

CYSSME Pristatymas

Kibernetinis saugumas MVĮ

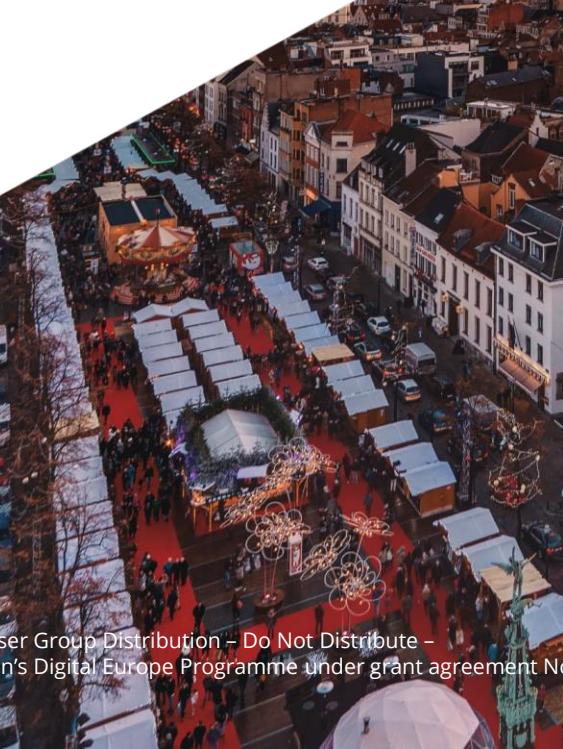
Jaroslav Urbanovič, L3CE
2024 gegužės 8, Vilnius



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



© CYSSME – LSEC, 2024, Private & Confidential – Closed User Group Distribution – Do Not Distribute –
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101



CYSSME
CyberSecurity and Data Protection for Small Medium and Micro Enterprises

KIBERNETINIO SAUGUMO SITUACIJA MVĮ



57%

mažųjų ir vidutinių
įmonių patyrė
kibernetinio saugumo
pažeidimą



26%

vidutinių įmonių per
pastaruosius 12 mėnesių
patyrė elektroninių
nusikaltimų



> \$500K

„Duvel“ atvejis:
įsilauželiai pareikalavo
daugiau nei pusės
milijono dolerių

Sources <https://guardz.com/go/survey/> - 2023 - Cyber security breaches survey 2023 – De Morgen, 2024

