
TeliaSonera

# Intrångsdetekteringssystem (IDS)

Håkan Kvarnström
TeliaSonera R&D

# Ur nyhetsflödet i sommar...

## Gartner: Intrusion Detection On The Way Out

June 13, 2003

EMAIL THIS ARTICLE
PRINT THIS ARTICLE
DISCUSS THIS ARTICLE
WRITE TO AN EDITOR

**The research firm says the software, which attempts to spot and report attacks against information systems, will no longer be necessary in a couple of years.**

By George V. Hulme

Intrusion-detection systems—software that attempts to spot and report attacks against information systems—will no longer be a defense in the information security pro's arsenal by 2005. That's the prediction coming out of research firm Gartner.

"IDS as a security technology is going to disappear," says Richard Stiennon, a Gartner research director.

"Imagine a world where there are no intrusions"

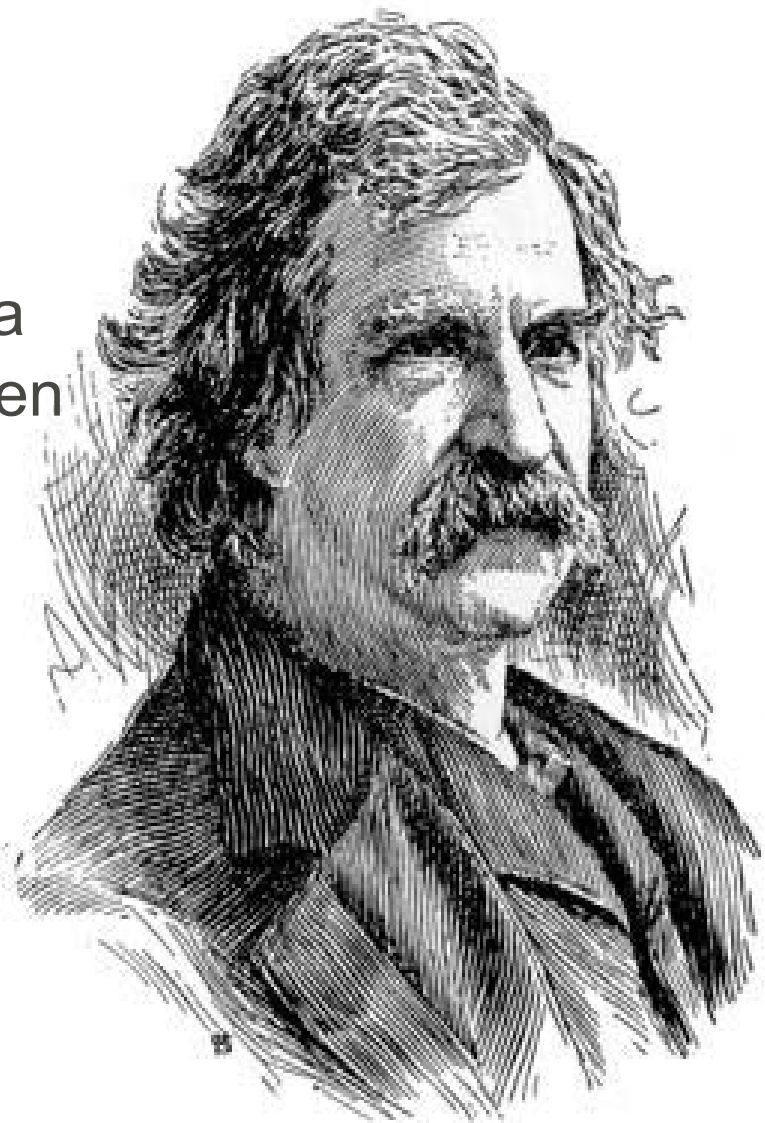
# Innehåll

- Varför behövs IDS?
- Kort introduktion till IDS
- Överväganden vid införande
- Vision
- Aktuella forskningsområden
- Sammanfattning

