TARTU ÜLIKOOL
arvutiteaduse instituut

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

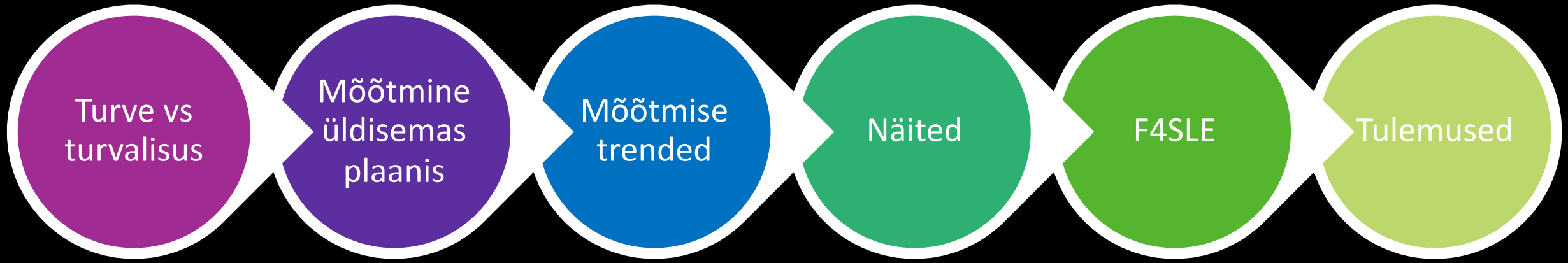
Turbe mõõtmisest

Mari Seeba
Küberturbe juhtivekspert (RIA)
Infoturbe doktorant (TÜ)

12. veebruar 2025

RIIGI INFOSÜSTEEMI AMET

NATIONAL CYBER SECURITY CENTRE NCSC-EE


Turve vs turvalisus
Mõõtmine üldisemas plaanis
Mõõtmise trended
Näited
F4SLE
Tulemused

INFO- / KÜBER-

turve

- Protsess, millega tagatakse millegi kokkulepitu kaitse
- Käideldavuse, konfidentsiaalsuse ja tervikluse säilitamise tegevused

turvalisus

- Kaitstud olek
- Olek, kus riskid on hoitud talutaval tasemel

Miks üldse turvet mõõta?

- Kui turvaline ma olen?
- Kas ma olen parem kui eelmine aasta samal ajal?
- Kas ma kulutan asja eest raha turbele?
- Kui turvaline ma olen võrreldes teistega?
- Milliseid riski ülekandmise võimalusi mul on?

Hubbard, D.W., Seiersen, R., How to measure anything in cybersecurity risk, (2014)

- Vastavus (E-ITS, GDPR, NIS2, elutähtsad teenused, jne)
- Progress (As-Is -> To-Be)
- Teadmine nõrkustest ja riskidest
- Teadmatuse vähendamine
- Partneri usaldamine
- Toetustegevuste plaanimine (riigi tasand)
- Eelarve

Miks turbe mõõtmine on nii… raske?

- Me ei saa mõõta kõiki turvanõudeid
- Keskkond, abstraktsioonitase ja kontekst mõjutavad turvet
- Mõõtmine protsessina mõjutab turvet
- Ükski süsteem pole sõltumatu
- Turvalisus on mitmekihiline
- Vastane muudab keskkonda
- Me oleme liiga optimistlikud
- Me tajume kasu kahjust erinevalt, kuigi numbriliselt on võrreldavad
- Mõõtmine on samaaegselt nii tagasiside kui eesmärk

Pfleefer, S., L., Cunningham, R., K., Why Measuring Security is Hard (2010), IEEE Computer and Reliability Societies

Mõõtmine	• Võrdleme ühikuga (measuring)
Taseme hindamine	• Anname hinnagu tasemele (evaluate) – tasemetööd
Hindamine	• Hindame hetke olekut (assessment) – diferentseeriv personaalne hindamine

Cybersecurity Assessment Methods by Leszczyna (2021)

- Compliance checking
- Vulnerability identification
- Vulnerability analysis
- Penetration testing
- Checklist-based Evaluation
- Simulation-based testing
- Emulation-based testing
- Model-based testing
- Formal analysis
- Reviews

Security Measurement Models by Khalenghi et al. (2022)

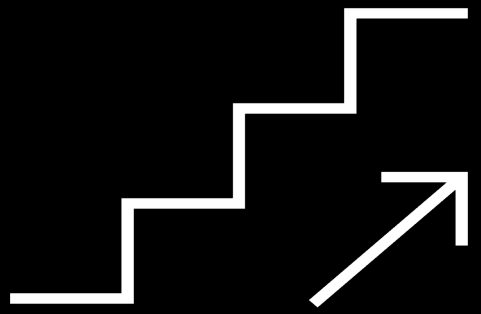
- Taxonomy-based (single security related subject)
- Scoring-based (sub-metrics)
- Attack Graph and Attack Graph based
- Stepwise (follows predefined steps, predicted actions)
- Conceptual (structural)
- Reference or Security Measurement Reference Model (standard based)
- Maturity based (security capabilities)
- Functional (operational, organisational or mission-based)
- Multi-dimensional
- Stochastic
- Contextual

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. Computers & Security.

Khaleghi, M., Aref, M. R., & Rasti, M. (2022). Comprehensive Comparison of Security Measurement Models. Journal of Applied Security Research,

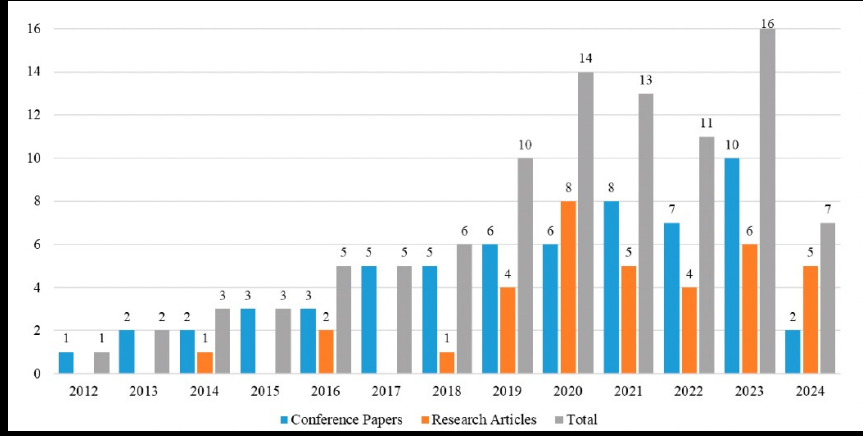
Küpsusmudelid

	Cyber Security Maturity Models (CSM2)	Organizations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information Security Evaluation Maturity Model (ISEM), 2000	City Group	Security awareness and evaluation	Complacency	Acknowledgement	Integration	Common practice	Continuous improvement
2	Systems Security Engineering Capability Maturity Model (SSE-CMM), 2001	The US National Security Agency (NSA)	Evaluation of software security engineering processes	Performed informally	Plan and track	Well defined	Control	Continuous improvements
3	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimized
4	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimized
5	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
6	Gartner's Information Security Awareness Maturity Model (GISMM), 2009	Gartner	Security awareness, and risk management in large international organizations	Blissful ignorance	Awareness	Corrective	Operations excellence	
7	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
8	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
9	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
10	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimized		
11	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
12	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	



N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," (2016), doi: 10.1109/PCCC.2016.7820663.

