Bendrai finansuoja Europos Sąjunga

INFORMACIJA APIE PASIRAŠYTAS KVIETIMO NR. CYBER-K02 „LABAI MAŽŲ, MAŽŲ IR VIDUTINIŲ ĮMONIŲ KIBERNETINIO ATSPARUMO DIDINIMAS“ PAGAL 2021–2027 M. SKAITMENINĖS EUROPOS PROGRAMOS 3 KONKRETŲ TIKSLĄ „KIBERNETINIS SAUGUMAS IR PASITIKĖJIMAS“ PROJEKTŲ ĮGYVENDINIMO SUTARTIS

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
UAB Flux pay ai	Vilnius	Kibernetinis Skydas	CYBER-K02-001	61 585,20	46 188,90	2025-08-04	2025-12-31	*Projekto tikslas*: įgyvendinti visapusišką kibernetinio saugumo programą įmonėje, siekiant sustiprinti įmonės atsparumą kibernetinėms grėsmėms, išlaikyti aukštą klientų duomenų ir finansinių operacijų saugumo lygį, apsaugoti įmonės reputaciją ir klientų pasitikėjimą, užtikrinti verslo tęstinumą, atitikti teisinius reikalavimus. *Projekto veiklos*: • Automatizuotos rizikų stebėsenos sistemos, automatizuotos incidentų valdymo sistemos, prieigos kontrolės ir slaptažodžių valdymo sistemos,

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								daugiafaktorės autentifikacijos sistemos, ugniasienės ir įsilaužimo aptikimo sistemos, saugumo stebėsenos sistemos ir šifravimo priemonės diegimas. • Dokumentų parengimas incidentų valdymo ir prieigos kontrolės bei slaptažodžių valdymo sistemų diegimui. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Thinking Organisations	Palanga	UNLOCK Test AI platformos kibernetinio atsparumo didinimas	CYBER-K02-002	54 315,70	40 735,70	2025-08-01	2025-12-31	*Projekto tikslas*: įmonės kibernetinio atsparumo didinimas sumažinant visas dabar nepriimtinas kibernetinio saugumo rizikas iki priimtino lygio. *Projekto veiklos*: • Kompiuterinių darbo vietų atnaujinimas. • Centralizuoto įrenginių valdymo ir atnaujinimų įdiegimas M365 aplinkoje. • Įmonės internetinės svetainės ir UNLOCK informacinės sistemos atsparumo įsilaužimams padidinimas suprogramuojant saugumo reikalavimus atitinkančias savybes.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• UNLOCK informacinės sistemos pažeidžiamumų vertinimas ir įsilaužimo testas. • Įmonės saugumo dokumentacijos ir procesų paruošimas ISO/IEC27001 sertifikavimui. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Attrel	Vilnius	UAB Attrel kibernetinio saugumo sistemos stiprinimas, atitikties NIS2 ir BDAR reikalavimams užtikrinimas	CYBER-K02-009	44 530,60	30 490,60	2025-08-02	2025-12-31	*Projekto tikslas*: sustiprinti UAB „Attrel“ kibernetinio saugumo sistemą ir užtikrinti ilgalaikį atitikimą NIS2 direktyvai, BDAR ir ISO 27001 standartui, įgyvendinant pažangias apsaugos priemones nuo DDoS atakų, socialinės inžinerijos, duomenų nutekėjimo bei kitų kibernetinių grėsmių. *Projekto veiklos*: • Ugniasienių, internetinių sistemų apsaugos sprendimų, žurnalo duomenų analizės sprendimo, agentų stebėsenos ir automatinio IOC grėsmių identifikavimo sprendimo įsigijimas ir diegimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
ANNVERY, UAB	Vilnius	UAB „Annvery“ tinklų ir informacinės sistemos kibernetinio atsparumo didinimas pagal NIS2 direktyvos ir Kibernetinio saugumo įstatymo reikalavimus	CYBER-K02-011	42 091,60	31 257,22	2025-08-01	2025-12-31	*Projekto tikslas*: padidinti UAB „Annvery“ kibernetinį atsparumą, įdiegti modernias kibernetinio saugumo priemones ir užtikrinti atitiktį NIS2 direktyvai bei Kibernetinio saugumo įstatymo reikalavimams. *Projekto veiklos*: • SIEM sistemos, prieigos valdymo sistemos (IAM), VPN/šifravimo sprendimo, atsarginių kopijų (backup) sprendimo bei ugniasienių įsigijimas ir diegimas. • Kibernetinio saugumo politikos ir dokumentacijos parengimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
SCODING, UAB	Kaunas	UAB Scoding kibernetinio atsparumo didinimas pagal NIS2 direktyvą ir ISO 27001 standartą	CYBER-K02-012	54 306,97	40 328,36	2025-08-05	2025-12-31	*Projekto tikslas*: padidinti UAB „Scoding“ kibernetinį atsparumą, užtikrinant atitiktį NIS2 direktyvai, ISO 27001 standartui ir Kibernetinio saugumo įstatymo reikalavimams, įdiegiant pažangius kibernetinio saugumo sprendimus.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								Projekto veiklos: • SIEM sistemos, ugniasienės, prieigos valdymo sistemos (IAM), duomenų atsarginių kopijų sprendimo bei duomenų šifravimo / VPN sprendimo įsigijimas ir diegimas. • Kibernetinio saugumo politikos ir dokumentų pagal ISO/IEC 27001 bei NIS2 reikalavimus parengimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Omniget	Vilnius	UAB Omniget kibernetinio saugumo sprendimų diegimas, didinantis įmonės kibernetinį atsparumą	CYBER-K02-013	80 238,84	59 238,84	2025-08-18	2025-12-31	*Projekto tikslas*: sustiprinti UAB „OmniGet“ kibernetinį saugumą, apsaugoti verslui kritiškai svarbią informaciją, duomenų bazes bei programinę įrangą nuo aktualių kibernetinių grėsmių. *Projekto veiklos*: • Automatizuotos bot’ų ir elgsenos atpažinimo sistemos, turinio tikrinimo, infrastruktūros architektūros pertvarkymo, žalingo JavaScript turinio analizės sistemos, moderavimo sprendimo, IP adresų filtravimo ir prisijungimų kontrolės sistemos, automatizuotos sistemų

