SECURITY DAYS

SOC PASLAUGOS: JŪSŲ ORGANIZACIJOS SAUGUMO ŠIRDIS

Ramūnas Liubertas,
NOD Baltic vyresnysis kibernetinio saugumo inžinierius, ESET ekspertas

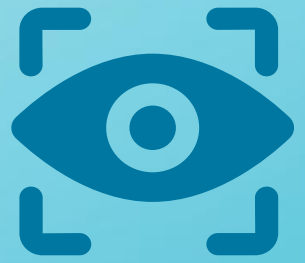
DI užklausa temos paveiksliukui:

+ ORGANIZACIJA

+ KIBERNETINIS SKYDAS

+ SAUGUMO ŠIRDIS

KAS YRA SOC?



KAS YRA SOC?

Saugumo operacijų centras (angl. Security Operations Center) - organizacijos dalis arba išorinė paslauga, kuri, pasitelkdama specialistus, procesus ir technologijas, nuolatinai stebi organizacijos įrenginius ir tinklą, nustato organizacijos silpnąsias vietas ir pažeidžiamumus, siekiant pagerinti saugumo funkcijas ir išvengti kibernetinių grėsmių.

AR MŪSŲ ĮMONEI REIKALINGAS SOC?

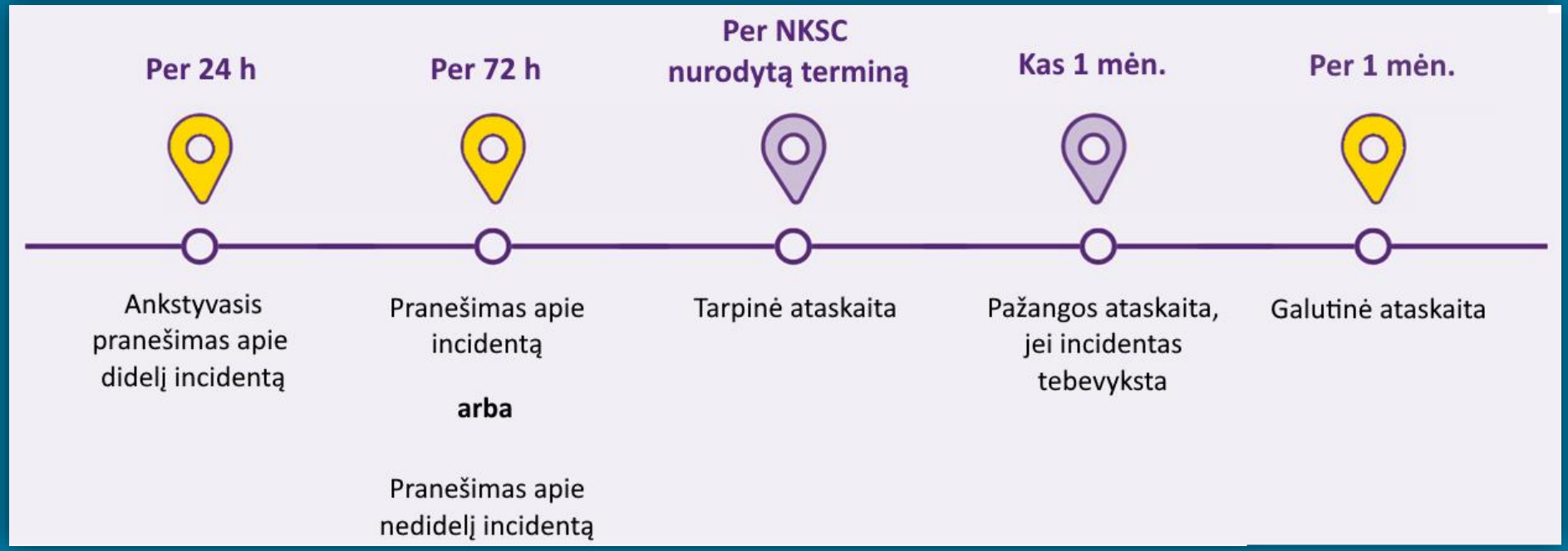
Atitiktis KSĮ reikalavimams

Kibernetinės atakos

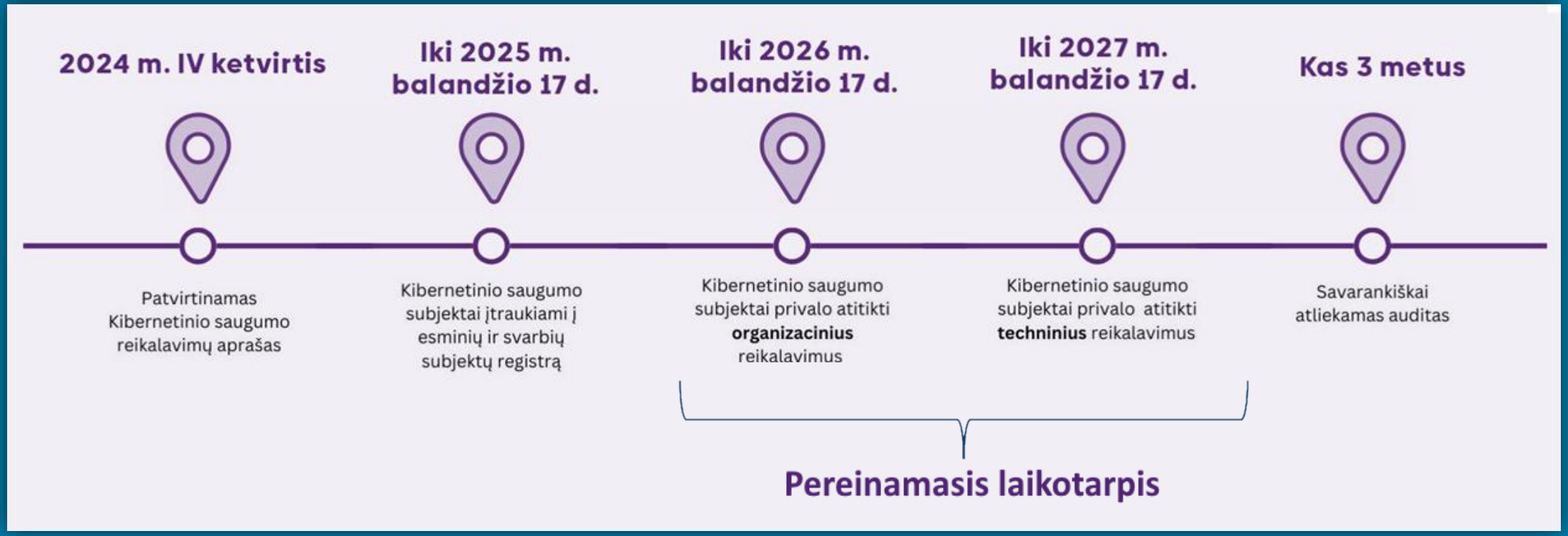
Specialistų, laiko ir žinių trūkumas

AR MŪSŲ ĮMONEI REIKALINGAS SOC?

- Saugumo įvykių stebėjimas, aptikimas, ištyrimas ir vertinimas
- Kenkėjiško kodo, vidinių grėsmių ir kibernetinio sukčiavimo stebėjimas ir analizė
- Pažeidžiamumų stebėjimas ir valdymas
- Incidentų identifikavimas, vertinimas ir šalinimas
- Reguliarių ataskaitų ir rekomendacijų teikimas



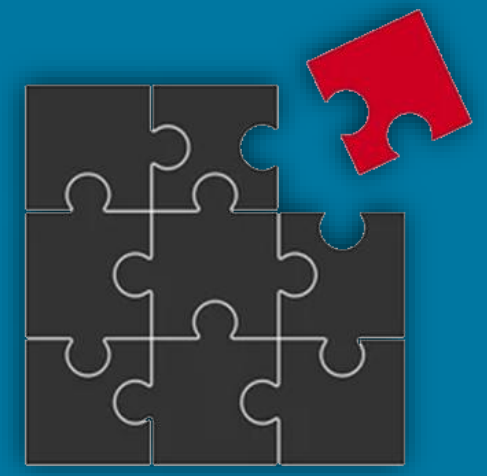
AR MŪSŲ ĮMONEI REIKALINGAS SOC?



