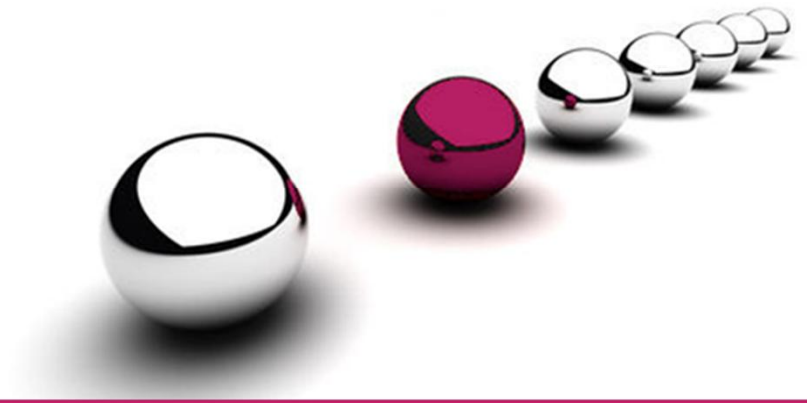
Lääkinnällisten ja talotekniste tietoverkkojen eriyttäminen

Sairaalatekniikan päivät Hämeenlinnassa 8.-9.2.2017

Tero Hemming
Palvelupäällikkö, Turvallisuus ja riskienhallinta
CEH,CNDA,CLPU,CPLA,CKM,C5,SO,ST



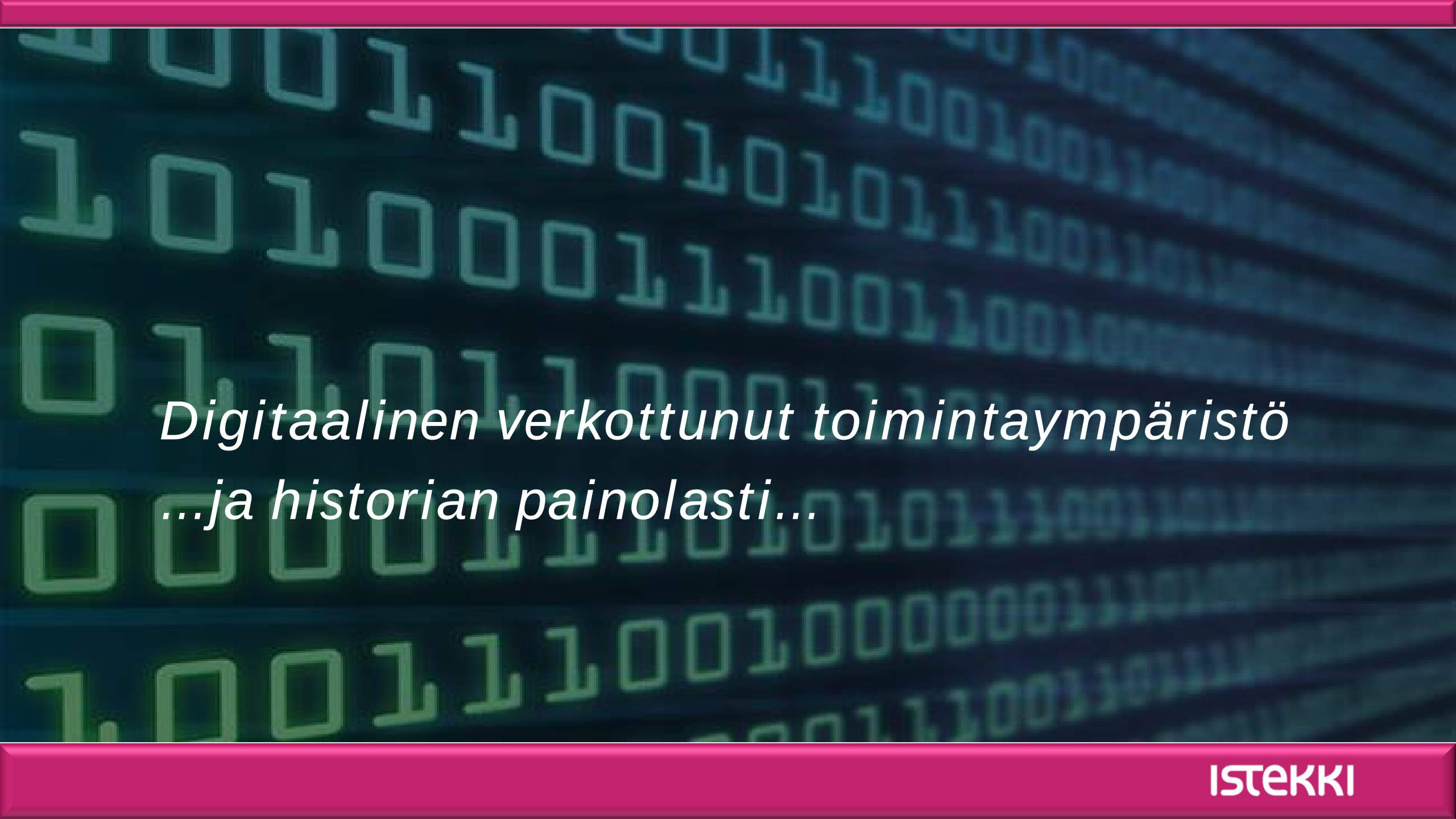
Certified Network Defense Architect

Certified Ethical Hacker

ORGANISATION CERTIFIED BY Inspecta ISO/IEC 20000

ORGANISATION CERTIFIED BY Inspecta ISO 9001

https://fi.pinterest.com/pin/238057530274191767/


Digitaalinen verkottunut toimintaympäristö
...ja historian painolasti...

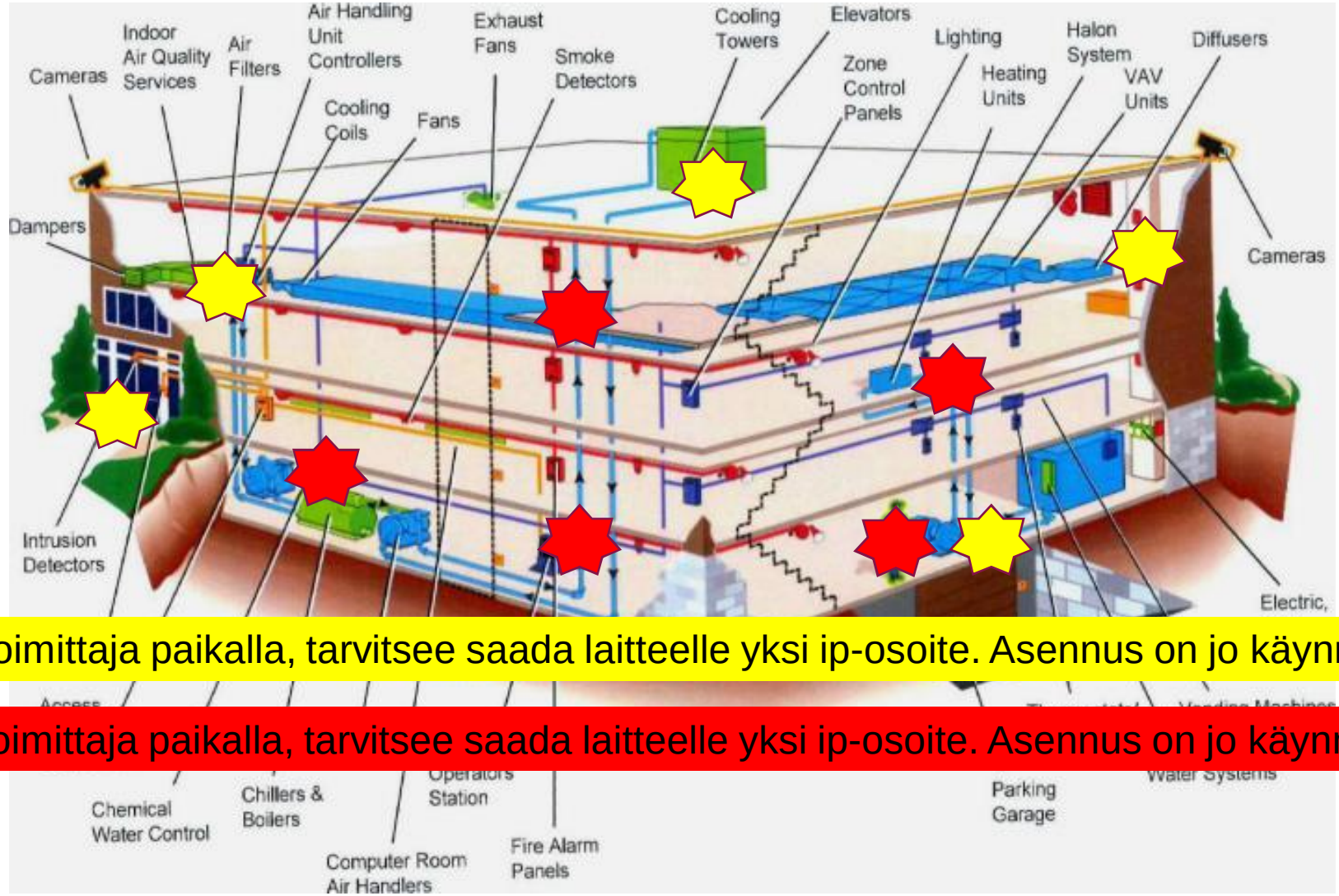
Lääkinnälliset tietoverkot 2017

….täällä on toimittaja paikalla, tarvitsee saada laitteelle yksi ip-osoite. Asennus on jo käynnissä !!!

….täällä on toimittaja paikalla, tarvitsee saada laitteelle yksi ip-osoite. Asennus on jo käynnissä !!!

http://endlessleadz.com/wp-content/uploads/2013/11/Bring-your-own-doctor-healthcare-device-marketing.png

Talotekniikka 2017



….täällä on toimittaja paikalla, tarvitsee saada laitteelle yksi ip-osoite. Asennus on jo käynnissä !!!

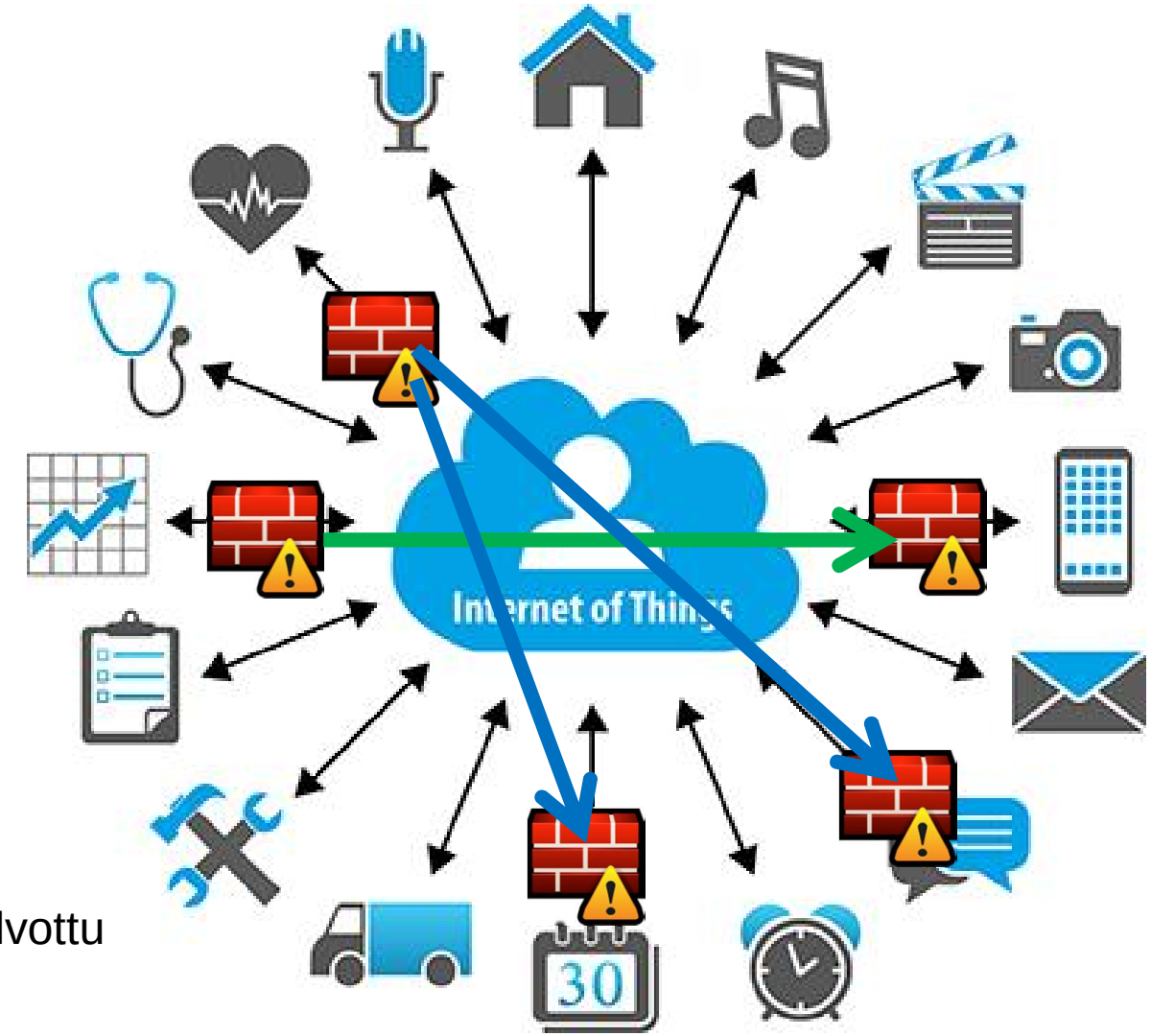
….täällä on toimittaja paikalla, tarvitsee saada laitteelle yksi ip-osoite. Asennus on jo käynnissä !!!

Miksi ympäristöt tarvitsevat erityishuomiota ?
(järjestelmien realiteetit edelleen vuonna 2017)

- Juurikin siksi että ne ainakin aiemmin tuotu tuotantoon ”adhoc-tyylisesti ja pirstaleisesti”
- Vanhentuneita käyttöjärjestelmiä, joita ei enää tueta, eikä niihin tule päivityksiä
  - Windows CE, XP
  - Sulautettuja Linux järjestelmiä jotka eivät ole minkään paketinhallinnan piirissä
- Oletusasetuksin käynnistyviä WWW-palvelimia, joita ei voi päivittää, eikä suojata turvallisemmaksi
  - Puutteellisia tai olemattomia autentikointimenetelmiä
- Vanhentuneita ja haavoittuvia sovelluskirjastoja ja liitännäisiä
- Suojaamattomia SNMP-rajapintoja (SNMP v1 tai v2)
- Suojauksia parametreille ei juurikaan ole
- Salaamattomia ja heikosti turvattuja liittymiä ja rajapintoja (ftp, http jne...)

Mitä IoT ”parhaimmillaan tai pahimmillaan” ?
(mielikuva vs. tavoitetila)

Mielikuva:
”Ketterä, helppo,avoin”
…mutta haavoittuva ?



Tavoitetila:
”Ketterä, helppo,avoin”
…mutta vakaa, suojattu ja valvottu
aidosti lisäarvoa tuottava

