Traffic Light Protocol (TLP)

TLP: RED
Henkilö ei saa luovuttaa tietoa edelleen edes tiedonvaihtoryhmän tai oman organisaationsa sisällä. "Vain sinun silmillesi".

TLP: AMBER+STRICT
Tieto voidaan jakaa vain vastaanottaneelle organisaatiolle ja ”yksilöity tarve tietää” periaatteella.

TLP: AMBER
Tieto voidaan jakaa muille tiedonvaihtoryhmän jäsenille, organisaation sisäisesti sekä sidosryhmissä toimenpiteisiin ryhtymiseksi välttämättömille henkilöille. "Yksilöity tarve tietää".

TLP: GREEN
Tieto voidaan jakaa vapaasti organisaation sisällä ja kumppaneille tai tiedon kontekstiin liittyvälle yhteisölle tai sektorille. **Tietoa ei saa kuitenkaan julkaista** esimerkiksi Internetissä.

TLP: CLEAR
Tieto voidaan jakaa pakottavasta lainsäädännöstä johtuvat rajoitukset huomioiden vapaasti.

Chatham House -sääntö

Chatham House -säännön perusajatuksena on, että kun sääntö on käytössä kokouksessa voivat sen osallistujat hyödyntää saamiaan tietoja edelleen, mutta eivät voi paljastaa tiedon antajaa, hänen organisaatiotaan tai muiden kokoukseen osallistujien identiteettiä. Säännön tarkoituksena on kannustaa avoimuuteen ja tietojen jakamiseen antamalla osanottajille takuu siitä, että lausunnon antajan lähde ei paljastu.

