



TARTU ÜLIKOOL  
arvutiteaduse instituut



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



```
graph LR; A((Turve vs turvalisus)) --> B((Mõõtmise üldisemas plaanis)); B --> C((Mõõtmise trended)); C --> D((Näited)); D --> E((F4SLE)); E --> F((Tulemused));
```

Turve vs turvalisus

Mõõtmise  
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

## 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)

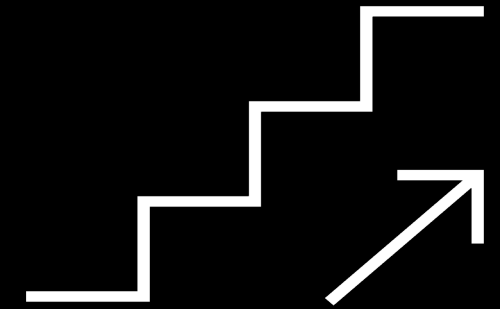
- Compliance checking
- Vulnerability identification
- Vulnerability analysis
- Penetration testing
- Checklist-based Evaluation
- Simulation-based testing
- Emulation-based testing
- Model-based testing
- Formal analysis
- Reviews

## 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

# Küpsusmodelid

	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	Acknowledgment	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	Policies	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	





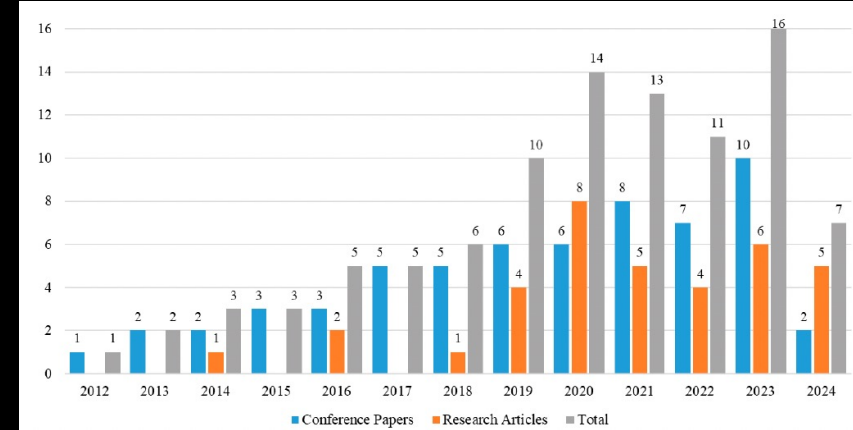
# Küpsusmõõdikute trendid

## 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 mitteamestamine
- Juhiste puudulikkus
- Kultuurilised ja inimlikud barjäärid
- Ärieesmärkidega mitteühildumine
- Automatiseerimise puudumine
- Standardiseerimata meetrika
- Integratsiooni puudumine eksisteerivate süsteemidega
- Majanduslikud barjäärid
- Fookuse puudumine intsidendi haldusele



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

---

Pilotprojekt (2020)

Word (2020)

Excel (2021)

MASS (2022)

E-ITS Hub (2025)



# 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

- **Privaatsus**printsip – toorandmed ei lahku vastaja juurest
- Serverisse saadetakse vaid **agregeritud** (keskmistatud andmed)
- **Kohene** tulemuse näitamise vastajale
- **Võrdlus**aluse esitamine vastajale
- Andmete **taaskasutus**

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



Toote keskkond



RIIGI INFOSÜSTEEMI AMET



TARTU ÜLIKOOL  
arvutiteaduse instituut

0/189

APP - Rakendused

Olukorra hinnang tarkvara, rühmatarkvara, kataloogiteenuste ja tellimustarkvara haldamisele, sh nende uuendamised turvalised seadistamised, vaid vajaduspõhised juurdepääsud, logimine.

1. Rakenduste kasutuselevõtul jälgitakse rakendustele antavaid õigusi ja neid piiratakse.

① Lisainfo

Vältes kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud	Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega	Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega	Väide vastab sinu organisatsiooni kontekstis täielikult tõele	Jätan vastamata	Ei kehti
---	--	--	---	-----------------	----------

2. Rakendusi, rühmatarkvara ja kataloogiteenusid on lubatud hallata vaid selleks määratud administraatoril.

① Lisainfo

Vältes kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud	Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega	Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega	Väide vastab sinu organisatsiooni kontekstis täielikult tõele	Jätan vastamata	Ei kehti
---	--	--	---	-----------------	----------

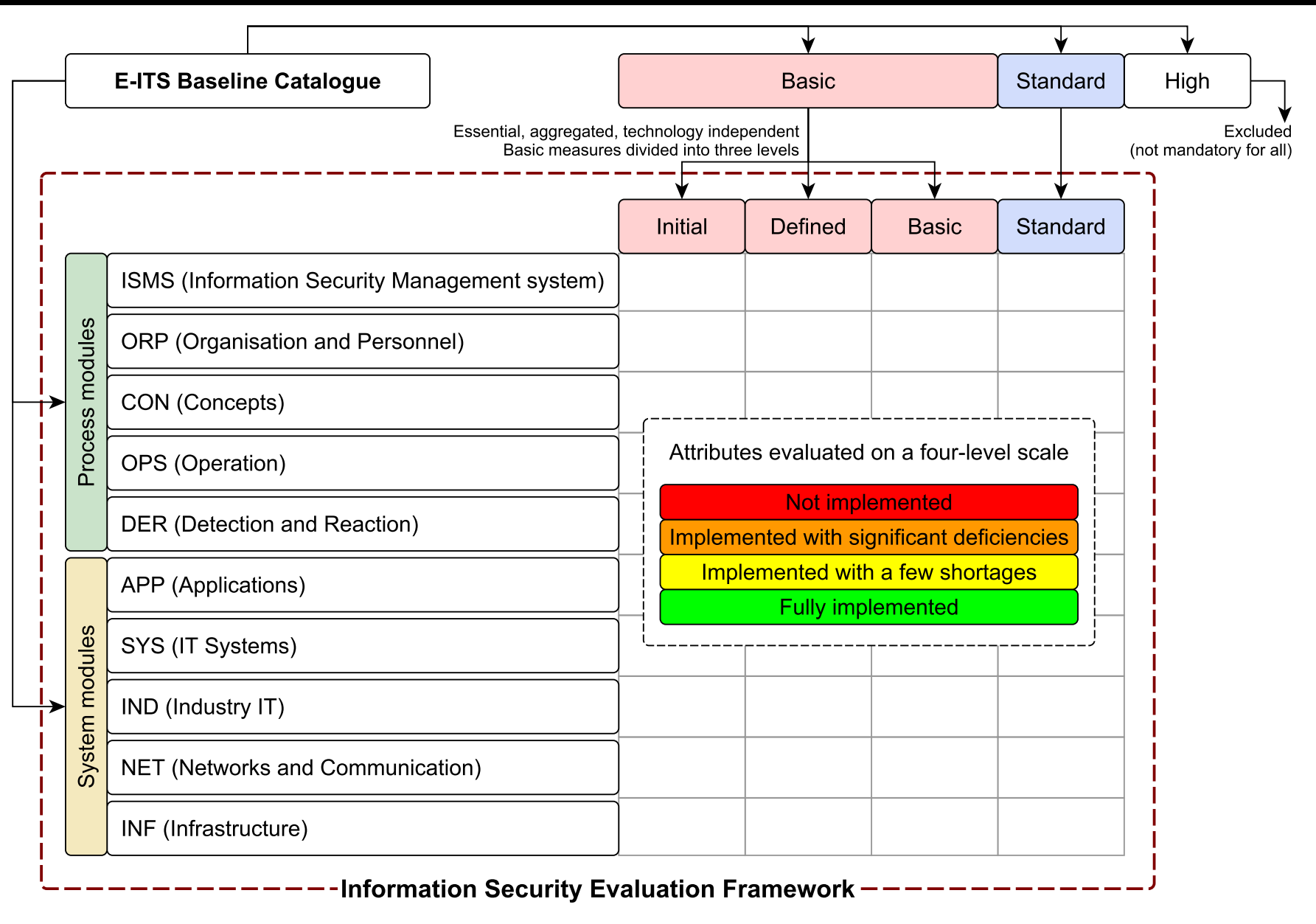
3. Kahjurvaravastast tarkvara kasutatakse e-posti serverites rämpsposti ja pahatahtliku sisu tuvastamiseks sissetulevates ja väljaminevates e-kirjades ning e-posti manustes.

