

Infoturve – kohustus või abiline?

Mari Seeba
Küberturbe juhtivekspert

11.04.2024

Palju õnne juhtiva rolli puhul!

- Finantsid ja eelarve
 - Protsessid, varad, ressursid
 - Kuidas neid siiani on kaitstud?
-
- Aga andmed?

Äriprotsessid ja teenused

- Mis teenuseid me pakume?
- Milliseid sisemisi protsesse ja välimisi teenuseid me selleks vajame?
 - Tugiprotsessid
 - Juhtimisprotsessid
 - Äriprotsessid
- Mis on protsesside omavahelised ristsõltuvused?

Nõuded

- Kas meil on üldse vaja midagi kaitsta?
- Kui palju, mis on meie piir? ... aga andmesubjekti piir?

KAITSETARVE

Riskihaldus: Formaalne nõue või eelarve alus?

Riskihaldus: Formaalne nõue või eelarve alus?

Alusohitude kataloog

Kahjustsenaariumid

Kaitsetarve

KOV VOIP telefonilt tehti libakõnesid öösel 1 tunni jooksul

- **Põhjus:** uuendamata serveri tarkvara ja nõrk parool
- **Kahju:** 3600€

KOV hallatavas asutuses pani töötaja serveriruumi püsti krüptoraha teenimise masina

- **Põhjus:** puudulik ülevaade võrgust
- **Kahju:** kordades suurenenud energia kulu, võrgukoormus, soovimatud külalised võrgus, mainekahju

KOV kodulehe serverisse häkiti sisse ja kasutati seda serverit ummistusrünnete tegemiseks (leht ise oli nähtav)

- **Põhjus:** Uuendamata veebikeskkond, vastutaja puudumine, puudus kontroll.
- **Kahju:** ründed serverist üle maailma, mille tulemusena oma teenuste blokkimine väljast, mainekahju

KOV maksis sotsiaaltoetust valele inimesele

- **Põhjus:** inimlik eksimus või pahatahlik rünne?
- **Kahju:** õigeaegsest toetusest ilmajäämine, oht inimese elule ja tervisele, võimalik kohtuvaidlus+kulud

KOV sai arve koostööpartnerilt ja maksis selle, kontrollimata üle partneri pangakonto numbri muutust

- **Põhjus:** protsesside puudulikkus (kontrollmehhanismi puudumine, tava puudumine) ja vähene riskihaldus
- **Kahju:** rahaline kahju

KOV sotsiaalmeedia konto paroolid peteti kasutajalt välja ja varastatati kogu konto koos 12tuh jälgijaga

- **Põhjus:** vähene teadlikkus, puudulik küberhügieen
- **Kahju:** mainekahju, uue identiteedi ja jälgijatega konto ülesehitamine vs lunavara nõue

