NIS2 izaicinājumi

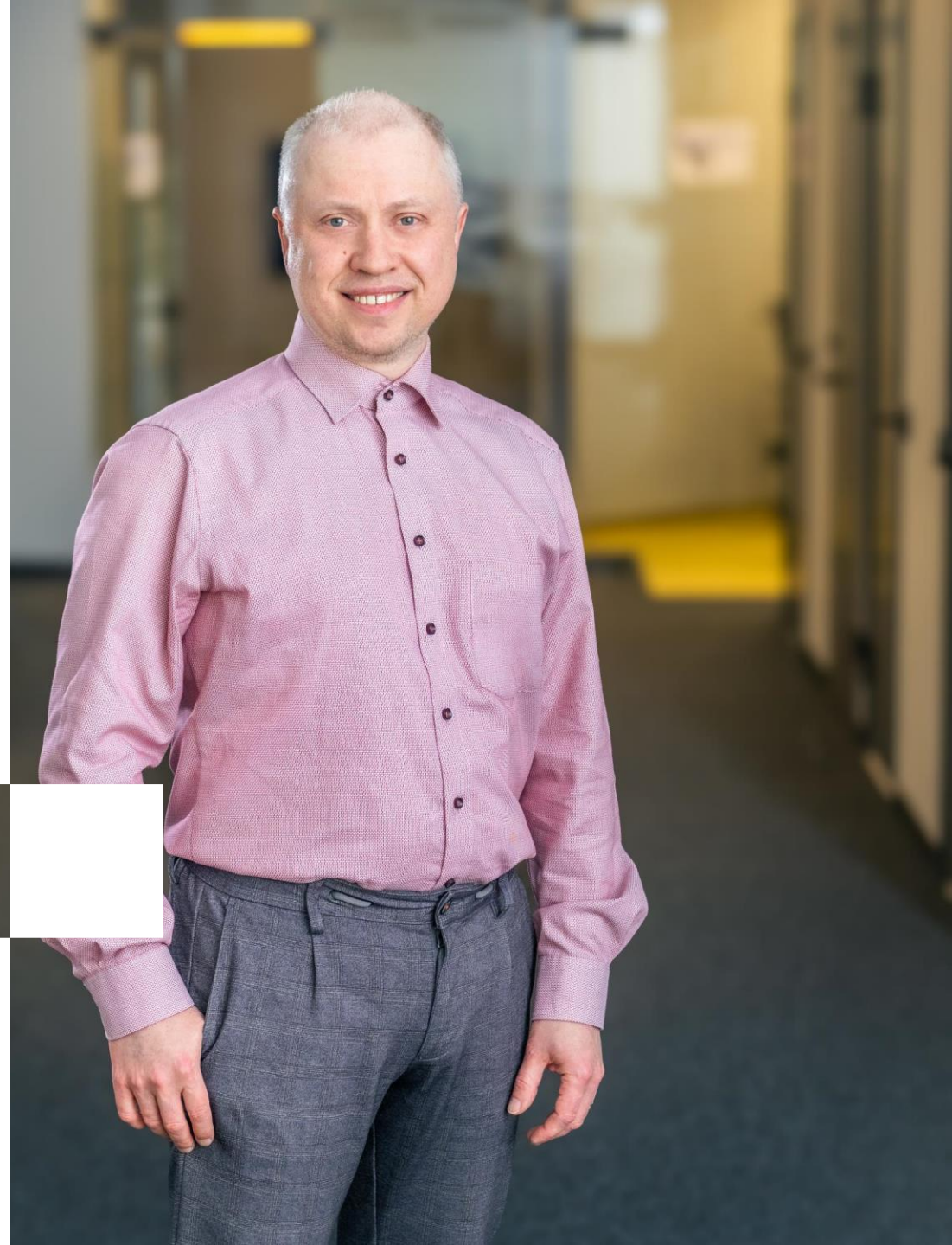
Papīri (politikas) jūs nepasargās no kiberincidentiem

Jānis Giniborgs
Informācijas tehnoloģiju drošības risinājumu vadītājs

squalio

Īsumā par mani

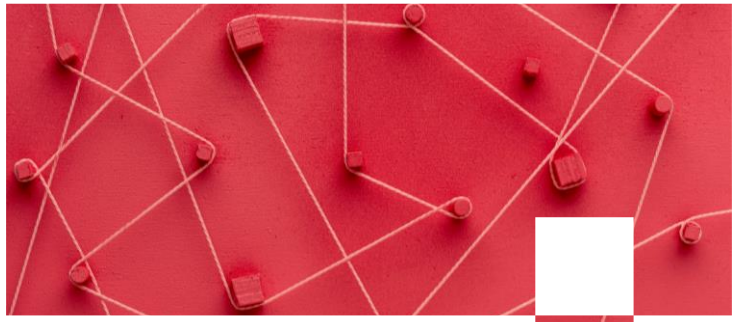
- Vairāk kā 23 gadi IT un drošības nozarē
- Sertificēts datu privātuma risinājumu inženieris
- Sertificēts informācijas drošību sistēmu inženieris
- Sertificēts informācijas sistēmu auditors



squalio

Ko prasa NIS2?

