ESET SECURITY DAYS

NUO ATITIKTIES PRIE ATSPARUMO: KĄ IŠ TIESŲ KEIČIA KIBERNETINIO SAUGUMO REGULIAVIMAS?

DONATAS VITKUS

„Ignitis grupės“ skaitmeninės saugos vadovas

Kibernetinio saugumo reguliavimas energetikos sektoriuje

Energetikos sektoriui aktualūs teisės aktai

01 **TIS2**

02 **NCCS**

03 **PETA**

04 **BDAR**

05 **CER**

06 **CRA ***

07 **DORA * ***

01	**NIS2 Ignitis grupėje**	Kaip atitikties projektą paversti realiu pokyčiu
02	**PETA reikalavimai**	Ką pamatėme vertindami 100 kW+ elektrines

TIS2 Ignitis grupėje

Centralizuota sauga nepašalina juridinio ir administracinio sudėtingumo

7 (LT)
1 (PL)
3 (LV)

TIS2 subjektai

10×

registracijos, klausimynai, tikrinimai

3x

lokalūs reguliatoriai ir jurisdikcijos

200+

Informacinės sistemos

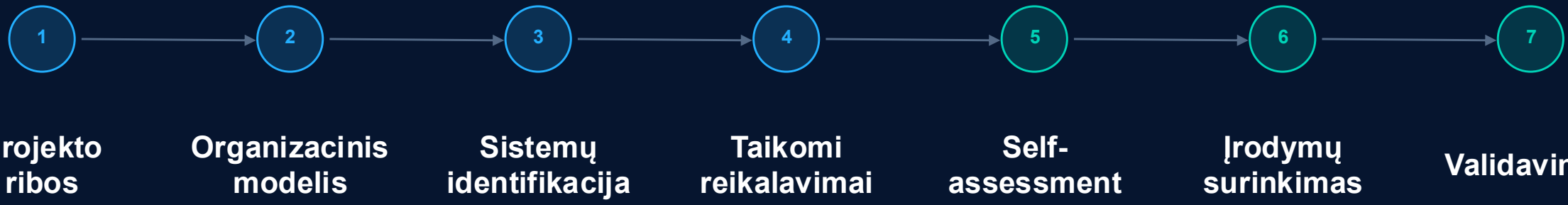
+

DORA, NCCS ir kt.

Norime vieningo valdymo modelio, tačiau atitiktį turime įrodyti kiekvienam subjektui ir kiekvienai sistemai.

TIS2 įgyvendinimas: 7 žingsniai

Ne nuo politikos, o nuo sistemų ir įrodymų



Vertinome konkrečias sistemas ir konkrečius įrodymus, o ne bendrą organizacijos „brandą“ apie saugumą.

Kur klydome

Atvirai apie tai, kas kainavo laiką ir energiją

01	**Per plati projekto apimtis**	Po TIS2 projektu bandėme pakišti per daug bendrų saugos darbų.
02	**Komunikacijos triukšmas**	Kai kur iniciatyvos trūko, kitur lygiagrečiai kūrėme tą patį.
03	**Nesukalibruoti lūkesčiai**	Verslas tikėjosi, kad projekto komanda ateis ir viską padarys.

Kas pasiteisino

Šešios praktikos, kurias kartotume dar kartą

- ✓ **Projektas spragoms šalinti, ne viskam**
- ✓ **Aiški paskirtis ir atsakomybės**
- ✓ **Sąžiningas projekto statusas**
- ✓ **Kritinės IS pirmiausia**
- ✓ **Vertinimas sistema po sistemos**
- ✓ **Bendri techniniai sprendimai + baseline**

Svarbiausia: „žalia“ būsena turi reikšti įrodytą progresą, ne optimizmą.

Ką reguliavimas pakeitė praktiškai

Atitikties veiksmai tapo saugumo ir turto valdymo mechanizmais

MATOMUMAS

Inventorizavome tai, ką iš tiesų turime

01

PRIORITETAI

Atskyrėme kritiška nuo tiesiog svarbaus

02

ATSKAITOS TAŠKAS

Self-assessment parodė realią būseną

03

STANDARTAS

Reikalavimai sukūrė bendrą minimumą

04

Keturi patarimai iš praktikos

Ką darytume anksčiau, paprasčiau ir griežčiau

1

Aiškiai apribokite projektą

Atitiktis nėra visų saugos problemų krepšys.

2

Eikite per sistemas

Vertinkite kontrolę ten, kur ji turi veikti.

3

Centralizuokite, ką verta

Bendri sprendimai mažina dubliavimą ir skirtumus.

4

Neignoruokite mažų objektų

Riziką kuria mastas, ryšys ir panašumas.

Tikslas nėra būti „compliant“. Tikslas yra būti sunkiau pažeidžiamam ir greičiau atsistatyti.

Kibernetinis saugumas elektrinėms: EEĮ 73(3) - PETA

Kibernetinio saugumo bazė 100 kW+ elektrinėms

REIKALAVIMAS — **Taikomas elektrinėms nuo 100 kW**

VERTINTOJAI — **ESO ir „Litgrid“ vertina atitiktį**

MASTAS — **ESO dalyje daugiau kaip 1500 objektų**

Tai buvo ne tik vertinimas. Tai buvo masinis decentralizuotos energetikos kibernetinio minimumo diegimas.