Turvameetmed

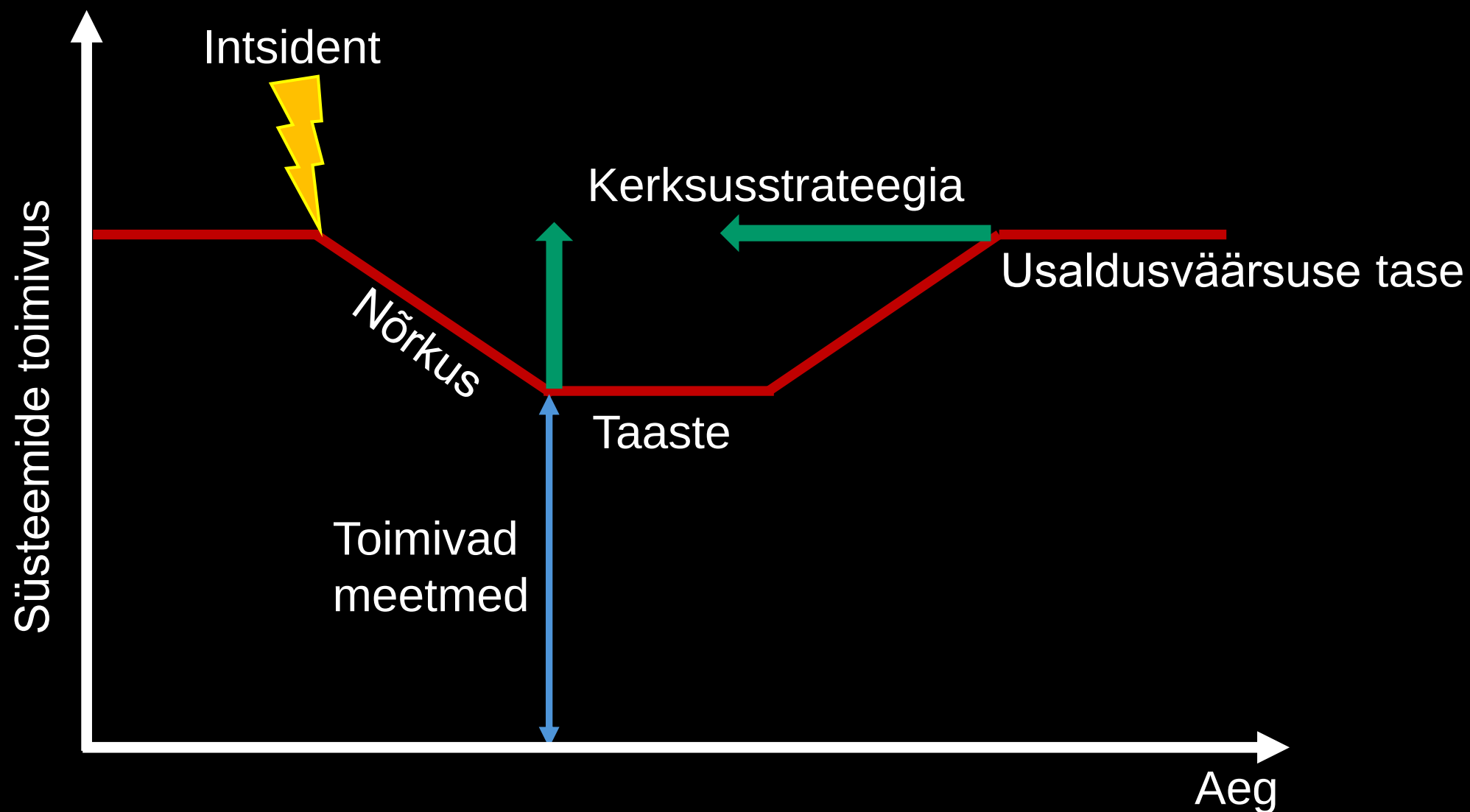
Abinõud riski muutmiseks:

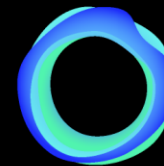
- Protsess - nt pääsuhood, logimine, seire
- Poliitika - nt personalipoliitika, nelja-silma-poliitika
- Vahend - nt VPN, spämmifilter, logiserver
- Tava - nt telefonikõned eraldi ruumis, tühi laud
- Muu toiming - nt lahkudes kustuta tuled ja sule aknad

- Tehniline
- Korralduslik
- Füüsiline
- Õiguslik

Aksepteerime riskid vs rakendamine turvameetmed

Kerksus (*resilience*)





E-ITS portal
<https://eits.ria.ee>



Eesti
Infoturbestandard

per

x

Q

Standardi versioon

2023



E-ITS põhidokumendid

E-ITS nõuded infoturbe
halduse süsteemile

Etalonturbe kataloog



ISMS. Turbehaldus



ORP. Organisatsioon ja
personal



CON. Kontseptsioonid ja
metoodikad



OPS. Käidutööd



DER. Avastamine ja
reageerimine



INF. Taristu



Eesti infoturbestandard tagab
avalike ülesannete täitmiseks
kasutatavate äriprotsesside ja
infosüsteemide kõikehõlmava
kaitse



Eesti infoturbestandardi põhidokumendid

E-ITS nõuded infoturbe halduse
süsteemile

Eesti infoturbestandardi peadokument, mis esitab
nõuded ning juhised organisatsiooni infoturbe
halduse süsteemile. Dokumendi lahutamatuks osaks
on E-ITSi etalonturbe kataloog.