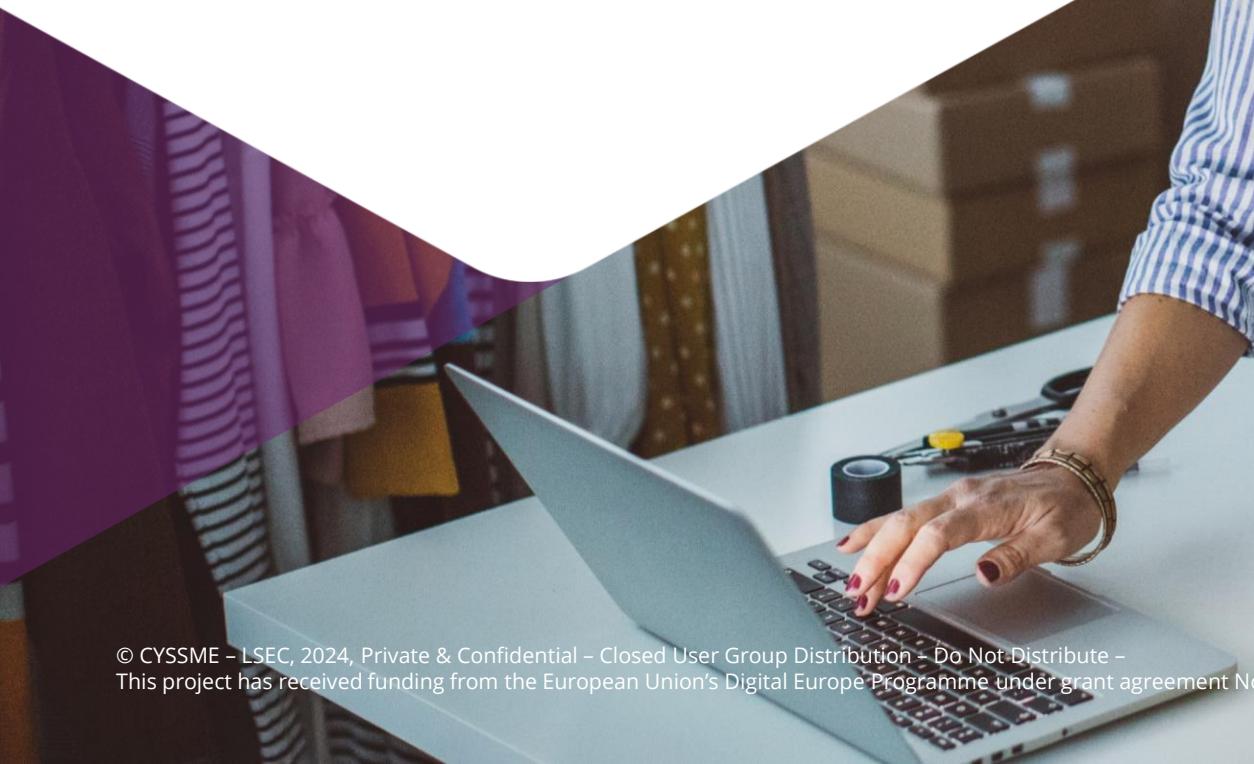
KIBERNETINIO SAUGUMO SITUACIJA MVĮ

- Labai mažos įmonės dažniausiai auditui atlikti **pasitelkia tik vidaus darbuotojus** (44 proc. labai mažų įmonių, kuriose atliekamas bet kokio tipo auditas).
- Mažosios įmonės yra labiausiai linkusios (45 proc.) **naudotis išorės rangovų** paslaugomis.
- Vienas iš dažnų elgsenos modelių tarp organizacijų, kurios suformavo aiškią strategiją, yra **kibernetinio saugumo atskyrimas** nuo kitų skyrių, kaip IT ar administravimas.
- „**Išlaidos paprastai yra reaktyvios.** Jei yra problema, ji sprendžiama. Neturime biudžeto skirto kibernetiniams saugumui. Sunku įsivertinti poreikį, nes nežinome duomenų atakų masto ir jų kainos“, - pirkimų ir IT vadovas, maža įmonė.



Cyber security breaches survey 2023

CYSSME Tisklinės auditorijos ir metodas



© CYSSME – LSEC, 2024, Private & Confidential – Closed User Group Distribution – Do Not Distribute –
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101



Tikslinės auditorijos

E-KOMERCIJA

- Vidutinės
- Mažos
- Labai mažos



PRAMONĖ

- Vidutinės
- Mažos
- Labai mažos



AUKŠTOSIOS TECHNOLOGIJOS

- Vidutinės
- Mažos
- Labai mažos



KITOS

- Vidutinės
- Mažos
- Labai mažos



CYSSME Metodas

Kibernetinis saugumas Europos mažosioms bei vidutinėms įmonėms, naudojant Europinius kibernetinio saugumo sprendimus ir ekspertiškumą

20 000 Eur pagalba MVĮ



PARTNERIAI

 <p>AXS GUARD INTERNET SECURITY SOLUTIONS</p>	 <p>IT & SECURITY BA WE KNOW HOW!</p>	 <p>Ceeyu</p>	 <p>CROSS-BORDER CBCOMMERCE.EU</p>
 <p>CYBER TRUST AUSTRIA</p>	 <p>EXALENS®</p>	 <p>L3CE</p>	 <p>LSEC LEADERS IN SECURITY</p>
 <p>Lupasafe</p>	 <p>nocode-x</p>	 <p>TOREON Business driven cyber consulting</p>	 <p>unizo</p>

KIBERNETINIS SAUGUMAS YRA PROCESAS

Padedami žmonių ir technologijų, galite pagerinti savo padėtį. Galime padėti sužinoti, kur ir kaip, ir įvardinti prioritetus. CYSSME gali padėti priimti teisingus sprendimus, nustatyti prioritetus ir imtis veiksmų, kuriuos reikia atlikti.

