Digitalisaation turvallisuus yrityksen hallitustyön, strategian ja riskienhallinnan ytimessä

Tuomo Haukkovaara
Hallituksen puheenjohtaja
IBM Finland
tuomo.haukkovaara@fi.ibm.com

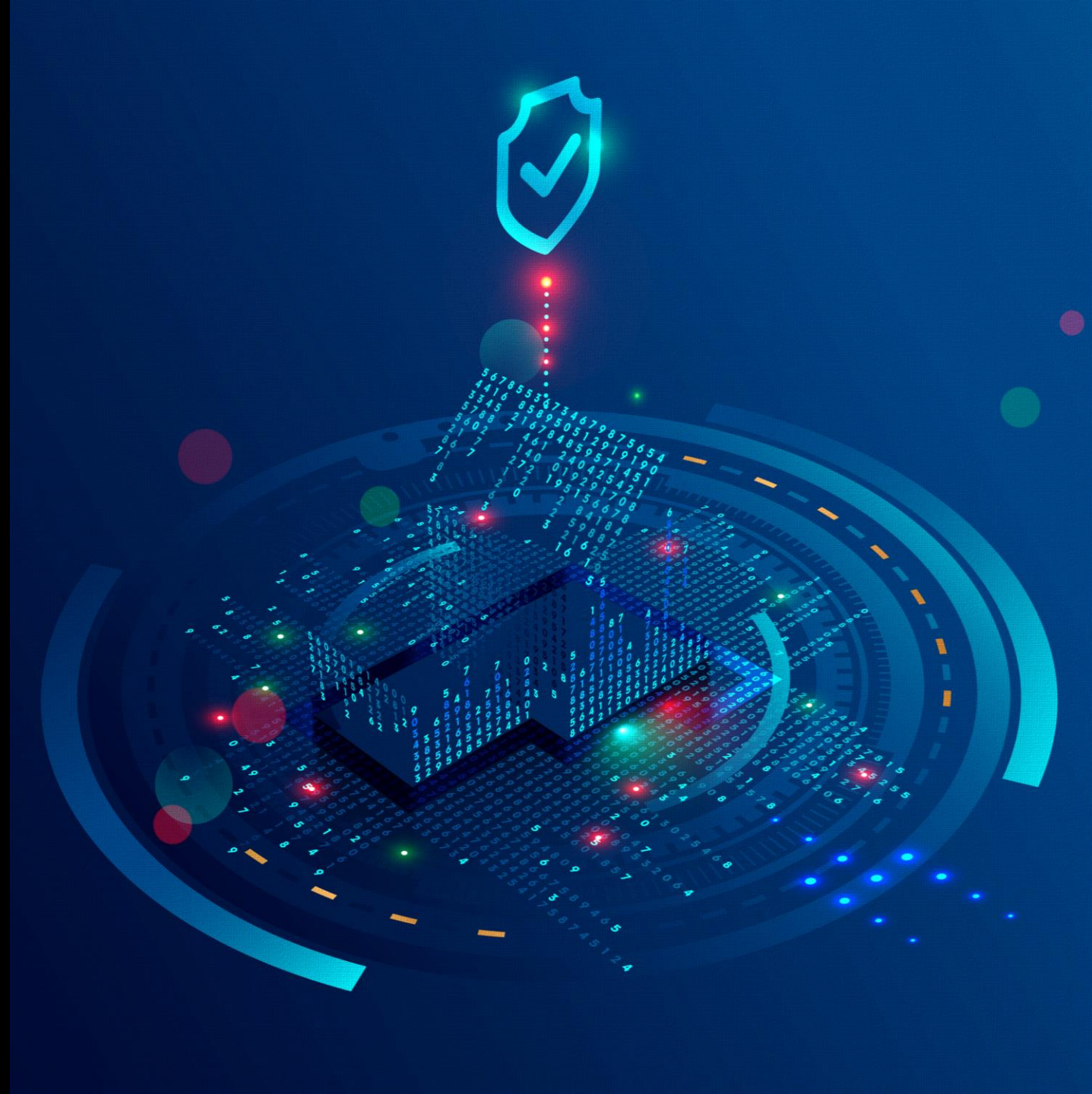
Sisältö

Miksi?

