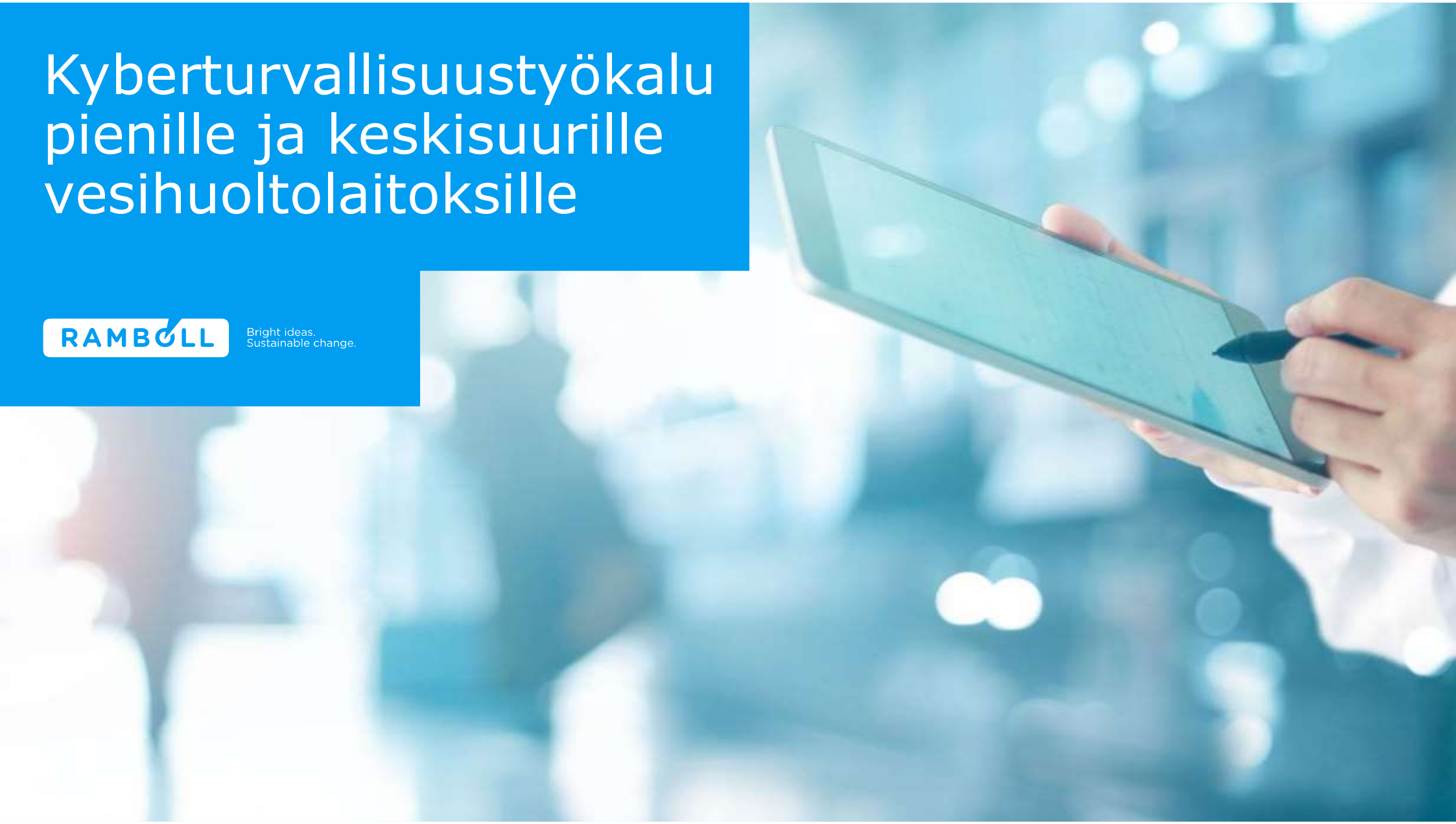
Kyberturvallisuustyökalu pienille ja keskisuurille vesihuoltolaitoksille

RAMBØLL

Bright ideas.
Sustainable change.



Miksi työkalua tarvitaan?

