



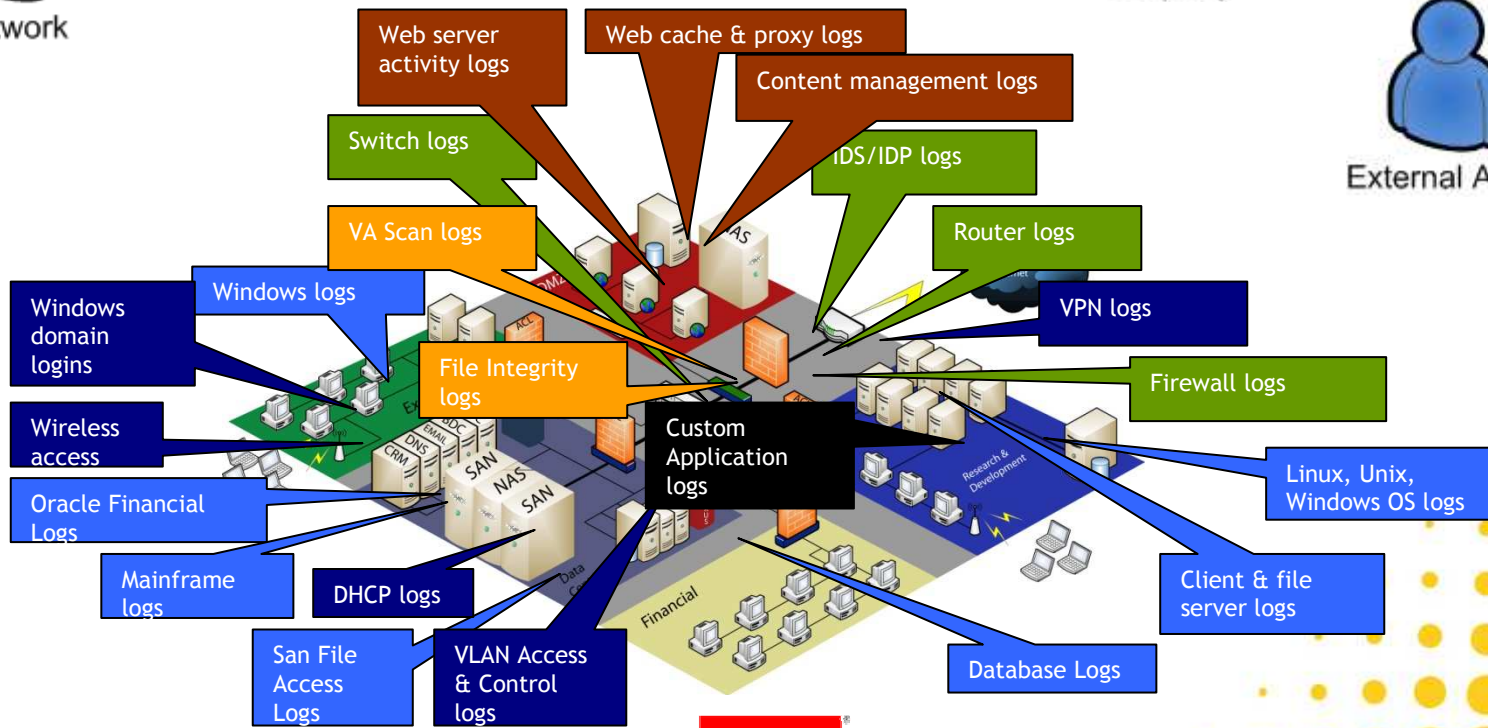
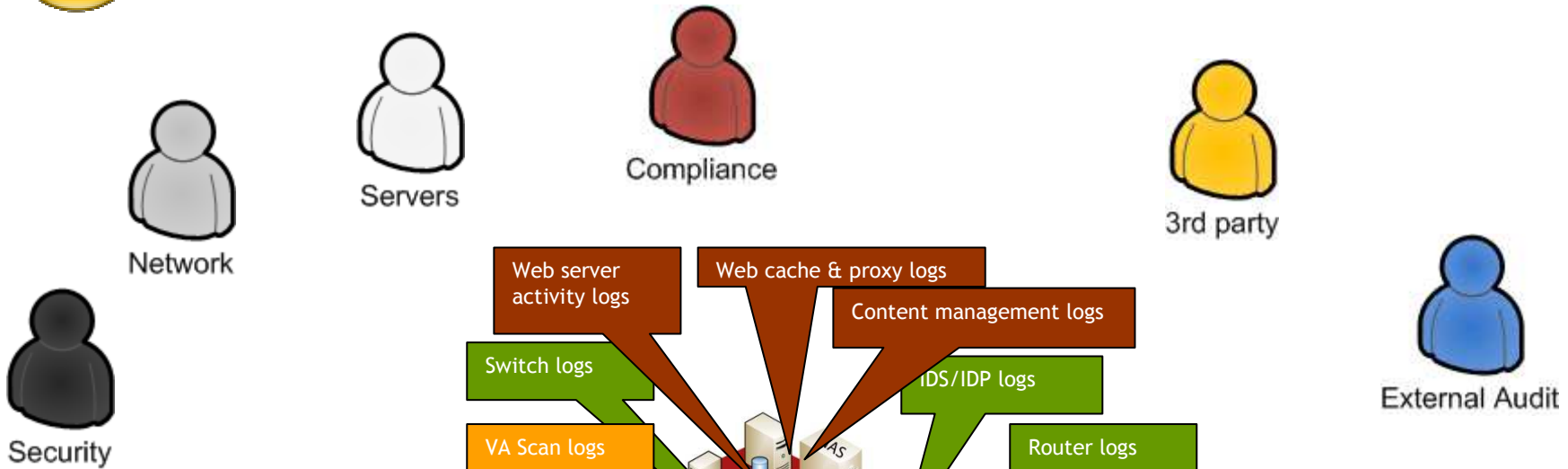
*tietoverkkojen tiennäyttäjä*

