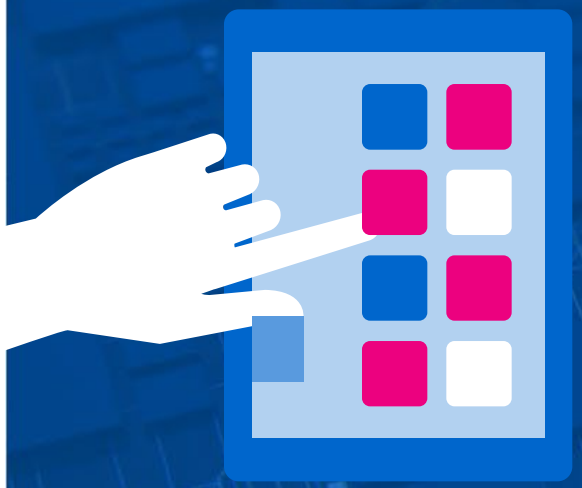
TRAFICOM
Liikenne- ja viestintävirasto

# Kyberturvallisuuskeskus, ajankohtaisia aiheita sekä taloyhtiöiden tietoturvakulmia 8.10.2024

# Kyberturvallisuuskeskus – kansallinen tietoturvaviranomainen



**Kerää tietoa** tietoturvaloukkauksista ja niiden uhkista

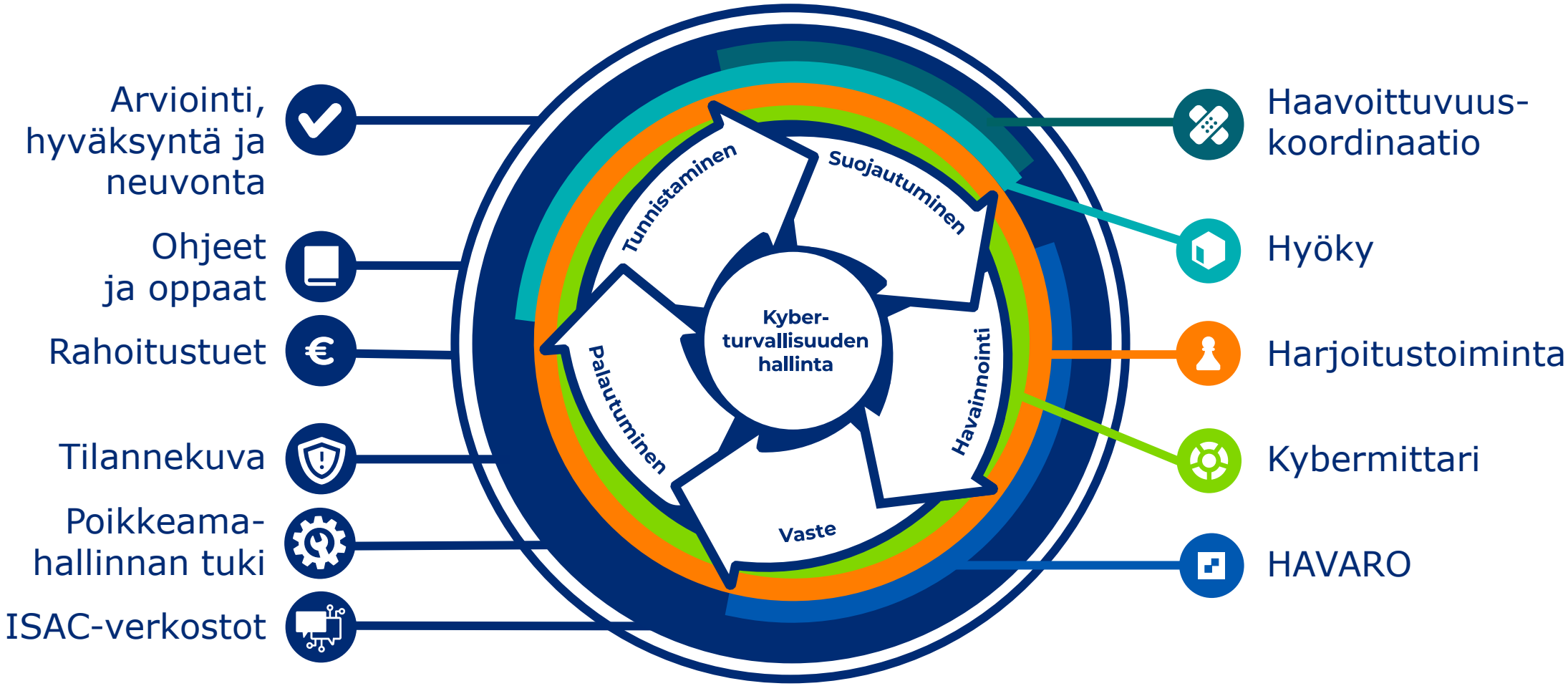
**Tiedottaa** tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta

**Selvittää** verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia sekä niiden uhkia

**Arvioi ja hyväksyy** järjestelmiä ja verkkoja

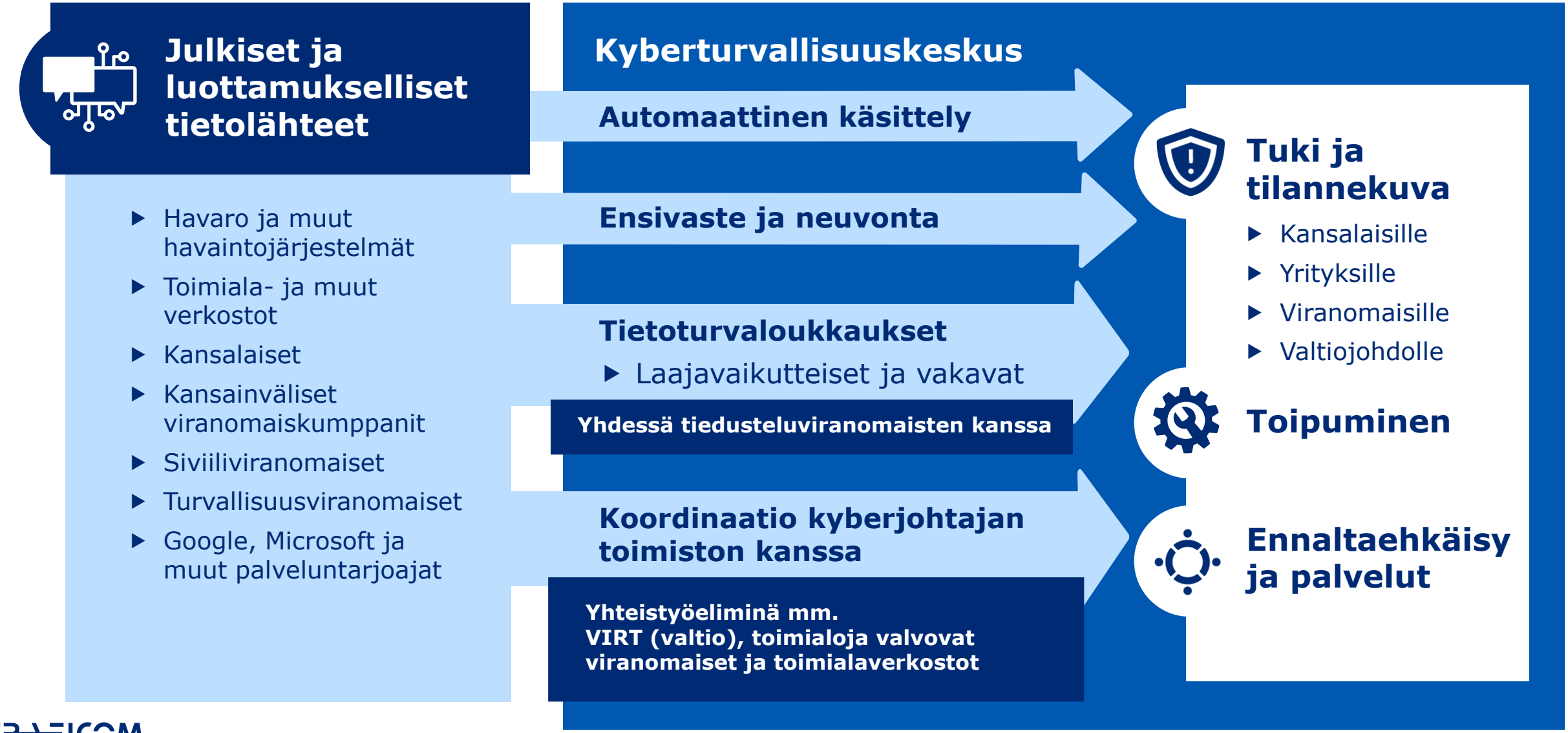
**Ohjaa ja valvoo**

- teleyritysten tietoturvallisuutta ja varautumista
- sähköisen viestinnän luottamuksellisuuden suojaa ja
- vahvojen sähköisten tunnistus- ja luottamuspalvelujen tietoturvaa




# Tarjoamme kyberturvallisuuden palveluita monipuolisesti koko yhteiskunnalle

# Kyberturvallisuuskeskus toimii yhdessä kerätyn tiedon