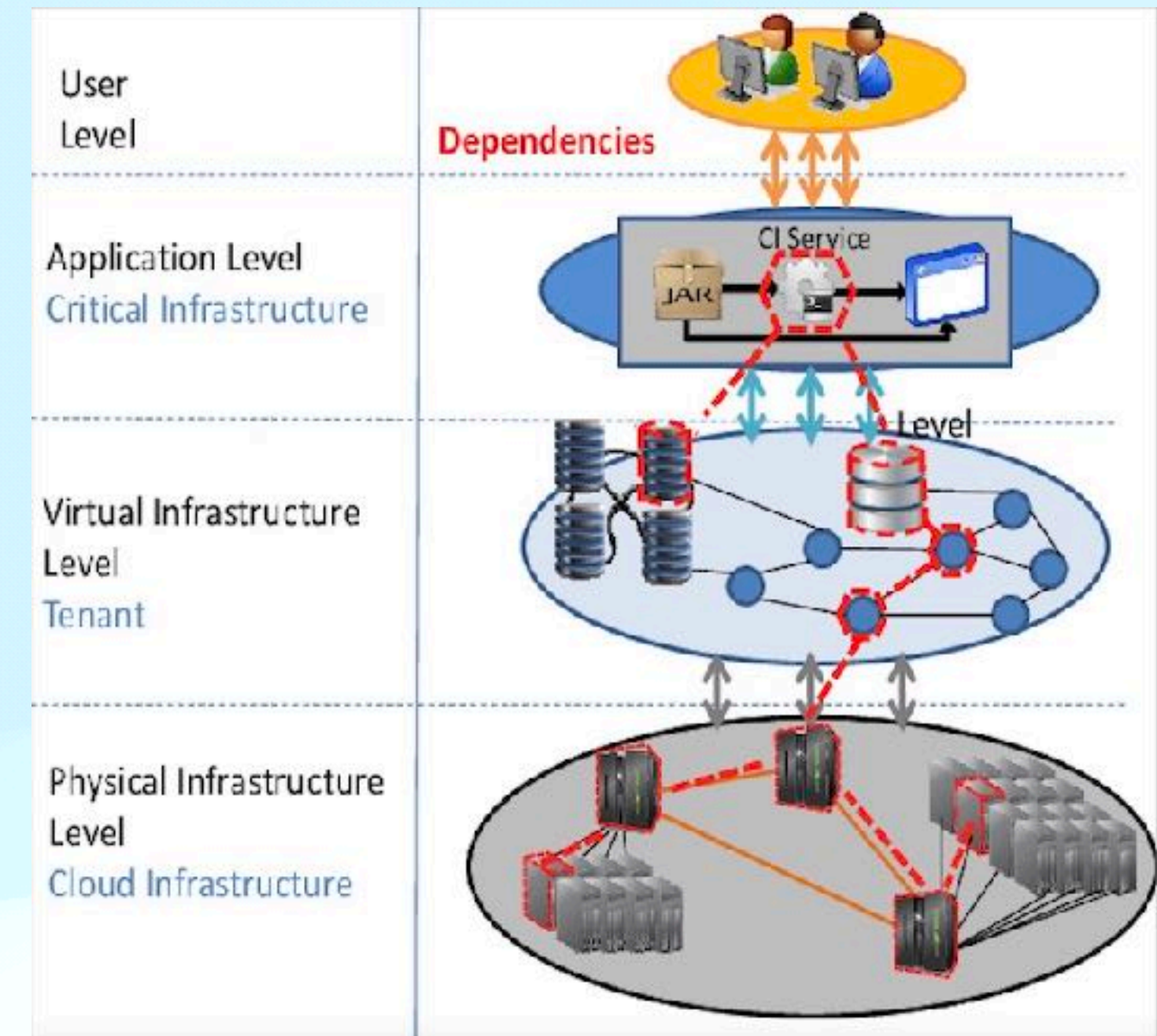


On yhteenvedon aika ...

Tietoturvan historia; Pilvipalvelut; Resilienssi; Tekoäly;



Kristian Salmi syyskuuta 12.09.2024

Kuka on Kristian Salmi?

CV

- Valmistunut 1972 peruskoulusta (keskikoulu) ja siirtynyt työelämään
- Tehnyt tehnyt työtä vuodesta 1975 konttoritekniikan parissa
- Rank Xerox 1975 - 1991 huollossa ja myynnin tuessa (mm. Viewpoint 8000 toimistojärjestelmät ja myynnin tukitoimet pienille ja keskisuurille laserkirjoittimille)
- Savonlinnan Ammattikurssikeskus 1992 mikrotukihenkilön koulutus
- Taloushallinnon merkonomitutkinto 1997-2000
- ATK suunnittelijana ja tietoturva-vastaavana 1992-2020 maa- ja metsätalousministeriön ja työ- ja elinkeinoministeriön hallinnon aloilla
- Eläkkeellä vuodesta 2020



**Mitä yhteenvedolla haetaan ..
Malware history - Resilience - Cloud - AI**

Mitä yhteistä näillä teemoilla on?