Tietoturvatapahtumien ja lokitietojen  
hallintajärjestelmä tarvitaan - mitä muuta?

Antti Jääskeläinen, Tietoturvakonsultti, Cygate Oy



# Käsiksi tietoon...



The Security Division of EMC



tietoverkkojen tietäjä



# Loki & tietoturvatapahtuma → käsite tutuksi



## ○ Loki on luettelo tietojärjestelmien tapahtumista

- Yksittäinen lokirivi kuvaa kokonaisuudessaan yhden tapahtuman tai pienen osa tapahtumasta
- Lokia on monessa muodossa - syslog, SNMP trap, tiedostot...
- Lokeista löytää vikahälytyksiä, suorituskykymerkintöjä, audit-tapahtumia, tunkeutumishälytyksiä, välitystietoja, yhteysstatistiikkaa...
- Lokilähteitä voi olla... paljon...

## ○ Tietoturvatapahtuma on yksittäinen lokimerkintä tai monen lokimerkinnän summa

- Tietoturvatapahtumat poimitaan lokeista
- Failed login, portscan, DoS-attempt...



# Miksi kaikkien tulisi kerätä ja tarkastella lokeja?

1. Kaikki hyvät tietoturvastrategiat ja -käytännöt ohjaavat tai pakottavat tähän
  - Käy lokeja läpi säännöllisesti/päivittäin - Valtionhallinnon tietoturvasot, PCI DSS, ISO 27002... - tilintarkastus?
2. Jotain tapahtui verkossa → vikatilanne, mahdollinen tietoturvaongelma
  - Mistä tiedät varmuudella, ellet tarkastele asiaa lokeista?
3. Are you owned!?
  - Miten voit tietää väärinkäytöksistä tai väärinkäytönyrityksistä, jos lokisi makaavat nauhoilla kassakaapissa?
4. Verkko on hidas, palvelu tökkii, palvelun kehittäjät syyttävät verkkoa ja päinvastoin
  - Osoita syyttävällä sormella oikeaan paikkaan, yksinkertaista ongelmanratkaisua ja säästä kustannuksissa
5. Käyttäjät aulaneidistä, järjestelmänvalvojan kautta toimitusjohtajaan
  - Jokainen jättää jälkensä, miksi/kuka admin teki muutoksen joka kaatoi koko palvelun (käyttö, muutokset jne.)
6. Erorria pukkaa ja trendikäyrät osoittavat koiliseen
  - Joskus vähän hölmöä lokia, mutta joskus se kertoo siitä, että kohta osuu tuulettimeen - katse tulevaisuuteen
7. Toimiiko luotu tietoturvapoliitikka?
  - Varmista toimivuus lokeista
8. Monitoimittajaympäristön tapahtumista ei ole selkeää kuvaa
  - Toimittaja x raportoi palvelussaan asiasta 1 ja 2, ja toimittaja y ei raportoi juuri mistään
9. Nuku yösi paremmin, kun tietosi ovat vakuutettuna