① Lisainfo

Vältes kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud	Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega	Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega	Väide vastab sinu organisatsiooni kontekstis täielikult tõele	Jätan vastamata	Ei kehti
---	--	--	---	-----------------	----------

4. Kataloogiteenustele (directory service) on kehtestatud reeglid.

① Lisainfo



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.



<0.75 INITIATED  
 Good practices have not been implemented, risks have not been recognized, and management has not taken the initiative. Security activities are sporadic and instead initiated at the grassroots level.

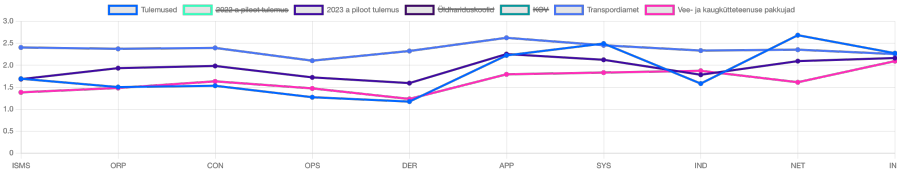
>=0.75 and <1.5 DEFINED  
 Processes and activities are initiated on an ad hoc basis. Documents have been prepared but are partially outdated or do not correspond to reality.

>=1.5 and <2.25 BASIC  
 Practices work and are documented, resources are planned, and roles and responsibilities are allocated. Regularity of activities has not yet been achieved.

>2.25 STANDARD  
 Organizational policies and principles are clear. Activities are monitored and traceable, and activities are standardized and documented. Continuous improvement is taking place. Exceptions are monitored.

- Generate PDF
- Save detailed answers to local disk
- Save summary metadata to local disk

Results compared to benchmark



Process dimensions

**ISMS** Situation assessment of the establishment and performance of the organisation's information security management system, including the involvement of management, distribution of responsibilities and allocation of resources and asset mapping.

**ORP** Situation assessment of information security management, including usage rules for computers and other devices, personnel policy, identity and access rights management, and training.

**CON** Situation assessment of the organisation's basic information security concepts used for all other areas, including backups, archiving, development, personal data protection principles, and cryptography-related procedures and awareness. In addition, data exchange agreements between data exchange partners.

**OPS** Situation assessment of the organisation's IT operation management regardless of specific hardware, software, or network components. This includes the management and documentation of Cloud services and remote work.

**DER** Situation assessment of security incident management, related activities (including IT forensics), audits, and emergency preparedness (including exercises).

System dimensions

**APP** Situation assessment of software, groupware, directory services, and subscription software management, including secure configurations of updates, need-based accesses, and logging.

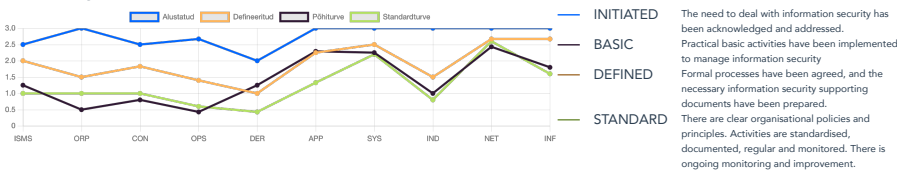
**SYS** Situation assessment of the hardware solutions and management (including setup, monitoring, and management) like servers, computers, tablets, phones, removable data media, and virtualization solutions.

**IND** Situation assessment of secure management (configuration and monitoring) and safety of machine tool control computers, sensors, robots, lab and diagnostic equipment, warehouse systems and other industrial IT systems.

**NET** Situation assessment of network, network components, telephone communications management, computer network project timeliness, regular updating, and outdated and unsafe solution avoidance (default passwords and manufacturer-unsupported solutions).

**INF** Situation assessment of security management for buildings, rooms, cabling, mobile workplaces, vehicle IT solutions and smart houses. Compliance with building fire safety requirements, special safety requirements and location in facilities for protected rooms, and the inclusion of smart infrastructure in the security policy are considered.

Maturity levels



**INITIATED** The need to deal with information security has been acknowledged and addressed.

**BASIC** Practical basic activities have been implemented to manage information security.

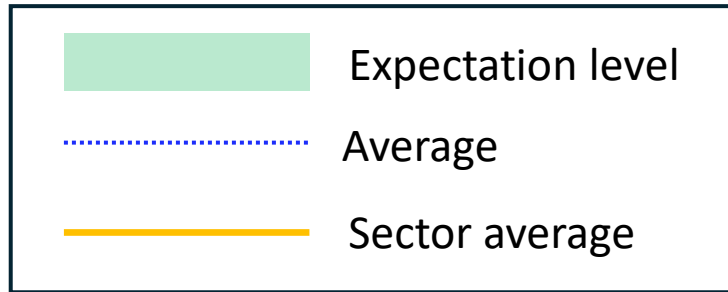
**DEFINED** Formal processes have been agreed, and the necessary information security supporting documents have been prepared.

**STANDARD** There are clear organisational policies and principles. Activities are standardised, documented, regular and monitored. There is ongoing monitoring and improvement.

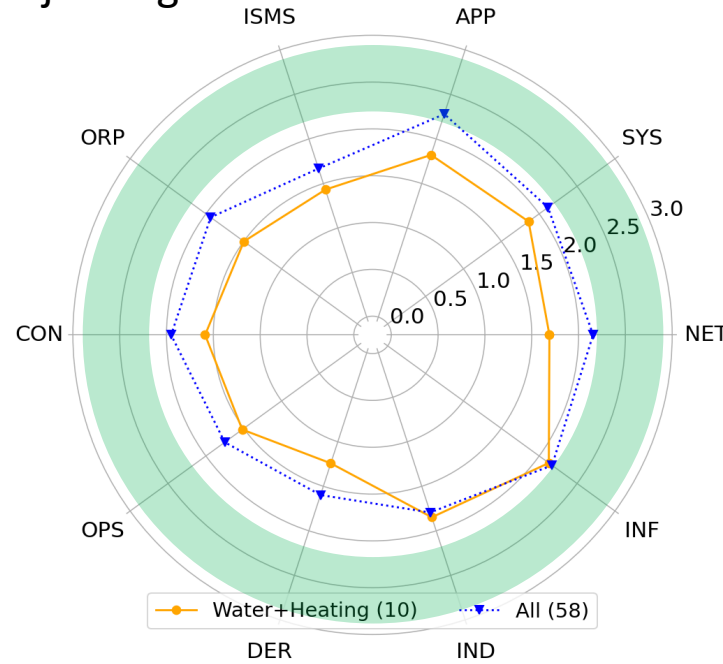
# Organisatsioon ja CISO

- Hinnang 10 dimensioonis
- Riski tasemed
- Võrdlus ootusega (roheline joon)
- Võrdlusalus teiste sektoritega
- Turbedimensioonide selgitused
- Küpsustasemed detailsemalt