Küpsusmõõdikute trendid



Miks

- Regulatsioonide vastavus
- Ohtudele vastupanu võime
- Andmekaitse
- Riskide leevendamine
- Intsidentidega toimetulek
- Investeeringud küberturbesse
- Küberturve kultuuri taseme tõstmine
- Jätkusuutlikkuse parendamine
- Kuluefektiivsed turbelahendused

Puudused

- Ressursipuudus
- Keerukus
- Sektorieripäradega mittearvestamine
- Juhiste puudulikkus
- Kultuurilised ja inimlikud barjäärid
- Ärieesmärkidega mitteühildumine
- Automatiseerimise puudumine
- Standardiseerimata meetrika
- Integratsiooni puudumine eksisteerivate süsteemidega
- Majanduslikud barjäärid
- Fookuse puudumine intsidendi haldusele

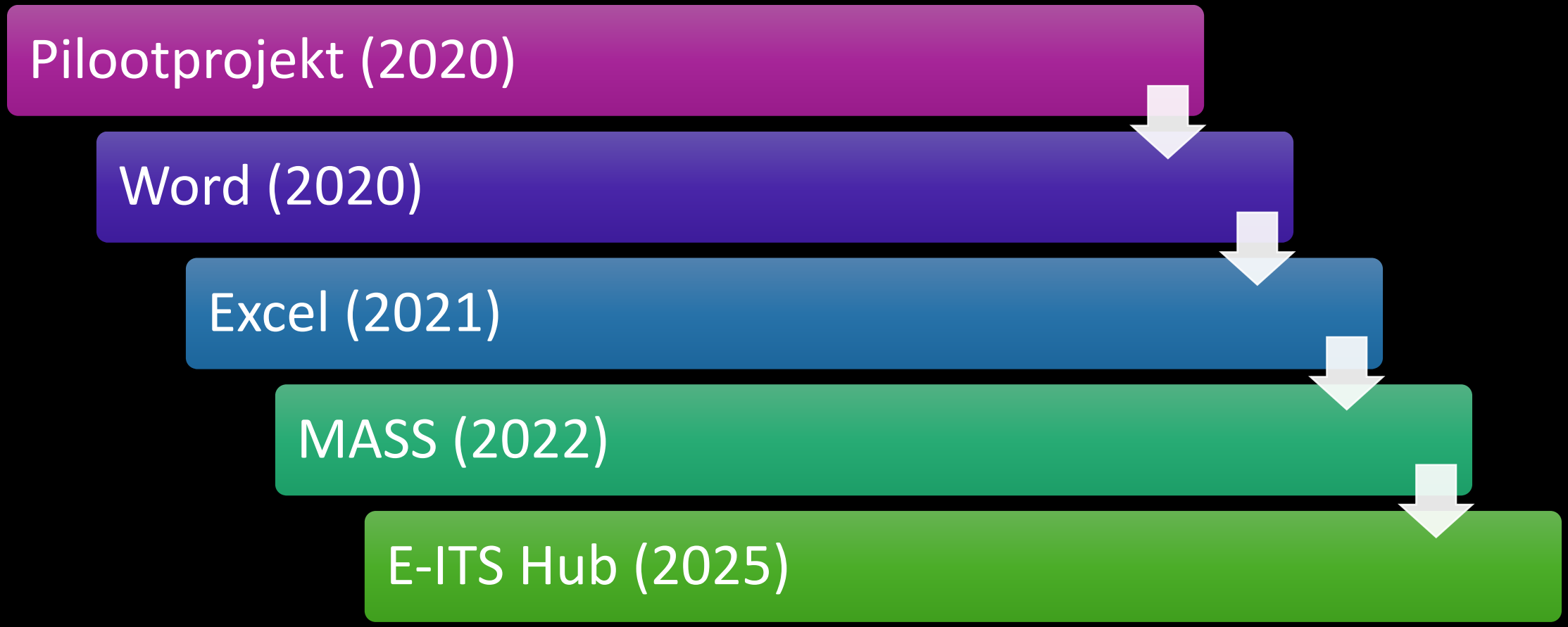
Alenka Brezavšček , Alenka Baggia (2024), Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review

Näited

25.01.2025

Organisastioon	NImetus	Link	Kommentaar
US CISA	CSET	https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset	Allalaetav rakendus paljude standardite jaoks (NIST CSF, CMMC). Keskele andmeid ei kogu
NSCS-BE	CyberFundamentals Framework	https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework	Nii vabatahtlikuks kasutuseks kui sertimiseks (Excel), NIST CSF 1.0
NCC-AT	WKO Online Ratgeber	https://ratgeber.wko.at/itsafe/	Sisselogimiseta, seansipõhine,kohene vastus, võrdlusalus (kogub andmeid) + soovituste nimekiri, ca 200 küsimust, neljane skaala
NCSC-IE	Cyber Security Baseline Standards Self-Assessment Form	https://www.ncsc.gov.ie/guidance/	Vabatahtlik hindamine, (Excel), NIST CSF 1.0 põhine
NC3-LU	Fit 4 Cybersecurity Assessment Tool	https://nc3.lu/assessment-testing-and-training/fit4cybersecurity	13 teemat 5-10 väitega, skoor üle 65p on aluseks NC3 muude teensute saamiseks (nt turvatestid), annab tagasi negatiivsed vastused (rakendusplaaniks)
TRAFICOM (FI)	Cybermeter	https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari	Vabatahlik hindamine, rakendamise alus (Excel)
Hellenic Ministry of Digital Governance Government department	Cybersecurity Self Assessment Tool	https://mindigital.gr/wp-content/uploads/2022/03/cybersecurity-self-assessment.xlsm	Vabatahtlik (Excel)
CNCS-PT		https://www.cncs.gov.pt/pt/quadro-nacional/#ciberchecku p	Online, NIST CSF 1.0, 3-30 küsimust plokkides, kokku 100 küsimust. Kolm vastust – keskmine neist asjakohane, tulemiks radar ja tervikloend vastustest

F4SLE
Framework for Security Level Evaluation



F4SLE
Framework for Security Level Evaluation

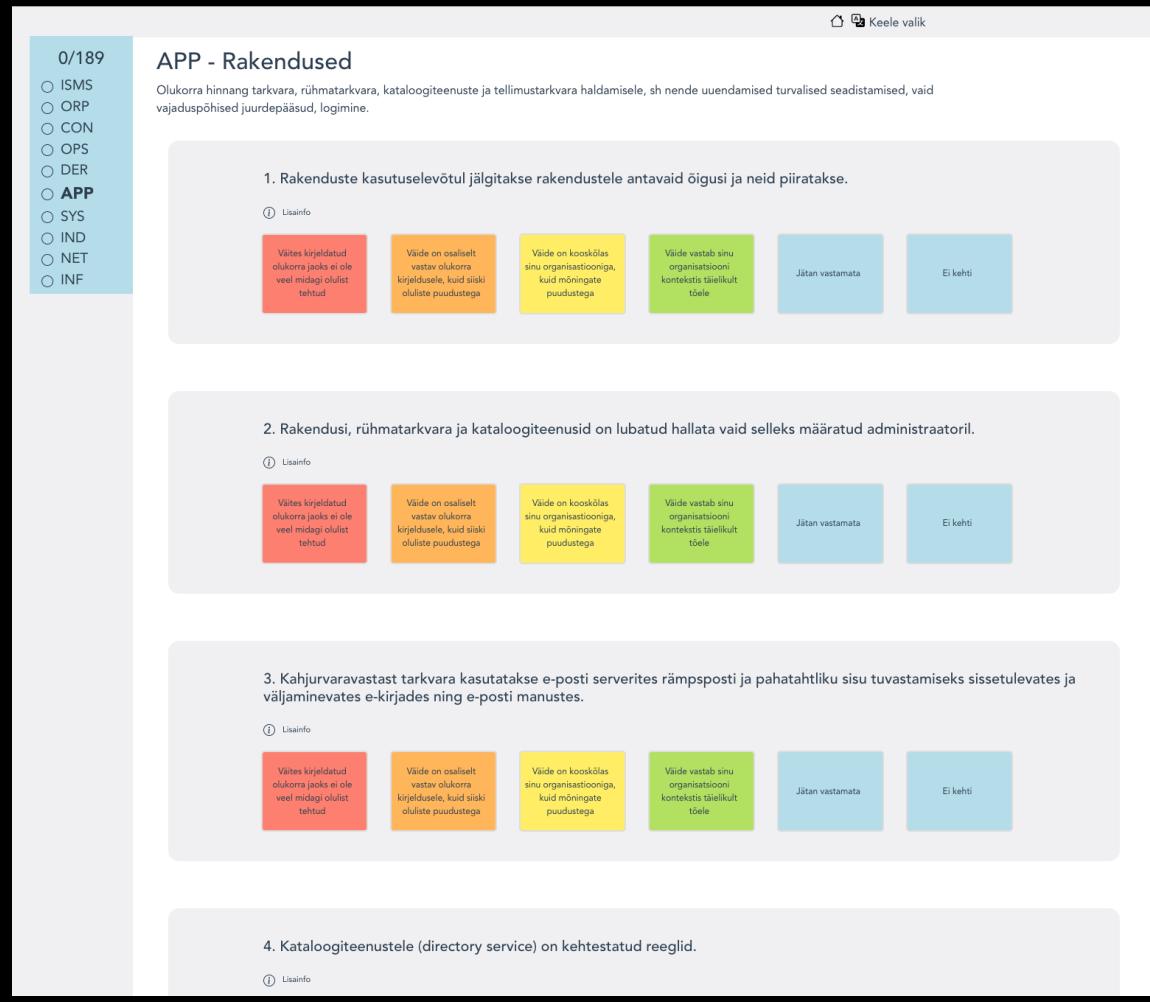
- Kohene vastus
- Võrdlusalus teistega, ootusega, riskitasemega
- Vastavus ja kõikehõlmavus + ohud (E-ITS, ISO27001, NIS2, ENISA TLR)
- Võimalikult madal sisenemisbarjäär
- Uuendamise võimalus nii et võrdlusvõimalus säilib (MUSE)
- Andmekogumise tööriist (automaatika) ja andmeprivaatsus
- Kordusmõõtmine
- Andmete taaskasutus erinevate sidusrühmade tarbeks
- Mitmekeelsus