Kiberhigiēnas pamati



Kiberdrošības risku vadība

Piegādātāju risku vērtēšana

Incidentu pārvaldība un ziņošana

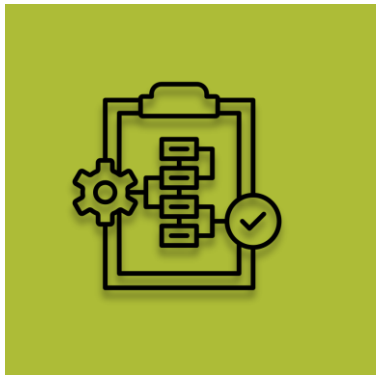
Datu šifrēšana un MFA

Lietotāju apmācība

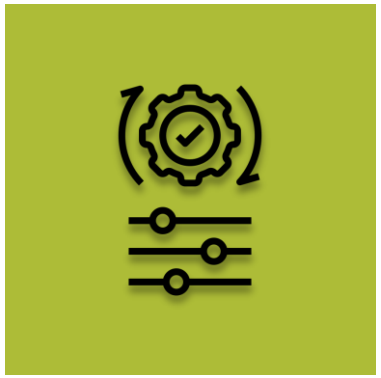
squalio

Atbilstība =/= Pareizi uzrakstīti dokumenti

Stabilai kiberdrošībai nepieciešamas šīs 3 lietas:



Politikas un procedūras

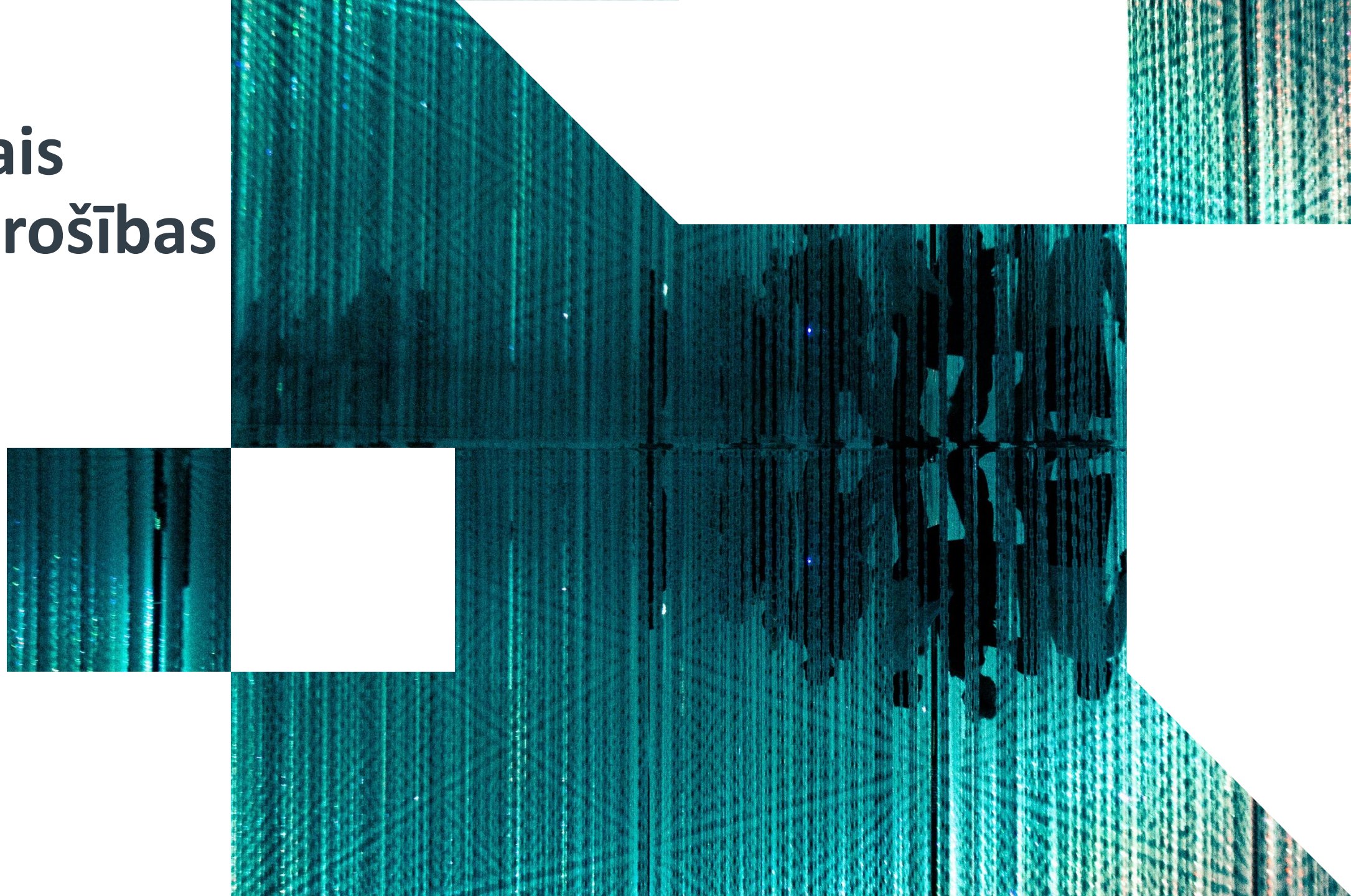


Tehniskās drošības kontroles sistēmās

Cilvēki, kas izpilda procedūras un pārrauga kontroles

squalio

Lielākais kiberdrošības risks



squalio

Cilvēki

Kiberdrošības lielākais izaicinājums līdz šim ir bijis un joprojām saglabāsies – **cilvēki.**

- Kiberdrošības speciālistu trūkst visa pasaulē
  - Daudzām organizācijām nav nepieciešams pilnas slodzes speciālists
- IT sistēmu lietotāji ikdienā nedomā par drošību (un tas ir normāli!)

Risks, ar kuru ir jārēķinās visiem tuvākos gadus

squalio

Papīru būšana – nepārspīlējiet!

