

Informacinio saugumo vadovo (CISO) vaidmuo ir vertė organizacijai

Grigorij Strelec, 2026

Išvadas

Organizacijos šiandien veikia vis sudėtingesnėje skaitmeninėje aplinkoje.

Pagrindiniai iššūkiai:



sparčiai augančios
kibernetinės
grėsmės



ransomware ir
duomenų nutekėjimo
incidentai



didėjantis IT sistemų
sudėtingumas



priklausomybė nuo
debesijos ir tiekėjų



griežtėjantys teisės
aktų reikalavimai
(NIS2, nacionaliniai
teisės aktai)

Todėl kibernetinis saugumas tampa **ne tik IT, bet ir verslo rizikos valdymo klausimu.**

Kas yra CISO?

CISO (Chief Information Security Officer) – organizacijos informacinio saugumo vadovas.

Pagrindinis tikslas: užtikrinti, kad organizacijos informacinis saugumas būtų strategiškai valdomas ir kontroliuojamas.

CISO atsako už:

- » kibernetinio saugumo strategiją
- » rizikų valdymą
- » incidentų valdymą
- » saugumo politiką ir procesus
- » atitiktį teisės aktams
- » saugumo kultūros formavimą organizacijoje



Informacinio saugumo realybė



Daugelyje organizacijų informacinis saugumas

- priskiriamas IT skyriui kaip papildoma funkcija
- neturi aiškaus strateginio valdymo
- dokumentacija ir procesai būna fragmentuoti
- incidentai sprendžiami reaktyviai

Daugelyje organizacijų informacinis saugumas

- ✗ nėra aiškaus rizikų valdymo
- ✗ neapibrėžta atsakomybė
- ✗ nepakankamas vadovybės įsitraukimas
- ✗ sunku užtikrinti atitiktį reguliavimui

CISO vaidmuo organizacijoje

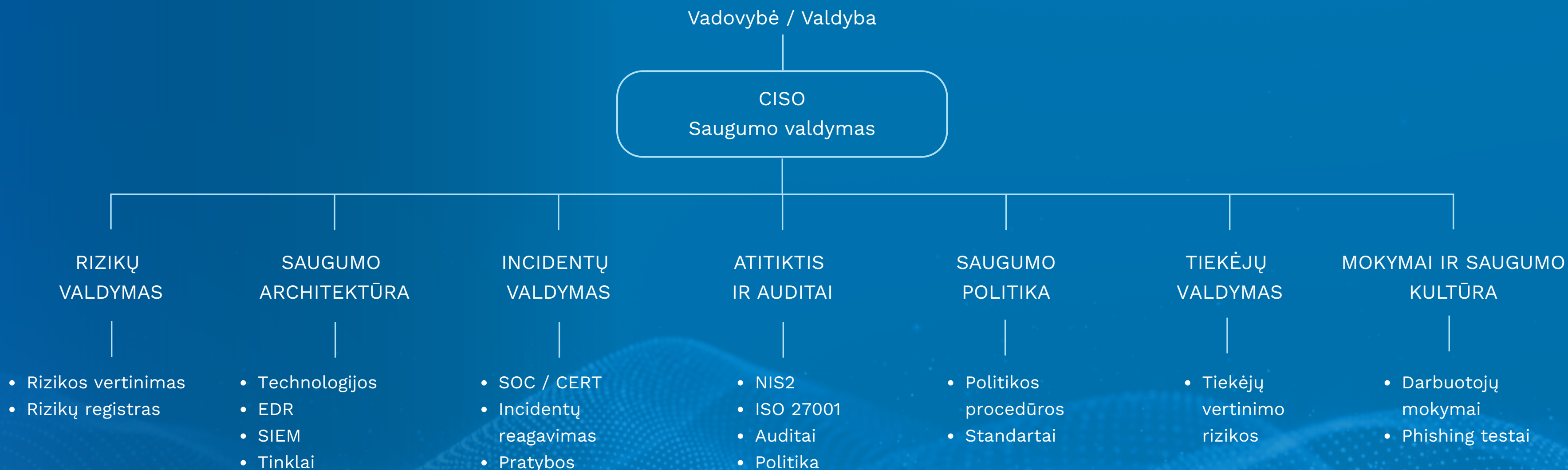
CISO veikia kaip **tiltas tarp technologijų, verslo ir vadovybės.**



CISO užtikrina, kad saugumas būtų integruotas į **visus organizacijos procesus.**

CISO vaidmuo organizacijoje

CISO užtikrina, kad organizacijos kibernetinis saugumas būtų valdomas sistemiškai – apimant technologijas, procesus, reguliacinius reikalavimus ir žmones.