JEI MŪSŲ ĮMONĖ NĖRA ĮTRAUKTA Į KSS REGISTRĄ?

Tačiau...

...yra paslaugos tiekėjas į KSS registrą įtrauktai įmonei.



<u>Netiesioginis teisinio reguliavimo poveikis:</u>

Kibernetinio saugumo subjektai turės reikalauti ir įsitikinti, jog tiekėjai atitinka kibernetinio saugumo reikalavimus, pvz., turi incidentų valdymo planus, saugumo sertifikatus, įvykus kibernetiniam incidentui bendradarbiaus su kibernetinio saugumo subjektu ir pan.

Bureau Veritas Certification

EN ISO/IEC 17021-1
S2-424

Sertifikatas

Išduotas

NOD Baltic, UAB
Baltimax UAB

Laisvės pr. 3, Vilnius, LT-04215, LIETUVA

Šiuo sertifikatu Bureau Veritas Certification patvirtina, kad įvertino nurodytos organizacijos vadybos sistemą ir nustatė, jog ji atitinka toliau nurodyto vadybos sistemos standarto reikalavimus

STANDARTAS

ISO/IEC 27001:2022

SERTIFIKAVIMO SRITIS

IT SPRENDIMŲ PLATINIMAS IR DIEGIMAS, IT PASLAUGŲ TEIKIMAS, MOKYMAI BEI KONSULTACIJOS.

Taikomumo pareiškimas 14.02.2025

Pradinio patvirtinimo data: 30.04.2025

Sertifikavimo audito data: 05.03.2025 – 30.04.2025

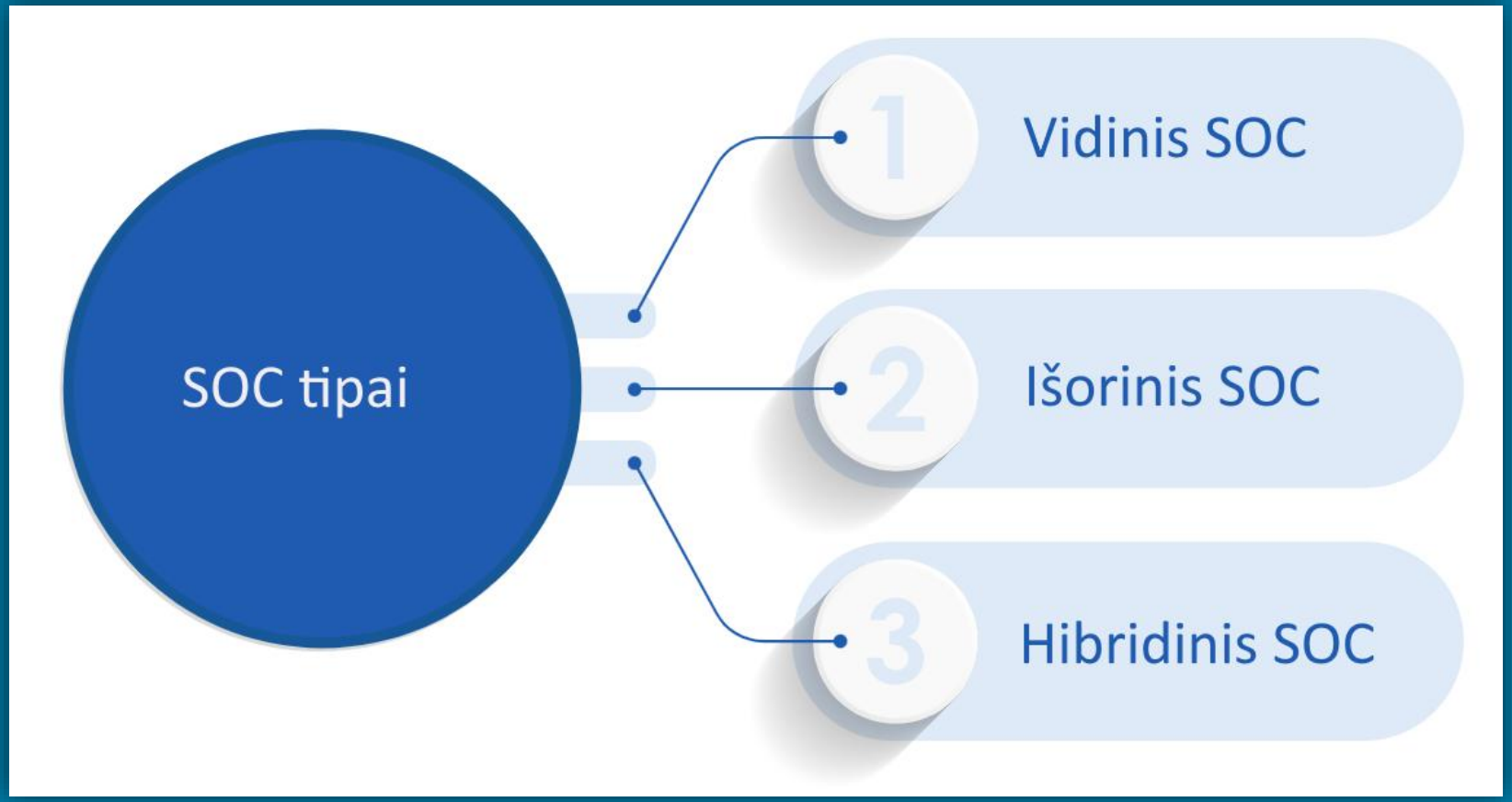
Organizacijos vadybos sistemai nuolat atitinkant nurodytus standarto reikalavimus, šis sertifikatas galioja iki: 29.04.2028

Sertifikato Nr.: LVRIG21025D/LT *Versijos Nr.:* 1 *Išleistas data:* 30.04.2025

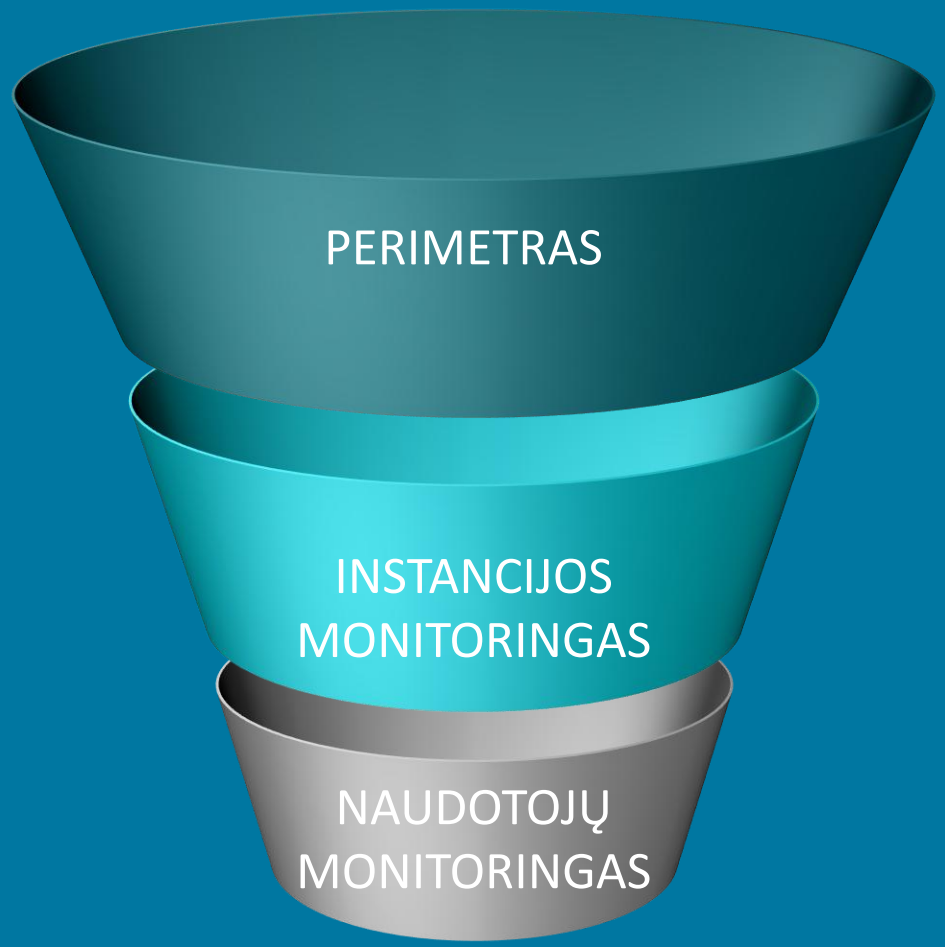
Sertifikacijos įstaigos adresas: Bureau Veritas Latvia SIA, Duntes street 17a, Riga, LV-1005, Latvija