Mitä?

Kuka?

Miten?

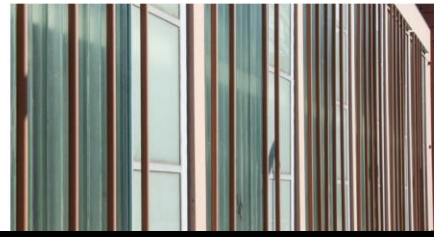


Miksi? Uhka- ja riskitaso on kohonnut

Kansallisen turvallisuuden katsaus: Venäjän tiedustelun toimintatapa muuttuu

29.9.2022

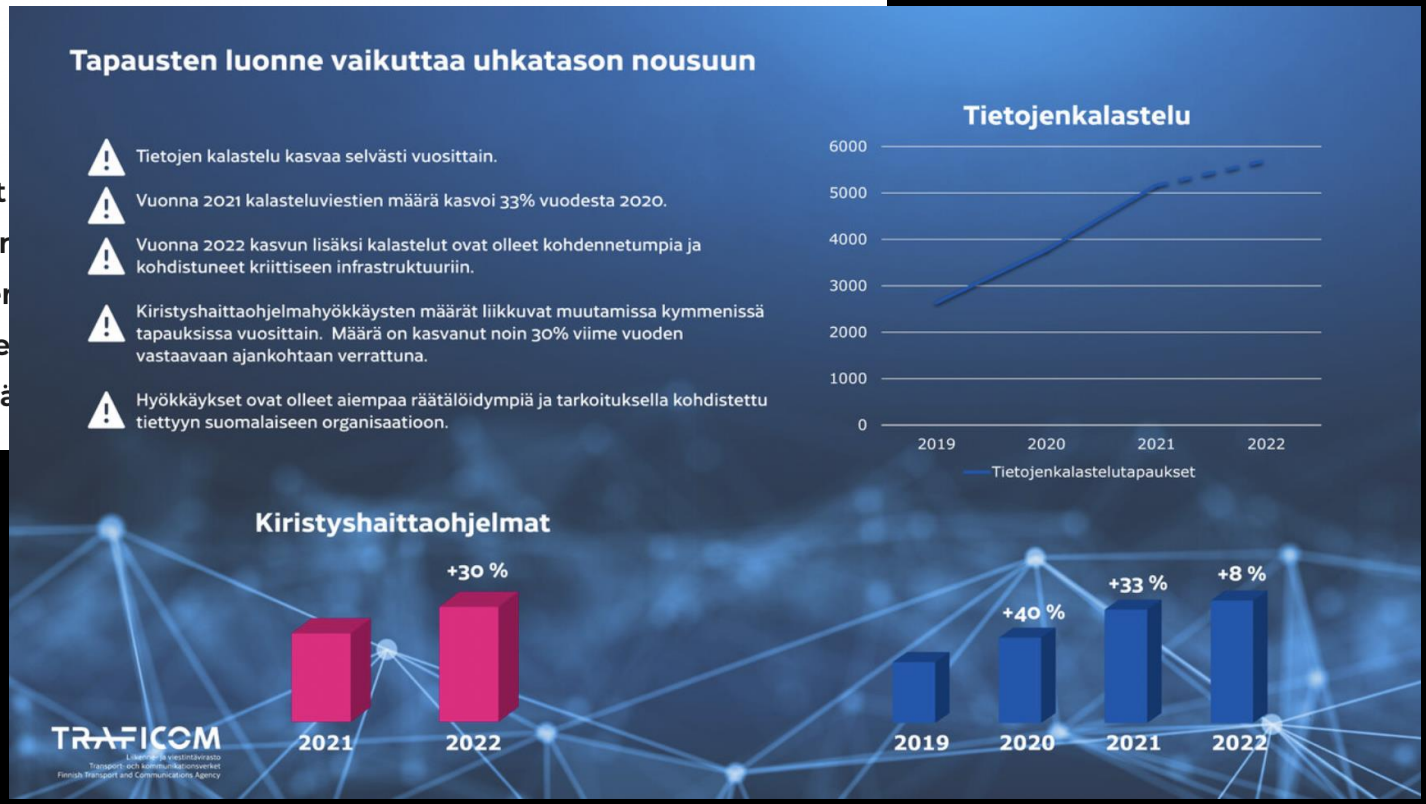
TIEDOTE



Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt

Julkaistu 12.09.2022 10:59

Kyberhyökkäykset ovat lisääntyneet
niitä kohdistuu hiljaisemman kevään
Kyberturvallisuuskeskuksen saamien
kohdistuvissa kyberhyökkäyksissä, e
palvelunestohyökkäysten lukumäärä



Miksi? Kyberhäiriön vaikutukset ja kustannukset ovat valtavat

REUTERS®

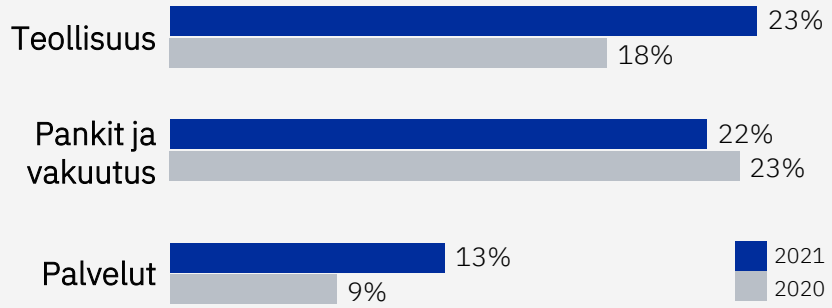
One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

Colonial Pipeline Company

In May of 2021, a cyber attack on a major U.S. gas pipeline caused operations to be shut down for five days, resulting in a temporary fuel shortage along the East Coast. The affected business was the Colonial Pipeline Company, which operates the largest pipeline system for refined oil products in the United States.