pohjalta



# Yhteistyöverkostot

Kehitetään toimialojen ja yhteiskunnan kyberturvallisuutta yhdessä tietoturva-asioiden tiedonvaihtoryhmissä ISAC (Information Sharing and Analysis Centre)

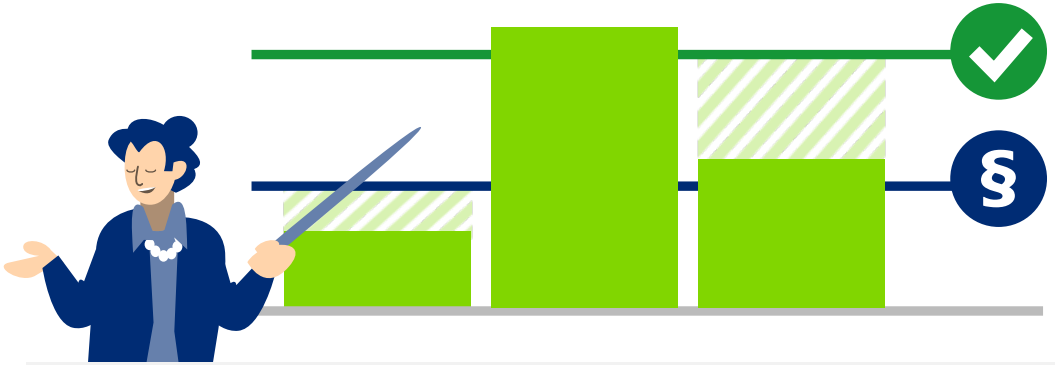
- riskianalyysit
- ohjeistukset
- tutkimukset
- tiedonvaihto


**+ Toimivaltaiset viranomaiset (NIS)**

PALVELUT ORGANISAATIOILLE

# Kybermittari

kybermittari.fi | kybermittari@traficom.fi




Miten suojaudutte kyberuhilta ja varmistatte liiketoiminnan jatkuvuuden häiriötilanteissa?