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								atstatymo infrastruktūros ir periodinio testavimo funkcionalumo diegimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
Abirankis, UAB	Kaunas	Kibernetinio saugumo didinimas UAB „Abirankis“	CYBER-K02-022	61 704,26	46 278,19	2025-08-04	2025-12-31	*Projekto tikslas*: užtikrinti UAB „Abirankis“ informacinių sistemų ir tinklų kibernetinį atsparumą, įdiegiant saugią, Apple ekosistemai pritaikytą infrastruktūrą, centralizuotą įrenginių valdymą, saugios prieigos ir kodo kūrimo aplinką bei stiprinant darbuotojų gebėjimus valdyti kibernetines grėsmes, siekiant pašalinti aukšto lygio rizikas, nustatytas kibernetinio saugumo vertinime. *Projekto veiklos*: • Serverio, nešiojamųjų kompiuterių, nepertraukiamo maitinimo šaltinio, Device Management Software, debesijos paslaugų paketo, apimančio saugų el. paštą, dokumentų dalijimąsi, 2FA autentifikaciją, SSO integraciją, duomenų šifravimą ir administravimo

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								įrankius, VPN programinės įrangos, ir slaptažodžių saugyklos įsigijimas. • Serverių ir kompiuterių konfigūravimas, infrastruktūros parengimas, diegimas, mokymai naudotis nauja infrastruktūra. • Kibernetinio saugumo mokymai įmonės darbuotojams.
Dicto Citius, UAB	Kaunas	DICTO CITIUS kibernetiniam atsparumui didinti reikalingų kibernetinio saugumo priemonių įsigijimas ir diegimas	CYBER-K02-023	75 200,00	56 400,00	2025-08-04	2025-12-31	*Projekto tikslas*: didinti DICTO CITIUS kibernetinį atsparumą. *Projekto veiklos*: • Pažeidžiamumų nustatymo įrangos, centralizuoto slaptažodžių valdymo sprendimo, DLP sprendimo, centralizuoto KDV įrenginių valdymo, MDM sprendimo kompiuterizuotoms darbo vietoms, apsaugos nuo kenkėjiško programinio kodo, centralizuoto saugumo sprendimo tinklo perimetro apsaugai ir standartizuotam valdymui, tinklo stebėsenos sistemos bei 2FA įsigijimas ir diegimas. • IT dokumentacijos bei procesų kūrimas ir atnaujinimas.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Tinklo įrangos parametrų peržiūra ir standartizacija. • Naudotojų teisių politikos peržiūra ir vykdymas centralizuotam saugios prieigos ir naudotojų autentifikacijos valdymui. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Pelno valdymas	Vilnius	UAB Pelno valdymas kibernetinio saugumo sprendimų diegimas, didinantis įmonės kibernetinį atsparumą	CYBER-K02-027	75 802,57	54 802,57	2025-08-11	2025-12-31	*Projekto tikslas*: sustiprinti UAB „Pelno valdymas“ kibernetinį saugumą, apsaugoti verslo valdymo sistemą, duomenų bazes bei naudotojų paskyras nuo aktualių kibernetinių grėsmių. *Projekto veiklos*: • Dviejų faktorių autentifikacijos (2FA), neįprastų prisijungimų atpažinimo sistemos, verslo valdymo sistemos įskiepių atnaujinimų registro, DDoS apsaugos sprendimo verslo valdymo sistemai diegimas, antivirusinės programinės įrangos ir ugniasienės įsigijimas ir diegimas. • Verslo valdymo sistemos atsarginių kopijų kūrimas į atskirą saugyklą.