Tavoitteena parempi vesihuoltolaitosten kyberturvallisuuden tila

- Toiminnan systemaattisuuden parantaminen
- Dokumentoinnin parantaminen
- Kumppanuusverkon parempi hallinta

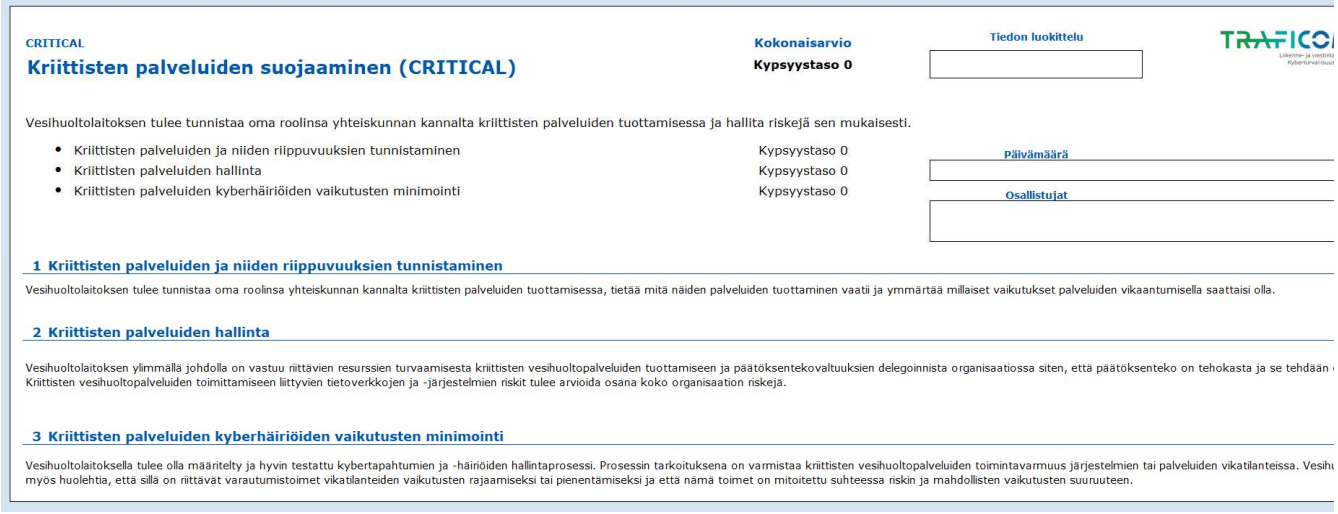
Kybermittarin käyttöä vesihuollossa testattu

- Hyödyllinen, mutta vaikeaselkoinen ja raskas työkalu
- Pienten vesihuoltolaitosten toiveena yksiselitteisempi ja rajatumpi työkalu

Kybermittari

- Kyberturvallisuuskeskus on kehittänyt Kybermittarin kyberturvallisuuden hallinnan tilan kartoittamiseen
- Excel-muotoinen työkalu
- Vapaasti saatavilla Kyberturvallisuuskeskuksen sivuilta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

- Haasteiksi Kybermittarin käytössä on tunnistettu
  - sovellettavien käytäntöjen laajuus
  - tietotekninen kieli
  - käytäntöjen kuvausten muotoilu
  - yleiset, kaikkia toimialoja koskevat käytäntöjen kuvaukset



CRITICAL

Kriittisten palveluiden suojaaminen (CRITICAL)

Kokonaisarvio
Kypsyystaso 0

Tiedon luokittelu

Vesihuoltolaitoksen tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja hallita riskejä sen mukaisesti.

- Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen — Kypsyystaso 0
- Kriittisten palveluiden hallinta — Kypsyystaso 0
- Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi — Kypsyystaso 0

