TIS2 direktyva
Veiksmų planas

Evaldas Valūnas
Grupės vadovas, Saugumo sprendimų kompetencijos centras, Atea

TIS2. Kas tai ?

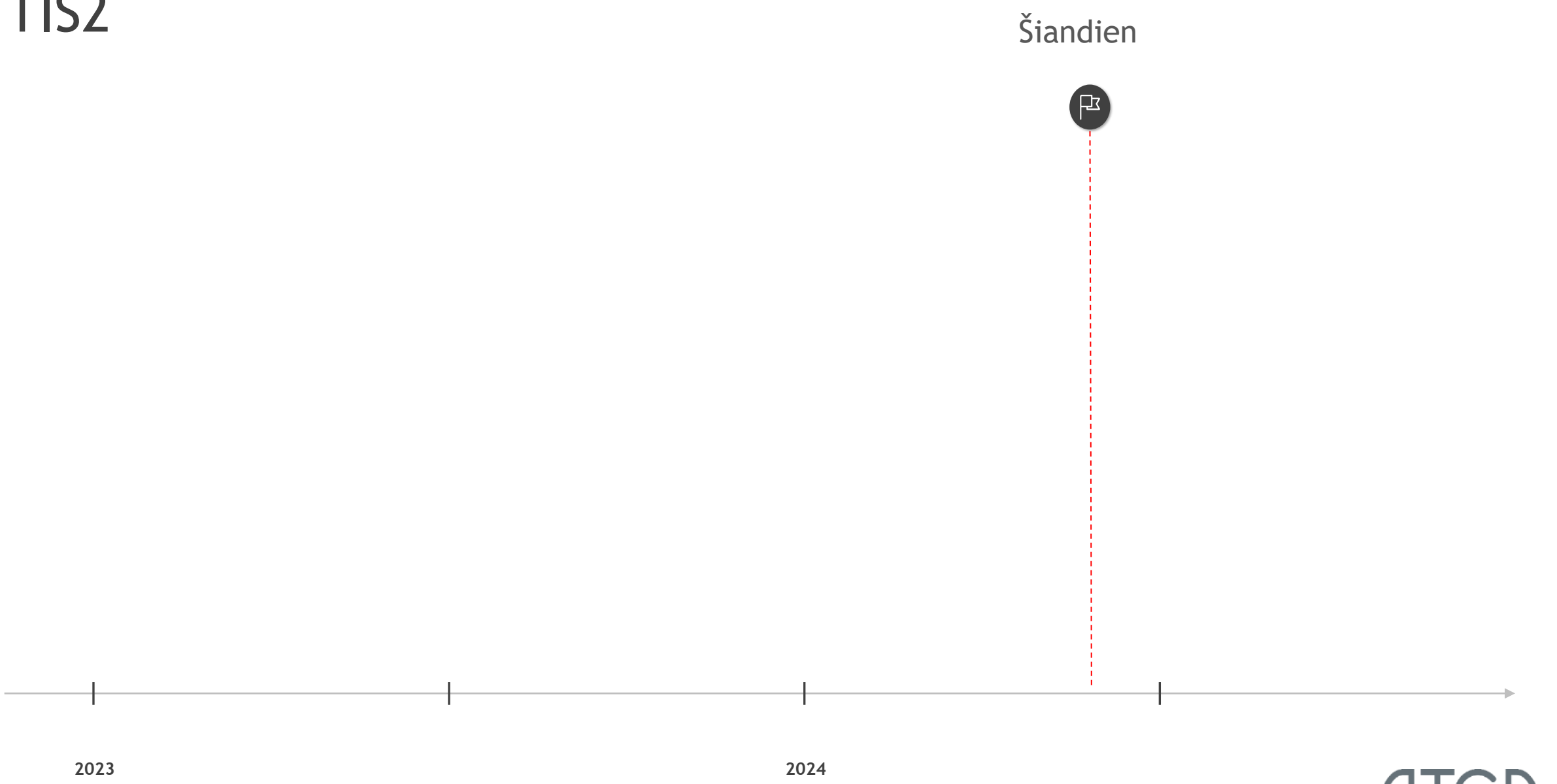
Direktyvos

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2016/1148
... dėl priemonių aukštam bendram **Tinklų ir Informacinių Sistemų** saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)