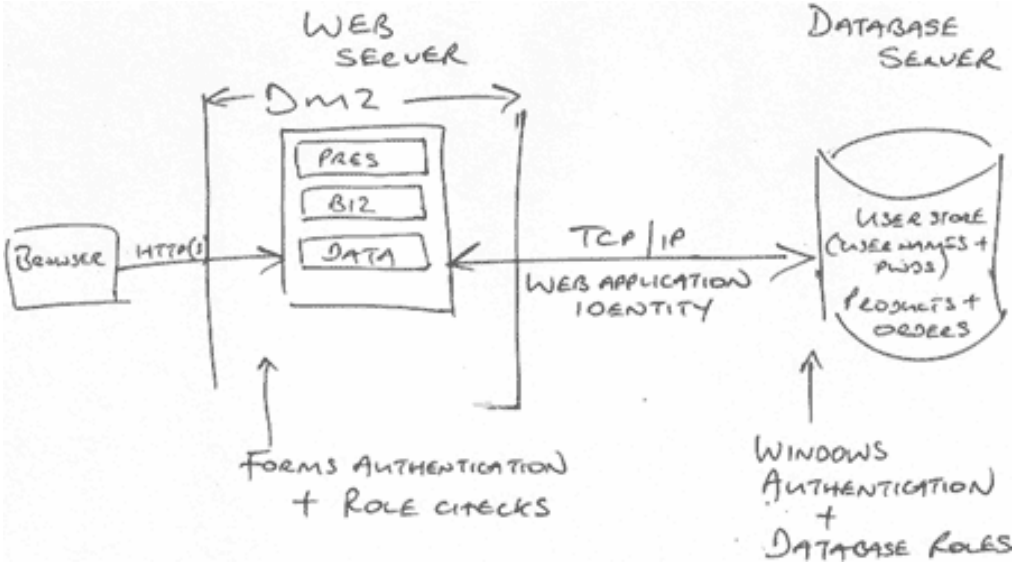
http://maylab.my/wp-content/themes/aviation/images/I_o_T.jpg
http://www.dts-solution.com/wp-content/uploads/2014/03/app-control.png

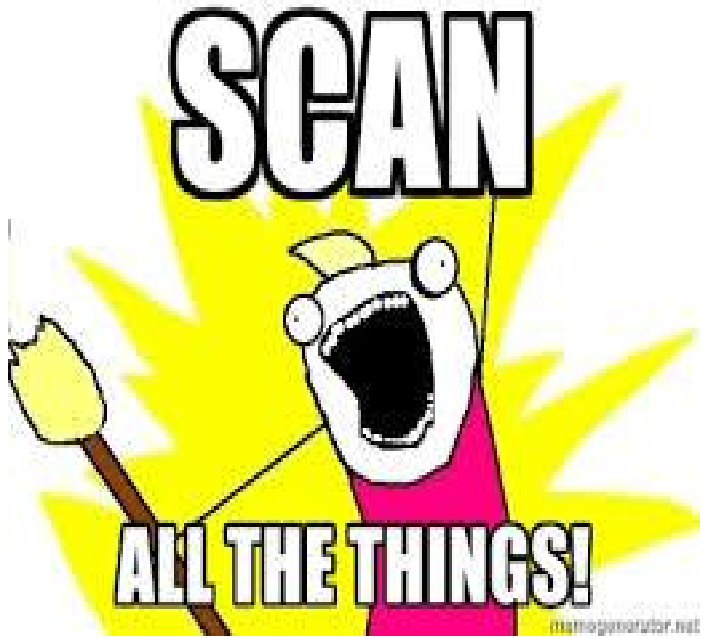
Miten eriytämme ja suojaamme lääkinnälliset ja talotekniset tietoverkot ?

ISTEKKI

Uudet järjestelmät:
(tai merkittävät muutokset nykyisiin...)

- ✓ Tieto- ja kyberturvallinen tietojärjestelmien käyttöönotto
- ✓ Uhkamallinnus, Haavoittuvuusskannaukset





Olemassaolevien järjestelmien läpikäyminen:

- Verkkojen ja toimintojen luokittelu ja osastointi:
  - Erikoislaitteet jaetaan käyttötarkoituksen, L2/L3 tarpeiden, ulkoisten liityntätarpeiden ja suojausvyöhykkeen mukaisesti mahdollisimman pieniin verkkosegmentteihin.
  - Verkon liikennettä verrataan ”Threat Intelligence Services” tietovuon tuottamaan informaatioon
  - **Erikoislaiteverkoissa käytettävät sovellukset tulee tunnistaa sovellustasolla ja verkkojen väliset yhteydet tulee sallia vain tunnettujen sovellusten osalta.**
  - Esimerkkeinä:
  - Potilaan hoitoon käytettävät laitteet | Ovia, puomeja, nesteitä, kaasuja ohjaavat laitteet
  - Potilastietoa käsittelevät laitteet | Mittaus, ohjaus ja raportointia tuottavat laitteet
  - Muut luottamuksellista tietoa käsittelevät laitteet | Kameravalvonnat ymv.
  - Muut laitteet

Etähallinta- ja huoltoyhteydet

- ✓ <u>Aina: sopimus, vastuut, raportointi, henkilökohtaiset tunnukset</u>
- ✓ Turvalliset etäyhteydet pääsääntöisesti julkaisuna ja 2-vaiheiseilla autentikoinnilla
- ✓ Organisaatioiden välisistä VPN tunneleista luovutaan, tai käytetään vain poikkeustapauksissa
- ✓ Poikkeuksiin tarkemmat sopimukset, tekninen malli ja vastuu (esim. Turvalliset etäyhteydet toimittajan dedikoidulla ratkaisulla)

Toimintaympäristön ja tietoturvakontrollien tilannekuvan muodostaminen

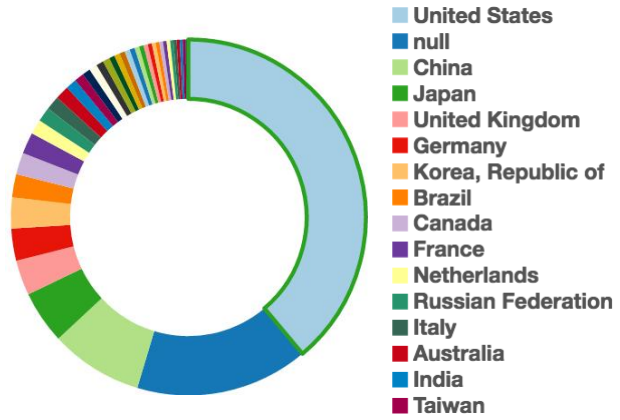
Tekninen tilannekuvapalvelu (SIEM)

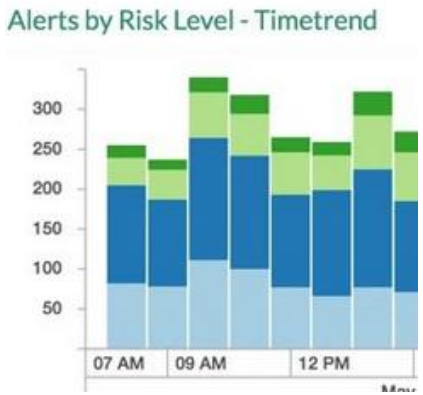
criticalstack®

EMERGING THREATS

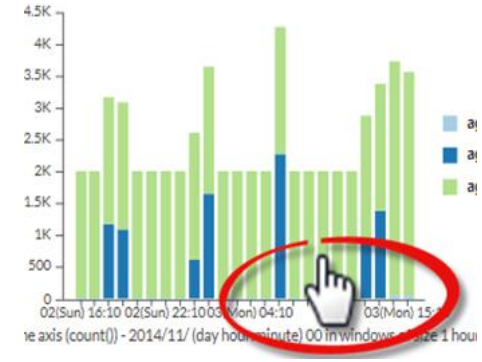
- Dashboard
- Alert Rule
- Labelling Rule
- Incident
- Public URL

EAL3+ Common Criteria CERTIFIED





- PCI-DSS
- SOX
- ISO27001 and ISO27002
- HIPAA
- FISMA
- BASEL-II
- GPG13



Kuvien lähteet: https://userscontent2.emaze.com/images, http://www.internet-creation-sites.net/images/ http://thesmartpanda.com https://stixproject.github.io/

ISTEKKI

Kysymyksiä?

tero.hemming[at]istekki.fi
040-8080805