## Ilmainen työkalu

kyberkyvykkyyksien selvittämiseen ja hallintaan

## Johdolle ja tietoturva-ammattilaisille

yrityksissä ja organisaatioissa

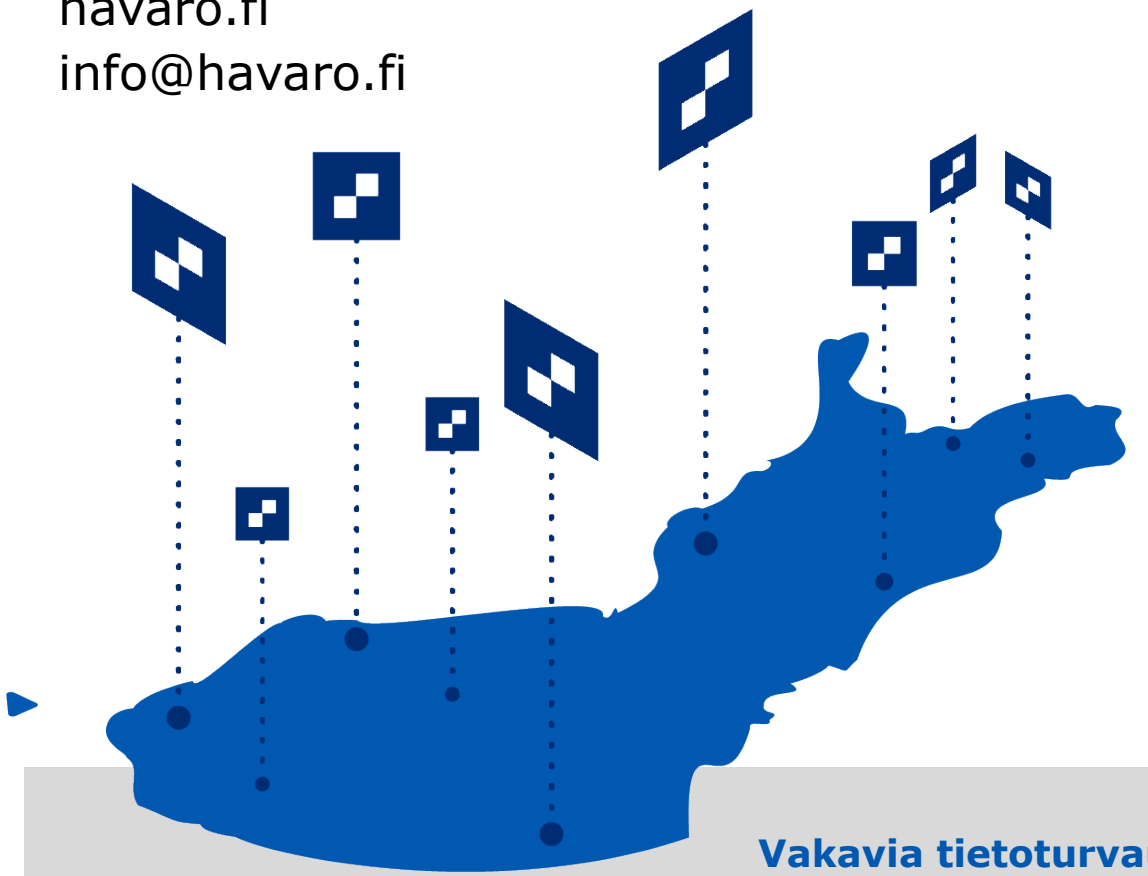
## Tiedolla johtamiseen

- tilannekuva ja omasta tietoturvasta
- kyberkyvykkyyksien arviointi ja vuotuinen seuraaminen
- kehityskohteiden tunnistaminen
- tavoitteiden asettaminen
- resurssien kohdentaminen
- oman tilanteen vertaaminen alan yleiseen tasoon

PALVELUT ORGANISAATIOILLE

# HAVARO

havaro.fi
info@havaro.fi



## Havainnointi- ja varoitusjärjestelmä

auttaa tuottamaan kansallista tilannekuvaa ja ehkäisemään vakavia tietoturvauhkia

- **Sensori**
  valvoo liikennettä organisaation verkon reunalla osana kansallista sensoriverkostoa
- **Havaintojen käsittely**
  palvelukeskuksessa tai Traficomissa
- **Asiakasraportit**
  näkymänä oman organisaation havaintoihin ja tuloksiin
- **Luottamusverkosto**
  jakaa tietoa jako yli organisaatiorajojen

**Vakavia tietoturvauhkia** ovat esimerkiksi valtiollisten eli APT-toimijoiden tekemät **kohdistetut hyökkäykset** ja **tietoa varastavat haittaohjelmat**.

