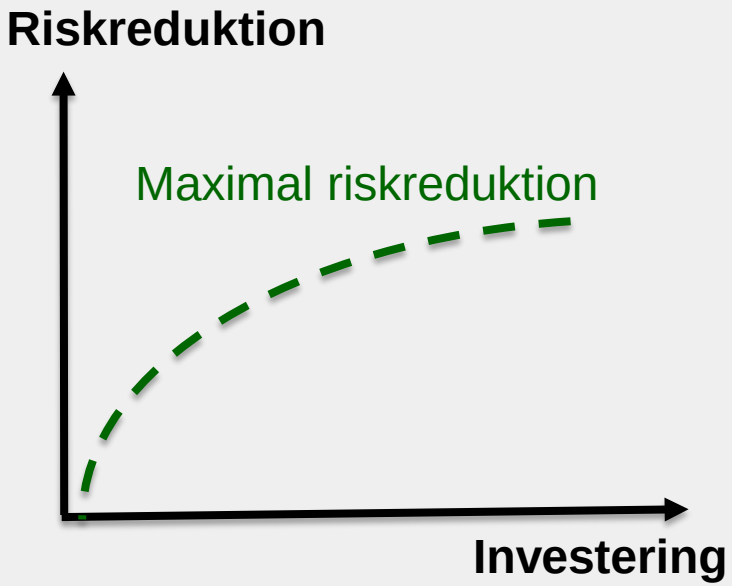
Cybersäkerhet – några utmaningar

Teodor Sommestad, Doktor, Förste forskare
Informationssäkerhet & IT-arkitektur
Linköping

FOI

Cybersäkerhet: En omogen disciplin

- **Empirisk data är ovanligt**, observationer i ”det vilda” är av tveksamt värde och experiment med god validitet är ovanliga i litteraturen.
- **Många viktiga storheter är okända**, t.ex. hur väl olika detektionsmetoder fungerar.
- **Design av nya lösningar** för aktuella problem dominerar disciplinen. Ordet teori används sällan.



Olika typer av utmaningar

System av system

Om man korrelerar enskilda händelser mot processmodeller för angrepp borde man kunna förstå vad som händer i nätet…

Jag har ett SIEM-system som jag kan korrelera loggar i. Titta vad fint!

State-of-the-art

State-of-practice

Med mitt språk för att beskriva sårbarheters semantik genom dataflöden kan jag generera signaturer som är bättre än signaturer baserade på attackkoder...

Jag har skrivit tre signaturer för sårbarheterna vi hittade i Siemens Step 7. Varsågod!

Komponenter

Exemplet intrångsdetektion: Forskning vs Praxis

Akademisk forskning	Praxis
Fokuserar nästan enbart på så kallad anomalidetektion som ska märka avvikelser från det normala/goda.	Använder signaturbaserade lösningar som letar efter kända tecken på missbruk eller angrepp.
Fokuserar nästan uteslutande på den matematik och modeller som byggs in i detektionslösningen.	Systemadministratören har en viktig roll. Hen både konfigurerar lösningar och analyserar de larm som kommer för att identifiera hot.
Slutsatser dras från tester på DARPA:s dataset från 1999 som är från en simulerad miljö. Det är känt sedan 2002 att datasetet inte är representativt.	Övervakar system av olika typer i olika typer av miljöer och mot olika typer av hot. Och ganska sällan angrepp på Windows 95-maskiner…