- Nedokumentētas kontroles darbojas tikai nelielos kolektīvos ar zemu kadru mainību
- Papīrs pacieš visu, bet jo vairāk ir uzrakstīts, jo grūtāk to būs ievērot
- Detalizācija palīdz, bet prasa ļoti regulāru jaunin--šanu

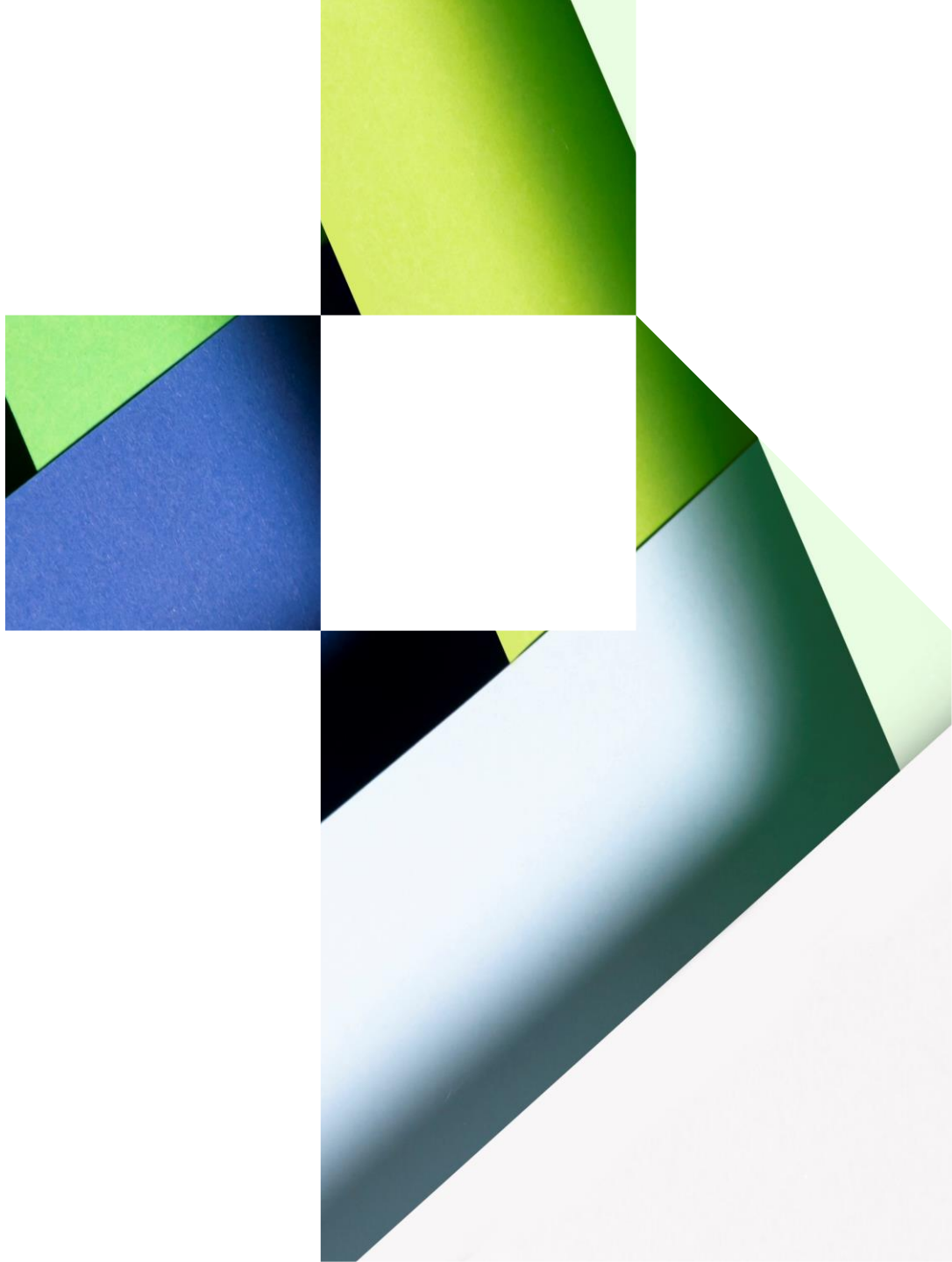
squalio

Vai izmantot zināmus ietvarus?