MASS – veebi-põhine tööriist F4SLE kasutamiseks ja andmete keskele kogumiseks

- Privaatsusprintsiip – toorandmed ei lahku vastaja juurest
- Serverisse saadetakse vaid agregeeritud (keskmistatud andmed)
- Kohene tulemuse näitamise vastajale
- Võrdlusaluse esitamine vastajale
- Andmete taaskasutus

Test keskkond: https://mass.cloud.ut.ee/test-massui/#/

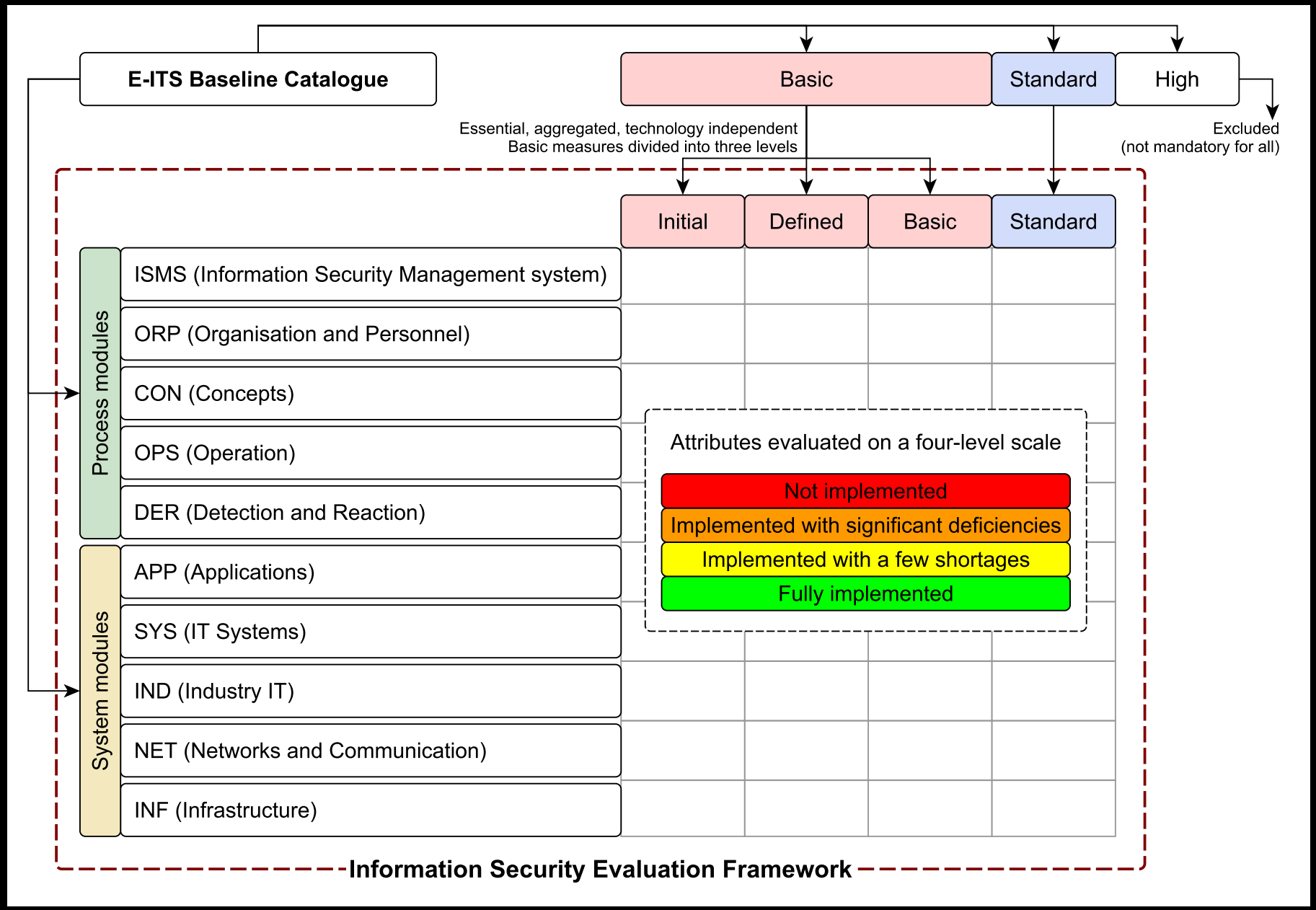
Toote keskkond



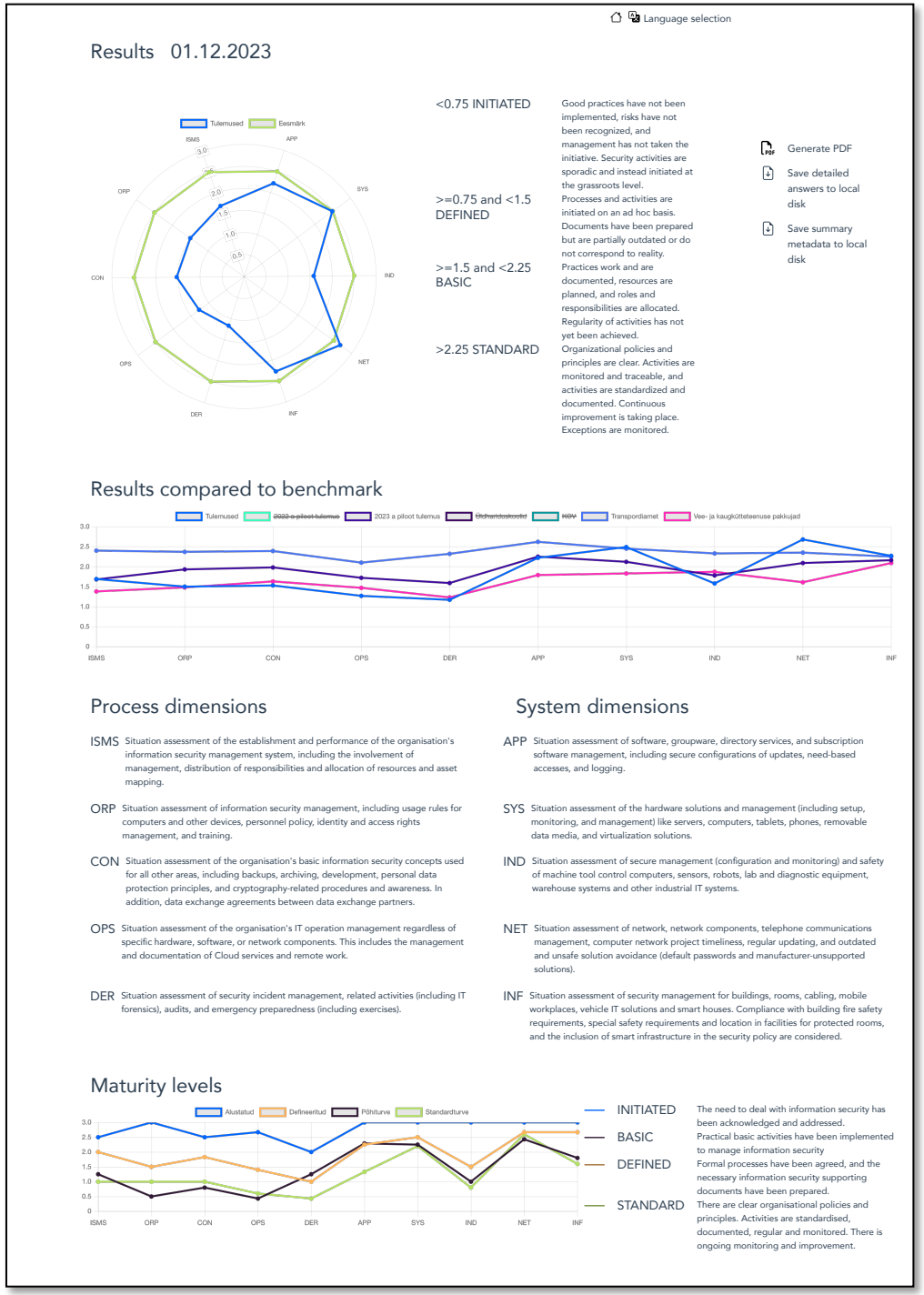
RIIGI INFOSÜSTEEMI AMET

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
arvutiteaduse instituut



Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: Guizzardi, R., Ralyté, J., Franch, X. (eds) Research Challenges in Information Science. RCIS 2022.



Organisatsioon ja CISO

- Hinnang 10 dimensioonis
- Riski tasemed
- Võrdlus ootusega (roheline joon)