Pagrindinės CISO atsakomybės

Strategija

- » Saugumo strategijos kūrimas
- » Saugumo programos planavimas

Rizikų valdymas

- » Reguliari rizikų analizė
- » Rizikų registro priežiūra

Atitiktis

- » Teisinių reikalavimų laikymasis
- » Standartų taikymas (pvz., ISO 27001)

Incidentų valdymas

- » Incidentų valdymo procesas
- » Pratybos ir pasirengimas incidentams

Saugumo kultūra

- » Darbuotojų mokymai
- » Saugumo sąmoningumo didinimas



Kokią vertę organizacijai kuria CISO

CISO suteikia organizacijai strateginę vertę.

1

Kibernetinio saugumo rizikų mažinimas

Sisteminis rizikų identifikavimas ir valdymas.

2

Aiškus informacinio saugumo valdymas

Apibrėžtos atsakomybės ir procesai.

3

Atitiktis teisės aktams

Organizacija pasirengusi auditams ir reguliavimo reikalavimams.

4

Verslo tęstinumas

Mažesnė veiklos sutrikimų tikimybė.

5

Informuoti sprendimai vadovybei

Vadovybė gauna aiškias saugumo ataskaitas ir rekomendacijas.



Informacinio saugumo valdymo trūkumo pasekmės

Kai organizacijoje nėra aiškaus saugumo valdymo:

- ❖ Rizikos lieka neidentifikuotos
- ❖ Incidentai valdomi chaotiškai
- ❖ Saugumo priemonės diegiamos fragmentiškai
- ❖ Dokumentacija neatitinka realios situacijos
- ❖ Sudėtinga užtikrinti reguliacinę atitiktį

Ilgainiui tai gali sukelti:

- ❖ Finansinius nuostolius
- ❖ Reputacijos žalą
- ❖ Veiklos sutrikimus



Ar kiekvienai organizacijai reikia CISO?

Didelėse organizacijose dažniausiai dirba **pilno etato CISO**.

Tačiau daugeliui organizacijų kyla iššūkių:



Aukštos kvalifikacijos specialistų trūkumas



Dideli darbo užmokesčio kaštai



Ne visada reikalingas pilnas etatas



Todėl svarbu rasti **efektyvų būdą užtikrinti saugumo valdymą.**

Alternatyva: CISO kaip paslauga

Viena iš alternatyvų – **CISO as a Service** modelis.

Organizacija gauna:

- Strateginę kibernetinio saugumo kompetenciją
- Reguliarią saugumo priežiūrą
- Rizikų vertinimą ir auditą
- Saugumo dokumentacijos parengimą
- Konsultacijas vadovybei

Tai leidžia užtikrinti profesionalų saugumo valdymą **be pilno CISO etato**.



Metinis kibernetinio saugumo valdymo ciklas

Pavyzdinis CISO veiklos ciklas organizacijoje.

I

1 ketvirtis

- » Esamos situacijos analizė
- » Trūkumų (GAP) analizė

II

2 ketvirtis

- » Saugumo politikų ir procedūrų atnaujinimas
- » Procesų diegimas

III

3 ketvirtis

- » Rizikos vertinimas
- » Saugumo priemonių peržiūra

IV

4 ketvirtis

- » Auditai
- » Incidentų pratybos
- » Metinė saugumo ataskaita vadovybei

Apibendrinimas

- Kibernetinis saugumas yra **verslo rizikos valdymo dalis**
- CISO užtikrina **strateginį informacinio saugumo valdymą**
- Organizacijoms svarbu turėti priskirtą saugumo atsakomybę
- CISO funkcija gali būti įgyvendinama **viduje arba kaip paslauga**

Efektyvus kibernetinio saugumo valdymas stiprina organizacijos atsparumą.



Ačiū už dėmesį.