squalio

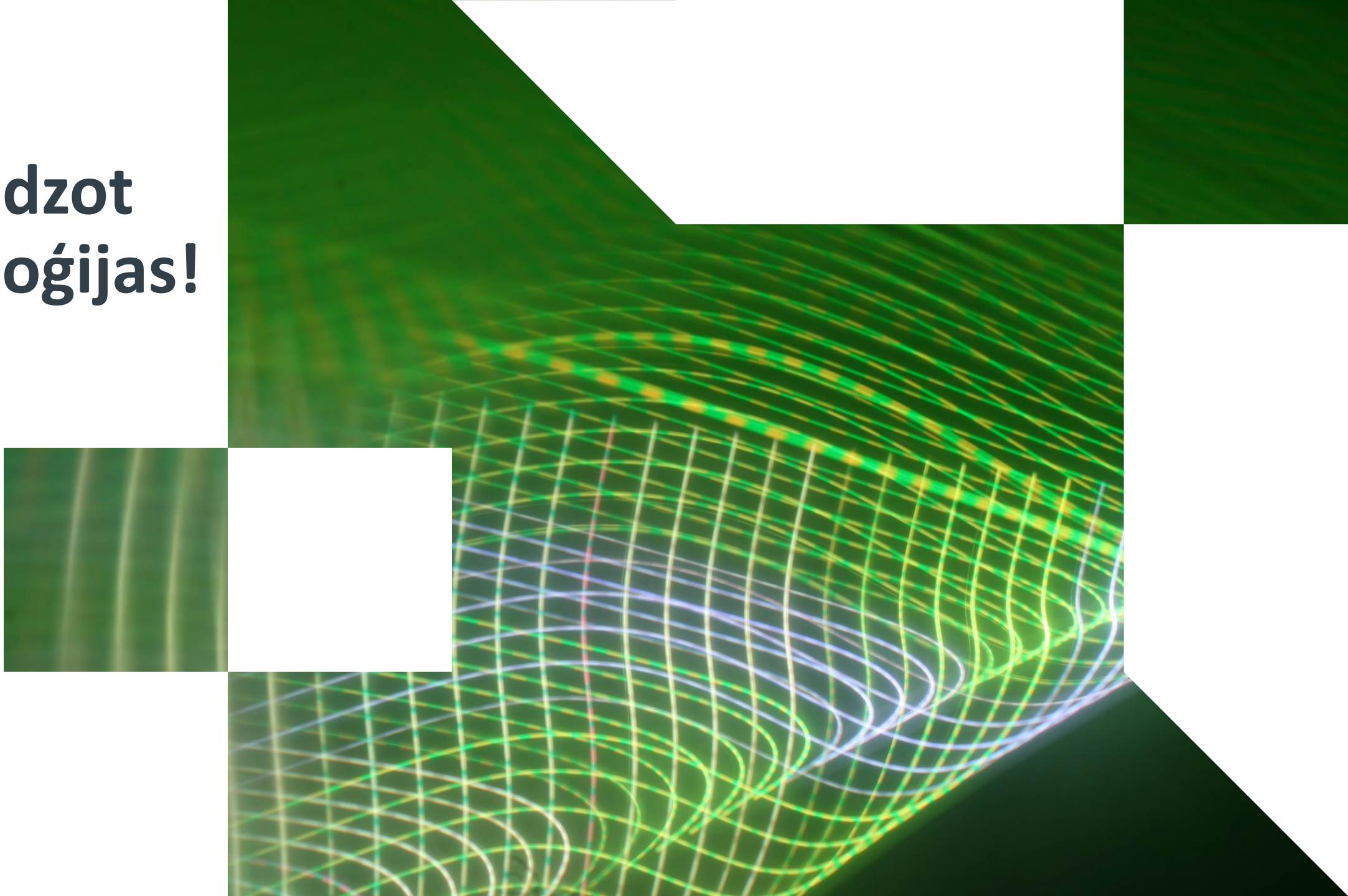
ISO 2700x un citi standarti

- Pārbaudītas vērtības (20+ gadu)
- Palīdz sadarbībā ar trešajām pusēm
- Atbilstības uzturēšana ir regulāras papildus izmaksas
- Ļoti vēlams pieredzējis kiberdrošības pārvaldnieks
- Ja organizācijas pusē nav uz sadarbību vērstas komandas, iznākums var būt ļoti formāls
- Lielai daļai organizāciju pietiek ar vienkāršāku pieeju



squalio

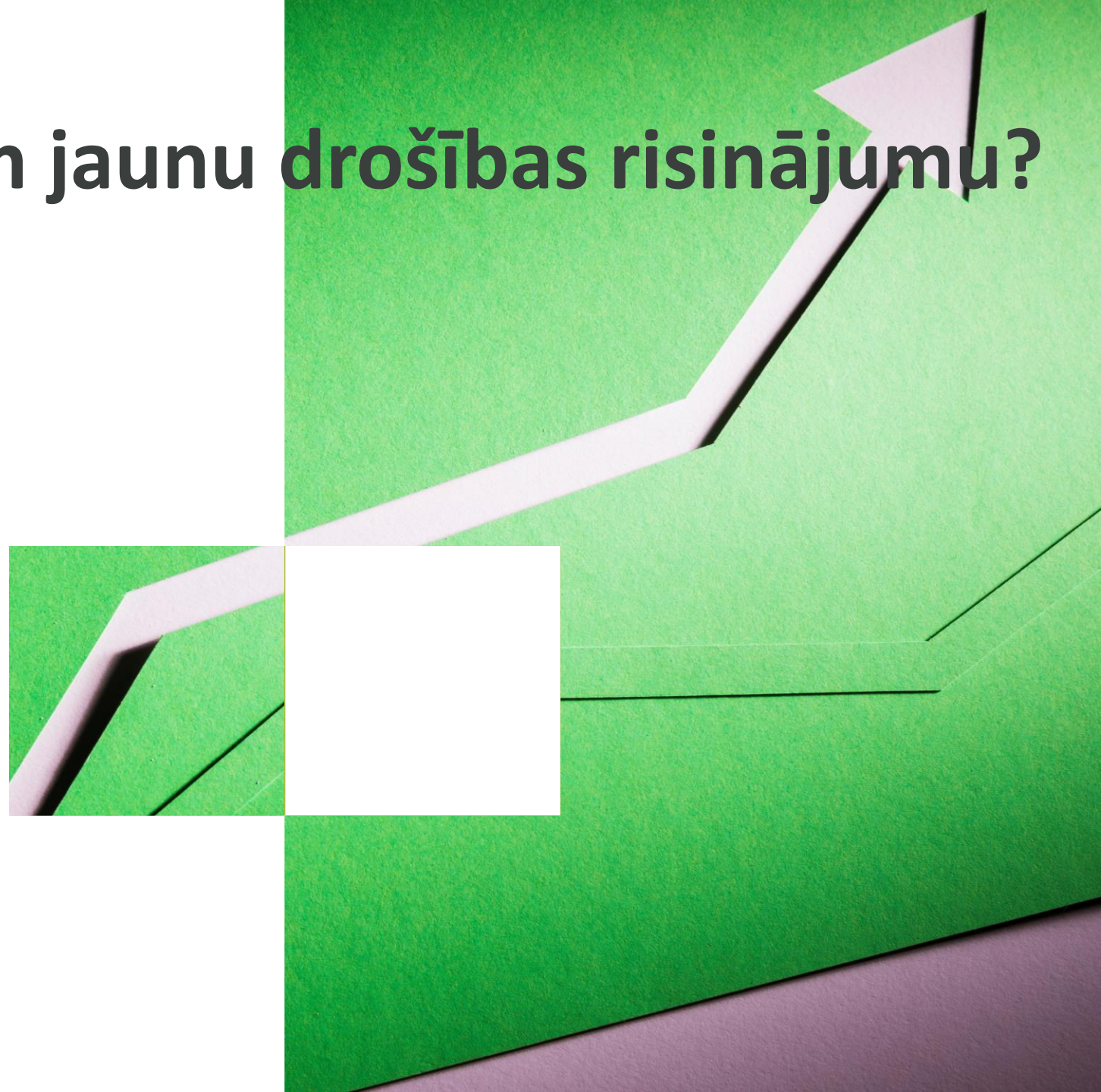
Un beidzot tehnoloģijas!



squalio

Riski pieaug – pērkam jaunu drošības risinājumu?

