



Vidinis tyrimas – tyriminiai įgūdžiai ir efektyvi komunikacija su finansinės žvalgybos padaliniu

Greta Barkauskienė
CFCS, PPPKC ekspertė





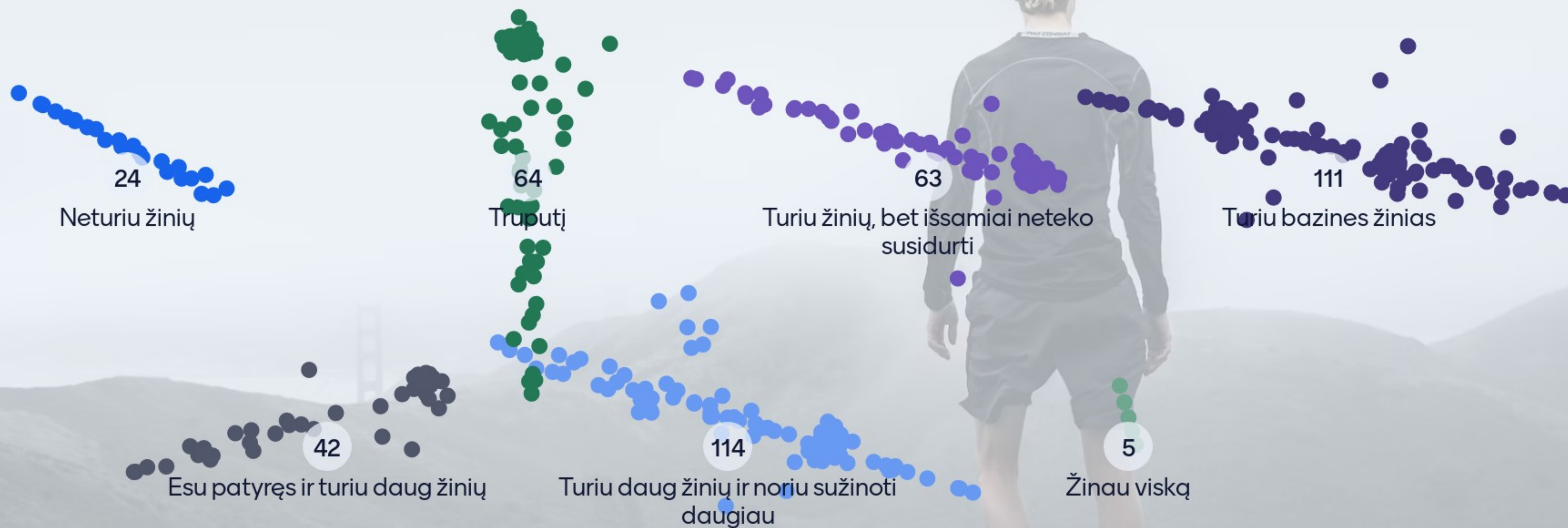
Instrukcija





Prieš paskaitą pasitikrinkime

Apie vidinį tyrimą žinau...



Šiandienos planas

- Kokybę lemiantys veiksniai
- Žingsniai efektyviam vidinio tyrimo organizavimui
- Turimos informacijos identifikavimas
- Būdai praplėsti turimos informacijos lauką
- Pagrindai sėkmingai komunikacijai su FŽP padaliniu

