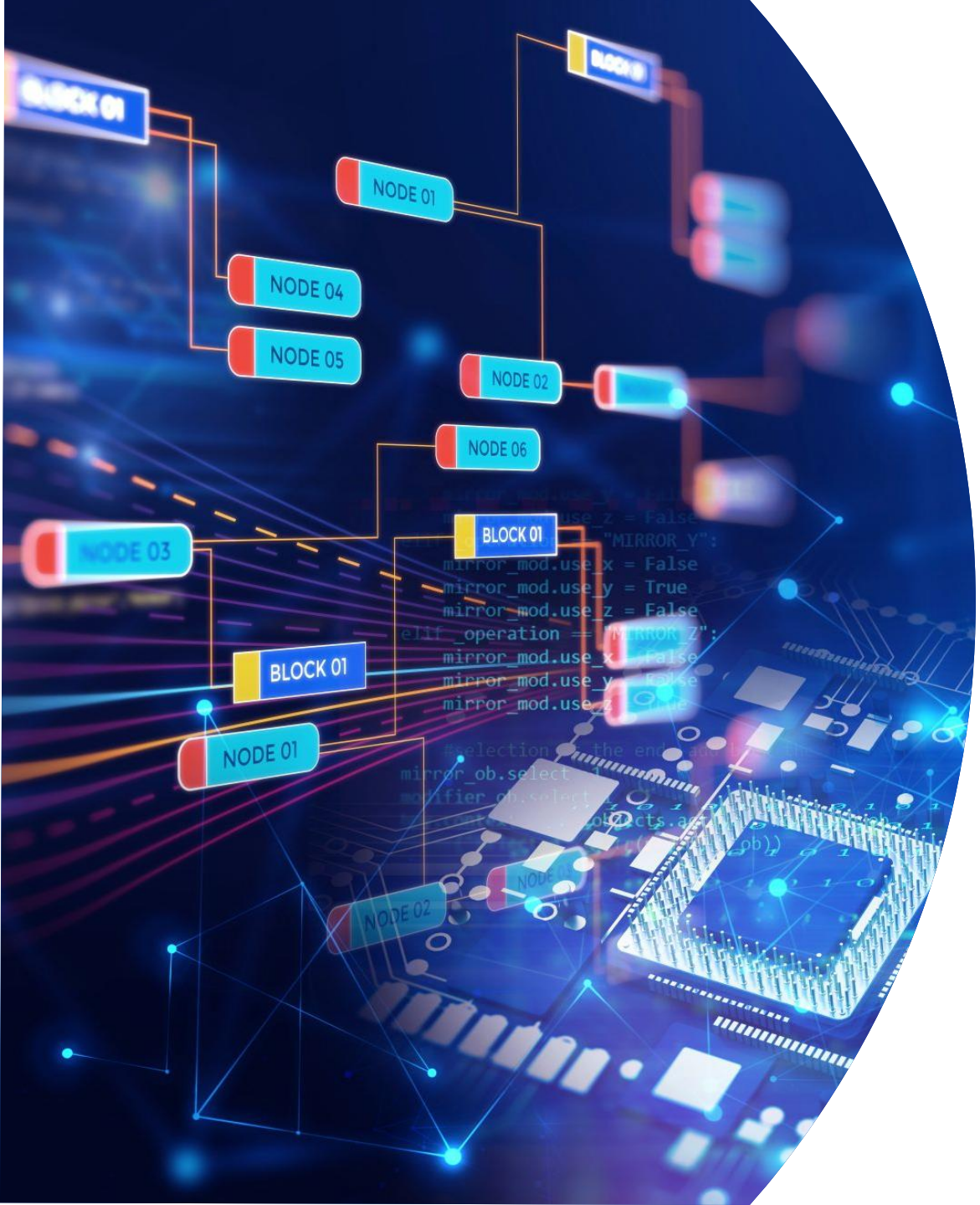
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Kyberturvallisuuden ohjaus ja valvonta