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Vartotojų atliekamų veiksmų registro funkcionalumo ir slaptažodžių sudėtingumo užtikrinimo ir pakartotinių slaptažodžių naudojimosi kontrolės programavimas įmonės verslo valdymo sistemoje. • Maršrutizatoriaus ir belaidžio interneto tinklo konfigūracija. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Grand ERP	Kaunas	UAB Grand ERP kibernetinio saugumo sprendimų diegimas, didinantis įmonės kibernetinį atsparumą	CYBER-K02-037	52 673,47	38 673,47	2025-08-04	2025-12-31	*Projekto tikslas*: sustiprinti UAB „Grand ERP“ kibernetinį saugumą, užtikrinant verslo valdymo sistemos, duomenų bazių, naudotojų paskyrų ir tinklo infrastruktūros apsaugą nuo aktualių vidinių ir išorinių kibernetinių grėsmių. *Projekto veiklos*: • Privilegijuotų paskyrų valdymo sprendimų ir programinės įrangos atnaujinimų sistemos diegimas. • Wi-Fi tinklo saugumo stiprinimas. • Fizinio serverio apsaugos, kompiuterių ir mobiliųjų įrenginių apsaugos diegimas.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Buvusių darbuotojų prieigos valdymo sprendimų diegimas. • Įmonės duomenų ir klientų duomenų apsaugos sprendimų diegimas. • Išorinių serverių saugumo stiprinimas. • Dokumentacijos parengimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Fintegry	Vilnius	UAB Fintegry įmonės kibernetinio saugumo didinimas	CYBER-K02-038	75 824,00	56 674,00	2025-08-01	2025-12-31	*Projekto tikslas*: didinti organizacijos kibernetinį atsparumą, pašalinti TIS rizikos vertinimo ataskaitoje identifikuotas reikšmingas grėsmes bei pasirengti įgyvendinti Skaitmeninės veiklos atsparumo reglamento (DORA) reikalavimus. *Projekto veiklos*: • Pažeidžiamumų skanavimo sprendimo, WAF ir DDoS filtravimo sprendimų interneto svetainei, išplėstinių aptikimo ir atsako (XDR), ugniasienės, el. pašto, atsarginių kopijų bei slaptažodžių valdymo sprendimų diegimas.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Išorinio ir vidinio įsilaužimo testavimas. • DORA atitikties vertinimas, trūkumų šalinimo plano parengimas, dokumentų (politikos, procedūros, planai) sukūrimas ar atnaujinimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
UAB Dineta	Kaunas	UAB Dineta įmonės kibernetinio saugumo didinimas	CYBER-K02-043	77 795,70	58 263,70	2025-08-04	2025-12-31	*Projekto tikslas*: padidinti UAB „Dineta“ kritinių IT sistemų (interneto svetainių, CRM, debesijos infrastruktūros) kibernetinį atsparumą, įdiegus pažangius technologinius sprendimus, skirtus grėsmių stebėsenai, atpažinimui, neutralizavimui bei prieigos valdymui, taip pat stiprinant organizacijos kibernetinio saugumo kultūrą per darbuotojų mokymus, atitinkančius Kibernetinio saugumo įstatymo 14 straipsnio 5 dalies reikalavimus. *Projekto veiklos*: • Interneto svetainės apsaugos diegimas.