Pistetään yhteen...

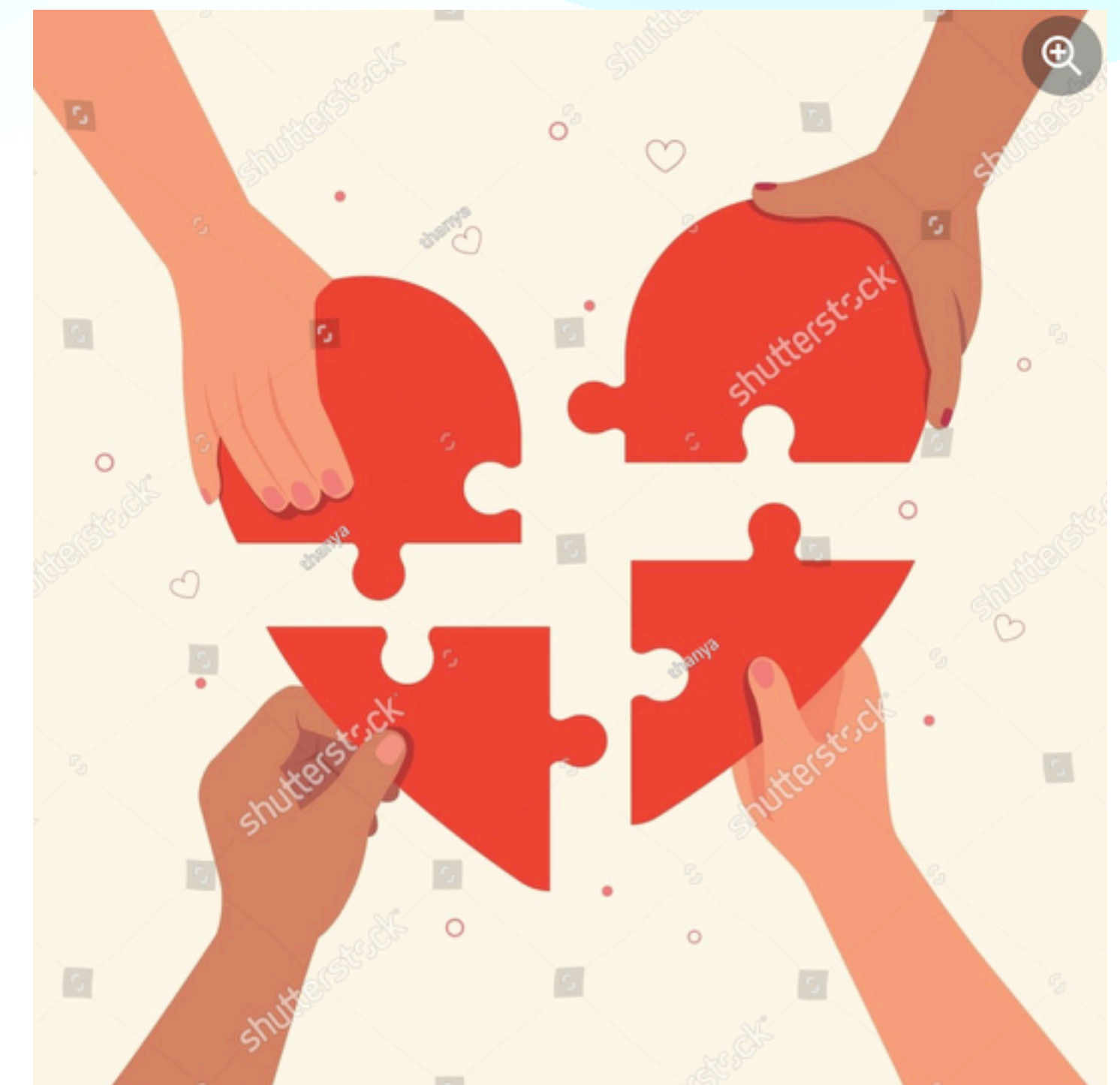
**Mitä yhteistä edellämainituilla asiakokonaisuuksilla voisi olla...
(Tietoturvan historia; Pilvipalvelut; Resilienssi; Tekoäly;)**

Kaikki aiheet voivat kohdistua yksittäiseen laitteeseen tai verkkoon tai palveluun tai jopa tietokonesaliin ja peräti kokonaisen maan informatio-teknologiaan?

Miten aiheet voidaan (pitäisi) vetää yhteen?

