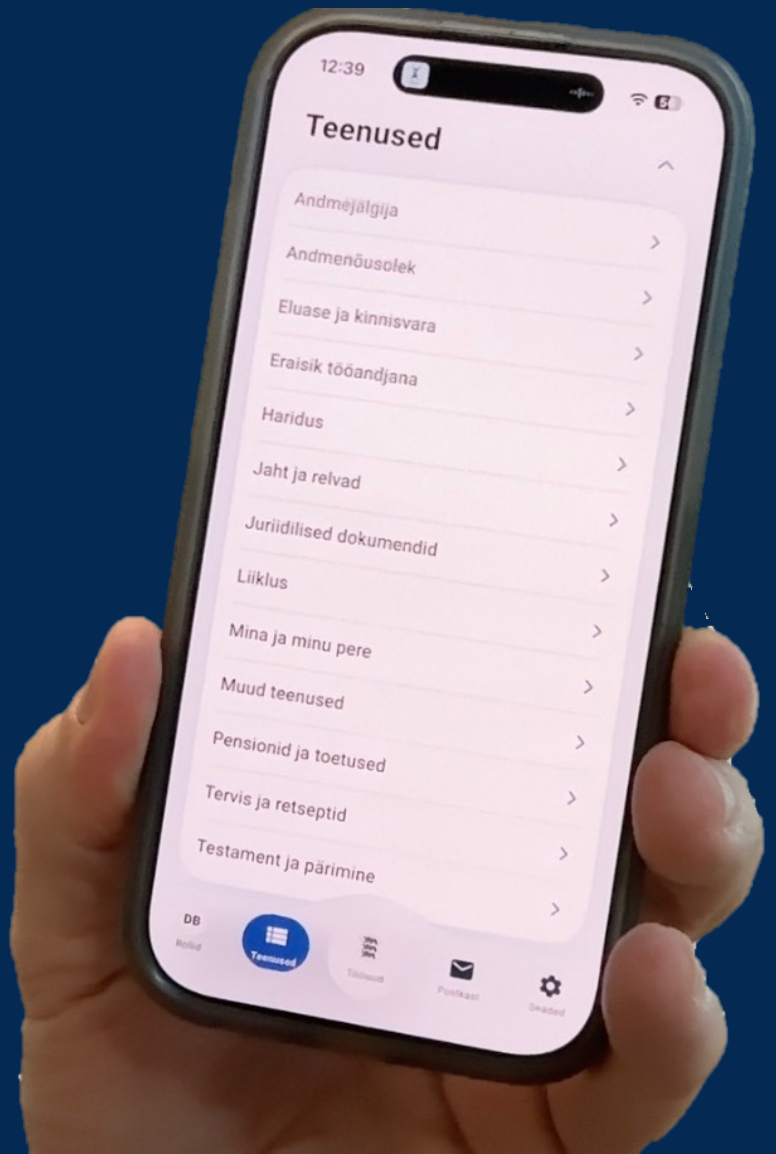
Teeme paremat riskianalüüsi Eesti riigile

Komisjoni materjalid
RIA koodivaramus

akad Dan Bogdanov
TA Küberturvalisuse komisjoni esimees
Cybernetica teadusdirektor

Eesti e-riik on sügavam, kui mujal



- Meil on rahvastikuregister ja isikukood.
- Me paneme oma lastele nimesid digitaalsete allkirjadega.
- Kinnisvara ostu- ja müügitehingud notari juures ei eelda enam kokku tulemist.
- Nüüd saab juba ka abielulahutuse avaldust digitaalselt teha

Tehnoloogia ei taga usaldatavust. Aga ka ainult seadustest ja protsessidest ei piisa!

ACADEMIA SCIENTIARUM ESTONIAE

Komisjoni tegevus 2023-2025

- 15. detsembril 2022 andis akadeemia juhatus akad Bogdanovile ülesandeks taaskäivitada küberturvalisuse komisjon.
- Uus küberturvalisuse komisjon kohtus esimest korda 14. augustil 2023

- 2023–2024 fookusteema oli valimiste tehnoloogia.
  - Hinnati 31 ohtu.
  - Korraldati esimene Usaldusest ja usaldatavusest konverents.
- 2024–2025 fookusteema oli samuti valimiste tehnoloogia.
  - Hinnati 20 ohtu.
  - Korraldati teine Usaldusest ja usaldatavusest konverents.