FOI

Komponentnivå: ofta rättfram & enkelt

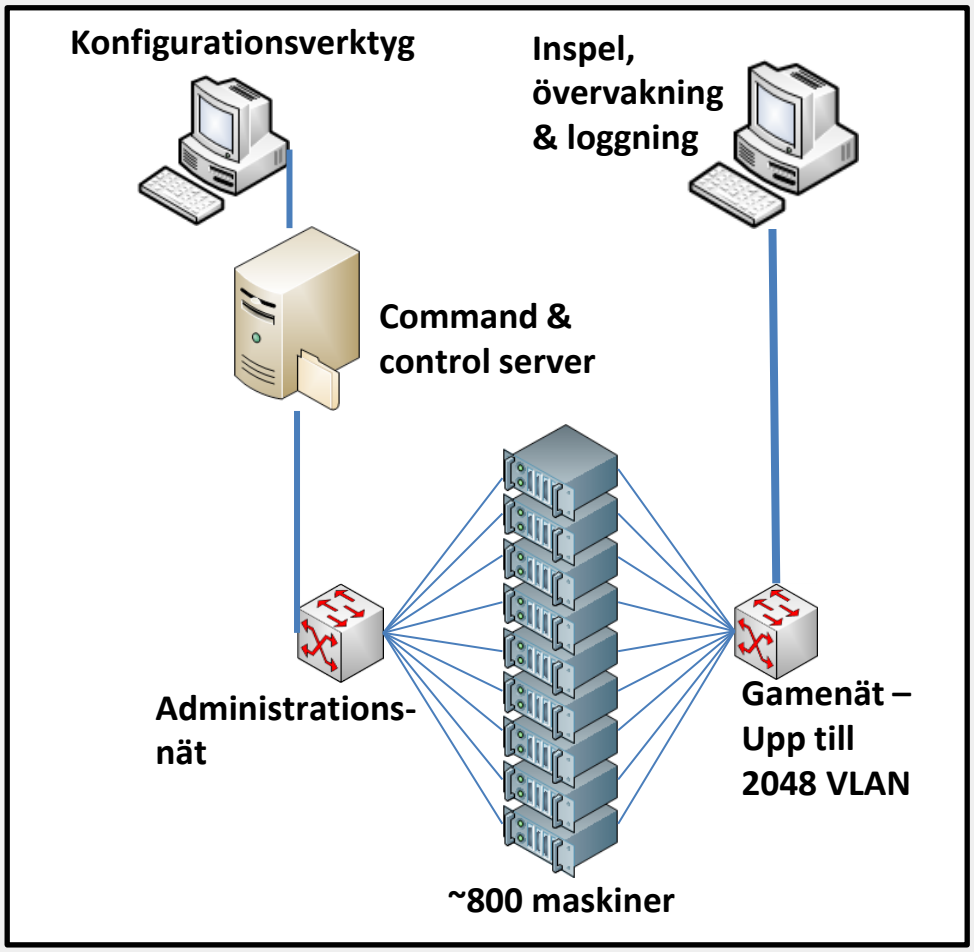
- **Tekniker för att skriva/generera signaturer för intrångsdetektion.**

  Hur många falsklarm och korrekta larm skapas för syntetisk testdata? Blir signaturerna bättre med metod A än metod B?

- **Göra sårbarhetsbedömningar och tekniker för kodverifiering.**

  Hur skulle man bedömt den öppen källkod som producerades för nåt år sedan och som vi nu har ett svar för?

System-av-system-nivå: cyber ranges



Forskning och tester, ofta i samband med övningar:

- Skapa realistiska situationer, men med loggning av alla händelser.
- Testa metoder för att bedöma nätverkssäkerhet. T.ex. analys av angrepp i flera steg.

Test 1: Nyttan med en operatör

- Från en övning 2011 samlades data om:
  - Angriparnas aktiviteter
  - Alarm från IDS-systemet
  - Alarm från IDS-systemets operatör
- Skript skapade bakgrundstrafik enligt samma användningsmönster som riktiga datoranvändare (på FOI, Universitet, etc.).
- I efterhand kunde alarm markerats som korrekta eller felaktiga.

	IDS	Admin
Alarm skapade	2107	70
Recall **P(Alarm=Ja | Attack=Nej)**	69%	58%
Precision **P(Attack=Ja | Alarm=Ja)**	11%	57%

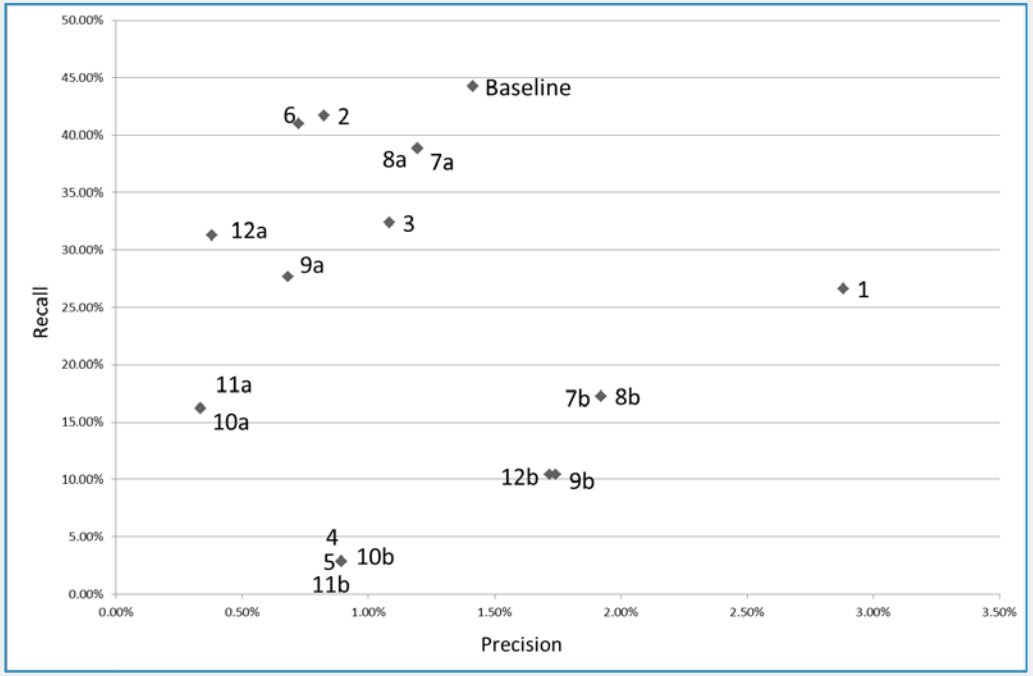
- Administratörens alarm är 5 grr mer precisa.
- Administratören använde kunskap om:
  - Datornätverket
  - Generell kunskap om säkerhet och IDS:er
  - Kunskap om hotbilden