# Ajankohtaisia kyberaiheita

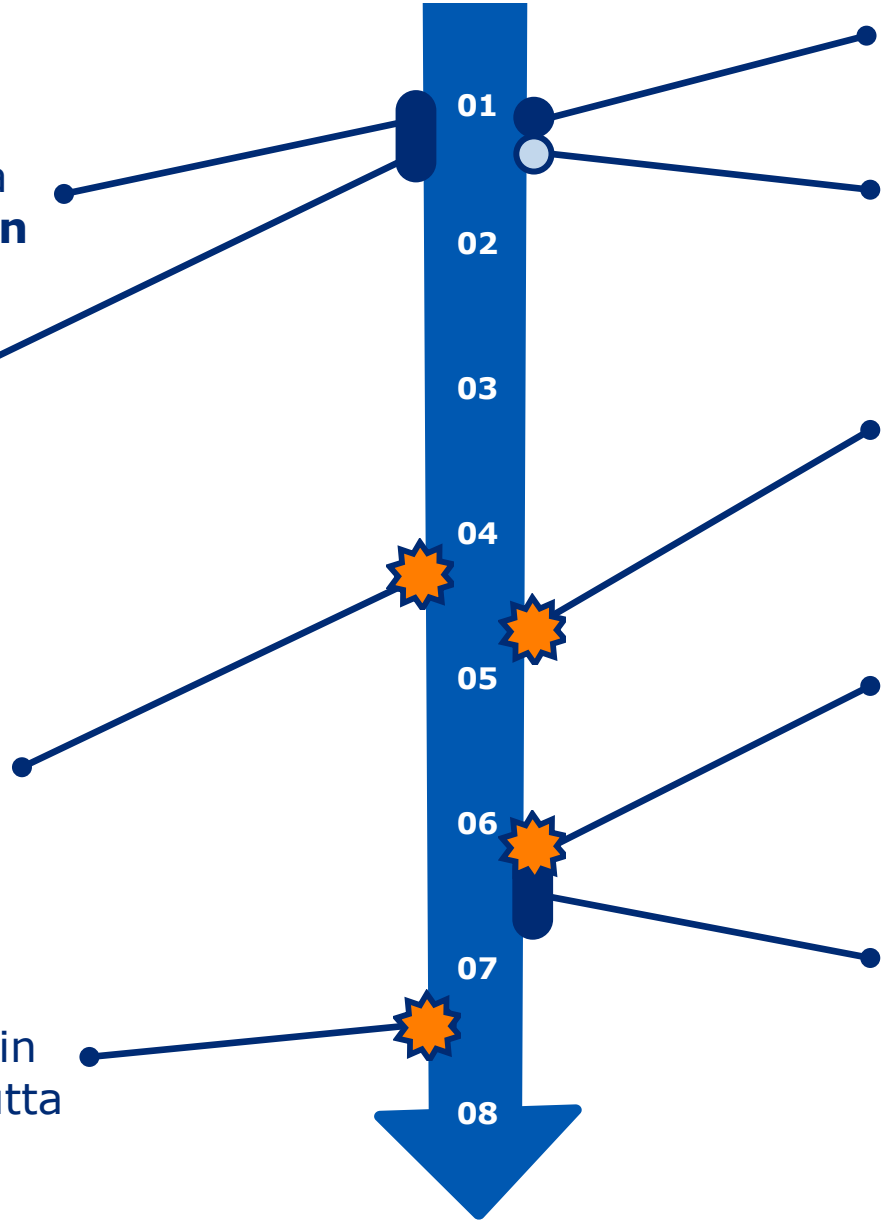
# VUOSI 2024

Suomalaisia organisaatioita **palvelunestohyökkäysten** kohdelistalla (NoName)