Norėdami gauti daugiau informacijos apie šio sertifikato veikimo sritį ir vadybos sistemos reikalavimų atitikimą, prašome kreiptis į organizaciją, kuriai išduotas sertifikatas. Norėdami papildomai pasitikrinti apie šio sertifikato galiojimą, prašome skambinti į Bureau Veritas Certification, tel. +371 67323246

PAGRINDINIAI SOC TIPAI



SOC FUNKCIJŲ APRĖPTIS



- IT infrastruktūros stebėjimas
- Pažeidžiamumų identifikavimas
- Grėsmių aptikimas
- Incidentų tyrimas
- Reagavimas į incidentus
- Reguliarus saugumo būklės ataskaitų teikimas
- Rekomendacijos ir prevencinės priemonės

SOC IŠŠŪKIAI

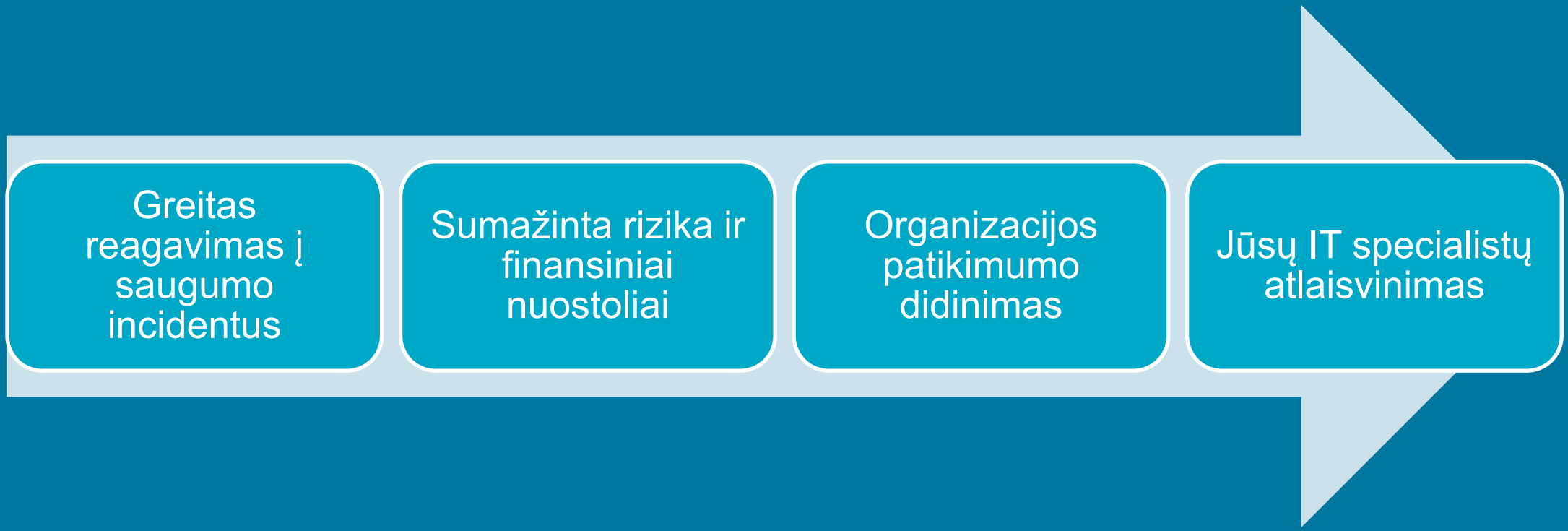
Didžiulis duomenų kiekis ir triukšmas

Tikslinių atakų ir kibernetinių grėsmių evoliucija

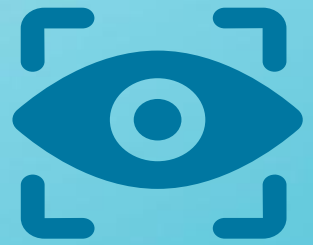
Būtina patikima specialistų komanda

VIDINIS SOC		IŠORINIS SOC
Didelės pradinės investicijos		Mažesnės veiklos sąnaudos
Sunku rasti ir išlaikyti specialistus		Greitai pasiekiama ekspertų komanda
Reikalingi nuolatiniai mokymai		Užtikrinama specialistų kompetencija
Ilgas įgyvendinimo laikotarpis	VS	Greitas startas
Sunku palaikyti technologijų įvairovę		Naudojami naujausi įrankiai
Platus atsakomybių spektras KSĮ atitikčiai		Lengviau išpildyti KSĮ atitiktį
Šališkumo ir subordinacijos iššūkiai		Objektyvi analizė

KODĖL VERTA RINKTIS IŠORINES SOC PASLAUGAS?