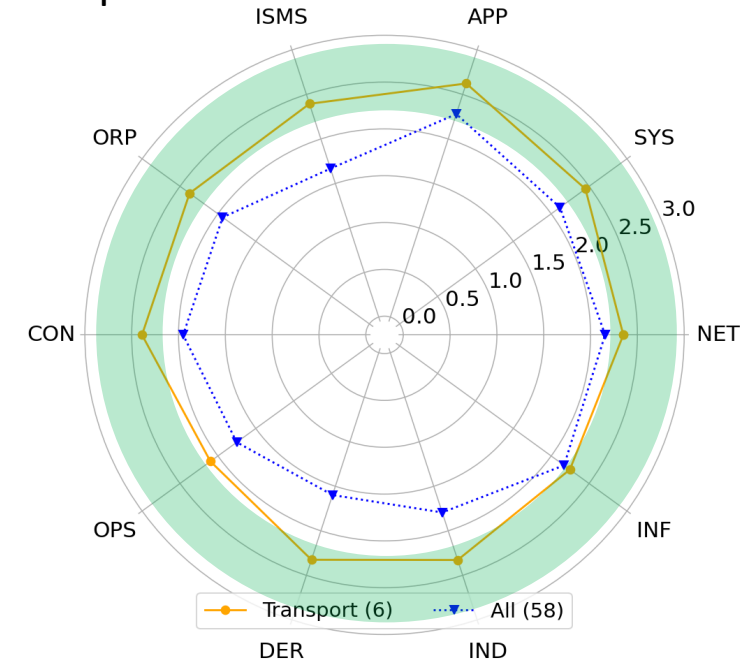
# Sektorite võrdlus 2023okt-2024okt



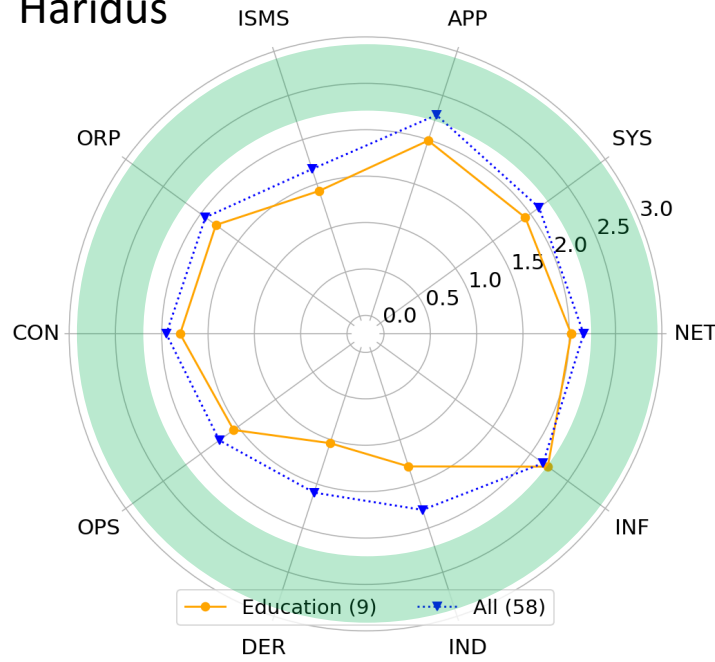
## Vesi ja kaugküte



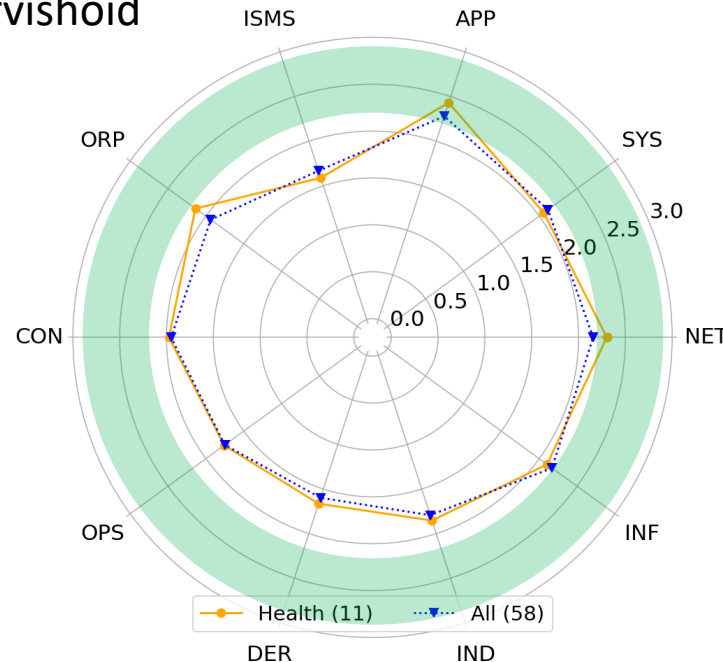
## Transport



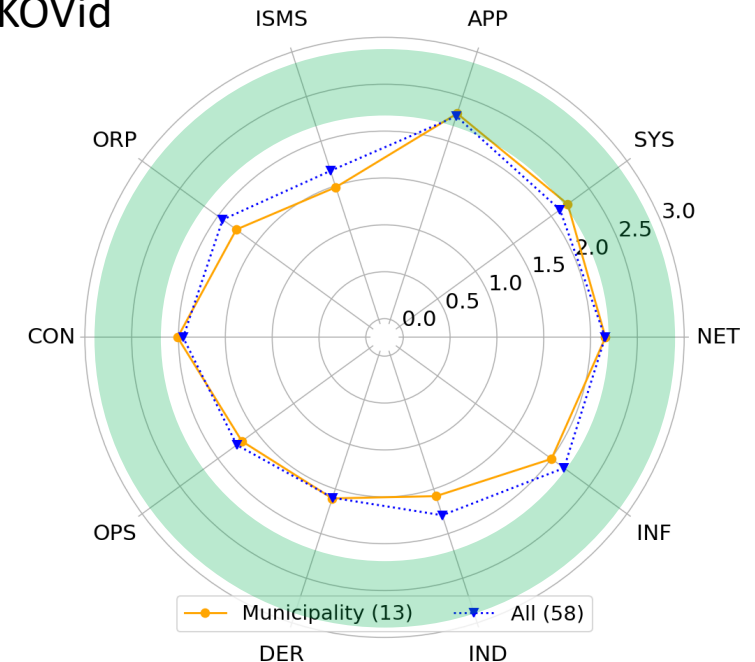
## Haridus



## Tervishoid

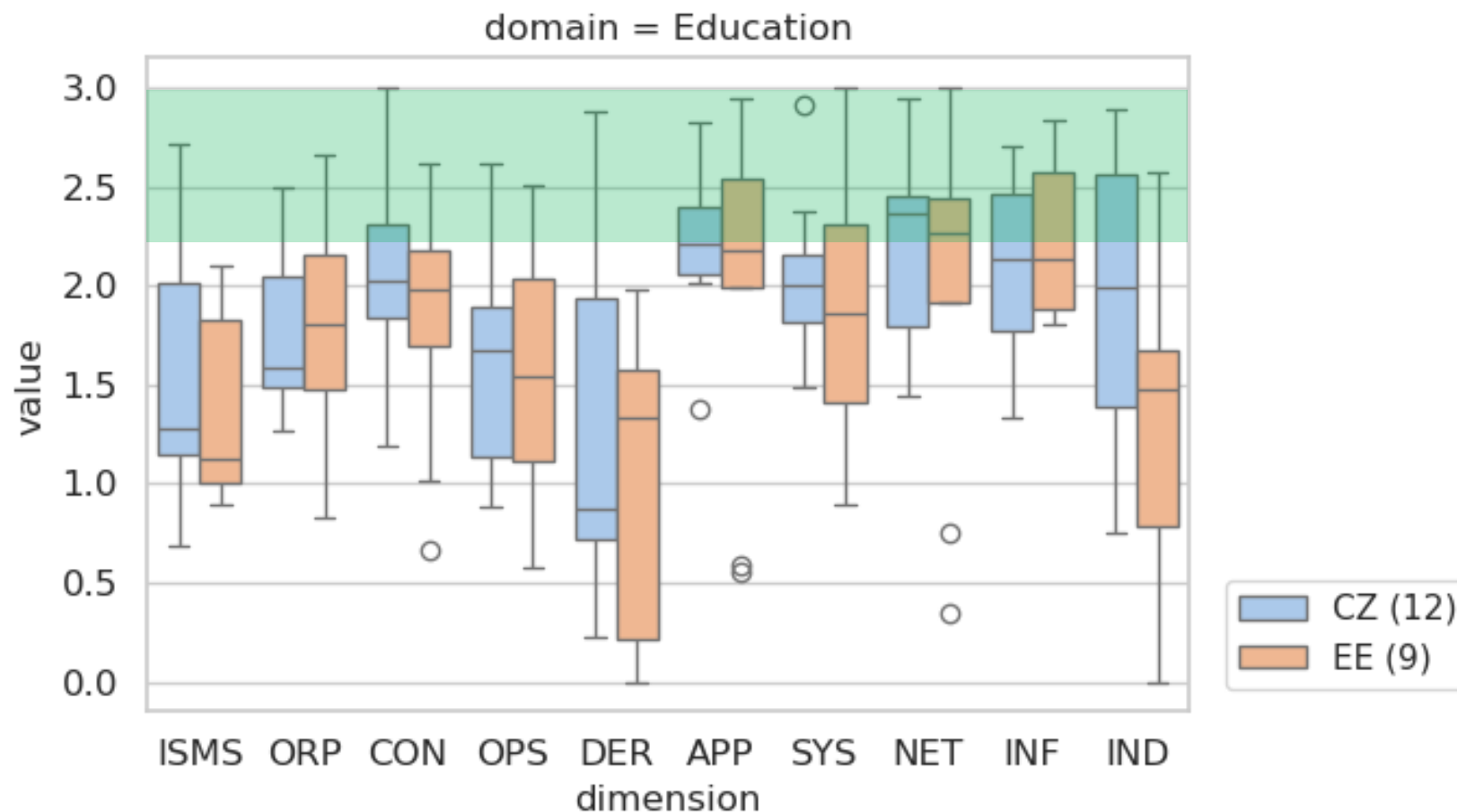