TRAFICOM

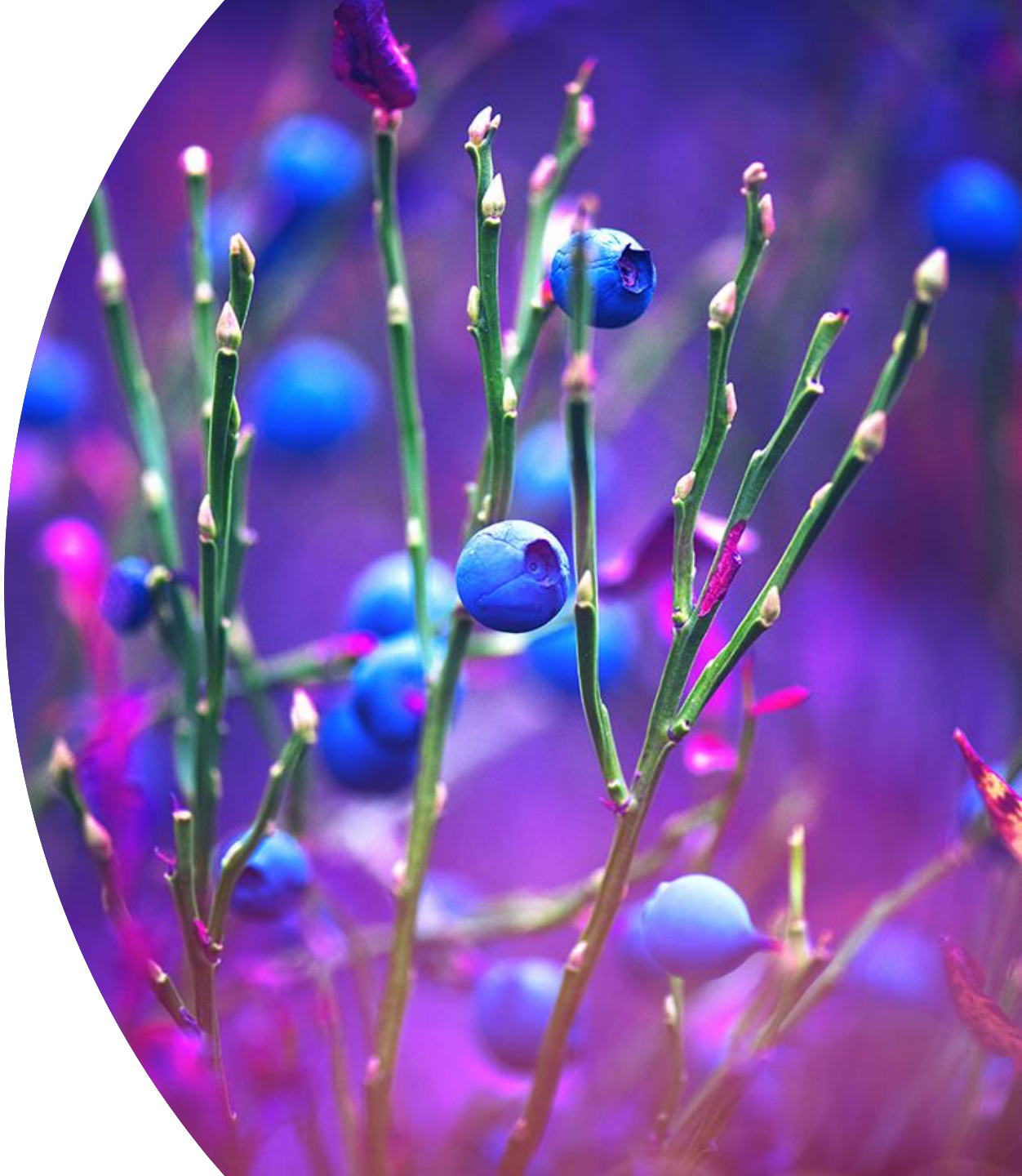
TLP:CLEAR

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari esittely palveluntarjoajille

13.6.2023



Kyberturvallisuus on...

- **tavoitetila**, jossa **kybertoimintaympäristöön** eli koko nykyiseen verkottuneeseen digitaaliseen yhteiskuntaamme **voidaan luottaa** ja jossa sen **toiminta turvataan.**

TLP:CLEAR

Kyberturvallisuuskeskus –tammikuun kybersää

”Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista”.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Tärkein tietoturvateko on tiedostaa, mikä on yrityksen nykyinen tietoturvallisuuden taso. Mitä tulisi kehittää? Tämän jälkeen pitäisi myös viedä läpi tarvittavat kehitystoimet.

Organisaation tietoturvaohjelma

- Organisaatiossa tulisi hyödyntää erilaisia kyberturvallisuuden viitekehyksiä
  - Riskienhallinta
  - Tietoturvallisuuden hallinta
  - Tietoturvakontrollit
  - Liiketoiminta-arkkitehtuuri
- Kypsyysmalli auttaa seuraamaan ja todentamaan organisaation tietoturvaohjelman etenemistä ja asetettujen tavoitteiden saavuttamista
  - Tässä mm. Kybermittari voi auttaa

Kyberriskien 10 lakia

Onnistuminen tietoturvassa syö hyökkääjän voittoja
Täydellistä tietoturvaa on mahdoton saavuttaa, joten vaikeuta hyökkääjän toimintaa ja lisää heidän kustannuksiaan ja vähennän oman suojattavan omaisuuden kiinnostavuutta.

Kyberturvallisuus on joukkuepeli
Kukaan ei pysty tekemään kaikkea yksin. Keskity niihin tehtäviin, jotka juuri sinä voit tehdä suojataksesi organisaation tehtäviä ja anna muiden tehdä muut tehtävät.

Jos et pidä yllä, jäät jälkeen
Kyberturvallisuus on jatkuva prosessi ja kokoajan tulee liikkua eteenpäin. Hyökkäysten toteuttaminen käy koko ajan hyökkääjille edullisemmaksi.

Verkkosi ei ole niin turvallinen kuin luulet
Turvallisuusstrategia, joka nojaa luottamukseen on helposti hyökkääjien murrettavissa. Noudata organisaatiossa nollaluottamusajattelua.

Tuottavuus voittaa aina
Jos tietoturva ei ole helppoa käyttäjille, he keksivät tavan ohittaa sen. Muista aina käytettävyys turvallisuuden ohella.

