

TIS2

Evaldas Valūnas

Grupės vadovas, Saugumo sprendimų kompetencijos centras



ATEA

SITUACIJA

- 2023-01-16 Priimta TIS2 direktyva
- 2023-05 Subjektų identifikavimo metodika
- 2024-07-11 KSĮ pakeitimas
- 2024-10-18 Įsigaliojo atnaujintas KSĮ
- 2024-11-06** **OTR patvirtinta**
- 2025-04-17 Subjektų sąrašas
- Po 2025-04-17 **O**TR - 12mėn.; **OTR** - 24mėn.

KĄ DARYTI?

KO NKSC **TIKISI**?

- Kibernetinio saugumo rizikų vertinimas
- Kibernetinių incidentų valdymo planas
- Veiklos tęstinumo planas
- Darbuotojų kibernetinis švietimas
- ...

OTR

TIS SAUGUMO POLITIKA

Ne rečiau kaip **kartą per metus** arba pasikeitus aplinkybėms, peržiūrėti ir atnaujinti kibernetinio saugumo politikos **dokumentus**.

RIZIKOS ANALIZĖ

Kibernetinio saugumo **rizikos vertinimas** turi būti atliekamas ne rečiau kaip **kartą per metus**, įvykus esminiams kibernetinio saugumo subjekto organizaciniam ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui.

Šaltinis - 818 11.

ATSAKINGI ASMENYS

Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis **negali** vykdyti funkcijų, susijusių su tinklų ar IS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

Šaltinis - 818 19.

INCIDENTŲ VALDYMAS

Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti kibernetinių **incidentų valdymo planą**.

VEIKLOS TĘSTINUMAS

Kritinių IS **prieinamumas**:

- Ne mažiau kaip 96% laiko – svarbiems subjektams
- Ne mažiau kaip 99% laiko – esminiams subjektams

TIEKIMO GRANDINĖ

Taikoma paslaugų, darbų, ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu.

SPRAGŲ VALDYMAS

Spragų vertinimo periodiškumas – ne rečiau kaip **kas ketvirtį** ir įvykus reikšmingiems pokyčiams.

VEIKSMINGUMO VERTINIMAS

Reguliariai, ne rečiau kaip **kartą per metus**, įvertinti kibernetinio saugumo subjekto **atitiktį** Kibernetinio saugumo įstatymui.

Reguliariai, ne rečiau kaip **kartą per 3 metus**, atlikti kibernetinio saugumo **audita**.

Šaltinis - 818 49.

HIGIENA

Ne rečiau kaip kartą per metus **visi** kibernetinio saugumo subjekto darbuotojai išklausytų kibernetinės higienos **praktikos mokymus**.

KRIPTOGRAFIJA

Duomenys **atsarginėse kopijose** turi būti **užšifruoti** (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų informacijai **neteisėtai atkurti**.

TURTO VALDYMAS

Parengti ir nuolat atnaujinti tinklų ir IS **turto sąrašą**.
Techninės priemonės, kurios **apribotų** neleistinių
įrenginių prijungimą prie tinklų ir informacinių sistemų.
Centralizuotai **valdyti** mobiliuosius įrenginius.

PRIEIGŲ VALDYMAS

Naudotojų, administratorių, paslaugų teikėjų grupių sudarymas, **teisių ir priedos** prie kibernetinio saugumo subjekto tinklų ir informacinių sistemų suteikimas ir **valdymas**.

Kelių veiksmų tapatumo priemonių naudojimo būdai.

Šaltinis - 818 69.

SUPRASTI

Kibernetinė sauga **NE** “**IT**šniko” darbas

ROLĖS



Chief Information Security Officer (CISO)



Cyber Incident Responder



Cyber Legal, Policy and Compliance Officer



Cyber Threat Intelligence Specialist



Cybersecurity Architect



Cybersecurity Auditor



Cybersecurity Educator



Cybersecurity Implementer



Cybersecurity Researcher



Cybersecurity Risk Manager



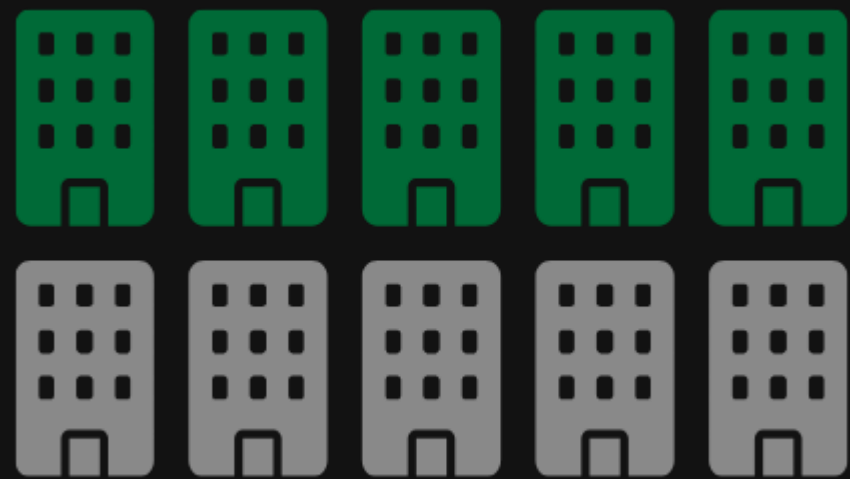
Digital Forensics Investigator



Penetration Tester

Šaltinis. ENISA

KĄ ORGANIZACIJS DARO?