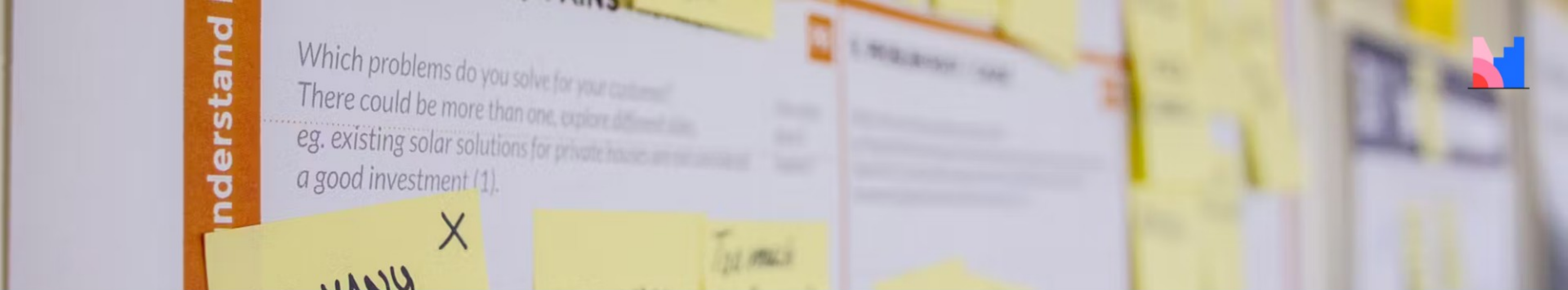




Vidinio tyrimo (analizės) kokybę lemiantys veiksniai

- turimų duomenų kiekis
- analitiko (-ų) įgūdžiai ir žinios
- tyrimo laiko kiekis
- sėkmė :)





Skirtingi tyrimai

Analizės/tyrimo apimtis ir metodai skirsis, priklausomai nuo to, kas atlieka analizę/tyrimą. Valstybės paprastai turi didesnes galimybes analizei nei privataus sektoriaus specialistai, todėl metodai gali skirtis. Taip pat, svarbu neperžengti tyrimo apimties.



Tinkamai fiksuojamas vidinis tyrimas

Itin svarbu fiksuoti vidinio tyrimo žingsnius,
nes informacija, laikui bėgant gali kisti.
Pravartu žinoti ir suprasti, kaip galovojo
tyrimą atlikęs asmuo, perduodant tyrimo
medžiagą.





Prieš pradedant analizę, vidinio tyrimo metu, svarbu...

Atsiriboti nuo išankstinių nuostatų - analizės tikslas yra išsiaiškinti, ar veikla įtartina, o ne ieškoti, kokį įtartinumo kriterijų turimi duomenys gali atitikti.





Svarbu prisiminti (1)

Informacija vertinama sistemiškai.

Paskubėjus padaryti išvadas, rizikuojama, kad vidinis tyrimas bus atliktas nevisapusiškai, o informacija įvertinta netinkamai. Taip pat, egzistuoja rizika tyrimą pakreipti "netinkama linkme" ieškant, kaip pagrįsti išankstinius įtarimus.





Svarbu prisiminti (2)

- Ne visada "prastai" parašytos sutartys signalizuoja, kad veikla įtartina
- Kliento pažinimo anketa yra įtartinos veiklos analizės pamatas, todėl svarbu ją laiku atsinaujinti
- Tinkamai ir laiku užduoti klausimai klientui gali pakreipti tyrimą sėkminga kryptimi
- Analizuojame žingsnis, po žingsnio, kol susidėlioja "bendras vaizdas"
- Viešieji šaltiniai gali labai pasitarnauti išpečiant savo turimas žinias