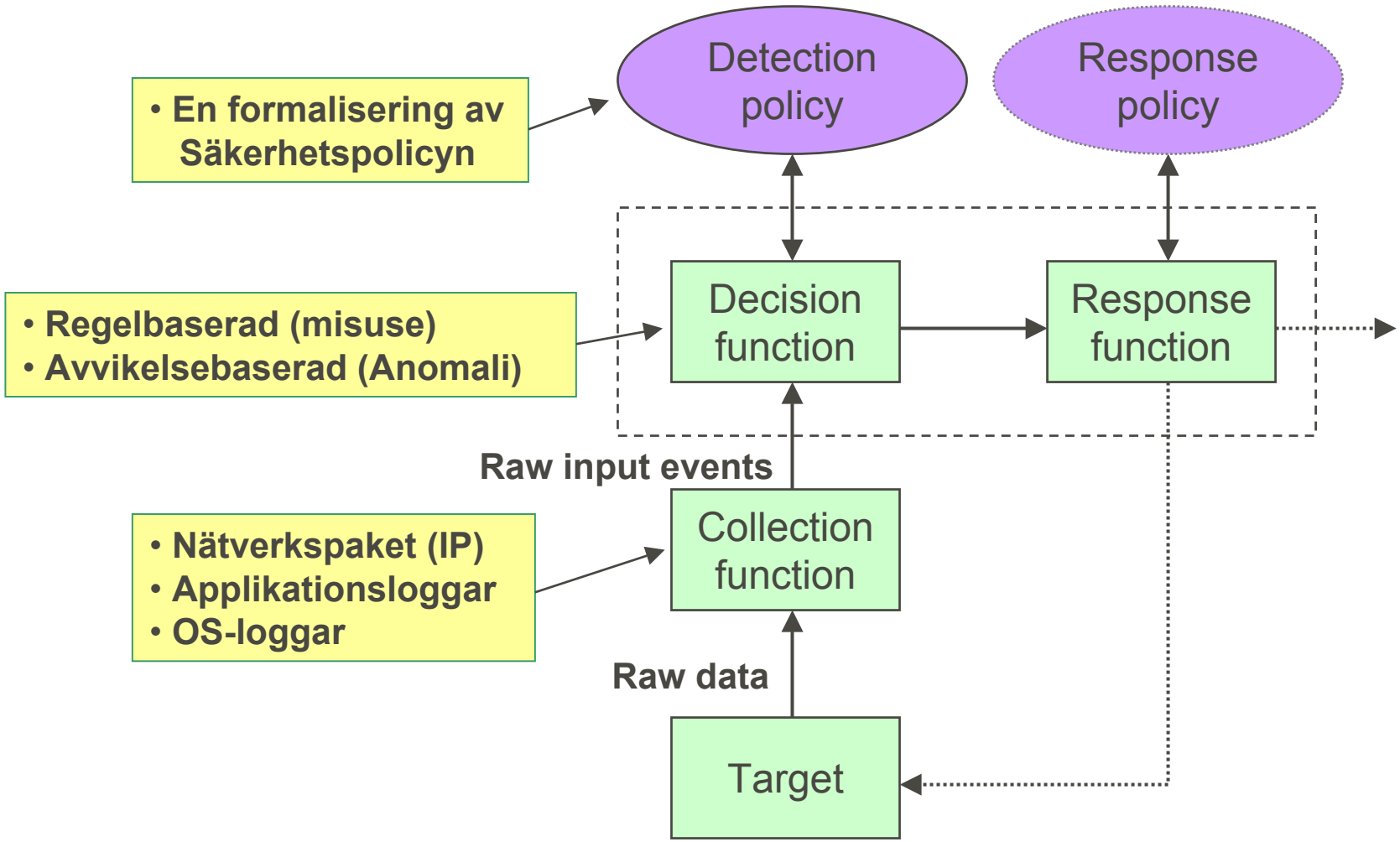
# “Ryktet om min död är betydligt överdrivet”

IDS har en framtid därför att:

- Människan är felbar och felar ofta
- Nya teknik innebär nya oförutsedda hot och buggar och det finns alltid en bug till, och en till...
- Djup i försvaret är en sund design
- Insiderhotet är inte försumbart
- Människan har ett starkt begär efter vinning, ära och berömmelse



# Kort introduktion till IDS



# Några överväganden vid införande av IDS

- COTS vs. Open Source
  - Vad får det kosta i inköp och underhåll?
  - Vem har ansvaret för att sköta uppdateringar av attackdatabasen?
- ”Host”- eller nätverksbaserad
  - Vilka attacker vill vi leta efter?
  - Vilka datamängder skall analyseras?
  - Hur ser mina kommunikationsmönster ut?
- Signatur- eller anomalibaserad
  - Vad är viktigast – Få falsklarm eller självlärande egenskaper?
  - Vilka attacker vill vi leta efter?

