisyhteisöksi

Toimii osana kansainvälisten koordinointikeskusten verkostoa. Perustettu Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/887.

Koordinointikeskukselta kattavat palvelut kyberalan EU-rahoitukseen

- ✓ Avustamme sopivan EU:n kyberrahoituksen löytämisessä
- ✓ Opastamme EU-rahoituksen hakemisessa
- ✓ Järjestämme koulutuksia, tiedotustilaisuuksia ja verkostoitumismahdollisuuksia
- ✓ Konsultoimme projektin hallinnollisissa prosesseissa ja rahoitussopimuksen valmistelussa (ei lakineuvontaa)
- ✓ Jaamme tietoa ajankohtaisista EU-rahoitushauista
- ✓ Tarjoamme verkostoitumismahdollisuuksia Euroopassa

Lisätietoja: ncc-fi@traficom.fi

Liity osaamisyhteisöön ja edistä organisaatiosi kansainvälistymistä ja TKI-mahdollisuuksia kyberalalla!

- Osana maksutonta osaamisyhteisöä saat kuukausittaisen uutiskirjeen, hankeyhteistyöilmoituksia EU-rahoitushakuihin liittyen, sekä kutsuja monipuolisiin tapahtumiin.
- Lisäksi saat ajankohtaista tietoa kyberturvallisuusalan TKI-kehityksestä sekä rahoitusmahdollisuuksista, tukea EU-rahoituksen hakemiseen, kanavia EU-vaikuttamiseen, sekä verkostoitumismahdollisuuksia niin Suomessa kuin Euroopassa.

- **Liity mukaan QR-koodin tai nettisivujemme kautta**
- Lisätietoja: ncc-fi@traficom.fi.

TRAFICOM

EU-rahoituksen perusteet

Tutkimus-, kehitys-, innovaatio- ja käyttöönottorahoitus

Ohjeita tutkimus-, kehitys-, innovaatio-, ja käyttöönottoprojekteihin osallistujille

- **Edellytykset**
  - Projekti-idean tulee perustua hakijan omiin tavoitteisiin ja tarpeisiin, joilla on kansainvälinen ulottuvuus.
  - Toteutuessaan projektilla on eurooppalaista lisäarvoa ja vaikuttavuutta. Se lisää hyvinvointia Euroopassa ja edistää kilpailukykyämme.
  - Projektin uutuusarvo on EU:n tutkimusohjelmissa tärkeää.
- **Osallistujat**
  - Muutamissa hankemuodoissa hakijana voi olla yksi osallistuja (esim. Digitaalinen Eurooppa). Pääsääntöisesti tutkimusprojekteissa vähimmäisvaatimus on kuitenkin kolme osallistujaa kolmesta eri jäsen- tai liitännäisvaltiosta.
  - Käytännössä konsortiossa on yleensä enemmän partnereita ja kansainvälistä konsortiota suositellaan myös hakuihin jossa se ei ole suorana vaatimuksena.
- **Hankkeen hyödyt**
  - Rahoituksen saaminen omaan tutkimus-, kehitys-, ja innovointityöhön.
  - Sen lisäksi teet yhteistyötä huippuosaajien kanssa, pääset uusille markkinoille, luot standardeja tai kehität liiketoimintaideaasi.

Hakijan ABC

1. Perehdy työohjelmaan (Work Programme).

Työohjelmassa on kuvattu haut, vaatimukset, budjetit ja aikataulut. Löydät ne komission Funding & Tenders -osallistujaportaalista.

2. Etsi ideaasi täsmäävä aihe (call topic) ja tarkista sen hakuajat.

Osallistujaportaalissa voit myös etsiä hakuja avainsanahaulla. Jokaisella aiheella on oma hakuohjesivu (Topic Conditions & Documents), josta löydät mm. hakua koskevat tärkeät reunaehdot, arviointikriteerit, malliavustussopimuksen sekä mallihakemuspohjan.

3. Konsortiohakemukseen tarvitaan kumppaneita!

Jo ennen hakuaiheen avautumista sinun pitäisi jo olla mukana kumppanien kanssa rakentamassa konsortiota ja hakemusta.