Yleisimmät toimialat kyberiskujen kohteena

Prosenntia hyökkäyksistä



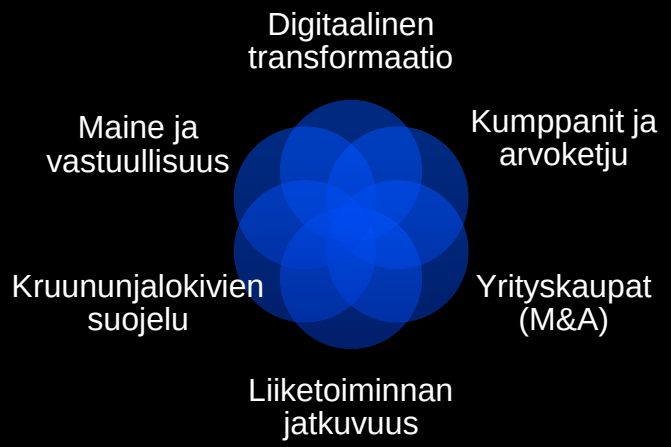
$4.35M

Keskimääräinen tietomurron suora kustannus (+13% 2 vuodessa)

Lähde: 2022 IBM X-Force Threat Intelligence Report; 2022 IBM Security Cost of a Data Breach Report

Mitä? Digi on kaikkialla ja kenttä on moninainen

Liiketoiminta digitalisoituu



Tietoturvateknologiat kehittyvät – samoin uhkat

- Uhkakuvat muuttuvat ja kehittyvät
- Liiketoiminta laajenee uusille alueille
- Teknologiat kehittyvät

Regulaatio lisääntyy

Digitaalisen turvallisuuden strategian täytyy huomioida kompleksinen ja lisääntyvä regulaation viidakko.

Digitaalisen turvallisuuden riskit vs. investoinnit

Digitaalisen turvallisuuden investoinnit kohtaavat kiristyvän taloudellisen tilanteen

Mitä? Tyypillisen kyberhyökkäyksen yksinkertaistettu anatomia

1)
kä

2)
laa

3)
(ka
tie

4)

5)

What Happened?

