# Tekoäly ja tietoturva

**Professori, laitosjohtaja Sasu Tarkoma**
**Tietojenkäsittelytieteen laitos**
**Helsingin yliopisto**

# Sisällys

Johdanto

Tekoäly

Tekoäly ja tietoturva

Tutkimusesimerkkejä

# Johdanto

Teknologia mahdollistaa esineiden ja asioiden reaali-aikaisen seurannan ja säätämisen

Tilat, liikenne, teollisuus, ketjut ja verkostot

Kehittyneet data-analytiikkaratkaisut mahdollistavat uudenlaisen lisäarvon löytämisen datasta

Tietoturvauhat kehittyvät nopeasti ja hyödyntävät uusinta teknologiaa

Miten kehittyvä tekoälyteknologia voi parantaa järjestelmien tietoturvaa ja tietosuojaa?

# Tietoturva

Tietoturva on tietojen, järjestelmien, palveluiden ja tietoverkkojen suojaamista

Tietosuoja on yksityisyyden ja luottamuksen turvaamista

Sekä tietoturva että tietosuoja ovat modernin yhteiskunnan keskeisiä vaatimuksia

# Meet the men who spy on women through their webcams

# TRUECALLER PATCHES BUG THAT HAS 100 MILLION ANDROID USERS AT RISK

## New "Stagefright" Hack Exposes 275 Million Android Phones

Remotely Exploitable Flaw in Truecaller Leaves 100 Million Android Devices Vulnerable

March 27, 2016 By Pierluigi Paganini

## Warning! Over 900 Million Android Phones Vulnerable to New 'QuadRooter' Attack

Sunday, August 07, 2016 Swati Khandelwal

MBURAJ DAS
RCH 30, 2016

Malware

## Inside Hummingbad, the Android virus infecting 10 million devices

# Stagefright: It Only Takes One Text To Hack 950 Million Android Phones

BRIAN BARRETT SECURITY 03.07.16 1:11 PM

# HACK BRIEF: RANSOMWARE STRIKES APPLE'S OS X FOR THE FIRST TIME

NEWS

## Apple devices held for ransom, rumors claim 40M iCloud accounts hacked

Apple ID hackers using Find My iPhone lock message to demand ransom

Ben Lovejoy - 3 weeks ago @benlovejoy

APR 1, 2016 @ 09:12 AM 18,001 VIEWS

The Little Black Book of Billionaire Secrets

## Ingenious Lightbulb Hack Can Cause Seizures, Spy On 'Air-Gapped' Networks

## Afraid of the Dark? Too Bad, Your Smart Bulbs Can Be Hacked

August 5, 2016 // 05:45 AM EST

## Car Thieves Can Unlock 100 Million Volkswagens With A Simple Wireless Hack

Thursday, August 11, 2016 Swati Khanc

ANDY GREENBERG SECURITY 03.17.16 6:59 PM

# THE FBI WARNS THAT CAR HACKING IS A REAL RISK

ANDY GREENBERG SECURITY

# HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

## Researchers find 'smart' door locks are easy to hack, surprising no one

By Chris Mills on Aug 11, 2016 at 5:10 PM

Security

## Samsung smart fridge leaves Gmail logins open to attack

## Fridge caught sending spam emails in botnet attack

SECURITY > NEWS

## 75 Percent of Bluetooth Smart Locks Can Be Hacked

by PAUL WAGENSEIL Aug 7, 2016, 2:28 PM

## Smile! Hackers Can Silently Access Your Webcam Right Through The Browser (Again)

Posted Jun 13, 2013 by Greg Kumparak (@grg)