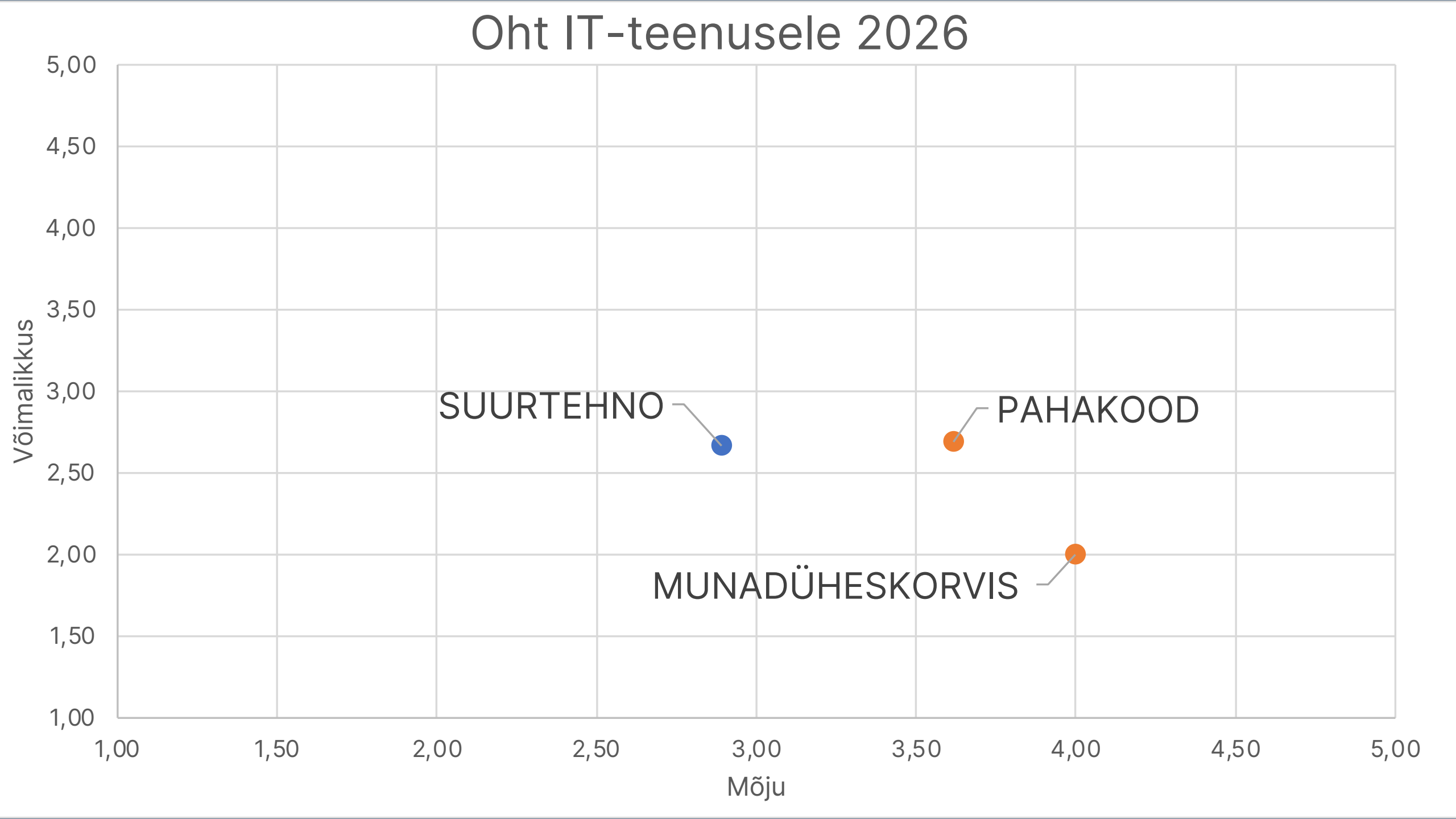
Alates 2025. aastast on fookus laiem

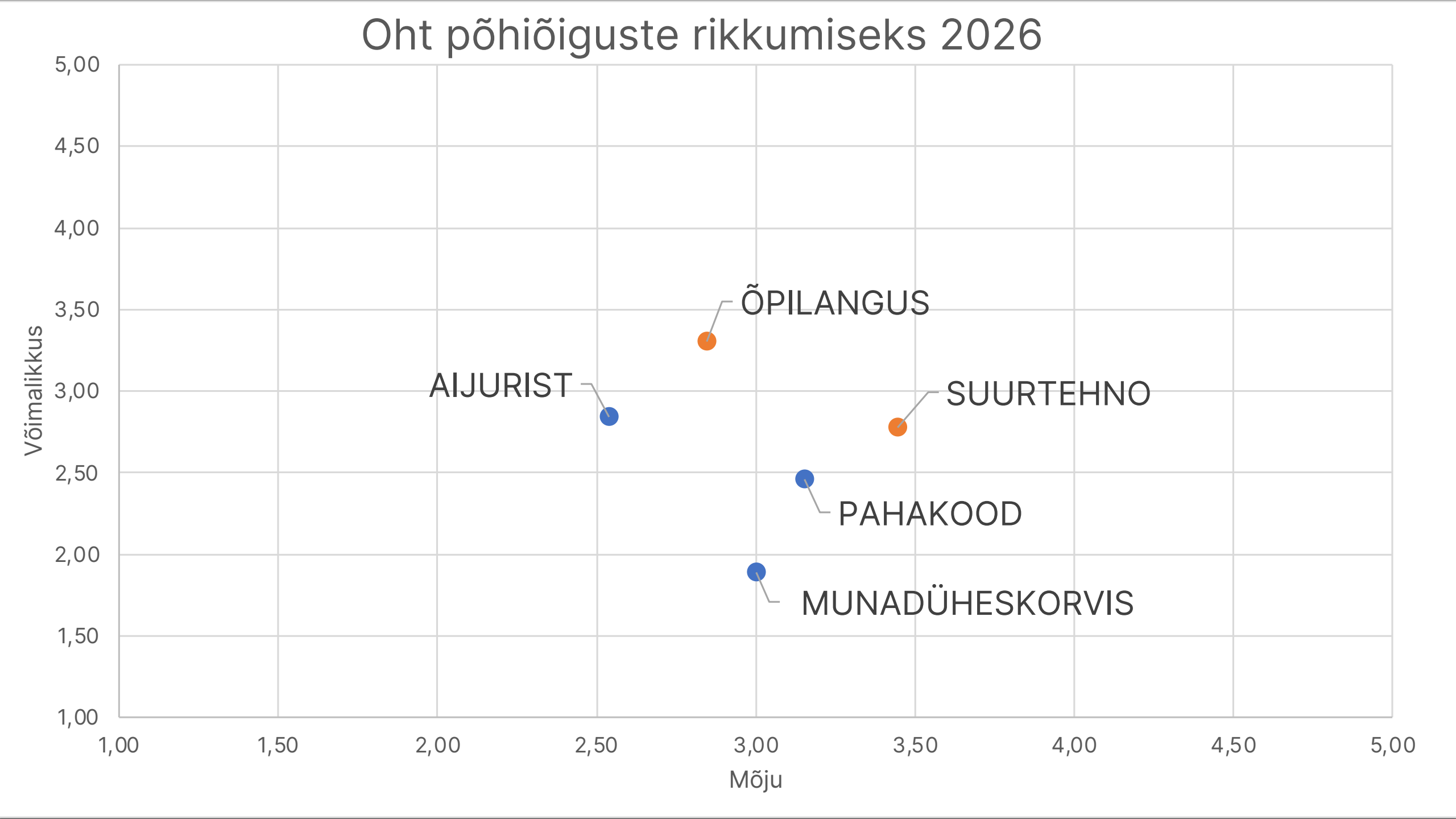
Katame suure osa e-riigist

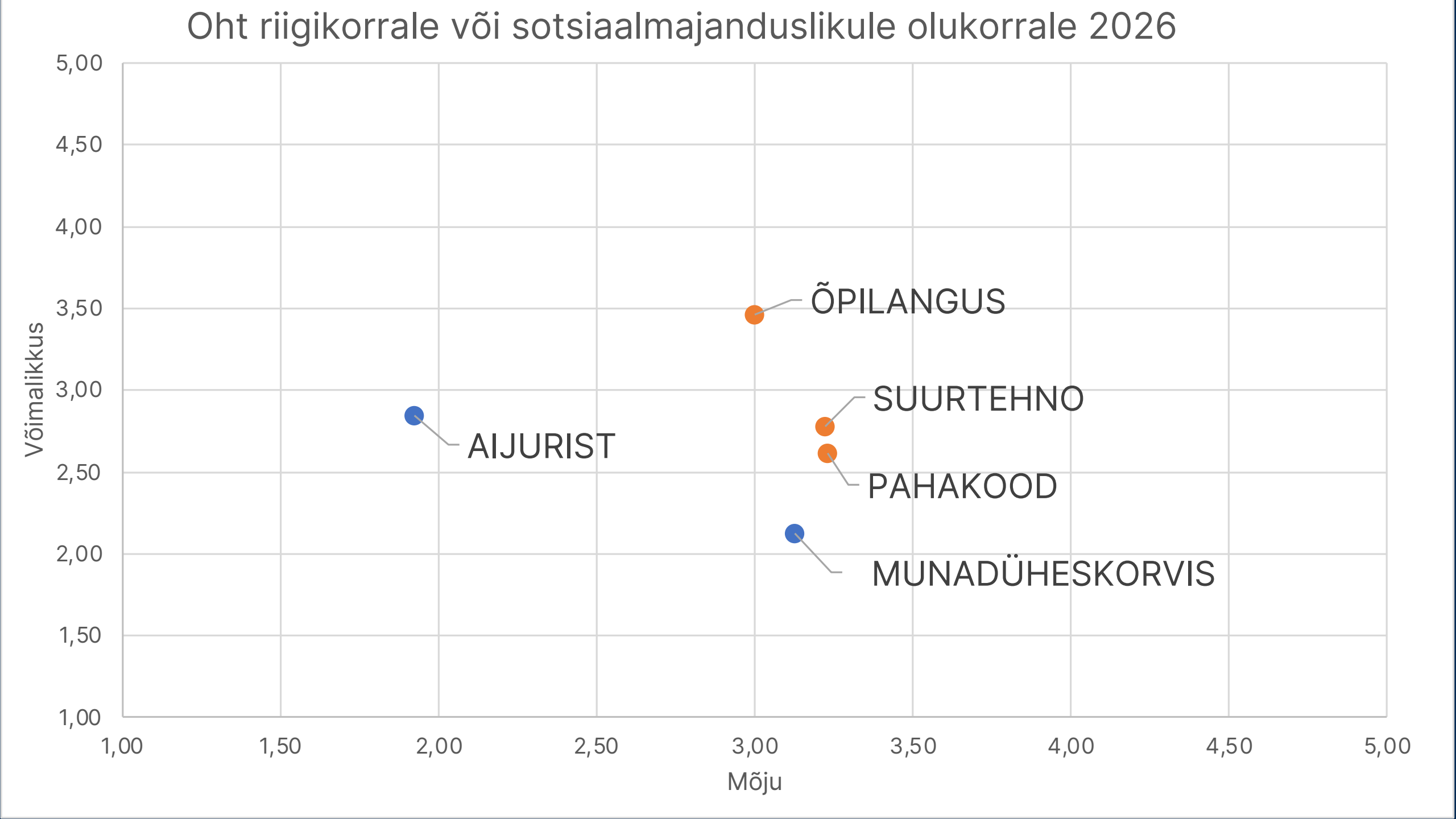
- Tarneahelate turve, sealhulgas
  - tarkvara,
  - riistvara,
  - pilvandmetöötlus.
- Tehisintellektisüsteemide ohutus ja küberturve
- Moodsate e-teenuste käideldavus, konfidentsiaalsus, terviklus, õiguspärasus ja ühiskondlik mõju.

Uus fookus tõi uue keerukuse

- Milliseid ohte me soovime Eestis ennetada?
- Kuidas me suudame tehniliste, õiguslike ja ühiskondlike ohtude hindamist ühendada?
- Kuidas teha nii, et meie töö viiks paremate süsteemide loomiseni?

