



**CYBERWATCH FINLAND**

**KYBERTURVALLISUUS OSAKSI KAUPUNKISTRATEGIAA**

**- CASE SALON KAUPUNKI -**

# DIGITAALINEN TOIMINTAYMPÄRISTÖ

Digitaalisessa maailmassa asukkaiden, henkilöstön ja yhteistyökumppanien turvallisuudesta huolehtiminen on yksi kaupunkien tärkeimmistä tehtävistä. Turvallisuus laaja-alaisena käsitteenä on ihmisten perusoikeus ja kaikkien yhteinen asia, johon eri viranomaiset, yhteisöt, elinkeinoelämä ja kansalaiset voivat omalla toiminnallaan vaikuttaa.

Kaupunkien palveluja tulee kehittää digitalisaatiota hyödyntäen, mutta samalla kyberturvallisuudesta huolehtien.





# KAUPUNKIEN KYBERTOIMINTAYMPÄRISTÖ

Kaupunkien palvelutuotannon turvaaminen nykyisessä kybertoimintaympäristössä edellyttää kattavan kyberriskianalyysin tekemistä ja digiturvallisuuden jatkuvaa kehittämistä.

Palvelut on suunniteltava asiakaslähtöisesti ja ulkoisia, sekä sisäisiä prosesseja suunnitelmallisesti kehittämällä ja ottaen huomioon niihin kohdistuvat hybridi- ja kyberuhat.

Näiden tavoitteiden saavuttaminen edellyttää digi- ja kybertaitojen kehittämistä hallinnon kaikilla tasoilla, kriittisissä yrityksissä, mutta myös kaupunkilaisten keskuudessa.

Digi- ja kyberturvallisuuskoulutus on otettava entistä kiinteämmäksi osaksi kaupungin koko opetustoimea.