A hacker group was able to access the Colonial Pipeline network and infect many of its systems with ransomware, including its billing and accounting systems. In a ransomware attack, hackers encrypt an organization's data and hold it hostage. They claim they will release the data or share a decryption key enabling victims to recover their data, once a ransom is paid. However, there have been many accounts of cyber criminals taking the ransom and never returning data access to their victims.

Colonial Pipeline shut down pipeline operations to prevent the ransomware from spreading. Meanwhile, the White House declared a state of emergency in 17 eastern states as a response to the shutdown. Colonial Pipeline said it ultimately paid the hackers the equivalent of nearly $5 million USD to get the decryption key and regain control of its systems.

How Did It Happen?

What allowed hackers to gain access to systems of the largest refined oil pipeline in the United States? The head of Colonial Pipeline stated that hackers who launched the cyber attack against the company were able to get into the system by stealing a single password. They found an employee's exposed password, which they suspect was the result of the employee reusing a password for more than one account. Moreover, two-factor authentication was not required to access the hacked system, so that one password was all the cyber criminals needed to start a large-scale ransomware attack and cripple the operations of a major fuel company.

What's the Lesson?

Use strong passwords and do not reuse passwords across accounts. Always choose to enable two-factor authentication when possible.

Miten? Tunnista kriittiset digitaaliset kohteet, “kruunun jalokivet”

- Tietojen suojaus
- Yksityisyyden suojaus
- Toimintojen suojaus
- Palautuminen

Miten? Avainkysymyksiä

Onko digitaaliset “kruununjalokivet” tunnistettu?

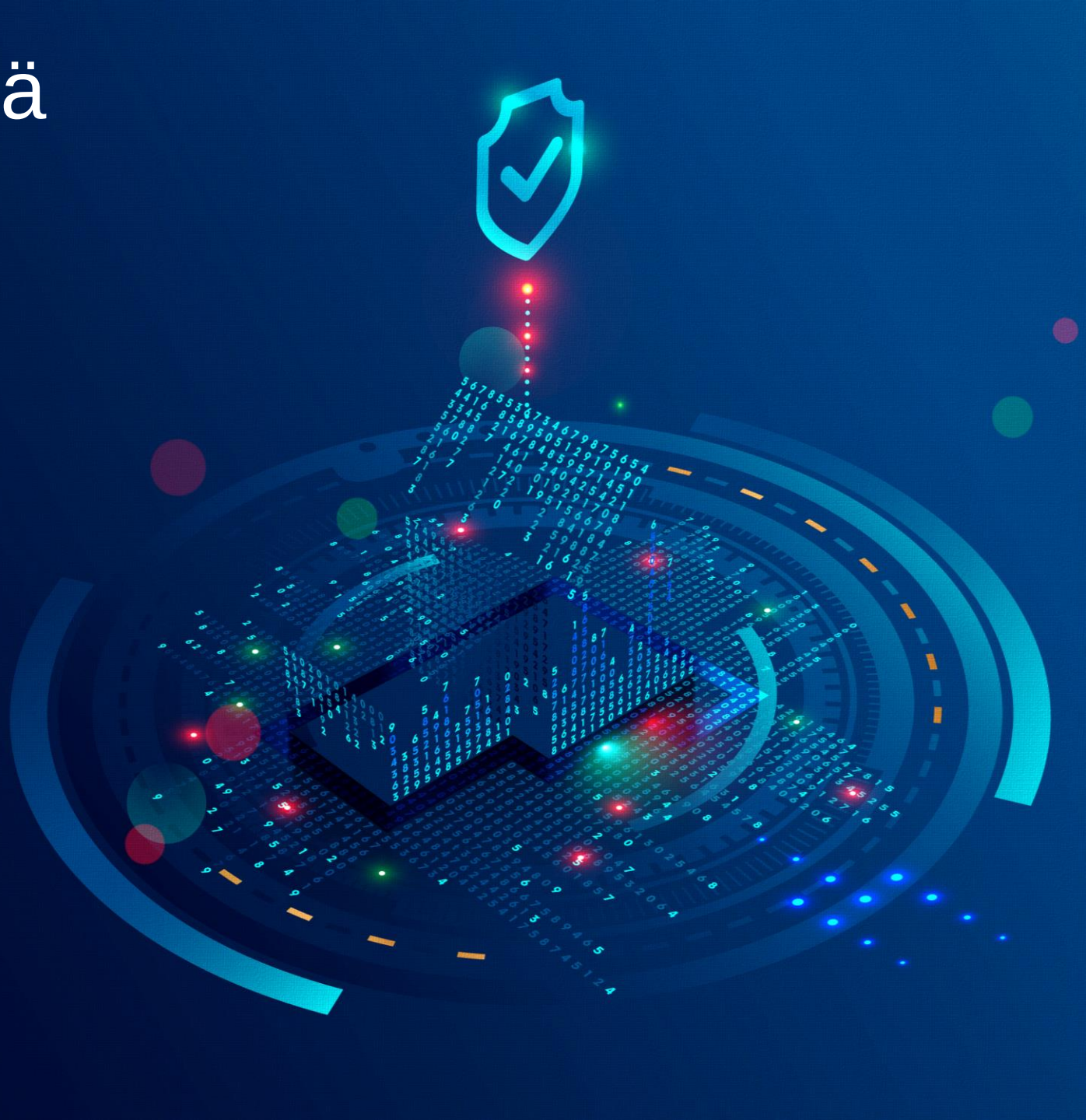
Onko niihin liittyvät sisäiset ja ulkoiset riippuvuudet selvillä?