Zzz. Tähän tarvitaan oikea lokijärjestelmä ja asiantuntemusta





# Miksi kaikkien tulisi kerätä ja tarkastella lokeja?

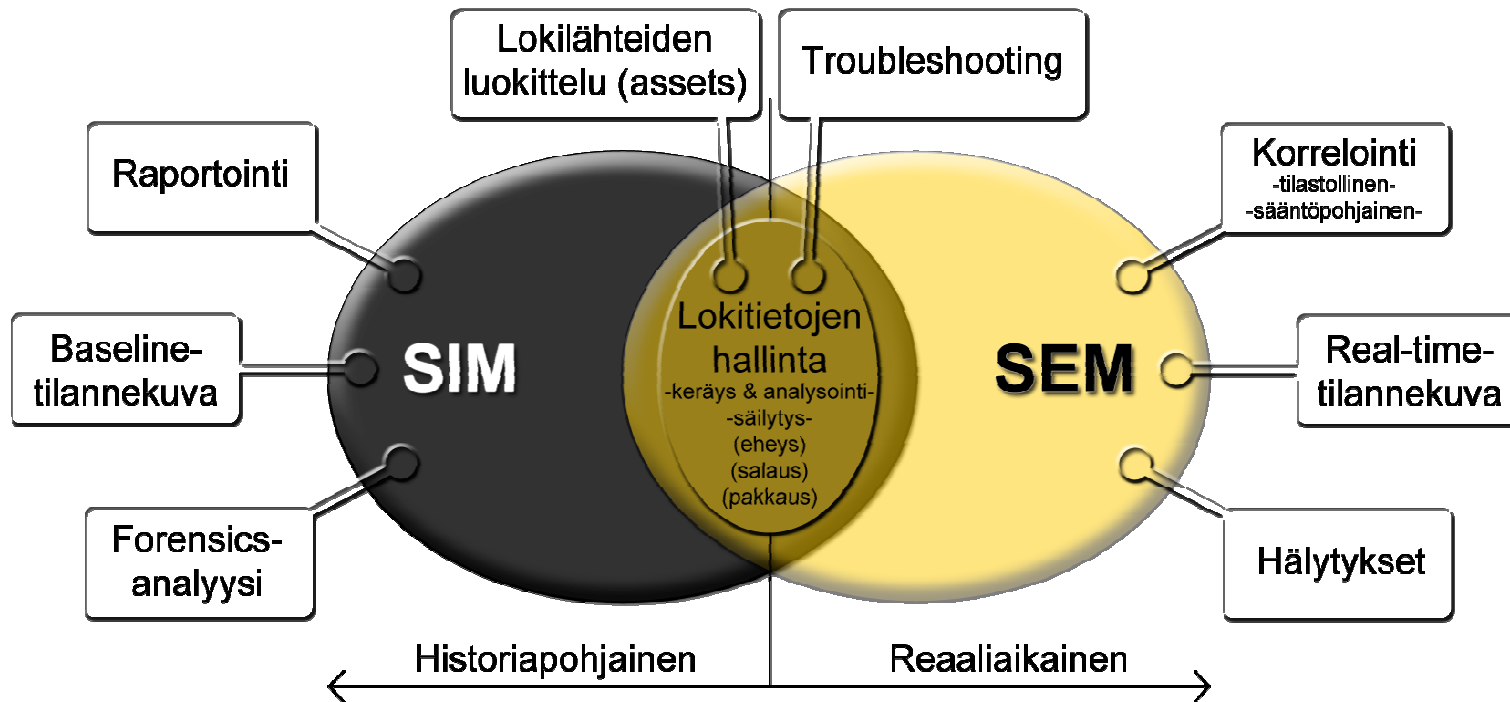
1. Kaikki hyvät tietoturvastrategiat ja -käytännöt ohjaavat tai pakottavat tähän
  - Käy lokeja läpi säännöllisesti/päivittäin - Valtionhallinnon tietoturvasatot, PCI DSS, ISO 27002... - tilintarkastus?
2. Jotain tapahtui verkossa → vikatilanne mahdollinen tietoturvaongelma
  - Mistä tiedät varmuudella, ellet tarkastele asioita?
3. Are you owned!?
  - Miten voit tietää väärinkäytöksistä tai... s lokisi makaavat nauhoilla kassakaapissa?
4. Verkko on hidas, palvelu tö...
  - Osoita syyttävällä sormella oike... ratkaisua ja säästä kustannuksissa
5. Käyttäjät aulaneidist...
  - Jokainen jättää jälkensä... palvelun (käyttö, muutokset jne.)
6. Erorria pukkaa...
  - Joskus vähän hi... - katse tulevaisuuteen
7. Toimiiko l...
  - Varmista...
8. Moni...
  - T...
- 9.