KIBERNETINIO SAUGUMO BRANDOS DIDINIMAS

1

RYŠYS

Ne viskas susiję su technologijomis. Mums idomi Jūsų istorija

2

BRANDA

CYSSME nori padėti Jūsų verslui augti saugiai

3

TIKSLAI

Užtikrinkite komandos, operacijų ar tiekimo grandinės saugumą

4

ATITIKIMAS

NIS/2, CRA, ISO, GDPR, ... mūsų ekspertai Jums padės

1

PATARIMAS



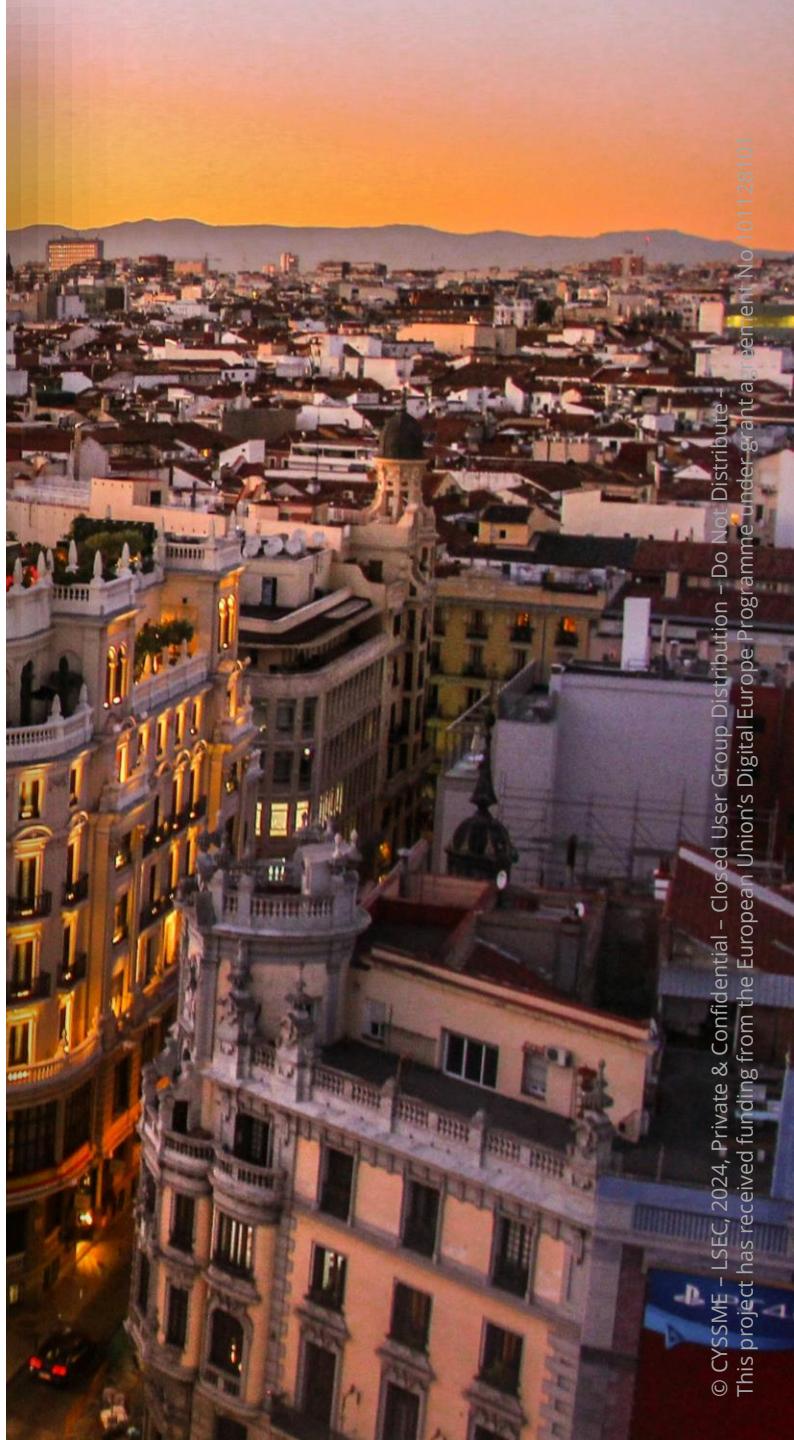
1

PATARIMAS

2

IDENTIFIKACIJA

- Turto pažeidžiamumų nustatymas
- Standartais pagrįsti vertinimai



1

PATARIMAS

2

IDENTIFIKACIJA

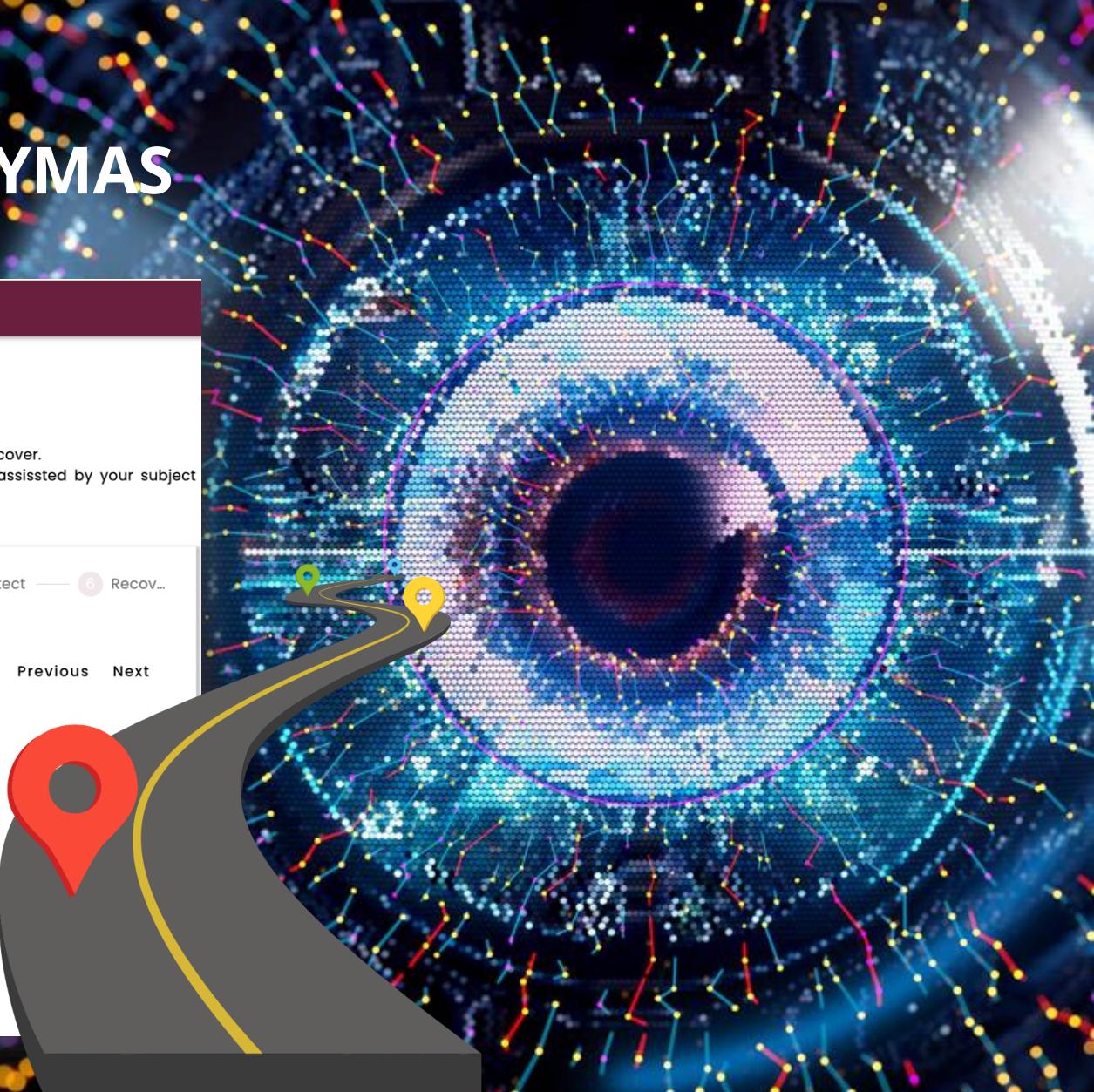
- Turto pažeidžiamumo nustatymas
- Standartais pagrįsti vertinimai

3

PREVENCIJA

- El. pašto, tinklo ir galutinių taškų rizikos
- Ugniasienė, aptikimas ir grėsmių valdymas

SAVO BRANDOS LYGIO NUSTATYMAS



CYBER FUNDAMENTALS

Survey results

Surveys

Company

Logout

Cyber fundamentals

Cyberfundamentals lets you assess in understandable laymens terms your cyber resilience. It will help to identify your maturity on the 5 levels of identify, protect, detect, respond and recover. HOW TO: Read the statement and according to your personnal interpretation (perhaps assissted by your subject matter experts) estimate how much your organization is in line with the statement. Where 1 is very little and 5 is very good.

