Tietoturvallisuuden standardit ja hyvät käytänteet

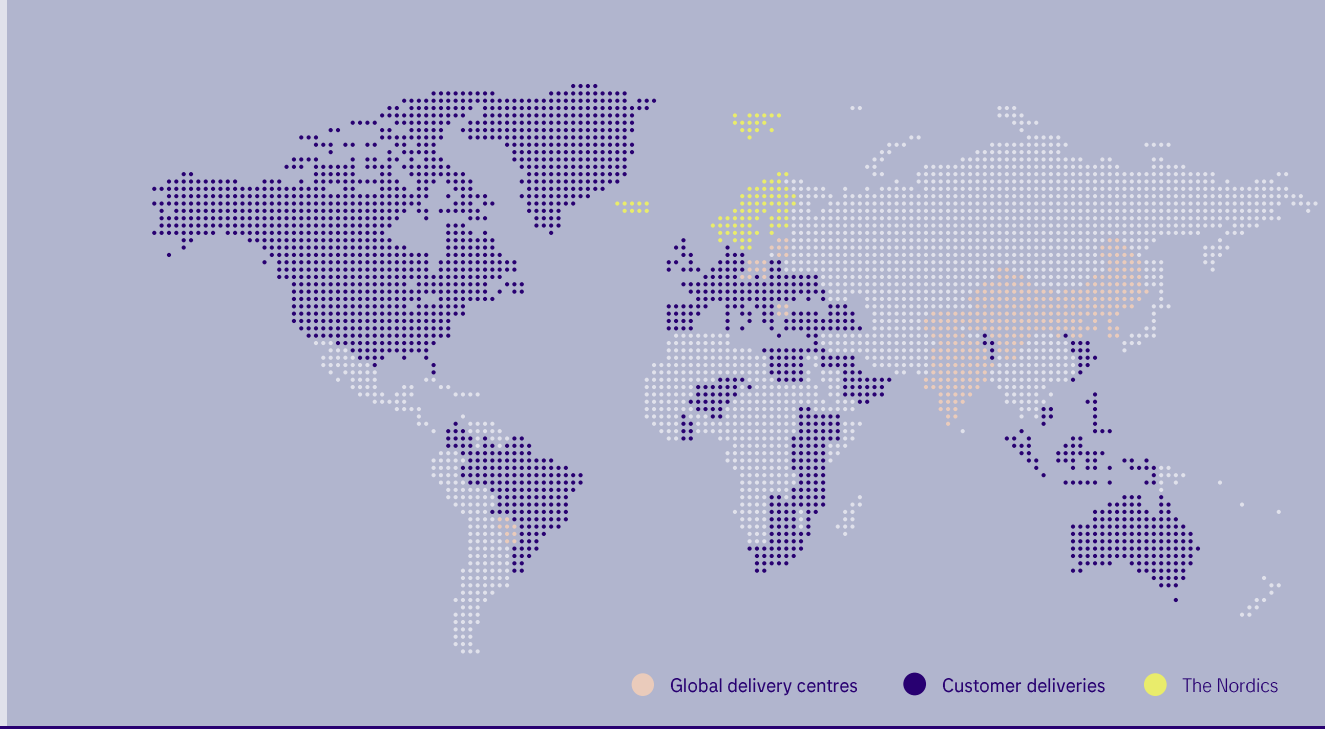
Kyberala murroksessa –seminaari 23.1.2024