Strategiat ja käytännöt ohjaavat toimintaa sekä prosessien kehittämistä





# Security Information and Event Management



SIEM-järjestelmä ei ole verkon ja sen palveluiden käytettävyyden valvontaan erikoistunut työkalu! → Security / Troubleshooting



# Netistä poimittua

## ◉ SIEM Market is a Failure

"I have always regarded Security Event Management (SEM) as **the most dysfunctional segment** in the security industry."

"SEM vendors would always preach rapid response and attack prevention, even though they only examine log file entries written **long after the attack has come and gone.**"

"It has just been a **brain-dead market segment.**"

*And, on the other hand,* what is needed is a "**good place to collect, filter, and manage audit logs of corporate activity.**"

Monday, April 24, 2006 - Posted by Dr Anton Chuvakin

<http://chuvakin.blogspot.com/>



# SIEM evoluutio / prosessit

**Tietämättömyys lokeista**  
- Lokeja ei kerätä eikä analysoida -

**Lokien kerääminen**  
- Lokeja kerätään ja taltioidaan, mutta niitä ei ikinä tarkastella -

**Lokien analysointi**  
- Lokeja kerätään + tarkastellaan, mikäli jotain on tapahtunut -

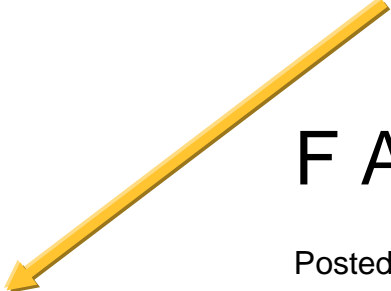
**Lokien raportointi**  
- Lokeja kerätään + raportteja tarkastellaan kerran kuukaudessa -

**Lokien säännöllinen tarkastelu**  
- Lokeja kerätään + tarkastellaan päivittäin -  
[Tapahtumien valvonta jälkikäteen]

**Lokien avulla tehtävä monitorointi**  
- Tietoturvallisuutta valvotaan lähes reaaliajassa -

~~SEM  
Täysin reaaliaikainen seuranta~~

Mitä tapahtuu, jos aloittaa jostain tuolta välistä?



**FAIL!**

Posted by Dr Anton Chuvakin



# Vaiheista tai feilaa!

Vaihe 1/4

## 🕒 Vaihe 1 - Lokitiedot keskitetysti & turvautusti talteen

- Lokijärjestelmän piiriin otetaan palomuurit, VPN-järjestelmät, kytkimet/reitittimet sekä Windows- ja Linux-palvelimet
- Lokijärjestelmät piiriin voidaan ottaa pelkästään myös kriittisimmät lähteet kuten esimerkiksi joku dedikoitu tietojärjestelmä
- Lokit tuodaan järjestelmään pääasiassa säilytystä ja mahdollisesti myös jälkikäteisanalysointia varten
- Lokien elinkaari toteutetaan kuntoon ja järjestelmän käytettävyys varmistetaan mahdollisimman hyvin

### Vaihe 1

Lokitiedot keskitetysti  
& turvautusti talteen



# Vaiheista tai feilaa!

Vaihe 2/4

## ○ Vaihe 2 - Lokitietojen analysointia ja raportointia

- Lisätään lokilähteitä
- Lisätään raportointia halutuista tapahtumista (Dashboard-näkymät, analysointiraportit, kuukausiraportit jne.)
- Suunnitellaan raporttien läpikäyntiin ja tapahtumien mahdollisiin analysointeihin formaalit prosessit
- Otetaan huomioon eri käyttäjäryhmät sekä tarpeet (erilaiset Dashboardit - Security/Network/Server)



