Euroopan unionin osarahoittama

Liikenne- ja viestintävirasto Traficom on myöntänyt rahoitustukea kyberturvallisuuslain (124/2025) soveltamisalaan kuuluville pienille ja keskisuurille organisaatioille kyberturvallisuuslain toimeenpanemisen tukemiseksi. Rahoitustuki myönnettiin kyberturvallisuuskeskuksen kansallisen koordinointikeskuksen EU-projektin rahoituksesta. Vuonna 2026 rahoitustukea myönnettiin seuraaville hankkeille:

Rahoitustuen saaja	Myönnetty summa (€)	Hankkeen nimi	Hankkeen kuvaus
ALM Partners Oy	82 175	Pilvipalvelun kyberturvallisuuskeskuksen (SOC) perustaminen	Otetaan käyttöön pankkiasiakkaan pilvipalvelun kyberturvallisuuskeskus vasteaikojen ja häiriönhallintaprosessin parantamiseksi.
atFlow Oy	45 603	Omaisuuden- ja palveluidenhallintajärjestelmä	Hankkeessa kehitetään keskitetty omaisuuden- ja palveluidenhallintajärjestelmä sekä asiakasportaali domain- ja DNS-palveluille. Tavoitteena on korvata manuaalisia ja virhealtteita prosesseja, parantaa tietoturvaa ja vastata kyberturvallisuuslain vaatimuksiin ottamalla käyttöön mm. pakollinen kaksivaiheinen tunnistautuminen ja tehostettu pääsynhallinta. Hanke vahvistaa asiakkaiden palveluiden hallinnan turvallisuutta ja luotettavuutta.
AWAKE.AI Oy	76 329	Tietoturvallinen ja skaalautuva käyttäjän todennus- ja käyttöoikeusjärjestelmä Awake.AI -alustalle	Hankkeessa rakennetaan moderni skaalautuva ja turvallinen käyttäjien sekä sovellusten todennus- ja käyttöoikeusjärjestelmäjärjestelmä Awake.AI:n pilvialustalle. Ratkaisu perustuu avoimen lähdekoodin Keycloak-teknologiaan, ja sen tavoitteena on parantaa alustapalvelun kyberturvallisuutta, mahdollistaa kansainvälinen skaalautuvuus sekä täyttää NIS2- ja EU:n digitaalisen identiteetin vaatimukset.
Ellego Powertec Oy	40 652	Tietoverkon valvonnan automatisointi ja tietoturvan prosessikehitys	Yritys automatisoi tietoverkon valvonnan ja kehittää liiketoiminnan palautumis- ja kriisinhallintakäytäntöjä.

ElmoNet Oy	53 643	Tukiasema- ja telekeskuspaikkojen fyysisen turvallisuuden sekä omaisuuden suojaamiseen tähtäävä hanke.	Tukiasema- ja telekeskuspaikkojen fyysisen turvallisuuden sekä omaisuuden suojaamiseen tähtäävä hanke. Hankkeessa asennetaan teletiloihin tekoälypohjainen hälytys- ja kameravalvontajärjestelmä sekä aidataan merkittävät tukiasemakohteet. Hankkeen vaikutus kyberturvallisuuslain 9§ mukaiseen toiminnan kehittämiseen; 1) pääsynhallinnan ja todentamisen menettelyt, 2) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi ja 3) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen.
Enerim Oy	48 350	Net2026	Net2026-hanke on Enerim Oy:n käynnistämä kehitysprojekti, jonka tavoitteena on vahvistaa energia-alan tietoturvaa ja varautumista kyberuhkiin Suomessa. Hankkeessa toteutetaan muun muassa verkon segmentointia, pääkäyttäjäoikeuksien hallintaa sekä kriisinhallintaharjoituksia yhteistyössä alan toimijoiden kanssa. Näillä toimenpiteillä parannetaan koko energia-alan toimintavarmuutta ja huoltovarmuutta, mikä hyödyttää sekä yritystä että yhteiskuntaa laajemmin.
Envor Group Oy	77 287	Envor Kyberturva 2026	Hankkeessa vahvistetaan Envor Groupin kyberturvallisuutta ja riskienhallintaa kyberturvallisuuslain vaatimusten mukaisesti. Toimenpiteillä parannetaan tietojärjestelmien ja toimitusketjun turvallisuutta sekä kehitetään henkilöstön kyberturvallisuusosaamista ja jatkuvuudenhallintaa.
Hangon Satama - Hangö Hamn Oy Ab	48 949	ISO ASKEL - 991753	Hangon Satama – Hangö Hamn Oy Ab:n hanke keskittyy sataman kyberturvallisuuden ja riskienhallinnan kehittämiseen vastaamaan kansallisen lainsäädännön ja Traficomin suositusten vaatimuksia. Hankkeessa rakennetaan ja otetaan käyttöön tietoturvan hallintajärjestelmä sekä toteutetaan konkreettisia toimenpiteitä viestintäverkkojen ja