NOD BALTIC IŠORINIO SOC PASLAUGOS TEIKIMAS



NOD Baltic išorinio SOC teikiamos funkcijos

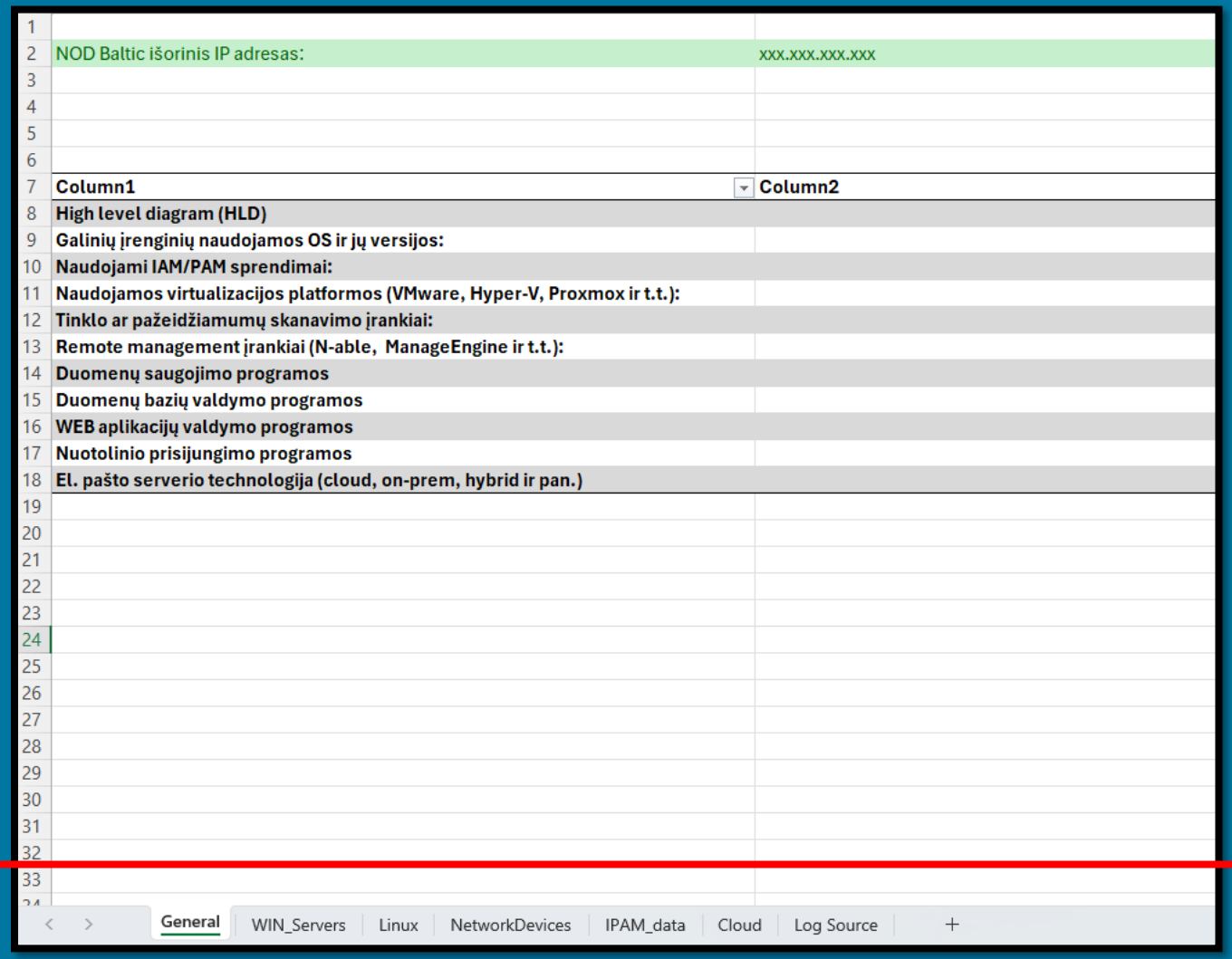
- Centralizuotas saugumo stebėjimas – darbo vietų, serverių, tinklo įrenginių ir kt. resursų
- Proaktyvi ir savalaikė informacija
- Antivirusinė apsauga + XDR įrankis (prevencija, reagavimas, informavimas ir stebėjimas)
- Pažeidžiamumų identifikavimas
- Kibernetinių incidentų tyrimas ir išsami failų analizė
- Aptikimų aptarimas ir išaiškinimas
- Žurnalinių įrašų kaupimas, analizė ir saugojimas – 90 d.
- Personalizuotos ataskaitos su rekomendacijomis, atliktais veiksmais ir kita informacija

NOD Baltic išorinio SOC teikimo reikalavimai

	PROTECT ENTRY	PROTECT ADVANCED	PROTECT ENTERPRISE	PROTECT COMPLETE	PROTECT ELITE
Valdymo konsolė debesyje **ESET Protect Cloud**	✓	✓	✓	✓	✓
Pažangi darbo vietų apsauga **Endpoint Security**	✓	✓	✓	✓	✓
Serverių apsauga **ESET Server Security**	✓	✓	✓	✓	✓
Mobiliųjų įrenginių valdymas **Mobile Device Management**	✓	✓	✓	✓	✓
Apsauga nuo pažangių grėsmių **ESET LiveGuard Advanced**		✓	✓	✓	✓
Pilnas disko šifravimas **ESET Full Disk Encryption**		✓	✓	✓	✓
Pašto apsauga **ESET Mail Security**				✓	✓
Debesijos paslaugų apsauga **ESET Cloud Office Security**				✓	✓
Pažeidžiamumų ir pataisų valdymas **ESET Vulnerability & Patch Management**				✓	✓
Išplėstinis aptikimas ir reagavimas **ESET Inspect**			✓		✓
Kelių veiksnių autentifikavimas **ESET Multi-Factor Authentication**					✓

NOD Baltic išorinio SOC teikimo reikalavimai

Tinklo žemėlapis (angl. Network map)



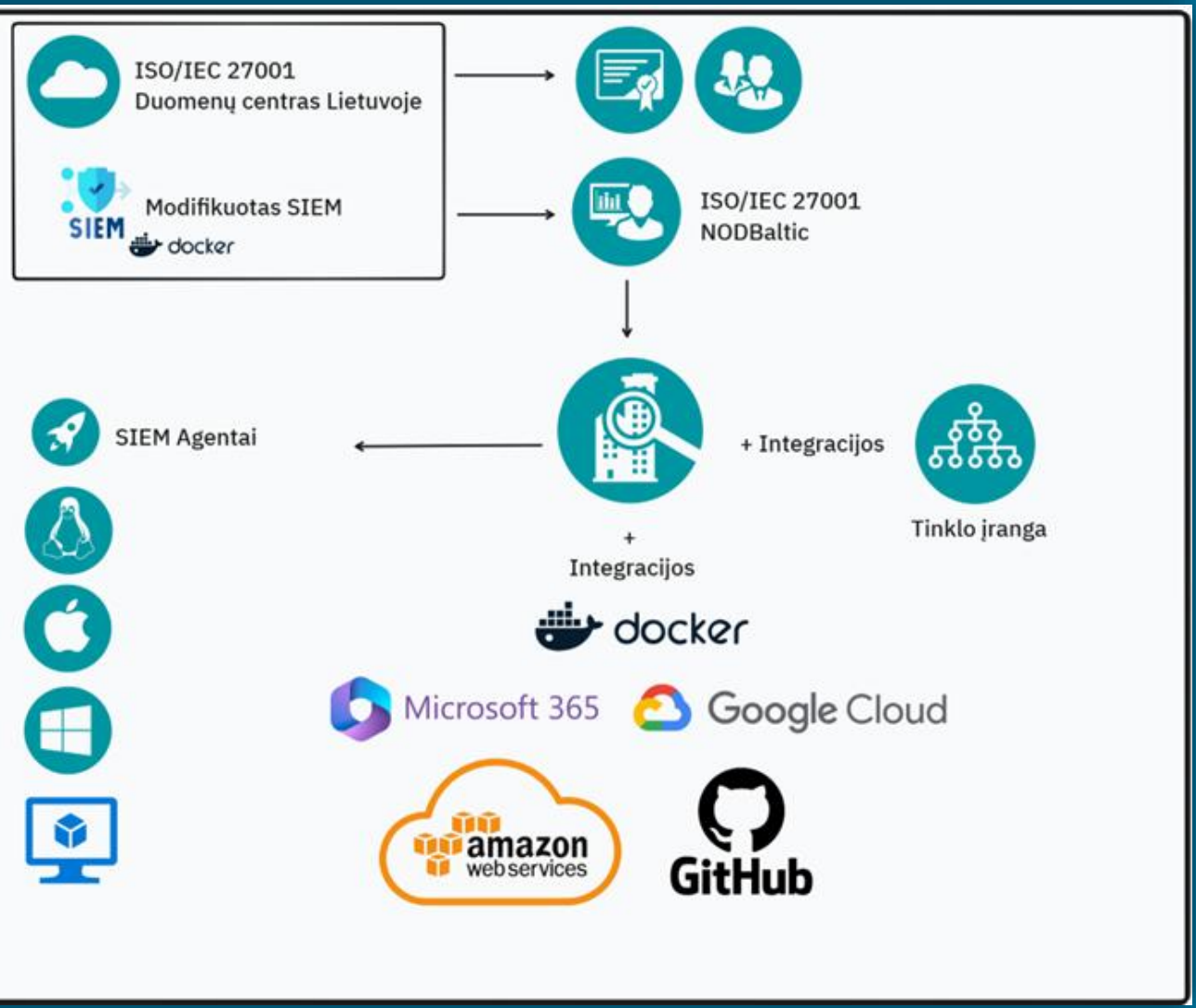
	Column1	Column2
2	NOD Baltic išorinis IP adresas:	xxx.xxx.xxx.xxx
7	**Column1**	**Column2**
8	**High level diagram (HLD)**	
9	**Galinių įrenginių naudojamos OS ir jų versijos:**	
10	**Naudojami IAM/PAM sprendimai:**	
11	**Naudojamos virtualizacijos platformos (VMware, Hyper-V, Proxmox ir t.t.):**	
12	**Tinklo ar pažeidžiamumų skanavimo įrankiai:**	
13	**Remote management įrankiai (N-able, ManageEngine ir t.t.):**	
14	**Duomenų saugojimo programos**	
15	**Duomenų bazių valdymo programos**	
16	**WEB aplikacijų valdymo programos**	
17	**Nuotolinio prisijungimo programos**	
18	**El. pašto serverio technologija (cloud, on-prem, hybrid ir pan.)**	

