Självlärande System för Cyberförsvar

IT-försvarsdagen

Kim Hammar

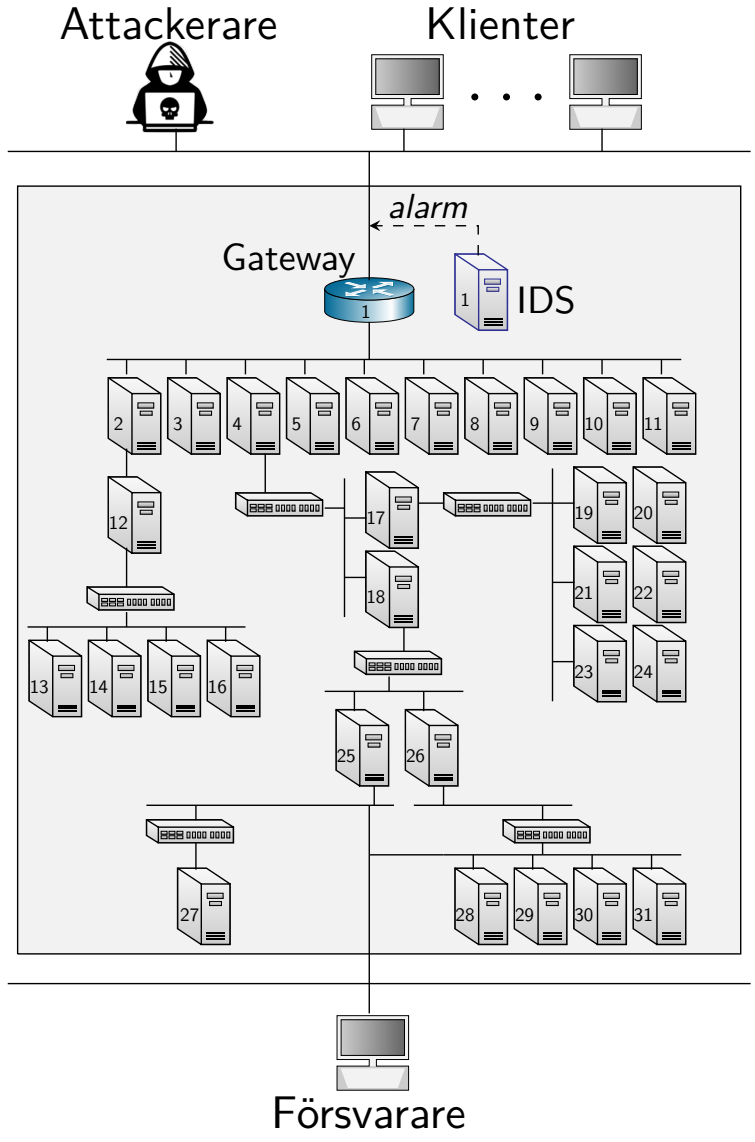
kimham@kth.se

CDIS, Centrum för cyberförsvar och informationssäkerhet
NSE, Avdelningen för nätverk och systemteknik
KTH Kungliga Tekniska Högskolan