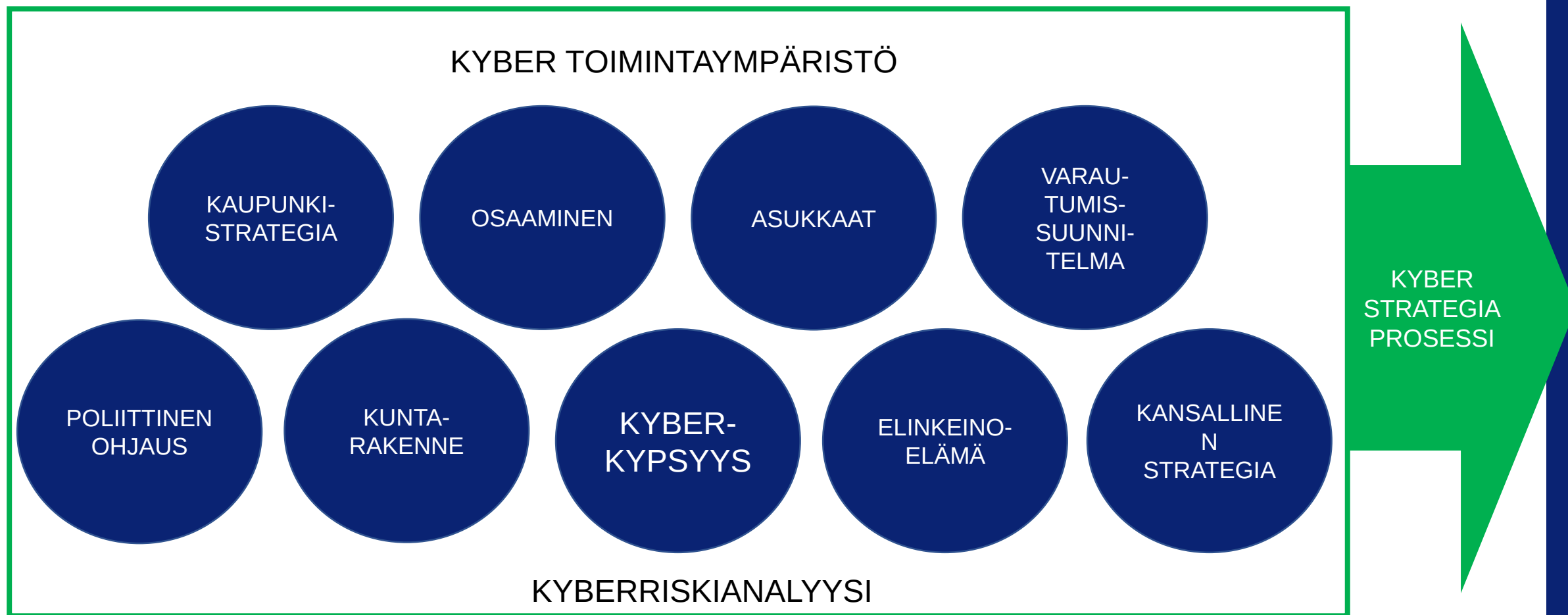


# SMART CITY

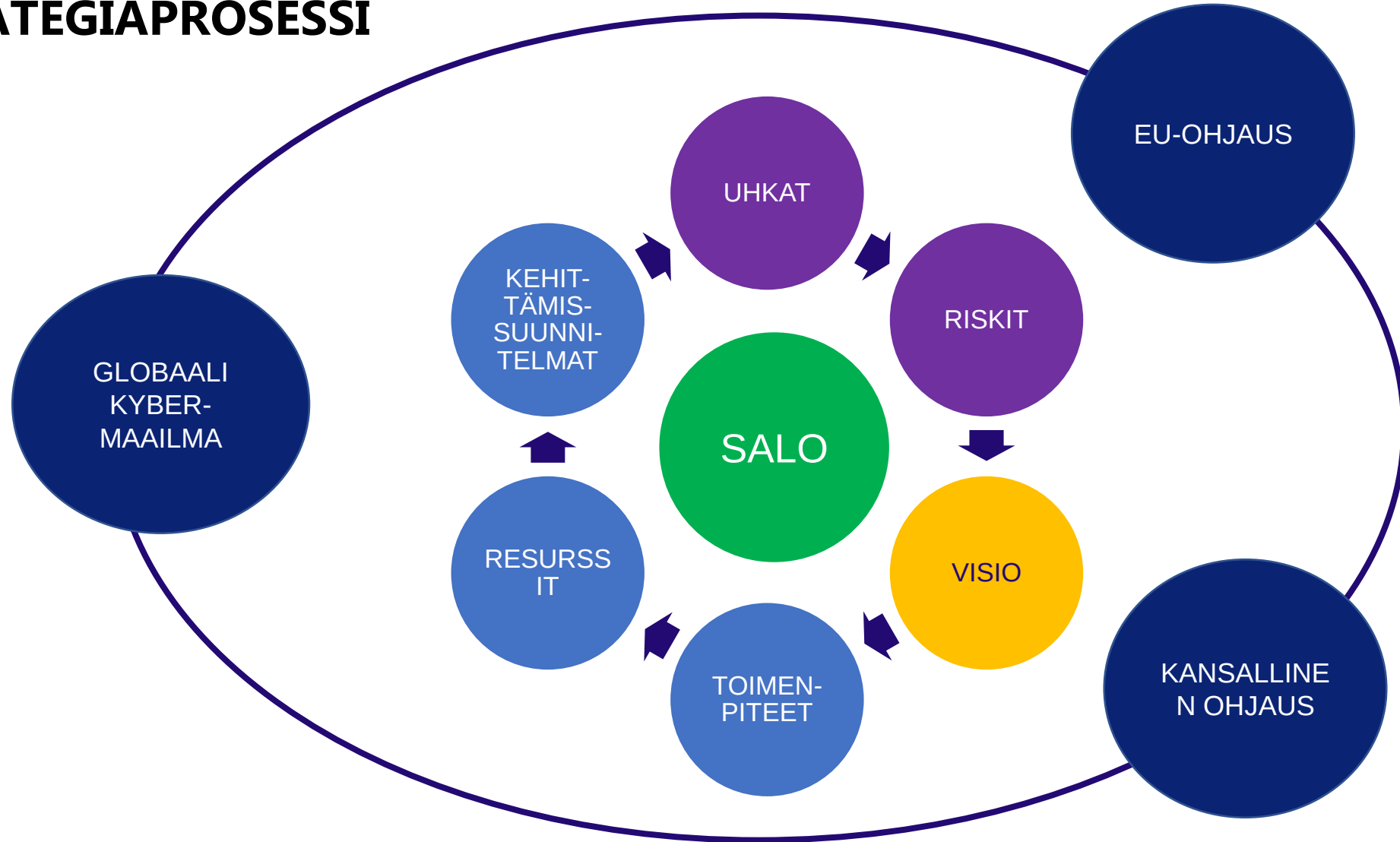