General | WIN_Servers | Linux | NetworkDevices | IPAM_data | Cloud | Log Source

NOD Baltic išorinio SOC technologinė bazė

Nepertraukiama IT aplinkos apsauga, prevencija
ir kibernetinių rizikų valdymas

Management Console	ESET PROTECT
Modern Endpoint Security	ESET Endpoint Security
Server Security	ESET Server Security
Advanced Threat Defense	ESET LiveGuard Advanced
Full Disk Encryption	ESET Full Disk Encryption
*Mail Security	ESET Mail Security
*Cloud App Protection	ESET Cloud Office Security
*Vulnerability & Patch Management	ESET Vulnerability & Patch Management
Detection & Response	ESET Inspect
*Authentication	ESET Secure Authentication
Services	NOD Baltic saugumo paslaugos



Paslaugos teikimo eiga

Per 20 d. d. nuo sutarties pasirašymo nuotolinė diegimo ir atnaujinimo sesija

Paslaugos paleidimo etapas 1-3 mėn.

SOC ataskaitos aptarimas 1 kartą per mėnesį

Proaktyviai

Neribotos nuotolinės sesijos dėl aptikimų aptarimo

NOD Baltic išorinio SOC stebėjimo objektai

Darbo vietos

OS: Windows, macOS, Linux

SOC dėmesys: XDR, vartotojų elgsenos stebėjimas, pažeidžiamumų skenavimas

Virtualūs serveriai

OS: Windows Server, Linux

SOC dėmesys: hipervizorių saugumas (VMware, Hyper-V), komunikacijų tarp VM stebėjimas

Serveriai

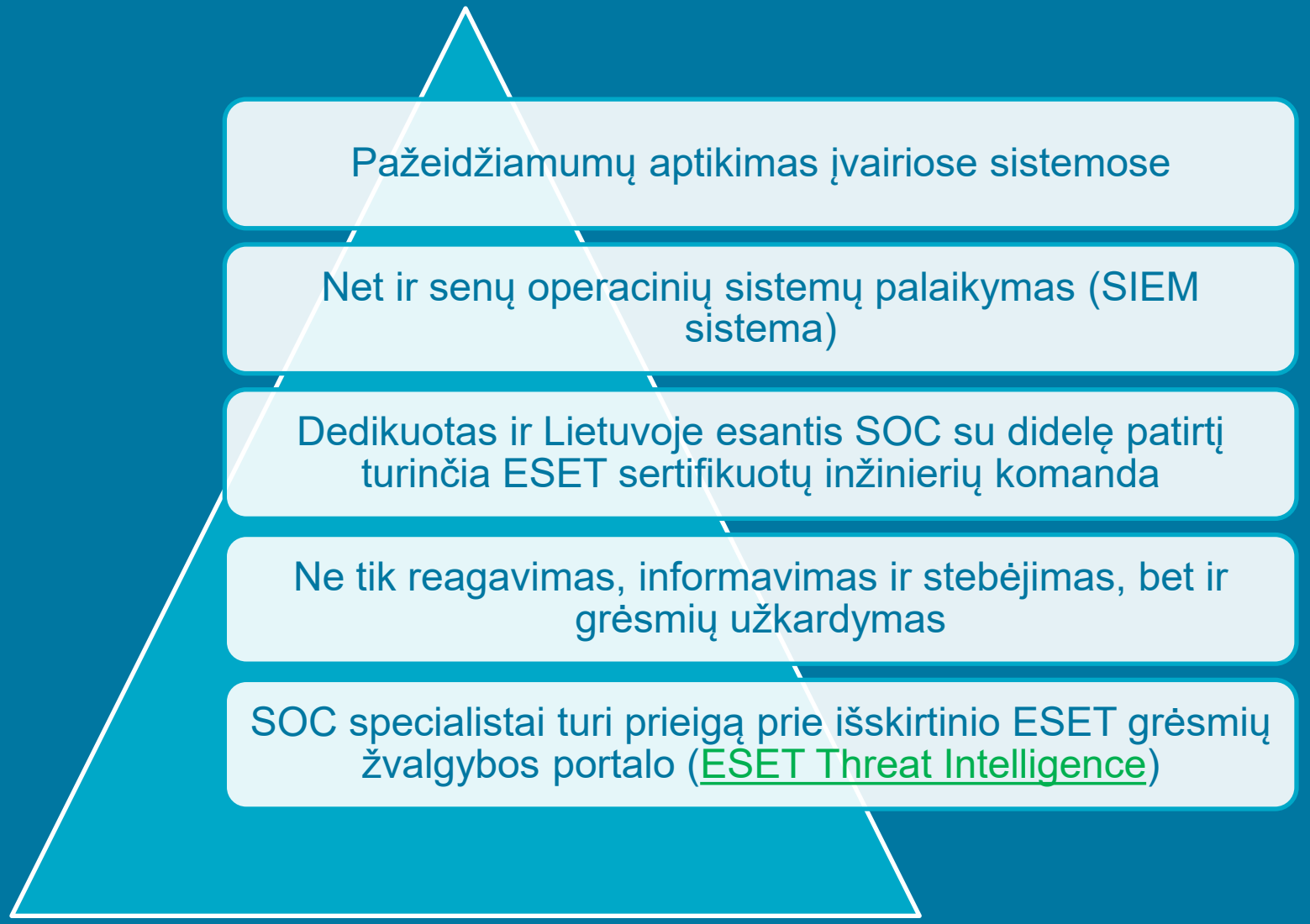
OS: Windows Server, Linux

SOC dėmesys: prieigos kontrolė, saugos atnaujinimai, logų surinkimas (syslog, event log)