Kuinka pitkä katko voidaan sallia?

Onko harjoiteltu?

Onko auditoitu?

Mikä on digitaalisen turvallisuuden kulttuuri, työkalut ja osaaminen?



Miten? Kulttuuri ja osaaminen

Welcome!

☆ YOUR TOTAL SCORE 3,920

BENCHMARK 3,192

1. Security Hygiene: Passwords and Device Management

☆ SCORE 720

2. Phishing and Human Error

☆ SCORE 320

3. Malware Threats and Cybersecurity Incidents

☆ SCORE 240

4. Security Hygiene: Software, Cloud, and Supply Chain

☆ SCORE 720

5. Handling Personal Information Responsibly

☆ SCORE 320

6. Respecting Data Privacy Rights

☆ SCORE 720

7. Trust and Transparency for AI

☆ SCORE 560

8. Your Choices Matter

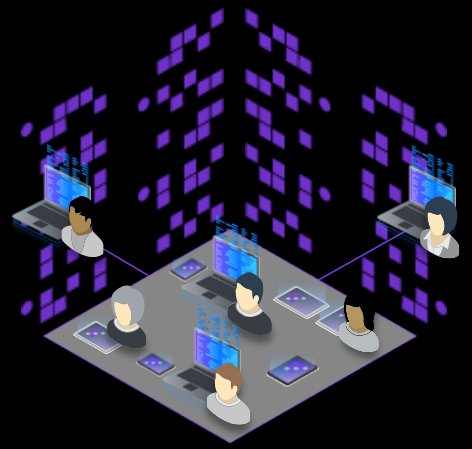
☆ SCORE 320

Miten? “Zero trust”

“Ulkorajapuolustuksen” sijasta tarkkaillaan jatkuvasti käyttäjiä, käyttäytymistä, laitteita, ohjelmistoja, data ja infrastruktuuria.

Perusperiaatteet:

- Myönnetään vain tarvittavat (minimi) oikeudet
- Jatkuva verifiointi
- Lähtökohtaolettamana tietomurto



Miten? Kättä pidempää Huoltovarmuusorganisaatiosta: www.digipooli.fi

KUTSU

TO 8.12.2022 KLO 9:00–11:00

#DigiSignaali22

Mitä maksaa hyvä varautuminen?