Päivämäärä

Osallistujat

1 Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

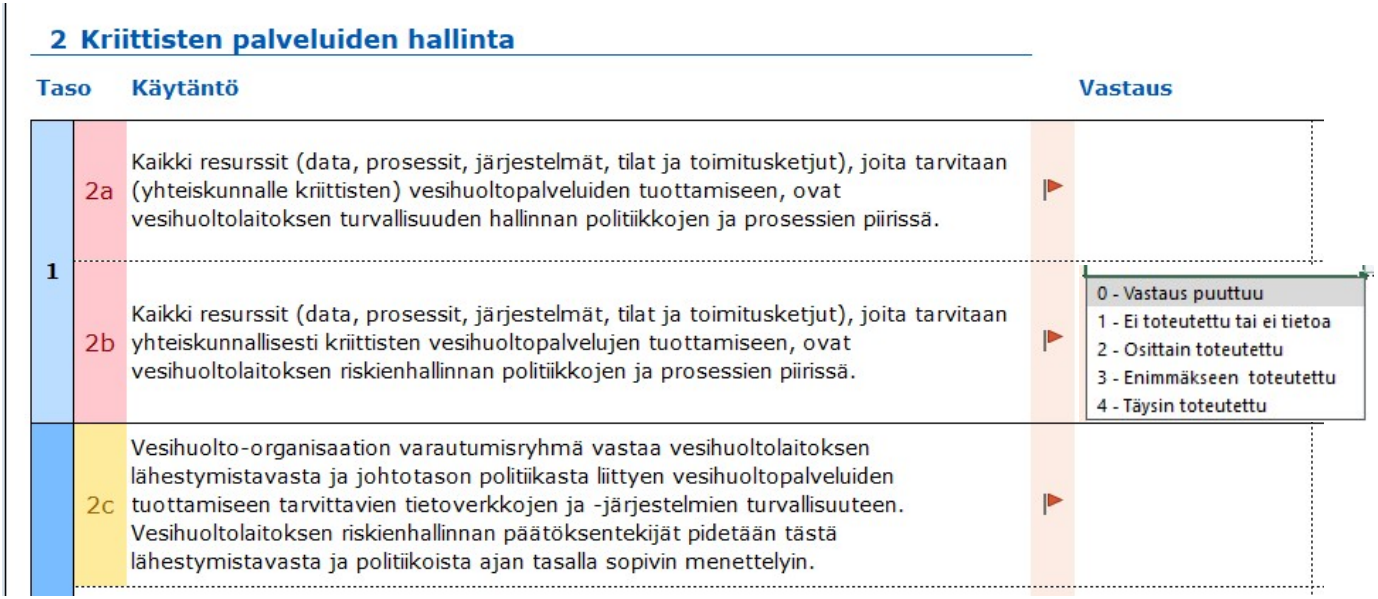
Vesihuoltolaitoksen tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa, tietää mitä näiden palveluiden tuottaminen vaatii ja ymmärtää millaiset vaikutukset palveluiden vikaantumisella saattaisi olla.

2 Kriittisten palveluiden hallinta

Vesihuoltolaitoksen ylimmällä johdolla on vastuu riittävien resurssien turvaamisesta kriittisten vesihuoltopalveluiden tuottamiseen ja päätöksentekovaltuuksien delegoinnista organisaatiossa siten, että päätöksenteko on tehokasta ja se tehdään
Kriittisten vesihuoltopalveluiden toimittamiseen liittyvien tietoverkkojen ja -järjestelmien riskit tulee arvioida osana koko organisaation riskejä.

3 Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

Vesihuoltolaitoksella tulee olla määritelty ja hyvin testattu kybertapahtumien ja -häiriöiden hallintaprosessi. Prosessin tarkoituksena on varmistaa kriittisten vesihuoltopalveluiden toimintavarmuus järjestelmien tai palveluiden vikatilanteissa. Vesihu
myös huolehtia, että sillä on riittävät varautumistoimet vikatilanteiden vaikutusten rajaamiseksi tai pienentämiseksi ja että nämä toimet on mitoitettu suhteessa riskin ja mahdollisten vaikutusten suuruuteen.



2 Kriittisten palveluiden hallinta

Taso		Käytäntö	Vastaus
1	2a	Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan (yhteiskunnalle kriittisten) vesihuoltopalveluiden tuottamiseen, ovat vesihuoltolaitoksen turvallisuuden hallinnan politiikkojen ja prosessien piirissä.	
	2b	Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan yhteiskunnallisesti kriittisten vesihuoltopalvelujen tuottamiseen, ovat vesihuoltolaitoksen riskienhallinnan politiikkojen ja prosessien piirissä.	0 - Vastaus puuttuu 1 - Ei toteutettu tai ei tietoa 2 - Osittain toteutettu 3 - Enimmäkseen toteutettu 4 - Täysin toteutettu
	2c	Vesihuolto-organisaation varautumisryhmä vastaa vesihuoltolaitoksen lähestymistavasta ja johtotason politiikasta liittyen vesihuoltopalveluiden tuottamiseen tarvittavien tietoverkkojen ja -järjestelmien turvallisuuteen. Vesihuoltolaitoksen riskienhallinnan päätöksentekijät pidetään tästä lähestymistavasta ja politiikoista ajan tasalla sopivin menettelyin.	