4. Hakemuksen teko on työtä, joka vie aikaa ja vaatii resurssia.

Varaa projektin suunnitteluun ja hakemuksen tekoon useita kuukausia. Isojen projektien kokoamisessa voi mennä puoli vuotta, joskus jopa vuosikin. Aikataulua suunnitellessasi tutustu myös komission arviointi- ja valintaprosesseihin.

5. Lähetä hakemus ajoissa – vältä riskit äläkä odota viimeiseen päivään!

Aloita hakemuksen tekeminen komission osallistujaportaaliin heti kun mahdollista. Vasta viimeisin versio otetaan arvioitavaksi, joten voit käyttää portaalin sähköistä hakemusjärjestelmää työskentelyyn.

1. Perehdy työohjelmaan (Work Programme).

- Haut perustuvat monivuotisiin rahoitusinstrumentteihin ja niiden vuosittaisiin työohjelmiin. Kyberaiheet löytyvät pääosin seuraavista työohjelmista:
  - Horisontti Eurooppa – Klusteri 3: Kansalaisturvallisuus yhteiskunnassa (Annex 2)
  - Digitaalinen Eurooppa
- Jokaisen työohjelman alussa kerrotaan mihin rahoituksella pyritään vastaamaan ja mihin poliittisiin ohjelmiin ne perustuvat.
  - Räätälöi hakemuksesi näitä silmälläpitäen.

2. Etsi ideaasi täsmäävä aihe (call topic) ja tarkista sen hakuajat.

- Voit aloittaa haun Funding-sivuston Calls for Proposals -osiosta. Hakua on mahdollista kohdentaa hakusanoin tai määrittämällä suodattimia rahoituskauden, hakuohjelman, hakuosion ja haun aktiivisuuden kautta.
- Listauksesta löydät asettamiasi kriteereitä vastaavat rahoitushaut, joiden alta avautuvat yksittäiset hakusivut, joilta saat tarkempia tietoja ja tarvittavat liitemateriaalit.
- Eri rahoitusohjelmien hauissa saattaa olla määrätty myös erityisehtoja, joten tarkista mahdolliset poikkeukselliset hakumenettelyt ja vaatimukset aina hakusivulla tarjolla olevista hakukohtaisista lisämateriaaleista.

3. Konsortiohakemukseen tarvitaan kumppaneita!

- Hakukonsortio, eli useamman toimijan yhteistyöryhmä, on yleinen hakukriteeri projektille. Konsortiossa useat organisaatiot hakevat yhteisellä hakemuksella rahaa yhdessä tehtävään projektiin.
  - Horisontti Eurooppa – TKI-rahoitus vaatii yleensä konsortion, jossa vähintään kolme organisaatiota kolmesta hakukelpoisesta maasta.
  - Digitaalinen Eurooppa ei usein vaadi konsortiota, mutta suosittelee vahvasti konsortiohakemuksia.
- Yhteistyökumppaneita kannattaa lähteä selvittämään omien verkostojen kautta.
  - Yliopistot, AMK:t ja tutkimuslaitokset ovat usein innokkaita ja kokeneita hakijoita.
  - Partnereita voi löytyä myös hakupalveluiden kautta, kuten hakemusportaalin hakokohtainen sivu ja b2match-sivusto.
  - Enterprise Europe Network (EEN) -verkosto auttaa löytämään sekä pk-yrityksiä että muitakin kumppaneita.
  - Euroopan Komissio sekä kansalliset kontaktipisteet, kuten Koordinointikeskus ja Business Finland, neuvovat myös partnereiden löytämisessä, järjestävät infotilaisuuksia ja brokerage-tapahtumia.