			tietojärjestelmien suojaamiseksi ja toimitusketjun riskienhallinnan parantamiseksi.
Haukiputaan Sähköosuuskunta	43 153	Haukiputaan Sähköosuuskunnan kyberturvallisuuden kehittäminen	Hankkeen tavoitteena on saavuttaa kyberturvallisuuslain, sekä vallitsevan uhkakentän edellyttämä IT/OT- infrastruktuurin kybersuojauksen taso ja tämän 24/7- jatkuva valvonta ja reagointikyvykkyydet.
Haverinen Logistics Oy	14 984	Haverinen Logistics Oy - Kyberresilienssi 2026: Teknologian, prosessien ja osaamisen kehityshanke	Hankkeessa parannetaan Haverinen Logistics Oy:n kyberturvallisuutta ja toiminnan jatkuvuutta kyberturvallisuuslain (124/2025) vaatimusten mukaisesti. Kehitämme teknistä suojausta, varmuuskopiointia sekä henkilöstön osaamista, mikä vahvistaa logistiikkapalveluidemme ja yhteiskunnan kriittisen infrastruktuurin häiriönsietokykyä.
ICT Elmo Oy	46 323	SOC tietoturvakeskus 24-7	Hankkeessa otetaan käyttöön 24/7 toimiva SOC-palvelu (Security Operations Center), joka valvoo organisaation ICT-infrastruktuuria ja tietoturvatapahtumia jatkuvasti. Tavoitteena on parantaa tietoturvan valvontaa, havaita poikkeamat reaaliaikaisesti ja varmistaa nopea reagointi mahdollisiin uhkiin.
Iin Energia Oy	52 912	Iin Energia: Kyberturvallisuuden kehittäminen	Hankkeen tavoitteena on saavuttaa Iin Energialla kyberturvallisuuslain, sekä vallitsevan uhkakentän edellyttämä IT/OT- infrastruktuurin kybersuojauksen taso ja tämän 24/7-jatkuva valvonta ja reagointikyvykkyydet.
KaseNet Oy	63 038	KaseNet kyberturvan kehittämisen hanke	Tietoturvallisuuden hallintajärjestelmän (ISMS) käyttöönotto. ISO27001 sertifiointi.
Koillis-Satakunnan Sähkö Oy	37 716	Viestintäverkkojen segmentoinnin ja jatkuvuuden kehittäminen	Sähkönjakelun sekä toimistoympäristön verkkojen segmentoinnin ja jatkuvuuden edelleenkehittäminen.
Kokemäen Sähkö Oy	12 908	Ulkoisen verkon penetraatiotestaus sekä kriittisen	Penetraatiotestauksessa pyritään saamaan pääsy verkon yli Kokemäen Sähkön laitteisiin ja järjestelmiin. Palautusharjoituksessa

		järjestelmän palautusharjoitus	harjoitellaan liiketoiminnalle kriittisen järjestelmän varmuuskopion palautus.
Kokkolan Satama Oy	50 424	Kyberturvallisuuden parantaminen Kokkolan Satama Oy:ssä	Hankkeen tavoitteena on toteuttaa kyberturvallisuuslaissa asetetut vaatimukset ja nostaa organisaation kyberturvallisuustaso vastaamaan nykypäivän uhkia. Hanke sisältää teknisen ympäristön kehittämistä, henkilöstön kouluttamista, prosessien ja tietoturvapolitiikkojen rakentamista sekä kyberturvallisuutta tukevien järjestelmä- ja henkilöstöresurssien vahvistamista.
Kustannus Oy Duodecim	36 126	Tietoturvan vaatimustenmukaisuuden, riskienhallinnan ja pääsynhallinnan kehittämishanke	Hankkeen tavoitteena on kehittää ja systematisoida tietoturvan hallintaa, vahvistaa vaatimustenmukaisuuden ja riskienhallinnan seurantaa, parantaa ohjelmistokehityksen elinkaaren tietoturvaa sekä kehittää menetelmiä ohjelmistokehitykseen liittyvien riskien tunnistamiseen ja lieventämiseen. Lisäksi hankkeessa kehitetään sekä sisäisten että ulkoisten käyttäjien pääsynhallinnan tietoturvaa.
Louhi Net Oy	100 000	Louhi DNSSEC-Valmius: Suomalaisen digitaalisen ekosysteemin perustusten vahvistaminen	Louhi Net Oy on kansallisesti merkittävä digitaalisen infrastruktuurin toimija, joka tarjoaa verkkotunnus- ja nimipalveluita kymmenille tuhansille suomalaisille yrityksille ja yhteisöille, mukaan lukien monille yhteiskunnan kannalta kriittisille toimijoille. Nimipalvelujärjestelmä (DNS) on internetin peruskivi, mutta samalla haavoittuvainen kohta. Sen suojaaminen on välttämätöntä koko digitaalisen toimitusketjun turvaamiseksi.
Magic Cloud Oy	100 000	Magic Cloudin kyberresilienssin vahvistaminen	Hanke parantaa Magic Cloud Oy:n kyberturvallisuuden ja riskienhallinnan kypsyystasoa vastaamaan uuden kyberturvallisuuslain (124/2025) 9 §:n vaatimuksia. Hankkeessa kehitetään erityisesti valvontatoimintoja ja riskienhallin-taa sekä toteutetaan kattavia kehitystoimia Magic Cloudin verkko- ja pilvi-infrastruktuurin suojaamiseksi, henkilöstön osaamisen vahvistamiseksi ja hallintamallien päivittämiseksi. Samalla vahvistetaan kyberresilienssiä mm. parantamalla poikkeamien