Jari Pirhonen
Security Lead, Finland
Tietoevry Tech Services

X: @japi999
Bluesky: @japi.bsky.social

tietoevry

We are developers of digital futures



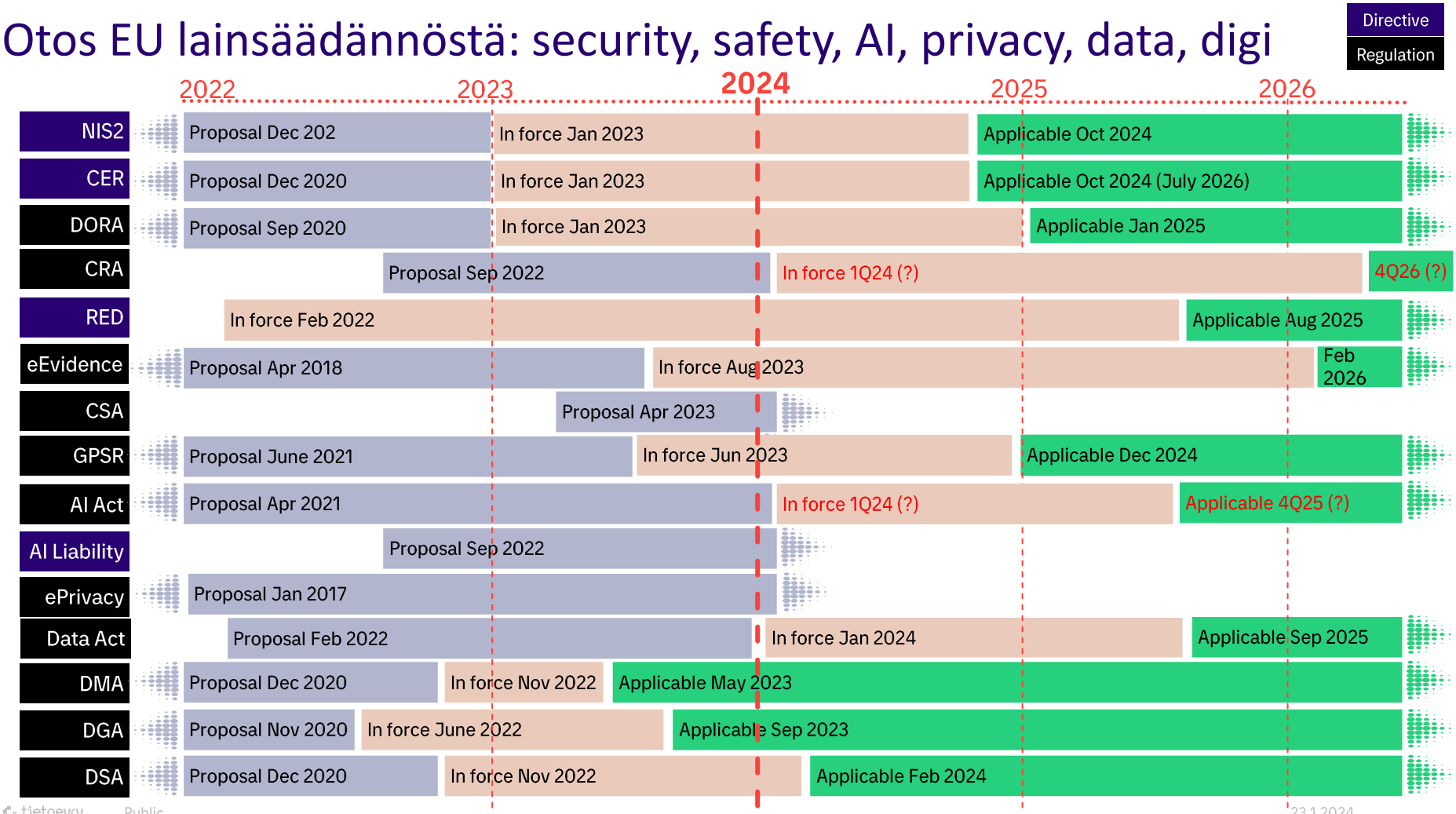
Over **24 000** professionals globally

More than **10 000** customers

Serving customers in over **90** countries worldwide

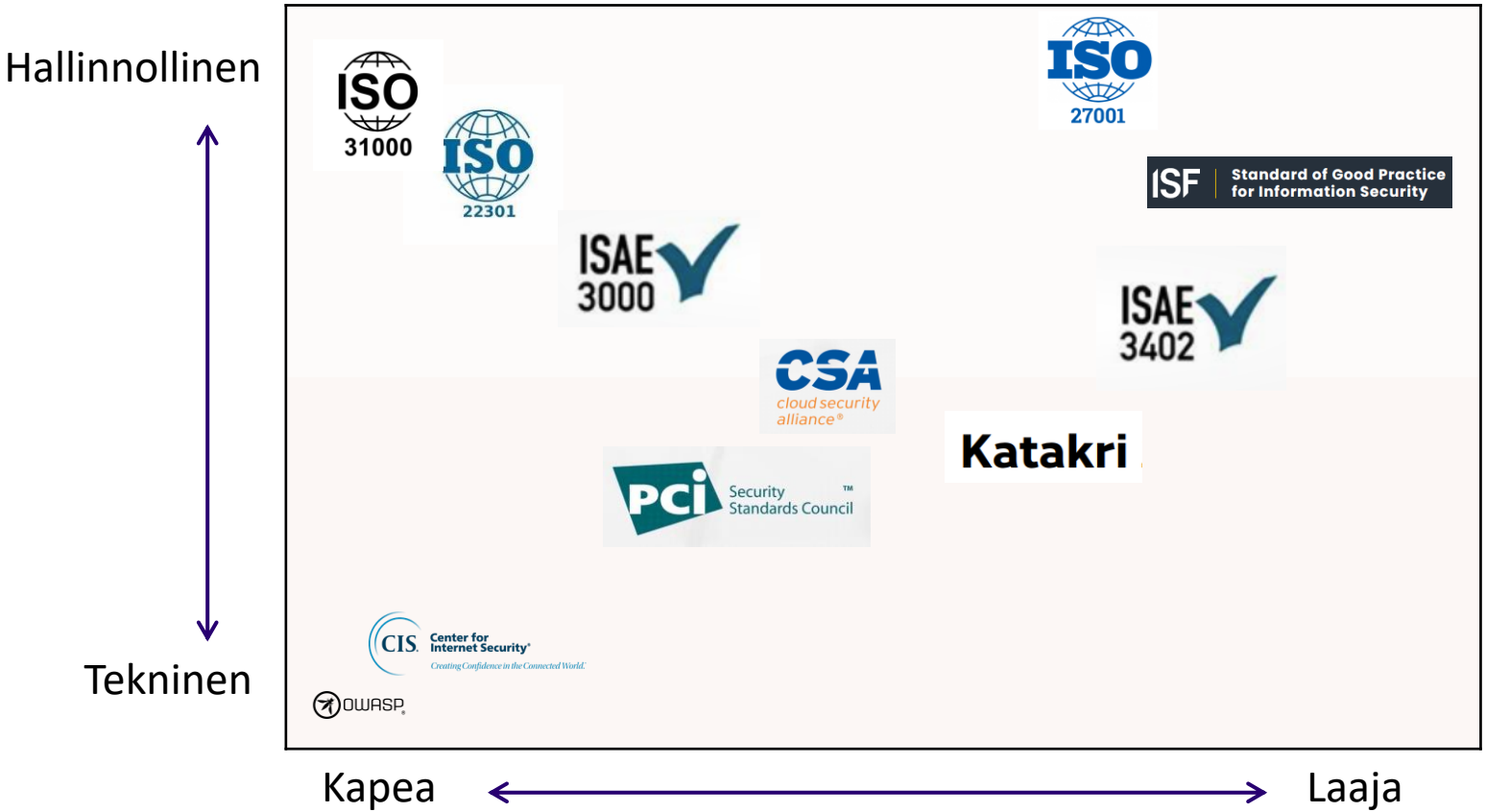
Annual revenue approximately **EUR 3 billion**

Otos EU lainsäädännöstä: security, safety, AI, privacy, data, digi



Katso myös https://iki.fi/japi/2023/12/ready-or-not-eu-legislation-will.html

Käytössämme olevia tietoturvastandardeja ja -viitekehyksiä



Käytössämme olevia tietoturvastandardeja ja -viitekehyksiä

- **ISF Standard of Good Practice for Information Security**
  - Konsernin tietoturvan hallintaa **ohjaava** standardi ja sitä tukeva kypsyysarviointimittari
- **ISO 27001**
  - Konsernin tietoturvan hallintajärjestelmän **sertifiointiin** käytettävä standardi (soveltuvuuslausunnossa kaikki kontrollit)
  - https://www.tietoevry.com/en/about-us/iso-certificates/
- **ISAE 3402**
  - Tietoturvaprosessit varmentavien kontrollien (100+ kpl) kattavuuden ja toimivuuden **varmistaminen** valituissa liiketoimintayksiköissä
- **ISAE 3000**