## KOvid





# 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

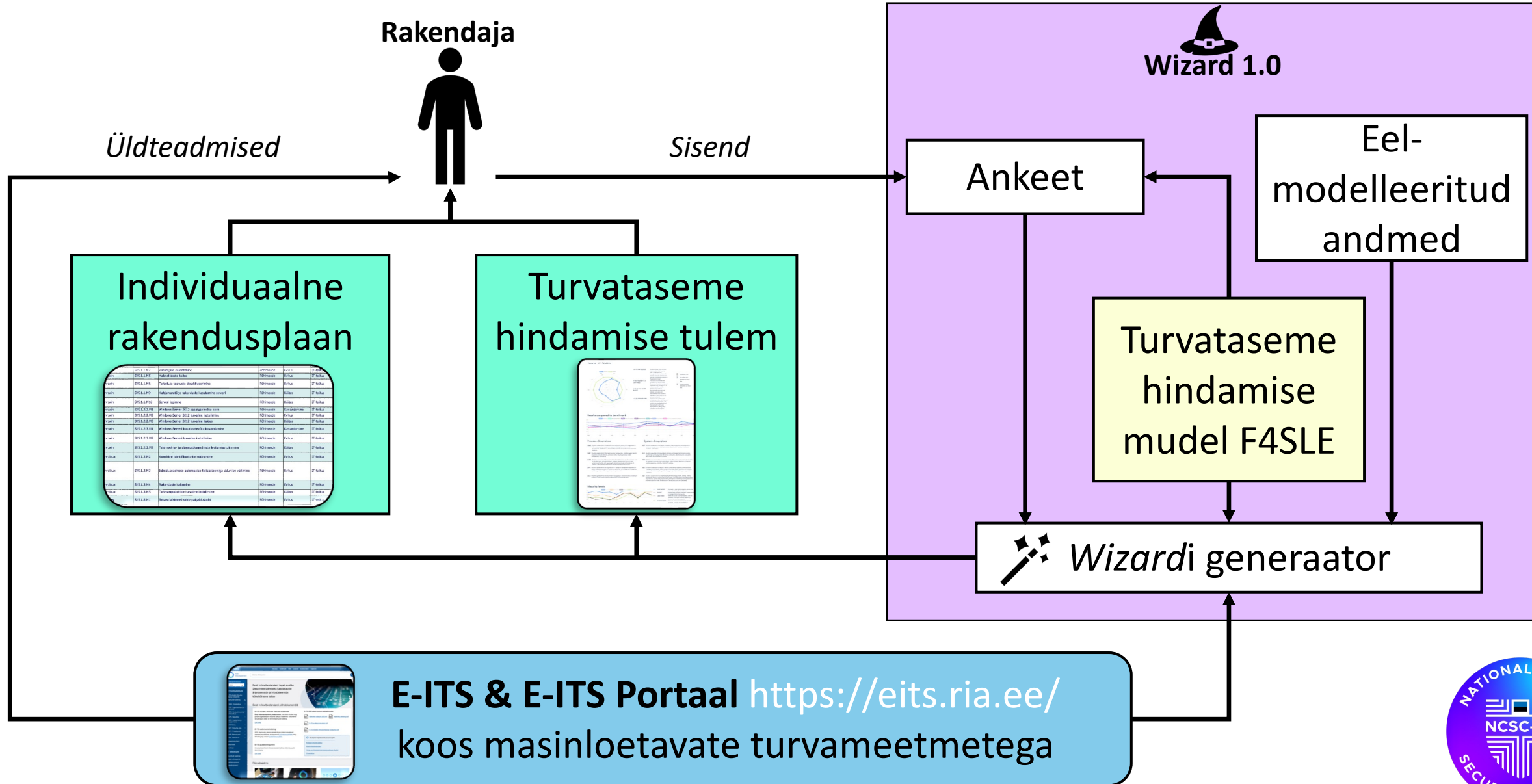
Organisatsioon

- Teadlikkus, tegevusplaan, võrdlus teistega, auditiasendus

Tarneaahela partner

- Teadlikkus, võrdlus teistega

# Teekaart: Q2 2025



# Küpsushindamise tulemused 2024 nov - dets

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