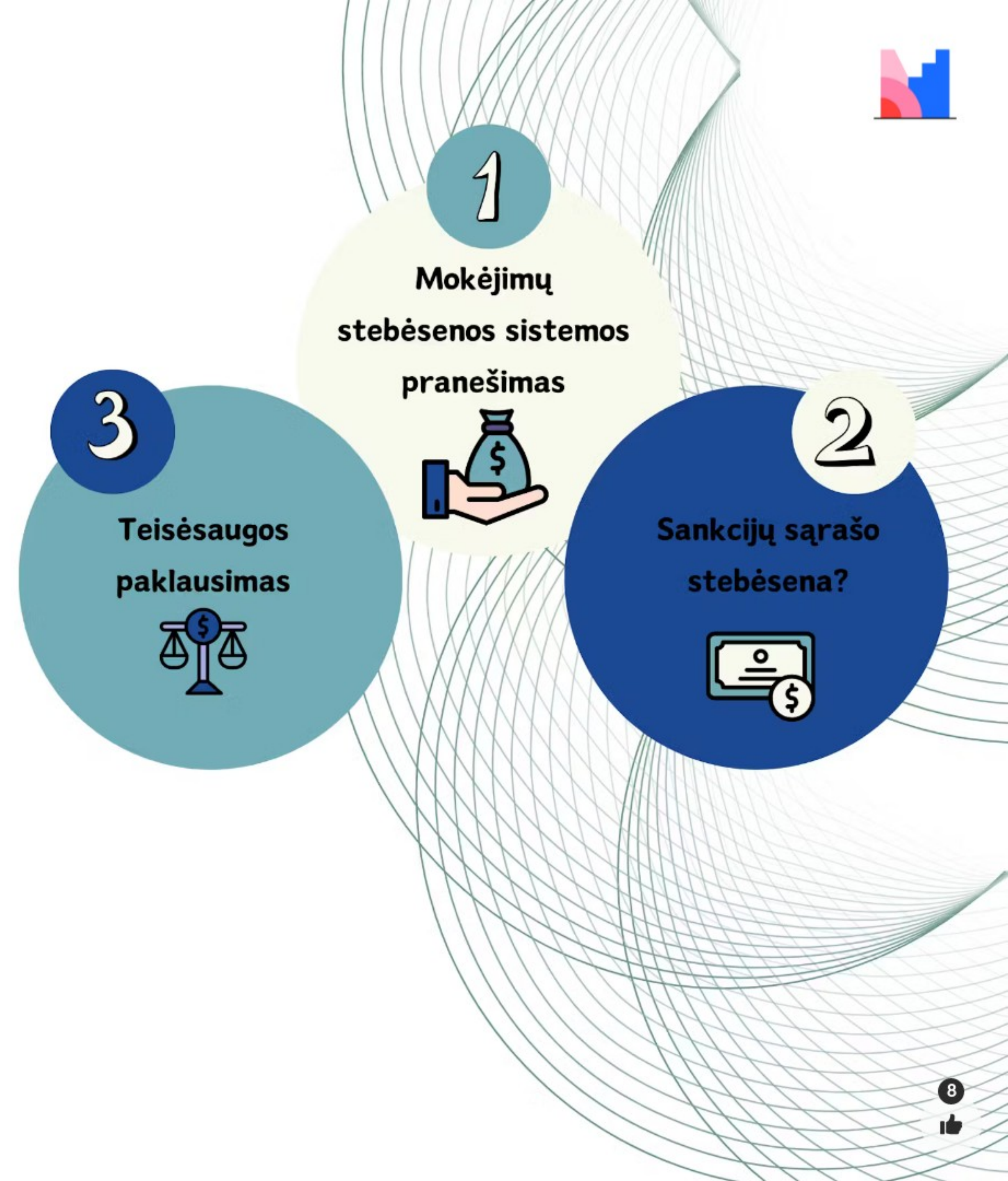
1 žingsnis - išsiaiškiname, kodėl prasidėjo vidinis tyrimas



Kodėl analizuojame?