**Tekoälypohjaisia** uskottavia huijauksia

**Vakava tietomurto** vaaransi useiden organisaatioiden tietohakurajapintoja

**Tietomurtoja** suomalaisiin organisaatioihin Microsoft-järjestelmien kautta




**M365-tilimurrot** lisääntyvät

Olemme mukana turvaamassa **presidentinvaalien** sujumista

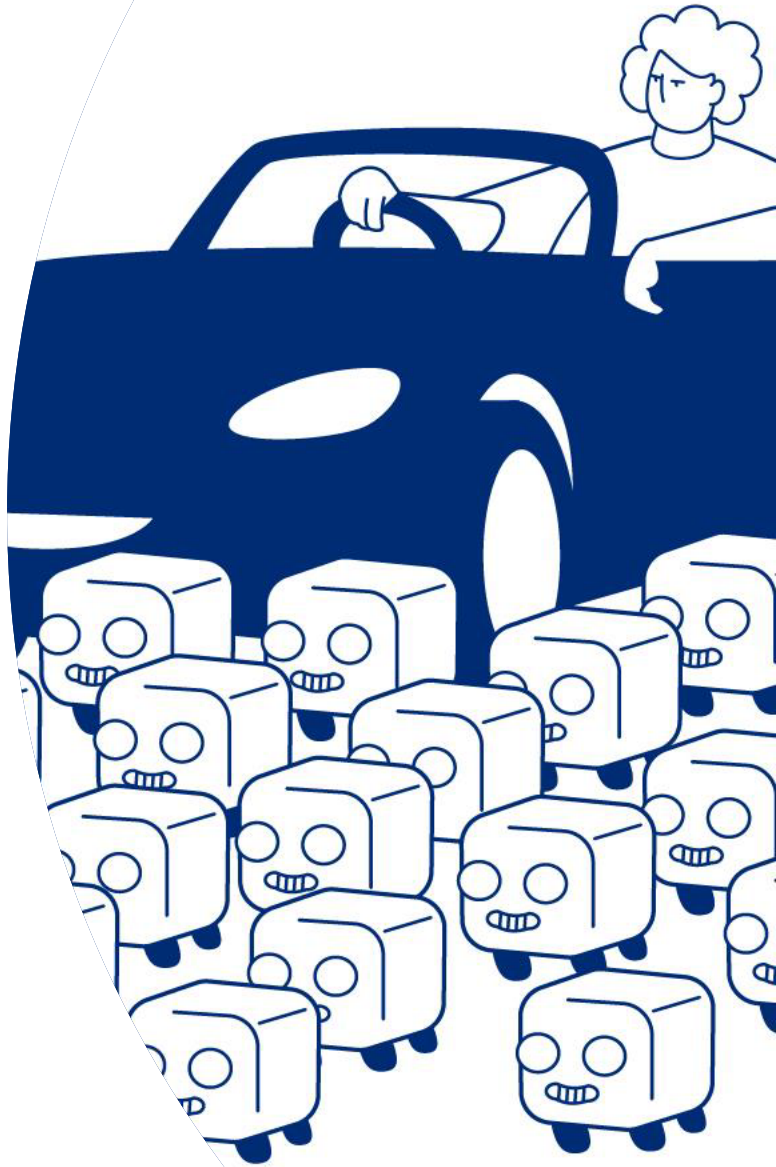
**Helsingin kaupungin tietomurto**

Nato-portaalista varastettuja **tietoja myynnissä pimeässä verkossa**

Laajoja **GPS-häiriöitä**

# Palvelunestohyökkäykset

- Hyökkääjän motivaationa yleensä mielen osoittaminen – informaatiovaikuttaminen!
  - Joskus myös hämäys vakavamman hyökkäyksen peittämiseksi tai internetpalvelusta riippuvaisen liiketoiminnan häiritseminen
- Liikennetulvalla hyökkääminen on helppoa ja halpaa
- Keskeinen suojautumiskeino on varautuminen oman internetpalveluntarjoajan kanssa
- Alkusyksystä DDoS:eja ollut tavanomaista enemmän
  - Monesti käytetty ns. mattopommitustekniikkaa
- Geoblokkaus ei aina auta



# M365-käyttäjätilien murrot

- Jatkuva ilmiö; selvästi kannattavaa toimintaa rikollisille
- Kalasteluviestien teemat vaihtelevat. Rikolliset seuraavat Suomen tapahtumia ja hyödyntävät niitä. Yleisimpiä teemoja:
  - SharePointissa tai DropBoxissa jaettu tiedosto
  - DocuSignissa allekirjoitettava tiedosto
  - Salattu sähköpostiviesti
- Monivaiheinen tunnistautuminen ei anna ehdotonta suojaa, kun rikollinen on saanut hämättyä käyttäjän kirjautumaan väärennetylle sivustolle
  - Rikolliset käyttävät yleisesti Adversary-in-the-Middle-tekniikkaa (AitM)
- Rikolliset käyttävät murrettuja käyttäjätilejä yleisimmin laskutuspetoksiin ja uusien kalasteluviestien lähettämiseen.
- Rikolliset voivat vastata uhrille saapuviin viesteihin ja poistaa viestejä uhrin sähköpostilaatikosta