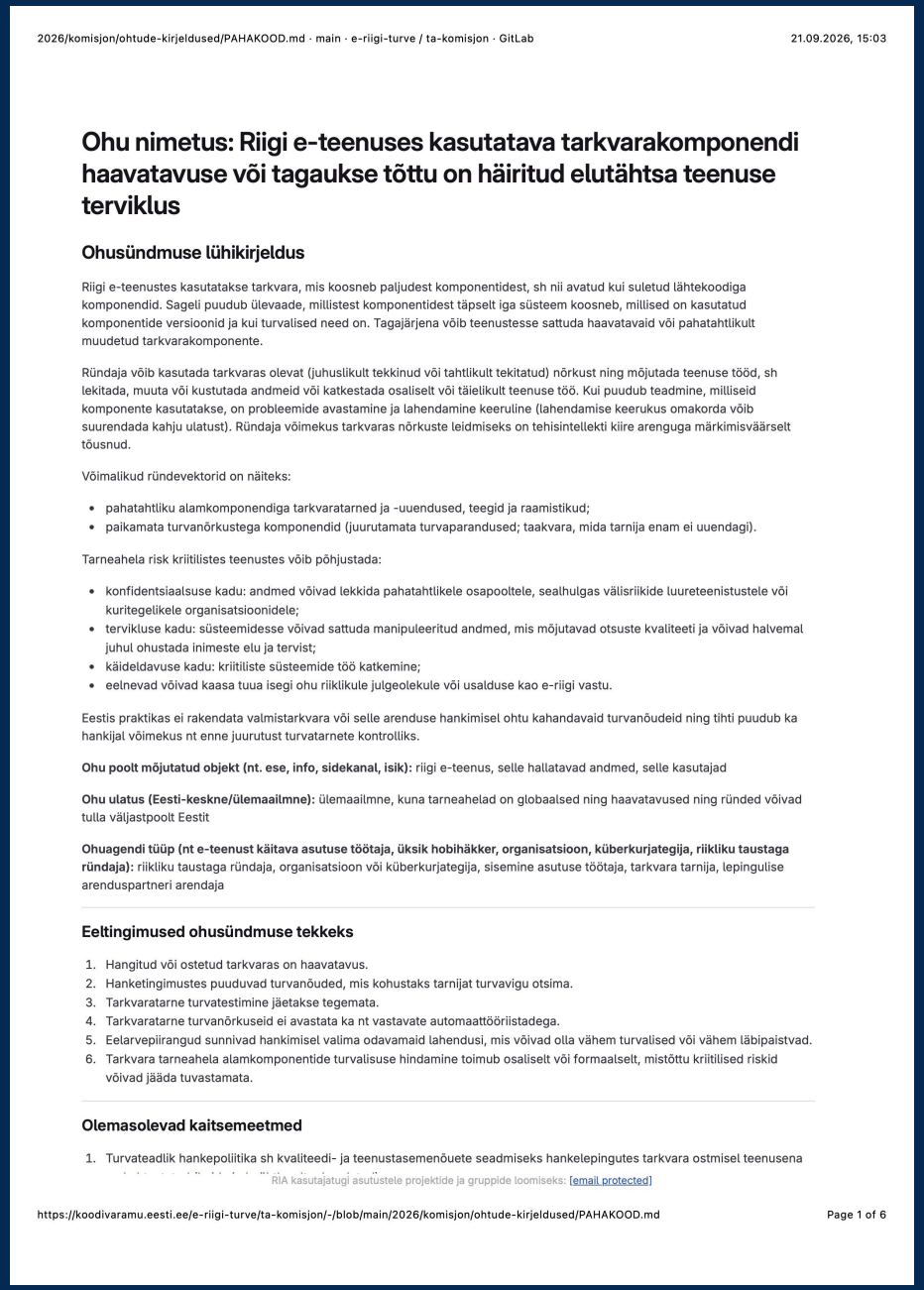

Oht IT-teenusele 2026
Võimalikkus
Mõju
5,00
4,50
4,00
3,50
3,00
2,50
2,00
1,50
1,00
1,00
1,50
2,00
2,50
3,00
3,50
4,00
4,50
5,00
SUURTEHNO
PAHAKOOD
MUNADÜHESKORVIS


Oht põhiõiguste rikkumiseks 2026
Võimalikkus
Mõju
5,00
4,50
4,00
3,50
3,00
2,50
2,00
1,50
1,00
1,00
1,50
2,00
2,50
3,00
3,50
4,00
4,50
5,00
ÕPILANGUS
AIJURIST
SUURTEHNO
PAHAKOOD
MUNADÜHESKORVIS


Oht riigikorrale või sotsiaalmajanduslikule olukorrale 2026
Võimalikkus
Mõju
5,00
4,50
4,00
3,50
3,00
2,50
2,00
1,50
1,00
1,00
1,50
2,00
2,50
3,00
3,50
4,00
4,50
5,00
ÕPILANGUS
SUURTEHNO
AIJURIST
PAHAKOOD
MUNADÜHESKORVIS

Milline näeb välja ohukirjeldus?