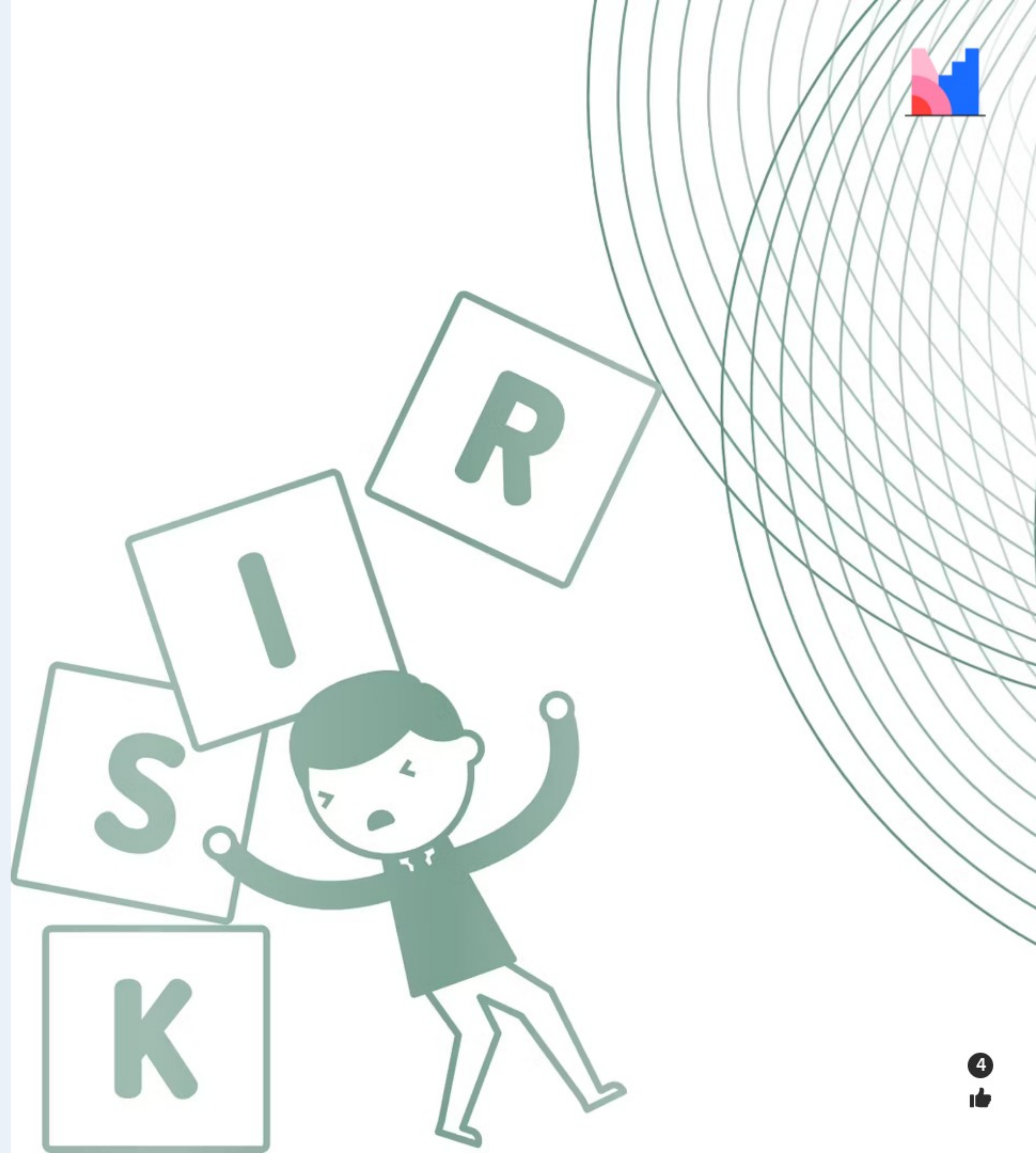
Tai yra trys įprasti tyrimų priežasčių pavyzdžiai, tačiau, atsižvelgiant į jūsų vaidmenį ir organizaciją, gali būti ir kitų, pvz., vidinių užklausų ar įspėjimų iš verslo linijų.

Svarbu nepamiršti, kad visi šie atvejai signalizuoja apie galimos rizikos lygį.



Rizika

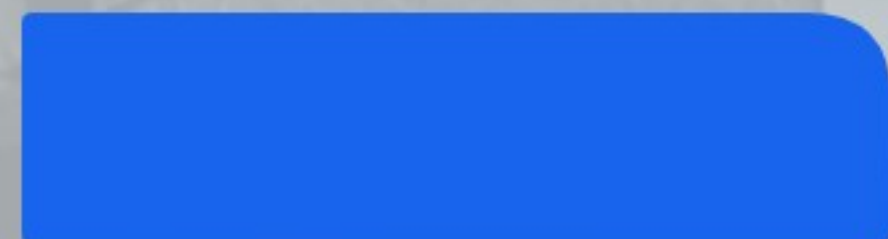
- Klientų tipai (fiziniai ir juridiniai asmenys)
- Produktas/transakcija
- Geografinė lokacija
- Kanalas





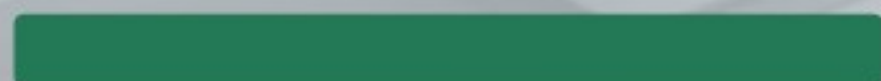
Kaip manote, ką pirmiausia reikia peržiūrėti mokėjimų stebėsenos sistemai sustabdžius mokėjimą?