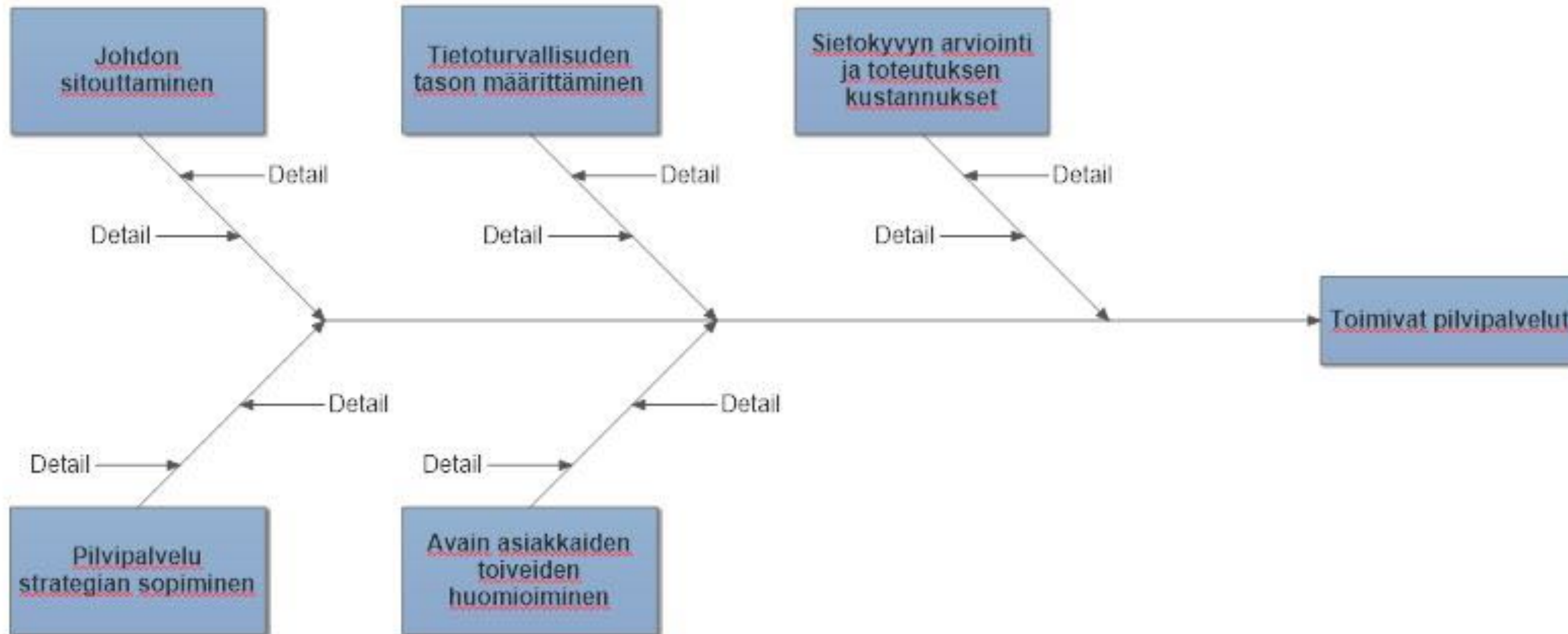
Mitkä ovat yhdistävät tekijät?

Tarvitsemmeko jotain lisää, joka voisi yhdistää nämä aiheet?



Tavoiteeni oli siis kuvata

Toimiva ja turvallinen moderniin teknologiaan perustuva tietopalvelu-ympäristö...