BUILDING TOMORROW'S CITIES



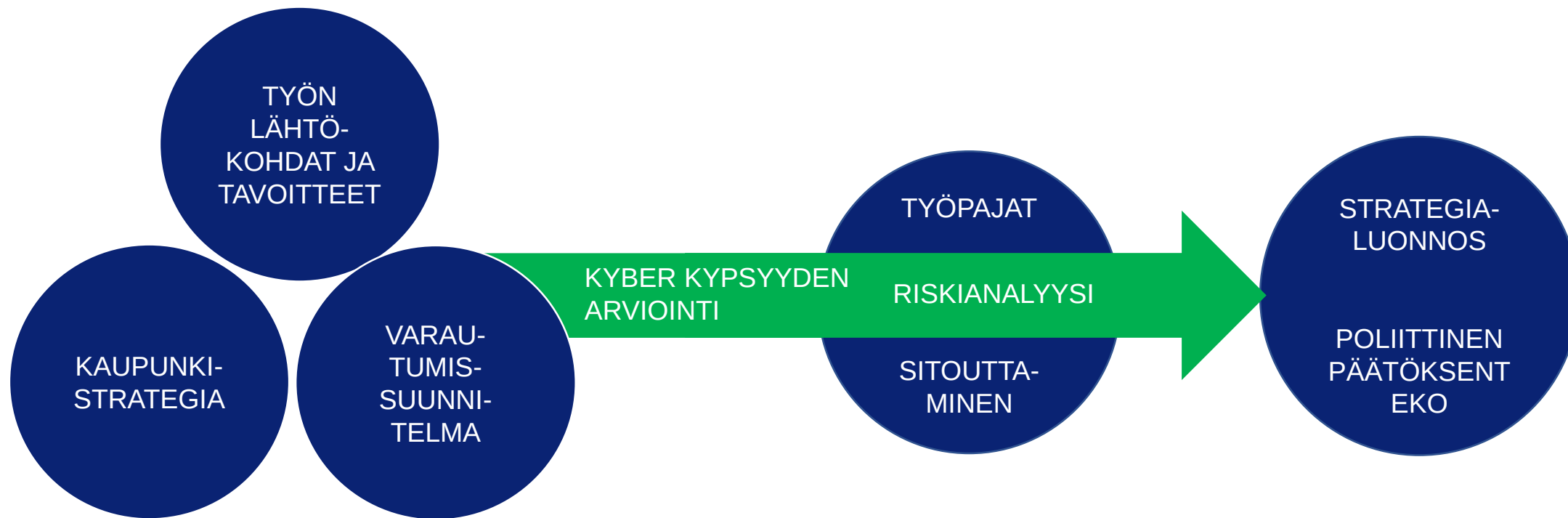
# KYBERTURVALLISUUDEN STRATEGISEN TYÖN LÄHTÖKOHDAT