37



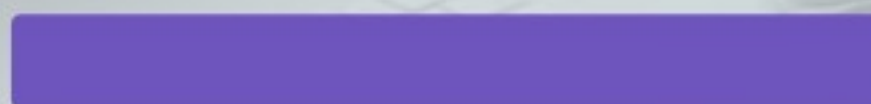
kliento KYC anketa

9



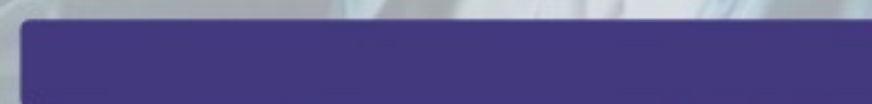
operacijos sumos dydį

13



Mokėjimo paskirtį

12



siuntėjo informaciją

217



Koks rizikos scenarijus
"aktyvavosi"

22



288





2 žingsnis - įsivertiname turimą informaciją





Paprastai turimi duomenys (galimybės)

- Kliento profilis (KYC)
- Sąskaitos išrašas
- Kiti vidiniai organizacijos duomenys (pvz., klientų aptarnavimo komandos komunikacija su klientu)
- Identifikuojame kitus, susijusius asmenis

OSINT





Išreitinguokite žemiau esančius teiginius

Vidiniam tyrimui viešieji šaltiniai neturi įtakos.

1.7

Viešųjų šaltinių analizė yra sudėtinga.

3.0

Kas yra viešųjų šaltinių analizė???

2.2

Strongly Disagree

Strongly Agree

18



263





Paieška viešuosiuose šaltiniuose prasideda nuo savo saugumo užtikrinimo

Atsijunkite nuo visų paskirų, uždarykite nereikalingus langus, išsivalykite naršymo istoriją.





Kitos anonimiškumo užtikrinimo priemonės

- VPN paslauga
- Proxy serveriai
- Koduotos naršyklės (pvz., TOR, BRAVE, kt.)
- Smėlio dėžės aplinka (pvz., Virtual Machine)





Paieškos varikliai

- Google
- duck duck go
- Yandex
- Baidu
- Dogpile
- Carrot
- kiti





Boolean operator	Function	Example
AND	Provides results that contain both or all keywords	paradigm AND syntagm
OR	Provides results that contain either keyword	meteor OR meteorite
NOT or AND NOT	Provides results that contain the first keyword but not the second	football NOT soccer
Quotation marks ""	Provides results with the exact phrase	"Newtonian mechanics"
Parentheses ()	Allows you to group together keywords and control the order in which the terms will be searched	(rural OR urban) AND sociology
Asterisk *	Provides results that contain a variation of the keyword	Develop* This will return results containing words such as "development," "developer," and "developing."

Paieškos operatoriai





Google

site:amlcenter.lt filetype:pdf

Viskas Vaizdai Vaizdo įrašai Knygos Žiniatinklis Naujienos Finansai Įrankiai

Pinigų plovimo prevencijos kompetencijų centras
https://amlcenter.lt › 2022/07 › PPPKC_Brandbook PDF

Antrastes tekstas 1.1

Prieš užmegzdama Dalykinius santykius arba atlikdama Vienkartines operacijas ar sandorius, Įstaiga privalo patikrinti, ar Klientas, Vienkartines operacijas ...

39 puslapiai

Pinigų plovimo prevencijos kompetencijų centras
https://amlcenter.lt › uploads › 2022/07 PDF

I-ojo pusmečio mokymų rezultatai

Banko sektoriaus atstovai. EPJ. Teisėsaugos institucijos. Kredito unijos. Kiti sektoriai. Viešojo sektoriaus atstovai. Teisininkų kontoros ar advokatai.

Pinigų plovimo prevencijos kompetencijų centras
https://amlcenter.lt › 2024/03 › Centro-istatai PDF

viešosios įstaigos „pinigų plovimo prevencijos kompetencijų

Viešoji įstaiga „Pinigų plovimo prevencijos kompetencijų centras“ (toliau – Įstaiga) yra

Efektyvaus paieškos operatorių panaudojimo pavyzdys





https://ipinfo.io

Medium - Where g...mempool - Bitcoin...ArkhamSpot On Chain - Pla...Blockchain Analytic...Ethereum (ETH) Bkt...WHOIS History API...Ahrefs - SEO Tools...OpenSea, the large...Cryptocurrency Pric...Cryptocurrency Pric...