E-ITSi 2023 aasta versioon allalaadimiseks:



[Meetmete kataloog 2023.xls](#)



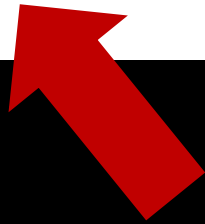
[Meetmete kataloog.pdf](#)

#	role	requirements	measures
1	Infoturbejuht	859	ISMS.1: Turbehaldus; ORP.1: Infoturbe korraldus; ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus; ORP.4: Identiteedi- ja õiguste haldus; ORP.5: Vastavusehaldus (nõuete haldus); OPS.1.2.4: Kaugtöö; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
2	Organisatsiooni juhtkond	290	ISMS.1: Turbehaldus; ORP.1: Infoturbe korraldus; ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus; ORP.4: Identiteedi- ja õiguste haldus; ORP.5: Vastavusehaldus (nõuete haldus); OPS.1.2.4: Kaugtöö; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
3	Ülemus	80	ISMS.1: Turbehaldus; ORP.2: Personal; ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus; ORP.5: Vastavusehaldus (nõuete haldus); OPS.1.2.4: Kaugtöö; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
4	Töötaja	118	ORP.1: Infoturbe korraldus; CON.3: Andmevarunduse kontseptsioon; CON.6: Andmete kustutus ja hävitamine; OPS.1.2.4: Kaugtöö; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
5	Haldusosakond	112	ORP.1: Infoturbe korraldus; ORP.4: Identiteedi- ja õiguste haldus; ORP.5: Vastavusehaldus (nõuete haldus); CON.6: Andmete kustutus ja hävitamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
6	IT-talitus	3683	ORP.1: Infoturbe korraldus; ORP.2: Personal; ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus; ORP.4: Identiteedi- ja õiguste haldus; CON.1: Krüptokontseptsioon; CON.3: Andmevarunduse kontseptsioon; CON.6: Andmete kustutus ja hävitamine; CON.8: Tarkvaraarendus; CON.9: Teabevahetus; OPS.1.1.4: Kaitse kahjurprogrammide kasutamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
7	Tehnikatalitus	565	ORP.1: Infoturbe korraldus; INF.1: Hoone üldiselt; INF.2: Serveriruum ja andmekeskus; INF.5: Tehnilise taristu ruum või kapp; INF.6: Andmekandjate arhiiv; INF.13: Hoonete tehniline seisund; OPS.1.1.4: Kaitse kahjurprogrammide kasutamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
8	Kasutaja	241	ORP.1: Infoturbe korraldus; ORP.4: Identiteedi- ja õiguste haldus; CON.7: Välislähetuste infoturve; CON.9: Teabevahetus; OPS.1.1.4: Kaitse kahjurprogrammide kasutamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
9	Personaliosakond	86	ORP.2: Personal; ORP.3: Infoturbe teadlikkuse tõstmine ja koolitus; CON.2: Isikuandmete kaitse; CON.7: Välislähetuste infoturve; OPS.1.1.2: IT-süsteemide kasutamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
10	Vastavushaldur	19	ORP.5: Vastavusehaldus (nõuete haldus); APP.3.2: Veebiserver
11	Vastutav spetsialist	571	CON.1: Krüptokontseptsioon; CON.3: Andmevarunduse kontseptsioon; CON.6: Andmete kustutus ja hävitamine; CON.8: Tarkvaraarendus; CON.9: Teabevahetus; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
12	Andmekaitse spetsialist	46	CON.2: Isikuandmete kaitse; CON.6: Andmete kustutus ja hävitamine; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
13	Testija	29	CON.2: Isikuandmete kaitse; CON.8: Tarkvaraarendus; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt
14	Hankeosakond	55	CON.6: Andmete kustutus ja hävitamine; OPS.2.3: Väljasttellimine; INF.1: Hoone üldiselt; INF.11: Sõidukite IT-komponendid; SYS.1.1: Server üldiselt; SYS.4.3: Sardisüsteemid (embedded systems); APP.4.3: Andmebaasisüsteemid
15	Arendaja	100	CON.8: Tarkvaraarendus; CON.10: Veebirakenduste arendus; SYS.4.3: Sardisüsteemid (embedded systems); APP.4.3: Andmebaasisüsteemid
16	Avariülem	60	OPS.2.3: Väljasttellimine; OPS.3.2: Teenuseandja infoturve; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
17	Auditirühm	50	DER.3.1: Auditid ja läbivaatused; DER.3.2: Infoturbe vastavusauditid
18	Infoturbe läbivaatuse rühm	32	DER.3.1: Auditid ja läbivaatused
19	Arhitekt	382	INF.1: Hoone üldiselt; INF.2: Serveriruum ja andmekeskus; INF.5: Tehnilise taristu ruum või kapp; INF.6: Andmekandjate arhiiv; INF.13: Hoonete tehniline seisund; OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt; OPS.2.2: Pilvteenuste kasutamine; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
20	Tuleohutusspetsialist	35	INF.1: Hoone üldiselt; INF.2: Serveriruum ja andmekeskus; INF.6: Andmekandjate arhiiv
21	Hooldepersonal	42	INF.2: Serveriruum ja andmekeskus; INF.5: Tehnilise taristu ruum või kapp; IND.2.1: Tööstusautomaatika komponendid üldiselt; IND.2.3: Andurid ja täiendavad komponendid; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus
22	Käidutehnoloogia talitus	208	IND.1: Käidu- ja protsessijuhtimissüsteemid; IND.2.1: Tööstusautomaatika komponendid üldiselt; IND.2.2: Programmeeritavad kontrollid; IND.2.3: Andurid ja täiendavad komponendid; DER.1: Turvaintsidentide käsitlemine; DER.2.1: Turvaintsidentide käsitlemine; DER.4: Avariialdus

Audit - kulu vői investeing?

E-ITS auditist, ISO sertifikaadist ja pilvandmetöötlustest teavitamine

Palume saata E-ITS auditite info, ISO/IEC 27001 sertifikaat või Vabariigi Valitsuse määrusest "Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel" (nn pilvemäärus) tulenevad teavitamised meiliaadressile kaustik@ria.ee.



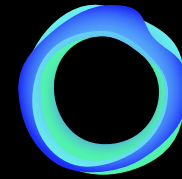
Juhi roll infoturbes

Eestvedu,
eeskuju ja
motivatsioon

Ressursid

Järelevalve

Rakenda E-ITSi asjakohased põhimeetmed eits.ria.ee – ca 200



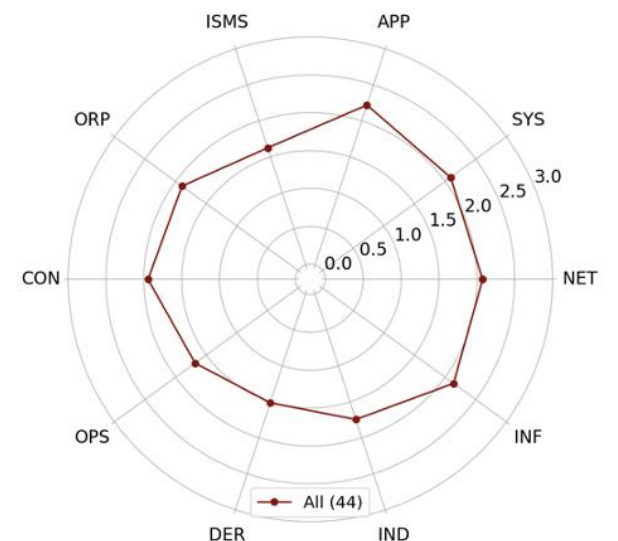
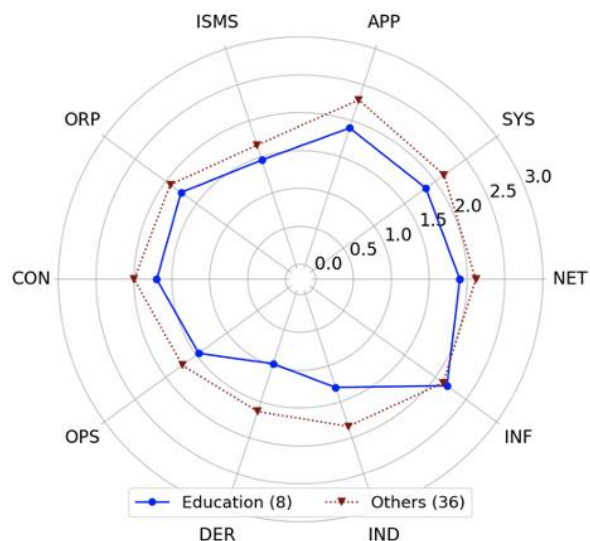
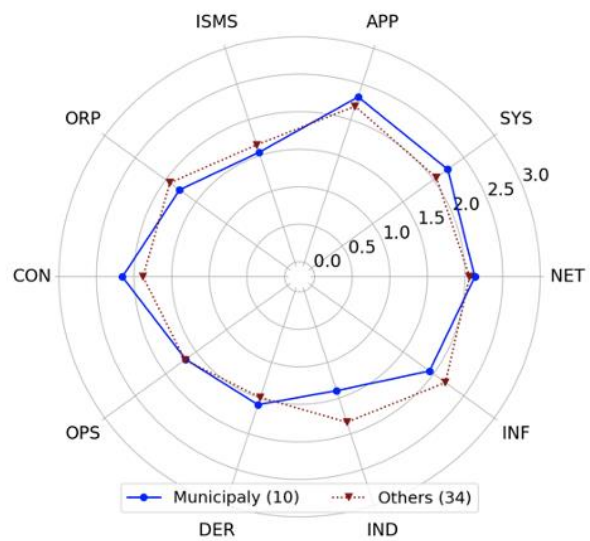
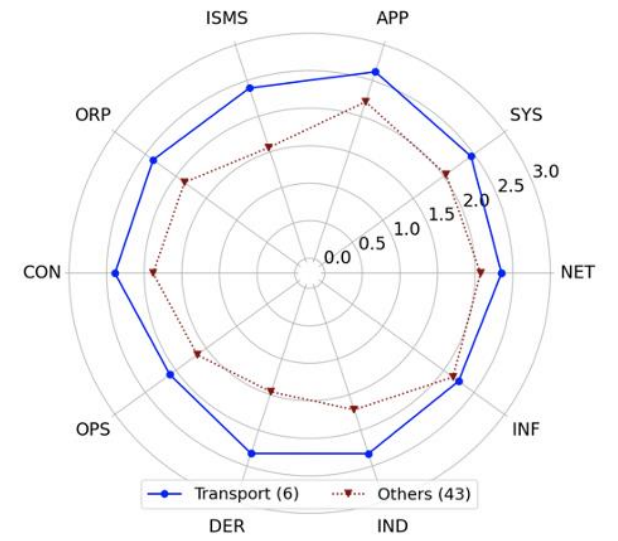
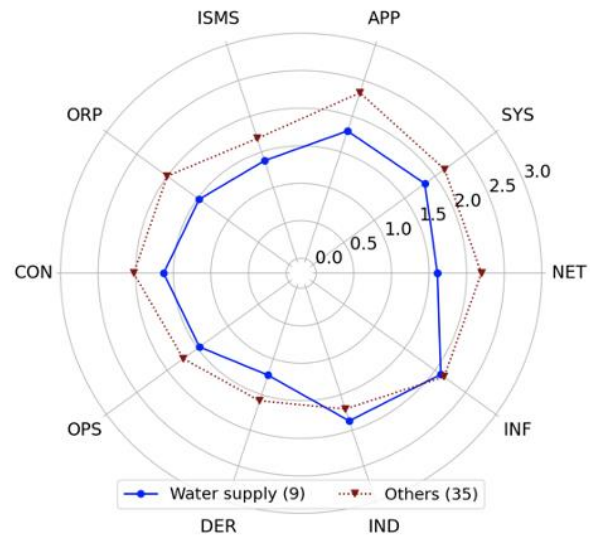
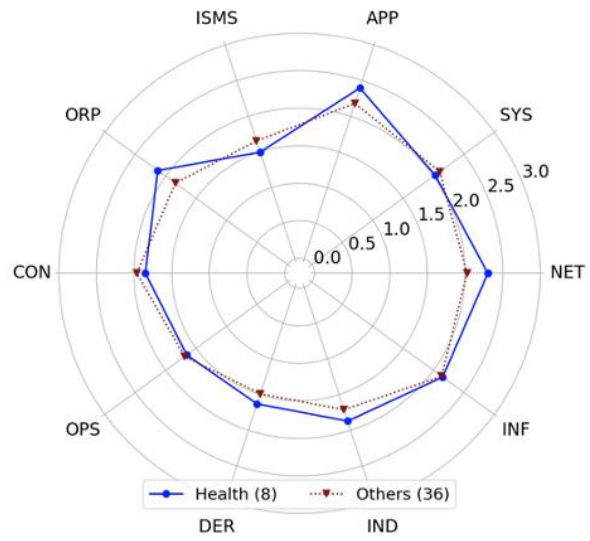
Eesti
Infoturbestandard

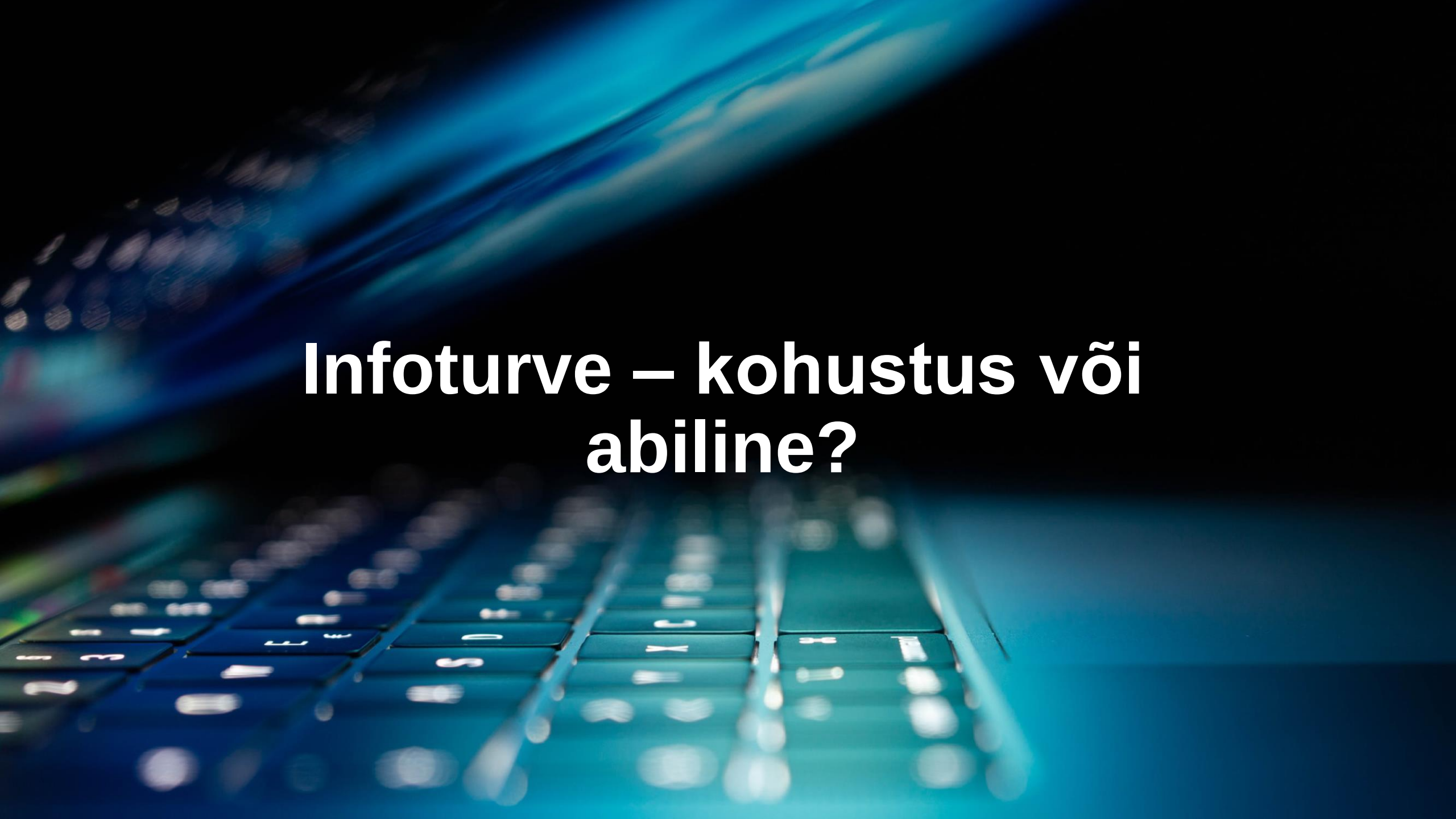
- Küberhügieen korda – kybertest.ee
- Uuendid – ole kiirem, kui ründaja!
- Kaitseala paika – tea kaitsetarvet ja enda kohustusi
- Tarneahela/partnerite turbe nõuded (SLA-d)
- Seire – “*Logs don’t lie!*”
- Intsidendihalduse protseduur



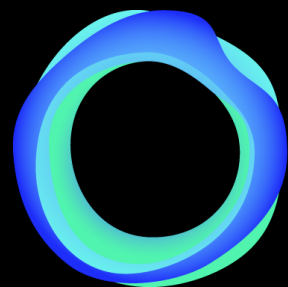
Oma olukorrale kiire hinnang 1-2h-ga:
TÜ tööriist <http://mass.cloud.ut.ee/massui/#!/>







**Infoturve – kohustus või
abiline?**



Eesti
Infoturbestandard

eits.ria.ee
standard@ria.ee