## Be careful of what you say in front our Smart TV, warns Samsung

When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

## Hackers Killed a Simulated Human By Turning Off Its Pacemaker

## Hacking into homes: 'Smart home' security flaws found in popular system

## $17 smartwatch includes a backdoor in the pairing

# Tekoäly

Tekoäly (artificial intelligence) on monitieteinen tieteenala

- Älykkääksi katsotun toiminnan analyysi
- Älykkäiden järjestelmien tuottaminen

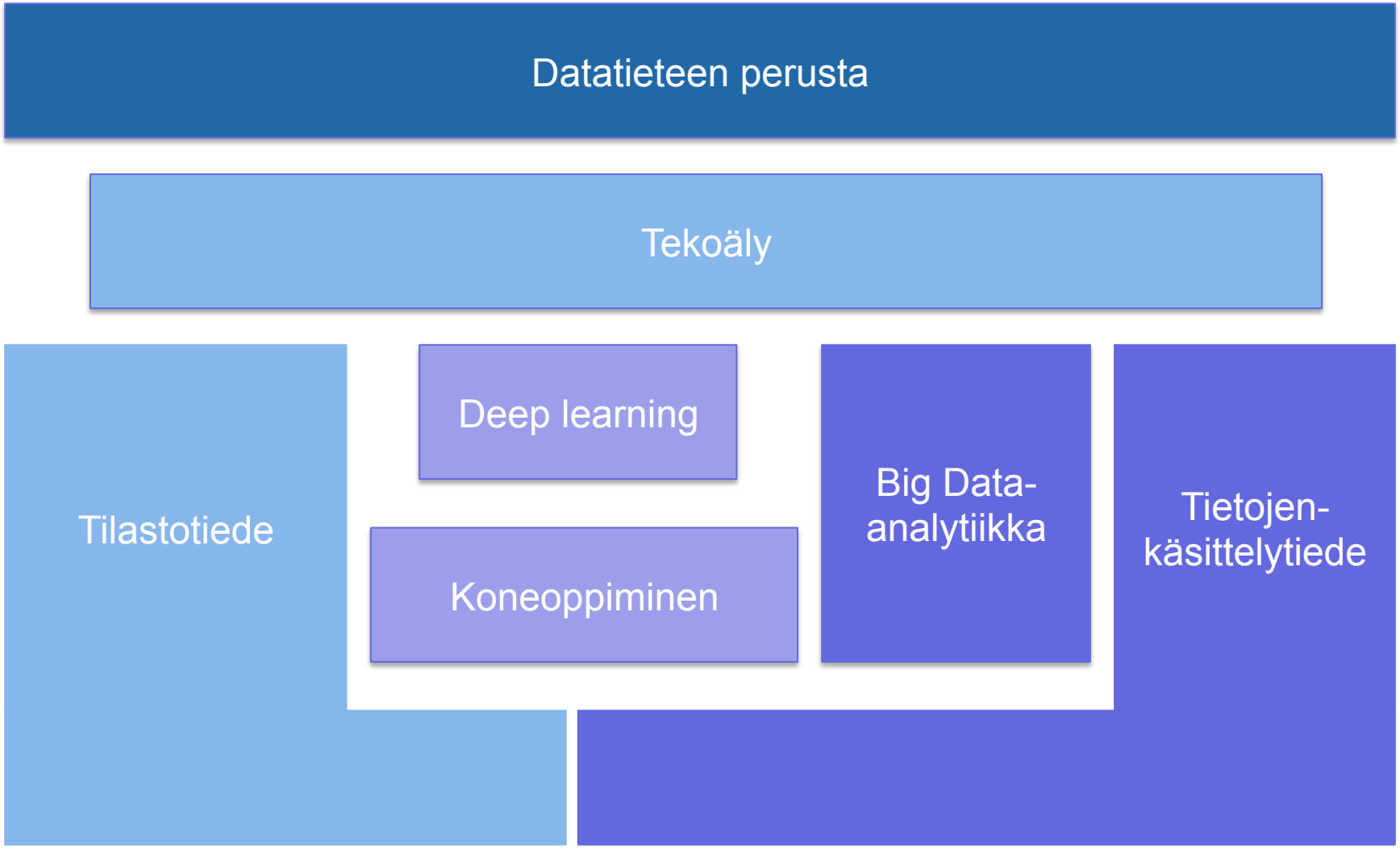
Suppeassa merkityksessä järjestelmä, joka kykenee johonkin älykkääseen toimintoon

Käsite Artificial Intelligence syntyi 1956 Darthmouth Collegen työpajassa ja siihen liittyy pitkä historia lähtien antiikin ajoista