Explore our IP Address Database Downloads for instant access to our IP address insights

Learn more

IPinfoProductsSolutionsWhy IPinfo?PricingResourcesDocsLoginSign up

The Trusted Source For IP Address Data

Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.

Sign up for freeContact sales

213.197.138.142

ip: "213.197.138.142",

city: "Vilnius",

region: "Vilnius",

country: "LT",

loc: "54.6892,25.2798",

org: "AS15440 UAB "Baltnetos komunikacijos",

postal: "01001",

timezone: "Europe/Vilnius",

Your IP

8.8.4.4

AS15169

1.1.1.4

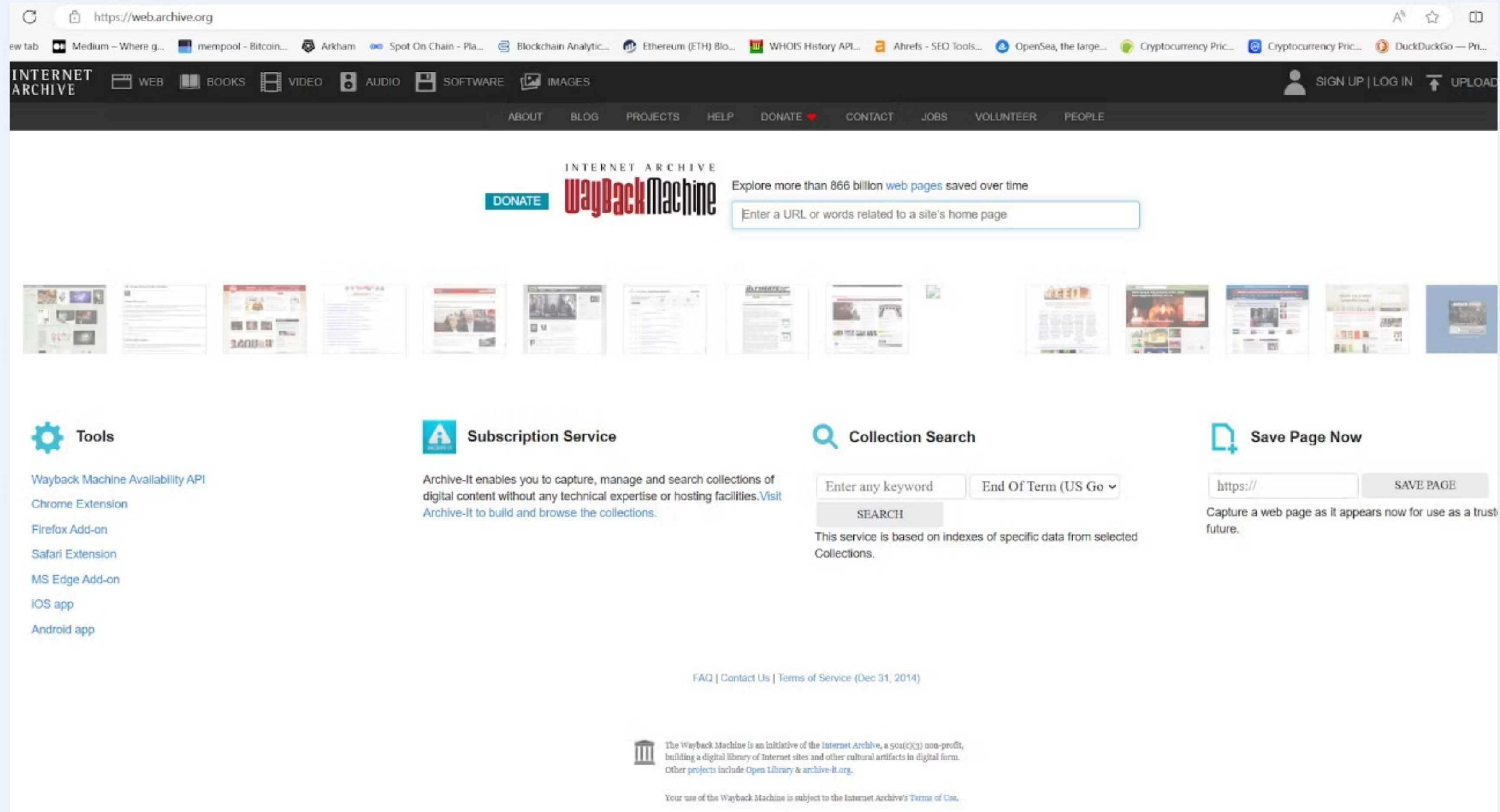
AS451!