Ident... — Prote... — Protect (i... — **Protect (ii... — Detect — Recov...**

Previous Next

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.
The organization shall develop, document, and maintain a baseline configuration for its business-critical systems. *

1 2 3 4 5

The organization shall configure its business-critical systems to provide only essential capabilities; Therefore the baseline configuration shall be reviewed, and unnecessary capabilities disabled. *

1 2 3 4 5

PR.IP-2: A System Development Life Cycle to manage systems is implemented

KIBERNETINIO SAUGUMO BRANDOS DIDINIMAS

KIBERNETINIO SAUGUMO PASIŪLYMAS

Kibernetinis saugumas Europos mažosioms bei vidutinėms įmonėms, naudojant Europinius kibernetinio saugumo sprendimus ir ekspertiškumą

1

TINKLO SAUGUMAS

galite nedelsiant apsaugoti tinklą ir kompiuterius

2

TREČIŲJŲ ŠALIŲ RIZIKA

jūsų ir jūsų tiekėjų pažeidžiamumo matomumas

3

ATITIKTIES VALDYMAS

prietaisų skydelis ir pagrindiniai irankiai

4

PRAMONĖ

aptikimas, stebėjimas ir veikiančių prietaisų valdymas

Tai ne pabaiga

Daugiau informacijos (anglų kalba)
www.cyssme.eu

egidija@l3ce.eu
jaroslav@l3ce.eu



Co-funded by
the European Union