6 Dec, 2022

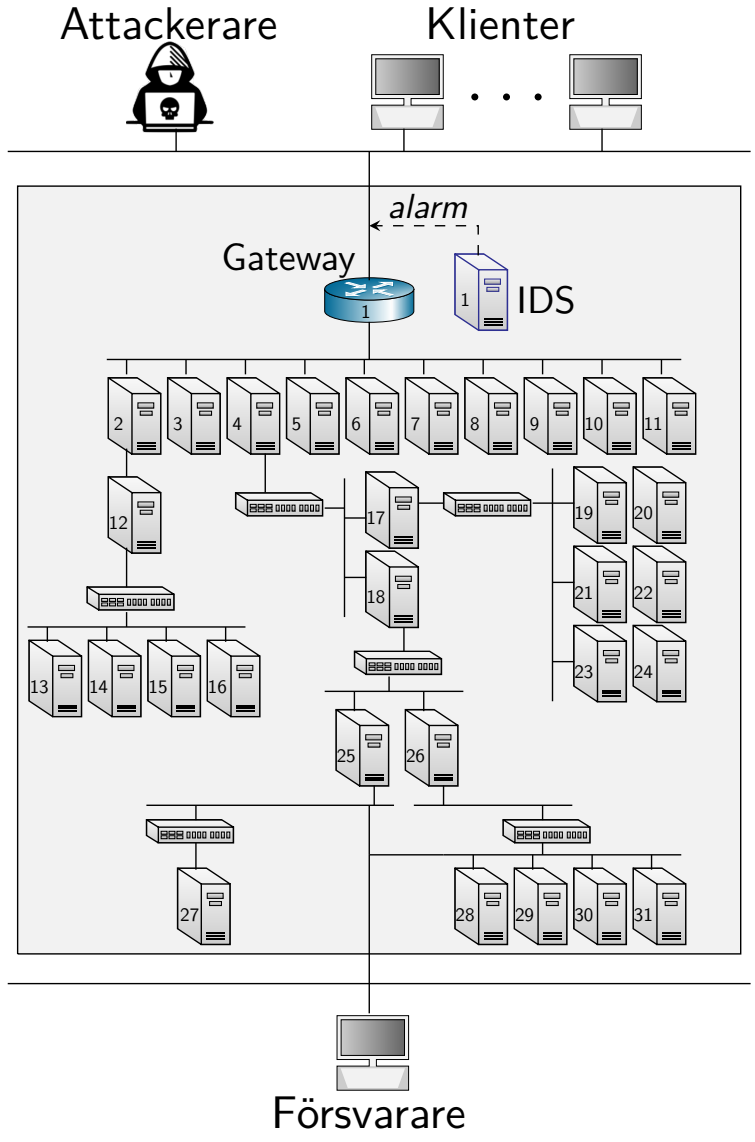
Utmaning: Automatiserade och föränderliga attackmetoder

- **Utmaningar**:
  - Attackmetoder är i en konstant förändring och utveckling
  - Komplicerade IT-infrastrukturer

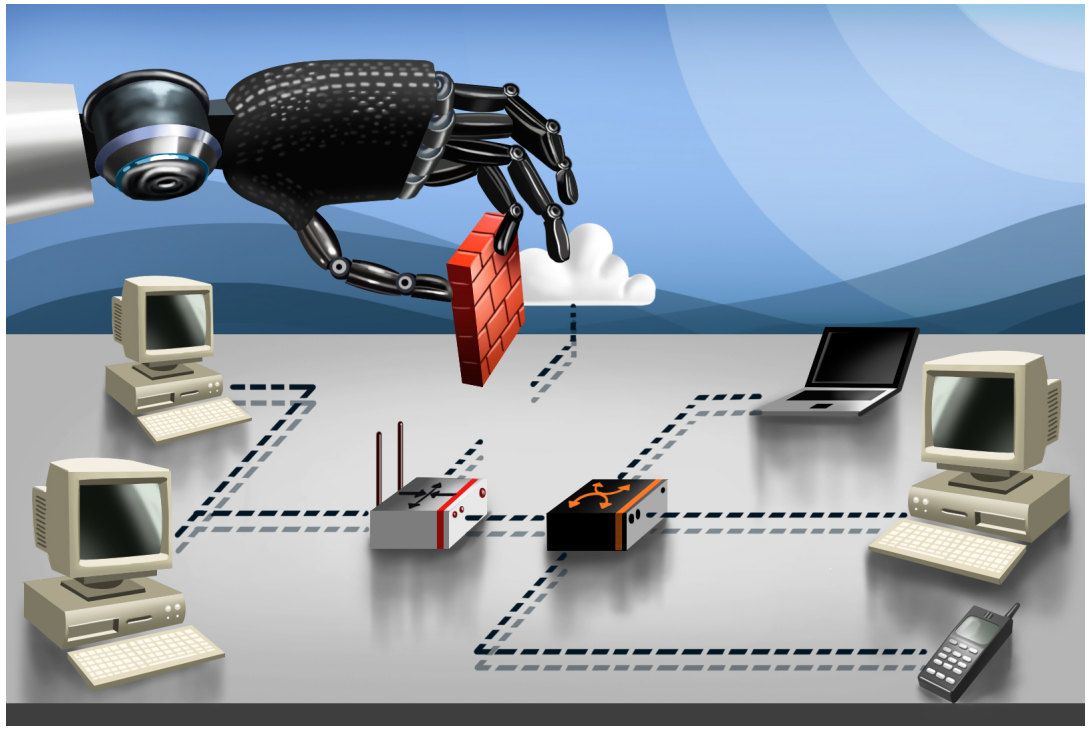


Forskningsmål: Automatiserad säkerhet och inlärning

- **Utmaningar**:
  - Attackmetoder är i en konstant förändring och utveckling
  - Komplicerade IT-infrastrukturer
- **Forskningsmål**:
  - Automatisera säkerhetsfunktioner
  - Anpassa system till föränderliga attackmetoder



Automatiserad Säkerhet: Nuvarande Forskningslandskap



Nivåer av säkerhetsautomatisering

Ingen automatisering.
Manuell detektering.
Manuell prevention.
Inga alarm.
Ingen automatiserad attack mitigering.
Brist på verktyg.