1. Lühikirjeldus
   mis valesti läheb?
2. Eeltingimused ohu tekkeks
   mis enne peab juhtuma?
3. Olemasolevad kaitsemeetmed
   mida me täna juba teeme?
4. Eeldused kaitse toimimiseks
   kas juba tehtav ka toimib?
5. Võimalikud lisameetmed
   mida me peaks veel tegema?
6. Hinnangud
   kui suur on komisjoni mure?



Ohu nimetus: Riigi e-teenuses kasutatava tarkvarakomponendi haavatavuse või tagaukse tõttu on häiritud elutähtsa teenuse terviklus

Ohusündmuse lühikirjeldus

Riigi e-teenustes kasutatakse tarkvara, mis koosneb paljudest komponentidest, sh nii avatud kui suletud lähtekoodiga komponendid. Sageli puudub ülevaade, millistest komponentidest täpselt iga süsteem koosneb, millised on kasutatud komponentide versioonid ja kui turvalised need on. Tagajärjena võib teenustesse sattuda haavatavaid või pahatahtlikult muudetud tarkvarakomponente.

Ründaja võib kasutada tarkvaras olevat (juhuslikult tekkinud või tahtlikult tekitatud) nõrkust ning mõjutada teenuse tööd, sh lekitada, muuta või kustutada andmeid või katkestada osaliselt või täielikult teenuse töö. Kui puudub teadmine, milliseid komponente kasutatakse, on probleemide avastamine ja lahendamine keeruline (lahendamise keerukus omakorda võib suurendada kahju ulatust). Ründaja võimekus tarkvaras nõrkuste leidmiseks on tehisintellekti kiire arenguga märkimisväärselt tõusnud.

Võimalikud ründevektorid on näiteks:

- pahatahtliku alamkomponendiga tarkvaratarned ja -uuendused, teegid ja raamistikud;
- paikamata turvanõrkustega komponendid (juurutamata turvaparandused; taakvara, mida tarnija enam ei uuendagi).

Tarneahela risk kriitilistes teenustes võib põhjustada:

- konfidentsiaalsuse kadu: andmed võivad lekkida pahatahtlikele osapooltele, sealhulgas välisriikide luureteenistustele või kuritegelikele organisatsioonidele;
- tervikluse kadu: süsteemidesse võivad sattuda manipuleeritud andmed, mis mõjutavad otsuste kvaliteeti ja võivad halvemal juhul ohustada inimeste elu ja tervist;
- käideldavuse kadu: kriitiliste süsteemide töö katkemine;
- eelnevad võivad kaasa tuua isegi ohu riiklikule julgeolekule või usalduse kao e-riigi vastu.

Eestis praktikas ei rakendata valmistarkvara või selle arenduse hankimisel ohtu kahandavaid turvanõudeid ning tihti puudub ka hankijal võimekus nt enne juurutust turvatarnete kontrolliks.

Ohu poolt mõjutatud objekt (nt. ese, info, sidekanal, isik): riigi e-teenus, selle hallatavad andmed, selle kasutajad

Ohu ulatus (Eesti-keskne/ülemaailmne): ülemaailmne, kuna tarneahelad on globaalsed ning haavatavused ning ründed võivad tulla väljastpoolt Eestit

Ohuagendi tüüp (nt e-teenust käitava asutuse töötaja, üksik hobihäkker, organisatsioon, küberkurjategija, riikliku taustaga ründaja): riikliku taustaga ründaja, organisatsioon või küberkurjategija, sisemine asutuse töötaja, tarkvara tarnija, lepingulise arenduspartneri arendaja