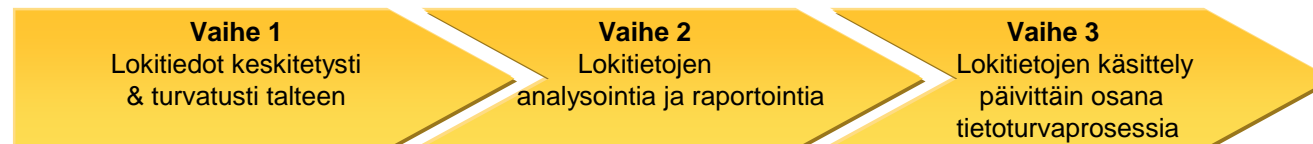


# Vaiheista tai feilaa!

Vaihe 3/4

## ○ Vaihe 3 - Lokitietojen käsittely päivittäin osana tietoturvasprosessia

- Kehitetään tietoturvasprosesseja siten, että lokeja seurataan tiettyjen tapahtumien osalta päivittäin
- Kehitetään analysointiraportteja ja Dashboard-näkymiä siten, että tietoturvaspoikkeukset ja vikatilanteet saadaan selvitettyä mahdollisimman nopeasti sekä tarkasti
- Luodaan tietyistä tapahtumista hälytyksiä (trendeistä, yksittäisistä tapahtumista, korreloituja hälyjä)





# Vaiheista tai feilaa!

Vaihe 4/4

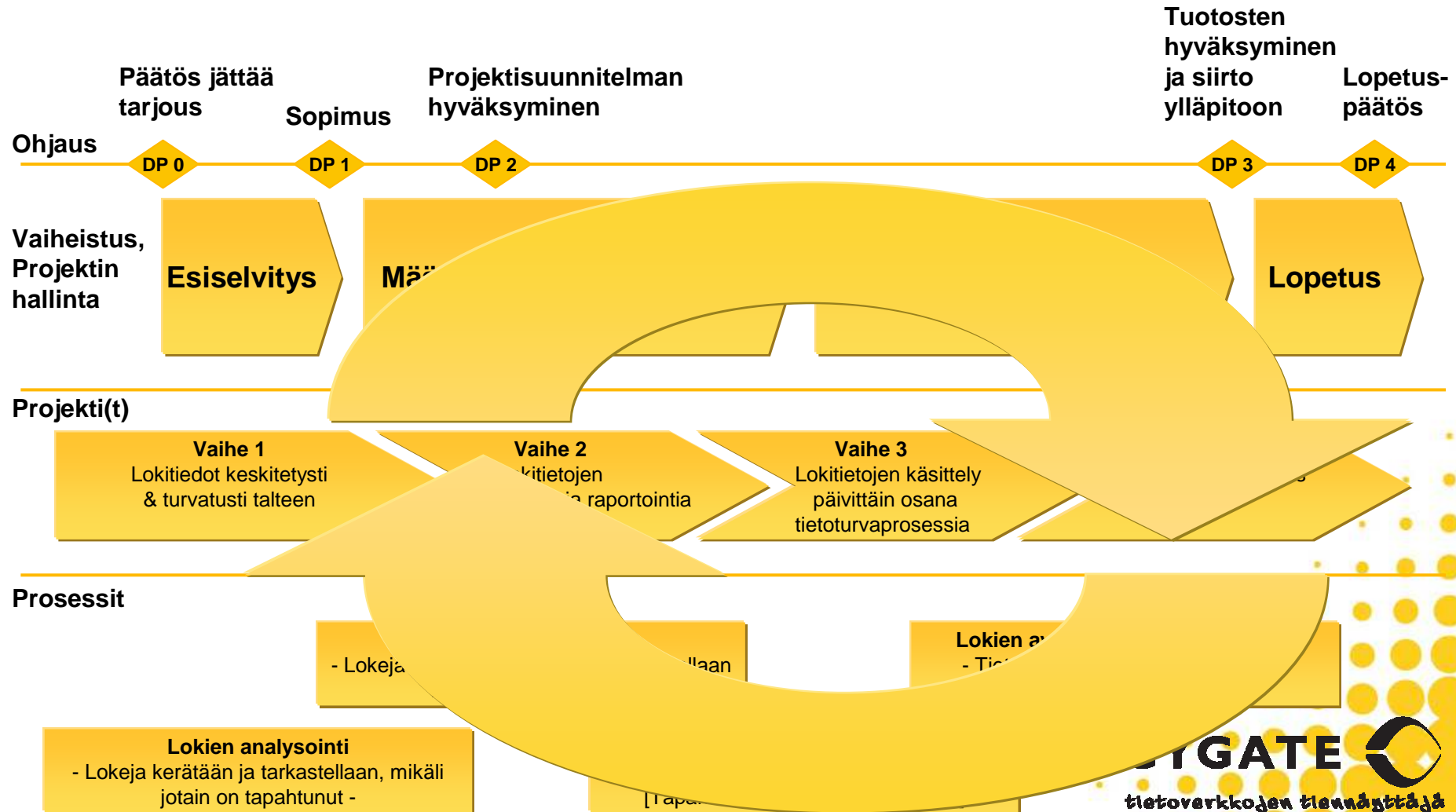
## ○ Vaihe 4 - Security Operations Center

- Tietoturvasprosessien tehostaminen Security Operations Center - toiminnallisuutta (SOC) ajatellen → ”Tietoturvavalvomo”
- Tietoturvatapahtumien käsittely jatkuvana prosessina - hälytyksistä syiden etsintään ja tapahtumien selvittämiseen
- Tietoturvapoikkeamien ilmoittaminen



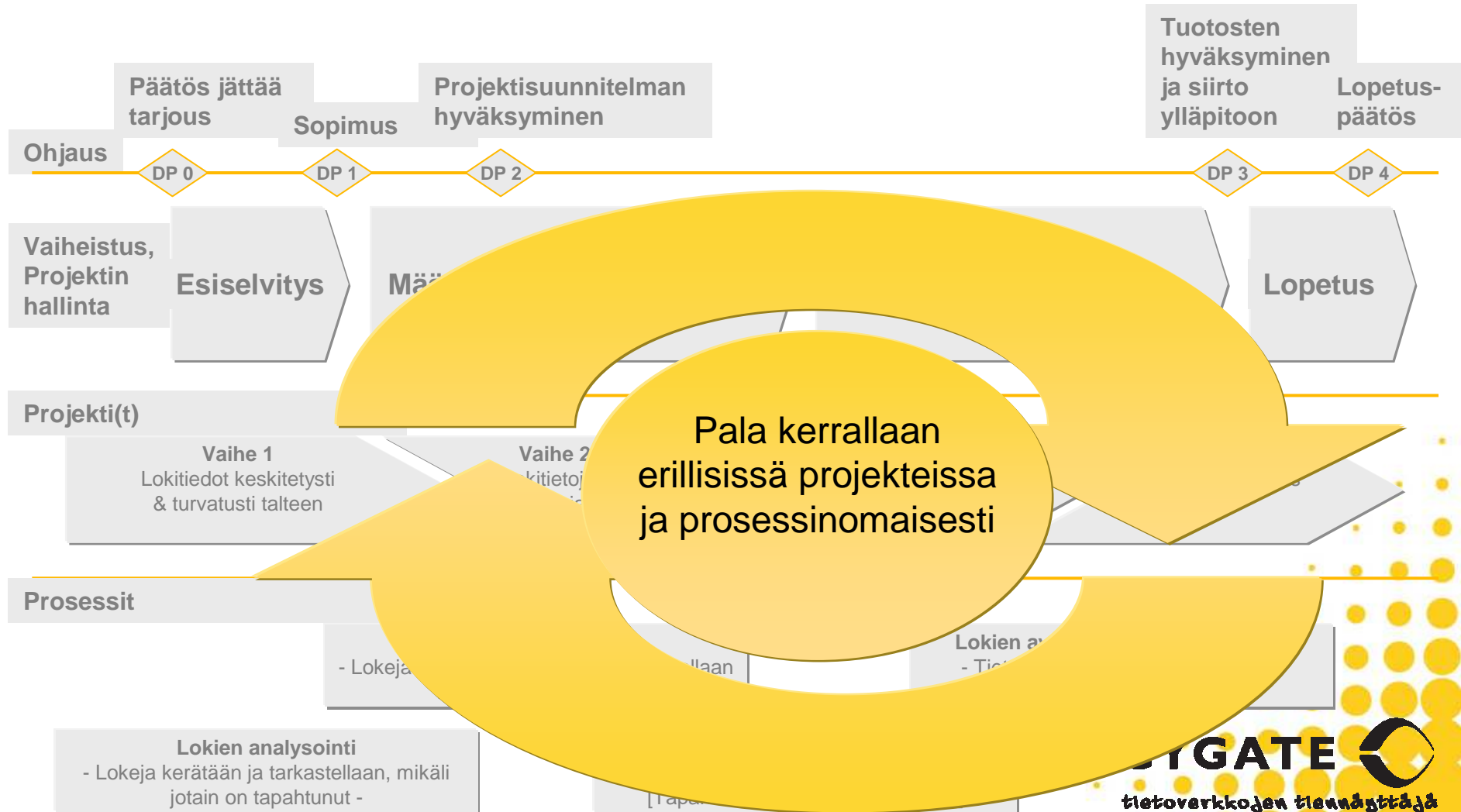


# Toteutus hallittuna projektina ja jalkautus prosesseihin





# Toteutus hallittuna projektina ja jalkautus prosesseihin





# Kokemuksia ja haasteita SIEM-projekteista

## ○ Ilman suunnitelmaa, vaiheistusta ja aikataulutusta homma ei rokkaa

- SIEM-järjestelmä ei yksistään ratkaise ongelmia
- Varaa resurssit, panosta projektin koordinointiin ja varaudu yllätyksiin
- Projektista prosessiksi → ei pidä unohtaa prosesseja
- Huomio lait ja ohjeistukset
- Dokumentoi → järjestelmä ja politiikat