Powering organizations around the world with reliable IP data

Customer stories >

<https://ipinfo.io/>





<https://web.archive.org/>



https://www.whoxy.com/whois-history/

Medium – Where g...mempool - Bitcoin...ArkhamSpot On Chain - Pla...Blockchain Analytic...Ethereum (ETH) Blo...WHOIS History API...Ahrefs - SEO Tools...OpenSea, the large...Cryptocurrency Pric...Cryptocurrency Pri

Our database now contains whois records of **556 Million** (556,395,015) domain names.

Login / Password / Signup

WHOXY
DOMAIN SEARCH ENGINE

Whois Lookup

Enter a domain name...

SEARCH

Home

Whois Lookup

Our Services

Pricing

Contact Us

Whois API / Whois History / Reverse Whois

Our [WHOIS API](#) returns consistent and well-structured WHOIS data in XML & JSON format. Returned data contain parsed WHOIS fields that can be easily understood by your application. Along with WHOIS API, we also offer [WHOIS History API](#) and [Reverse WHOIS API](#).

powered by
amazon
webservices

With support for **1563 TLDs**, our cloud-based API lets you quickly access any domain's WHOIS data through [Bulk Whois Lookup](#), [Newly Registered Domains](#), [Dropped Deleted Domains](#), [Expiring Domains](#) and [Whois Database Download](#).

Live Demo

Whois Lookup API

Whois History API

Reverse Whois API

UNBEATABLE
LOW PRICE
GUARANTEE!

Our Services	Price	Order
1000 WHOIS Lookup API Queries	\$2	Details
1000 WHOIS History API Queries	\$5	Details
1000 Reverse WHOIS API Queries	\$10	Details
Newly Registered Domains Database	\$495	Details
Whois Database [556 Million Domains]	\$10,000	Details

Free Account Signup • Zero Monthly Fee • Pay As You Go

Whois History

Simply enter a domain name below to check it's WHOIS History and Website Ownership History.

Whois History

Enter a domain name...

GO

DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
gymnasticplanet.com	Netistrar Limited	29 Sep 2006	31 Jul 2023	29 Sep 2024
yatisoftware.com	PDR Ltd. d/b/a PublicDomainRegistry.com	13 Sep 2023	13 Nov 2023	13 Sep 2024
durafabindustries.com	In2net Network, Inc.	12 Oct 2010	25 Oct 2023	12 Oct 2024
kilogs.com	NameCheap, Inc.	5 May 2021	5 May 2024	5 May 2025
thebeamstore.com	DomainPeople, Inc.	26 Oct 2005	30 Jun 2020	26 Oct 2029

www.whoxy.com

6



Ką dar galima rasti viešuosiuose šaltiniuose?

- Patikrinti IP adresus
- Istorinius svetainės duomenis
- Peržiūrėti retrospektyvius domeno duomenis
- Surasti atvaizdo šaltinį
- Pasitikrinti vardą
- Žemėlapiai
- Tvarkaraščiai
- kita





bellingcat

Investigations

Guides

Ukraine

Justice & Accountability

Workshops



EN ▾

Donate

How Russia's Invasion Flattened a Ukrainian Border City

October 28, 2024 Russia Ukraine

Scroll down ↓

<https://www.bellingcat.com/news/2024/10/28/how-russias-invasion-flattened-a-ukrainian-border-city/>