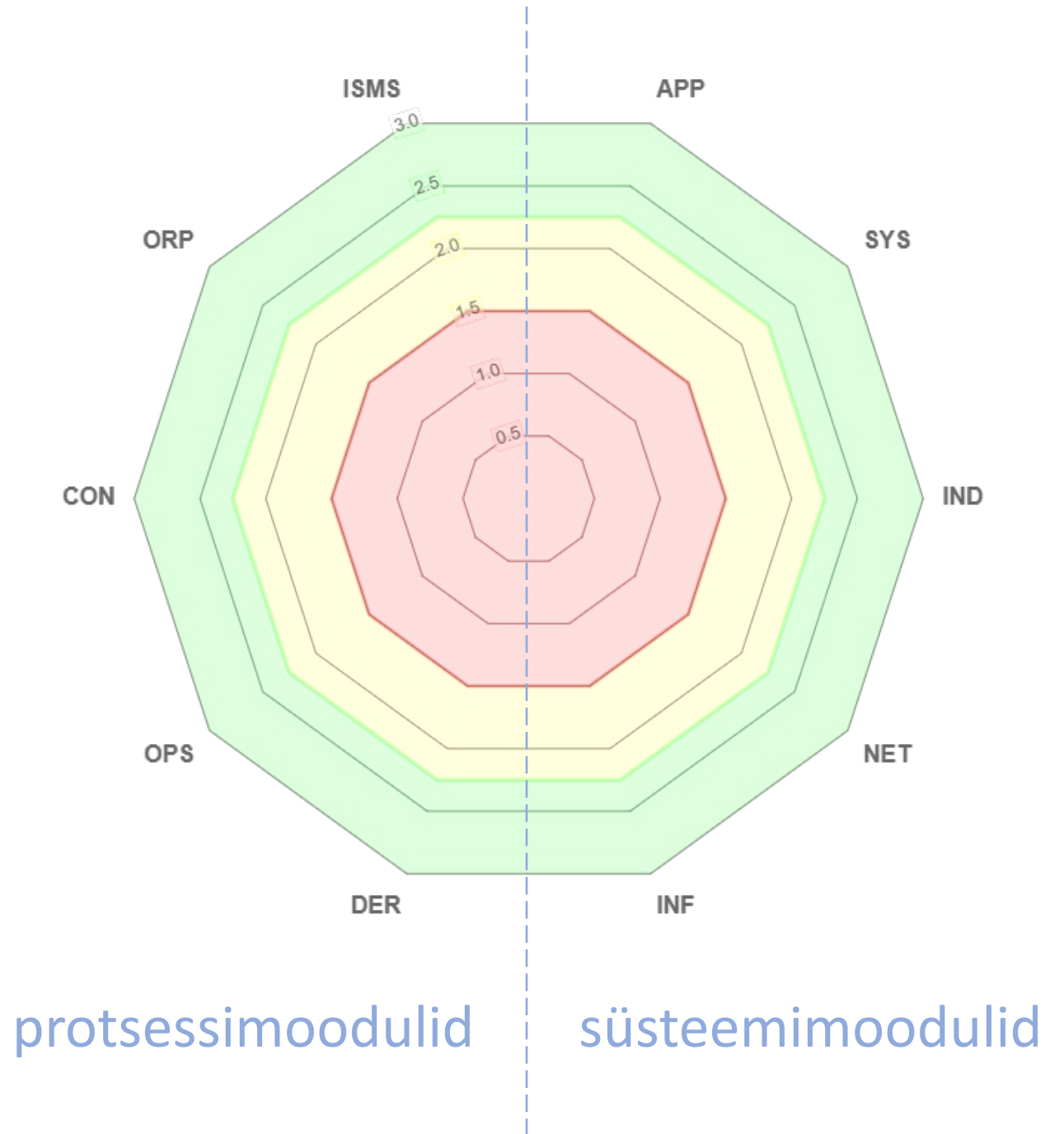
Sten Mäses, Mari Seeba

# E-ITS

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

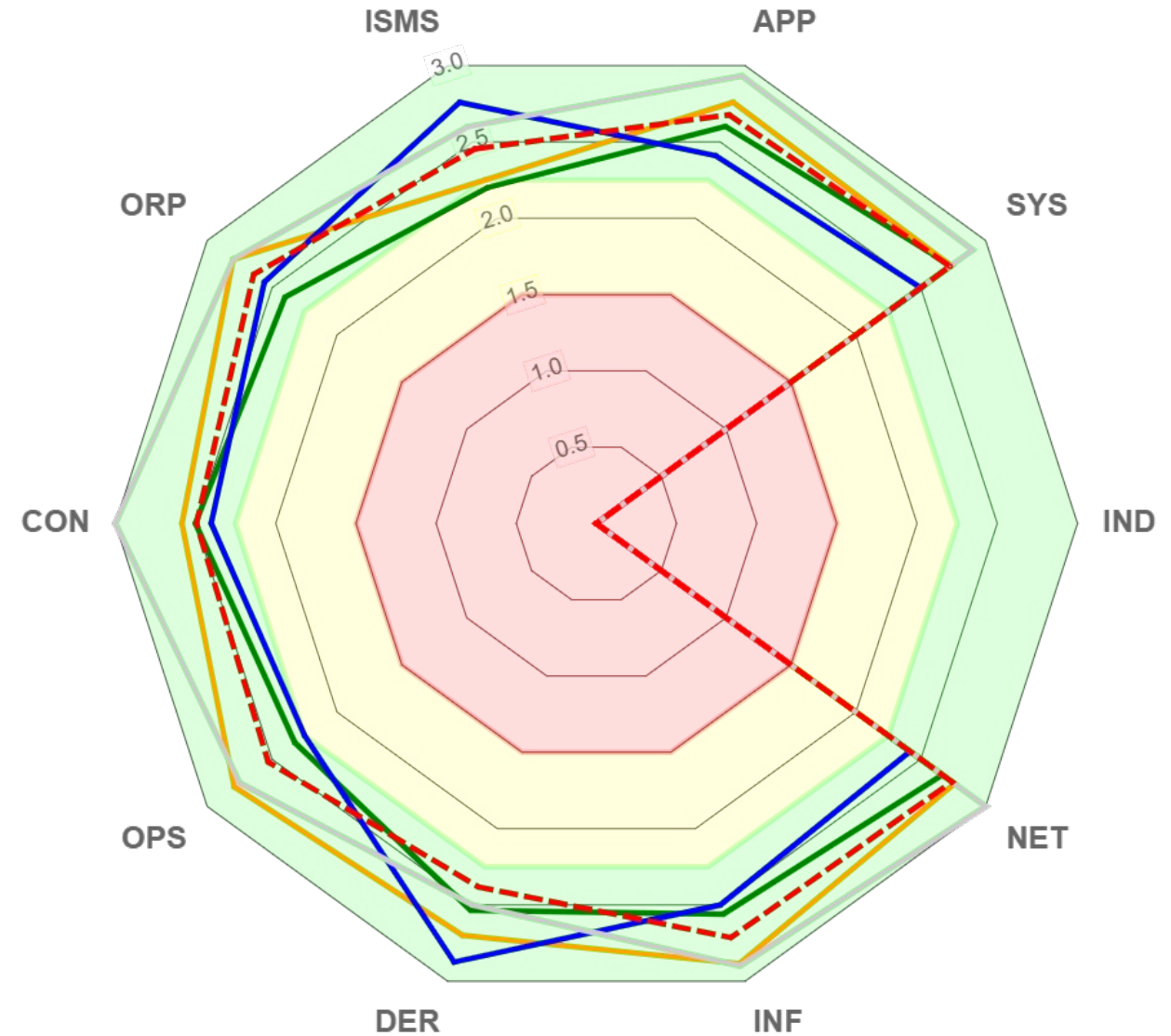
# F4SLE




F4SLE aitab moodulgruppide kaupa turvataset hinnata.  
*(Framework for Security Level Evaluation)*