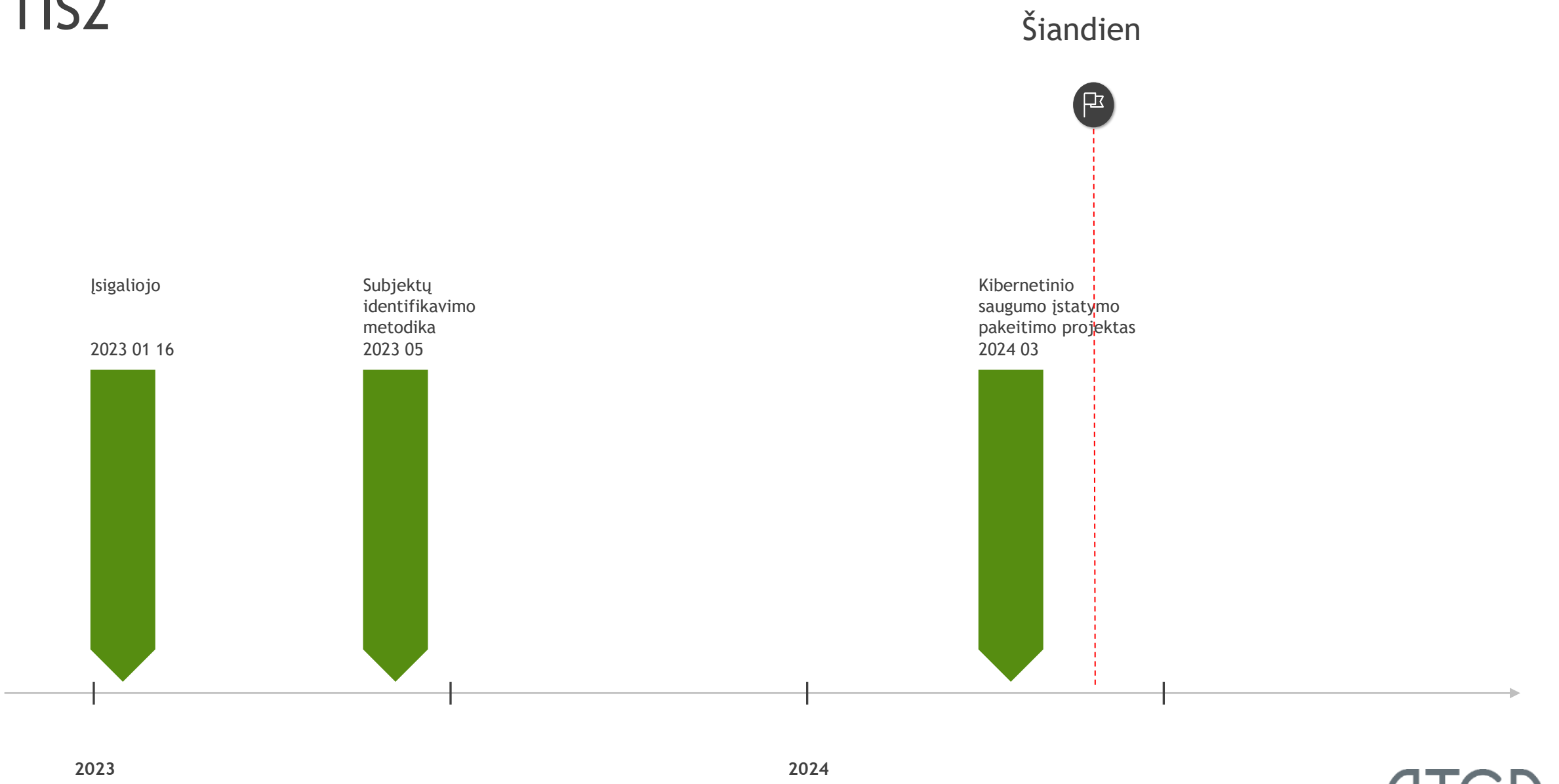
EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555
... dėl priemonių aukštam bendram **kibernetinio saugumo lygiui** visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas ... ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)