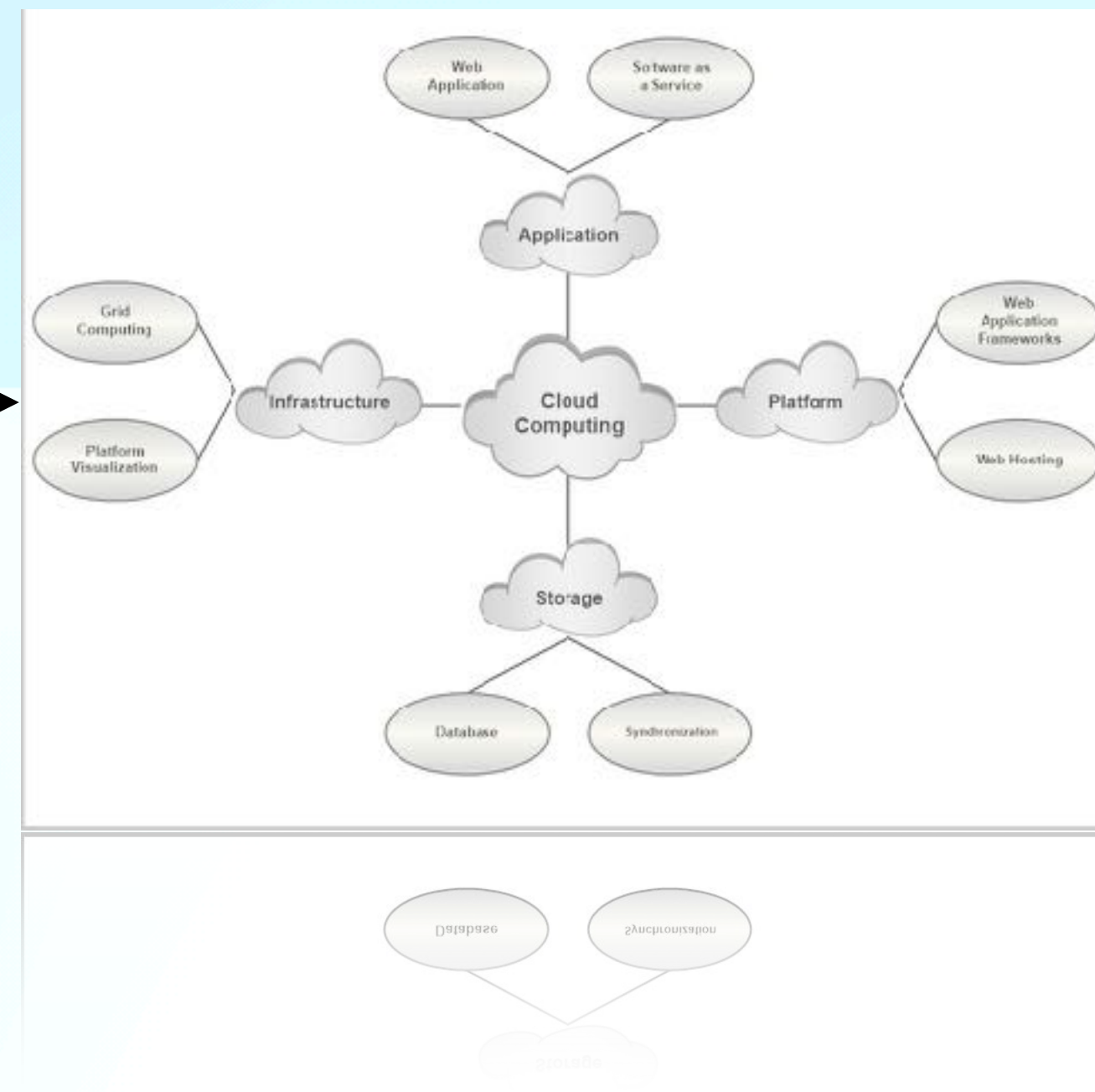


Mitä pilvipalvelut sisälsivät 2020? Riittääkö tämä?

2030-luku?

2000-luku

2020-luku





Johdon sitouttaminen...

Tämä niin tuttu aihe...

COBIT 5.0



Mikä COBIT?

COBITIN historiaa...

- Miksi nykyinen nimi on "COBIT", eli "Control Objectives for Information and Related Technology" tai COBIT, miten tämä kehys sai alkunsa?
- COBIT julkaistiin ensimmäisen kerran 1990-luvun puolivälissä. Tuolloin COBIT keskittyi pääosin tilintarkastukseen ja ***auttoi erityisesti tilintarkastajia IT-ympäristöissä navigoinnissa*** (auditoinnissa). Se on sittemmin mennyt auditointia pidemmälle. Kolmannessa versiossaan ISACA lisäsi COBITiin johtamisohjeet.
- Versiossa 4 ohjeistoon lisättiin myös ICT-hallinta. Nykyisessä vuonna 2019 julkaistussa versiossa tietohallinto ja sen rooli liiketoiminnan menestymisessä sekä yritysriskien hallinta korostettiin entistä enemmän, ja ITIL lisättiin siihen.

Mikä on cobit?

Siis mitä sillä tehdään?

COBIT 5.0 on viitekehys, joka auttaa organisaatioita ohjaamaan ja hallitsemaan tietotekniikkaa tehokkaasti. Se tarjoaa periaatteet, käytännöt, työkalut ja mittaamisen keinot tietotekniikan hallintaan. COBIT 5.0 auttaa organisaatioita saavuttamaan liiketoimintatavoitteenensa ja varmistamaan, että IT-tuotteet ja -palvelut ovat laadukkaita ja turvallisia. Tämä viitekehys auttaa organisaatioita optimoimaan tietotekniikan käytön ja vähentämään riskejä.

COBIT 5 viitekehys

Mikä on COBIT viitekehys ?

COBIT 5.0:ssa on viisi peruseriaatetta eli viitekehystä, jotka ohjaavat organisaatioiden tietotekniikan hallintaa. Nämä periaatteet ovat:

1. **Tietotekniikan hallinnan tehtävät ja tavoitteet:**

- Auttaa organisaatiota saavuttamaan strategiset tavoitteet tietotekniikan avulla.
- Varustaa organisaation johto tehokkailla työkaluilla ja prosesseilla IT:n hallintaan.

