



**SECURITY  
DAYS**

# KIBERNETINIS SAUGUMAS PO TIS2: KODĖL SOC TAMPA NE PRABANGA, O VEIKLOS TĘSTINUMO SĄLYGA?



**RAMŪNAS LIUBERTAS**

„NOD Baltic“ vyresnysis  
kibernetinio saugumo  
inžinierius, ESET ekspertas

Teisinė prievolė

# TIS2 / KSĮ: subjektų įsipareigojimai kibernetiniam saugumui

## Privalomos rizikos valdymo priemonės:

01

**Techninės**

Valdyti rizikas

02

**Operacinės**

Aptikti  
incidentus

03

**Organizacinės**

Mažinti poveikį  
paslaugoms



Vadovybės atsakomybė

## Finansinė ir asmeninė vadovų atsakomybė

### Finansinė rizika

Baudos gali siekti tūkstantines,  
ar netgi milijonines sumas arba  
dalį apyvartos

### Asmeninė atsakomybė

Vadovas turi suvokti rizikas bei  
prioriterizuoti organizacijos  
saugumo stiprinimo strategiją

Pagrindinis pokytis

# Iš „rekomenduojama“ į „privaloma“



## Anksčiau

Gerosios praktikos, rekomendacijos,  
periodiniai patikrinimai

## Dabar

Nuolatinė kontrolė, incidentų  
valdymas ir veiksmingumo įrodymas

Teisinis kontekstas

# Ką turi užtikrinti organizacija?

## Stebėseną

Nuolatinis saugumo įvykių matomumas ir anomalijų aptikimas

## Incidentų valdymas

Aiškų procesą: aptikti, analizuoti, izoliuoti, atkurti

## Atsparumas

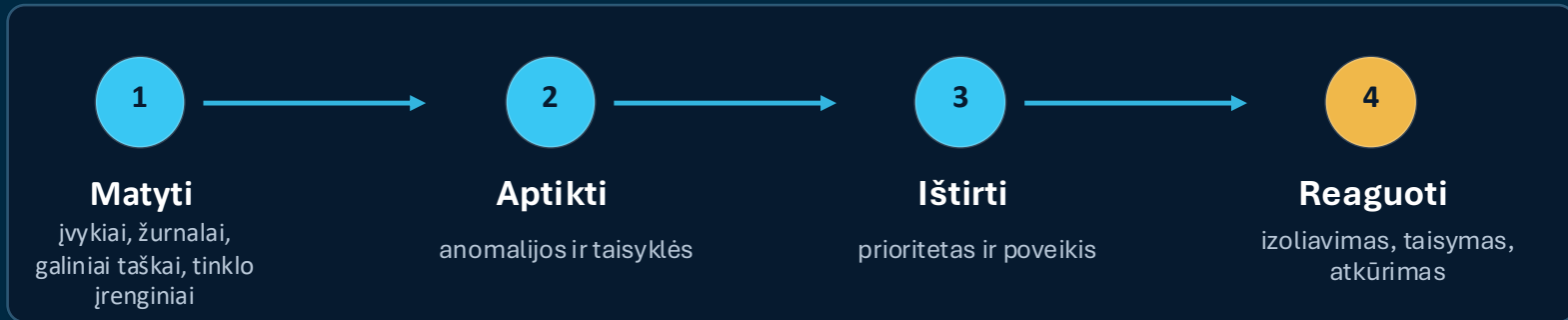
Tęstinumo, atkūrimo ir krizių valdymo pasirengimas

## Įrodumumas

Įrodymai, ataskaitos, kontrolės efektyvumo vertinimas

Operatyvus reagavimas

# Aptikimas be reagavimo nėra pakankamas



**SOC pagrindai**

# Kas yra SOC ir kaip tai apsaugo verslą?

## Stebėseną

24/7  
matomumas į  
sistemas, tinklą  
ir naudotojų  
veiklą

## Logų rinkimas

Centralizuojami  
įvykiai iš darbo  
vietų, serverių,  
tinklo įrenginių ir  
debesijos paslaugų

## Analizė

Koreliuojami  
signalai ir atskiriami  
triukšmai nuo realių  
grėsmių

## Reagavimas

Grėsmės  
aptinkamos ir  
eskaluojamos prieš  
joms padarant žalą

**SOC tikslas – pamatyti grėsmę anksčiau, nei ji tampa incidentu**

24/7 stebėseną

**Įsilaužėliai nedarba nuo 8 iki 17 val.**

**Rizikos langai per parą**



**Naktimis**

Mažesnis vidinis  
budėjimas ir lėtesnis  
pastebėjimas

**Savaitgaliais**

Mažiau darbuotojų,  
daugiau delsos  
eskalavime

**Per šventes**

Atakos taikosi į  
sumažėjusį dėmesį ir  
kontrolę

# Veiklos tęstinumas vs. visiškas paralyžius

## Veiklos tęstinumas

Kai SOC anksti aptinka signalus:

- **Ankstyvas aptikimas**

Pastebimi įtartinai prisijungimai, skverbimasis gilyn ir šifravimo požymiai.

- **Greitas izoliavimas**

Pažeisti įrenginiai atjungiami, kol ataka neišplito per infrastruktūrą.

- **Mažesnis poveikis**

Išsaugomas paslaugų tęstinumas, sumažinamas prastovų ir duomenų praradimo mastas.

## Visiškas paralyžius

Kai grėsmė nepastebima laiku:

- **Užrakinti duomenys**

Ransomware šifruoja failus, sistemas ir atsargines kopijas.