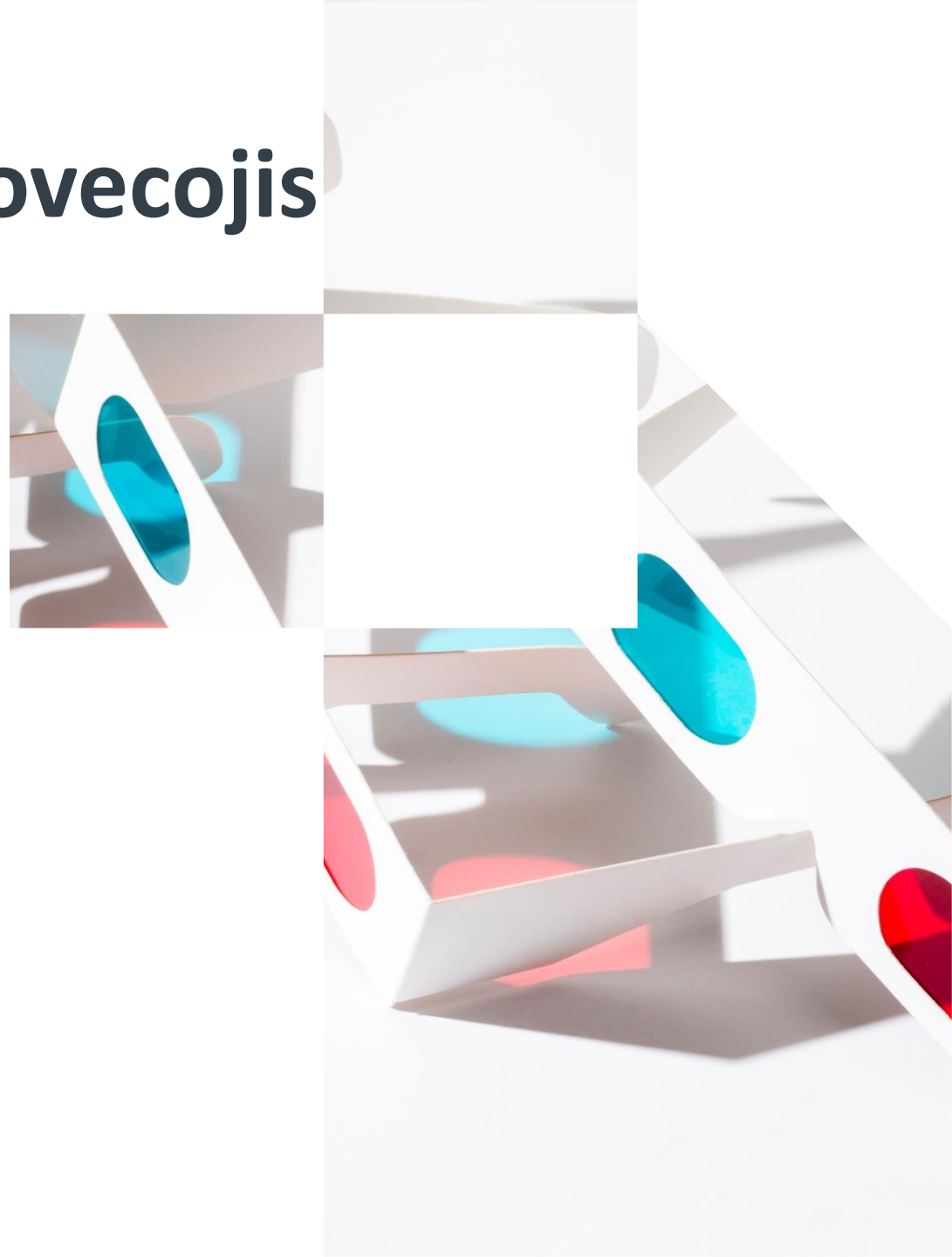
- Vienkāršākais ceļš var nebūt efektīvākais!
- Izvēloties jaunu sistēmu atceramies par procesiem un cilvēkiem!
- Viltus drošības izjūta, ja nopirkts dārgs risinājums
- AI (ne)atrisinās visas mūsu problēmas



squalio

Dženteļmeņa komplekts ir novecojis

- Tipiskās drošības tehnoloģijas:
- Ugunsmūris (kontrolē tikai perimetru, reti pilnībā nodalīti serveri, pavisam reti atsevišķi nodalīti legacy serveri)
- Antivīrusa pārbaude e-pastos (datu apmaiņai mūsdienās ir efektīvāki risinājumi)
- Antivīrusa pārbaude uz ugunsmūra (bieži bezjēdzīga, jo visi dati šifrēti)
- MFA – mums nepatīk, nav ērti, koplietojam kontus, privātas iekārtas, …