80-talet

Operatörassistans.
Manuell detektering.
Manuell prevention.
Granskningsloggar.
Säkerhetsverktyg.

90-talet

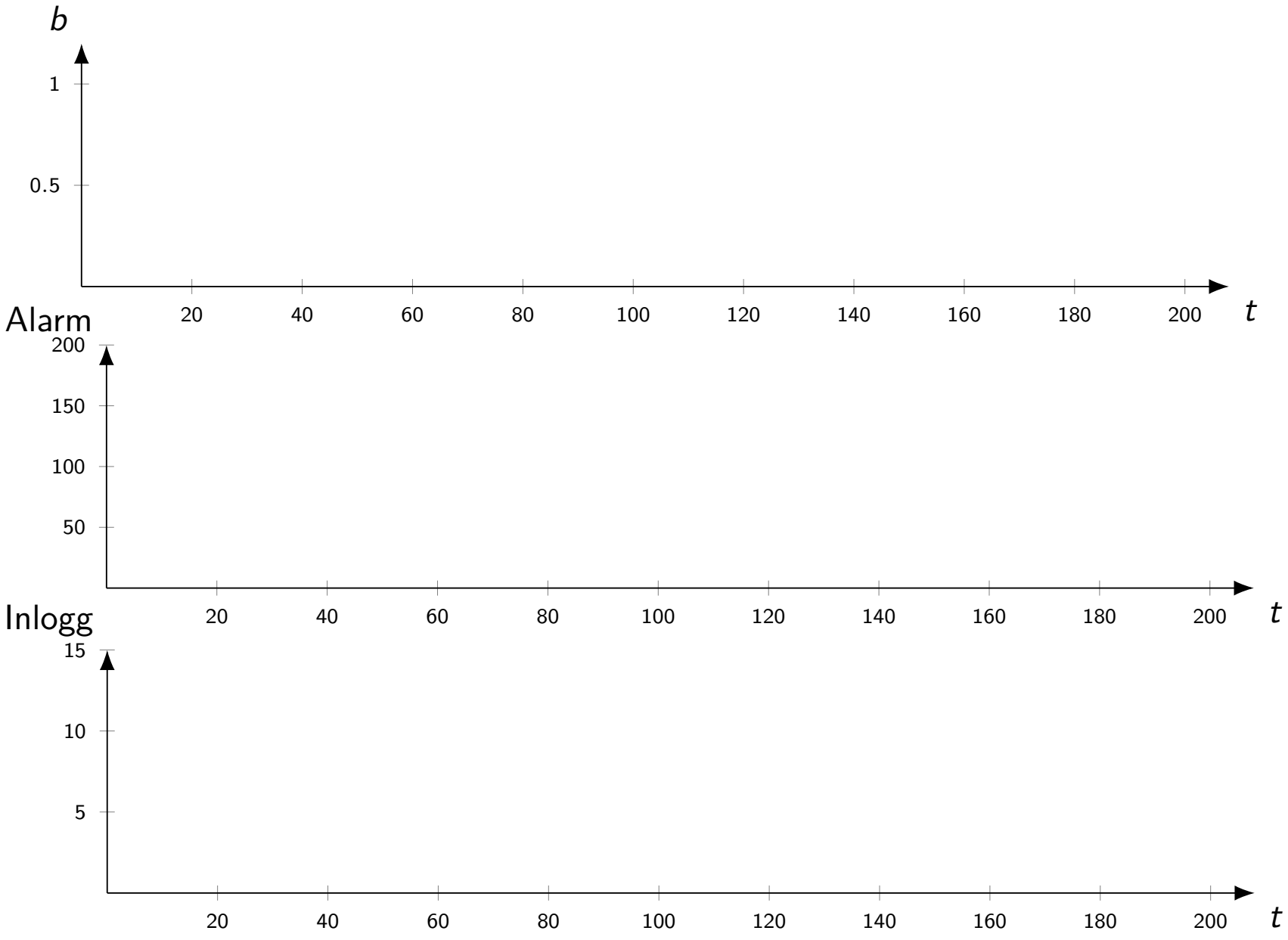
Partiell automatisering.
System har automatiserade funktioner för detektering/ prevention men kräver manuell uppdatering och konfiguration.
Intrångsdetekteringssystem.
Intrångspreventeringssystem.