- Võrdlusalus teiste sektoritega

- Turbedimensioonide selgitused

- Küpsustasemed detailsemalt

https://mass.cloud.ut.ee/massui/

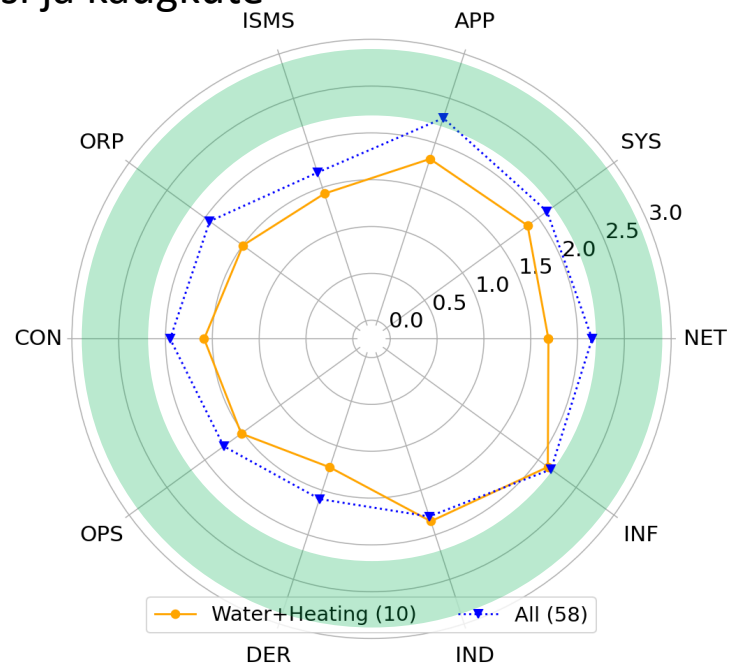
Sektorite võrdlus 2023okt-2024okt

Expectation level

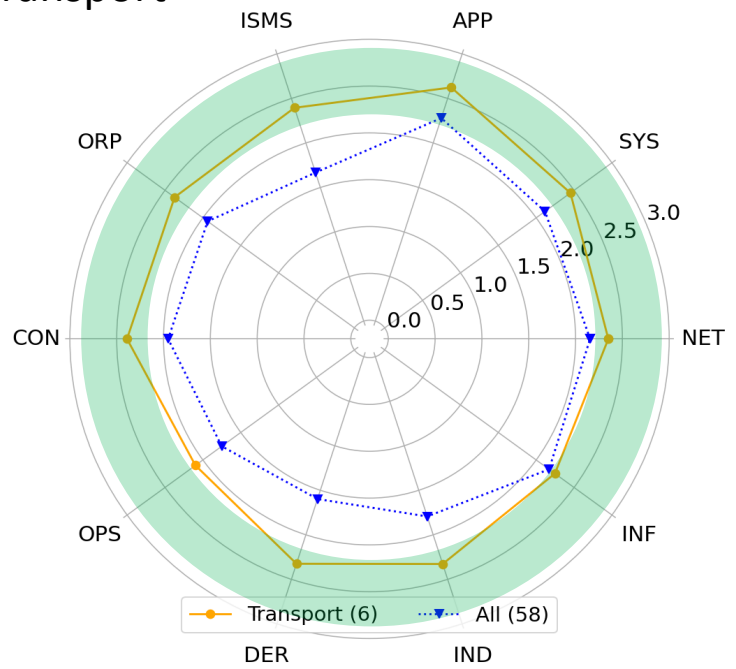
Average

Sector average

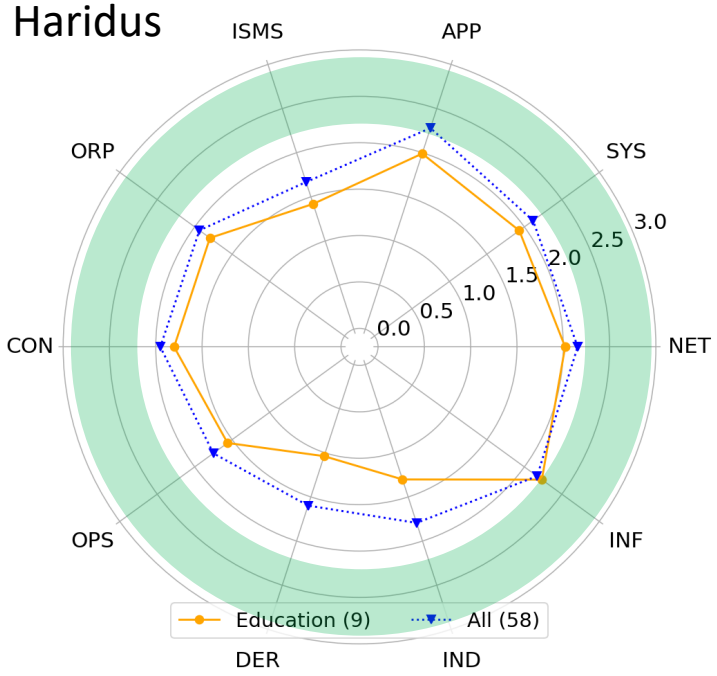
Vesi ja kaugküte



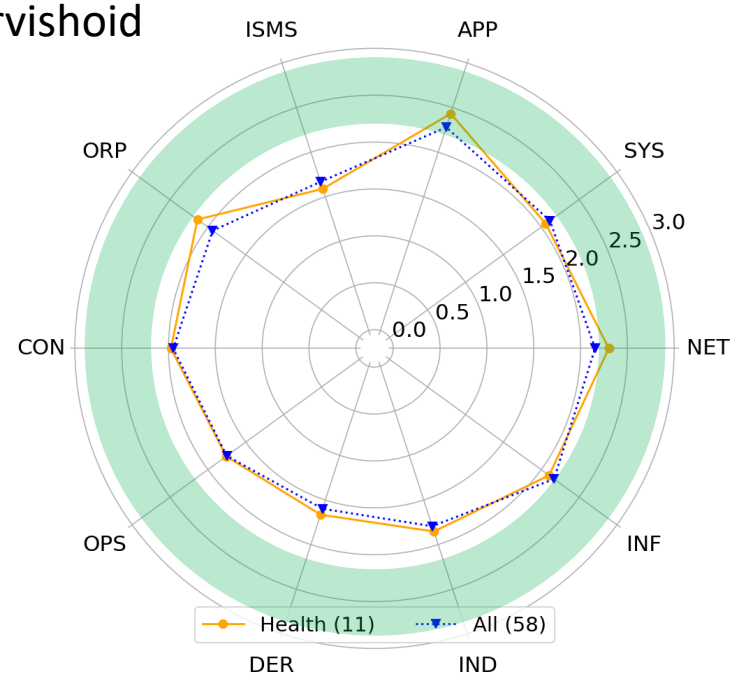
Transport



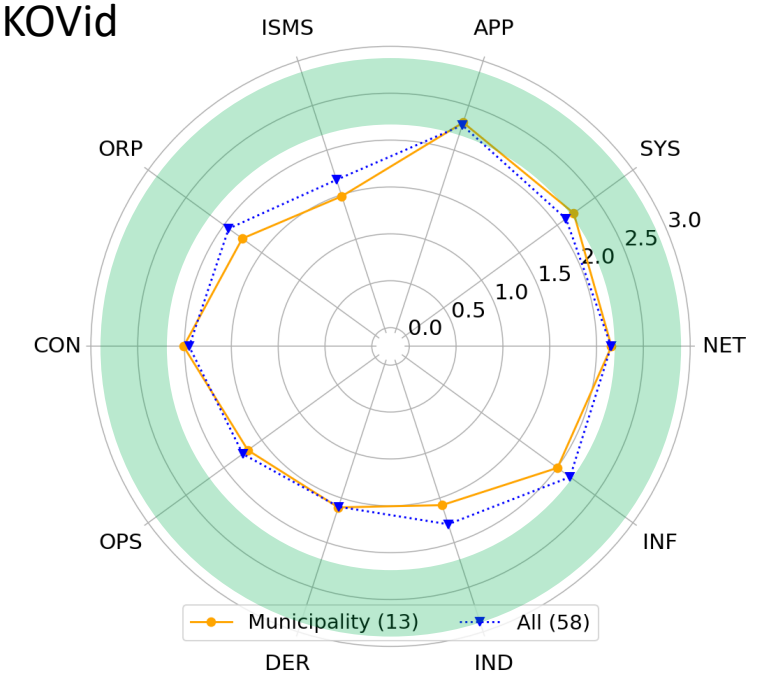
Haridus



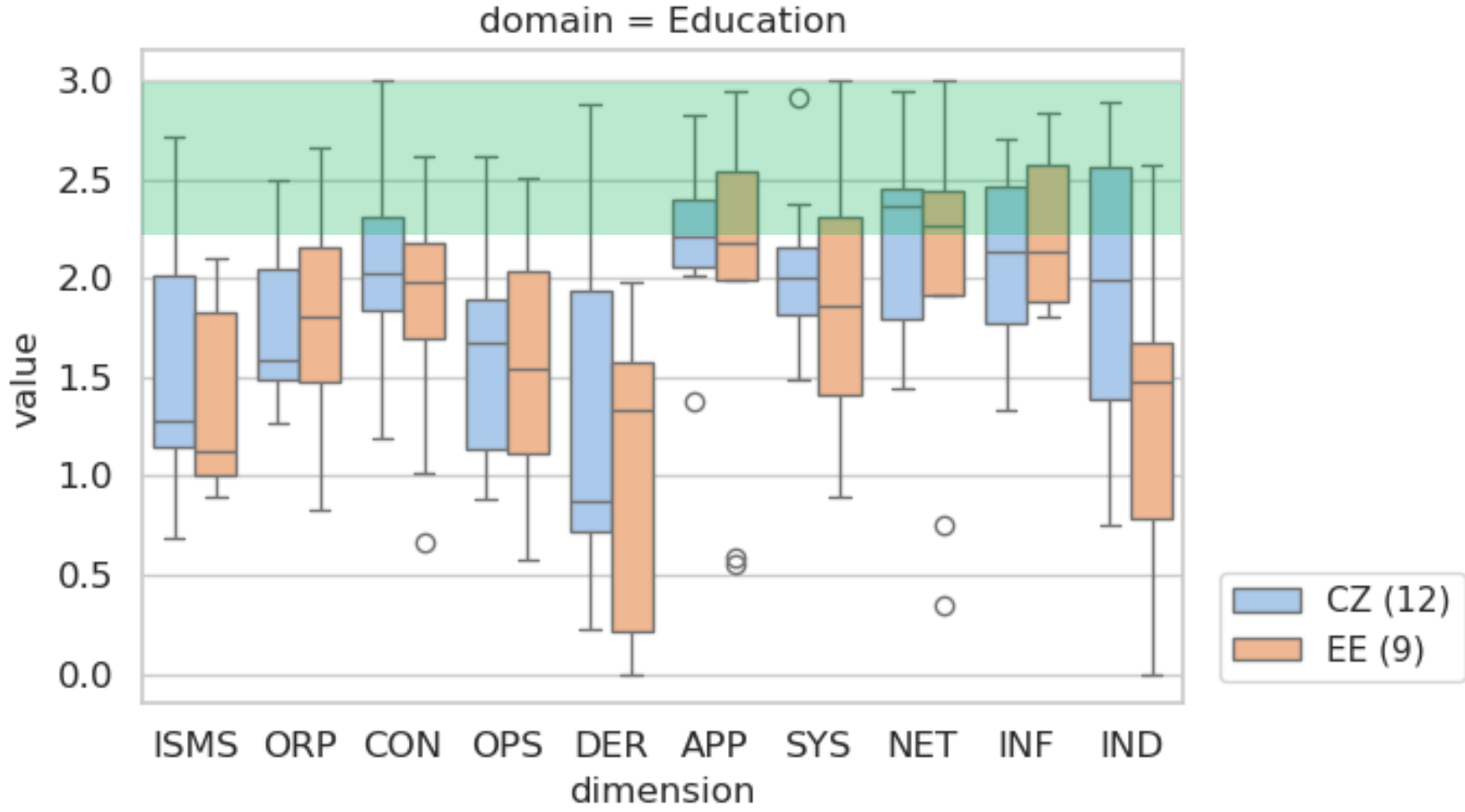
Tervishoid



KOVid



Estonia vs Tšehhi – Haridussektor 2024okt



Kasutuslood (andmete taaskasutus NIS2 järgi)

Poliitikakujundaja	• Teadlikkus, toetusmeetmed, muutuste jälgimine
Järelevalve	• Automatiseerimine, fokusseerimine
ENISA	• Teadlikkus, võrdlus
Konsultant	• Fookuspunktide seadmine, muutuste jälgimine
Organisatsioon	• Teadlikkus, tegevusplaan, võrdlus teistega, auditiasendus
Tarneahela partner	• Teadlikkus, võrdlus teistega

Teekaart: Q2 2025

Rakendaja

Üldteadmised

Sisend

Wizard 1.0

Ankeet

Eel-modelleeritud andmed

Individuaalne rakendusplaan

Turvataseme hindamise tulem

Turvataseme hindamise mudel F4SLE

*Wizard*i generaator

E-ITS & E-ITS Portaal https://eits.ria.ee/
koos masinloetavate turvameetmetega

Küpsushindamise tulemused 2024 nov - dets

E-ITS & F4SLE (Framework for Security Level Evaluation)

Sten Mäses, Mari Seeba

E-ITS

E-ITS etalonturbe kataloog esitab ohtude tõrjeks kasutatavad meetmed moodulitena.

F4SLE

F4SLE aitab moodulgruppide kaupa turvataset hinnata.