Eristetyt verkot eivät ole automaattisesti turvallisia
Kunnolla eristetyt verkot voivat oikein hallittuina tarjota korkeaa tietoturvaa, mutta usein verkko ei ole täysin eristetty ulkoisilta riskeiltä.

Hyökkääjät eivät välitä
Hyökkääjät käyttävät mitä tahansa saatavilla olevia menetelmiä päästääkseen organisaatiosi ympäristöön ja tietoihin.

Salaus yksinään ei ole tiedon suojauksen ratkaisu
Salaus suojaa tietyn tyyppisiltä hyökkäyksiltä, mutta data on vain niin turvassa kuin salausavain ja muut pääsynhallinnan käytännöt sitä suojaavat.

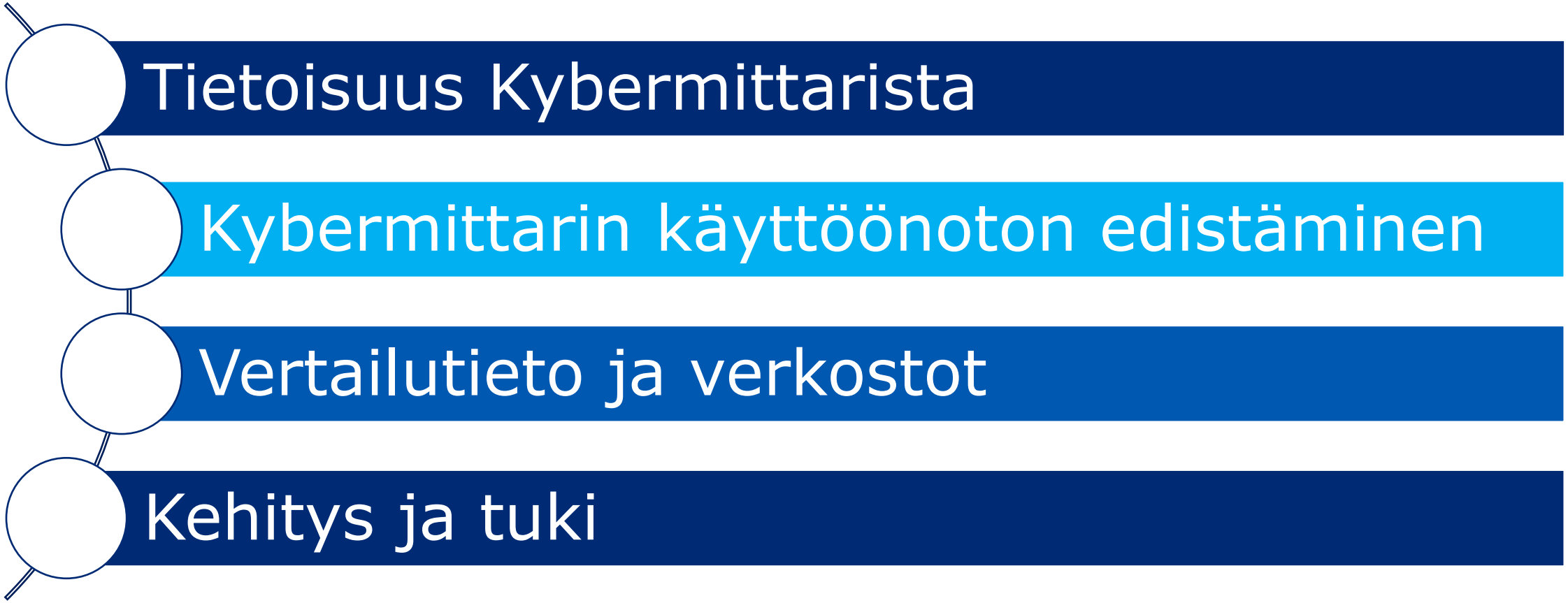
Ankara priorisointi on selviytymiskeino
Kenelläkään ei ole riittävästi aikaa ja resursseja päästäkseen eroon kaikista riskeistä, joten aloita aina siitä, mikä organisaatiollesi on tärkeintä (”kruununjalokivet”).