squalio

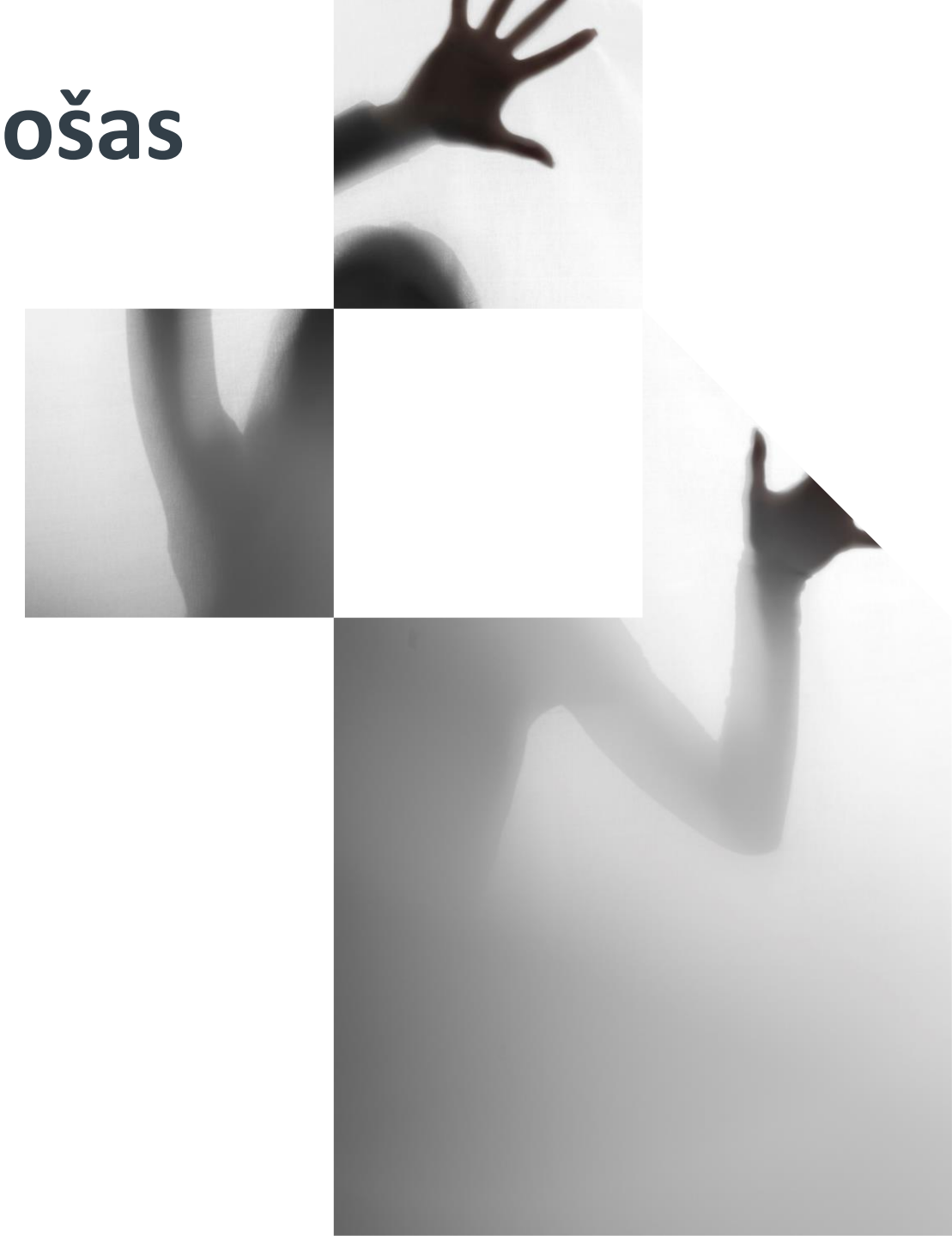
Kā izvēlēties piemērotus risinājumus?

squalio

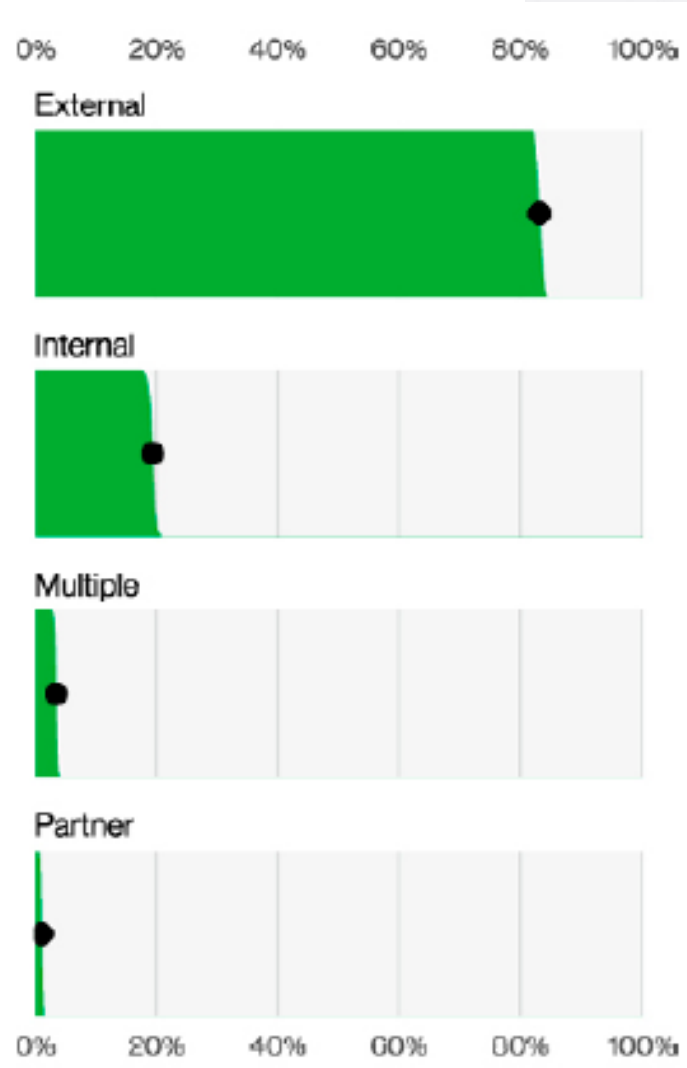
Tehnoloģijas jāizvēlas atbilstošas aktuāliem draudiem

- Izmantojam pasaulē populārākos drošības ziņojumus:
- Verizon Data Breach Investigations Report
- IBM® X-Force® Threat Intelligence Index
- Microsoft Digital Defense Report