TIS2 įgyvendinimas

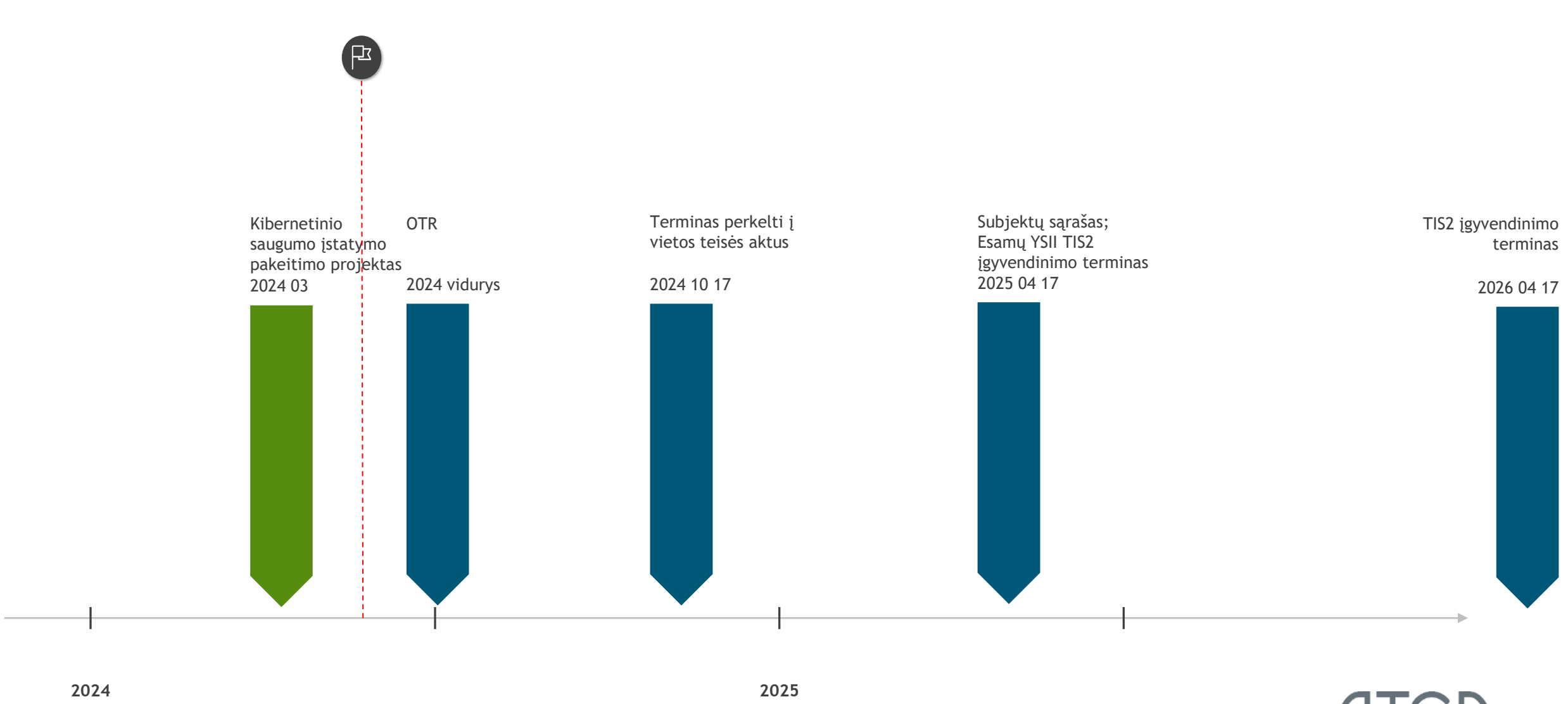
TIS2



TIS2


Šiandien
Įsigaliojo
2023 01 16
Subjektų identifikavimo metodika
2023 05
Kibernetinio saugumo įstatymo pakeitimo projektas
2024 03
2023
2024