# STRATEGIAPROSESSI



# STRATEGIATYÖN TIEKARTTA



# KYBERTURVALLISUUDEN KEHITTÄMISOHJELMA





- ✓ Jos 35-40% kyberuhkista pystytään torjumaan teknologisilla ratkaisulla
- ✓ Millä keinoin torjutaan loput 65 – 60% ?



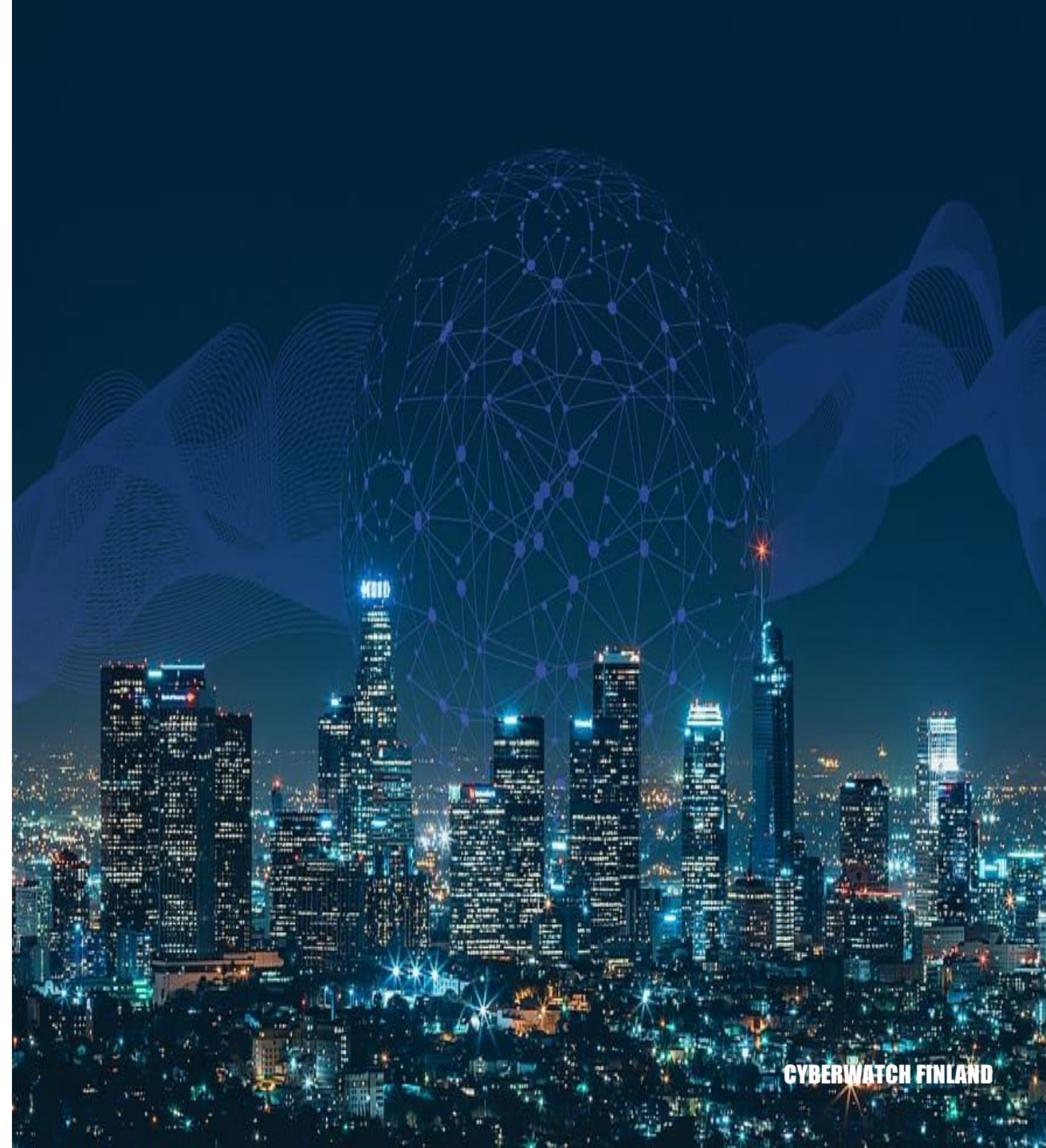
# ÄLYKAUPUNKI ÄLYRAKENNUS ÄLYKOTI

Älykaupunki, älyrakennukset ja älykoti tuovat hallittavaksi uusia tietoturvan, tietosuojan ja kyberturvallisuuden riskejä.

