



Det här är SIEM & Log Management

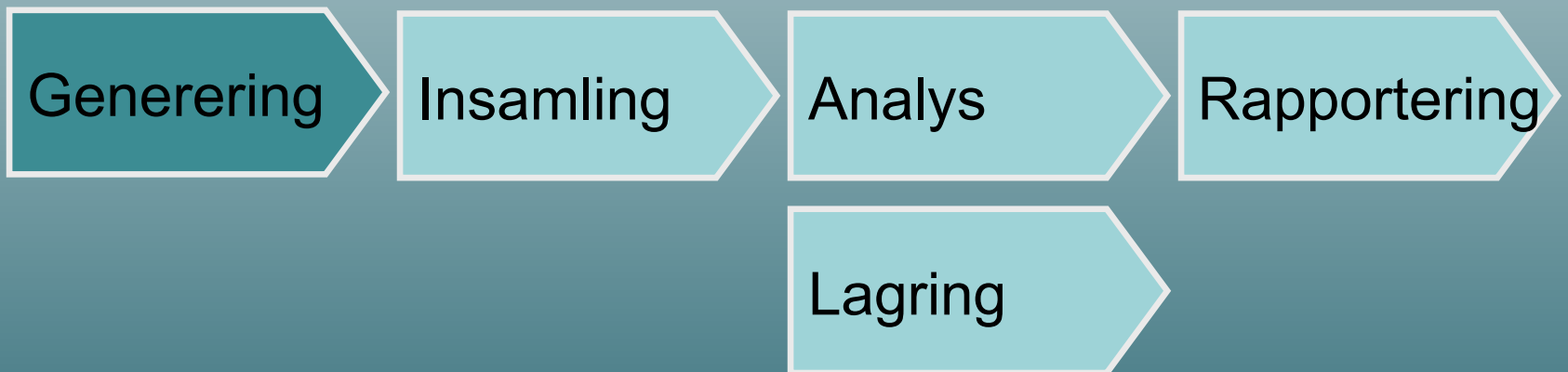
Mats Pettersson
IT-Säkerhetskonsult – SIEM Expert
mats.t.pettersson@heimore.com

Vad är Log Management & SIEM?

- Många termer
 - LM (Log Management)
 - SIM (Security Information Management)
 - SEM (Security Event Management)
 - SIEM (Security Information and Event Management)
- Betydelse
 - Vad betyder de?
 - Vilka behov uppfyller de?
 - Vilka problem löser de?
- Vad är vårt problem och vilket är vårt behov?

SIEM-processen

- Kontroll av händelser i IT-infrastrukturen
 - Säkerhetsrelevanta händelser
- Aktiviteter som behöver utföras



Aktivitet - Generering

- Funktionalitet
 - Definiera säkerhetsrelevanta händelser
 - Skapa nödvändig information
 - Vem gör vad på vilken information?
- Komplexitet
 - Kan all nödvändig information verkligen skapas?
 - Hur påverkar detta exempelvis prestanda?

Aktivitet - Insamling

- Funktionalitet
 - Samla in information utspridd i infrastrukturen
 - Läsa och tolka informationen
 - Prioritera informationen

- Komplexitet
 - Vad betyder egentligen informationen?
 - Påverkan på infrastrukturen?
 - Måste informationen bevaras i sin ursprungliga form?

Aktivitet - Analys

- Funktionalitet
 - Vem gör / har gjort vad på vilken information
 - Regler för kontinuerlig kontroll i nära realtid
 - Sökfunktionalitet och identifiering utav mönster
- Komplexitet
 - Vem är användaren?
 - Vad är en otillåten händelse eller ett mönster?

Aktivitet - Lagring

- Funktionalitet
 - Lagra informationen under längre tid
 - Garantera att informationen är oförändrad
 - Gallra gammal information
- Komplexitet
 - Vilka informationsmängder och volymer skall lagras?
 - Ej förändringsbar men ändå möjlig att rensa

Aktivitet - Rapportering

- Funktionalitet
 - Presentera analysresultat
 - Larm, sökresultat, rapporter
 - Exportera och distribuera
- Komplexitet
 - Många olika intressenter
 - Effektiv koppling till incidenthanteringsprocess

Strategier emot komplexitet

- Informationsmängd och dess volym
 - 10 EPS = 864 000 EPD, 1000 EPS = 86 400 000 EPD
 - 1 händelse = 500 Bytes => ca 40 GB / dag
- Relevant information
 - Utreda eller inte
 - Bortfiltrering alternativt insamla allt
- Prioriterad funktionalitet
 - Snabba åtgärder?
 - Detaljerad information om händelsen?

Strategi - SIM

- Security Information Management
 - Insamling och lagring med grundläggande funktionalitet för analys och rapportering
 - Informationscentrerad
 - Fokuserar på att samla in så komplett information som möjligt
 - Kräver längre tid för att göra analys och rapportering
 - Det är först när du gör analysen som du vet vilken information som är viktig!

Strategi - SEM

- Security Event Management
 - Insamling, analys och rapportering med grundläggande korttidslagring av informationen
 - Händelsecentrerad
 - Fokuserar på snabb insamling och analys med rapportering (larm)
 - Bortfiltrering av information
 - Korttidslagring av insamlad information
 - Du vet redan vilka händelser som är viktiga och du vill ha möjligheten att reagera snabbt på dem!

Strategi - SIEM

- Security Information and Event Management
 - En kombination av SIM och SEM
 - Det bästa av båda världar

Frågeställningar

- Innebär detta all funktionalitet?
- Om inte – vilken delmängd?
- Matchar detta just din prioritering?
- En eller två produkter?

Avslutning & frågor

- Hur passar denna process in i din verksamhet?
 - Säkerhetspolicy och incidenthanteringsrutin
 - Vad i denna process prioriterar du?