# Några överväganden vid införande av IDS

- Arkitektur – Centraliserad vs. distribuerad
  - Var samlar vi in och var lagrar vi loggdata?
  - Hur, var och när sker analys av data?
  - Ger tydliga säkerhetskonsekvenser
- Placering i IT-infrastrukturen
  - Innanför eller utanför brandväggen?
    Eller både och?
- Affärsmässigt motiverat
  - Skadekostnad vs. Investerings- och driftskostnad
- Legala krav
  - T.ex. EU-direktiv (privacy)

# Vart är vi på väg?

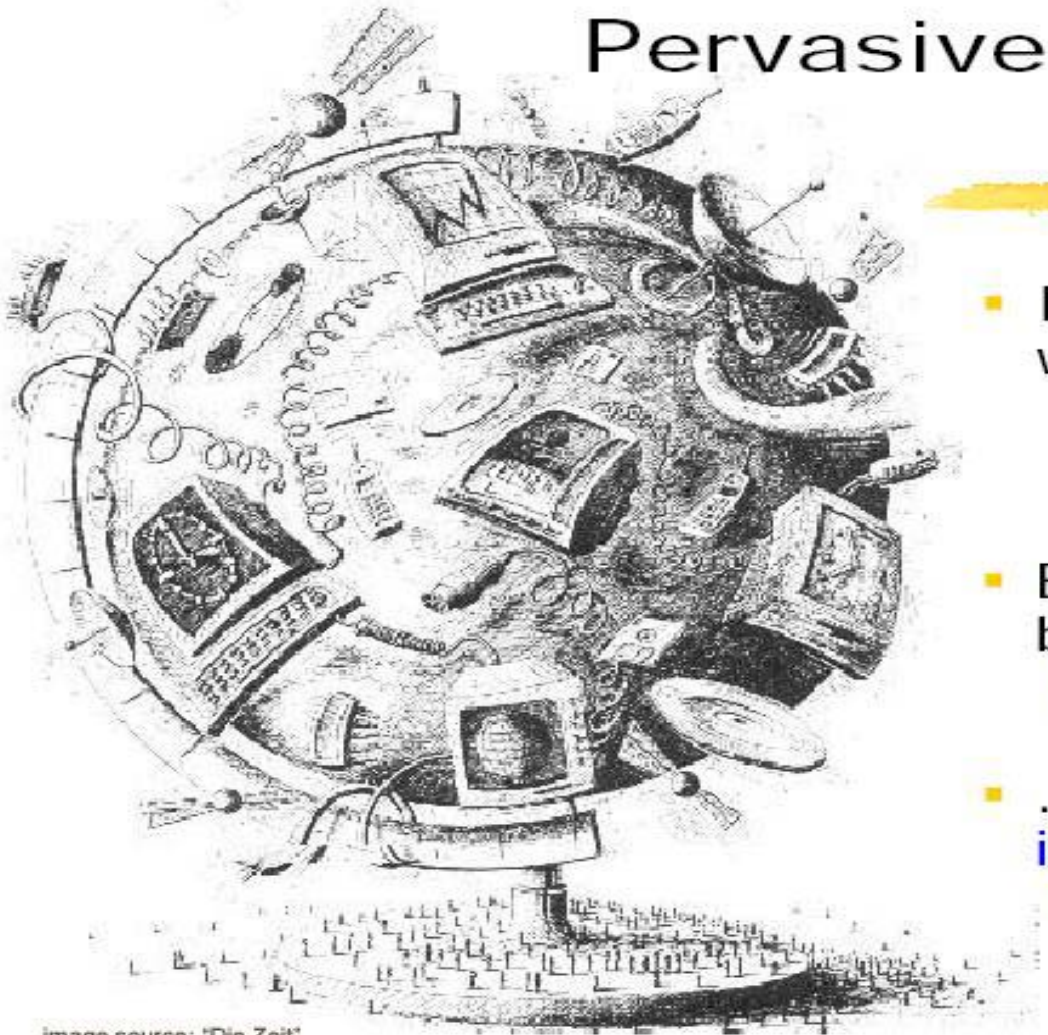


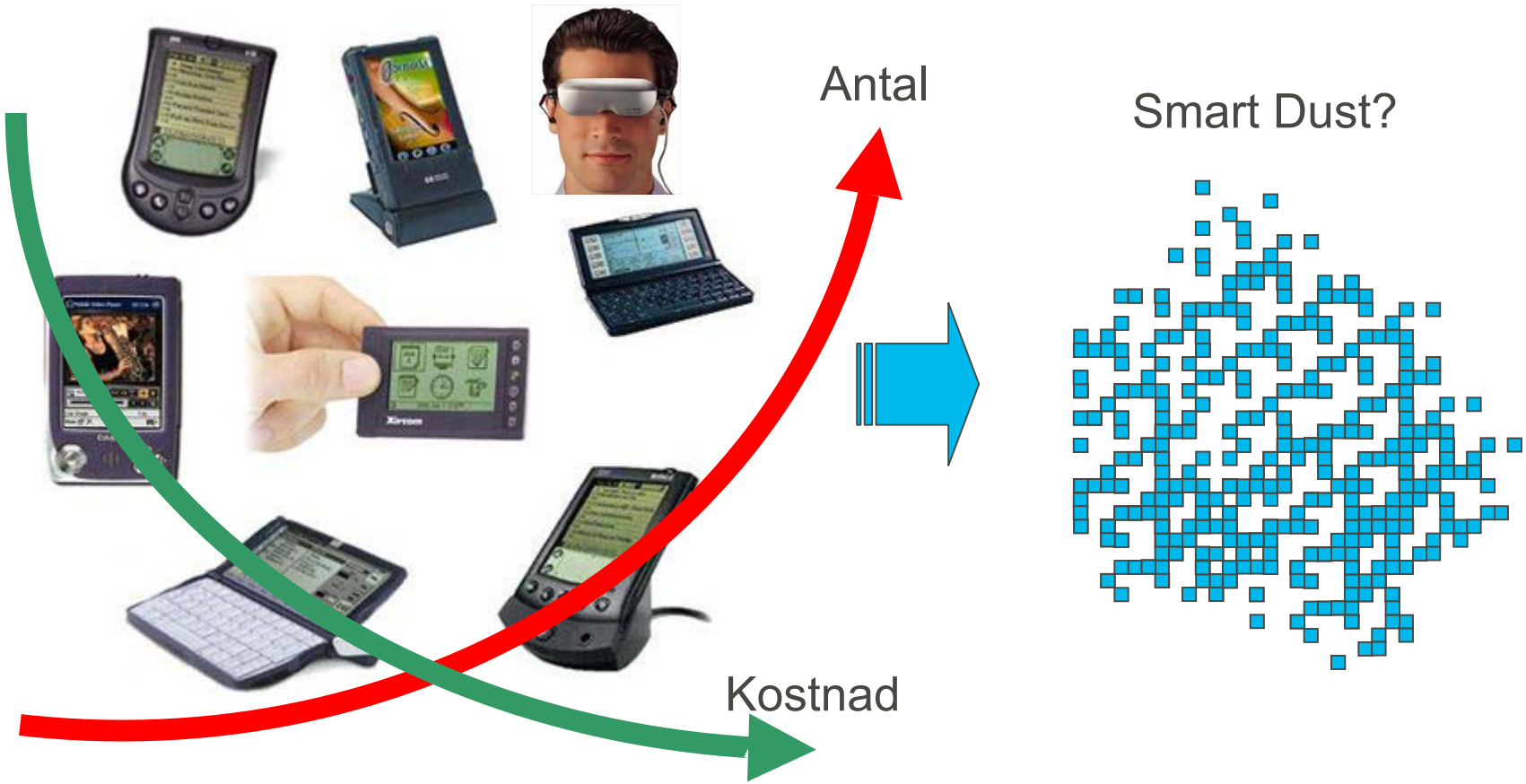
image source: "Die Zeit"

## Pervasive / Ubiquitous Computing

- Information technology will be everywhere
- Everyday objects will become smart
  - embedded processors
- ...and they will all be interconnected
  - wireless communication

F. Ma. 10

# Vart är vi på väg?



# Aktuella forskningsområden

- Hitta en korrelation mellan logg-data och de attacker som kan härledas ur denna.
- Kombinera signaturbaserade systems fördelar med få falsklarm med anomalibaserade systems förmåga att upptäcka nya attacker
- Korrelera information från många olika källor för att hitta distribuerade attacker
- Hantera användarnas krav på personlig integritet (privacy)
- Skydda företagets/användarens säkerhetspolicy (confidentiality)

# Sammanfattning och slutsats

- IDS är en teknik som kompletterar övriga säkerhetslösningar - Den andra försvarslinjen.
- Många ställningstaganden att fundera över när man inför ett IDS. Inte lika enkelt som att köpa ett virusskydd.
- Dagens IDS arkitekturer kommer att få svårt att fungera i framtiden IT-infrastrukturer. Nya lösningar måste till.
- Fortfarande flera olösta problem som är föremål för F&U
  - Ej en helt mogen teknik

# Kontaktinfo

Håkan Kvarnström
R&D Security
TeliaSonera AB
hakan.kvarnstrom@teliasonera.com
http://www.ce.chalmers.se/staff/hkv