Digitalisaation hyötyjen täysimääräinen hyödyntäminen on mahdollista ainoastaan silloin, kun hallitsemme digiturvallisuuden osa-alueiden riskit.

Kokonaisuuden koordinointi ja vastuut.

Haasteeksi saattaa muodostua tietotekniikan ja operatiivisen teknologian integraation laajuuden ymmärtäminen.





## KYBERRISKIEN ”LUKUTAITO”

Ei tarkoita, että meidän kaikkien olisi oltava teknisiä asiantuntijoita.

Tarkoittaa, että meidän on kyettävä vahvistamaan yrityksemme ja organisaatiomme vastustuskykyä kyberriskeille, määriteltävä tavoitteet, jotka ovat tärkeimpiä kyberturvallisuusinvestointien ohjauksessa, ja kyettävä edistämään kyberturvallisuuden ja kyberkyvykkyyden kulttuuria.





# “SECURITY BY DESIGN” JA “ZERO TRUST”

Selkeät vastuut: suunnittelu, toteutus,  
ylläpito ja käyttäjä

Läpinäkyvyys: tunnettava toimittajat,  
osaaminen, ekosysteemi

Kyberturvallisuus osaksi kaikkia prosesseja:  
riskianalyysit, auditointi

Luotava parempi kyberturvallisuuskulttuuri

Johtaminen: ihmiset, toimintatavat ja  
teknologia



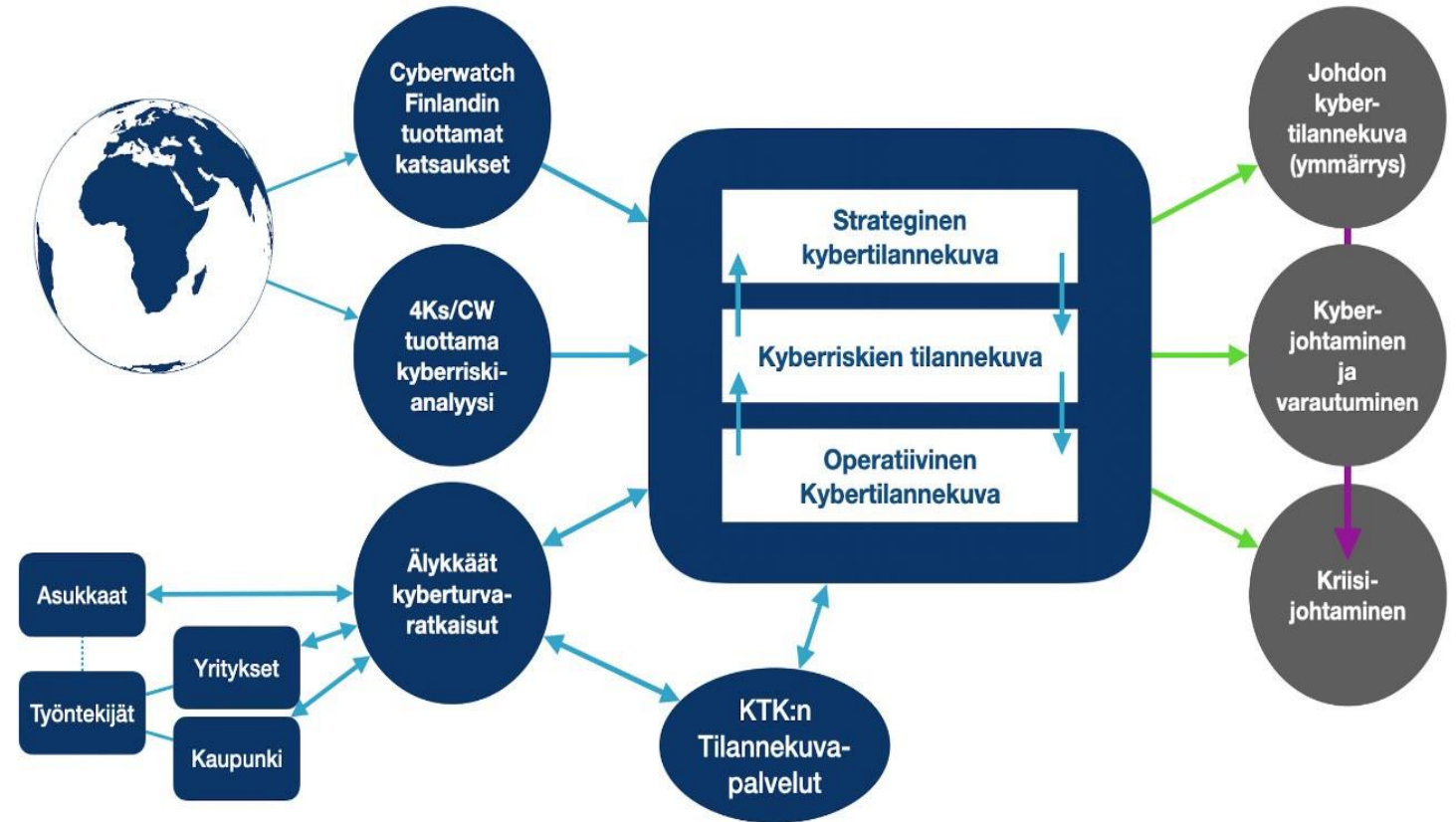


# KYBERTURVALLISUUDEN JOHTAMINEN JA YHTEISTOIMINNAN JÄRJESTELYT

Kybertoimintaympäristössä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan ennalta arvaamattomia. Kaupungin elintärkeisiin toimintoihin ja palveluihin kohdistunut kyberhyökkäys käynnistää aina kriisijohtamistoimenpiteet.

Kaupungin normaalia johtamisjärjestelmää kehitetään niin, että kyberhyökkäystilanteissa pystytään joustavasti nostamaan valmiutta ja aloittamaan kriisijohtamistoimenpiteet, joita tuetaan kokonaisvaltaisella kybertilannekuvalla.

Kokonaisvaltainen tilannekuva otetaan osaksi kaupungin johtoryhmätyöskentelyä ja poliittiset päättäjät informoidaan tilanteesta säännöllisin väliajoin. Samalla kehitetään tarvittavat välineet ja prosessit tilannekuva toiminnan käytännön toteuttamiseksi.



Kaupungin kybertilannekuva muodostuu strategisesta tasosta, kyberriskien tilannekuvasta ja operatiivisesta tasosta.