Mervi Malinen, lakimies, KTK



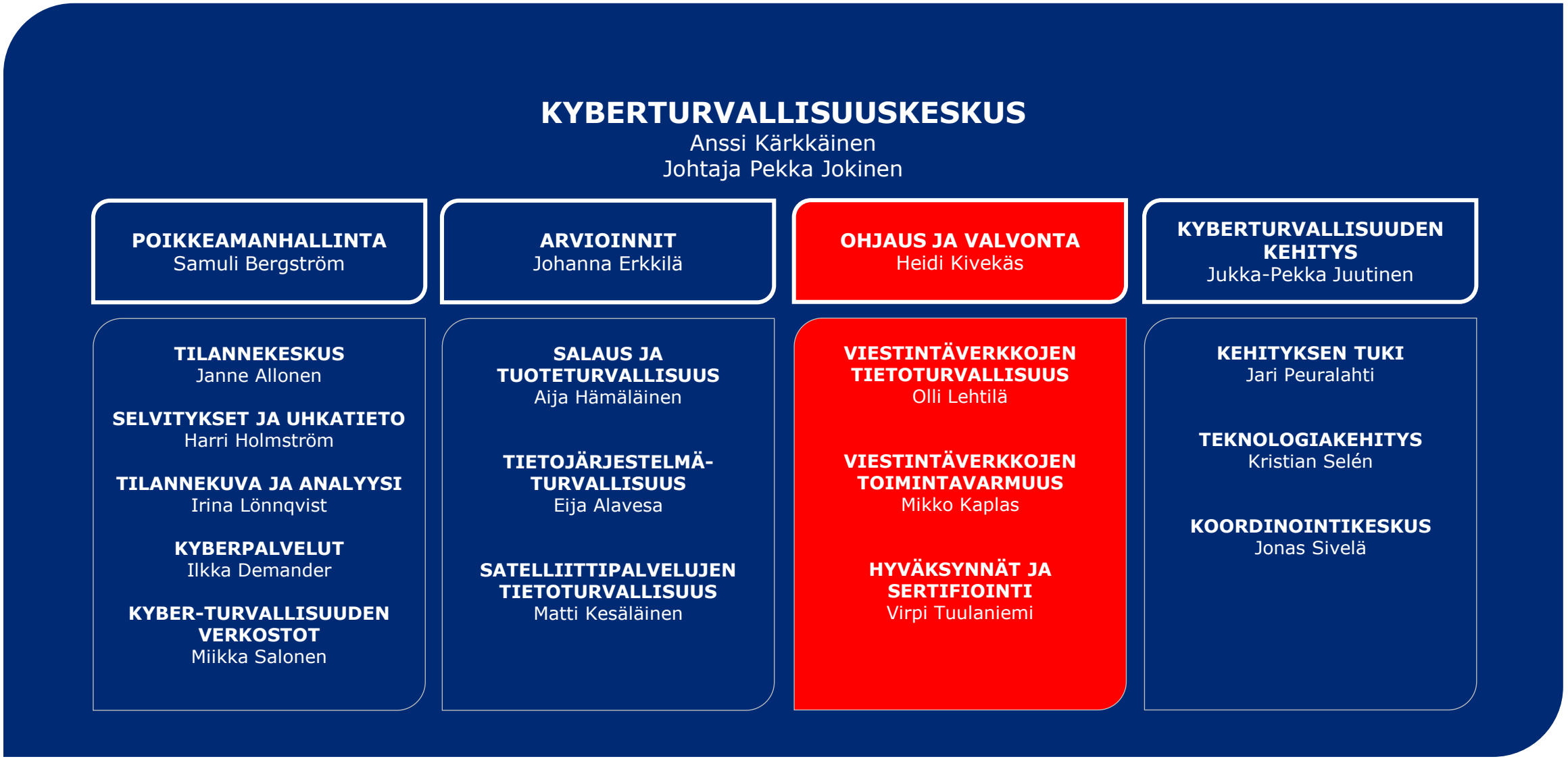

# Sisältö

Lyhyesti ohjauksesta ja valvonnasta

Kyberturvallisuusvelvoitteet toimijalle

Suositus kyberturvallisuuden riskienhallinnan toimenpiteistä

# Kyberturvallisuuskeskus




# NIS2 - Eri sektoreiden valvovat viranomaiset

TRAFICOM
Liikenne- ja viestintävirasto

Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

tukes

RUOKAVIRASTO
Livsmedelsverket • Finnish Food Authority

fimea

Elinkeino-, liikenne- ja ympäristökeskus

FIN-FSA
FINANSSIVALVONTA

energiavirasto

# KTK:n NIS2-valvontatehtävät (lakia ei vahvistettu)

- Aluetunnusrekisterit (.fi)
- Luottamuspalvelut
- Yleisten sähköisten viestintäverkkojen tarjoajat
- Yleisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoajat
- Julkishallinnon toimiala

- koosta riippumatta

- CDN-palvelut
- Datakeskuspalvelut
- Pilvipalvelujen tarjoajat
- Internetin yhdysliikennepisteiden ylläpitäjät
- ICT-palveluiden hallinta
  - Hallintapalvelujen tarjoajat (MSP)
  - Tietoturvapalveluntarjoajat (MSSP)
- Sosiaalisen median palvelut
- Tutkimusorganisaatiot → VTT
    - Suuret ja keskisuuret toimijat