Tavoitteena helppokäyttöinen työkalu

- Tavoitteena oli, että työkalua on vesihuollon edustajien helppo käyttää
  - Kun vesihuoltolaitos käyttää työkalua, mukana arviointitilanteessa täytyy silti aina olla myös kunnan tai palveluntarjoajan ICT-henkilö
- PIKSU-projektissa muokattiin Kybermittarista versio pienille ja keskisuurille vesihuoltolaitoksille
  - käsiteltävien kohtien määrän rajaus 66:een - kypsyystason 1 kohdat
  - enemmän taustatietoja ja lisätietoja
  - kytkeminen muuhun vesihuoltolaitoksen toimintaan

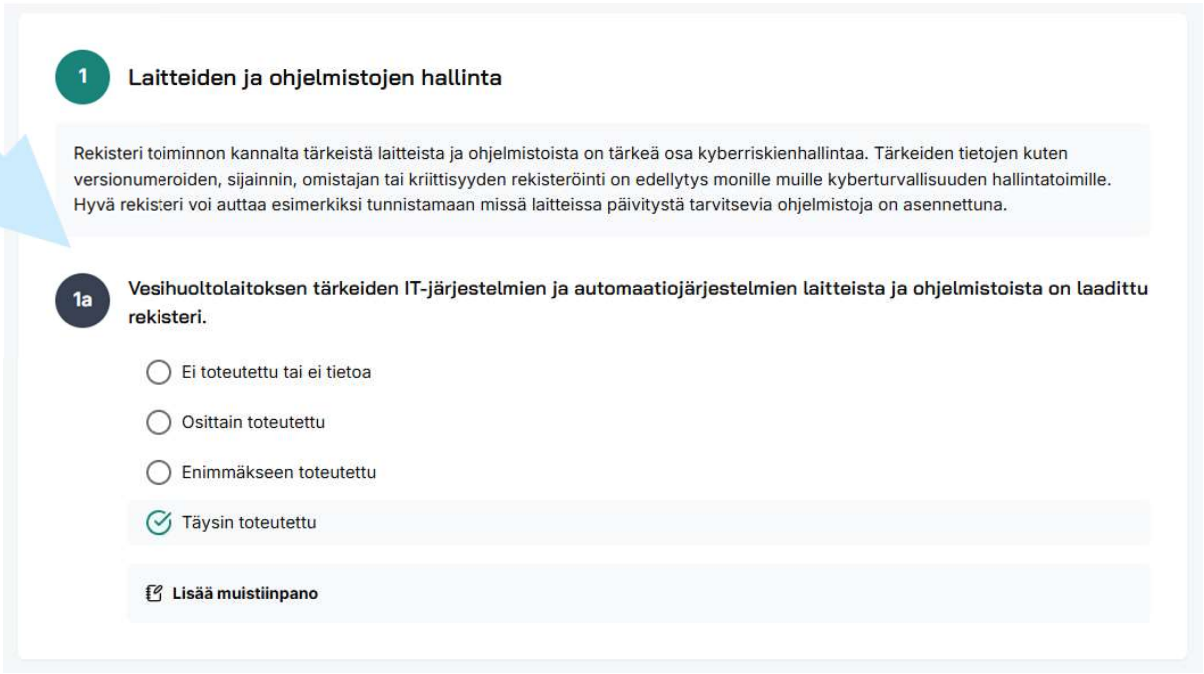
- Projektin rahoittivat Etelä-Savon ELY-keskus (/MMM), Vesihuoltolaitosten kehittämisrahasto, vesihuoltolaitokset ja Ramboll