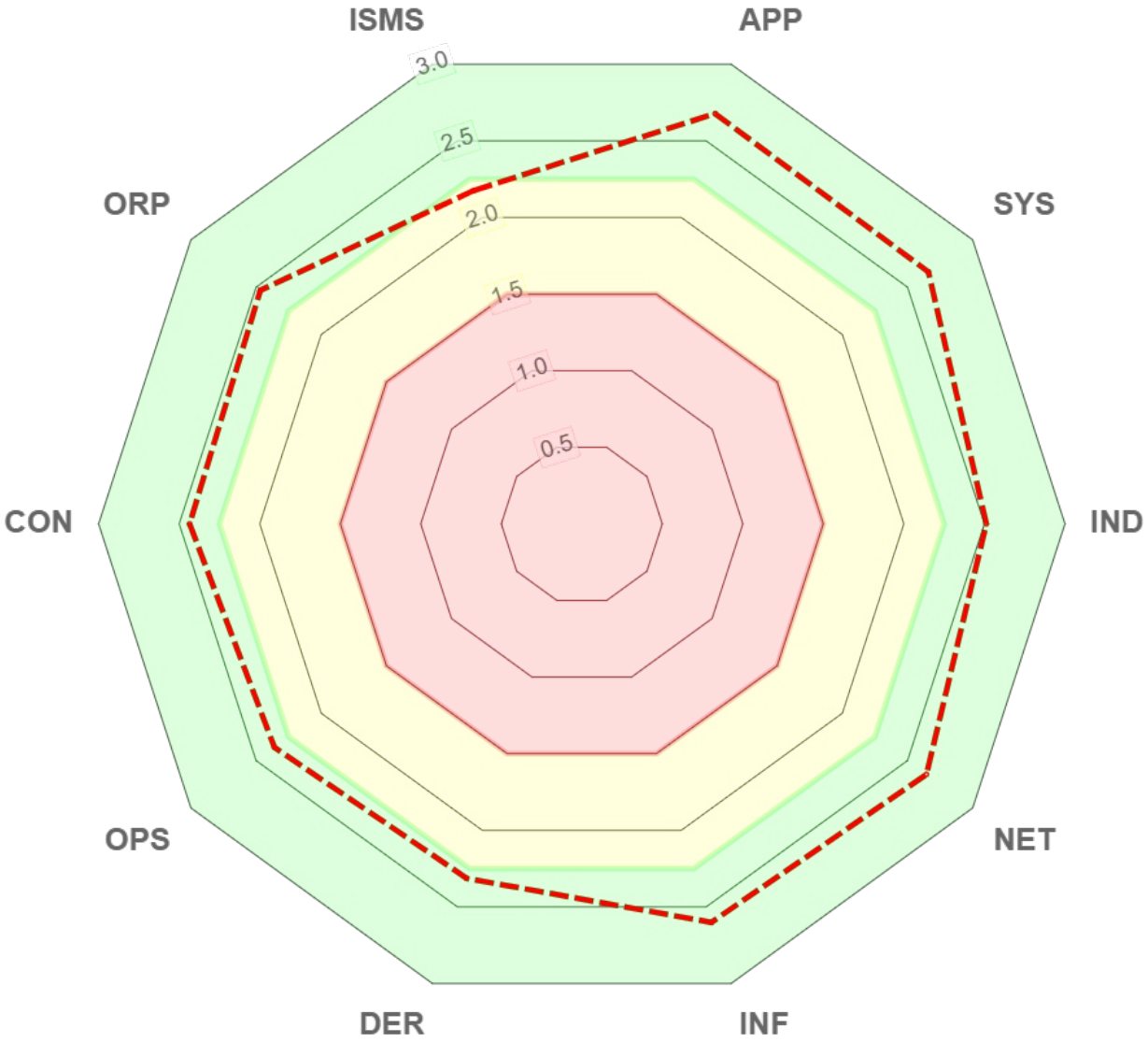
(Framework for Security Level Evaluation)

Eesmärk

- Tulemused “rohelises”
- Dokumentatsioon ja Praktilisus peavad olema rohelises (seadusest tulenevalt).
- IND võib olla nullis, kui tööstusautomaatikat, robotseadmeid pole.

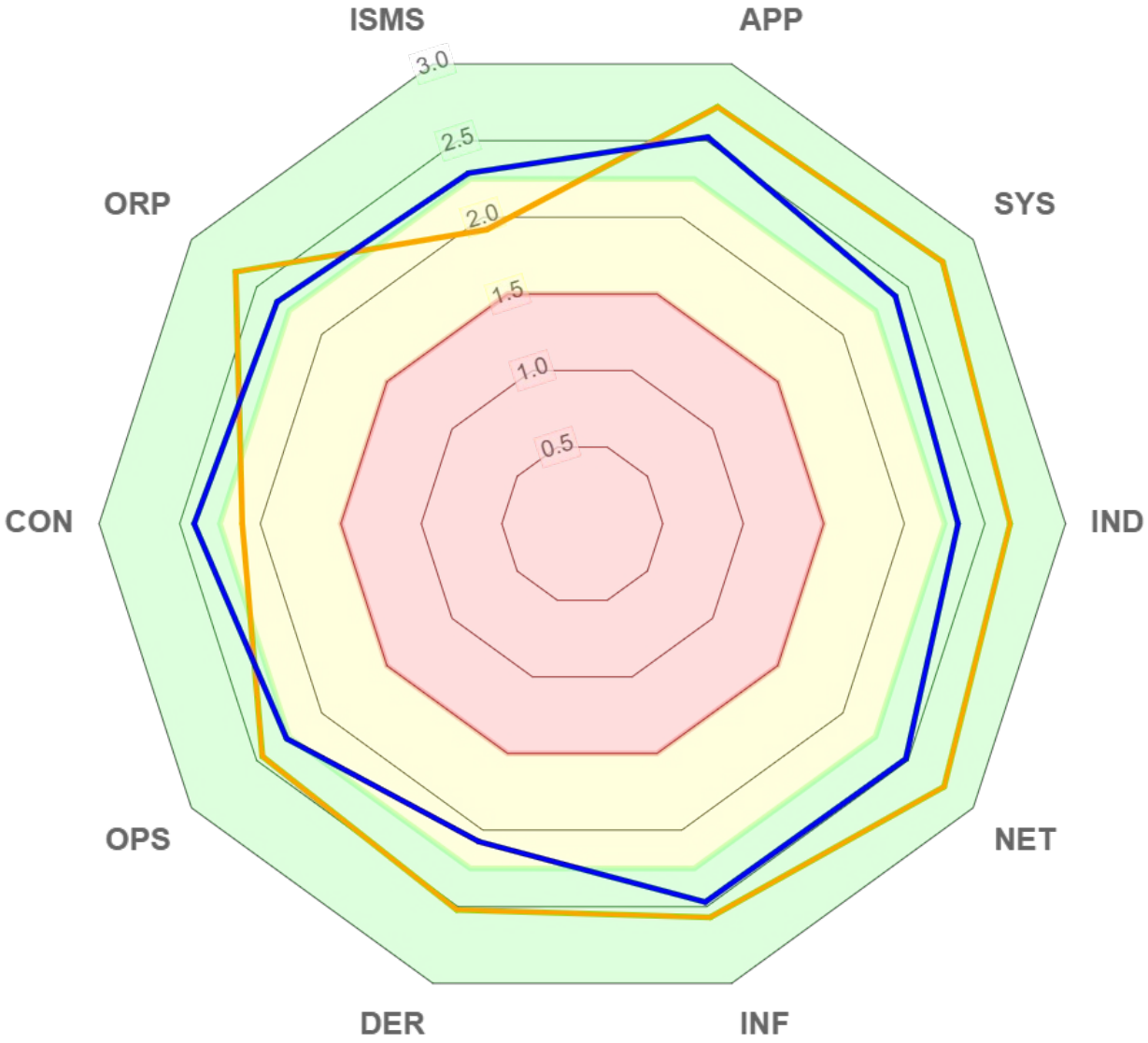
Tulemused keskmiselt

- Keskmiselt läheb pigem hästi
- ISMS moodulgrupp vajab rohkem tähelepanu (infoturbe haldus, juhtkonna kaasatus…)