Teknologia ei ratkaise ihmis- ja prosessiongelmia
Edistyneet teknologiat, kuten tekoäly ja koneoppiminen tarjoavat suuria harppauksia eteenpäin, kyberturvallisuus on yhteiskunnallinen ja ihmisiin liittyvä haaste.

Kybermittari

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2023->
Pääteemat



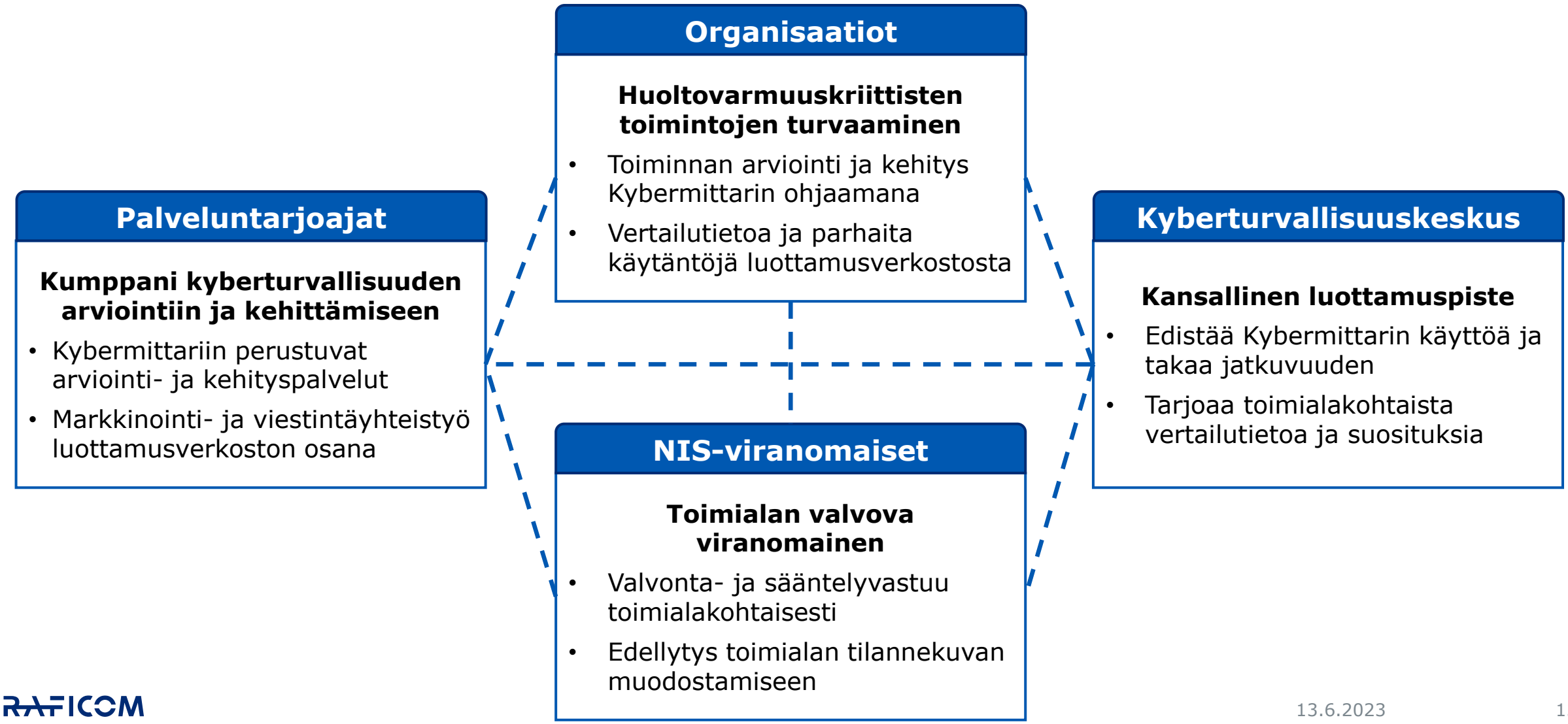
Ilmainen Kybermittari sisältää hyviä käytäntöjä riskien hallintakeinoiksi