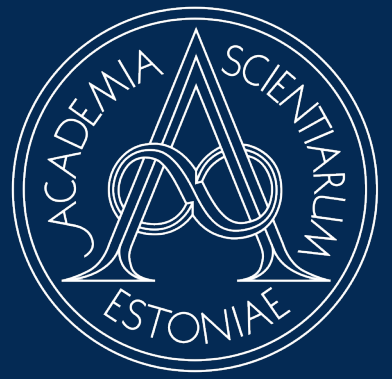
Eeltingimused ohusündmuse tekkeks

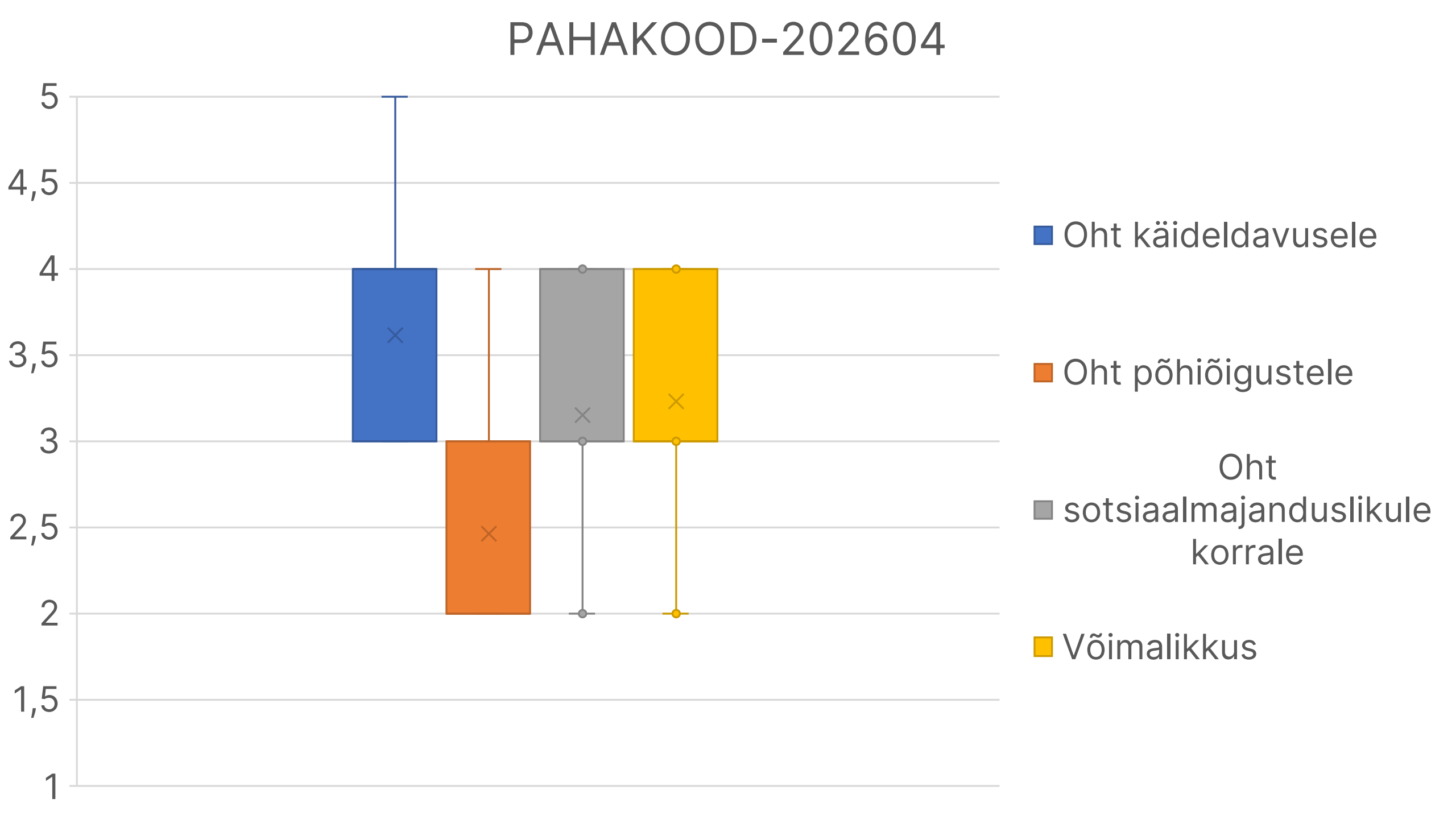
1. Hangitud või ostetud tarkvaras on haavatavus.
2. Hanketingimustes puuduvad turvanõuded, mis kohustaks tarnijat turvavigu otsima.
3. Tarkvaratarne turvatestimine jäetakse tegemata.
4. Tarkvaratarne turvanõrkuseid ei avastata ka nt vastavate automaattööriistadega.
5. Eelarvepiirangud sunnivad hankimisel valima odavamaid lahendusi, mis võivad olla vähem turvalised või vähem läbipaistvad.
6. Tarkvara tarneahela alamkomponentide turvalisuse hindamine toimub osaliselt või formaalselt, mistõttu kriitilised riskid võivad jääda tuvastamata.