# Eesmärk

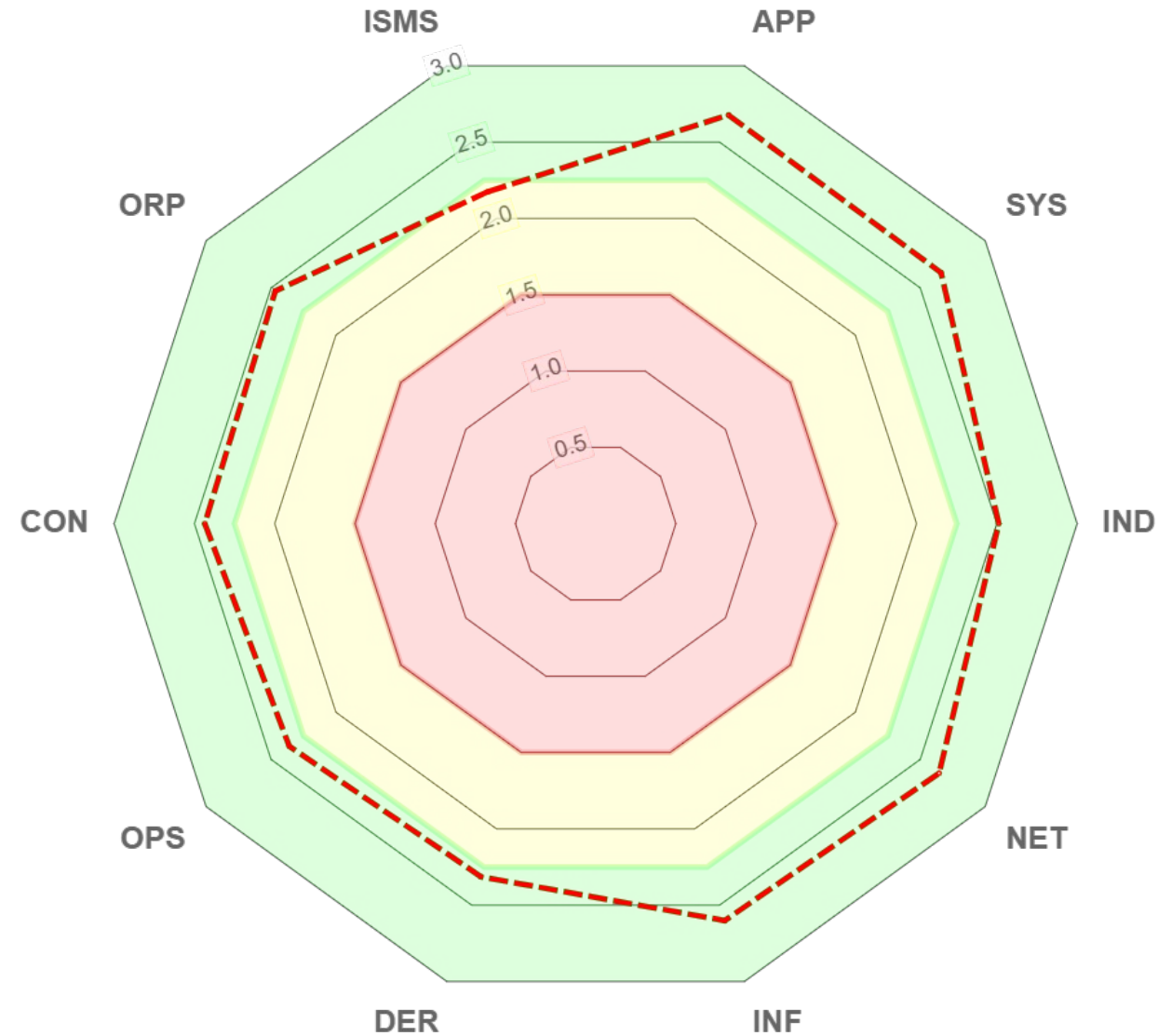
- Tulemused “rohelistes”
- Dokumentatsioon ja Praktilisus peavad olema rohelistes (seadusest tulenevalt).
- IND võib olla nullis, kui tööstusautomaatikat, robotseadmeid pole.




 Keskmine  Teadlikkus  Dokumentatsioon  Praktilisus  Küpsus

# Tulemused keskmiselt

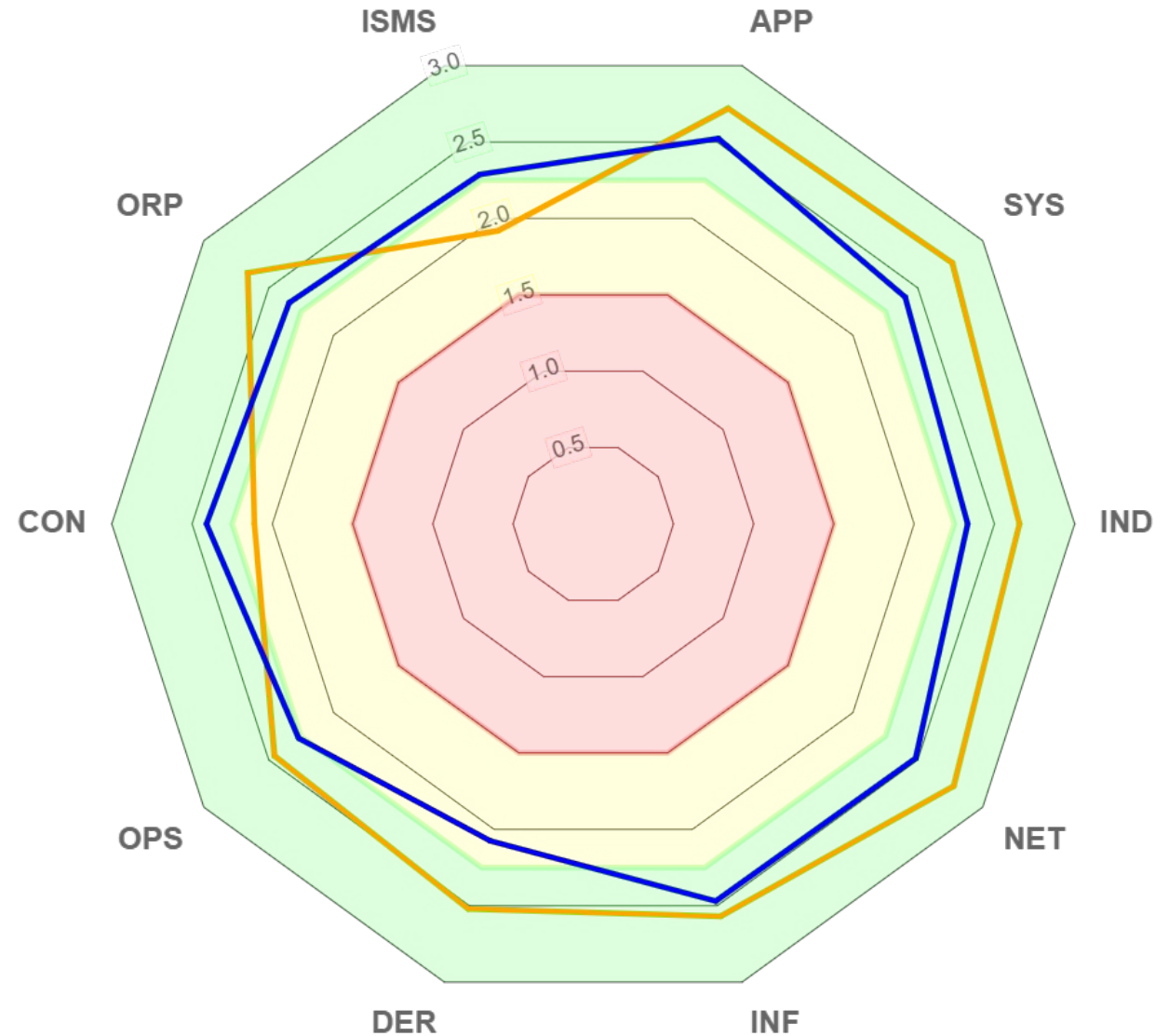
- Keskmiselt läheb pigem hästi
- ISMS moodulgrupp vajab rohkem tähelepanu (infoturbe haldus, juhtkonna kaasatus...)