## Kalasteluviesti

Lähetetään aiemmin murretulta käyttäjätililtä

## Kalastelu

Kalastelusivu rikollisten AiTM-palvelimella

Rikollinen saa tunnukset haltuunsa ja kopioi istuntoevästeen

## Tietomurto

Rikollinen kirjautuu palveluun evästeen avulla

## Rikollinen hyödyntää murrettua käyttäjätiliä

Lukee sähköposteja ja tutki tiedostoja

Luo omia sääntöjä postin käsittelyyn

Lisää oman kaksivaiheisen tunnistautumisen

Käyttää tiliä esimerkiksi laskutuspetoksiin

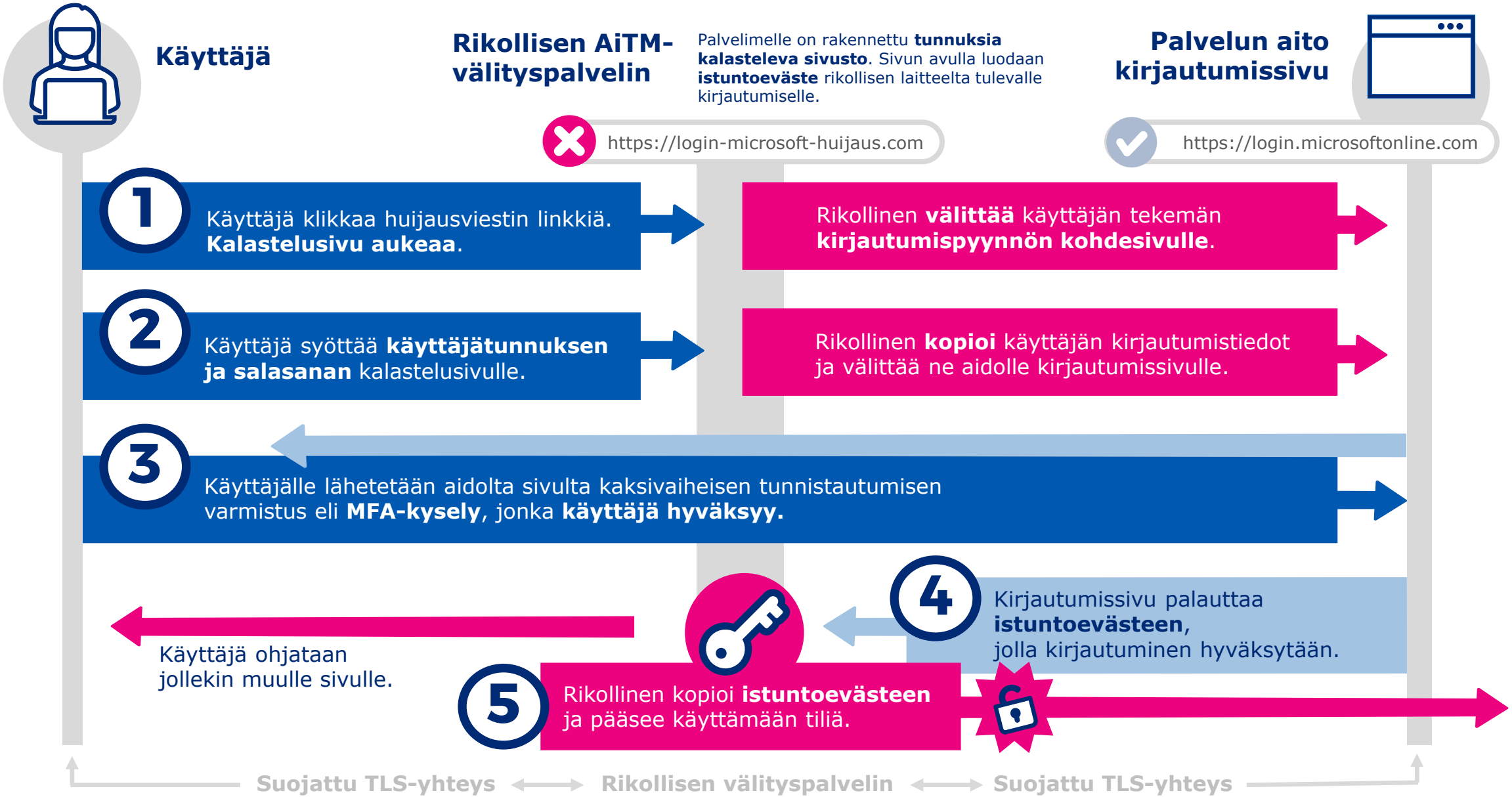
Levittää kalasteluviestejä uusille uhreille