4. Hakemuksen teko on työtä, joka vie aikaa ja vaatii resurssia.

- Yleiset pdf-muotoiset hakemuspohjat löytyvät komission osallistujaportaalista: Reference Documents
- Editoitavat hakemuskohtaiset dokumentit löytyvät hakemusportaalista, kun olet rekisteröinyt projektin otsikon, aiheen, hallinnoivan organisaation ja kontaktihenkilön. Käytä aina haussa annettua dokumenttia!
- Jokainen osallistuja päättää, kuinka suurella panoksella haluaa osallistua hankkeeseen.
  - Suurimman työn tekee, ja eniten pääsee vaikuttamaan, hankkeen vetäjä eli koordinaattori. Koordinaattori kokoaa hakemuksen (yhdessä konsortion kanssa) ja vastaa sen jättämisestä. Hankkeen aikana koordinaattorin tehtäviin kuuluu yhteydenpito komission kanssa, EU-rahoituksen vastaanotto ja jakaminen osallistujille, kirjanpito rahaliikenteestä ja raporttien toimittaminen komissiolle.
  - Hankkeen riviosallistujana pääsee helpommalla. Ennen koordinaattoriksi ryhtymistä on usein hyvä tutustua puiteohjelmahankkeiden arkeen osallistujan ominaisuudessa.

5. Lähetä hakemus ajoissa – vältä riskit äläkä odota viimeiseen päivään!

- Hakemukset valmistellaan ja lähetetään Euroopan komissioon sähköisesti osallistujaportaalissa.
  - Seuraa tarkkaan dokumentin ohjetta muotoilusta ja pituudesta. Liian pitkiä hakemuksia ei lueta kokonaan.
- Jokaisella hakuun osallistuvalla organisaatiolla täytyy olla PIC-koodi.
  - Se on helppo ja nopea hakea. Jos organisaatio on osallistunut aikaisemmin puiteohjelmahakuihin, sillä todennäköisesti on jo PIC-koodi ja on etsittävissä hakiessa.
- Koordinaattori rekisteröi hakemuksen sähköiseen hakujärjestelmään.
  - Tietoja voi päivittää kunnes haku sulkeutuu. Sähköisen hakuohjelman avulla hankkeen koordinaattori ja osallistujat voivat täyttää hakulomakkeet, liittää hakemukseen tarvittavat osat, päivittää tietoja ja lopulta lähettää hakemuksensa komissioon.
  - Hakemuksen A-osa täytetään hakusivulla ja se sisältää perustietoa hankkeesta sekä partnereista. Hakemuksen varsinainen sisältöosa, osa B - kattava ja yksityiskohtainen projektisuunnitelma, tulee ladata mukaan omaksi liitteekseen.

Hakemuksen osa-alueet

- Hakemuksen B-osa koostuu kolmesta arvioitavasta osiosta:
  - **Excellence (Horisontti Eurooppa) / Relevance (Digitaalinen Eurooppa)**
    - Osio keskittyy projektin tieteellis-tekniseen puoleen (Horisontti) ja hakuaiheeseen vastaavuuteen (Digitaalinen Eurooppa)
  - **Impact**
    - Osio keskittyy erityisesti pidemmän tähtäimen arvon luomiseen. Osoita projektin tulosten järkevyys, tarve markkinoilla sekä projektin kestoa laajemmalle ulottuvat vaikutukset.
  - **Implementation**
    - Tässä osiossa tärkeimpänä on projektisuunnitelman laatu. Osoita, että projektin eri vaiheet on suunniteltu riittävällä tarkkuudella ja vastuualueet jaettu ja resursoitu osallistujien kesken parhaalla mahdollisella tavalla. Projektille mahdolliset riskit tulee myös tiedostaa ja esitellä.
    - Koostuu yleensä esittelevästä Implementation- kappaleesta sekä projektin työpaketteihin ja tehtäviin jaetusta projektisuunnitelmasta.
- Projekti tulee myös budjetoida jo hakuvaiheessa eri kulukategorioihin.