 Keskmine  Teadlikkus  Dokumentatsioon  Praktilisus  Küpsus

# Dokumentatsioon & Praktilisus

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

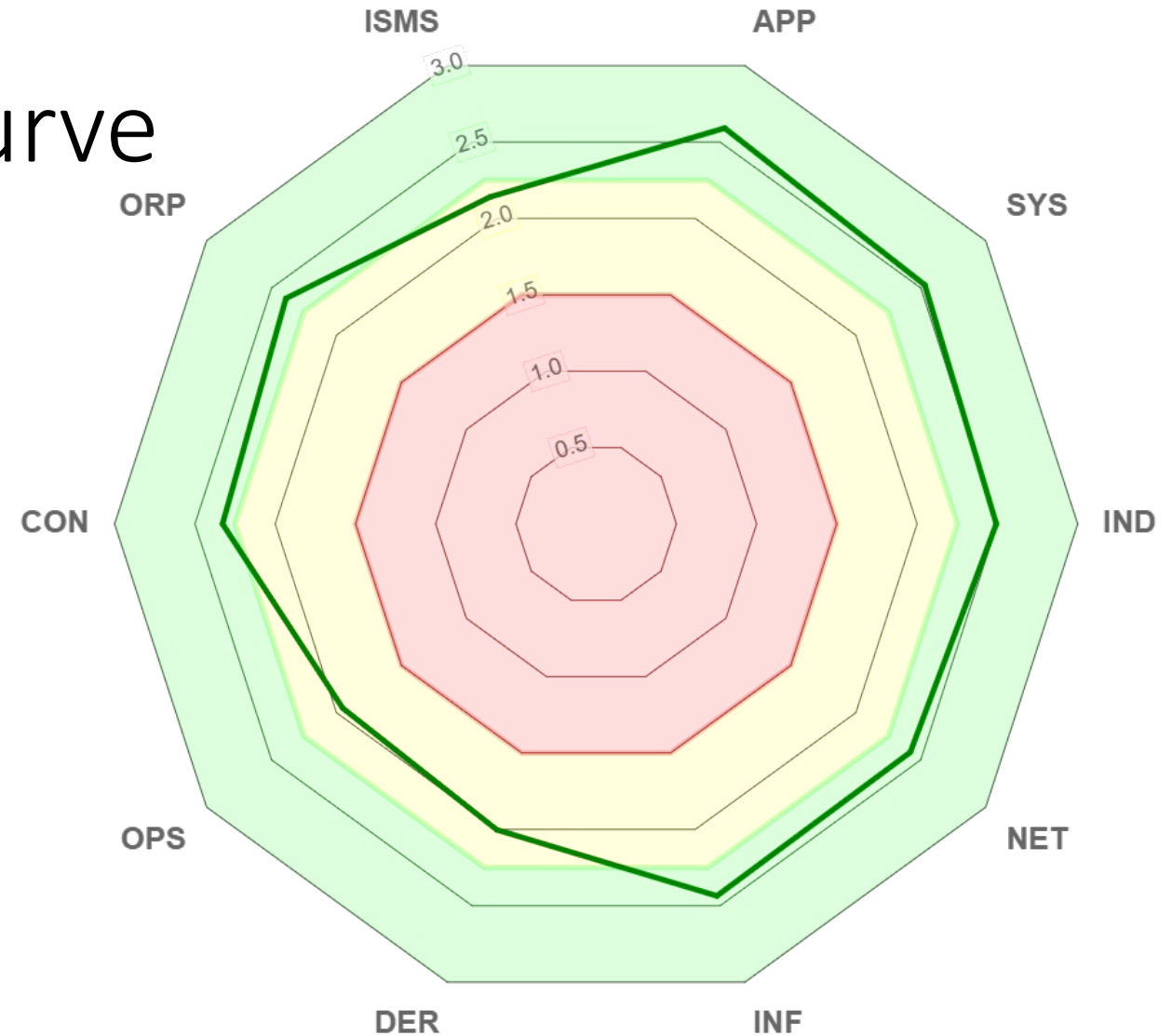


 Keskmine  Teadlikkus  Dokumentatsioon  Praktilisus  Küpsus



# Küpsus ehk Standardturve

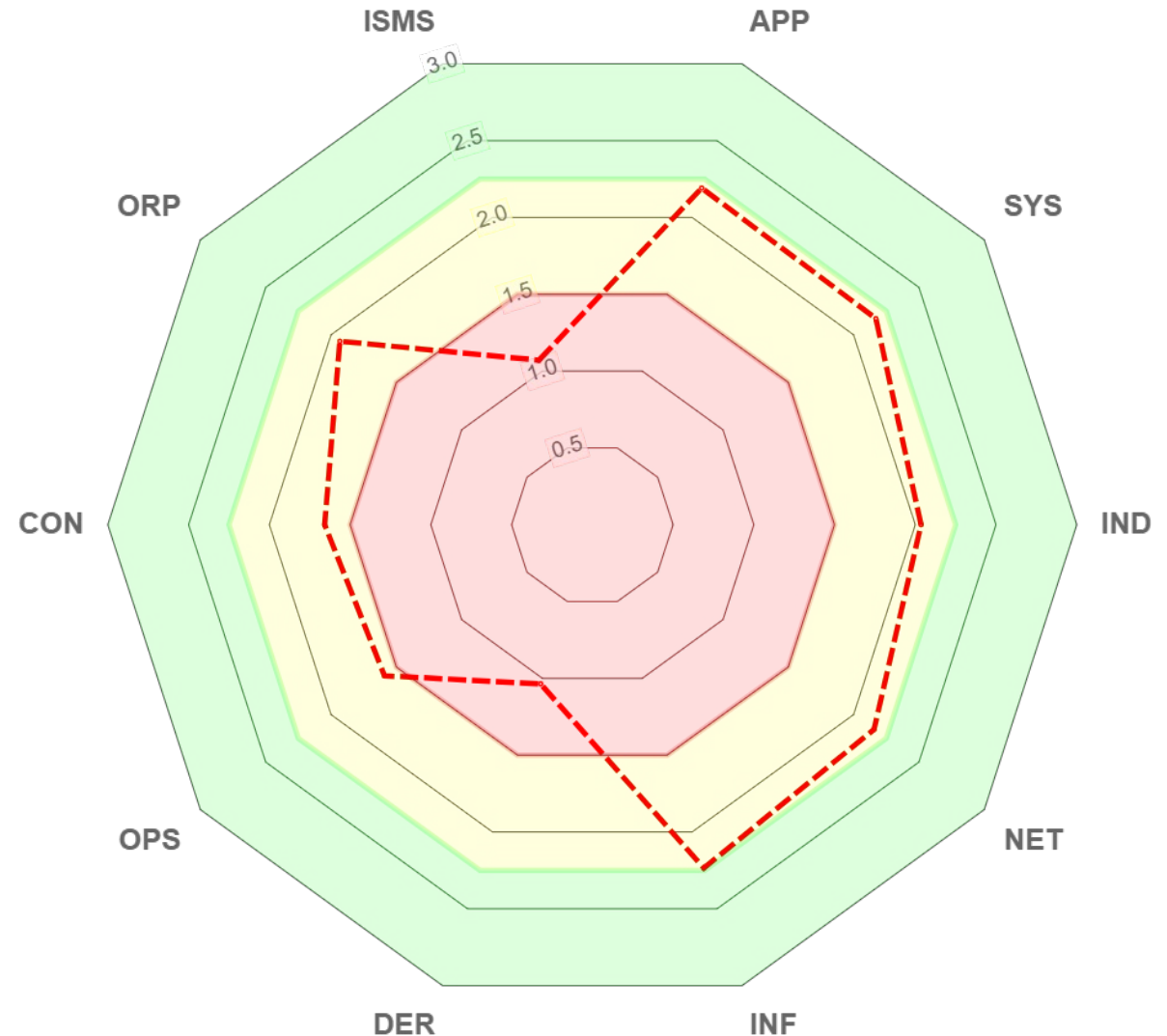
- Kõrgema küpsustaseme meetmete rakendamisel vajavad rohkem tähelepanu:
  - ISMS – juhtimine
  - OPS – käidutööd
  - DER – avastamine, reageerimine