Tilaisuus on maksuton.
Etä/läsnä

TURVALLISEN DIGITALISAATION TYÖKALUPAKKI YRITYSJOHTAJALLE

HUOLTOVARMUUSORGANISAATIO DIGIPOOLI

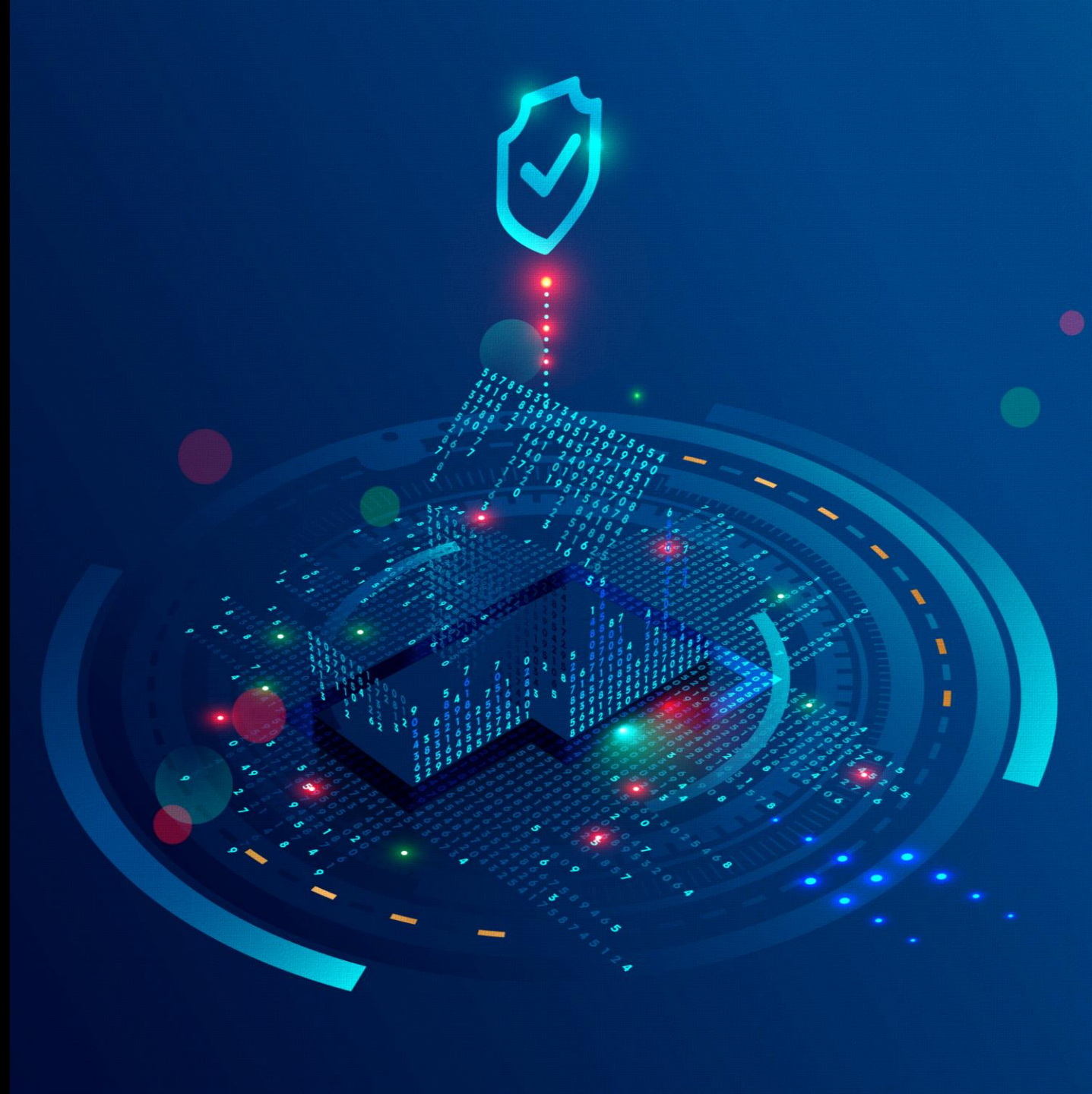
Kuka? Digitalisaation turvallisuus yrityksen hallitustyön, strategian ja riskienhallinnan ytimessä

Hallitus: strategia, riskienhallinta, vastuullisuus, valuaatio

Toimiva johto: kruununjalokivet, investoinnit, kulttuuri, osaaminen

IT & tietoturva: tekniikka, “zero trust” –toteutus

Jokainen organisaation jäsen: perusosaaminen ja etulinjan puolustus




IBM