TIS2


Šiandien
Kibernetinio saugumo įstatymo pakeitimo projektas
2024 03
OTR
2024 vidurys
Terminas perkelti į vietos teisės aktus
2024 10 17
Subjektų sąrašas; Esamų YSII TIS2 įgyvendinimo terminas
2025 04 17
TIS2 įgyvendinimo terminas
2026 04 17
2024
2025

TIS2 taikymo sritis

Subjektai (~ 4000 org.)

Esminių paslaugų tiekėjai

- Energetika (elektra, nafta, dujos, vandenilis, centralizuotas šildymas /vėsinimas)
- Transportas (oro, geležinkelių, vandens, kelių)
- Bankininkystė
- Finansų rinkų infrastruktūra
- Sveikatos priežiūra
- Geriamasis vanduo
- Nuotekos
- Skaitmeninė infrastruktūra
- IRT paslaugų valdymas (B2B)
- Viešasis administravimas
- Kosmosas

Svarbių paslaugų tiekėjai

- Pašto ~~ir kurjerių~~ paslaugos
- Atliekų tvarkymas
- Cheminių medžiagų gamyba ir platinimas
- Maisto gamyba, perdirbimas ir platinimas
- Gamyba (med. priemonės, elektronika, el. įranga, motorinių transporto priemonių, kita)
- Informacinės visuomenės paslaugos (paieška, prekyvietės, socialiniai tinklai, priegloba)
- Moksliniai tyrimai

ATEA

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

Subjektai (~ 4000 org.)

Esminiai

Svarbūs

Įmonių kategorija	Darbuotojų skaičius: metiniai darbo vienetai (MDV)	Metinė apyvarta	arba	Bendras metinis balansas
Vidutinės	< 250	≤ 50 mln. EUR	arba	≤ 43 mln. EUR
Mažosios	< 50	≤ 10 mln. EUR	arba	≤ 10 mln. EUR
Labai mažos	< 10	≤ 2 mln. EUR	arba	≤ 2 mln. EUR

ATEA

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

TIS2 reikalavimai

Kibernetinio saugumo rizikos valdymo priemonės

Kibernetinio saugumo subjektai **privalo** Nacionaliniam Kibernetinio Saugumo Centrui **pateikti** duomenis apie kibernetinio saugumo **rizikos valdymo priemonių** įgyvendinimą.

Kibernetinio saugumo reikalavimai apima šiuos elementus:

1) kibernetinio saugumo **rizikos analizės**, tinklų ir informacinių sistemų kibernetinio saugumo politiką;

2) už kibernetinį saugumą atsakingų asmenų, nurodytų šio įstatymo 15 straipsnyje, ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas;

3) kibernetinių **incidentų valdymą**;

4) **veiklos tęstinumą**;

5) **tiekimo grandinės saugumą**, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykius;

6) tinklų ir informacinių sistemų **įsigijimą**, plėtojimą ir **priežiūros saugumą**, įskaitant **spragų** valdymą ir atskleidimą;

7) **politiką ir procedūras**, skirtas kibernetinio saugumo reikalavimų **veiksmingumui** įvertinti;

8) kibernetinės higienos praktiką ir reguliarius kibernetinio **saugumo mokymus**;

9) **kriptografijos ir šifravimo** naudojimo politiką ir procedūras;

10) žmogiškųjų išteklių saugumą, **prieigos kontrolės** politiką ir **turto valdymą;**

11) **kelių veiksnių** tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, **saugių** balso, vaizdo ir teksto **ryšių** bei saugių avarinių ryšių sistemų subjekto viduje naudojimą;

12) kibernetinio saugumo subjektų naudotojų, administratorių, tiekėjų, jų subtiekėjų ir kitų ūkio subjektų **teisių ir prieigos** prie kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų ir (ar) skaitmeninių duomenų suteikimo ir **valdymo politiką;**