			havaitsemista ja palautumissuunnitelmia. Asiakasnäkökulmasta tämä tarkoittaa muun muassa parempaa palvelujen käytettävyyttä ja jatkuvuutta, lyhyempiä katkoja sekä läpinäkyvää häiriöviestintää. Tavoitteena on varmistaa, että Magic Cloud hallitsee tehokkaasti kyberriskejä ja pystyy minimoimaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvien uhkien haitalliset vaikutukset.
Mico Botnia Oy Ab	10 000	NIS2-direktiivin käyttöönotto Mico Botnia Oy:ssä	Mico Botnia Oy ottaa käyttöön Digiturvamallipalvelun NIS2-direktiivin vaatimusten täyttämiseksi ja kyberturvallisuuden hallinnan systematisoimiseksi. Kehittämishankkeen tuloksena syntyy pysyvä toimintamalli, joka parantaa kyberturvallisuutta ja varautumiskyvykkyyttä.
Mylab Oy	100 000	Kyberturvallisuushanke 2026	Kyberturvallisuushanke 2026 kehittää Mylab Oy:n valmistamien terveydenhuollon laboratoriojärjestelmien ja niihin liittyvien lääkinnällisten laitteiden tietoturvaa, parantaen yhteiskunnan kriisinkestävyyttä ja ennaltaehkäisten palveluiden saavutettavuuden häiriöitä. Hankkeessa rakennetaan mm. systemaattinen tietoturvan hallintajärjestelmä, joka täyttää esim. kyberturvallisuuslain ja NIS2-direktiivin vaatimukset.
OpSec Oy	36 604	Projekti Aallonmurtaja	Hankkeen tavoitteena on parantaa OpSec Oy:n ylläpito- ja pilvipalveluiden kyberturvallisuutta sekä riskienhallintaa. Hanke toteuttaa rahoitustuen käyttötarkoitusta kehittämällä prosesseja, jotka vähentävät palvelukatkosten, tietomurtojen ja inhimillisten virheiden riskiä. Hankkeessa keskitytään tunnistettuihin riskeihin käyttöpalveluiden.
Oulun Autokuljetus Oy	39 882	Toimitusketjujen kyberturvallisuuden kehittäminen	Hankkeella parannetaan toimitusketjujen turvallisuutta kehittämällä tietoverkkojen rakennetta ja lisäämällä avainhenkilöiden ja muun henkilökunnan kyberturvallisuustietoisuutta.
Prog-It Oy	46 787	Kati-projekti	Hankkeessa laaditaan toimintatapa ja prosessi, joka tukee kyberuhkiin varautumista sekä ehkäisee niiden toteutumista. Osana