 Keskmine  Teadlikkus  Dokumentatsioon  Praktilisus  Küpsus

# 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 – Infoturbe 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:

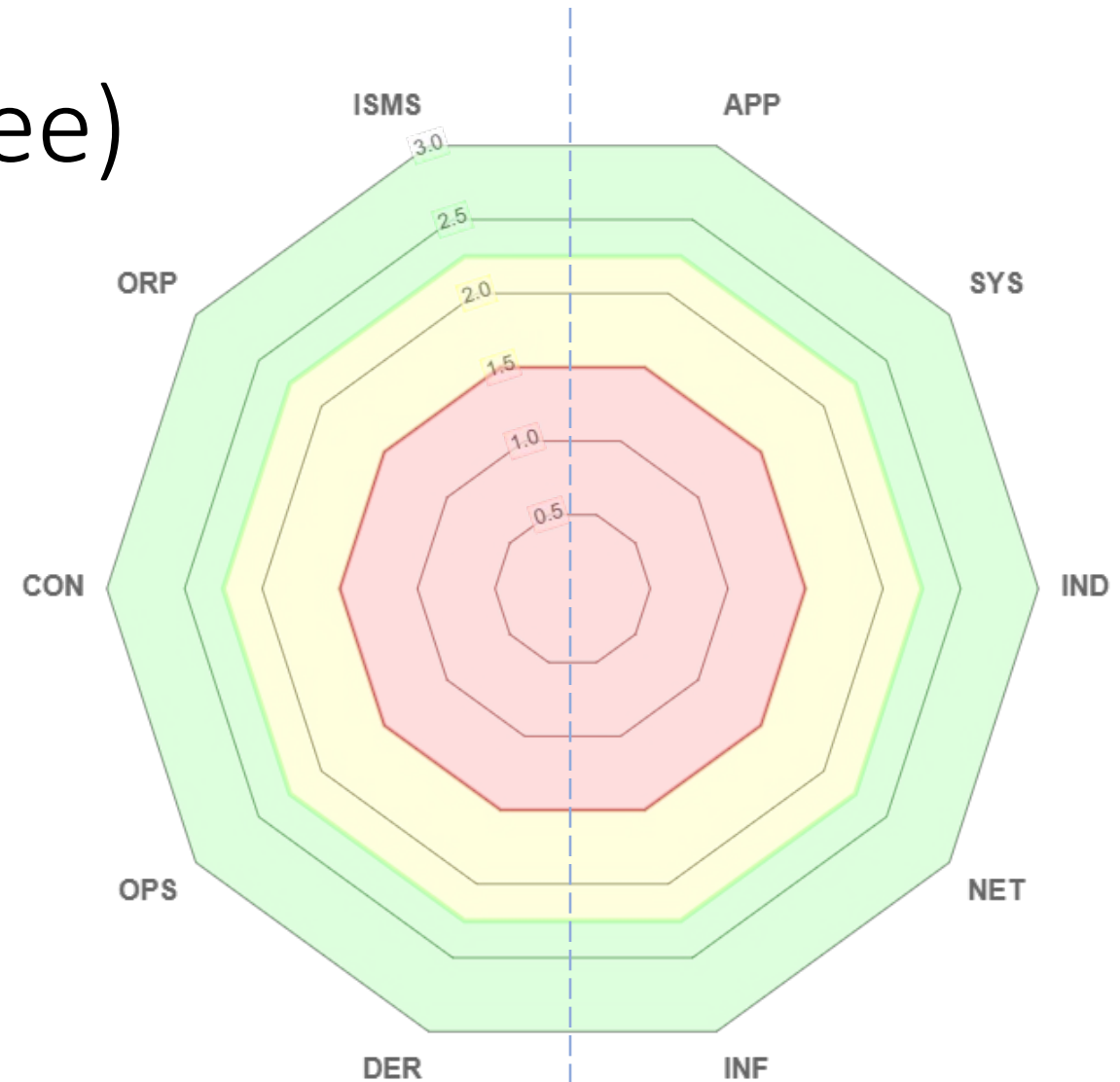
- APP – tarkvara ja koostöö lahendused – rakendused, videokõne tarkvara jms
- SYS – saab käega katsuda ehk riistvara – serverid, telefonid. *Endpoint*'id ehk lõppseadmed
- IND – tööstusautomaatika ja robotseadmed, SCADA kontrollid
- NET – võrguseadmed, mida kasutajad ei näpi – ruuterid, tule müürid
- INF – taristu, hooned, ruumid, seadmekapid, kaabeldus, targad majad, hooneautomaatika, värgvõrk. RKAS peamiselt haldab

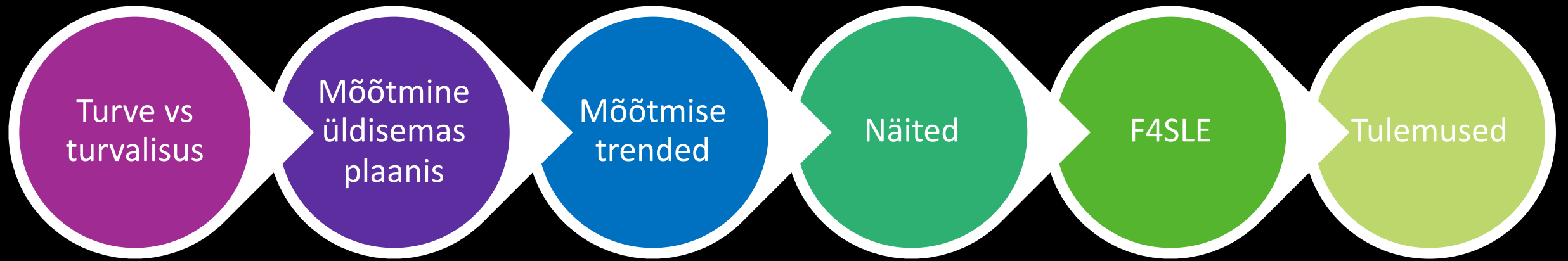
## • Protsessimoodulid:

- 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 töö on, kuidas me neid ära saadame.
- ISMS – juhtimine ehk haldus, ressurside jaotamine, vastutus, järjepidevus.

protsessimoodulid

süsteemimoodulid





Olek vs protsess

Mõõdikute paljusus ja taasavastamine

Eesti katsetused

Mõõtmise keerukus  
usaldusväärsus

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](mailto:Mari.Seeba@ut.ee)  
[Mari.Seeba@ria.ee](mailto:Mari.Seeba@ria.ee)