HUOM! Lukuisia muita valvontatehtäviä viraston muille osaamisalueille

- Esim. kaikki liikennemuodot

# Kyberturvallisuuskeskus – Ohjaus ja valvonta

Toimintamme periaatteita ovat yhteistyö, avoimuus, luotettavuus ja tasapuolisuus

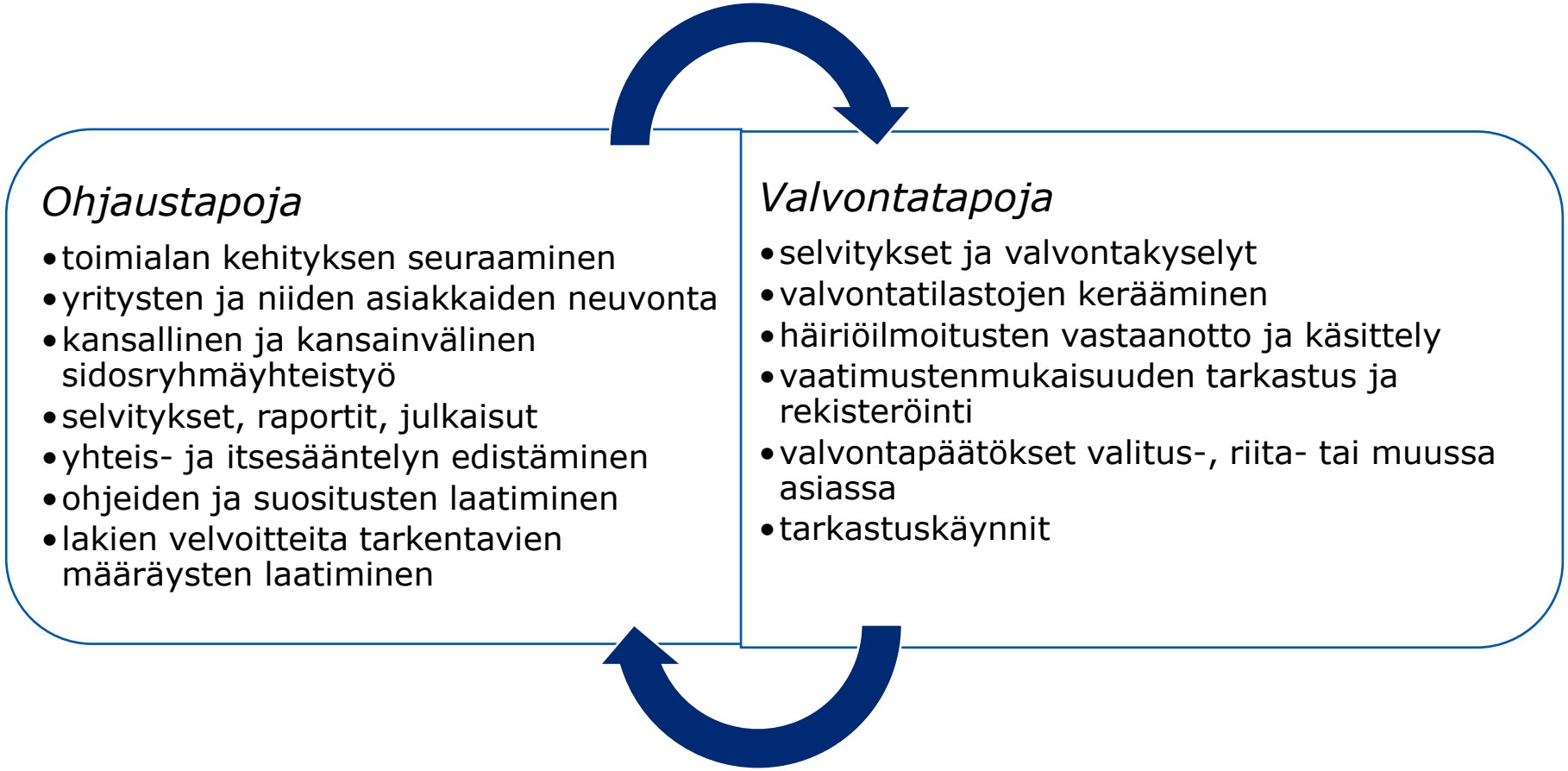
Suosimme ennaltaehkäisevää ja laajavaikutteista ohjausta

Panostamme perusluonteisten palvelujen toimivuuden ja tietoturvan ohjaukseen ja valvontaan