2. **Organisaation tietotekniikan hallinnan kehys:**

- Tarjoaa rakenteen organisaation tietotekniikan hallinnalle.
- Määrittelee vastuut, prosessit ja käytännöt IT-hallinnalle.

3. **IT-hallinnon suuntaaminen:**

- Ohjaa organisaatiota kohti tehokasta ja strategisesti kohdistettua IT-hallintaa.
- Auttaa varmistamaan, että IT tukee organisaation liiketoiminnan tavoitteita.

4. **IT-hallinnan toteutus:**

- Käsittelee käytännön toteutusta ja toimintaa IT-hallinnassa.
- Ohjaa resurssien käyttöä, suorituskyvyn hallintaa ja riskien hallintaa.

5. **IT-hallinnan arviointi:**

- Tarjoaa keinoja arvioida ja seurata IT-hallinnan tehokkuutta ja toimivuutta.
- Auttaa organisaatiota parantamaan jatkuvasti IT-prosessejaan ja toimintaa.

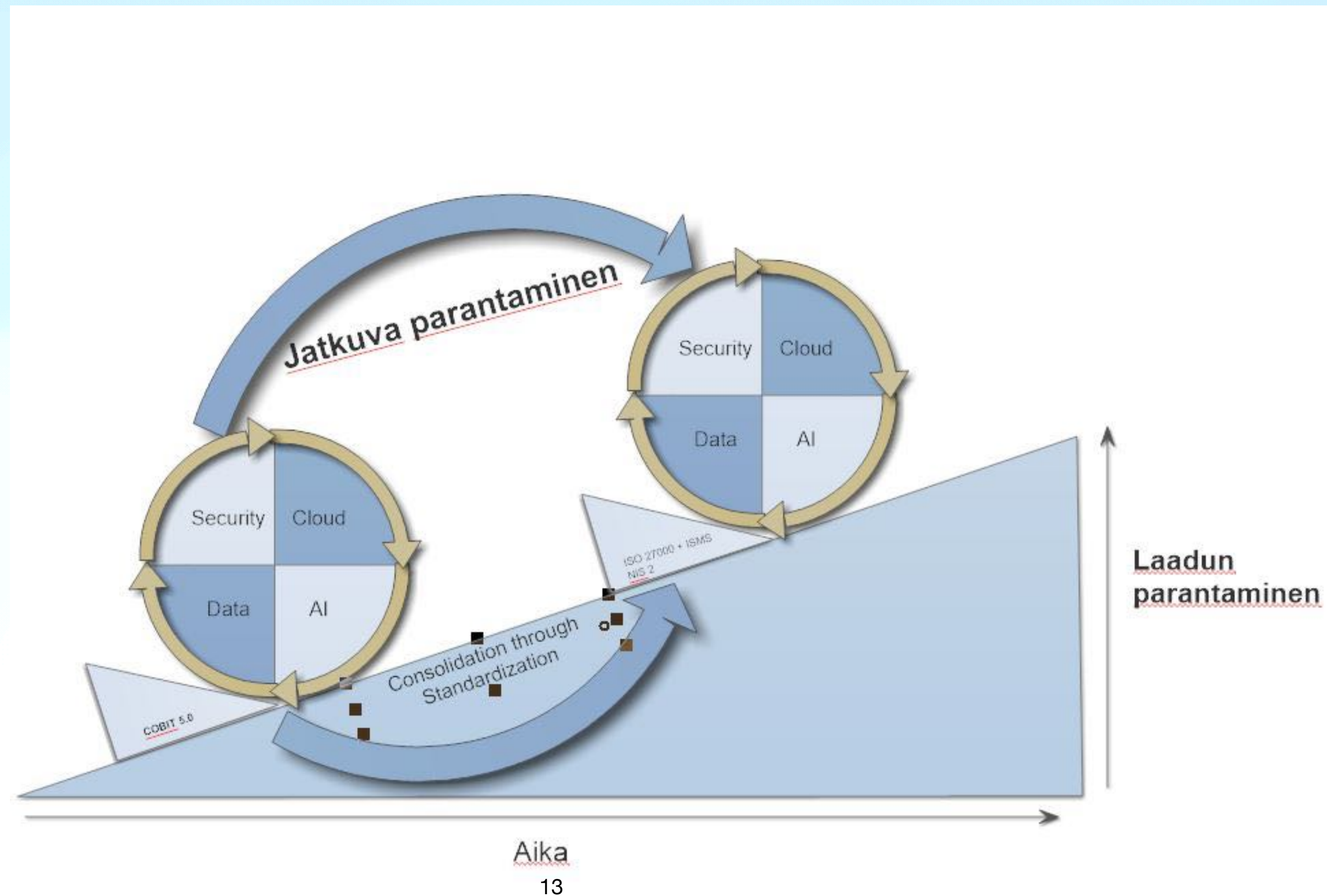
Muut viitekehykset?