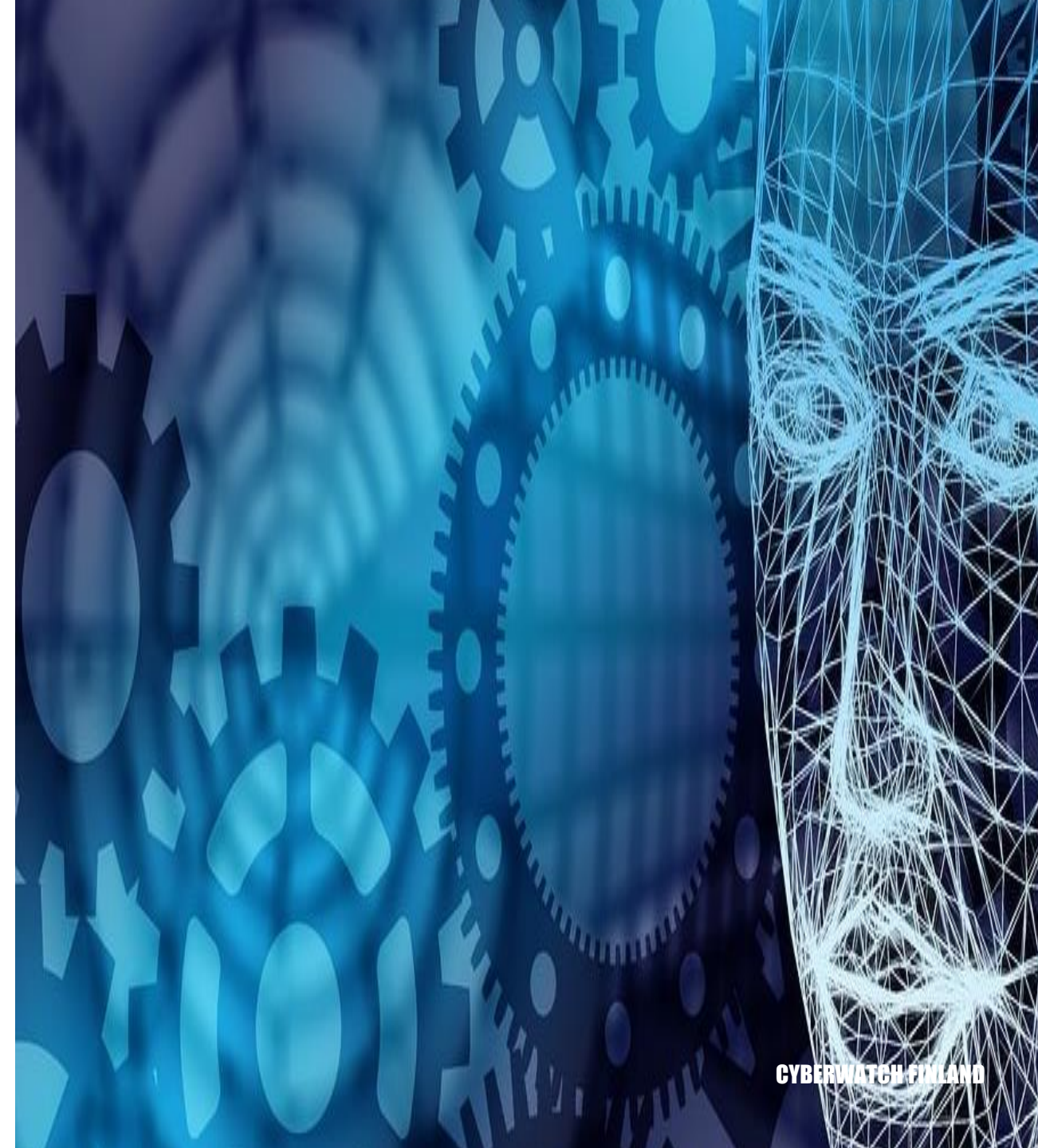
# KYBERRISKIANALYYSIN RAKENNE

- ✓ Selkeät strategiset tavoitteet ja ohjeet
- ✓ Kyberriski on mukana jokaisessa strategisessa riskissä
- ✓ Läpinäkyvyys ja ylemmän johdon tilannekuva
- ✓ Kyberturvallisuus osaksi kaikkia prosesseja:
- ✓ Kyberriskin seurannaisvaikutukset ovat merkittävämpiä kuin itse hyökkäys
- ✓ Johtaminen: ihmiset, toimintatavat ja teknologia



# ÄLYKKÄÄN ASUIN- YMPÄRISTÖN KRIITTISET TURVALLISUUS- RATKAISUT JA PALVELUT

- Suunnittelu ja ratkaisut?
- Uudet teknologia
- Verkkopalvelut
- Kameravalvonta
- Paikantaminen
- Ulkoistetut turvallisuuspalvelut





# KODIN ÄLYLAITTEET

Älykkäiden kodin laitteiden turvallisuus on yhtä kriittinen kuin kannettavien ja älypuhelimien turvallisuus - ja koska monet laitteet ovat asetusten muuttamisen kannalta vähemmän käyttäjäystävällisiä, saattaa muutoksen tekeminen vaatia vähän enemmän vaivaa.

Vaikka ei ole epäilystäkään siitä, että älykäs kaupunki, älykäs rakennus ja älykäs koti laitteineen helpottavat elämäämme ja nostavat asumismukavuutta, niin ne ovat myös erittäin helposti hakkeroitavissa.

Muistathan että vaikka sinä et kokisi olevasi kiinnostava hyökkäyskohde joku sidosryhmästäsi sitä saattaa olla tai työpaikkasi tai asiakasyritys jonka toimittajaketjussa toimitte.





# RIITTÄVÄTKÖ NYKYMALLISET TURVALLISUUS- RATKAISUT TULEVAISUUDESSA?

- Teknologian kehitys
- Valmiuden kasvattaminen
- Uudenlaisiin uhkiin valmistautuminen
- Osaamisen parantaminen
- Ekosysteemiajattelu
- Parempi yhteistyö
- Lainsäädäntö ajan tasalle



# Älykaupungin Kyberkulttuuri

**Kulttuuri** on kattotermi, joka kattaa yhteiskunnassa esiintyvän sosiaalisen käyttäytymisen ja normit, samoin kuin näiden yhteisöjen osaamisen, uskomukset, taiteet, lait, tavat, kyvyt ja käytännöt.

CYBERWATCH FINLAND

Johtajuus

Inhimilliset  
tekijät

Kyber-  
turvallisuus-  
strategia

**Kyber-  
kulttuuri**

Turvallisuus-  
kulttuuri

Turvallisuus-  
ympäristö

Tilannekuva

Kyber-  
hygieniä

OT-  
turvallisuus

Kyber-  
riskianalyysi



# MIKSI DIGILOIKATAAN

- Ympäristö
- Ilmasto
- Teknologian kehitys
- Kestävä kehitys
- Kustannussäästöt
- Kaupungistuminen
- Kasvaneet odotusarvot
- Parempi elämän laatu
- Luodaan arvoa ja kilpailukykyä



# MITEN DIGILOIKATAAN TURVALLISESTI

Kyberturvallisuuden hallinta tämän mittakaavan ympäristöissä, tulee sisältää perusteellisen riskinarvioinnin laatimisen koko toimitusketjun haavoittuvuuksien tunnistamiseksi.

- Tarkista laitteiden tietoturvaominaisuudet
- Toimi security by design konseptin mukaisesti
- Valitse kumppaneita, jotka ovat tietoturvallisiksi sertifioituja
- Aseta sopiva budjetti turvallisuudelle
- Asenna ohjelmisto haavoittuvuuksien hallitsemiseksi
- Varmista yhteistyö eri toiminnallisuuksien välillä
- Ymmärrä ekosysteemi kokonaisvaltaisesti, älä pelkästään asenna IT-ratkaisuja.
- Yhteistyö eri toimijoiden/osaajien välillä
- Uudista suunnittelutiimejä ja kerää parhaita käytäntöjä.
- Ota käyttöön jatkuvan oppimisen malli.
- Läpinäkyvyys





# KYBERTURVALLISEMPI SALO!

Kyberturvallisuusstrategia  
2021 - 2026

CYBERWATCH FINLAND



# STRATEGIA KOKONAISUUS:

- Kybertoimintaympäristön muutos
  - Kyberturvallisuuden visio
  - Kyberturvallisuuden johtaminen ja yhteistoiminnan järjestelyt
  - Kyberturvallisuuden kehittämisen päälinjaukset
  - Strategian toimeenpano
- 
- Kehittämisohjelma 2021-2026
  - Kokonaisvaltainen kyberriskianalyysi
  - Älykkäiden kyberturvaratkaisujen toteuttaminen