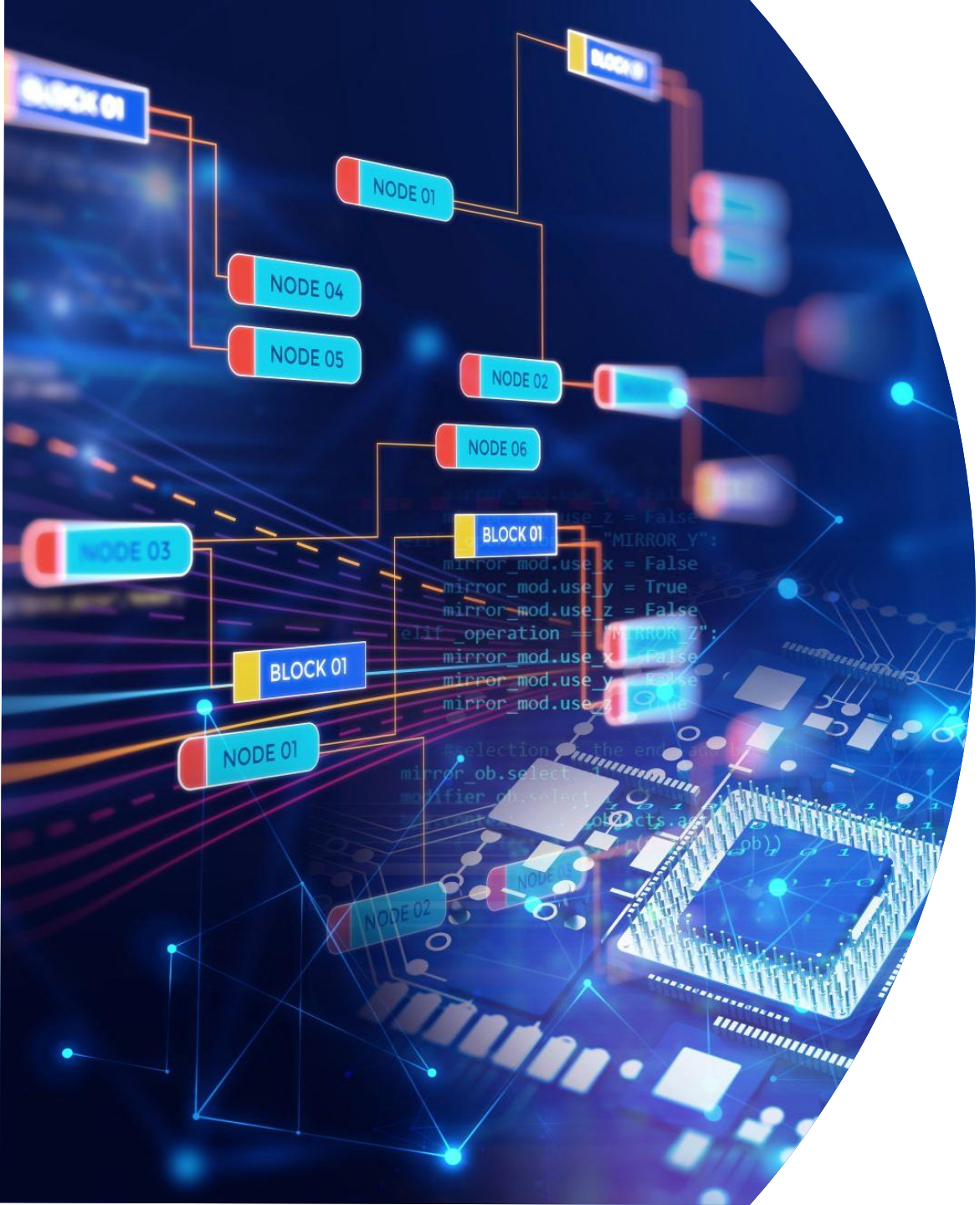
Haluamme tunnistaa ja ehkäistä ongelmat ajoissa sekä selvittää asiat yhteistyössä toimijoiden kanssa

Kyberturvallisuuskeskuksen valvontatehtävien määrä on voimakkaassa kasvussa

# Ennakoivalla ohjauksella ja vaikuttavalla valvonnalla positiivista tukea yhteiskunnalle



# Toimijan kyberturvallisuusvelvoitteet




# Tässä osiossa:

- Toimijaksi ilmoittautuminen
- Merkittävän poikkeaman ilmoittaminen
- Riskienhallintavelvoite

# Toimijaksi ilmoittautuminen (1/3)

- Traficomin valvontaan kuuluvien toimijoiden on mahdollista ilmoittautua Traficomille lain voimaantulon jälkeen. Ilmoittautuminen suomi.fi-tunnistautumisella.
  - toimijaluetteloon ilmoittautumisessa 1 kk siirtymäaika
- Ilmoittautumislomake tulee Traficomin ja Kyberturvallisuuskeskuksen verkkosivuille.
- Toimijoiden on ilmoitettava oman toimialansa valvovalle viranomaiselle seuraavat tiedot:
  1. Toimijan nimi
  2. Yhteystiedot, kuten osoite, sähköposti ja puhelinnumero
  3. Julkiset IP-osoitealueet
  4. Onko toimija keskeinen toimija
  5. EU:n jäsenvaltiot, joissa toimija tarjoaa palvelujaan
  6. Osallistuminen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn
- Mikäli kuulut useaan eri toimialaan, on huolehdittava ilmoittautumisesta jokaiselle toimialakohtaiselle valvovalle viranomaiselle.

# Toimijaksi ilmoittautuminen (2/3)

## Tapahtuma

Tällä lomakkeella kerätään kyberturvallisuuslain ja tiedonhallintalain vaatimusten mukaiset tiedot toimijoilta, jotka tulevat Traficomin valvonnan piiriin.