- **Kybermittari** on organisaatioiden johdolle ja tietoturva-ammattilaisille suunnattu **ilmainen** palvelu kyberturvallisuuden hallintaan.
- Arviointityökalun avulla organisaatio **mittaa kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla**. Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat **kehitysalueet**.
- Organisaatio voi halutessaan jakaa mittaustuloksensa Kyberturvallisuuskeskukselle, joka anonymisoi tulokset ja tarjoaa organisaatiolle niiden pohjalta tuotettua **toimialan vertailutietoa ja suosituksia**.
- Tutustu kybermittariin: www.kybermittari.fi
- Ota yhteyttä: kybermittari@traficom.fi

Kybermittari-palvelun tarkoitus

- Onko organisaatiollanne ymmärrys, **millainen kyberkyvykkyys teillä on suojautua kyberuhilta** ja varmistaa liiketoimintanne **jatkuvuus** häiriötilanteissa?
  - Kybermittari auttaa
    - **johtamaan** kyberturvallisuutta sekä auttaa henkilöstöä **yhteisen ymmärryksen saavuttamisessa ja kehittämään** toimintaa.
    - Arvioimaan **säännöllisesti** ja systemaattisesti kyberkyvykkyyttänne eri osa-alueilla **englannin**, **suomen tai ruotsin** kielellä.
    - ***tunnistamaan kehityskohteita****, asettamaan* ***tavoitetason*** *ja* ***investoimaan*** *oikeisiin asioihin.*
- Kybermittari antaa myös **vertailutietoa ja helpottaa yhteistyötä sekä tiedonjakoa** verkostoissa ja sidosryhmien kanssa.
  - Kerätty vertailutieto auttaa myös **kansallisen tilannekuvan muodostamisessa** ja investointien kohdentamisessa.

Kybermittarin luottamusverkosto



Kyberturvallisuuskeskuksen rooli kansallisena luottamuspisteenä

Puolueeton kumppani

Viranomaisrooli mittarin käytön tukemissa ja edistämisessä

- Kyberturvallisuuskeskus tarjoaa mittarin vapaasti käytettäväksi
- Edistää mittarin käyttöönottoa ja käyttöä verkostojensa kautta
- Tarjoaa neuvoja ja suosituksia
- Ylläpitää ja kehittää mittaria

Kansallinen luottamuspiste

Mittaustulosten koonti, säilytys ja anonymisointi

- Kyberturvallisuuskeskus kerää organisaatioilta mittaustuloksia
- Luottamuksellinen tiedonkäsittely ja tulosten anonymisointi
- Pohjana vertailutiedolle ja KTK:n tarjoamille suositustasoille

Anonyymi vertailutieto

Toimialakohtaisen vertailutiedon tarjoaminen

- Kyberturvallisuuskeskus tuottaa mittaustuloksista anonymisoitua toimialakohtaista vertailutietoa
- Lisäksi tuloksiin pohjautuvia suositustasoja ja ohjeistusta
- Jakelu suoraan osallistuville asiakasorganisaatioille

Kybermittari palveluntarjoajille

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari palveluntarjoajille

- Palveluntarjoajilla on keskeinen rooli Kybermittarin käytössä ja organisaatioiden kyberturvallisuuden edistämisessä

- Kyberturvallisuuskeskus haluaa tehdä yhteistyötä palveluntarjoajien kanssa
  - Tarjoamalla Kybermittarin ja sen materiaalit **vapaasti käytettäväksi, soveltuvin ehdoin**
  - **Viestintäyhteistyötä**
  - **Rajattua tuotetukea** kipukohtien ratkaisemiseksi
  - **Yhteistyötä ja vaikuttamismahdollisuuksia Kybermittarin kehitykseen**