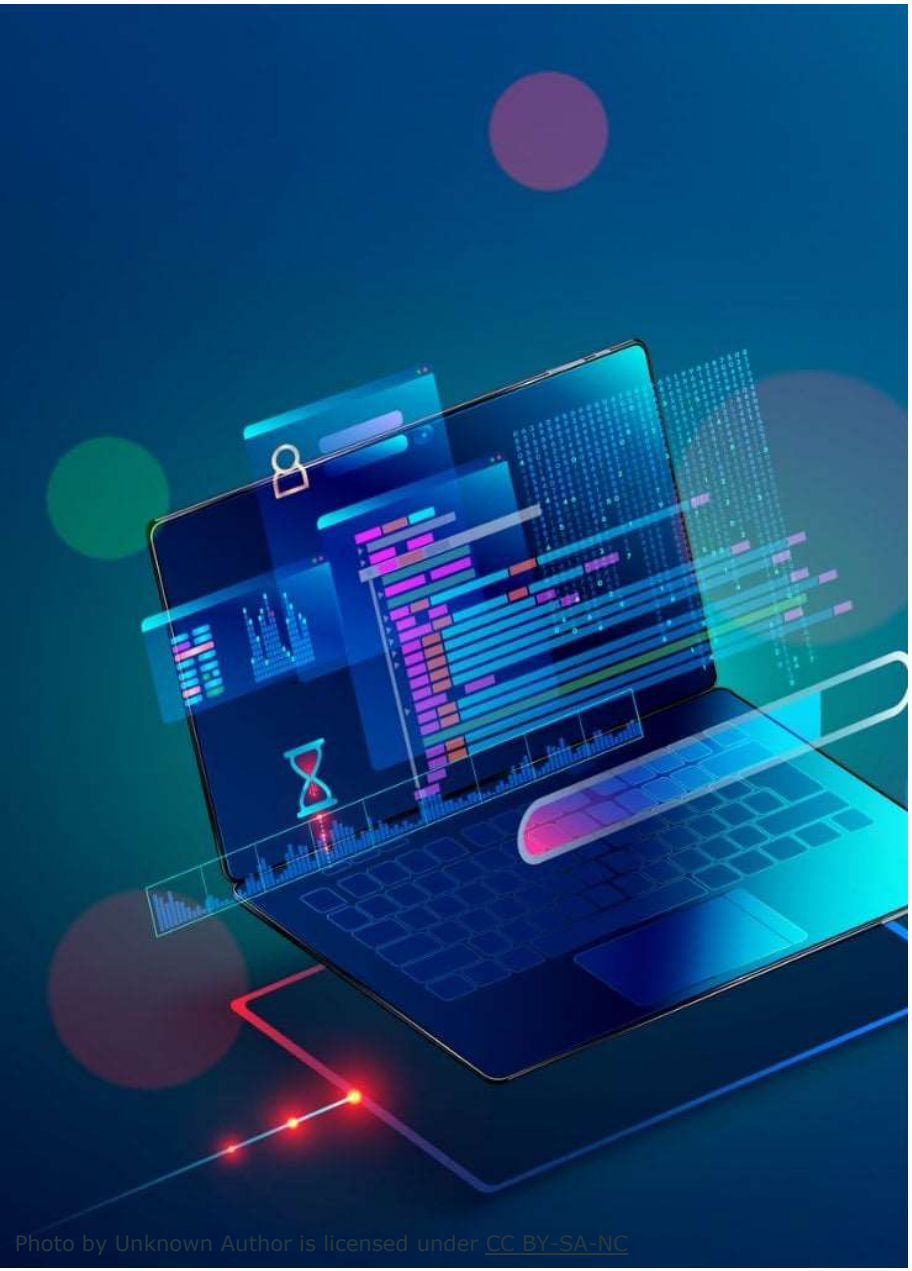
Kyberturvallisuuden hallinta tarkoittaa paitsi teknisiä ratkaisuja, myös sitä tapaa, jolla vesihuoltolaitos varmistaa, että asiat ovat kunnossa

Esimerkki muokkauksista

1 Laitteiden ja ohjelmistojen hallinta

Taso	Käytäntö	Vastaus
1	1a Toiminnon kannalta tärkeistä laitteista ja ohjelmistoista on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen laitteet ja ohjelmistot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.	