Lisätietoja NIS2-direktiivistä, kyberturvallisuuslaista ja tiedonhallintalain vaatimuksista Kyberturvallisuuskeskuksen verkkosivuilta osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

**Valitse ilmoituksen tyyppi: ***

- (●) Uusi NIS2-toimijailmoitus
- ( ) Muutokset toimijan tietoihin
- ( ) Tietojen poistaminen rekisteristä

# Toimijaksi ilmoittautuminen (3/3)

# Merkittävän poikkeaman ilmoittaminen (1/3)

**Kaikkien NIS2-toimijoiden on aina ilmoitettava merkittävästä poikkeamasta valvovalle viranomaiselle.**


**24 h kuluessa ensi-ilmoitus**

- Havainto merkittävästä poikkeamasta
- epäilläänkö, että kyseessä on rikos tai vihamielinen teko
- Rajat ylittävien vaikutusten mahdollisuus


**72 h kuluessa jatkoilmoitus**

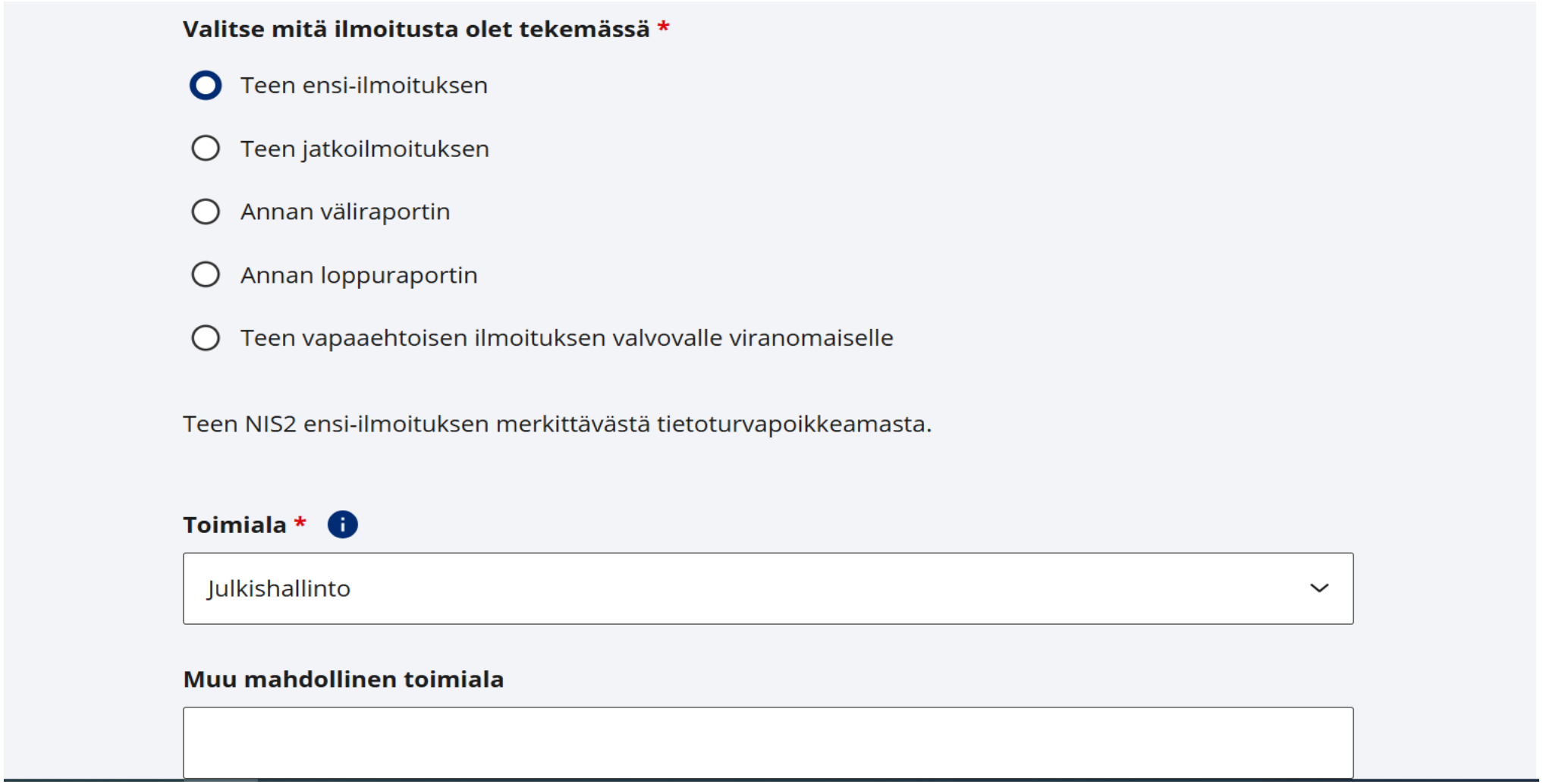
- Arvio poikkeaman laadusta, vakavuudesta ja vaikutuksista
- Vaarantumis-indikaattorit (IOC), jos mahdollista
- Mahdolliset täydennykset