Esimerkki Kybermittarin arviointiprosessista

Perustuen Kyberturvallisuuskeskuksen 2020-22 toteuttamiin pilottiarvointeihin

ITSEARVIOINTI	HAASTATTELU	TULOSTEN RAPORTOINTI

Organisaatio

Vastuuhenkilöiden nimeäminen	Vastausten täydentäminen	½ päivän työpaja	Raportointi johdolle

Arvioinnin fasilitoija

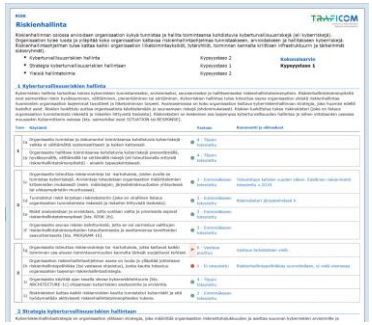
Valmistelu	Tuki, tarvittaessa	½ päivän työpaja	Loppuraportti

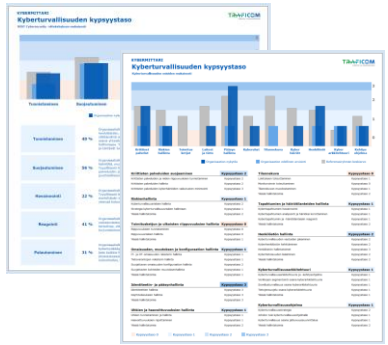
Esimerkki rooleista ja vastuista

Organisaatio nimeää vastuualueiden edustajat vastaamaan mittarin arviointikysymyksiin. Fasilitoija valmistelee ja aikatauluttaa arvioinnin ja tukee tarvittaessa vastausten tulkinnassa.	Yhteistyöpaja, jossa käydään läpi ja täydennetään organisaation täyttämät vastaukset. Tässä vaiheessa voidaan jo käydä läpi tärkeimpiä kehitysalueita.	Fasilitoija analysoi tulokset ja valmistelee loppuraportin, jota organisaatio voi käyttää raportointiin ja kehitystoiminnan ohjaamiseen.

Kybermittarin ja materiaalien käytön ehdot

- Kyberturvallisuuskeskus tarjoaa valmiin materiaalipaketin
  - Kybermittarin arviointityökalu, käyttöohjeet, valmiit raportit ja muu tukimateriaali





- Kybermittari on Kyberturvallisuuskeskuksen omistama tavaramerkki (PRH, Rno: 279095)
- Kybermittarin materiaalin lisensointia tarkennetaan Creative Commons Nimeä 4.0 -lisenssiksi (CC BY 4.0)

Kybermittarin käytön ehdot, tarkemmin

- Cybersecurity Capability Maturity Model (C2M2) ehdot:

© 2022 Carnegie Mellon University. This version of C2M2 is being released and maintained by the U.S. Department of Energy (DOE). ***The U.S. Government has, at minimum, unlimited rights to use, modify, reproduce, release, perform, display, or disclose this version the C2M2 or corresponding tools provided by DOE, as well as the right to authorize others, and hereby authorizes others, to do the same****.*

During the creation of the original C2M2, Capability Maturity Model® and CMM® were registered trademarks of Carnegie Mellon University. Information Systems Audit and Control Association, Inc. (ISACA) is the current owner of these marks but did not participate in the creation of C2M2.

- Kybermittarin ehdot:

1. *”Kybermittari” on Kyberturvallisuuskeskuksen omistama tavaramerkki (sanamerkki) (PRH, Rno: 279095)*

2. *Kybermittariin liittyvä materiaali on julkaistu* ***Creative Commons Nimeä 4.0 -lisenssillä (CC BY 4.0).*** *Se tarkoittaa, että saat käyttää listaa mihin tarkoitukseen haluat, muokata sitä niin kuin haluat ja jakaa sitä eteenpäin niin kuin haluat, seuraavilla ehdoilla:*