Useita lasku- ja nousukausia vuosien aikana

- Uusi tekoälyrenesanssi

# Käsitteitä


Datatieteen perusta
Tekoäly
Tilastotiede
Deep learning
Koneoppiminen
Big Data-analytiikka
Tietojen-käsittelytiede

# Tekoäly ja tietoturva

Järjestelmien tietoturva- ja tietosuojaympäristöt muuttuvat koko ajan

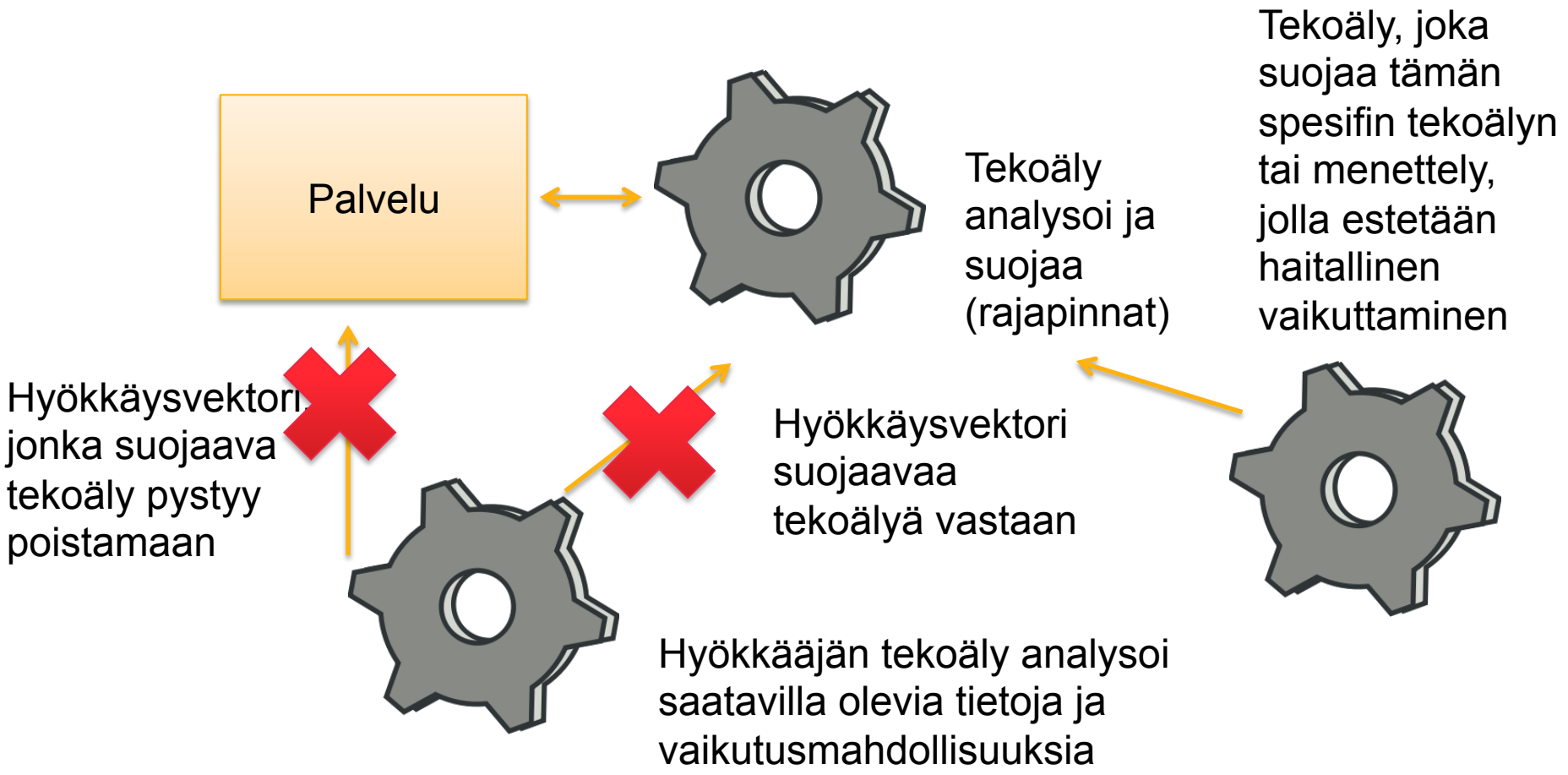
- Jatkuvasti uusia heikkouksia ja hyökkäyksiä