Tinklo įranga

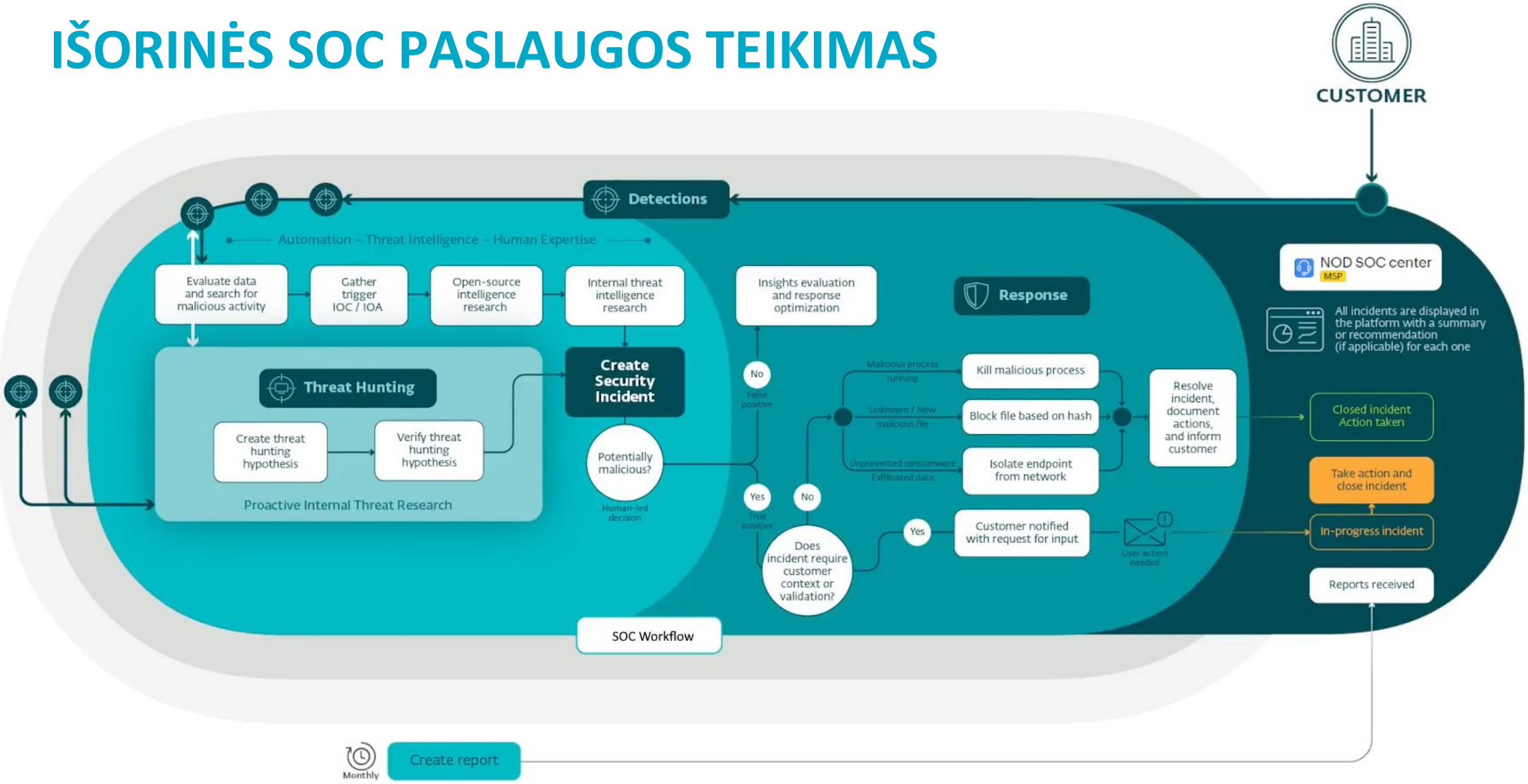
Įranga: maršrutizatoriai, switch'ai, ugniasienės (Cisco, Fortinet, MikroTik)
SOC dėmesys: konfigūracijų auditas, tinklo srautų stebėjimas

NOD Baltic SOC išskirtinumai

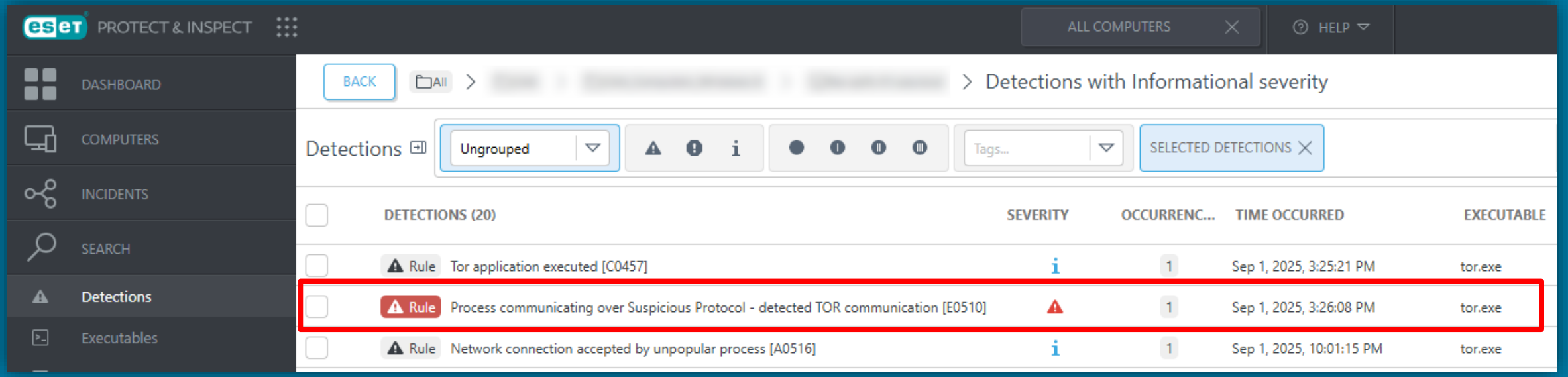


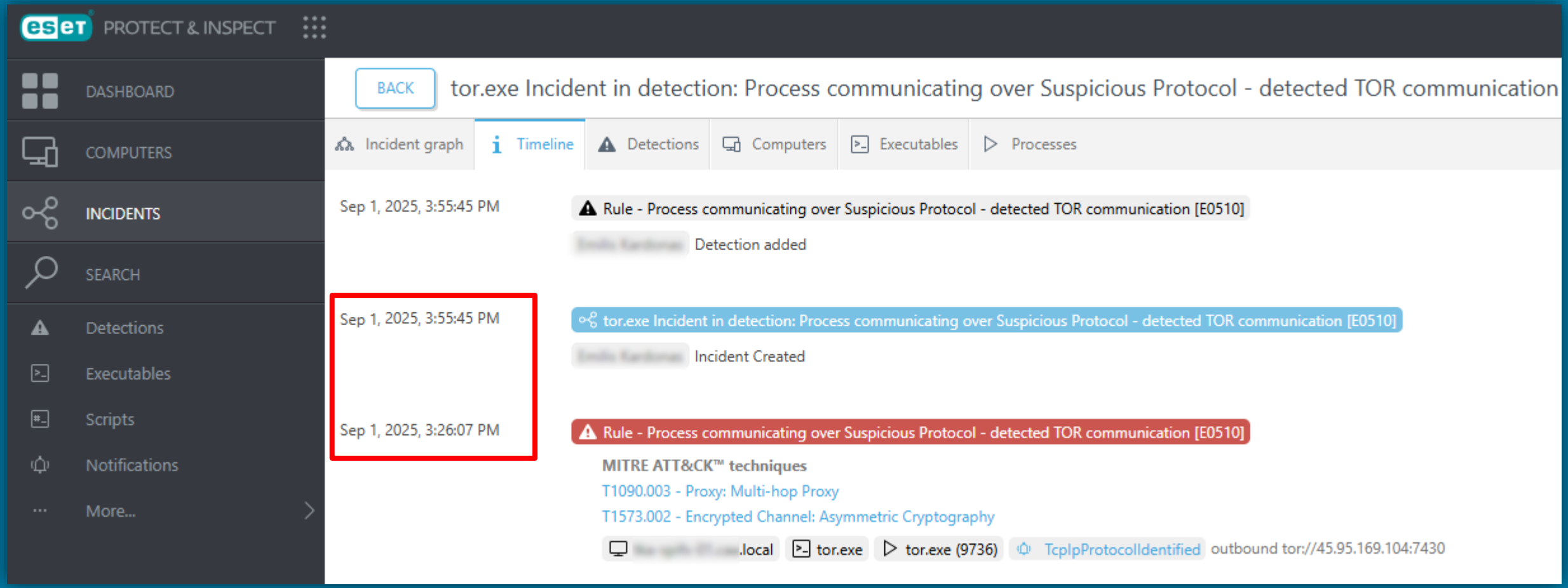
KAIP VYKSTA KOMUNIKACIJA SU NOD BALTIC IŠORINIU SOC?