48%

IŠORĖS PASLAUGOS



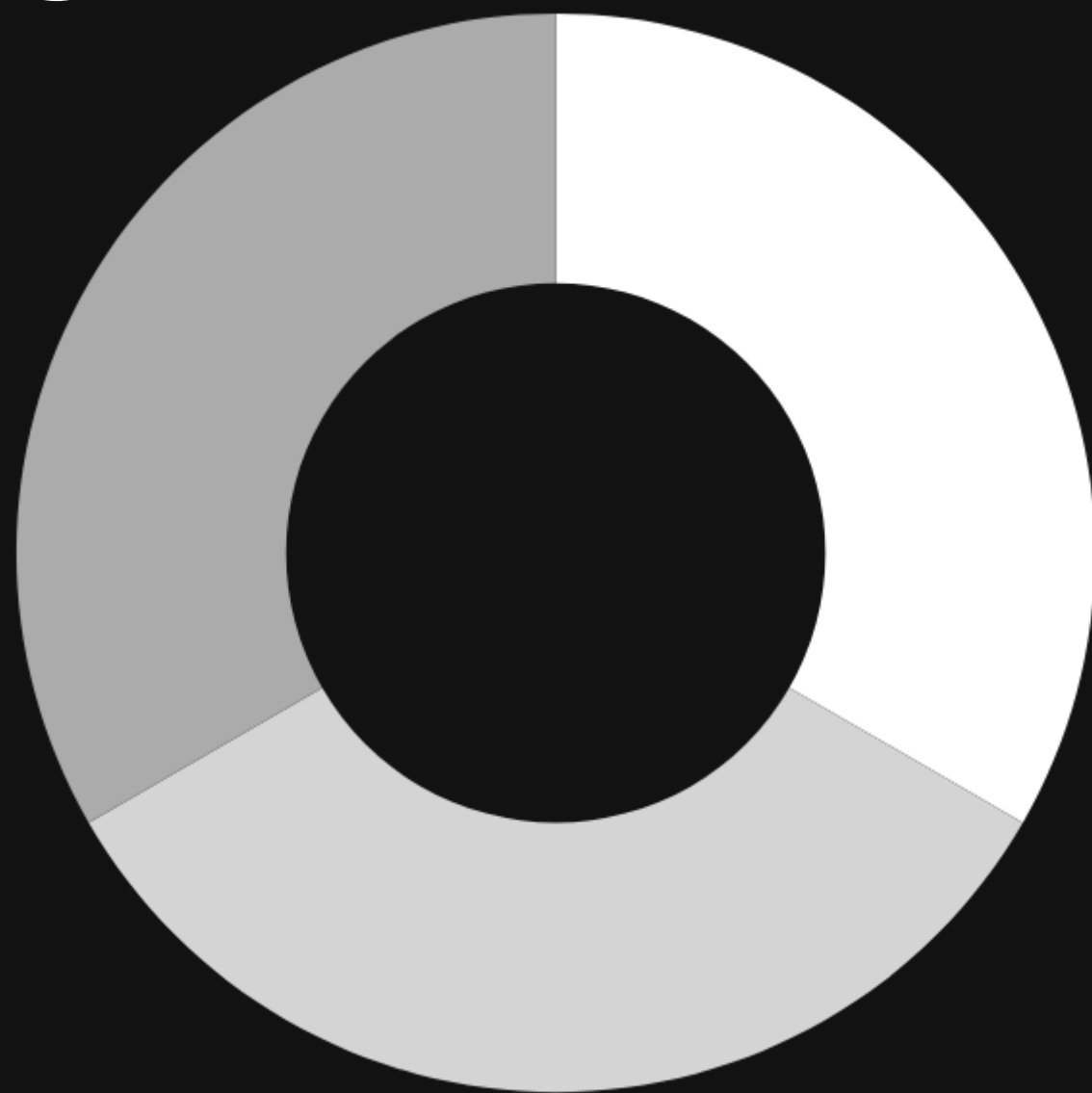
27%

IŠORĖS SPECIALISTAI

NUSPREȘTI

Technologijos

SOC
Pentest
MDR
MSSP
...



Žmonės

CISO
Auditas
Rizikų vertinimas
Atitikties vertinimas
Dokumentų rengimas
Mokymai
Soc. inžinerija
...

Procesai

Turite klausimų ?

Susisiekiame:

evaldas.valunas@atea.lt

+370 682 55171



<https://www.linkedin.com/in/evaldas-valunas/>