- *Nimeä - Sinun on mainittava lähde asianmukaisesti, tarjottava linkki lisenssiin sekä merkittävä, mikäli olet tehnyt muutoksia. Voit tehdä yllä olevan millä tahansa kohtuullisella tavalla, mutta et siten, että annat ymmärtää lisenssinantajan suosittelevan sinua tai teoksen käyttöäsi.*
- *Ei muita rajoituksia - Et voi asettaa sellaisia oikeudellisia ehtoja tai teknisiä estoja, jotka estävät oikeudellisesti muita tekemästä mitään sellaista, minkä lisenssi sallii*

Viestintä- ja markkinointiyhteistyötä

- Kyberturvallisuuskeskus kannustaa organisaatioita palveluntarjoajan käyttöön, mikäli organisaatiot kaipaavat laajaa tukea mittarin läpiviemiseen.
- Kyberturvallisuuskeskus voi listata Kybermittari-verkkosivulla yrityksiä, jotka tarjoavat Kybermittariin pohjautuvia arviointi- ja kehityspalveluja
- Palveluntarjoajien on mahdollista päästä listalle ja käyttää Kybermittari-sanaa markkinoinnissa sitoutumalla Kybermittarin markkinointiehtoihin ja palvelunkuvaukseen, joissa määritellään mm.
  - Miltä osin Kybermittarin käytännöt tulee toteutua ja miten muokkaukset alkuperäiseen on dokumentoitu asiakkaalle
  - Miten vertailutietoa pitää pystyä vaihtamaan

Esimerkkinä harjoitus- ja koulutuspalveluita tarjoavat yritykset:
(https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta)

Ohje tulosten jakamiseen

Organisaation tulokset

- Täytä arviointi ja tallenna tulokset.
- Voit käyttää jakamiseen esimerkiksi .csv muotoa (työkalun sivu Export_KTK)

Tulosten lähettäminen

- Voit käyttää tulosten lähettämiseen omaa turvapostia tai lähetä viestin, jossa yhteystietosi (nimi ja puhelinnumero*) osoitteeseen kybermittari@traficom.fi niin saat ohjeet.
- Lähetä tulokset turvapostilla Traficomiin osoitteeseen kybermittari@traficom.fi

Tulosten käsittely

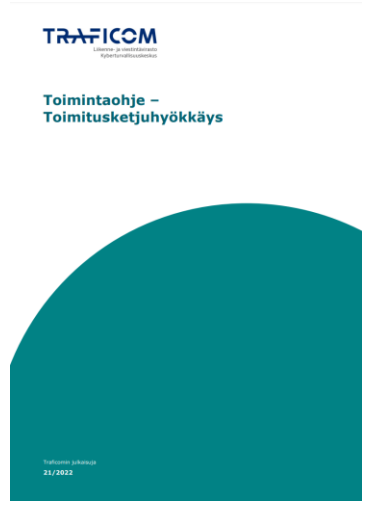
- Kyberturvallisuuskeskus käsittelee ja anonymisoi tulokset
- Tuottaa tulosten pohjalta toimialakohtaista vertailutietoa
- Kun riittävä määrä tietoa on saatavilla, jakaa tapauskohtaisesti vertailutietoa organisaatiolle turvasähköpostilla

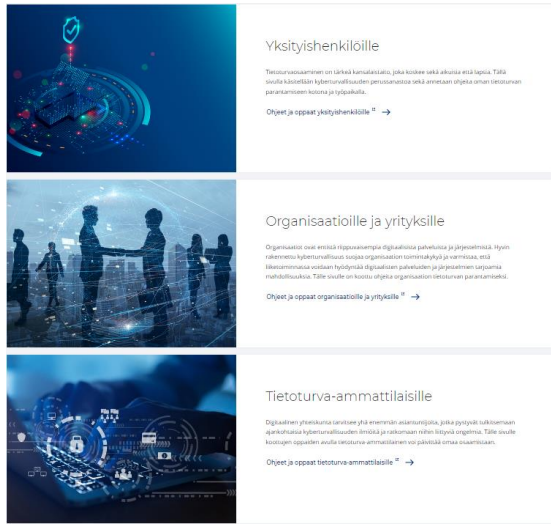
*Puhelinnumero vaaditaan, jotta Traficom pystyy toimittamaan toimialan vertailutiedot varmennetulle vastaanottajalle.