**Mahdollinen väliraportti**

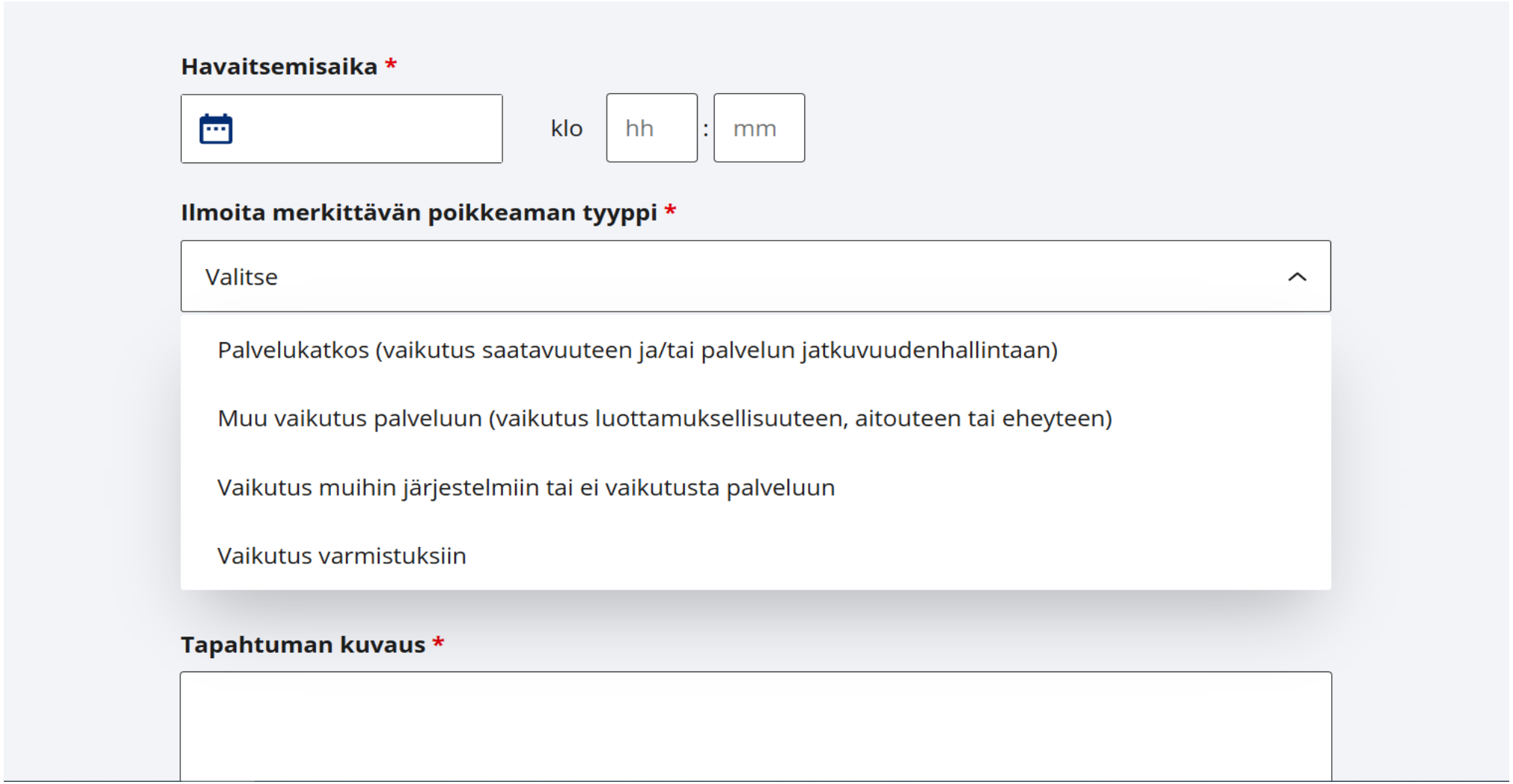
**1 kk kuluessa loppuraportti**

- Yksityiskohtainen kuvaus poikkea-masta, sen vakavuudesta ja vaikutuksista
- Poikkeaman arveltu aiheuttaja
- Toimenpiteet tilanteen hoitamiseksi
- Mahdolliset rajat ylittävät vaikutukset