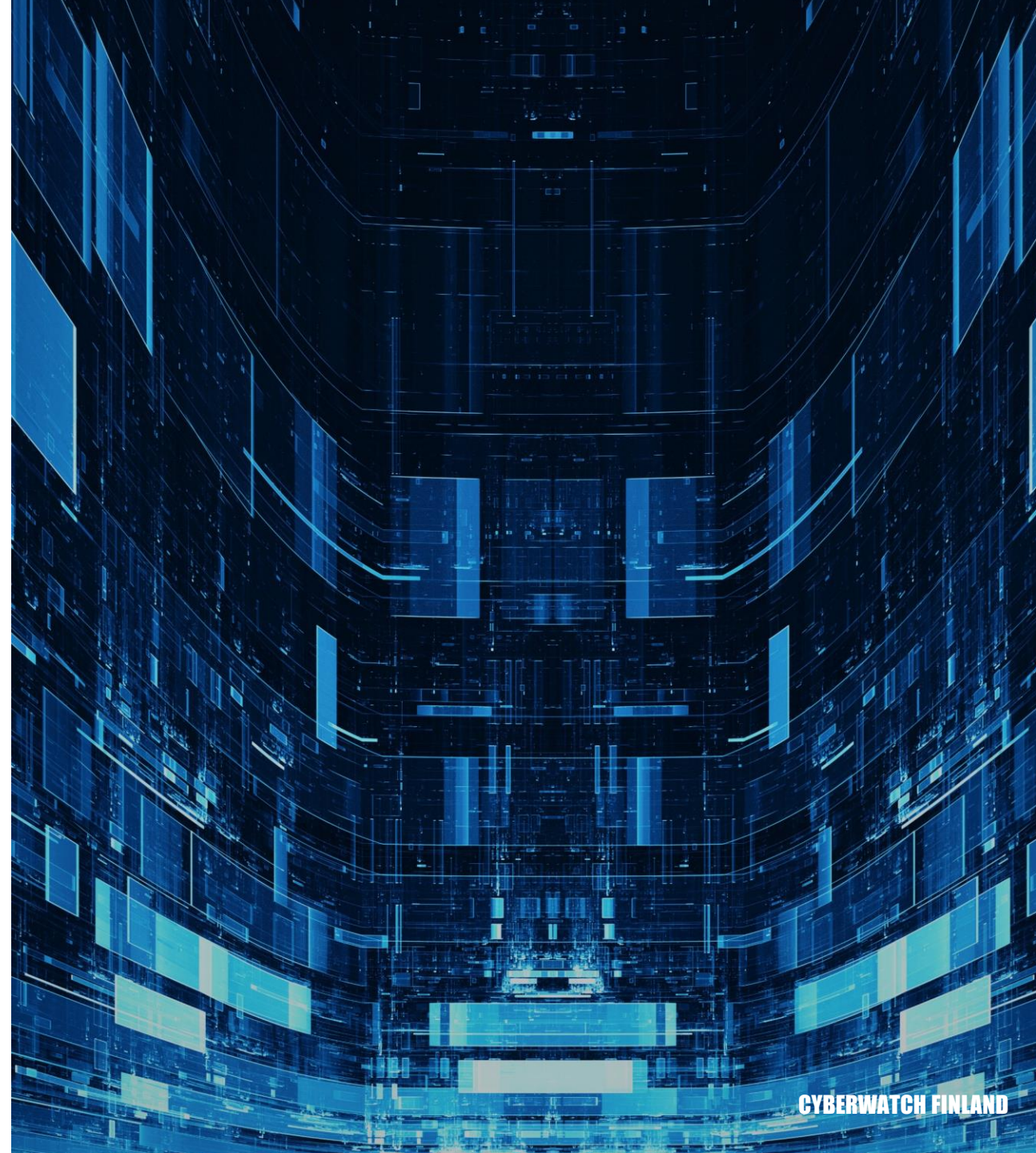




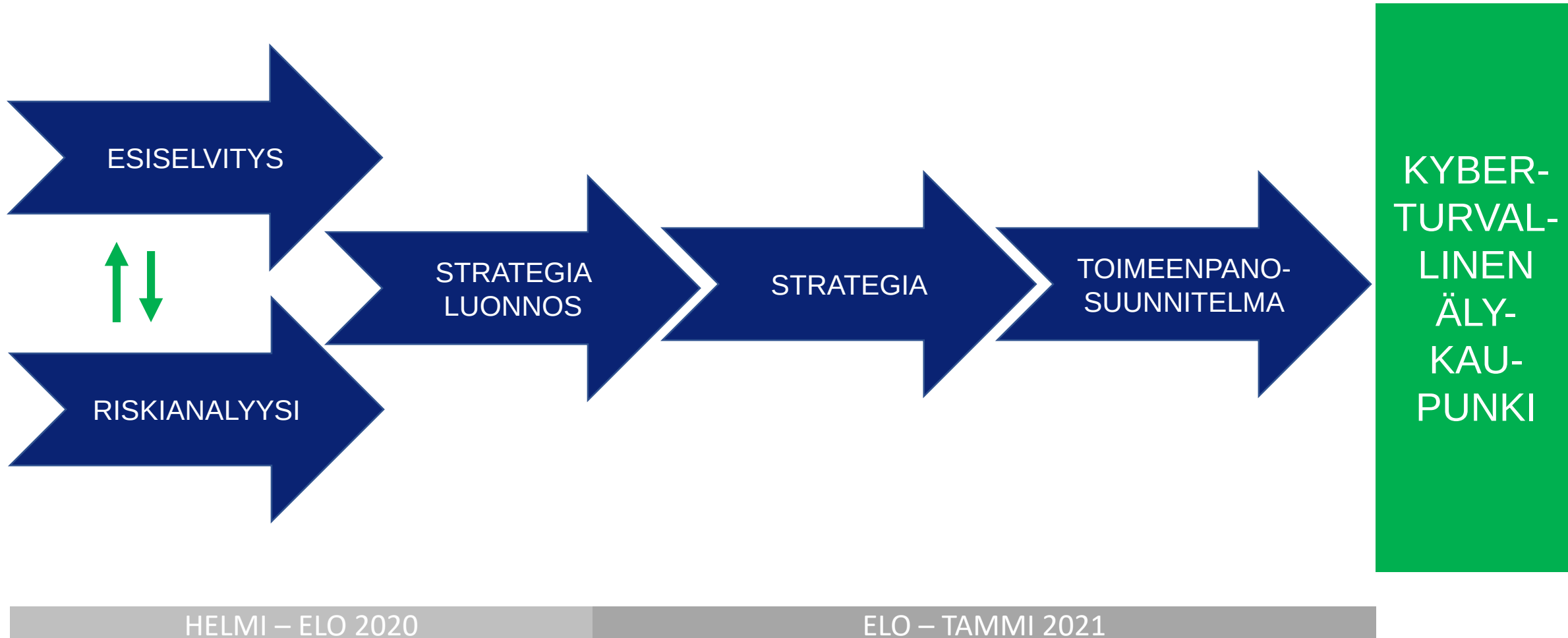
# **SALON KYBERTURVALLISUUS- STRATEGIAN TEHTÄVÄT JA KEHITTÄMISTOIMENPITEET:**

- Kaupungin johtaminen ja hallinto
- Hallintopalvelu (varautuminen ja kriisijohtaminen)
- Kaupunkikehityspalvelut
- Rakennus- ja ympäristöpalvelut
- Sivistyspalvelut
- Sosiaali- ja terveystyöpalvelut
- Talous- ja henkilöstöpalvelut