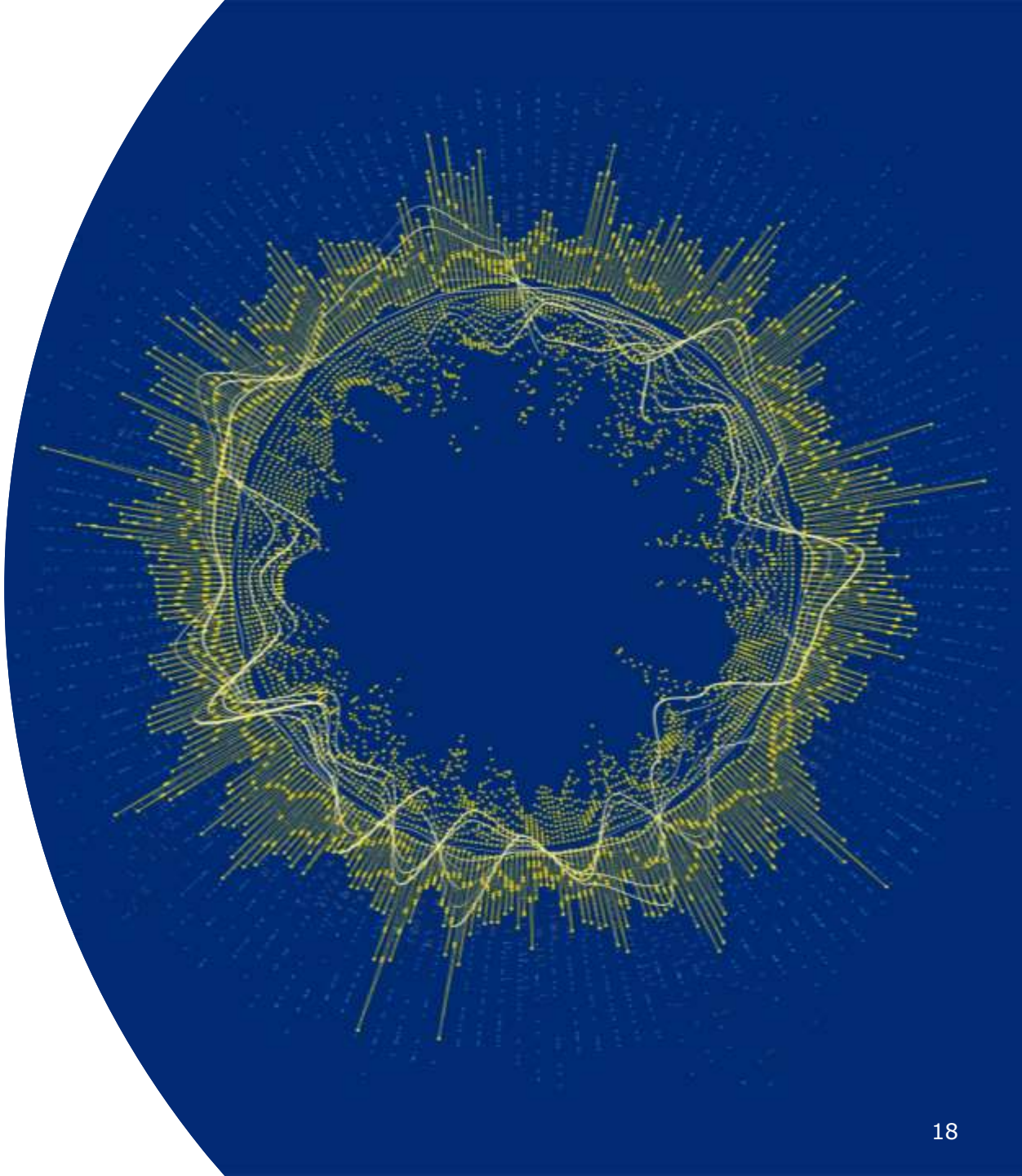
5 askelta kohti parempaa hakemusta

1. Ole selkeä
2. Mieti, voisiko asian kertoa tekstin lisäksi myös havainnollistavan kuvan, taulukon tai kaavion kautta
3. Vastaa jokaiseen kysymykseen kattavasti mutta tiiviisti
4. Todista esittämäsi väitteet esimerkiksi tieteellisten julkaisujen, markkinatutkimusten tai asiakkaiden lausuntojen kautta
5. Osoita toimien mitattavuus mahdollisimman konkreettisesti

Lähteet

- Tämän osion materiaali on koottu pääosin kolmesta lähteestä:
  - Business Finlandin ylläpitämä Hakijan opas
  - Traficomin Koordinointikeskuksen yleiset hakuohjeet-sivu sekä Näin laadit hyvän hakemuksen-sivu
  - Euroopan komission How to Participate – sivusto
- Ohjeet ovat pääosin yleispäteviä sekä Horisontti Eurooppa sekä Digitaalinen Eurooppa rahoitusinstrumentteihin.