# Merkittävän poikkeaman ilmoittaminen (2/3)

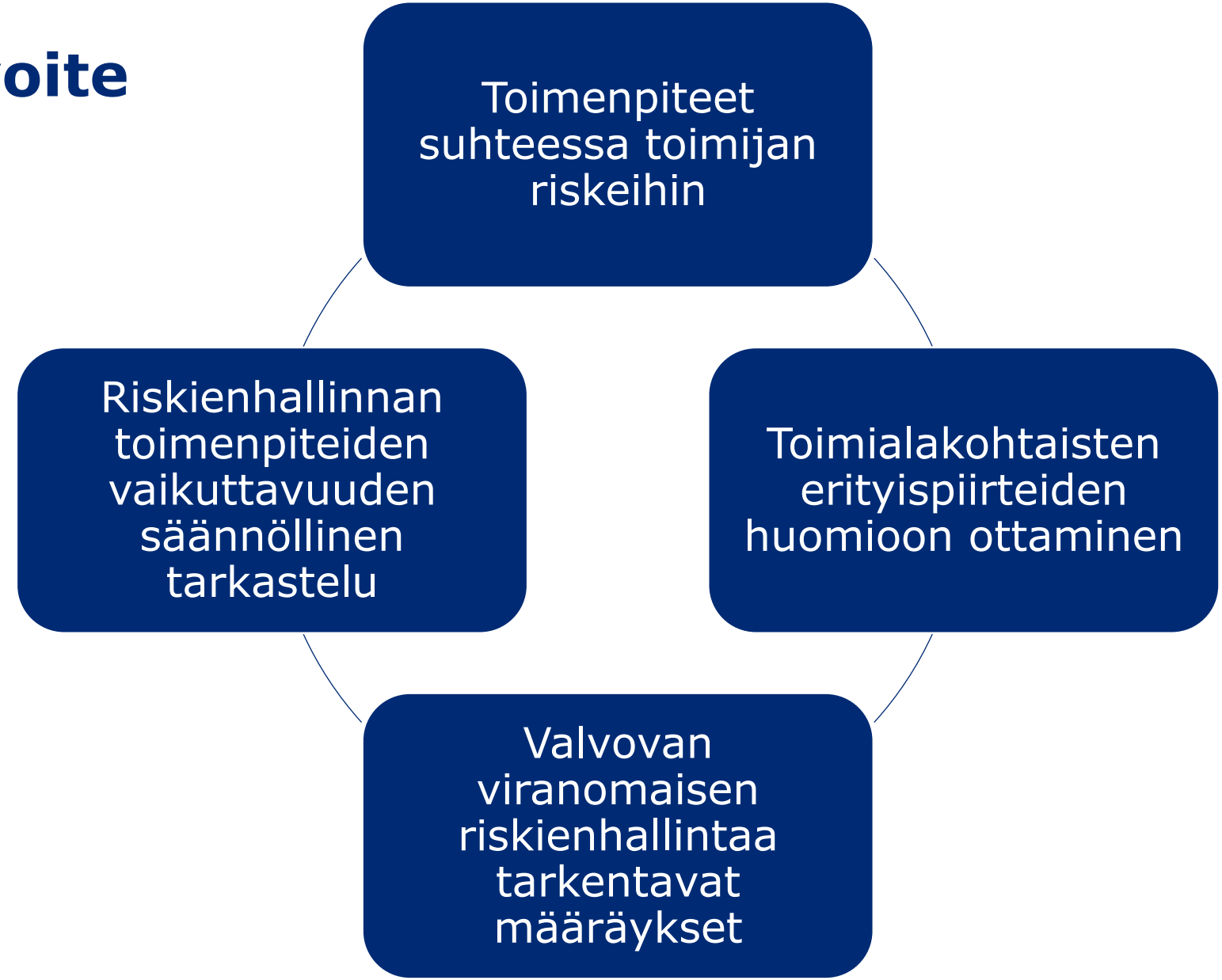


# Merkittävän poikkeaman ilmoittaminen (3/3)



# Riskienhallintavelvoite

- NIS 2 -direktiivin (2022/2555) 21 artiklassa.
- Tiedonhallintalain 4 a luvun 18 b ja 18 c § (kyberturvallisuuslain 7-9 §)
- Viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien tunnistaminen, arviointi ja hallinta.
- Riskienhallinnan tavoitteena on estää tai vähentää poikkeamien vaikutuksia toiminnan jatkuvuuteen ja palveluihin.
- Johto vastaa kyberturvallisuuden riskienhallinnan toteuttamisesta ja valvonnan järjestämisestä



# Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

Suositus **valvoville viranomaisille** NIS2-direktiivin mukaisista kyberturvallisuuden riskienhallinnan toimenpiteistä.

Suositus voi tukea myös **toimijoiden** kyberturvallisuuden **riskienhallinnan suunnittelua**.

Suositukseen on koottu **tietoa ja käytännön esimerkkejä** siitä, millaisia toimenpiteitä laissa säädettyihin **vaatimuksiin** voi kuulua.

Suosituksessa kuvataan myös erilaisia **keinoja**, joita valvova viranomainen voi harkintansa ja arvionsa mukaan käyttää **ohjaus- ja valvontatehtävissään**.

# Säädöspohja

- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on laatinut suosituksen osana keskitetyn yhteyspisteen viranomaisyhteistyötä ja koordinointitehtävää.
- Suosituksen taustalla NIS 2 –direktiivin riskienhallintavelvoitteiden täsmentäminen ja tulkintakäytännön yhteensovittaminen

# Suosituksen soveltamisesta

- Ei sido viranomaisia eikä toimijoita. Sitovat velvoitteet säädetään:
  - Laeissa,
  - Euroopan komission antamassa tarkentavassa sääntelyssä ja
  - toimialakohtaisen viranomaisen määräyksissä.

  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.
  - Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

# Suosituksen sisällöstä

- Riskienhallintavelvoite tiedonhallintalain 4 a luvussa (kyberturvallisuuslain 2 luku).
- Suositus käsittelee TiHL 18 c § (kyberturvallisuuslain 9 §) kyberturvallisuuden riskienhallinnan toimenpiteitä.
- Suositukseen on koottu yleisimmin käytetyt kyberturvallisuuden riskienhallintakeinot.
  - Esimerkkejä toteutuksista, joita valvova viranomainen saattaa kohdata valvonnan yhteydessä.
  - Esimerkkejä todennusmenetelmistä  ja viittaukset yleisimpiin kansallisiin ja kansainvälisiin viitekehyksiin