Koneoppimismenetelmät ja tekoäly mahdollistavat datavetoisen järjestelmien suojauksen

- Poikkeamien tunnistaminen
- Ennaltaehkäistä tietoturva- ja tietosuojaongelmia
- Järjestelmien generointi

On kuitenkin tärkeää suojata myös tekoäly hyökkääjiltä, että siihen ei voi haitallisesti vaikuttaa

# Esimerkki


Palvelu
Tekoäly analysoi ja suojaa (rajapinnat)
Tekoäly, joka suojaa tämän spesifin tekoälyn tai menettely, jolla estetään haitallinen vaikuttaminen
Hyökkäysvektori jonka suojaava tekoäly pystyy poistamaan
Hyökkäysvektori suojaavaa tekoälyä vastaan
Hyökkääjän tekoäly analysoi saatavilla olevia tietoja ja vaikutusmahdollisuuksia

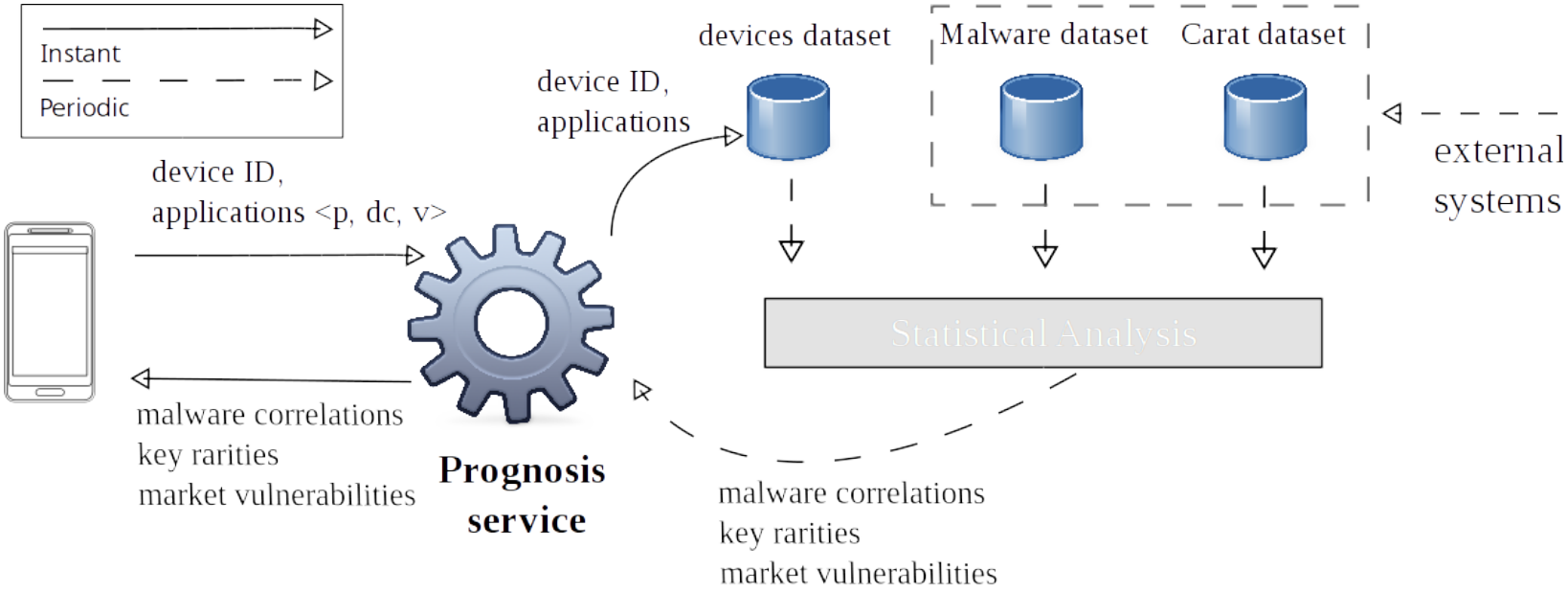
# Tutkimusesimerkkejä

## Tutkimusta CS laitoksella ja Tietotekniikan tutkimuslaitos HIIT:ssä

# Varhainen varoitusjärjestelmä

Kehitimme varhaisen varoitusjärjestelmän, joka tunnistaa riskipitoiset laitteet

Käytettyjen sovelluksien ja haittaohjelmien välistä korrelaatiota käyttämällä voidaan ennustaa laitteen saastuminen 5 kertaa paremmin kuin laitteiden satunnainen valikoiminen testausta varten