  - Tietosuojaprosessit varmentavien kontrollien kattavuuden ja toimivuuden **varmistaminen** valituissa palveluissa (tietojen käsittelijän rooli)
- **CSA STAR**
  - Pilvipalvelualustojen **sertifiointi** (edellyttää ISO 27001 sertifikaattia)
- **PCI DSS**
  - Korttitietoja käsittelevien palvelualustojen **sertifiointi**
- **ISO 22301 Continuity Management**
  - Yhden liiketoimintayksikön valittujen palveluiden jatkuvuuden hallintajärjestelmän **sertifiointi**

- **ISO 31000**
  - Konsernin riskienhallintaa **ohjaava** standardi
- **CIS tietoturvakontrollit**
  - Teknisten alustojen (Windows, Linux, etc.) tietoturvakonfiguraatioiden **arviointi**
- **Katakri**
  - Viranomaisten luokitellun tiedon turvallisuusjärjestelyjen riittävyyden **arviointi** asiakasvaatimusten mukaisesti
- **OWASP**
  - Sovelluskehityksen **tietoturvaohjeita**
- **Muita ISO sertifiointeja**
  - ISO 9001 laadunhallintajärjestelmä
  - ISO 20000-1 IT palvelunhallintajärjestelmä
  - ISO 14001 ympäristöasioiden hallinta
  - ISO 13485 terveydenhuollon laitteet ja tarvikkeet – johtamisjärjestelmä
- **Lisäksi**
  - Sisäiset auditoinnit
  - Asiakkaiden teettämät auditoinnit

Not everything that happens happen for a reason, but everything that survives survive for a reason.
-- Nassim Nicholas Taleb