# Kyberturvallisuuden riskienhallinnan toimenpiteet

1. Kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

2. Viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet**

3. Viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon turvallisuus** sekä tarvittavat menettelyt **haavoittuvuuksien** käsittelyyn ja julkistamiseen

4. **Toimitusketjun** välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja **häiriönsietokyky**, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien **kyberturvallisuuskäytännöt**

5. **Omaisuudenhallinta** ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

6. **Henkilöstöturvallisuus ja kyberturvallisuuskoulutus**

7. **Pääsynhallinnan ja todentamisen** menettelyt

8. **Salausmenetelmien** käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

9. **Poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

10. Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan **jatkuvuuden hallinta** ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

11. **Perustason tietoturvakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

12. Toimenpiteet viestintäverkkojen ja tietojärjestelmien **fyysisen ympäristön** ja tilaturvallisuuden sekä **välttämättömien resurssien** varmistamiseksi

## 7.4 Pääsynhallintaan liittyvä kirjanpito ja vähimpien oikeuksien periaate

### Toteutusesimerkki

- Toimijalla on olemassa kirjanpito tai vastaava menettely, jolla käyttöoikeudet ja käyttöoikeusroolit kirjataan. Tämän kirjanpidon ajantasaisuuden ylläpitoon on olemassa menettely.
- Kirjanpidon perusteella käyttäjälle on annettu vain ne käyttöoikeudet, jotka ovat välttämättömiä työtehtävien suorittamista varten (vähimpien oikeuksien periaate). Käyttäjään perustuvia valtuutuksia on pyritty mahdollisuuksien mukaan välttämään ja niiden sijaan on käytetty roolipohjaista käyttöoikeuksien hallintaa.

### Todennus

1. Valvova viranomainen todentaa toimijan dokumentaation pääsynhallintaan liittyvän kirjanpidon menettelyistä. Dokumentaatiosta käy ilmi, miten käyttöoikeudet ja -roolit kirjataan. Toimijan pääsynhallintaan liittyvästä kirjanpidosta käy ilmi järjestelmien käyttöoikeudet ja käyttöoikeusroolit. Tämä kirjanpito voi olla joidenkin järjestelmien kohdalla manuaalista kirjanpitoa, mutta se voi olla myös automaattista ja esimerkiksi käyttäjäryhmiin perustuvan roolipohjaisen käyttöoikeuksien hallinnan järjestelmätason kirjanpitoa.
2. Valvova viranomainen todentaa toimijan järjestelmän käyttöoikeuksia ja niiden vastaavuutta kirjanpitoon. Tämä voidaan tehdä esimerkiksi käyttäjistä satunnaisotannalla tai tiettyjä käyttöoikeuksia, kuten järjestelmän pääkäyttäjä- tai muita korotettuja oikeuksia tarkastellen. Käyttöoikeuksien tulisi vastata niistä pidettyä kirjanpitoa. Mikäli järjestelmässä hyödynnetään esimerkiksi rooli- tai käyttäjäryhmäpohjaista käyttöoikeuksien hallintaa, ei näiden lisäksi tulisi olla myönnetty etenkään dokumentoimattomia käyttäjään perustuvia käyttöoikeuksia.

### Perustelut

Ylimääräiset käyttäjätunnukset ja pääsyoikeudet voivat mahdollistaa hyökkääjän pääsyn järjestelmään. Hyökkääjä voi hyödyntää dokumentoimattomia tai unohdettuja pääsyoikeuksia liikkuessaan järjestelmässä tai järjestelmästä toiseen. Liian laajasti myönnetyt pääsyoikeudet saattavat mahdollistaa myös muut epätoivotut tiedon paljastumiset.

### Viitteet

IEC 62443-2-1:2013 (4.3.3.7)

ISO/IEC 27002:2022 (5.15, 5.18)

NIST CSF 1.1 (PR.AC-4)

NIST CSF 2.0 (PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Reference document (3.7.3 Privileged and administration accounts)

NIS CG Implementation guidance (11.2. Management of access rights)

NIS CG Implementation guidance (11.3. Privileged accounts and system administration accounts)

### Työkalut

Julkri (HAL-14, TEK-07.2)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3)

# NIS2 ohjauksen ja valvonnan nostot 2025

- Traficom julkaisee poikkeamailmoitus- ja toimijaluettelolomakkeet sekä suosituksen riskienhallintatoimenpiteistä, kun kyberturvallisuuslaki/tiedonhallintalain muutokset tulleet voimaan
- Kanavat päivitetään NIS 2 -sivuille: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi
- Suositus NIS2-valvoville viranomaisille tullaan julkaisemaan: Säädökset ja määräykset | Kyberturvallisuuskeskus

# Valvonnan ja ohjauksen nostot

- KTK painottaa ennakko-ohjauksen ja neuvonnan merkitystä NIS2-toimijoille vuonna 2025
- Uutta sääntelyä ja monia uusia valvottavia toimijoita
- Toiveena luottamuksen ja yhteistyön rakentaminen uusien valvottavien toimijoiden ja valvovan viranomaisen välillä

# Kiitos!

nis.valvonta.ktk@traficom.fi

mervi.malinen@traficom.fi

paivi.timlin@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus