



**SECURITY
DAYS**

**NUO ASMENINĖS
ATSAKOMYBĖS IKI
BENDROS JĖGOS:
SEKTORINIO
ATSPARUMO
ARCHITEKTŪRA
LIETUVOJE**



DR. VILIUS BENETIS

„NRD Cyber Security“
vadovas

Mūsų veikla

- Kibernetinio saugumo operacijų kūrimas
- Kibernetinės saugos vertinimas
- Kibernetinio saugumo technologiniai sprendimai

Klientai

Privataus sektoriaus organizacijos bei valstybinės institucijos.

Veiklos principai

Kibernetinėms atakoms vis stiprėjant, nuolatos ieškome naujų būdų kovoti su kibernetinėmis grėsmėmis tiek pritaikydami jau esamus modelius ir technologijas, tiek patys investuodami į naujų kūrimą.

Projektų geografija

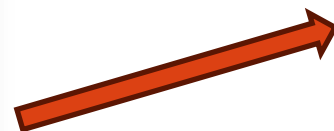


Ši vasara - galinga!

2026-06-03

ncsi.ega.ee/ncsi-index/?order=rank

NCSI national cyber security index				
INDEX METHODOLOGY SERVICES FAQ ABOUT US NCSI 2016-2023				
ALL COUNTRIES TERRITORIES				
Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	 Czechia	98.33	72.93	25.40
2.	 Canada	96.67	78.14	18.53
3.	 Estonia	96.67	82.56	14.11
4.	 Finland	95.83	85.76	10.07
5.	 Lithuania	95.00	75.53	19.47
6.	 Moldova (Republic of)	94.17	62.66	31.51
7.	 Belgium	94.17	73.55	20.62
8.	 Jordan	93.33	57.77	35.56
9.	 Hungary	93.33	67.88	25.45
10.	 Albania	92.50	62.34	30.16
11.	 Romania	92.50	64.57	27.93
12.	 Slovakia	92.50	67.55	24.95
13.	 Poland	92.50	73.21	19.29
14.	 Germany	90.83	75.73	15.10



2026-09-03

NCSI national cyber security index

INDEX METHODOLOGY SERVICES FAQ

ALL COUNTRIES TERRITORIES

Rank	Country	National Cyber Security Index
1.	 Albania	98.33
2.	 Finland	95.83
3.	 Lithuania	95.00
4.	 Estonia	94.17
5.	 Jordan	93.33
6.	 Hungary	93.33
7.	 Romania	92.50
8.	 Moldova	90.83
9.	 Poland	90.00
10.	 Italy	90.00
11.	 Czechia	89.17
12.	 Slovenia	89.17
13.	 France	89.17
14.	 Spain	89.17
15.	 Denmark	89.17
16.	 Ukraine	88.33
17.	 Slovakia	87.50
18.	 Latvia	87.50

National Cyber Security Defence Architecture

3 Lines of Defence

1

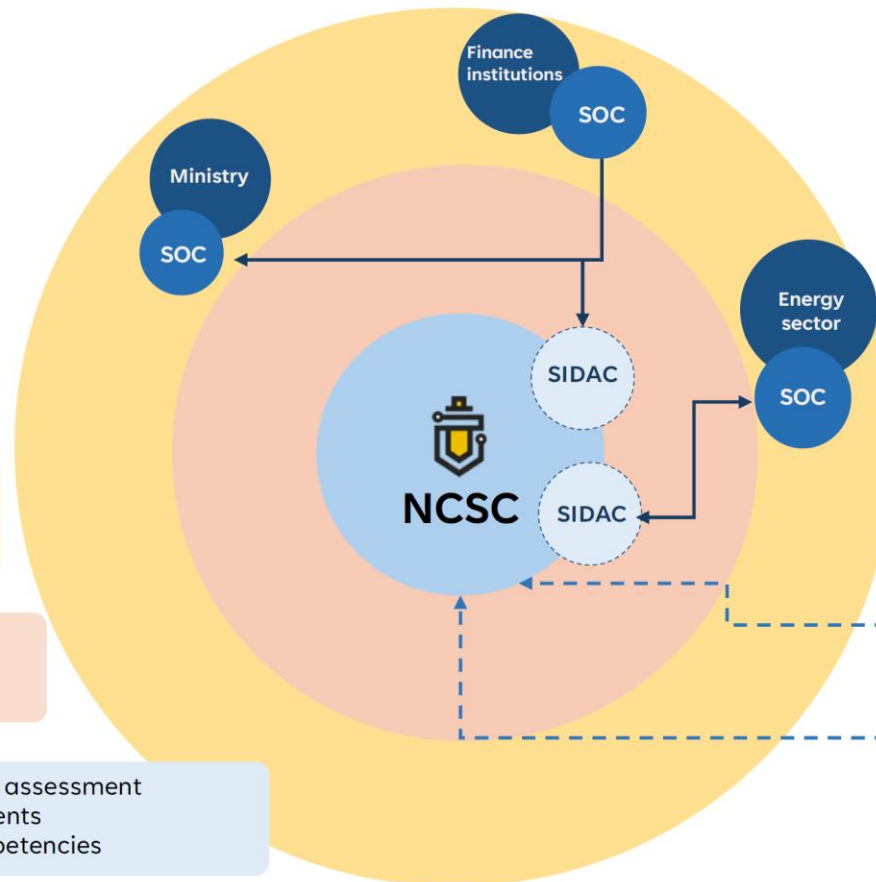
- Continuous monitoring
- Incident and vulnerabilities management

2

- Threat intel exchange
- Mutual aid / support

3

- National situational awareness and assessment
- Support mitigating significant incidents
- Support building maturity and competencies



Stakeholders

Essential / Important Organization

Organization's Cyber Security Operations Centre (SOC)

SECTORIAL Information exchange and analysis (Virtual | CHAT | MISP)

National Cyber Security Centre (CSIRT-LT)

National and international partners (CTI+)



Už kibernetinį saugumą atsakingas išteklių savininkas

Tai kokia nauda iš sektorinio, kai šis atsakingas tik už “orą”?



Kokie individualių organizacijų - išteklių savininkų - norai ir poreikiai:

1



Žinios ir resursai

Turėti reikiamas žinias ir resursus reaguojant į kibernetinio saugumo grėsmes.

2



Galimybė atsiremti į kitus

Įskaitant: Galėti atsiremti į kitų žinias ir rankas/galvas, kai:

- Reikia greičiau aptikti ir identifikuoti kibernetinio saugumo bėdas.
- Valdyti / spręsti incidentus.

Sektorinis poreikis: atsparesnės organizacijos

Kiekvienos organizacijos atsparumas didėja, kai:

1



Pasiekiamos žinios atsparumui gerinti

Sektoriai naudoja specializuotus veiklos procesus ir technologijas, todėl dalis informacijos yra specifinė.

2



Pasitikėjimas ir bendruomenė

- Augina norą padėti ir prisidėti.
- Skatina proaktyvumą tarp bendruomenės narių.
- Pagal veiklos pobūdį formuojasi natūralios bendruomenės.

3



Patikrinta atsparumo būklė

Yra patikrintas žinojimas, kokia reali atsparumo ir veiklos tęstinumo bei krizių valdymo būklė.

ENISA kuriama SIM3-CCM kibernetinių krizių valdymo brandos vertinimo metodika

Metodika: įsivertinimas

39 parametrai (iš kurių - 8 nauji šiam modeliui):

O Organizaciniai

Naujų parametrų nėra

H Žmogiškieji ištekliai

1 naujas parametras

H-CCM-1 Pratybos

T Įrankiai

1 naujas parametras

T-CCM-1 Krizių valdymo infrastruktūra

P Procesai

6 nauji parametrai

P-CCM-1 Mokymosi procesas

P-CCM-2 Pasirengimo testavimas

P-CCM-3 Krizių valdymas

P-CCM-4 Išteklių mobilizavimas

P-CCM-5 Krizės paskelbimas

P-CCM-6 Krizės deeskalavimas

Sektorinis poreikis: atsparesnės organizacijos

Kiekvienos organizacijos atsparumas didėja, kai:

1



Pasiekiamos žinios atsparumui gerinti

Sektoriai naudoja specializuotus veiklos procesus ir technologijas, todėl dalis informacijos yra specifinė.

2



Pasitikėjimas ir bendruomenė

Augina norą padėti ir prisidėti,
Skatina proaktyvumą tarp bendruomenės narių.
Pagal veiklos pobūdį formuojasi natūralios bendruomenės.

3



Patikrinta atsparumo būklė

Yra patikrintas žinojimas, kokia reali atsparumo ir veiklos tęstinumo bei krizių valdymo būklė.

Sektorinių centrų tipai



Sutelktiniai / bendradarbiavimo / resursų pasidalinimo centrai

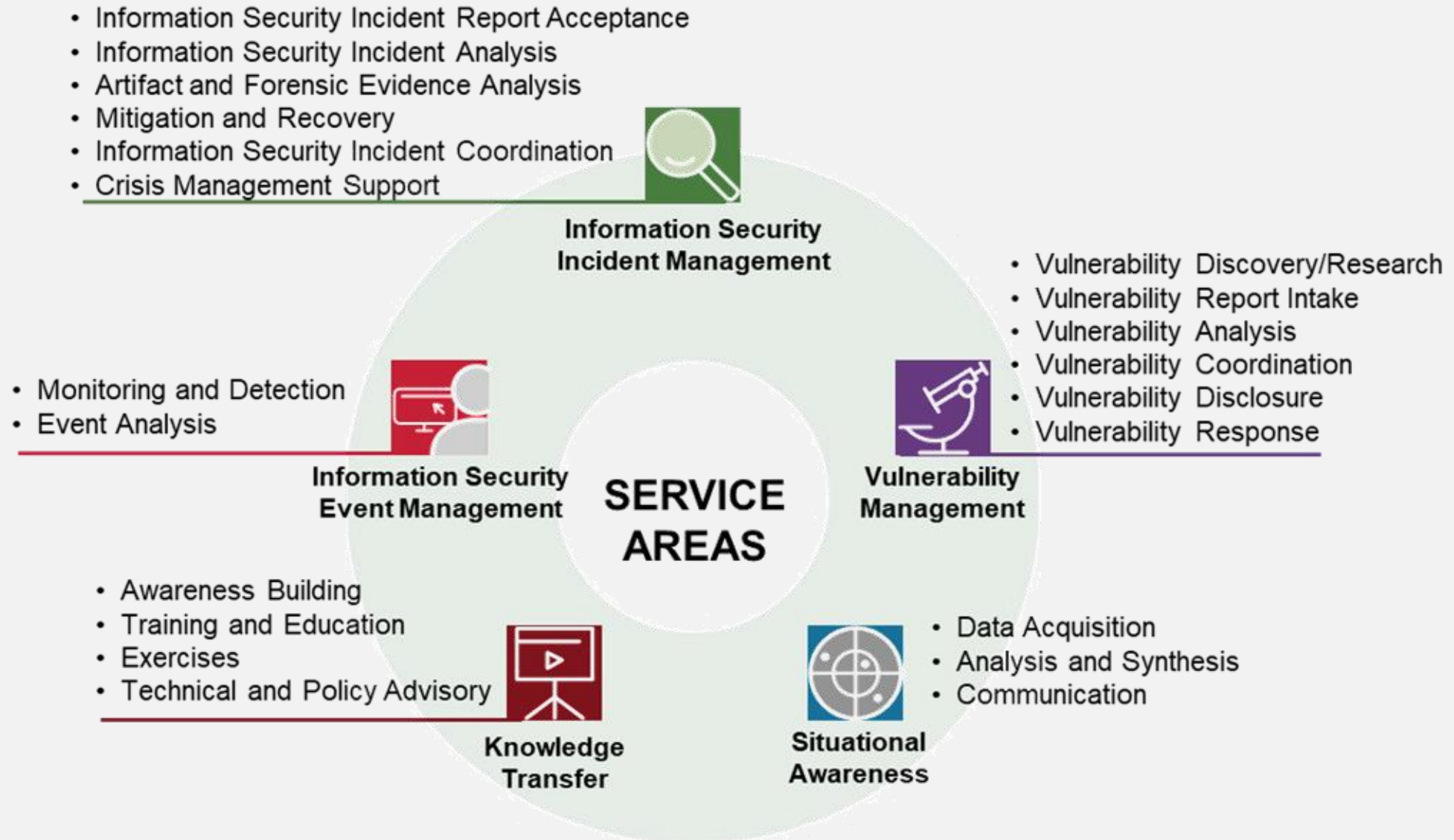
- Aplinkos ministerijos
- Vandens jėgos
- Kauno klinikų pažeidžiamumų valdymo (konstruojamas)
- LitnetCERT
- Nordic Financial CERT
- Danijos energetikos SektorCERT
- Olandų savivaldybių CERT
- Olandų sveikatos sektoriaus Z-CERT



Reguliacinė pagalba ir priežiūra

- Egipto, Nigerijos, Kenijos, Europos finansiniai CSIRT
- GovCERT įvairiose šalyse

Centrų paslaugų modelis



Apjungtos jėgos: Sektorinio atsparumo architektūra Lietuvoje – kokia ji bus?

Tikriausiai - sektoriai CSIRT/SOC/ISAC Lietuvoje bus įvairūs, nevienodi:

- Paslaugomis, narystėmis, finansavimo modeliu, darbuotojų profiliais.

Mano palinkėjimas kiekvienam iš jūsų pagalvoti:

- Koks jūsų lūkestis sektorinei kibernetinei saugai? Ko norėtumėte?
- Kokią rolę užimsite?
Pasyvia – stebėti, kad konstruojasi tokie centrai
Aktyvia – diskutuosite, gryninsite, kaip geriausiai veiktų jūsų sektorius



Kviečiu susijungti ir kalbėtis – kaip konstruoti atsparią Lietuvą, kurioje gera ir bendruomeniška gyventi!