IŠORINĖS SOC PASLAUGOS TEIKIMAS



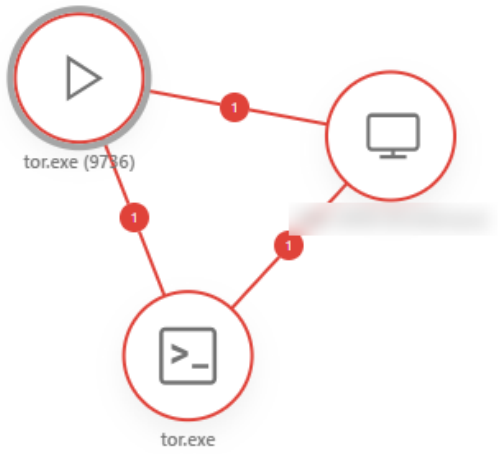
SOC ATVEJO ANALIZĖS PVZ.




eset PROTECT & INSPECT
DASHBOARD
COMPUTERS
INCIDENTS
SEARCH
Detections
Executables
Scripts
Notifications
More...
BACK
tor.exe Incident in detection: Process communicating over Suspicious Protocol - detected TOR communication
Incident graph
Timeline
Detections
Computers
Executables
Processes
Sep 1, 2025, 3:55:45 PM
Rule - Process communicating over Suspicious Protocol - detected TOR communication [E0510]
Detection added
Sep 1, 2025, 3:55:45 PM
tor.exe Incident in detection: Process communicating over Suspicious Protocol - detected TOR communication [E0510]
Incident Created
Sep 1, 2025, 3:26:07 PM
Rule - Process communicating over Suspicious Protocol - detected TOR communication [E0510]
MITRE ATT&CK™ techniques
T1090.003 - Proxy: Multi-hop Proxy
T1573.002 - Encrypted Channel: Asymmetric Cryptography
.local
tor.exe
tor.exe (9736)
TcpIpProtocolIdentified
outbound tor://45.95.169.104:7430

Incident graph | Timeline | Detections | Computers | Executables

Processes



INCIDENT | REMEDIATION | COMMENT | EDIT | ...

Incident | Timeline | Details | Process tree | Related objects

tor.exe Incident in detection: Process communicating over Suspicious Protocol - detected TOR communication [E0510]

Status Open

Severity Medium

Assignee [redacted]

Tags Select tags

Description

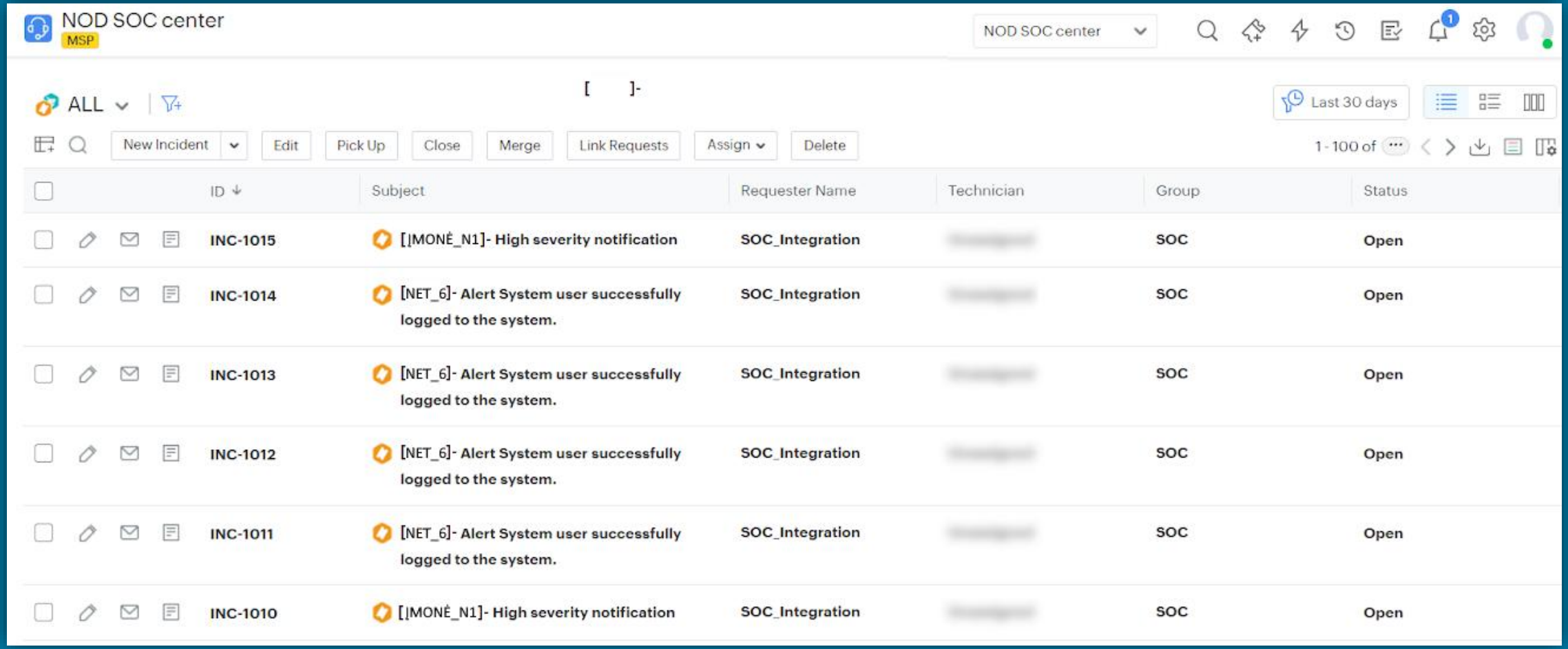
Trumpas aprašymas (Short description): Aptiktas portable programos tor.exe naudojimas bei išorinė komunikacija su prastos reputacijos IP adresu.
Kategorija (Detection Category): Kitos grėsmės priežastys
Kritiškumas (Criticality): Medium
Aptikimo laikas (Detection Timestamp): Sep 1, 2025, 3:26:08 PM
Paveiktų įrenginių/naudotojų skaičius: 1
Aptikti grėsmių indikatoriai:
SHA1: E7659E9BD45856DA7CF7740194543A4B3F1B4DF3
Hostname: [redacted]
Username: [redacted]
Command line: outbound tor://45.95.169.104:7430
Triggering process: tor.exe