EU-rahoitus kybertoimijoille



Horisontti Eurooppa – tutkimusrahoitusta kyberturvan kehitykseen

Mitä rahoituksella tuetaan?

Tutkimusta, tuotekehitystä, innovaatioita ja esikaupallista toimintaa.

Kenelle?

Mahdollisuuksia kaikille julkisesta sektorista akatemiaan, oppilaitoksiin ja yrityksiin, sekä kolmannelle sektorille.

Projekteissa vaatimuksena vähintään kolmen maantoimijoista muodostuva konsortio.

Projektien kokoluokka?

Yleensä rahoittaa 1-6 M€ projektia kohti.

Projektit kestävät 3-4 vuotta.

Kattaa 70% - 100% projektin kuluista.

Tarkemmat tiedot?

Horisontti Eurooppa työohjelma vuosille 2026-2027 julkaistu Komission nettisivuilla. Kyberturvallisuudella erillinen liite, jota hallinnoi ECCC.

TRAFICOM

Digitaalinen Eurooppa – rahoitusta kyberturvan käyttöönottoon

Mitä rahoituksella tuetaan?

Teknologioiden, tuotteiden ja tutkimustulosten käyttöönottoa ja markkinoille vientiä.

Kenelle?

Mahdollisuuksia kaikille julkisesta sektorista yksityiseen.

Erityisesti pk-yrityksiä kannustetaan mukaan.

Mahdollisuus hakea yksin, kansallisena- tai kv-konsortiona.

Projektien kokoluokka?

n. 1-3 vuotta ja n. 3-5 M €/projekti

(Kattaa n. 50-75% kustannuksista)

Tarkemmat tiedot?