- Tie satur informāciju par pašlaik populārākajiem uzbrukumu veidiem



squalio

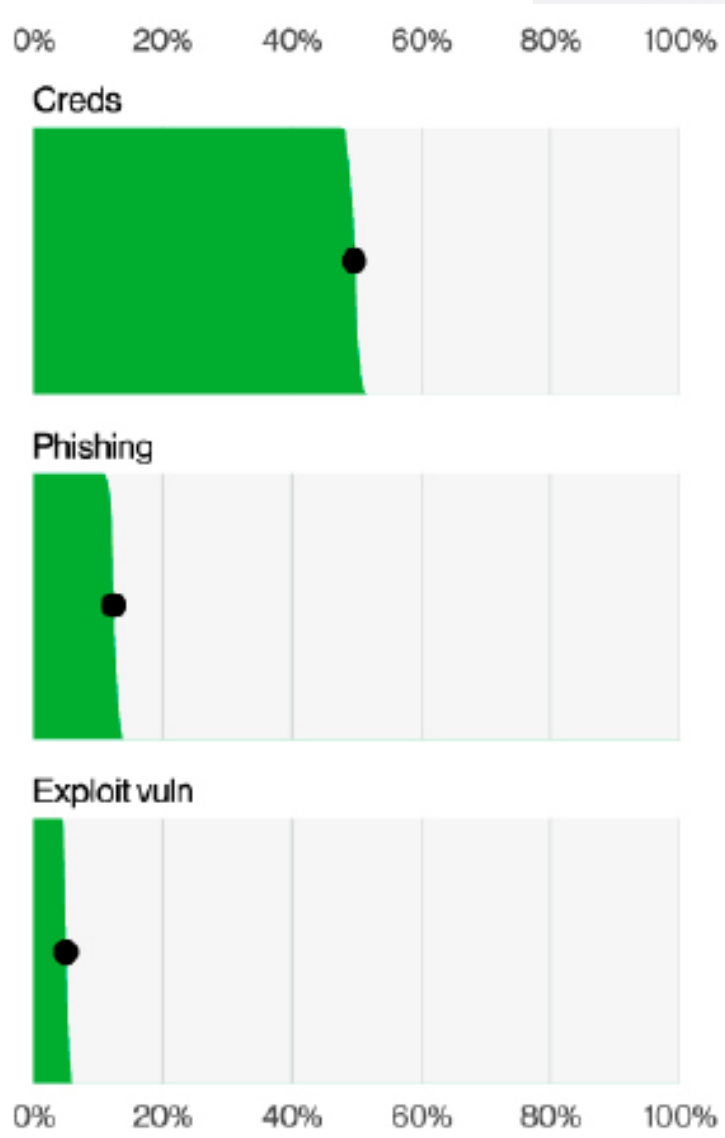


Incidentus izraisa ne tikai uzbrucēji!

Gandrīz 20% ir iekšējie lietotāji! (kļūdas un neatbilstoša izmantošana)

Verizon Data Breach Investigations Report 2023

squalio



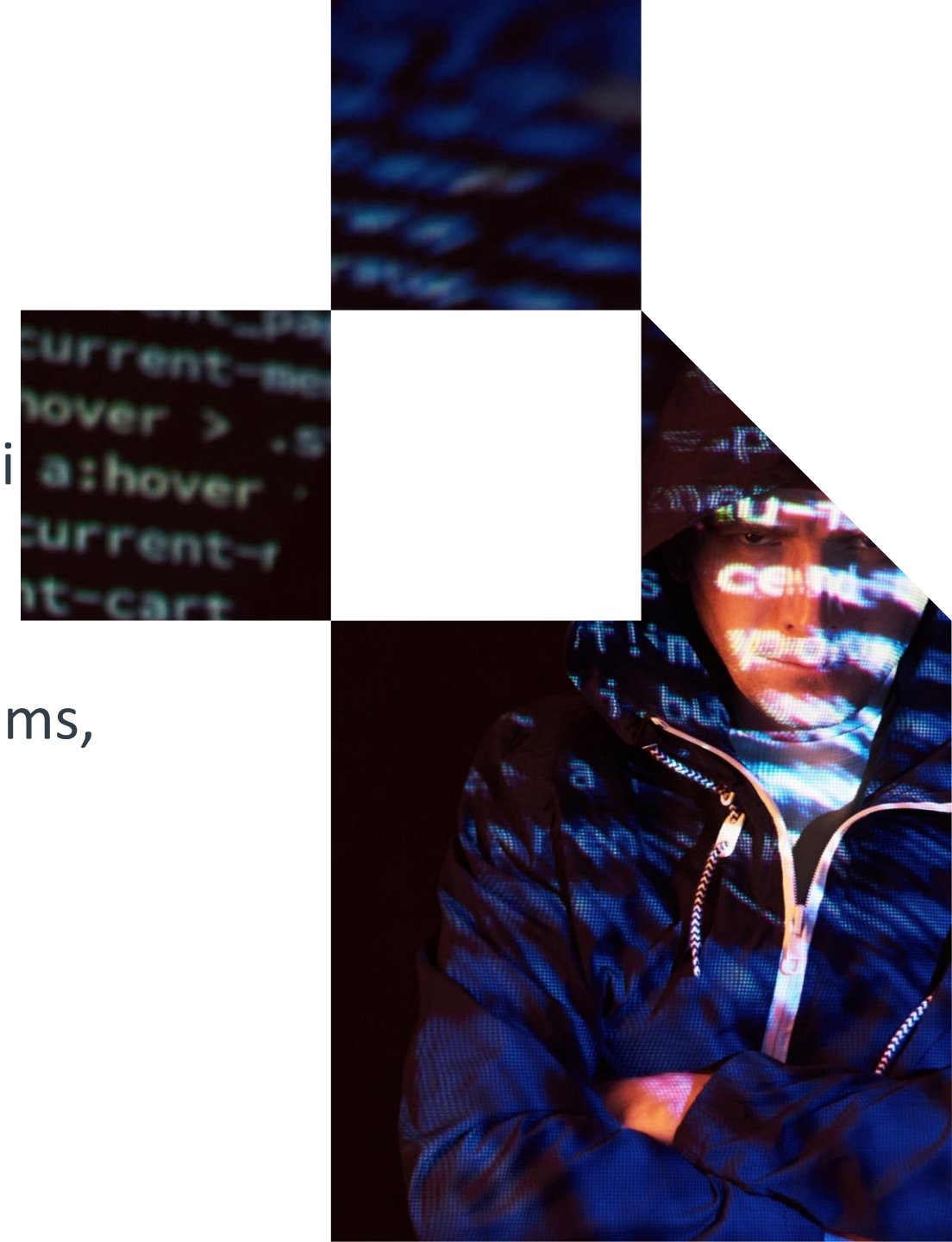
Populārākie uzbrukumu veidi:
- piekļuves datu izmantošana
- *pikšķerēšana*
- ievainojamības