			hanketta laaditaan myös henkilöstön roolipohjainen osaamis- ja vastuumalli sekä suunnitelma yhtiön henkilöstön kyberturvallisuusosaamisen tason nostamiseksi.
Puhas Oy	17 699	Puhas Oy:n kyberturvallisuuden kehittämishanke	Puhas Oy:n kyberturvallisuuden kehityshankkeella parannetaan organisaation kokonais- ja kyberriskienhallintaa sekä parannetaan kykyä täyttää kyberturvallisuuslain vaatimukset.
Raseborgs Energi Ab	12 422	Suojatut etäyhteydet operatiivisissa verkoissa (OT)	Hankkeen tavoitteena on kehittää kyberturvallinen etäyhteysratkaisu operatiivisille verkoille (OT) mahdollistamalla suojattu yhteys, joka ei vaaranna verkkojen toimintaa tai eheyttä. Ratkaisun tavoitteena on suojella kriittisiä järjestelmiä kyberuhkilta ja samalla helpottaa etäseurantaa ja -valvontaa.
Rovakaira Oy	29 512	Turvallisen verkkoarkkitehtuurin kehittämishanke	Tuotanto tietoliikenneverkon uudelleen suunnittelu ja kyberturvallisuustason nosto.
S1 Networks Oy	89 207	Kyberturvallisuuden kehittäminen ja kyberturvallisuuslain toimeenpano S1 Networksissa	S1 Networks Oy kehittää toimintaansa kyberturvallisuuslain vaatimusten mukaiselle tasolle parantamalla riskienhallintaa, hallinnollista tietoturvaa ja poikkeamailmoituskäytäntöjä. Tavoitteena on vahvistaa yrityksen tietoliikenne- ja pilvipalveluiden kyberturvallisuutta, häiriönsietokykyä sekä varmistaa toiminnan jatkuvuus osana yhteiskunnan kriittistä digitaalista infrastruktuuria.
Turun seudun puhdistamo Oy	15 194	Kyberturvallisuuden pelikirjat	Hankkeessa kehitämme kyberturvallisuuttamme ja riskienhallintaa kyberturvallisuuden pelikirjoilla. Pelikirjat auttavat meitä toteuttamaan käytännössä helposti, säännöllisesti ja mitattavasti kyberturvallisuuslain vaatimia toimenpiteitä.
Turun Seudun Vesi Oy	14 445	OT-ympäristön kyberturvallisuuden kehittäminen	Hankkeen aikana otetaan käyttöön Turun Seudun Vesi Oy:n automaatiojärjestelmän keskitetty lokienhallinta sekä järjestetään

			automaatioon kohdistuvaa kyberturvallisuus-koulutusta.
Turun Vesi-huolto Oy	44 731	Turun Vesihuolto Oy - Kyberturvalli-suuden paranta-minen	Hankkeen tavoitteena on saavuttaa Turun Vesihuolto Oy:llä kyberturvallisuuslain, sekä uhkakentän edellyttämä kypsyystaso IT/OT-infrastruktuurin suojaukseen. Hankkeessa otetaan käyttöön Microsoft Posture Manage-ment- palvelu, TI- kyberuhkien metsästämi-nen sekä jatkuvaluonteinen arviointi ja hal-linta.
Vestia Oy	42 279	Vestia Kyberturva 2026	Vestialla tietoturva- ja tietosuojatyö on ha-jautunut mikä johtaa hallinnan tehottomuu-teen ja kyberturvallisuustyön epäsäännölli-seen tekemiseen. NIS2-direktiivi ja Trafico-min rahoitustuen ehdot edellyttävät syste-maattista kehittämistä. Hankkeen tarkoituk-sena on nostaa Vestian kyberturvallisuustaso kansallisten vaatimusten mukaiseksi ja var-mistaa jatkuvuus.
Westenergy Oy	23 243	Atea Defense Vali-dation -palveluko-konaisuus	Jatkuvuudenhallintaa panostamalla jatkuva-luonteiseen penetraatiotestaukseen, identi-teettipalvelun ja verkon segmentointiin, MS Applockerin hyödyntämiseen sekä AD Tier -malliin, jolla pyritään ehkäisemään mahdolli-sen hyökkääjän lateraalinen liikkuminen tie-toliikenneympäristössämme.
Wisenetwork Oy	76 414	WiseNetwork – Kyberturvallisuu-den ja SaaS-re-silienssin kehitys-hanke	WiseNetwork Oy toteuttaa Traficomin rahoi-tustuella kyberturvallisuuden kehityshank-keen, jonka tavoitteena on nostaa yhtiön ja sen tarjoamien SaaS-palveluiden turvalli-suustasoa ja resilienssiä. Hanke vahvistaa kykyämme suojata satojen suomalaisten PK-yritysten käyttämiä kriittisiä järjestelmiä. In-vestoimalla kattavasti teknologiaan, proses-seihin ja henkilöstön osaamiseen varmis-tamme palveluidemme luotettavuuden ja vastaamme tiukentuviin lainsäädännöllisiin vaatimuksiin.
Xetpoint Oy	23 449	DDoS suojaus	DDoS-suojauksen kehittämishanke