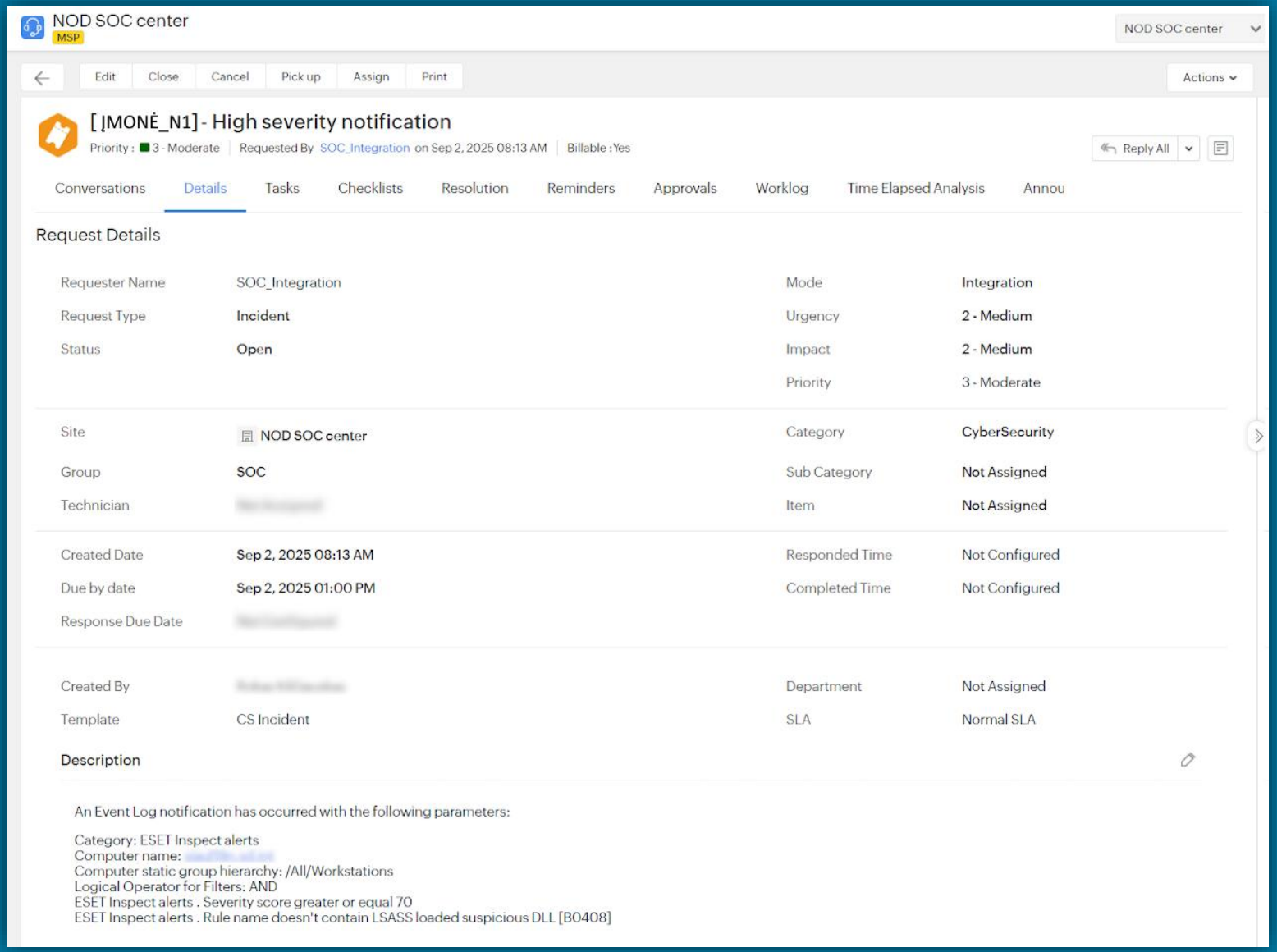
Detalus aptikimo aprašymas:
Kompiuteryje [redacted] naudotojas [redacted] paleido portable programą tor.exe, kuri su komanda "outbound tor://45.95.169.104:7430" per anoniminį TOR tinklą sukomunikavo su išoriniu prastos reputacijos serveriu (IP:45.95.169.104).

Rekomenduojami veiksmai:
a) siūlome kreiptis į darbuotoją ir išsiaiškinti, kokioms tiesioginėms darbo funkcijoms prireikė naudoti TOR programėlę;
b) įspėti darbuotoją apie TOR tinkle slypinčius pavojus;
c) uždrausti TOR programėlių naudojimą bei leisti mums sukurti taisyklę, kuri blokuotų panašaus tipo programas bei komunikacijas.

Recommended actions *None*

NOD BALTIC


NOD SOC center
MSP
NOD SOC center
ALL
Last 30 days
New Incident
Edit
Pick Up
Close
Merge
Link Requests
Assign
Delete
1 - 100 of
ID
Subject
Requester Name
Technician
Group
Status
INC-1015
[ĮMONĖ_N1]- High severity notification
SOC_Integration
SOC
Open
INC-1014
[NET_6]- Alert System user successfully logged to the system.
SOC_Integration
SOC
Open
INC-1013
[NET_6]- Alert System user successfully logged to the system.
SOC_Integration
SOC
Open
INC-1012
[NET_6]- Alert System user successfully logged to the system.
SOC_Integration
SOC
Open
INC-1011
[NET_6]- Alert System user successfully logged to the system.
SOC_Integration
SOC
Open
INC-1010
[ĮMONĖ_N1]- High severity notification
SOC_Integration
SOC
Open


NOD SOC center
MSP
NOD SOC center
Edit
Close
Cancel
Pick up
Assign
Print
Actions
[ĮMONĖ_N1] - High severity notification
Priority : 3 - Moderate
Requested By SOC_Integration on Sep 2, 2025 08:13 AM
Billable : Yes
Reply All
Conversations
Details
Tasks
Checklists
Resolution
Reminders
Approvals
Worklog
Time Elapsed Analysis
Annou
Request Details
Requester Name
SOC_Integration
Request Type
Incident
Status
Open
Mode
Integration
Urgency
2 - Medium
Impact
2 - Medium
Priority
3 - Moderate
Site
NOD SOC center
Group
SOC
Technician
Category
CyberSecurity
Sub Category
Not Assigned
Item
Not Assigned
Created Date
Sep 2, 2025 08:13 AM
Due by date
Sep 2, 2025 01:00 PM
Response Due Date
Responded Time
Not Configured
Completed Time
Not Configured
Created By
Template
CS Incident
Department
Not Assigned
SLA
Normal SLA
Description
An Event Log notification has occurred with the following parameters:
Category: ESET Inspect alerts
Computer name:
Computer static group hierarchy: /All/Workstations
Logical Operator for Filters: AND
ESET Inspect alerts . Severity score greater or equal 70
ESET Inspect alerts . Rule name doesn't contain LSASS loaded suspicious DLL [B0408]

PASLAUGŲ KREPŠELIS

PASLAUGŲ KREPŠELIS

Saugumo paslaugų paketai	Inžinieriaus pagalba Starter	Premium palaikymas	Aptikimas ir reagavimas (MDR)	Išorinio SOC paslauga
Pagalba darbo vietų ir serverių saugumo produktams	+	+	+	+
ESET Inspect palaikymas	+	+	+	+
Paslaugos teikimas (SLA)	-	+	+	+
Incidento tyrimas	+/-	+	+	+
Proaktyvi grėsmių medžioklė	-	-	+	+
Darbo vietų ir serverių stebėjimas	-	-	+	+
Tinklo įrenginių stebėjimas	-	-	-	+
API integracijos	-	-	-	+
Pažeidžiamumų aptikimas	-	-	-	+
Prieiga prie ESET Education portalo	Iki 2 asm.	Iki 5 asm.	Iki 5 asm.	Iki 5 asm.
Aptikimų aptarimo sesijos	1 sesija /mėn.	Iki 4 sesijų /mėn.	Neribotos	Neribotos
Mėnesinė grėsmių ataskaita ir rekomendacijos	-	-	+	+

Galimybė įsigyti papildomai:

Įsilaužimų testavimo paslauga	Priega prie ESET Education portalo	Incidento tyrimo paslauga
Kibernetinio saugumo mokymų paslauga	Socialinės inžinerijos pratybos	Mokymų ir fišingo atakų simuliacijos platforma

TAKE AWAY

Investicija į SOC: mažesnė rizika ir didesnis saugumas

SOC - neatskiriama organizacijos saugumo širdis

KLAUSIMAI?

SUSISIEKIME:

NOD BALTIC
Ramūnas Liubertas
ramunas@nodbaltic.com

https://nodbaltic.com

Bendraukime