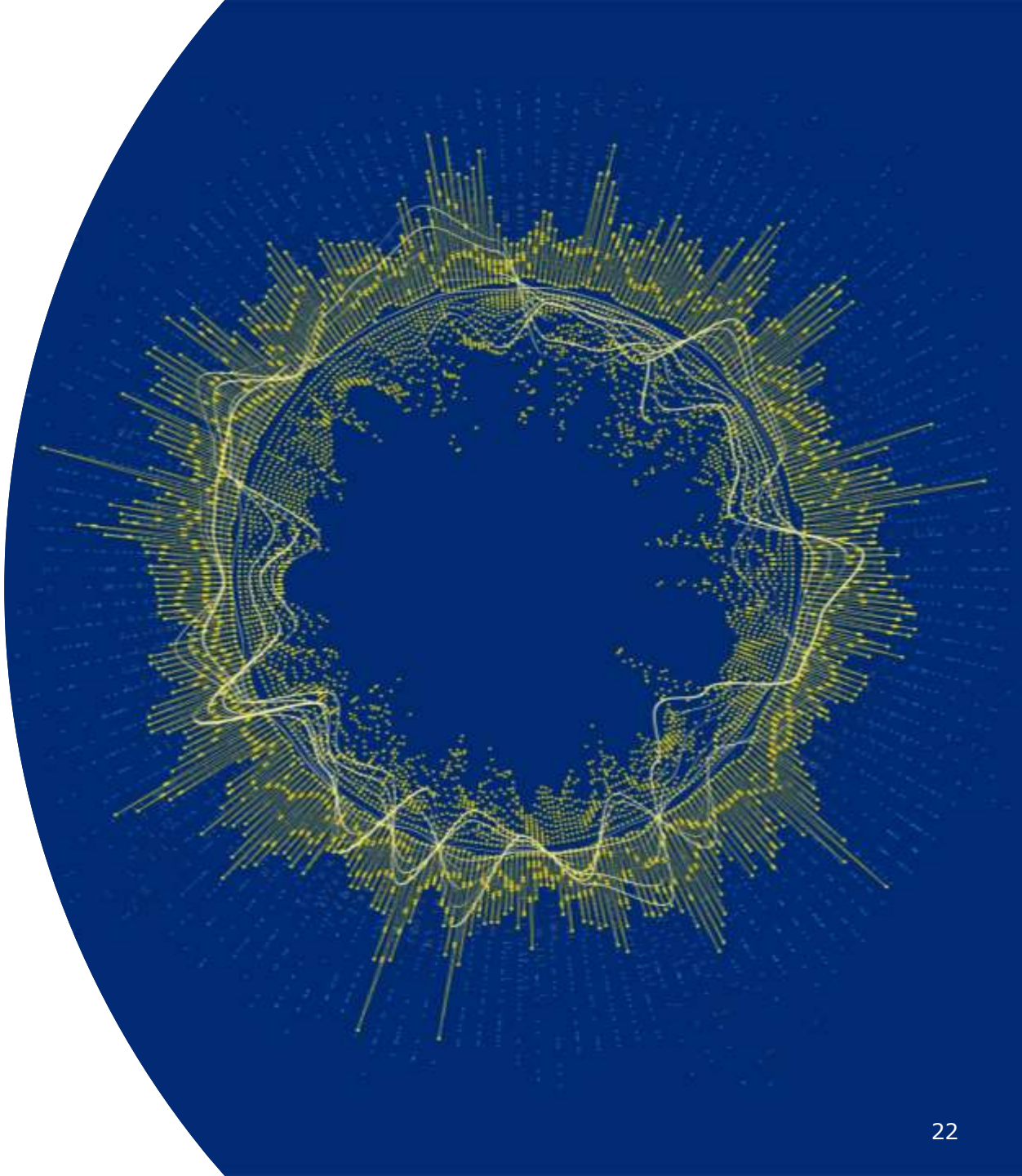
DEP-työohjelmat julkaistu vuosille 2025-2027.
Kyberturvallisuudella erillinen työohjelma, jota hallinnoi ECCC.

Arvoketjuajattelu - Projekteissa tarvitaan kaiken tyyppisiä ja tasoisia toimijoita

- Toimija voi olla konsortiossa kehitys- ja tutkimustoiminnan sijaan mukana mm. käyttöönottajana, integraattorina tai loppukäyttäjänä
- Kehitykseen voi osallistua mm. pilotoimalla ja testaamalla, sekä antamalla palautetta
- Tarjoaa arvokasta tietoa sovelluksen toiminnasta omalla vastuualueella ja omassa käyttökohteessa

Digitaalinen Eurooppa –kybertyöohjelma

Avoimet CYBER-09 haut sekä katsaus tulevaan



TRAFICOM

DEP CYBER-09 rahoituskierros:

Haut avautuneet 28.10.2025

- Hakutekstit löytyvät Komission Funding and Tenders portaalista
  - https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

Haettavissa olevat aiheet

- Cybersecure tools, technologies and services relying on AI
- Uptake of innovative cybersecurity solutions for SMEs
- Coordinated preparedness testing
- Regional Cable Hubs

Haut sulkeutuvat 31.3.2026!

- Arvioinnin tulokset kesä- heinäkuussa 2026

Cybersecure tools, technologies and services relying on AI

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI

OBJECTIVE: AI-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies, private entities from the NIS 2 directive, and NCCs.

These enabling technologies should allow for more effective creation and analysis of Cyber Threat Intelligence (CTI), automation of large-scale processes, as well as faster and scalable processing of CTI and identification of patterns that allow for rapid detection and decision making.

The security of AI itself, especially for the systems in the learning phase, also needs to be addressed, including the misuse of AI by malicious actors. In addition to being secure, the AI technologies being developed should perform well, and be robust and trustworthy.

SCOPE: Actions in this topic should 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. These activities must also comply with intellectual property rights (IPR) and the GDPR.

EXPECTED OUTCOMES: [E.g. At least one of the following made available to Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others. Full list in call text.]