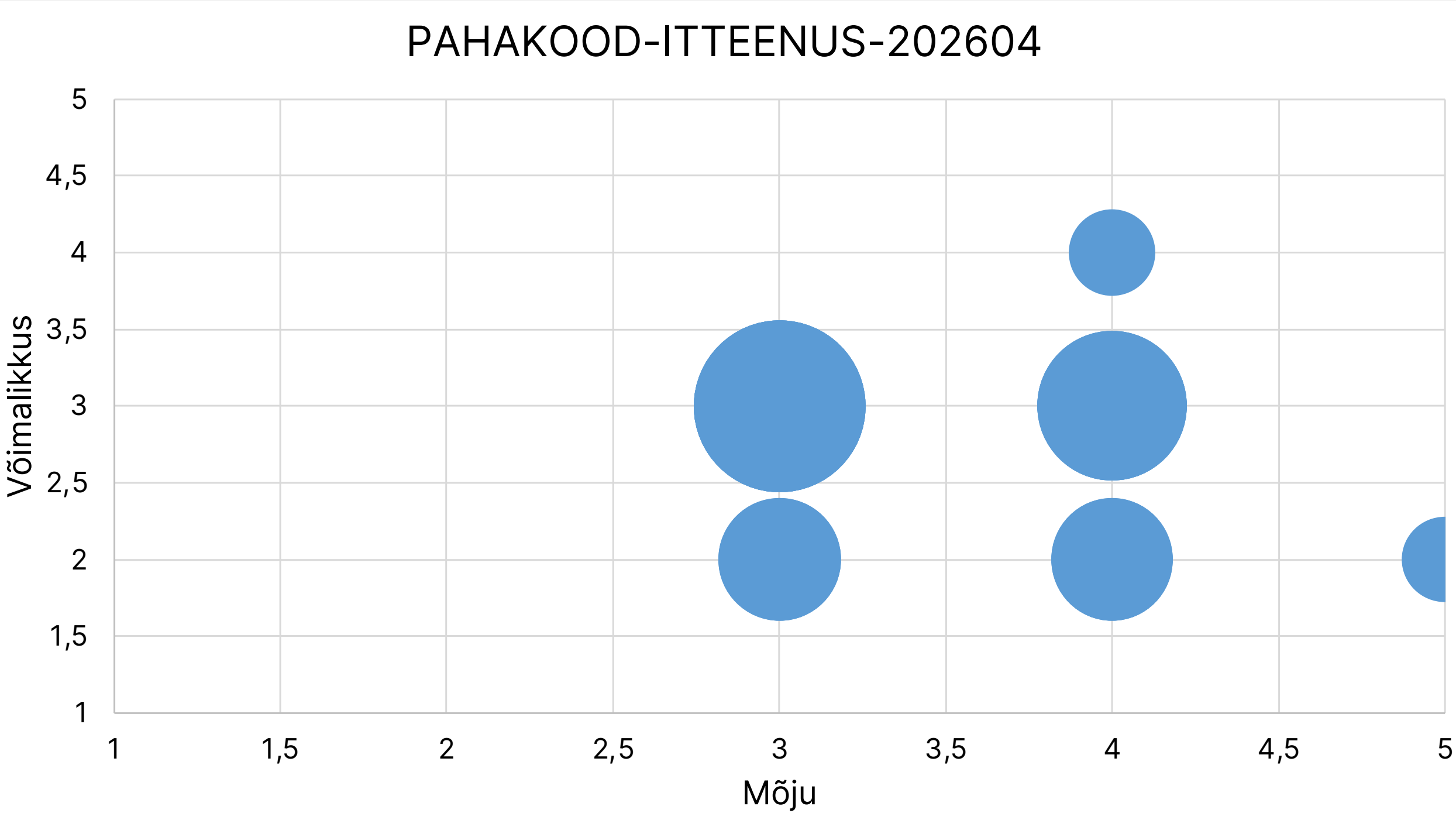
Olemasolevad kaitsemeetmed

1. Turvateadlik hankepoliitika sh kvaliteedi- ja teenustasemenõuete seadmiseks hankelepingutes tarkvara ostmisel teenusena

RIA kasutajatugi asutustele projektide ja gruppide loomiseks:




PAHAKOOD-202604
5
4,5
4
3,5
3
2,5
2
1,5
1
Oht käideldavusele
Oht põhiõigustele
Oht sotsiaalmajanduslikule korrale
Võimalikkus


PAHAKOOD-ITTEENUS-202604
Võimalikkus
5
4,5
4
3,5
3
2,5
2
1,5
1
1
1,5
2
2,5
3
3,5
4
4,5
5
Mõju

TA küberturvalisuse komisjoni avalikud materjalid RIA koodivaramus