

Keskitetyn lokienhallinnan esitys

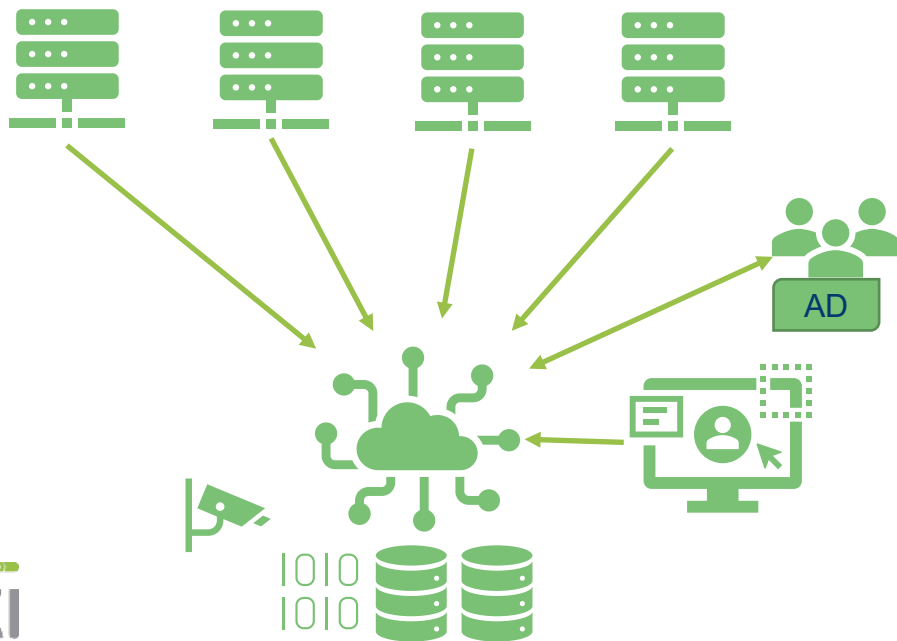


Esittely

- Hiski Jaatinen
- Istekki Oy Tietoturvapalvelut
- Tietoturva-asiantuntija - Lokienhallintapalvelut
- 8 vuotta IT-alalla
- Tekninen sekamies

Keskitetty lokienhallinta

- Security Information and Event Management – SIEM
- Kaikki tietosuojalokit yhdessä paikassa
 - Lokitietopyyntöihin vastaaminen
 - Luotettavat tapahtumaketjut
- Varmistetaan järjestelmien eheys



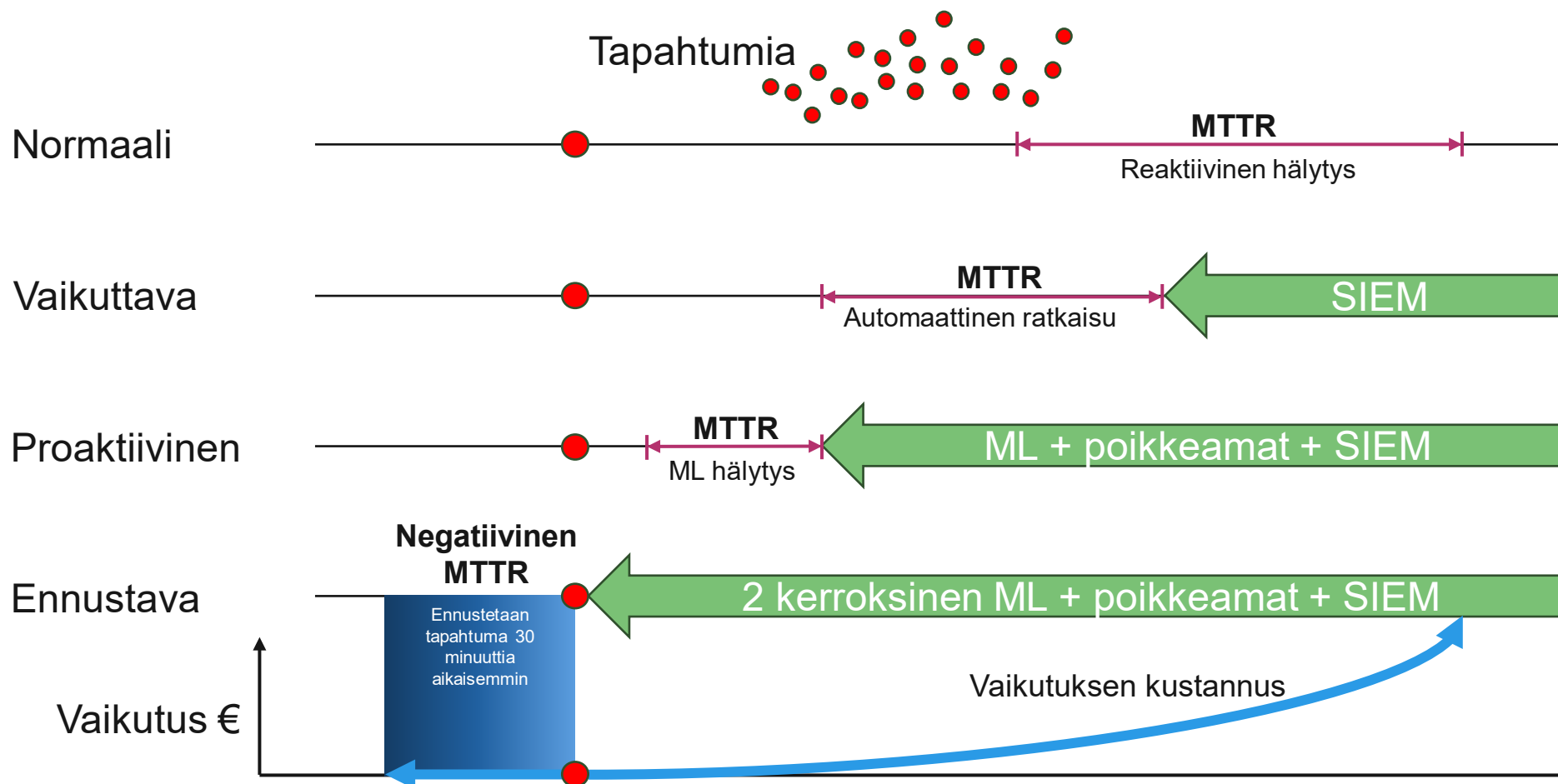
Lokienhallintapalvelussa mm.:
Asiakas- ja potilastietojärjestelmät
Laboratorio- ja kuvantamisjärjestelmät
HR-, työaika-, kulunvalvontajärjestelmät

- Käyttö- ja luovutuslokien tallennus ja säilytys
- Lokien valvonta
- Raportointi

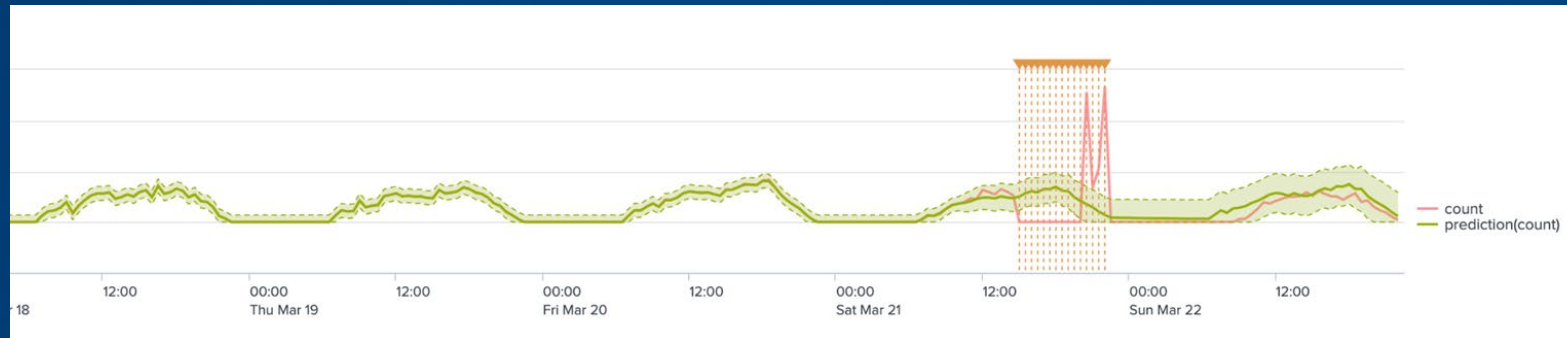
Milloin ja mihin käyttöön?

- Toteutus yleisesti käytössä organisaatioissa
 - Tiedon kerääminen, koostaminen ja analysointi
- Tietoturva ja tietosuoja
 - Monitorointi ja raportointi
 - AI ja ML
 - Varautuminen
 - Muuttuvat vaatimukset
 - Disaster recovery
- AI ja automatisointi
- Tilannekuva
 - Tekninen
 - Auditointi

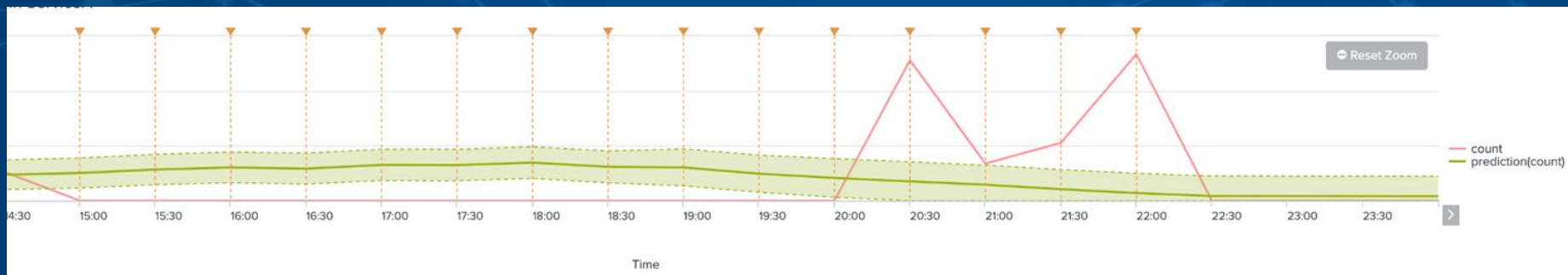
Miksi koneoppimista? MTTR



Poikkeaman havaitseminen

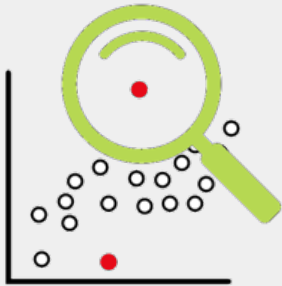


Tarkempi kuva



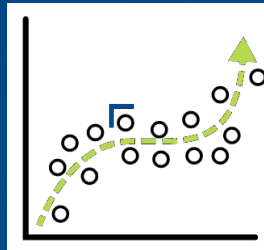
Asiakkaat haluavat vastauksia datasta

Poikkeamien havaitseminen



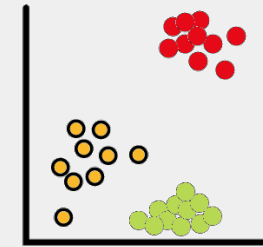
- ▶ Poikkeama aikaisemmasta käytöksestä
- ▶ Poikkeama yhtäläisyyksistä
- ▶ Epätyypilliset muutokset ominaisuuksissa

Ennakoiva analytiikka



- ▶ Ennusta palvelun tila / vaihtelu
- ▶ Tapahtumien ennakointi
- ▶ Trendien ennustaminen
- ▶ Vaikuttavien entiteettien havaitseminen
- ▶ Aikaiset varoitukset vikaantumisesta

Klusterointi



- ▶ Tunnista yhtäläisyydet
- ▶ Tapahtumien korrelaatio
- ▶ Vähennä hälytysmelua
- ▶ Käytöksellinen analytiikka

Mitä jos on useampi lokijärjestelmä?

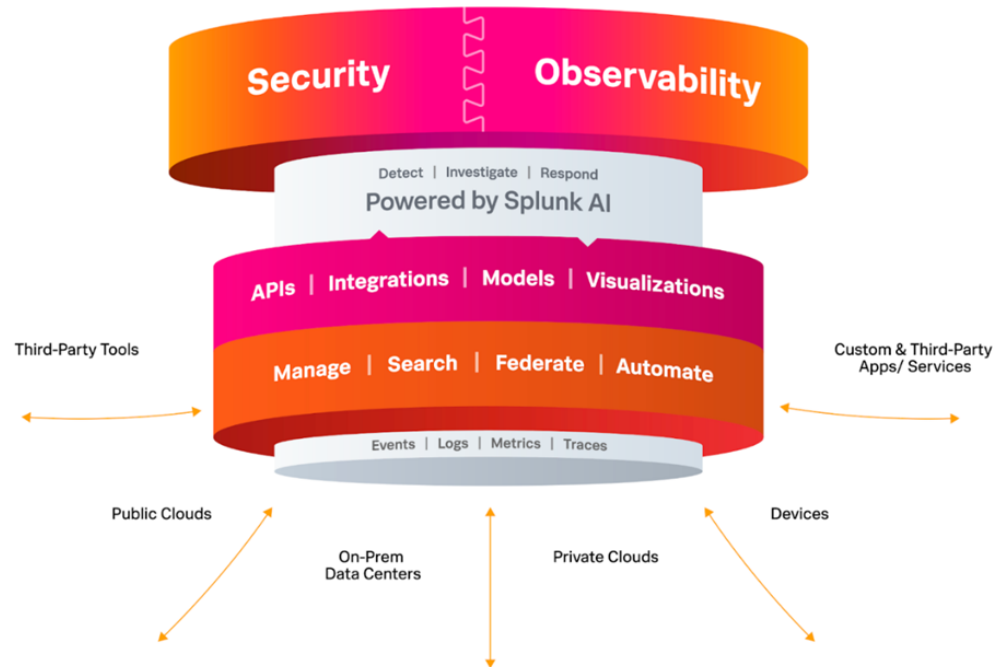
- Monia ratkaisuja ja tuotteita
 - Erilaiset toteutukset
 - Ylläpidolliset ongelmat
 - Ei kuitenkaan aina huono ratkaisu
- Räätelöidyt ratkaisut käyttökohteittain
 - Lukittuja ratkaisuja
 - Integraatiotyöt voivat kestää
 - Erillinen kehitystyö

Miten parantaa lokienhallintaa?

- Tehdään keskitetystä lokienhallinnasta oikeasti keskitettyä
 - Karsitaan monimutkaisuutta
 - Yksinkertaistaa:
 - Toteutus
 - Ylläpito
 - Laajennus
 - Robusti toteutus
 - Suojataan data
 - Todennetaan
- Monitorointi
 - AI ja koneoppiminen
 - Automaatio
 - CIM

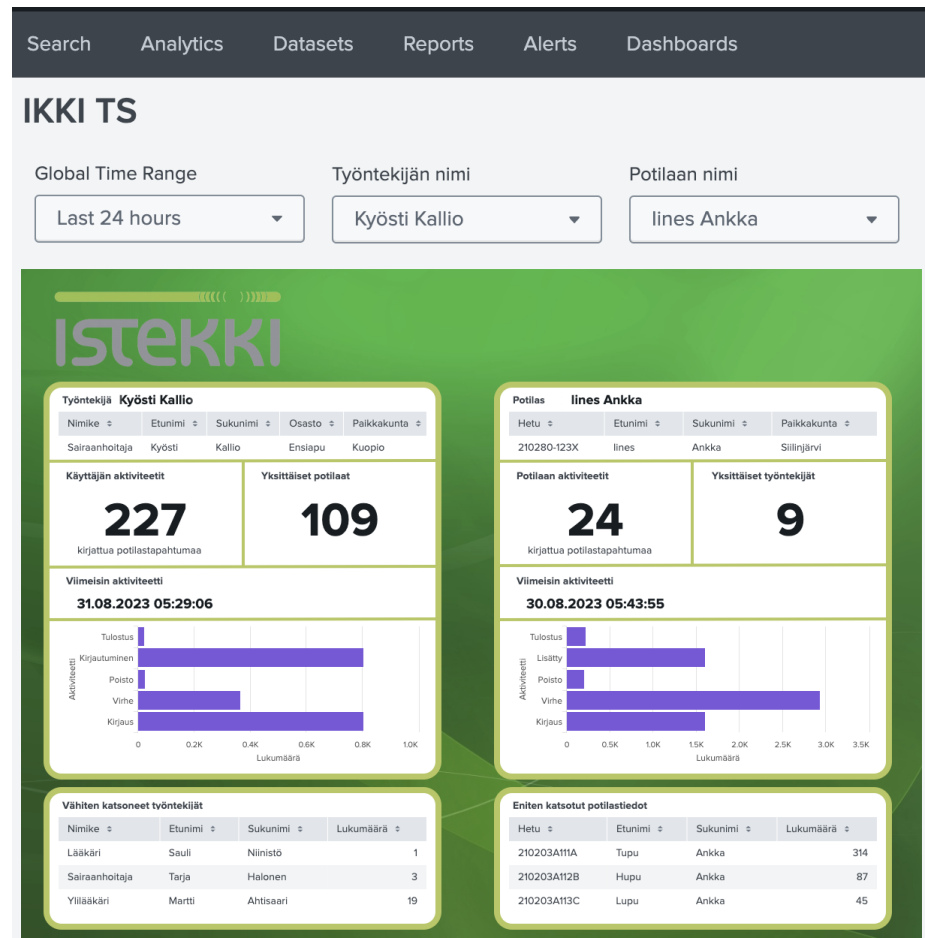
Keskitetty järjestelmä

The Unified Security and Observability Platform



splunk>

Esimerkkejä tulevaisuutta varten



Esimerkkejä tulevaisuutta varten

Search Dashboards Sairaala 1 Sairaala 2 Sairaala 3

Lääkkeet

Global Time Range
Last 24 hours

▼ Lääkkeet
sydän
kasvomaskit

	Varostossa	Tilattu	Keskusvarasto	Saapumis päivä	Inventaatio tehty	Inventaatio OK	Todellinen Varasto
Lääke 1	10	20	●	Keskiviikko	●	●	10
Lääke 2	1	3	●	26.6.2023	●	-1	0
Lääke 3	45	800	●	Keskiviikko	●	-14	31

Lääke 2

Lähin saattavuus	Korvaava lääke	Varastossa	Keskusvarasto
Sairaala 3	Lääke 99	●	●
	Lääke 33	●	●

Search Dashboards Sairaala 1 Sairaala 2 Sairaala 3

Lääke haku

Lääke haku
Burana

	Varostossa	Varasto	Hyllypaikka
Burana 400mg	130	A	H 3
Burana 600mg	230	A	D 1
Burana 800mg	0	B	B 11

Korvaava lääke	Varasto	Hyllypaikka
Ibumax 800	B	B 14

Kiitos!