1

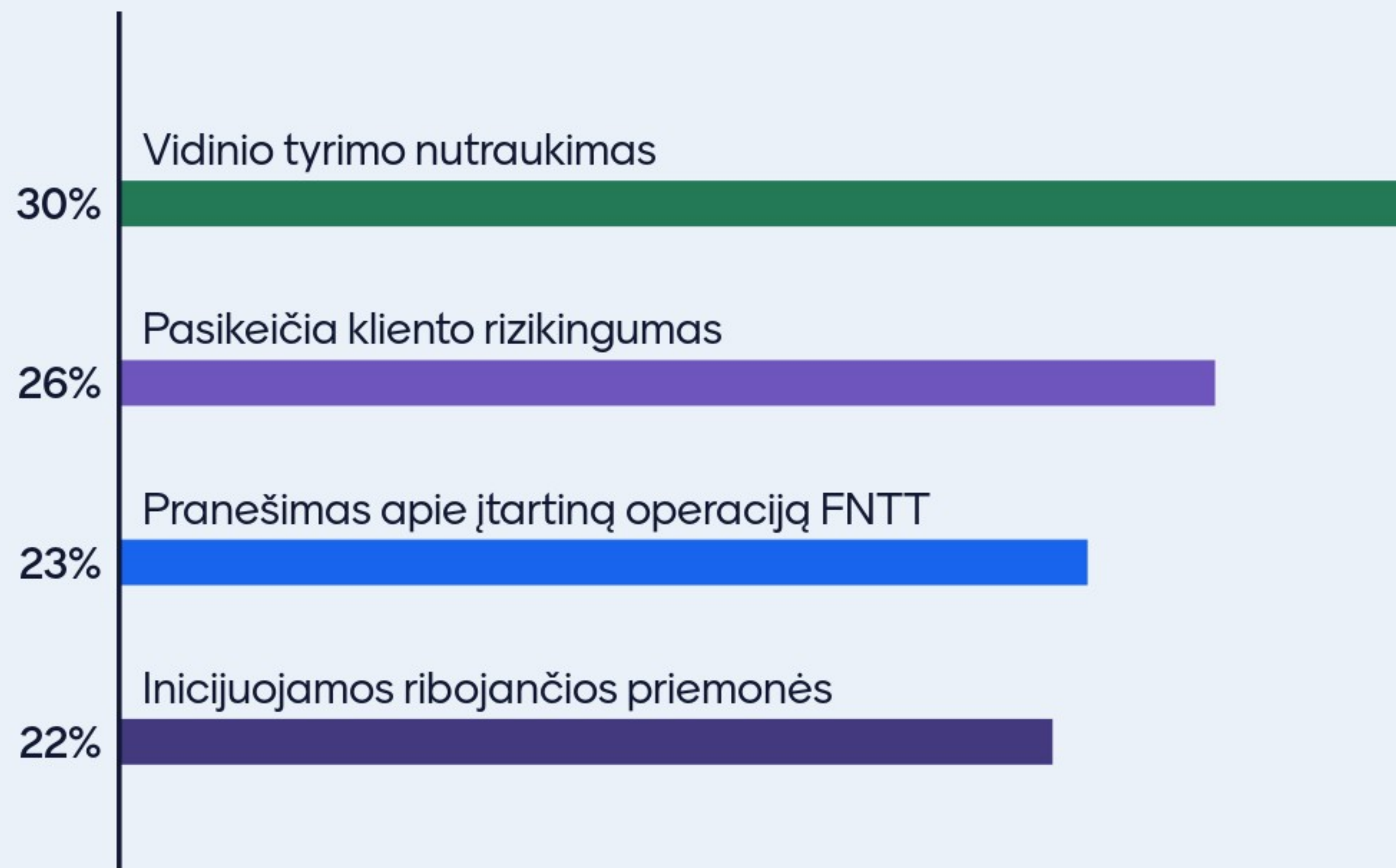




Ne visi vidiniai tyrimai privalo baigtis informacijos pateikimu FNNT



Kuri vidinio tyrimo baigtis jūsų praktikoje labiausiai tikėtina?





Sèkminga komunikacija su FŽP





Šaltiniai

- <https://opensea.io/> (open sea NFT)
- <https://academy.binance.com/en> (kripto pagrindai)
- <https://www.whoxy.com/> (retrospektyvi domeno paieška)
- <https://ahrefs.com/traffic-checker> (svetainės lankytojų srautas)
- perplexity.ai
- ipinfo.io (IP adreso analizė)
- <https://www.whoxy.com> (retrospektyvi domeno paieška)





Ačiū!