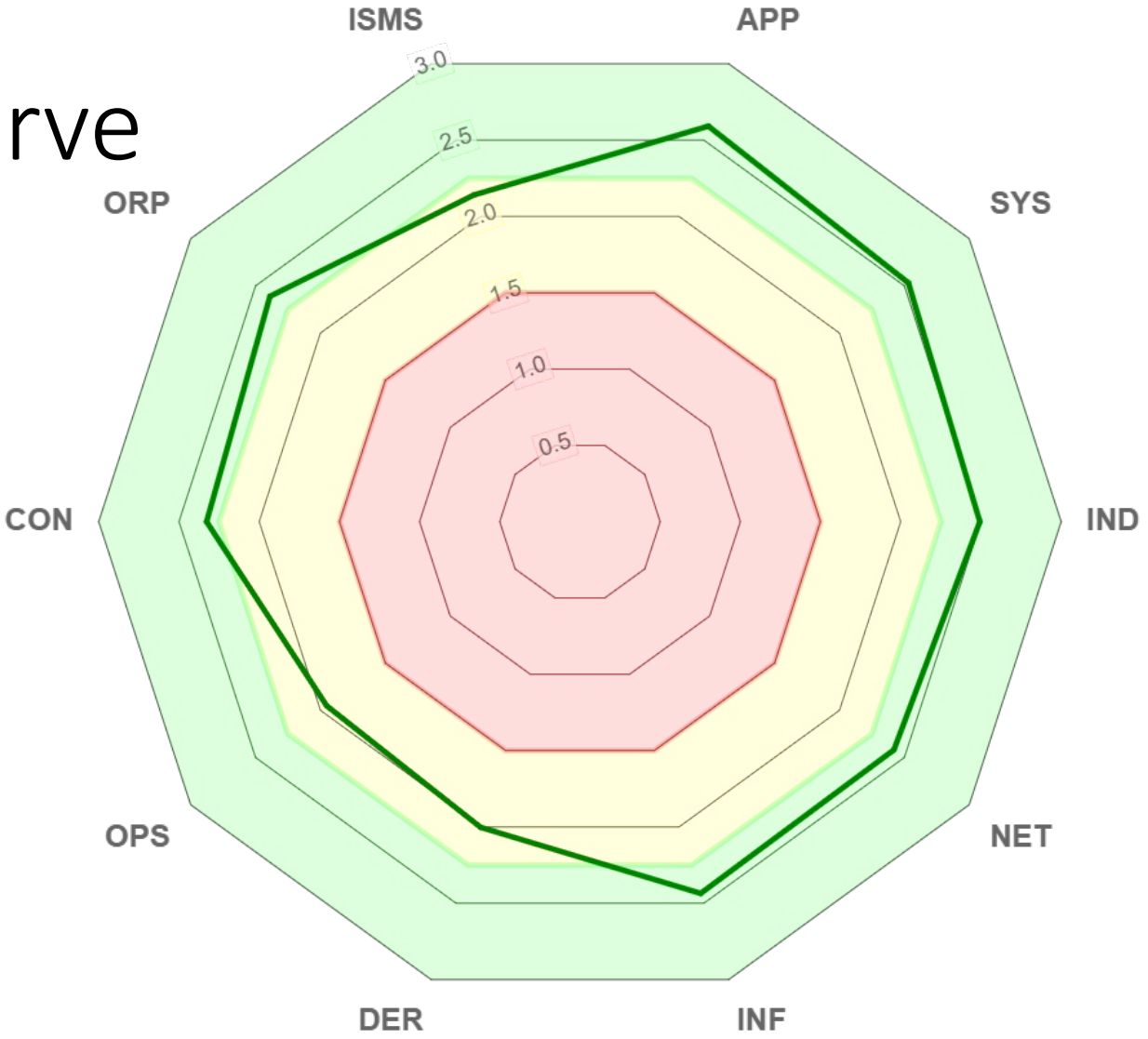
Dokumentatsioon & Praktilisus

- Praktilisus üldiselt kõrgem kui Dokumentatsioon – see tähendab, et pigem tehakse asjad kõigepealt ära ja hiljem dokumenteeritakse.
- Dokumenteerimine aitab tagada jätkusuutlikkust.



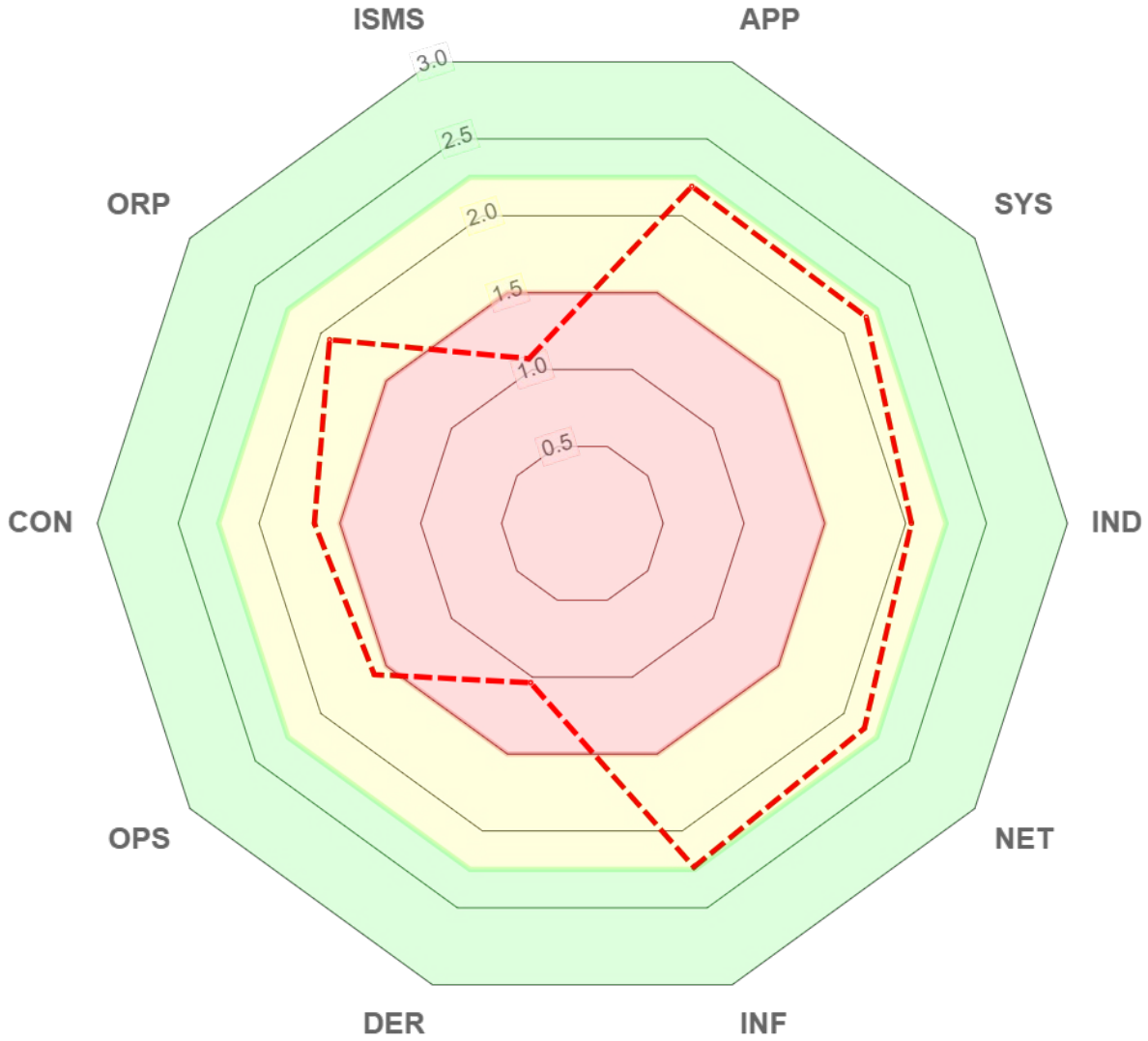
Küpsus ehk Standardturve

- Kõrgema küpsustaseme meetmete rakendamisel vajavad rohkem tähelepanu:
  - ISMS – juhtimine
  - OPS – käidutööd
  - DER – avastamine, reageerimine



Tulemused – EDU

- Valdkonniti on tulemused väga erinevad.
- Sageli on süsteemimoodulid (joonisel paremal) paremas korras kui protsessid (joonisel vasakul).
- Koolides vajab rohkem tähelepanu:
  - ISMS – juhtimine ja haldus
  - DER – avastamine, reageerimine, audit



Keskmine Teadlikkus Dokumentatsioon Praktilisus Küpsus

Jooned graafikul

Keskmine – teiste joonte keskmine

Teadlikkus – Infoturbega tegelemise vajadus on teadvustatud ja sellega tegeletakse.