Verizon Data Breach Investigations Report 2023

squalio

Nozagti kontu piekļuves dati

- Paroles atrastas iepriekšējās noplūdēs
- Sistēmkontu paroles nav aizsargātas un droši pārvaldītas
- Netiek izmantots MFA
- Tiek izmantoti koplietošanas konti (ietaupījums, vienkāršāka administrēšana, utml..)
- Lietotāji izmanto vienādas paroles



squalio

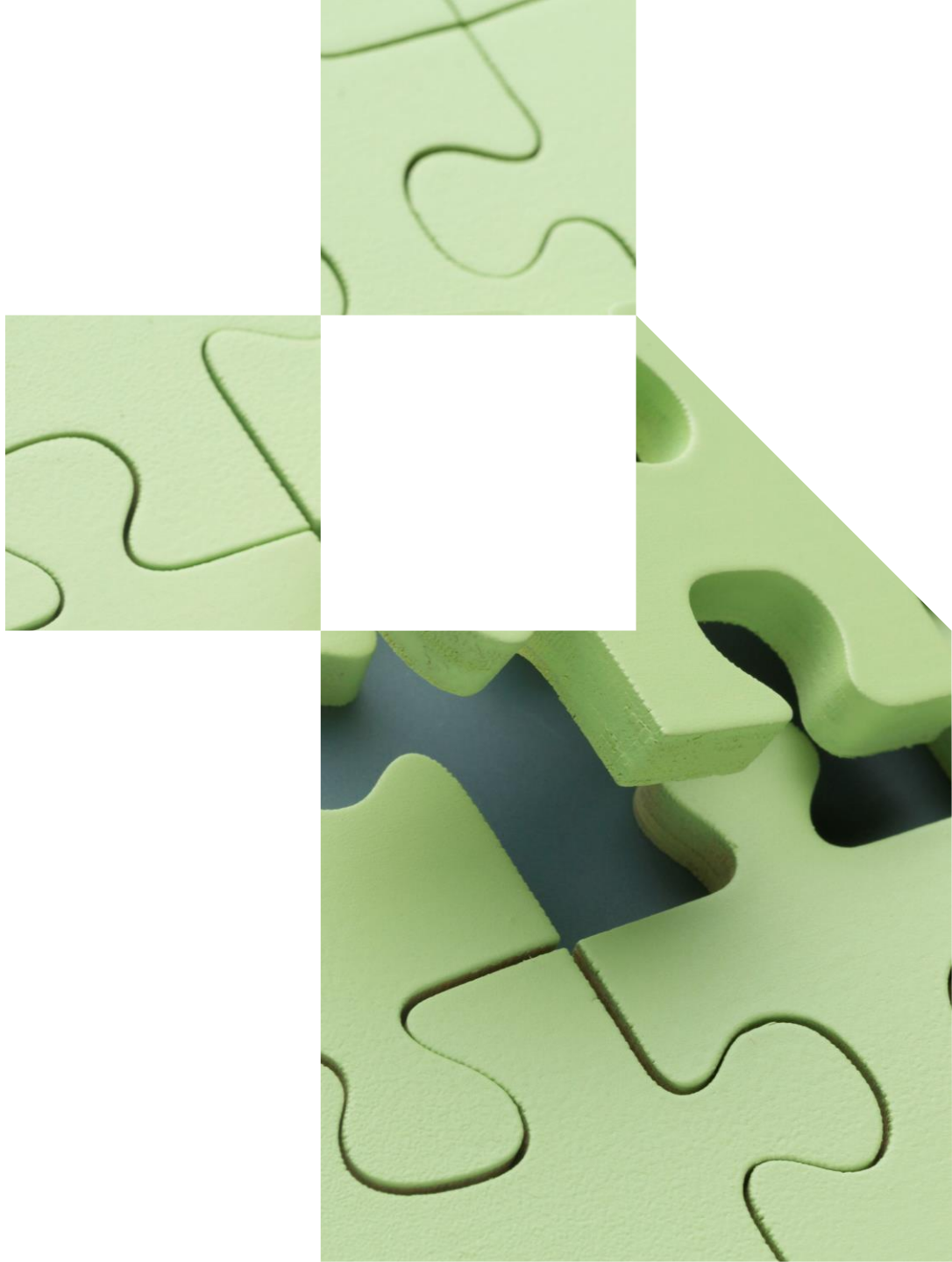
Sociālās inženierijas uzbrukumi

- Pieeja tieši lietotājam – e-pasts, zvans, saziņa soctīklos
- Netiek veiktas regulāras apmācības un simulācijas
- Sargājam perimetru, bet lietotājs strādā no dažādām vietām
- Organizāciju kultūra pieļauj kontroļu ignorēšanu !!!
- Mākoņservisu pieejamība veicina ShadowIT attīstību

squalio

Secinājumi par aktuāliem riskiem 2024 gadā.

- Jāsargā piekļuves konti un gala lietotāja iekārta:
- MFA ir praktiska nepieciešamība
- EDR uz iekārtām ir daudz efektīvāks risinājums par jaunu ārējo ugunsmūri un SIEM sistēmu
- Lietotāju (arī IT) apmācībai jābūt regulārai
- Izmantojam Zero-Trust pieeju, palielinām drošību līdzīgi visos pīlāros!



squalio

squalio