Muut käyttäjät organisaation sisällä

Organisaation kumppanit, asiakkaat ja muut kontaktit

## Kalastelu

Uusi kampanja seuraaville uhreille


Käyttäjä
Rikollisen AiTM-välityspalvelin
Palvelimelle on rakennettu **tunnuksia kalasteleva sivusto**. Sivun avulla luodaan **istuntoeväste** rikollisen laitteelta tulevalle kirjautumiselle.
Palvelun aito kirjautumissivu
https://login-microsoft-huijaus.com
https://login.microsoftonline.com
1
Käyttäjä klikkaa huijausviestin linkkiä. **Kalastelusivu aukeaa**.
Rikollinen **välittää** käyttäjän tekemän **kirjautumispyynnön kohdesivulle**.
2
Käyttäjä syöttää **käyttäjätunnuksen ja salasanan** kalastelusivulle.
Rikollinen **kopioi** käyttäjän kirjautumistiedot ja välittää ne aidolle kirjautumissivulle.
3
Käyttäjälle lähetetään aidolta sivulta kaksivaiheisen tunnistautumisen varmistus eli **MFA-kysely**, jonka **käyttäjä hyväksyy.**
4
Kirjautumissivu palauttaa **istuntoevästeen**, jolla kirjautuminen hyväksytään.
Käyttäjä ohjataan jollekin muulle sivulle.
5
Rikollinen kopioi **istuntoevästeen** ja pääsee käyttämään tiliä.
Suojattu TLS-yhteys
Rikollisen välityspalvelin
Suojattu TLS-yhteys

# Taloyhtiöiden tietoturvakulmia

# IoT & automaatio mietteitä

- Laitteiden liittäminen internetiin yhä jatkuvassa nousussa
  - Myös OT-puolella laitteiden liittäminen julkiseen verkkoon (etä)hallinnan helpottamiseksi
  - → pahantahtoinen vaikuttaminen helpompaa
- Laitteiden tietoturvan taso kysymysmerkkinä
  - Kilpailu on kovaa → tehdään ”kustannustehokkaasti” → tietoturva kirveen alla?
- Avoimeen verkkoon näkyvien laitteiden kaappaus rikollisten käyttöön
  - Rikolliset tahot voivat käyttää kaapattuja laitteita mm. välittääkseen liikennettä
- 3G-verkon alasajon vaikutukset
  - Laitteet eivät välttämättä aina osaa/pysty automaattisesti vaihtamaan toiseen mobiiliverkkoon
  - Vanhemmat laitteet 2G-verkkoon (pienempi datamäärä), uudemmat laitteet 4G/5G

# Toimittajien valinta ja vastuukysymykset

- Toimittajien valinnassa monia elementtejä
  - Hinta merkittävä tekijä (näennäinen valinnanvapaus)
  - Kestävä kehitys
  - Vaihtoehtojen laajuus/suppeus
  - Hankkivan (joskus myös myyvän) tahon ymmärrys tietoturva-asioista
  - Toimittaja lupailee paljon → toimittaa vähän
- Kun laite/ohjelmisto on hankittu, kenellä vastuu tietoturvasta?
- Vastuukysymykset pitää leipoa osaksi sopimuksia, jotta tietoturva ei unohdu!
  - Ostatko laitetta/ohjelmistoa, vai myös ylläpitopalvelua? Onko omaa osaamista ylläpitää tuotetta?

# Epäiletkö tietoturvaloukkausta?

**Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.**

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin kello 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi.

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

TRAFICOM
Liikenne- ja viestintävirasto

# Kiitos!

kyberturvallisuuskeskus@traficom.fi

taneli.vuori@traficom.fi