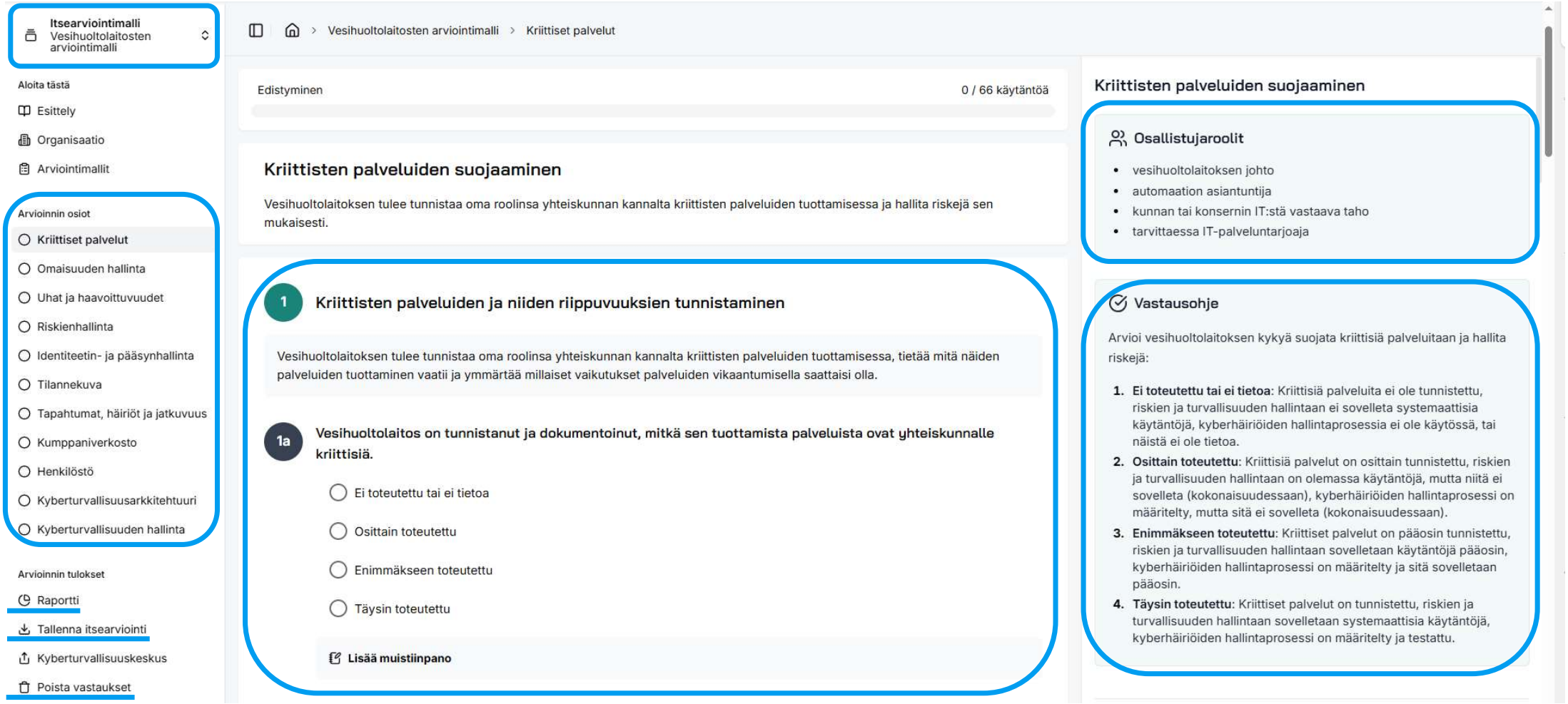




Työkalun toteutus

- Työkalu valmistui 4/2025
- Käyttöliittymää kehitetty yhdessä SAMK:n RoboAI Cyberlab:n kanssa
  - ➢ Selainpohjainen versio Kybermittarista
- Työkalun jakelukanavaksi tullee Kyberturvallisuuskeskuksen sivut
  - Samoin kuin alkuperäisen Kybermittarin jakelu

https://cyberlab-self-assessment-tool.roboai.fi/intro => Valitse vasemmalta ”Itsearviointimalli”-valikosta ”Vesihuoltolaitosten arviointimalli


Itsearviointimalli
Vesihuoltolaitosten arviointimalli
Aloita tästä
Esittely
Organisaatio
Arviointimallit
Arvioinnin osiot
Kriittiset palvelut
Omaisuuden hallinta
Uhat ja haavoittuvuudet
Riskienhallinta
Identiteetin- ja pääsynhallinta
Tilannekuva
Tapahtumat, häiriöt ja jatkuvuus
Kumppaniverkosto
Henkilöstö
Kyberturvallisuusarkkitehtuuri
Kyberturvallisuuden hallinta
Arvioinnin tulokset
Raportti
Tallenna itsearviointi
Kyberturvallisuuskeskus
Poista vastaukset
Vesihuoltolaitosten arviointimalli
Kriittiset palvelut
Edistyminen
0 / 66 käytäntöä
Kriittisten palveluiden suojaaminen
Vesihuoltolaitoksen tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja hallita riskejä sen mukaisesti.
1
Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
Vesihuoltolaitoksen tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa, tietää mitä näiden palveluiden tuottaminen vaatii ja ymmärtää millaiset vaikutukset palveluiden vikaantumisella saattaisi olla.
1a
Vesihuoltolaitos on tunnistanut ja dokumentoinut, mitkä sen tuottamista palveluista ovat yhteiskunnalle kriittisiä.
Ei toteutettu tai ei tietoa
Osittain toteutettu
Enimmäkseen toteutettu
Täysin toteutettu
Lisää muistiinpano
Kriittisten palveluiden suojaaminen
Osallistujaroolit
vesihuoltolaitoksen johto
automaation asiantuntija
kunnan tai konsernin IT:stä vastaava taho
tarvittaessa IT-palveluntarjoaja
Vastausohje
Arvioi vesihuoltolaitoksen kykyä suojata kriittisiä palveluitaan ja hallita riskejä:
1. Ei toteutettu tai ei tietoa: Kriittisiä palveluita ei ole tunnistettu, riskien ja turvallisuuden hallintaan ei sovelleta systemaattisia käytäntöjä, kyberhäiriöiden hallintaprosessia ei ole käytössä, tai näistä ei ole tietoa.
2. Osittain toteutettu: Kriittisiä palvelut on osittain tunnistettu, riskien ja turvallisuuden hallintaan on olemassa käytäntöjä, mutta niitä ei sovelleta (kokonaisuudessaan), kyberhäiriöiden hallintaprosessi on määritelty, mutta sitä ei sovelleta (kokonaisuudessaan).
3. Enimmäkseen toteutettu: Kriittiset palvelut on pääosin tunnistettu, riskien ja turvallisuuden hallintaan sovelletaan käytäntöjä pääosin, kyberhäiriöiden hallintaprosessi on määritelty ja sitä sovelletaan pääosin.
4. Täysin toteutettu: Kriittiset palvelut on tunnistettu, riskien ja turvallisuuden hallintaan sovelletaan systemaattisia käytäntöjä, kyberhäiriöiden hallintaprosessi on määritelty ja testattu.

1a Vesihuoltolaitoksen tärkeiden IT-järjestelmien ja automaatiojärjestelmien laitteista ja ohjelmistoista on laadittu rekisteri.

Kysymys

Onko vesihuoltolaitoksella käytössä rekisteri, johon on kirjattu toiminnan kannalta tärkeät IT- ja automaatiolaitteet ja -ohjelmistot?

Vastausohjeet

Rekisteri voi yksinkertaisimmillaan koostua esimerkiksi useasta Excel-listauksesta. Laite tai ohjelmisto on tärkeä, mikäli sen rikkoutuminen tai poissa käytöstä olo vaikuttaa merkittävästi vesihuoltopalveluiden tuottamiseen. Tärkeiden laitteiden ja ohjelmistojen tunnistamiseen voi hyödyntää kriittisen **datan**, **prosessien** ja **järjestelmien** tunnistamista käsittelevien kohtien listauksia. Rekisterin on suositeltavaa sisältää esimerkiksi verkkolaitteet, työasemat, ohjelmistot, puhelimet, tabletit sekä pumput ja muut toiminnan jatkuvuuden kannalta keskeiset laitteet.

2a Vesihuoltolaitos on tunnistanut tietolähteitä, joiden avulla se voi tunnistaa toimintaansa kohdistuvia uhkia.

Kysymys

Onko vesihuoltolaitos tunnistanut, mitä tietolähteitä voi hyödyntää uhkien tunnistamiseksi?

Vastausohjeet

Tällaisia tietolähteitä ovat esimerkiksi Vesihuoltopoolin, valvovan viranomaisen, Supon ja Kyberturvallisuuskeskuksen tiedotteet, Kyberturvallisuuskeskuksen uutiskooste ja viikkoraportti, automaatiotoimittajan haavoittuvuustiedotteet, Microsoftin tiedotteet, sekä vesihuoltolaitoksen tärkeimpien järjestelmien toimittajien tiedotteet.

1a Vesihuoltolaitoksen työntekijöille ja muille entiteeteille osoitetaan erilliset identiteetit.

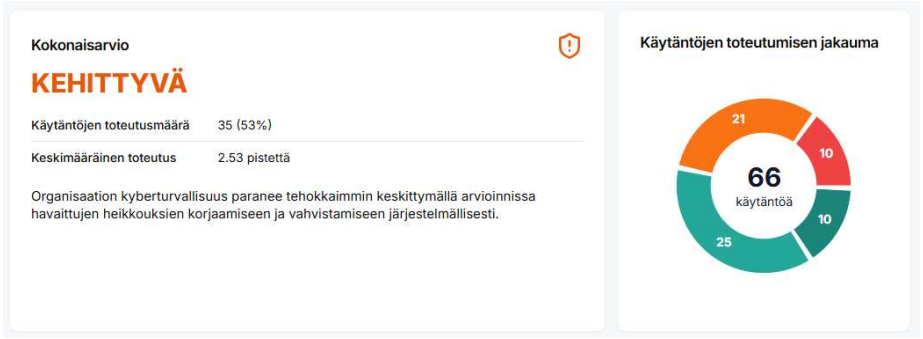
Kysymys

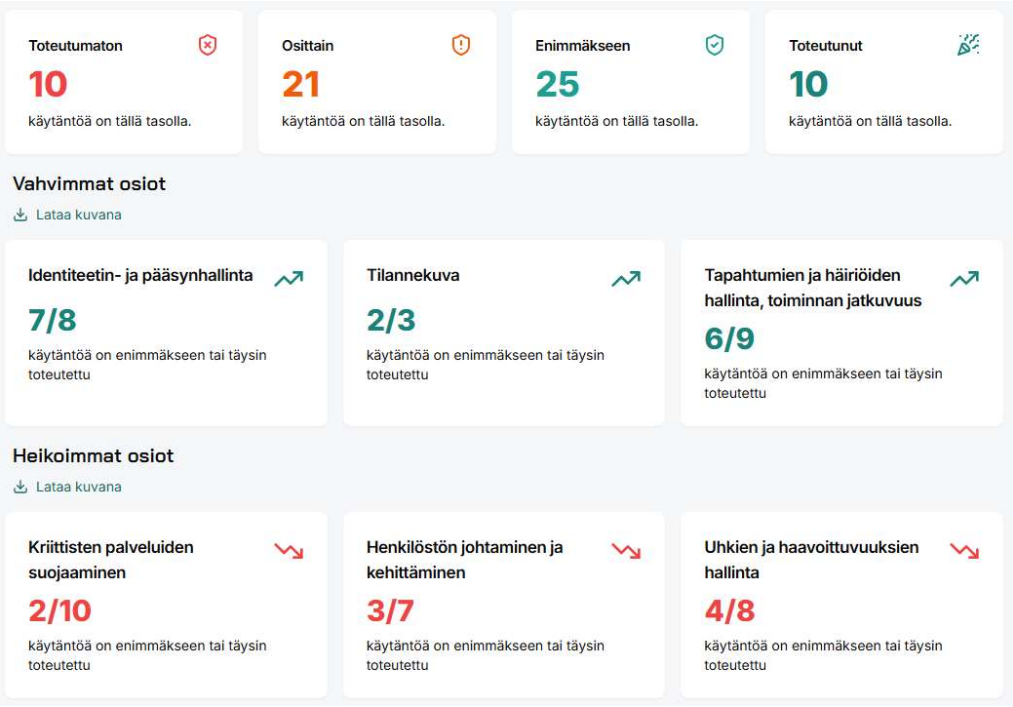
Onko vesihuoltolaitoksella määritelty yksilölliset identiteetit kaikille käyttäjille, laitteille ja prosesseille?

Vastausohjeet

Muilla entiteeteillä tarkoitetaan prosesseja ja laitteita, jotka tarvitsevat pääsyn toiminnan kannalta tärkeisiin laitteisiin, ohjelmistoihin tai tietovarantoihin. Identiteetillä tarkoitetaan käyttäjätunnuksia ja laitetunnuksia. Erillisillä identiteeteillä tarkoitetaan, ettei yhteiskäyttötunnuksia käytetä. Erillisillä identiteeteillä hallitaan sitä, kuka pääsee käsiksi mihinkin järjestelmään tai tietoihin.

Kartoituksesta tieto kehityskohteista





Tunniste	Vastaus	Käytäntö
critical-1a	2	Vesihuoltolaitos on tunnistanut ja dokumentoinut, mitkä sen tuottamista palveluista ovat yhteiskunnalle kriittisiä.
critical-1c	3	Vesihuoltolaitos on tunnistanut ja dokumentoinut prosessit, joita se tarvitsee vesihuoltopalveluiden tuottamiseen.
critical-1d	3	Vesihuoltolaitos on tunnistanut ja dokumentoinut, mitä järjestelmiä ja varajärjestelmiä se tarvitsee vesihuoltopalveluiden tuottamiseen.
critical-1b	2	Vesihuoltolaitos on tunnistanut ja dokumentoinut tiedot, joita se tarvitsee kriittisten vesihuoltopalveluiden tuottamiseen. Lisäksi vesihuoltolaitos on luokitellut tiedot niiden turvallisuustason perusteella.
critical-2a	1	Vesihuoltolaitoksen turvallisuuden hallinnan periaatteissa ja toimintatavoissa on huomioitu kaikki yhteiskunnalle kriittisten vesihuoltopalveluiden tuottamiseen tarvittavat resurssit.
critical-2b	1	Vesihuoltolaitoksen riskienhallinnan periaatteissa ja toimintatavoissa on huomioitu kaikki yhteiskunnalle kriittisten vesihuoltopalveluiden tuottamiseen tarvittavat resurssit.
critical-3a	2	Vesihuoltolaitoksella on kybertapahtumien ja -poikkeamien hallintasuunnitelma, joka kattaa kaikki kriittiset vesihuoltopalvelut.
critical-3b	1	Hallintasuunnitelma keskittyy tunnettuihin hyökkäystyyppeihin ja käsittelee yksityiskohtaisesti kyseisten hyökkäysten mahdollisia seurauksia.