Mitä niitä olikaan?

- Entäs ITIL (2019 jälkeen COBIT:in mukana) Information Technology Infrastructure Library ja ITGI Information Technology Governance Institute?
- Onhan näitä
- Jos halutaan tehdä hyvä tietojärjestelmäkokonaisuus niin siihen löytyy kyllä työkalut (viitekehykset) A = yllin B = kyllin
- NIS II on tuleva "base standard" Hyvin tehtynä **KAIKKI** muut ISO standardien noudattaminen helpottuu ja yksinkertaistuu (esim. ISO 27017 ja ISO/IEC 22123-3:2023 SFS-ISO/IEC 19086-1:2017 pilvipalvelun tarjoajille)

Jatkuva parantaminen ,,

Pitää viedä standardien mukainen toiminta eteenpäin ja nostaa tasoa ylemmäksi, pysyvästi.
Standardien seuraaminen ja toteuttaminen antaa ymmärtämystä ja rahaa ja turvallisuutta! Sertifiointi vain kokonaistyön 'mitali ja kukkapuska'.



Tietoturvan taso

Pitää olla kiinteästi yhteydessä muuhun resilienssiin ..

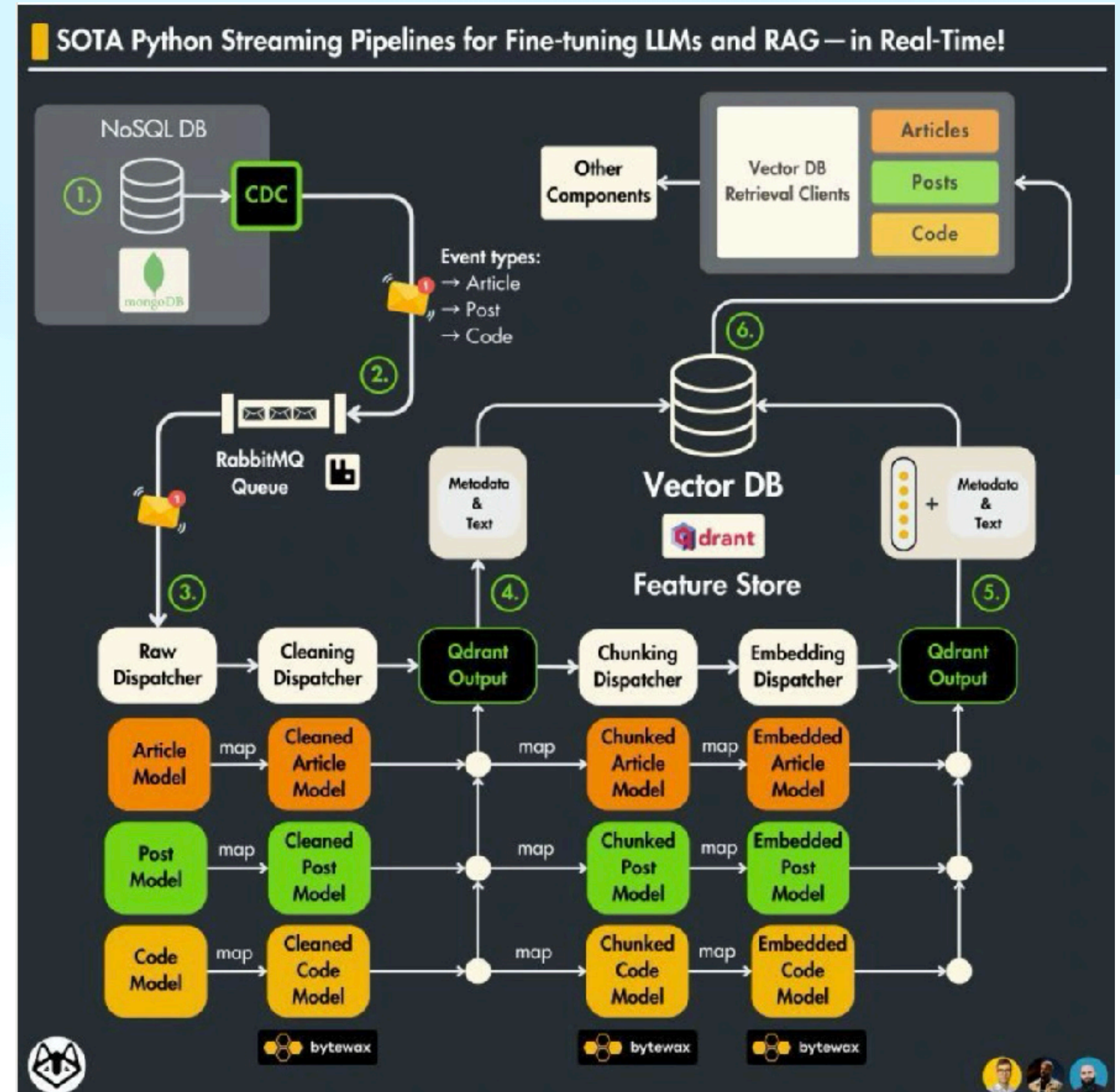
- 25 haittaohjelmatasoa (kokonaisuutta) olemassa
 - (Sisältää lukemattomia, tuhansia alatasoja < versioita >)
 - Kaikki APT 10 - APT XX huomioitava (pitkäaikaisia rahoitettuja toimijoita)
- Rosvot käyttävät näitä uudelleen korjattuina / muunneltuina noin 3 - 5 vuoden välein!
- Vaatii 24/7 valvonnan! (AI valvonta ja analysointi paras, kattavin ja turvallisin)

Resilienssi

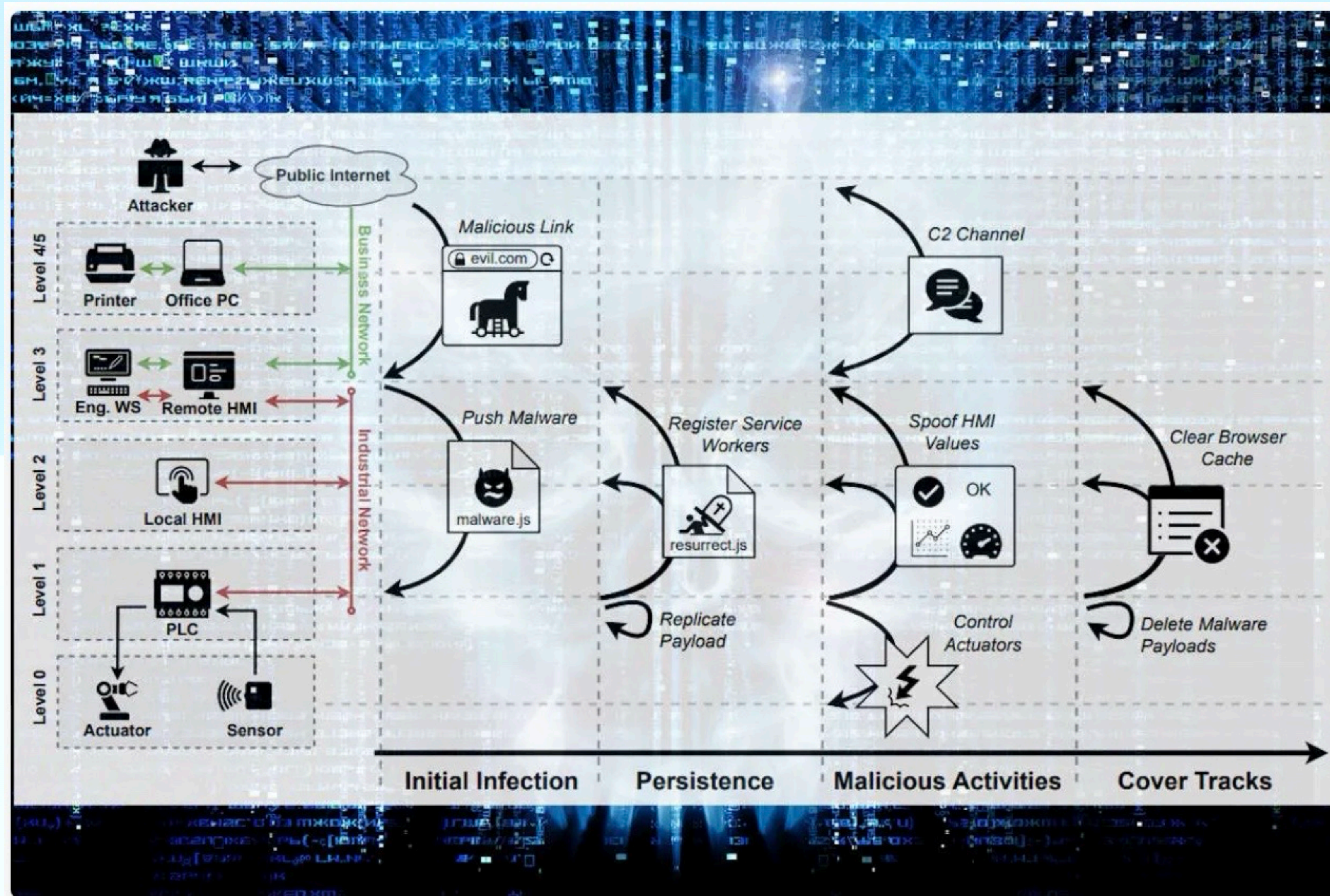
Vaatii teknisen kokonaisuuden uudelleen ajattelemisen ja toteutuksen

- **COBIT:in** tuomien johdon rajaukset ja vaatimukset huomioon ottaminen
- **NIS II (ISO 27001 ja 2 + ISMS)** läpivienti ajatuksella ja pieteetillä.
- Sertifiointi !! EI SAA OLLA TAVOITE !! se on tulos (palkinto) **oikeasta toiminnasta!**
- Saadaan aikaan pilvipalvelukokonaisuus, joka sisältää valmiiksi automaattisen valvonnan toiminnasta ja virhesietokyvyn
- Ymmärtää käsittelyssä olevan datakokonaisuuden tavoitteet
- Huolehtii sujuvasti pilven rakennekokonaisuuden yhteenkuuluvuudesta muihin sidosryhmiin ja niiden tarjoamiin palveluihin sujuvasti

Mitä tietokantatyyppejä on käytössä ja mahdollisesti tulee käyttöön



Mitkä vihollisten tiedonriisto-ohjelmakokonaisuudet ovat tyypillisiä tiedollemme



Uudet, uusittavat tai korjattavat OSI-kohteet 2020 luvulla (**kakkosesta seiskaan**)



Toimintamalliehdotus

Miten edetä (walk through)



- **COBIT** (Halutaan taata johdon mukaantulo ”Stake holder”)
- **NIS II + ISMS** (käydään läpi nykyinen ja / tai tuleva tiedon rakenne)
- Päätetään käyttöön tulevan **pilvipalvelun rakenne (esim. multcloud)**
- Käydään läpi **palvelualustat + (XXX aaS)**
- Käydään läpi kaikki **yhteystarpeet ja luodaan käytettävä SASE-malli**
- Luodaan **kattava 24 / 7 toimiva käytönvalvonta ja turvatoimet**
- Siirryttäessä pilvipalveluihin **ei oteta** vanhoja ohjelmistoja mukaan ...eihän?

Loppukaneetti.....

Näinkin ”erikoisista” asiakokonaisuuksista löytyy yhteinen toimiva kokonaisuus?

- Miksi?
- Miksi uusiminen / siirtyminen kannattaa tehdä **pohjamutia myöten?**
- **Miksi kannattaa datan kautta uusia tiedon käsittely pilveen siirryttäessä?**
- Miksi **COBIT + NIS II (+ ISMS)** voisi olla hyvä yhdistelmä lähtökohtana?
- Miksi tavoitteena pitää olla **kokonaan modernisoitu** toimintaympäristö?
- Miksi **tekoälyn osuus uudessa ympäristössä on niin keskeinen?**
- Miksi **tekoälyn osuus ympäristön suojaamisessa ja ylläpidossa on niin keskeinen?**

Uutisia kotimaasta

SITRA esitti kesäkuun 2024 lopussa, että julkishallinto voisi säästää noin 2 miljardia atk-menoistaan..

- Säästöt tulisivat siitä, että järkipästäisiin datan käyttöä ja lisättäisiin yhteisiksi luonnehdittavia palveluita(henkilö-, paikka- ja yritystiedot).
- Säästöt syntyisivät siitä, että järjestelmiä olisi merkittävästi vähemmän ja käytössä oleva yhteinen data tarjottaisiin keskitetysti.
- >> Vastaus tuli välittömästi. Mm KELA ja THL vastusti ehdotusta vahvasti! ”Järjestelmät toimivat nyt hyvin” !! <<
- **!!!** Ei toimivia järjestelmiä suositella lopetettaviksi **!!!** Niiden toimintaa järkipästäisiin. Vähemmän tautofoniaa tallennetussa datassa ja turvallisuuden lisäystä **!!!**
- Kun toimivia järjestelmiä olisi vähemmän mm. käytössä säästyisi energiaa **!!!** Ja ylläpidon vastuut selkenisivät..

Uutisia maailmalta kesä 2024

Miten tällaisiin uutisiin tulisi reagoida?



Microsoft Azure Globally Down –
What's Happening!

Muuta keskustelua herättävää

- Teknisen velan kuormat?
- Julkisen hallinnon yhteydet valvottaviin kohteisiin (esim. Hukkajoki, Vastaamo, Helsingin kaupungin tietovuodot)?
- Julkishallinnon sirpaleisuus?
- Toimitusketjujen hallinta (crowdstrike)?
- Turhan työn tekeminen ja teettäminen?
- Tekoälyn osittelu?
- Teollisuuden ja energiatuotannon kytkökset talouteen ja hallintoon (IOT2B)
- Windows Server 2025? (Legacy (stand alone) versio)?

Tämän esityksen lähdetiedot

Tieto kerätty vapaasta internetistä, muun muassa ->

- Techrepublic
- Technopedia
- The Hacker News
- Bleeping computer
- academia.edu
- Microsoft
- Google
- AWS
- ISACA



Kiitoksia mielenkiinnosta

