FUJITSU

shaping tomorrow with you

Big Data ajatusmallin käyttäminen lokienhallinnassa

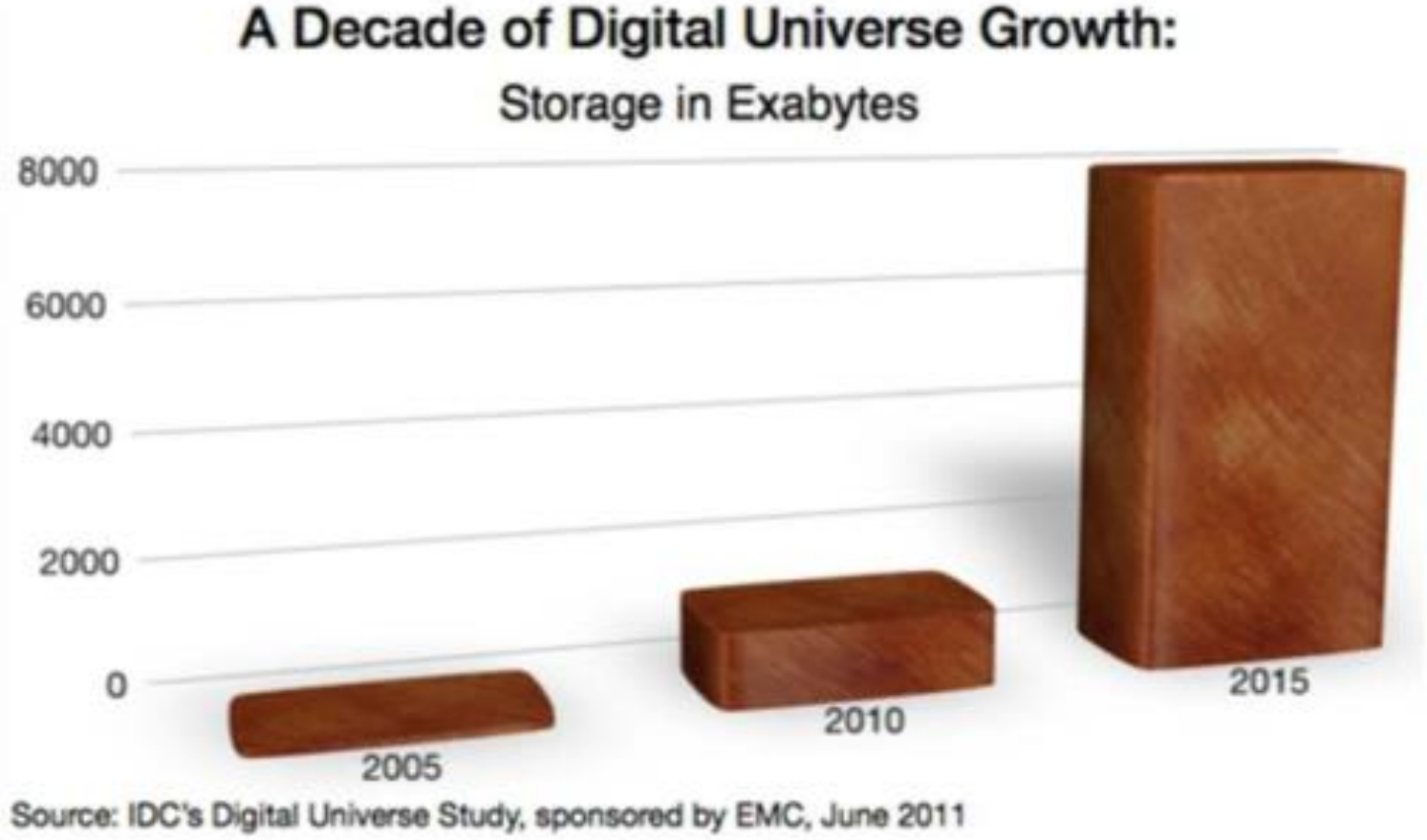
Tietoturvapäivä 2013

Jan von Hintze

Tietopaketti Big Datasta

- Vuonna 2011 datamäärä joka luotiin tai replikoitiin kaikissa tietokoneissa ympäri maailman ylitti 1800 exabyteä (1.8 triljoonaa gigaa) = 250 miljardia DVD levyä…
- Informaation määrä jonka ihmiset itse luovat on paljon pienempi kuin se mikä heistä luodaan!

Datan kasvun määrä



Big Data / Lokienhallinta mitä yhteistä?

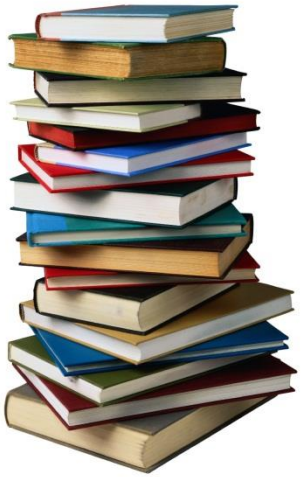
- Kerätään isosta määrästä datalähteitä tietoa.
- Yhdistelemällä tietoja saadaan tietää sellaisia asioita mitkä normaalisti jäisivät pimentoon.
- Tiedot indeksoidaan.
- Tehdään lukematon määrä automaatti sääntöjä joidenka tuloksia ei muuten saataisi selville.
- Johtotuloksena lokien hallinta on Big Dataa.

Faktoja ja väitteitä tietoturvasta

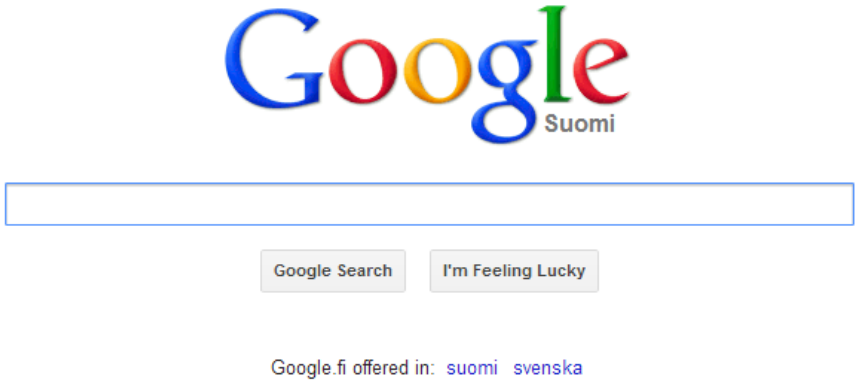
- Kaikki organisaatiot kärsivät tietoturva ”tapahtumista” on toinen asia ovatko nämä tiedossa.
- Kun mediassa ei puhuta viruksista ei se tarkoita sitä että viruksia ei olisi vaan ne toimivat ”paremmin”.
- Kun on tapahtunut jotain ikävää ei todellisia saada selville syitä / tapahtuma ketjua.
- Väittäisin että 90% tietoturva ”tapahtumista” jää organisaatiossa havaitsematta.

Esimerkkini lokienhallinnasta

- Perinteinen
  - Jokainen kirja on oma lokin lähteensä
  - Tietojen etsiminen työlästä



- Keskitetty lokien hallinta.
  - Kaikki kirjat ovat indeksoituja



Miksi lokeja kerätään?

- Nykytilanne
  - Jotta täytettäisiin erilaiset standardit esim Katakri, PCI-DSS, Vahti, SOX jne.
  - Tutkitaan lokeja kuin jokin menee pieleen.

- Ideaalitilanne
  - Täytetään standardien vaatimukset ja …
  - Pystytään löytämään ongelmat ja syyt suuremmalla todennäköisyydellä ja nopeammin.
  - Pystytään ennakoimaan tapahtumia.

Kun jotain sattuu…

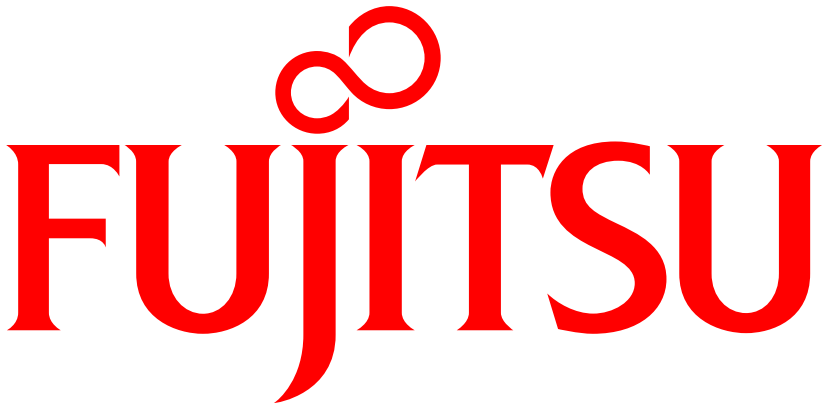
- Perinteinen
  - Kerätään mahdollisimman nopeasti lokit ja aletaan analysoimaan niitä. Tämä voi tarkoittaa esim. Active Directory, palomuuri, IPS, verkkolaitteet jne. eri lokilähteitä ja formaatteja voi olla kymmeniä. Tämä on erittäin työläs lähestymistapa jossa on erittäin vaikea saada kokonaiskuvaa.
- Keskitetty lokien hallinta
  - Ongelman sattuessa kaikki loki lähteet ovat samassa paikassa ja voidaan hakea tietoa erittäin helposti ja nopeasti. Näet yhdestä paikasta kaiken oleellisen tiedon kaikista lokilähteistä ja pystytään helposti rakentamaan kokonaiskuva.

Haasteita keskitetyssä lokien hallinnassa

- Yritykset ovat tyytyväisiä kun eivät tiedä mitä todella tapahtuu vaan elävät omassa ”kuplassaan”
- Kun kerätään lokit yhteen paikkaan ei ymmärretä mitä kaikkea sillä pysytään tekemään esim. tietoturvan ja ongelman selvityksen kannalta.
- Koitetaan tehdä valmista kerralla.

Lopuksi

- Pelkästään lokien keruu ei tulevaisuudessa tule riittämään jotta ulkoa tulevat vaateet täyttyisivät.
- Tietoturva loukkaukset monimutkaistuvat ja niistä on vaikeampi saada selkoa.
- Kannattaa muistaa että on suhteellisen helppoja ja halpoja ratkaisuja lokienkäsittelyyn.
- Lokien keruu järjestelmällä voidaan saada mahtavia hyötyjä tietoturva on vain yksi alue…
- Jos lokien hallinta kiinnostaa …



shaping tomorrow with you