- Deployment of Artificial Intelligence and various AI-powered technologies
- Novel cybersecurity tools based on AI that have been developed, tested and validated
- Enhanced information sharing and collaboration [...] supported by CTI produced by AI-powered tools.
- Tools for automation of cybersecurity processes e.g. creation, analysis and processing of CTI
- Original European CTI feeds or services
- Advanced and innovative secure AI solutions developed and implemented for NIS sectors.
- Contribution to the standardisation and certification of cybersecure, trustworthy AI technologies.

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: Teknologioiden tarjoajat, Cyber Hubit, akatemia, tutkimuslaitokset, kyberturvallisuustoimijat, NIS2 direktiivin alaiset toimijat, loppukäyttäjät

Rahoitus: Simple Grant 50%

Budjetti: 3-5 M€

Projektin ehdotettu kesto: 3 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Uptake of innovative cybersecurity solutions for SMEs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE

The action aims at improving industrial and market readiness for the cybersecurity requirements for SMEs ensuring more secure hardware and software products.

OBJECTIVE: Proposals should contribute to achieving at least one :

- Availability of innovative tools and services that support SMEs in complying with the EU legislation or reporting incidents and in assisting with recovery if possible.
- Improved security and notification processes and means in the EU, Improved security of network and information systems in the EU, Industrial and market readiness for CRA, Support for Cybersecurity certification (CSA).
- Support for supply chain partners in standardised self-assessments and certifications. Helping downstream supply chain partners in a step-by-step approach to increase cyber resilience.
- Overcome the challenge of finding the technical skills
- Cyber toolkit as a service to support for SMEs managing cyber risks, defining, and implementing their cybersecurity strategy, including several functions dedicated to risk assessment, vulnerabilities and threats detection, etc.

SCOPE: The action will focus on supporting at least one of the **EXPECTED OUTCOMES:**

- The development of a cyber toolkit as a service to support SMEs managing cyber risks, defining, and implementing their cybersecurity strategy
- Support and incident response capabilities to SMEs
- Support tools and platforms

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: PK-yritykset, julkiset ja yksityiset toimijat jotka toimeenpanevat NIS2 ja CRA käytänteitä, tutkimus, akatemia, jne.

Rahoitus: SME Support Actions 50%; PK-yrityksille 75%

Budjetti: 3 M€

Projektin ehdotettu kesto: 3 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Coordinated preparedness testing
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP

This topic covers actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism, namely coordinated preparedness testing of entities operating in sectors of high criticality across the Union, specifically the health sector, and in particular hospitals, and the digital infrastructure sector, including electronic communication sector, and in particular fixed networks and submarine cable infrastructure.

OBJECTIVE: [...] to increase the level of protection and resilience to cyber threats, in particular for critical industrial installations and infrastructures, by assisting Member States in their efforts to improve their preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving coordinated preparedness testing of entities operating in sectors of high criticality across the Union (including penetration testing and threat assessment) considering ICT as well as Operational Technology/Industrial Control Systems.

SCOPE: The provision of preparedness support services shall include the activities listed below, for entities in the sector or sub-sector as identified by the Commission [...].

- **Support for testing for potential vulnerabilities:** Development of penetration testing scenarios; Support for conducting testing of essential entities; Support for the deployment of digital tools and infrastructures supporting the execution of testing scenarios; Evaluation and/or testing of cybersecurity capabilities of MS entities; Consulting services, providing recommendations on how to improve infrastructure security and capabilities, etc.
- **Support for threat assessment and risk assessment,** such as Threat Assessment process implementation and life cycle; Customised risk scenarios analysis.

EXPECTED OUTCOMES:

- Enhanced cooperation, preparedness and cybersecurity resilience in the EU; preparedness support services
- Threat assessment and risk assessment services.