- **Sustabdyta veikla**

Nepasiekiamos verslo sistemos, gamyba, klientų aptarnavimas ar finansai.

- **Dideli nuostoliai**

Atsiranda prastovos, reputacinė žala, atkūrimo kaštai ir teisinė rizika.

Kompetencijų trūkumas

# Žmogiškųjų išteklių krizė kibernetiniame saugume

## Minimalus vidinio 24/7 SOC pajėgumas

### L1

Pirminis įvykių monitoringas

### L2

Analizė ir incidentų eskalacija

### L3

Sudėtingų grėsmių tyrimas

### IR

Incidentų reagavimas

### TH

Grėsmių medžioklė / tobulinimas

### Lead

Budėjimo koordinavimas

## Kodėl tai sudėtinga?

- **Brangu**  
24/7 budėjimas reiškia ne tik atlyginimus, bet ir pamainas, mokymus bei kaitos valdymą.
- **Trūksta specialistų**  
Rinkoje sertifikuotų inžinierių paklausa viršija pasiūlą.
- **Sunku išlaikyti kokybę**  
Reikia nuolatinio taisyklių, technologijų ir procesų atnaujinimo.

**Todėl daugelis organizacijų renkasi išorinį SOC modelį**

**Kaštų analizė**

# Vidinis SOC vs išorinis SOC – kaštų analizė

| Vertinimo kriterijus  | Vidinis SOC                                                                     | Išorinis SOC                                                      |
|-----------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Pradinės investicijos | Didelės investicijos į žmones, SIEM, procesus ir integracijas                   | Minimalios pradinės investicijos – paslauga aktyvuojama greičiau  |
| Kompetencija          | Reikia pačiai organizacijai samdyti ir išlaikyti aukštos kvalifikacijos komandą | Gaunama brandi komanda ir sukaupta praktika per paslaugos teikėją |
| Pasiekiamumas         | 24/7 aprėptis sudėtinga ir brangi be kelių pamainių                             | Nuolatinė 24/7 stebėseną ir reagavimo procesai iš karto           |
| Kaštų modelis         | Dažniau kintantys ir sunkiau prognozuojami kaštai                               | Fiksuotas mėnesinis mokestis ir aiškesnis biudžetas               |

**Išorinio SOC paslauga**

# Kodėl verta rinktis „NOD BALTIC“ išorinį SOC?

## Ką apima paslauga?

### 24/7 stebėseną

Automatizuota IT infrastruktūros stebėseną vykdoma nuolat, visą parą

### Logų centralizavimas

Centralizuotas 90 d. žurnalinių įrašų saugojimas, analizė ir incidentų identifikavimas.

### Matomumas vadovybei

Savitarnos portalas ir mėnesinės ataskaitos suteikia aiškų saugumo vaizdą.

### Atitikties pagalba

Padedą įgyvendinti NIS2 / kibernetinio saugumo reikalavimus ir taupo vidinius resursus.

## Kodėl tai aktualu verslui?

**Išorinis SOC = aukšto lygio apsauga be vidinio 24/7 SOC kūrimo kaštų.**

## Technologijos

# SIEM + XDR su ESET technologija

### SIEM sluoksnis

- Centralizuotas žurnalinių įrašų surinkimas
- Įvykių koreliacija ir analizė
- Istorija, ataskaitos ir paieška
- Integracijos su infrastruktūra

### XDR sluoksnis

- ESET Inspect (XDR)
- Pažangus grėsmių aptikimas
- Endpoint signalų kontekstas
- Incidentų tyrimo pagrindas

### Ką gauna klientas?

#### ● Visapusiškas matomumas

SIEM + XDR apima IT infrastruktūrą ir tinklo perimetrą.

#### ● Automatizuotas monitoringas

Nuolatinė 24/7 stebėsena ir įvykių identifikavimas.

#### ● Portalas ir ataskaitos

Savitarnos portalas realiu laiku ir mėnesinės ekspertų rekomendacijos.

#### ● ESET ekosistema

Paslauga teikiama su ESET sprendimais arba turimu jų prenumeratos pagrindu.

**Kompetencijos**

# Patirtis, sertifikatai ir brandi organizacija

**1****10+ m. patirties**

Komandoje dirba kibernetinio saugumo ekspertai, turintys daugiau kaip 10 metų praktinės patirties.

**2****CISSP / ITIL**

Kompetencijos grindžiamos aukšto lygio profesinėmis žiniomis.

**3****ISO 27001:2022**

„NOD Baltic“ informacijos saugumo valdymo sistemos atitinka ISO 27001:2022 reikalavimus.

**4****ESET partnerystė**

Įmonė yra oficialus ESET partneris Lietuvoje, o SOC paslauga grindžiama ESET technologija.

**20+ metų veikla kibernetinio saugumo srityje ir daugiau kaip 20 000 klientų Lietuvoje bei Latvijoje**

## TAKE AWAY

TIS2/KSI – tai ne tik  
techn./org.  
reikalavimai, bet ir  
valdymo bei  
atsakomybės klausimas

SOC padeda užtikrinti,  
kad incidentai neliktų  
tik loguose — jie būtų  
laiku pastebėti,  
įvertinti ir suvaldyti

Atsakingai rinkimės  
išorinį SOC paslaugų  
tiekėją, jis privalo turėti  
kvalifikuotus saugumo  
specialistus

# KLAUSIMAI?

SUSISIEKIME:

**NOD BALTIC**

Ramūnas Liubertas

ramunas@nodbaltic.com

<https://www.nodbaltic.com>



Bendraukime 



**Plačiau apie NOD Baltic išorinę  
SOC paslaugą - prie ESET stendo**