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Debesijos pagrindu veikiančios interneto svetainių priežiūros paslaugos diegimas. • Apsaugos nuo DDoS atakų, 2 dviejų faktorių autentifikacijos (2FA) įmonės sistemų aplinkose diegimas. • 2 išsamūs informacinių sistemų saugumo testavimai (penetraciniai testai) įmonės sistemose, identifikuotų technologinių pažeidžiamumų pašalinimas, pakartotinis testavimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.
MB „Alvsim Consulting“	Vilnius	Kibernetinio saugumo didinimas MB „Alvsim Consulting“	CYBER-K02-051	49 858,96	37 394,22	2025-08-05	2025-12-29	*Projekto tikslas*: sustiprinti MB „Alvsim Consulting“ kibernetinį atsparumą, įdiegiant pagrindines tinklų ir informacinės sistemos saugumo valdymo priemones, skirtas apsaugoti įmonės IT infrastruktūrą, vartotojų prieigą ir duomenis nuo vidinių bei išorinių grėsmių, taip užtikrinant atitiktį teisės aktų reikalavimams ir verslo tęstinumą. *Projekto veiklos*:

Projekto vykdytojo pavadinimas	Projekto vykdytojo adresas	Projekto pavadinimas	Projekto kodas	Projekto tinkamų finansuoti išlaidų suma, Eur	Projektui skirtų finansinės paramos lėšų suma, Eur	Projekto įgyvendinimo sutarties pasirašymo data	Projekto įgyvendinimo terminas	Trumpas projekto aprašymas
								• Valdomo konteinerių klasterio, aplikacijų srautų paskirstymo sistemos, valdymo prieigos tunelio, interneto aplikacijų ugniasienės (WAF), rakto valdymo sistemos, objektinio duomenų saugojimo sprendimo, centralizuoto logų ir metrikų surinkimo sprendimo, valdomų metrikų surinkimo sprendimo diegimas, vizualizacijos platformos, NoSQL duomenų bazės konfigūracijų, naudotojų ir logų saugojimui, duomenų perdavimo (iki 100 GB) sprendimo bei naudotojų tapatybės valdymo decentralizuotoje infrastruktūroje diegimas. • Sprendimų konfigūravimas, testavimas, diegimas. • Informacijos saugumo valdymo sistemos (ISVS) sukūrimas ir įdiegimas. • Kibernetinio saugumo mokymai įmonės darbuotojams.