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: CSIRT toimijat ja julkiset reguloidut toimijat (NIS2, CRA, CSA, CSoA, DORA, etc.), muut toimijat konsortiossa

Rahoitettavat toimialat (2025): Terveydenhuolto - erityisesti sairaalat; digitaalinen infrastruktuuri - erityisesti kiinteät verkot ja merikaapelit

Rahoitus: Simple Grant 50%

Budjetti: 1,5 M€

Projektin ehdotettu kesto: 2 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Regional Cable Hubs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS

As part of the EU Action Plan on Cable Security, it was announced that the Commission, together with voluntary Member States, will work on Cable Integrated Surveillance Mechanisms per sea basin ('Regional Cable Hubs') to enhance the detection capacity against threats to undersea cables as they are critical infrastructure. Taking into account the fact that these cables are covered by the scope of NIS2 Directive that follows an all-hazards approach, it is crucial to protect their physical environment from events such as malicious acts, including cuts as integral part of the cable cybersecurity measures.

OBJECTIVE/SCOPE: The objective is to support the progressive establishment of Regional Cable hubs, one per sea basins of the EU, whose role will be to concretely enhance threats detection and operational security around these strategic infrastructures.

[...] aimed at supporting the set-up of processes, tools and services for detection and analysis of emerging threats, to establish a near real time situational awareness to protect the undersea cables. It includes the capacity to aggregate data and security information from all available sources and analyse them in an automated way.

EXPECTED OUTCOMES:

The Regional cable hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection, supporting the development of an operational capacities to ensure the security and resilience of undersea cables. The hubs should:

- act as a central point allowing for broader pooling of data and information
- allow a rapid exchange of information, even if classified among participating authorities
- make use of existing systems which were not developed necessarily for Cable Security
- integrate direct cooperation with private entities, especially cable operators to increase access to information on ongoing and future threats
- integrate the defence dimension

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: Julkishallinnot/virastot/tahot jotka ovat vastuussa valtioiden merikaapeli-infrastruktuurista, merialueen turvallisuustoimijat, kyberturvatoimijat, jne.

Rahoitus: Simple Grant 70%

Budjetti: 3 M€

Projektin ehdotettu kesto: 3 vuotta

Konsortio: Vähintään kaksi toimijaa kahdesta eri valtiosta samalta merialueelta. Suositellaan mahdollisimman suurta kattavuutta per merialue.

DEP kyber – Vilkaisu vuosiin 2026 ja 2027

- Haut tulevat alustavien tietojen mukaan aukeamaan Q1/Q2 vaihteessa.
- Vuonna 2026 on odotettavissa haku kyberpuolustustoimijoille ”Dual-use Technologies”
- Vuonna 2026 ja 2027 myös suunniteltu enemmän julkishallinnolle suunnattuja hakuja
- Työohjelmassa jo esiteltyjä hakuja mm:
  - Cybersecure tools, technologies and services relying on AI (2026,2027)
  - Uptake of innovative cybersecurity solutions for SMEs (2027)
  - Coordinated preparedness testing and other preparedness actions (2026, 2027)
  - Strengthening cybersecurity capacities of European SMEs with cybersecure AI solutions (2026)
  - Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements (2026,2027)
- Muutokset mahdollisia!

Hetki kysymyksille ja vastauksille

Liity osaamisyhteisöön ja edistä organisaatiosi kansainvälistymistä ja TKI-mahdollisuuksia kyberalalla!

- Osana maksutonta osaamisyhteisöä saat kuukausittaisen uutiskirjeen, sekä
  - Ajankohtaista tietoa kyberturvallisuusalan TKI-kehityksestä sekä rahoitusmahdollisuuksista
  - Hankeyhteistyöilmoituksia EU-rahoitushakuihin liittyen
  - Kutsuja monipuolisiin tapahtumiin
  - Tukea EU-rahoituksen hakemiseen
  - Verkostoitumismahdollisuuksia niin Suomessa kuin Euroopassa

- **Liity mukaan QR-koodin tai nettisivujemme kautta**
- Lisätietoja: ncc-fi@traficom.fi

TRAFICOM

Kiitos!

NCC-FI(at)traficom.fi

koordinointikeskus.fi

Co-funded by
the European Union

Timo Mustonen

Eritysiasiantuntija - Digital Europe (Cyber)
Traficom – NCC-FI
etunimi.sukunimi(at)traficom.fi