Palveluntarjoajan käytössä

- *www.kybermittari.fi*
  - *Työkalu ja tukimateriaali*
  - *Tulkintaohje (C2M2, eng)*
  - *Tiedonjako-ohje*
  - *Käyttöehdot*
  - *Kybermittari V1 vs V2 vs 2.1*
  - *Esimerkkitäyttö numeroin*
  - *Versiomuunnostyökalut*
  - *Tiedon tuonnin työkalut*
  - *Jne.*
- *Markkinointiehdot*
- *Palvelukuvaus*
- *Luonnosvaiheessa:*
  - *NIS2 ja Kybermittari*
- *Pyydettäessä:*
  - *Logot*
  - *Viestinnän tuki*

Kyberturvallisuuskeskuksen ilmaiset ohjeet ja oppaat





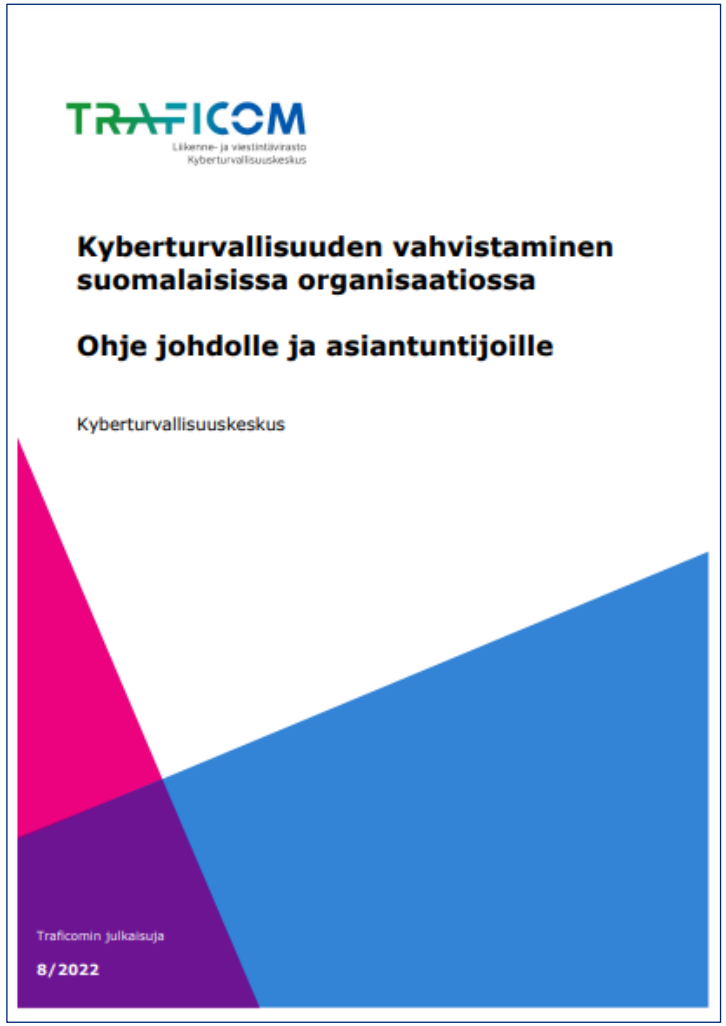
https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

TRAFICOM

TLP:CLEAR

”Tavanomaiset torjuntatoimenpiteet” käytännössä

1. Ottakaa kaikkialla käyttöön **monivaiheinen tunnistautuminen**.
2. Asentakaa **tietoturvapäivitykset** viipymättä.
3. Huolehtikaa **varmuuskopioista**.
4. Varmistakaa **etäyhteyksien** turvallisuus.
5. Tehkää **henkilöstöstä** tietoturvan vahvin lenkki (koulutus, tietoisuus ja poikkeamista ilmoittamisen kulttuuri).



https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

kybermittari@traficom.fi