- Alueen yritykset ja sidosryhmät (yhteistoiminta)

**KYBERUHKAT - KYBERRISKIT – HAAVOITTUVUUDET –  
SUORITUSKYKYPUUTTEET → OSAAMINEN –  
TOIMINTATAVAT – TEKNOLOGIA**

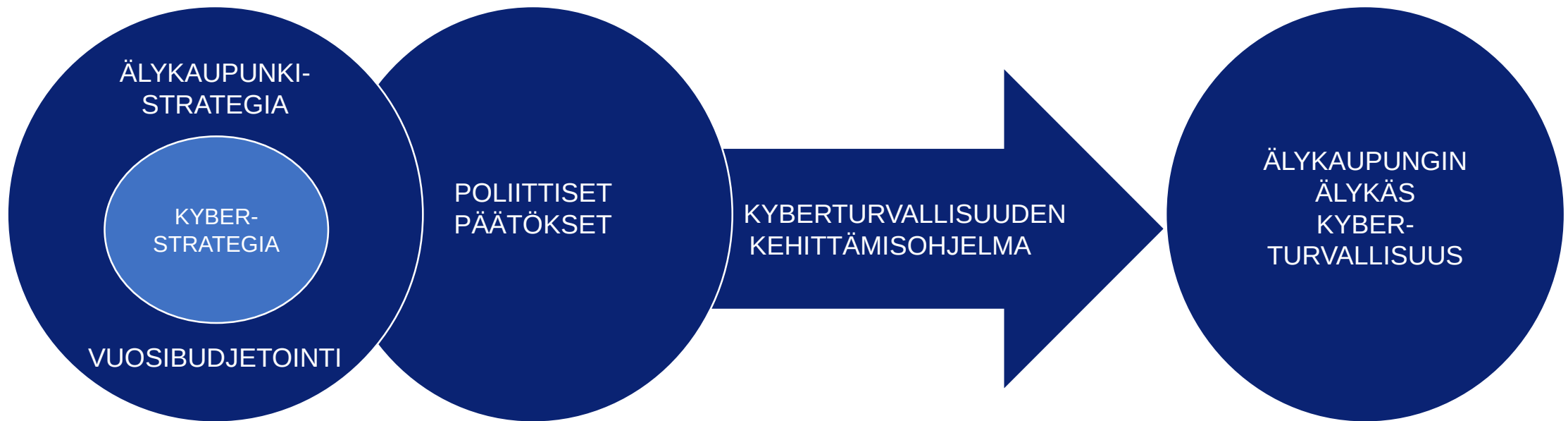


# SALON KAUPUNGIN KYBERTURVALLISUUSSTRATEGIA PROSESSINA





# ESITYS JATKOTOIMENPITEIKSI





Kiitos !

[aapo@cyberwatchfinland.fi](mailto:aapo@cyberwatchfinland.fi)  
[www.cyberwatchfinland.fi](http://www.cyberwatchfinland.fi)