## ○ Käytännössä?

- Lokiprojekti koskee ”parhaimmillaan” kaikkia järjestelmiä - kuka vastaa muutoksista ja millä aikataululla?
- Lokia ja raportteja on paljon - mitä pitäisi seurata / mistä liikkeelle?
- Tekninen haaste vs tekemisen haaste?
- Omat sovellukset - saadaanko sitä lokia?
- Muut projektit venyttävät SIEM-projektia



# Quick & Dirty

## Tietämättömyys lokeista

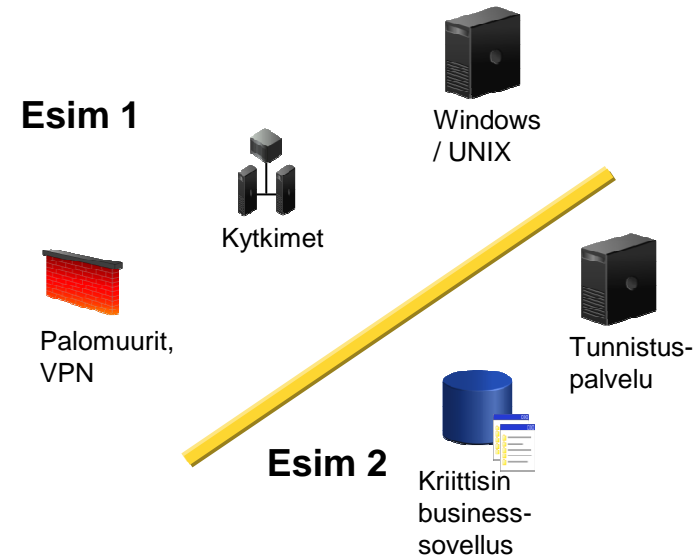
- Lokeja ei kerätä eikä analysoida -

## Lokien kerääminen

- Lokeja kerätään ja taltioidaan, mutta niitä ei ikinä tarkastella -

## Lokien analysointi

- Lokeja kerätään + tarkastellaan, mikäli jotain on tapahtunut -



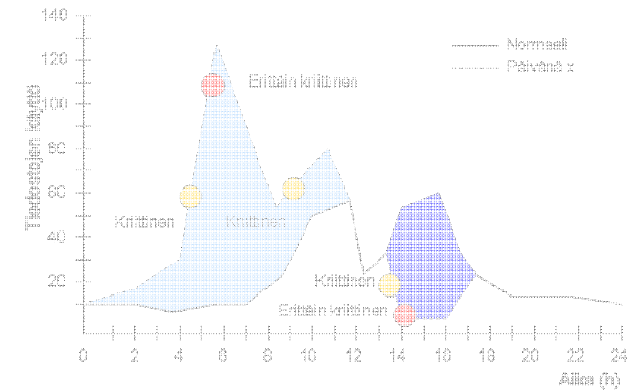
- Liikkeelle kevyesti
- Vaihe 1 ja kriittisimmät järjestelmät - kiistämättömyys
- Joskus tämä tulee vastaan kuitenkin