73(3) kibernetinio saugumo bazė

Paprasti reikalavimai, didelis bendras poveikis

VALDYMAS

- ✓ Atsakingas asmuo
- ✓ Prieigos kontrolė
- ✓ Periodinis auditas
- ✓ Tiekėjų rizika

KONFIGŪRACIJA

- ✓ Unikalūs slaptažodžiai
- ✓ Nenaudojami prievadai
- ✓ Bevielis ryšys išjungtas
- ✓ Programinė įranga atnaujinta

RYŠYS

- ✓ Ugniasienės
- ✓ Ribota interneto prieiga
- ✓ Šifravimas
- ✓ Saugumo deklaracija

1500+ elektrinių: koks realus pokytis

Kibernetinio saugumo minimumas tapo patikrinamu standartu

01

UGNIASIENĖ

Ryšys nebe paliktas „kaip yra“

02

SLAPTAŽODŽIAI

Numatytieji pakeisti unikaliais

03

PRIEVADAI

Nenaudojamos sąsajos išjungtos

04

ATNAUJINIMAI

Programinė įranga prižiūrima

1500+ objektų × keli baziniai pokyčiai = sisteminis rizikos sumažinimas visame tinkle

Ką pamatė vertintojas

Atitiktis nėra dokumentas. Ji matoma konfigūracijoje, architektūroje ir įrodymuose.

~40 %

Šiuo metu objektų pilnai atitinka

NUOTOLIS

dalis auditų „vyko nuotoliniu“ būdu

KVALIFIKACIJA

ISO 27001 Lead auditor, 2026 kovas-balandis

Vertinimo vertė: iš abstraktaus reikalavimo padaryti konkretų pokalbį su objekto savininku ir tiekėju.

Riba, kurios reguliavimas dar nepadengia

Iki 100 kW elektrinės taip pat sudaro reikšmingą decentralizuoto tinklo dalį

< 100 kW

Nereguliuojama zona

100 kW+

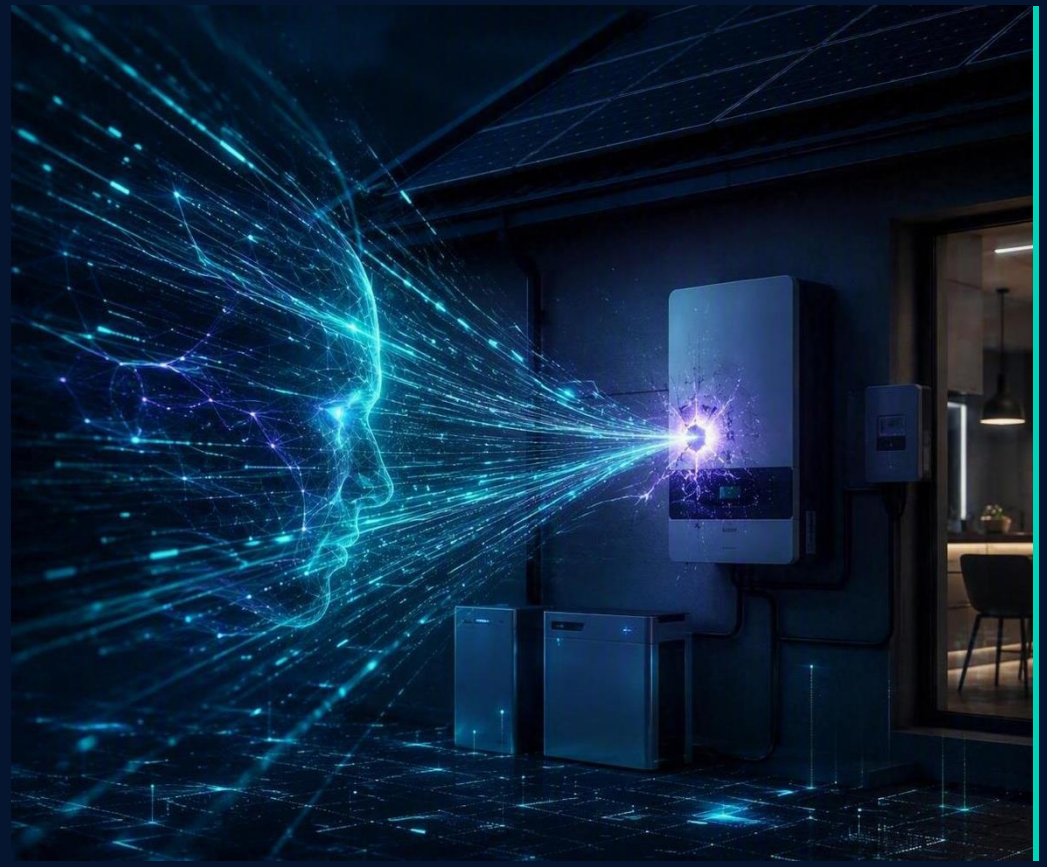
Baseline ir vertinimas

1 GW+ įrengtosios galios

1500+ objektų pagrindai sutvarkyti

Rizika tinkle nesustoja ties teisine galios riba.

[DI] spragas gali išnaudoti greitai



TOP 3 apsaugos prioritetai namų elektrinėje

01 **UGNIASIENĖ**

Riboja nepageidaujamą ryšį su elektrinės įranga.

02 **STIPRUS SLAPTAŽODIS + MFA**

Sustiprina prieigos kontrolę net nutekėjus slaptažodžiui.

03 **ATNAUJINIMAI**

Užtaiso žinomas spragas prieš jomis pasinaudojant.

AČIŪ

Klausimai?

Donatas Vitkus | Ignitis grupė

Reguliavimas duoda kryptį.
Atsparumą sukuriame mes.