13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus **kibernetinio saugumo reikalavimus**, nustatytus **atsižvelgiant** į atskiruose sektoriuose identifikuotas kibernetinio **saugumo rizikas.**

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

Kibernetinio saugumo reikalavimai apima šiuos elementus:

2) už kibernetinį saugumą atsakingų asmenų, nurodytų šio įstatymo 15 straipsnyje, ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas;

Kibernetinio saugumo subjektui leidžiama iš tiekėjo įsigyti paslaugas, kurių metu būtų vykdomos už kibernetinį saugumą atsakingų asmenų funkcijos.

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

Tiekimo grandinė

Esminių ir svarbių subjektų **tiekimo grandinėje** esantiems tiekėjams **bus taikomi** kibernetinio saugumo **reikalavimai**, pvz., bus reikalaujama sutartyse numatyti, kad **rangovai** laikytųsi perkančiosios organizacijos nustatytų informacijos saugumo bei kibernetinio saugumo reikalavimų **visą sutarties** vykdymo **laikotarpį**...

Šaltinis: https://kam.lt/duk_kategorijos/tis-2-direktyva/

Pareiga pranešti

Nedelsiant, bet ne vėliau kaip per **24 valandas**

– **ankstyvasis** perspėjimas

Nedelsiant, bet ne vėliau kaip per **72 valandas**

– incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas

Per **30 d.**

– **išsamus** kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;
– grėsmės arba pagrindinės **priežasties**, dėl kurios kibernetinis incidentas galėjo būti sukeltas, rūšis;
– taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo **priemonės**;

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

Atsakomybė

Valstybės narės užtikrina, kad esminių ir svarbių subjektų **valdymo organai** patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis 21 straipsnio, prižiūrėtų jo įgyvendinimą ir galėtų būti **patraukti atsakomybėn** už tai, kad subjektai pažeidžia tą straipsnį.

Šaltinis: L_2022333LT.01008001.xml (europa.eu)

Baudos

Esminiams subjektams 10 000 000 EUR arba 2 proc.
Svarbiems subjektams 7 000 000 EUR arba 1,4 proc.
Biudžetinei (Esminis subjektas) įstaigai iki 60 000 Eur
Biudžetinei (Svarbus subjektas) įstaigai iki 30 000 Eur

Pavojingas pažeidimas	- iki 100%
Vidutinio pavojingumo pažeidimas	- iki 50%
Nedidelio pavojingumo pažeidimas	- iki 10%

Šaltinis: LR Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas 24-6889(3) (projektas)

Nuo ko pradėti?

Ką daryti, jau dabar?

- **Atlikti rizikų analizę** ir atsižvelgiant į gautus rezultatus, susidėlioti rizikų valdymo politiką ir nusimatyti priemones, tiek organizacines tiek ir technines, kuriomis tos rizikos bus valdomos.

- Pasirengti ir/ar atnaujinti **dokumentaciją,** tai, ko tikrai reikės ir nuo ko verta pradėti:
  - **IS saugumo politika**
  - **Veikos tęstinumo planas**
  - **Incidentų valdymo planas**
- **Planuoti** kibernetinio saugumo **priemonių diegimą** ir naudojimą atsižvelgianti į rizikų valdymo plane numatytas priemones.

Reikalingi resursai

- Beveik 50 % ES (EPT/SPT) organizacijų samdė rangovus, kad padėtų jų informacijos saugos darbuotojams
- Beveik 50 % ES (EPT/SPT) organizacijų samdė naujus darbuotojus įgyvendinant direktyvą
- Tipiškame ES EPT/SPT reagavimui į incidentus dirba vidutiniškai du etatai

Šaltinis: NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist — ENISA (europa.eu)

Turite klausimų apie TIS2 direktyvos taikymą Jūsų organizacijai ?

Susisiekime:

evaldas.valunas@atea.lt

+370 682 55171


Kuriame Lietuvą su IT
ATEA