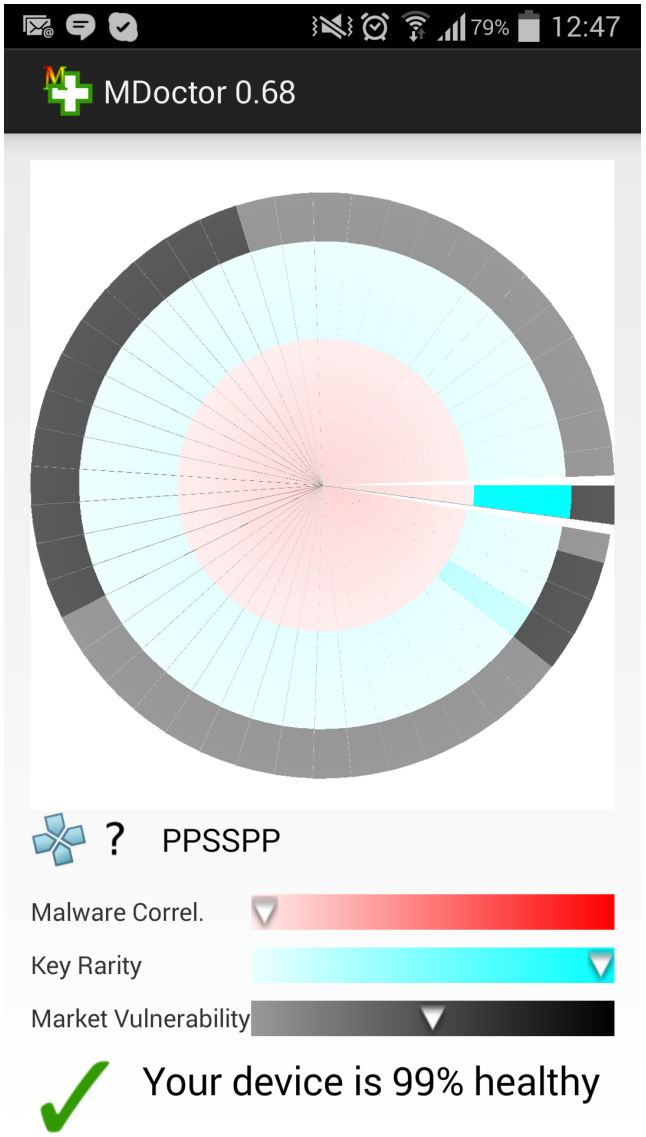


# MDoctor: Mobiililaitteen haittaohjelma-tilannekuva

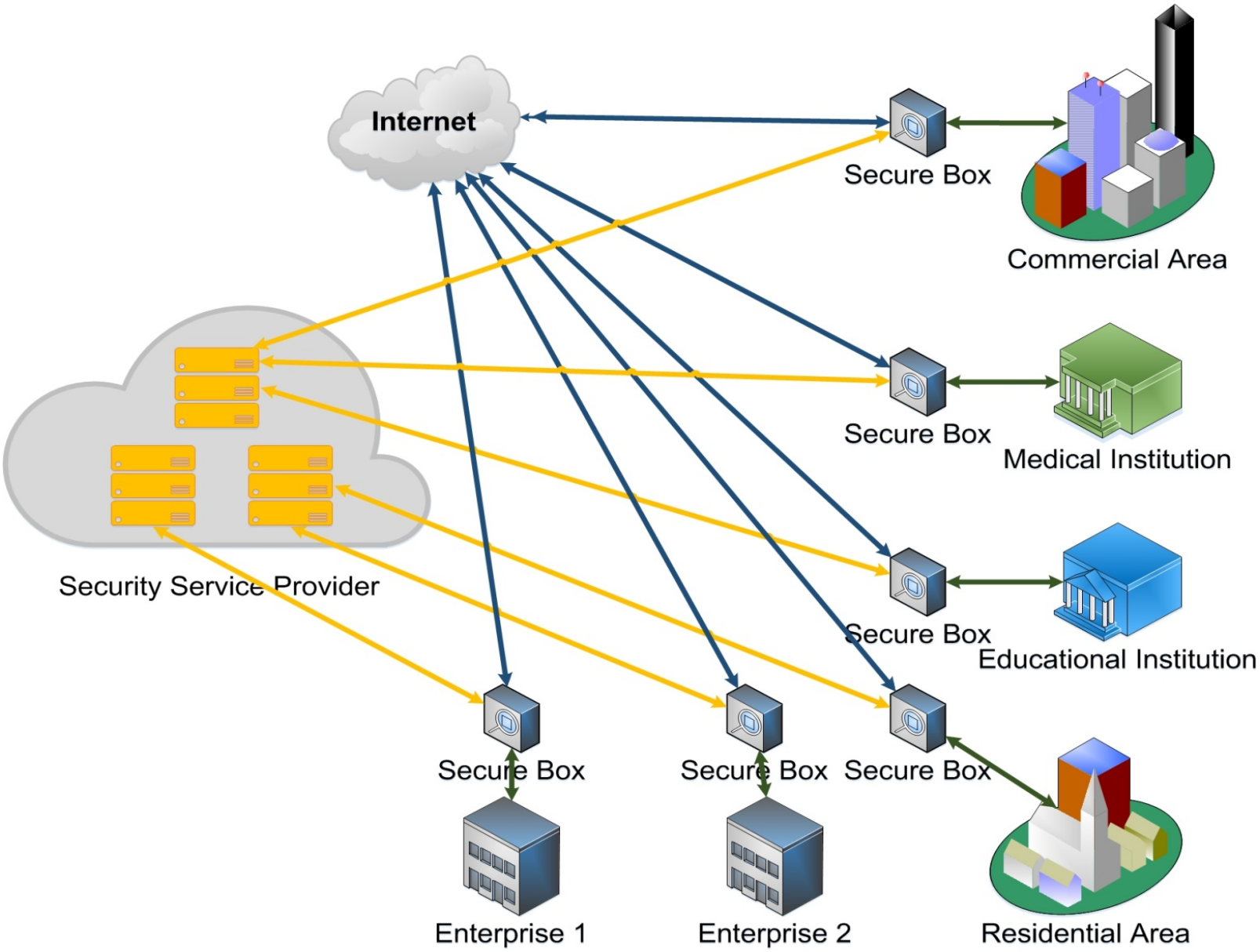
MDoctor sovellus näyttää tilannekuvan mobiililaitteen haittaohjelmariskeistä

Ohjelma laskee tunnusluvun riskille saada haittaohjelmia ja näyttää kunkin sovelluksen vaikutuksen kokonaisriskiin

Ohjelma käyttää kolmea keskeistä metriikkaa: haittaohjelmakorrelaatio allekirjoitusavainten analyysi sovellusmarkkina-analyysi



# SecureBox -arkkitehtuuri



# Yhteenveto

Rakennamme datavetoista reaaliaikaista digitaalista infrastruktuuria.

Koneoppiminen ja tekoäly mahdollistavat oppivat ja ennakoivat tietoturvaratkaisut

Tekoäly tekee ympäristöstä monimutkaisemman
Oikein toteutettuna tekoäly mahdollistaa tietoturvaprosessien automatisoinnin ja tehostamisen