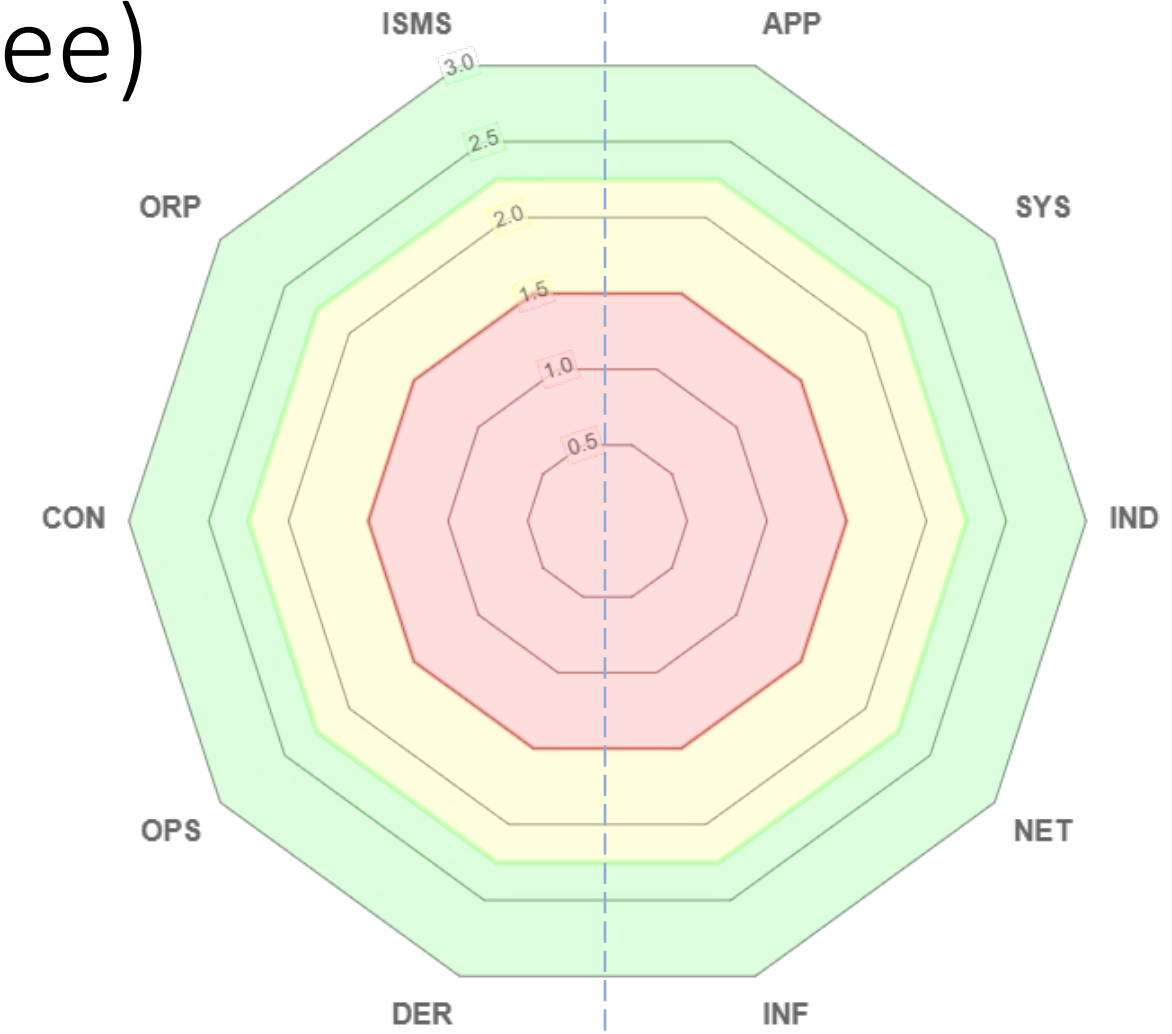
Dokumentatsioon – Formaalsed protsessid ja vajalikud infoturvet toetavad dokumendid.

Praktilisus – Rakendatud on praktilised tegevused infoturbe haldamiseks.

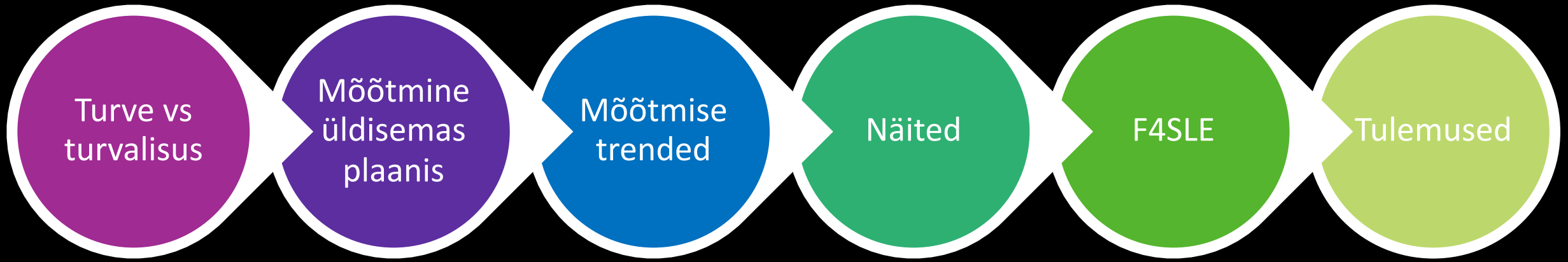
Küpsus – On selged üle-organisatsioonilised poliitikad ja printsiibid.
Tegevused on standardiseeritud, dokumenteeritud, regulaarsed ja jälgitavad.
Toimub pidev seire ja parendamine.

E-ITS moodulid (eits.ria.ee)

- Süsteemimoodulid:
  - APP – tarkvara ja koostöö lahendused – rakendused, videokõne tarkvara jms
  - SYS – saab käega katsuda ehk riistvara – serverid, telefonid. *Endpoint'*id ehk lõppseadmed
  - IND – tööstusautomaatika ja robotseadmed, SCADA kontrollerid
  - NET – võrguseadmed, mida kasutajad ei näpi – ruuterid, tulemüürid
  - INF – taristu, hooned, ruumid, seadmekapid, kaabeldus, targad majad, hooneautomaatika, värkvõrk. RKAS peamiselt haldab
- Protsessimoodulid:
  - DER – avastamine, reageerimine, parendamine ehk audit
  - OPS – käidutööd – sarnased asjad, mis tuleb tehniliste asjade puhul teha. Näiteks väljast tellimise moodul. Uuenduste paigaldamine. Juhendid admin tasemele.
  - CON – üldised asjad, mis kehtivad nii kasutajatele kui ka süsadminnidele. Kehtivad igal pool, aga ei ole otseselt kuskil teises kategoorias. Näiteks isikuandmete kaitse, andmete varundus ja hävitamine jms.
  - ORP – organisatsioon ja personali korralduslikud asjad – kes meil tööl on, kuidas me neid ära saadame.
  - ISMS – juhtimine ehk haldus, ressurside jaotamine, vastutus, järjepidevus.



protsessimoodulid süsteemimoodulid



Olek vs protsess

Mõõtmise keerukus usaldusväärsus

Mõõdikute paljusus ja taasavastamine

Eesti katsetused

Saab minna pigem paremaks

Me ei saa mõõta turvalisust,
aga saame hinnata seda, mida me selle jaoks ära teinud oleme!

Aitäh kuulamast!

Mari.Seeba@ut.ee
Mari.Seeba@ria.ee