Sommestad & Hunstad, "Intrusion Detection and the Role of the System Administrator", *Information & Computer Security* 21 (1): 30 – 40, 2012.

FOI

Test 2: Korrelera larm med systeminformation

- Liknande test som innan, men med data från 2012 med mer komplex miljö.
- Administratörens resonemang om falsklarm automatiseras genom att korrelera larm mot:
  - Systemets arkitektur och tjänster
  - Kända sårbarheter i systemet



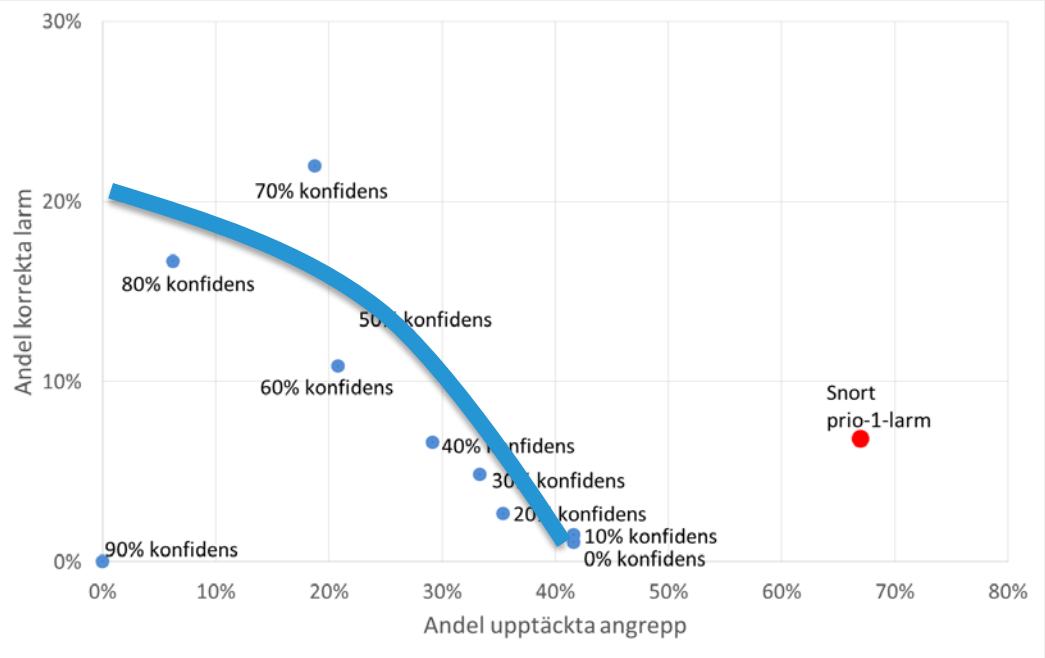
- Gick åt skogen!
- Inget av de 18 filtren eller någon kombination av dem presterar bra.

Sommestad & Franke, “A test of intrusion alert filtering based on network information”, *Security and Communication Networks*, *8*(3), 2291–2301, 2015.

FOI

Test 3: Korrelera larm med en attackmodell

- SnIPS är en av få existerande lösningar för att resonera som en operatör.
- Gissar om en maskin blivit komprometterad baserat på:
  1. Skanningar mot den
  2. Angrepp mot den
  3. Skanningar från den
  4. Angrepp från den
- Ger en skattning av hur säker man kan vara på att maskinen blivit komprometterad.



- Ger ett en intuitiv lösning för att höja relevansen i alarmen, men till kostnad av andelen upptäckta kompromettеringar.
- Konfidensvärdena stämmer inte med vår data

Sommestad, T. & Holm, H., Alert verification through alert correlation – an empirical test of SnIPS, forthcoming

FOI

Utmaningar: Mer rigorös kunskap

- Skaffa tid och resurser att testa om metoder/idéer funkar.
- Skapa incitament för forskare, utvecklare och praktiker att ”bevisa” sina förslags braighet.
- Hantera hemlighetsaspekten, som inte finns inom exempelvis medicin.