### Vaihe 1

Lokitiedot keskitetyksi  
& turvatusi talteen

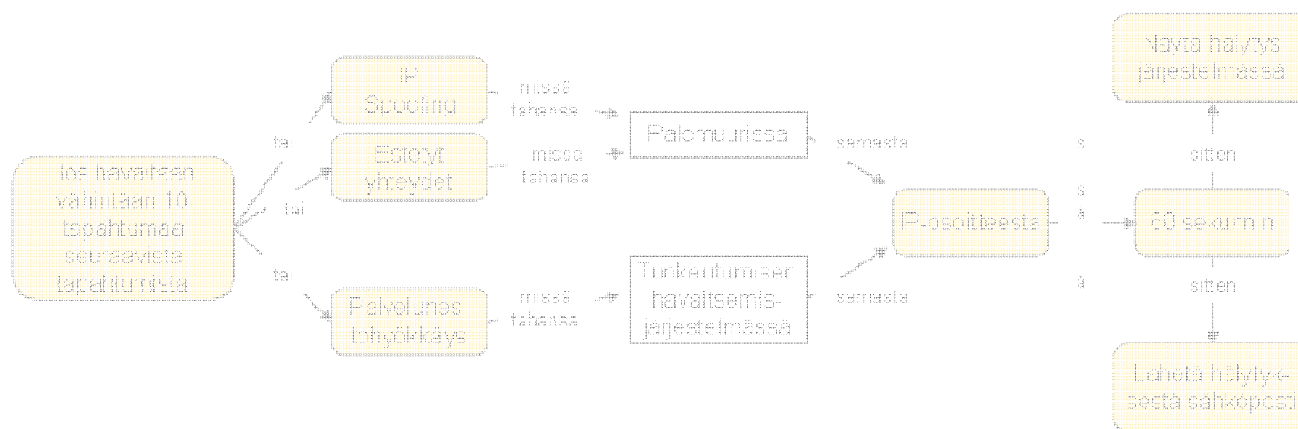


# Mites se SEM sitten?



## SIEM-tukee SEM:ia, mutta ei kata kaikkia tarpeita

- SIEM skouppaa host-tason (login failures, trend-hälyt jne.) ja säilyttää jäljen, mutta IDS/IPS ja haavoittuvuustietoisuus kannattaa jättää hälytysten osalta erilleen → sama AntiVirus -ratkaisujen osalta
- Verkkopohjaisesti suosittelemme ”sikamaisempaa” ratkaisua





# Miksi kaikkien tulisi kerätä ja tarkastella lokeja?

1. Kaikki hyvät tietoturvastrategiat ja -käytännöt ohjaavat tai pakottavat tähän
  - Käy lokeja läpi säännöllisesti/päivittäin - Valtionhallinnon tietoturvasot, PCI DSS, ISO 27002... - tilintarkastus?
2. Jotain tapahtui verkossa → vikatilanne, mahdollinen tietoturvaongelma
  - Mistä tiedät varmuudella, ellet tarkastele asiaa lokeista?
3. Are you owned!?
  - Miten voit tietää väärinkäytöksistä tai väärinkäytönyrityksistä, jos lokisi makaavat nauhoilla kassakaapissa?
4. Verkko on hidas, palvelu tökkii, palvelun kehittäjät syyttävät verkkoa ja päinvastoin
  - Osoita syyttävällä sormella oikeaan paikkaan, yksinkertaista ongelmanratkaisua ja säästä kustannuksissa
5. Käyttäjät aulaneidistä, järjestelmänvalvojan kautta toimitusjohtajaan
  - Jokainen jättää jälkensä, miksi/kuka admin teki muutoksen joka kaatoi koko palvelun (käyttö, muutokset jne.)
6. Erorria pukkaa ja trendikäyrät osoittavat koiliseen
  - Joskus vähän hölmöä lokia, mutta joskus se kertoo siitä, että kohta osuu tuulettimeen - katse tulevaisuuteen
7. Toimiiko luotu tietoturvapolitiikka?
  - Varmista toimivuus lokeista
8. Monitoimittajaympäristön tapahtumista ei ole selkeää kuvaa
  - Toimittaja x raportoi palvelussaan asiasta 1 ja 2, ja toimittaja y ei raportoi juuri mistään
9. Nuku yösi paremmin, kun tietosi ovat vakuutettuna

Zzz. Tähän tarvitaan oikea lokijärjestelmä ja asiantuntemusta





Kysymyksiä ?

Antti Jääskeläinen, Tietoturvakonsultti, Cygate Oy

Lisätietoja Cygaten tietoturvaratkaisuista ja -palveluista

[www.cygate.fi](http://www.cygate.fi)