00-talet-Nu

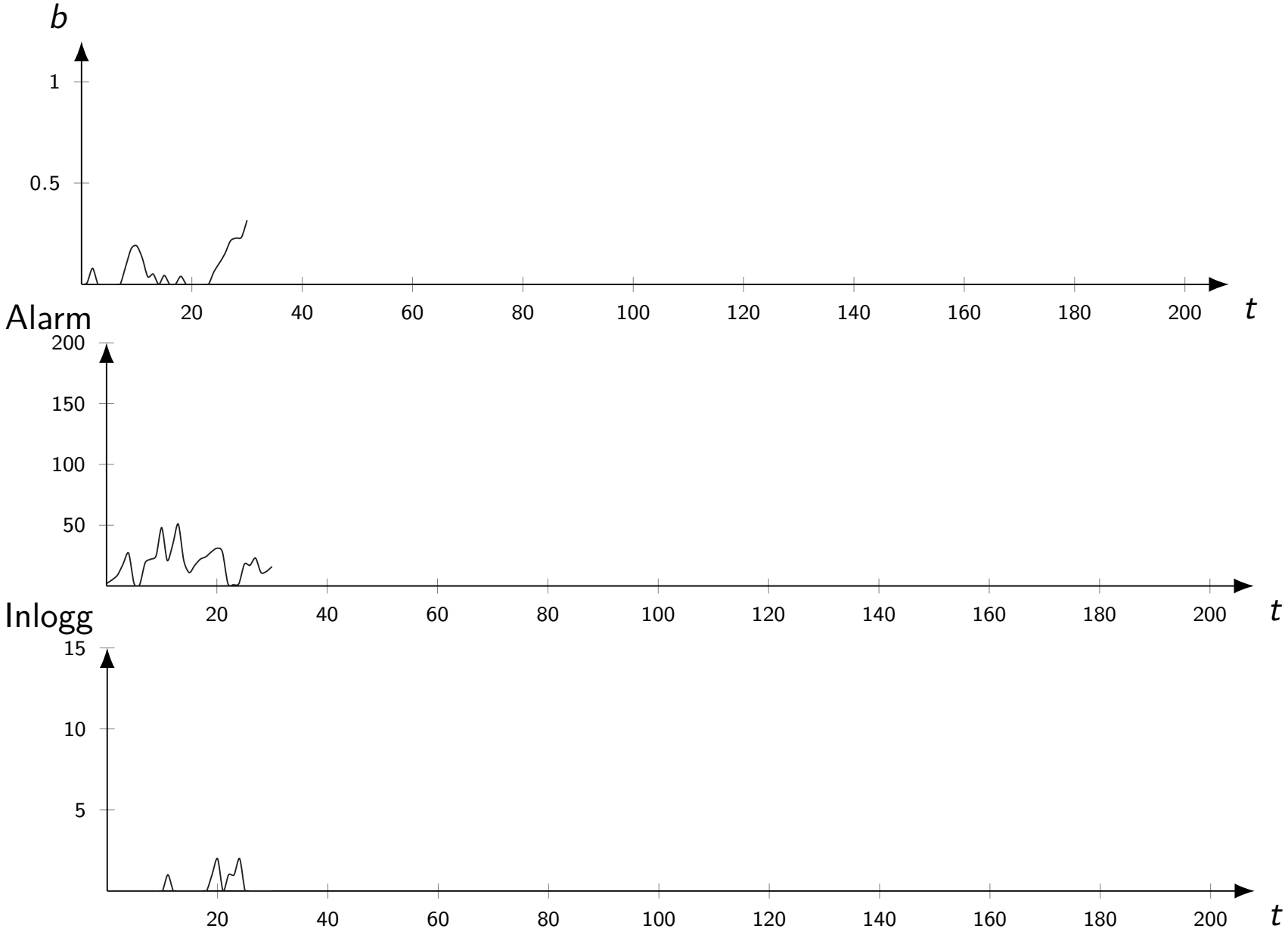
Hög automatisering.
Systemet uppdaterar sig självt automatiskt.
Automatiserad attackdetektering.
Automatiserad attackmitigering.

Forskning

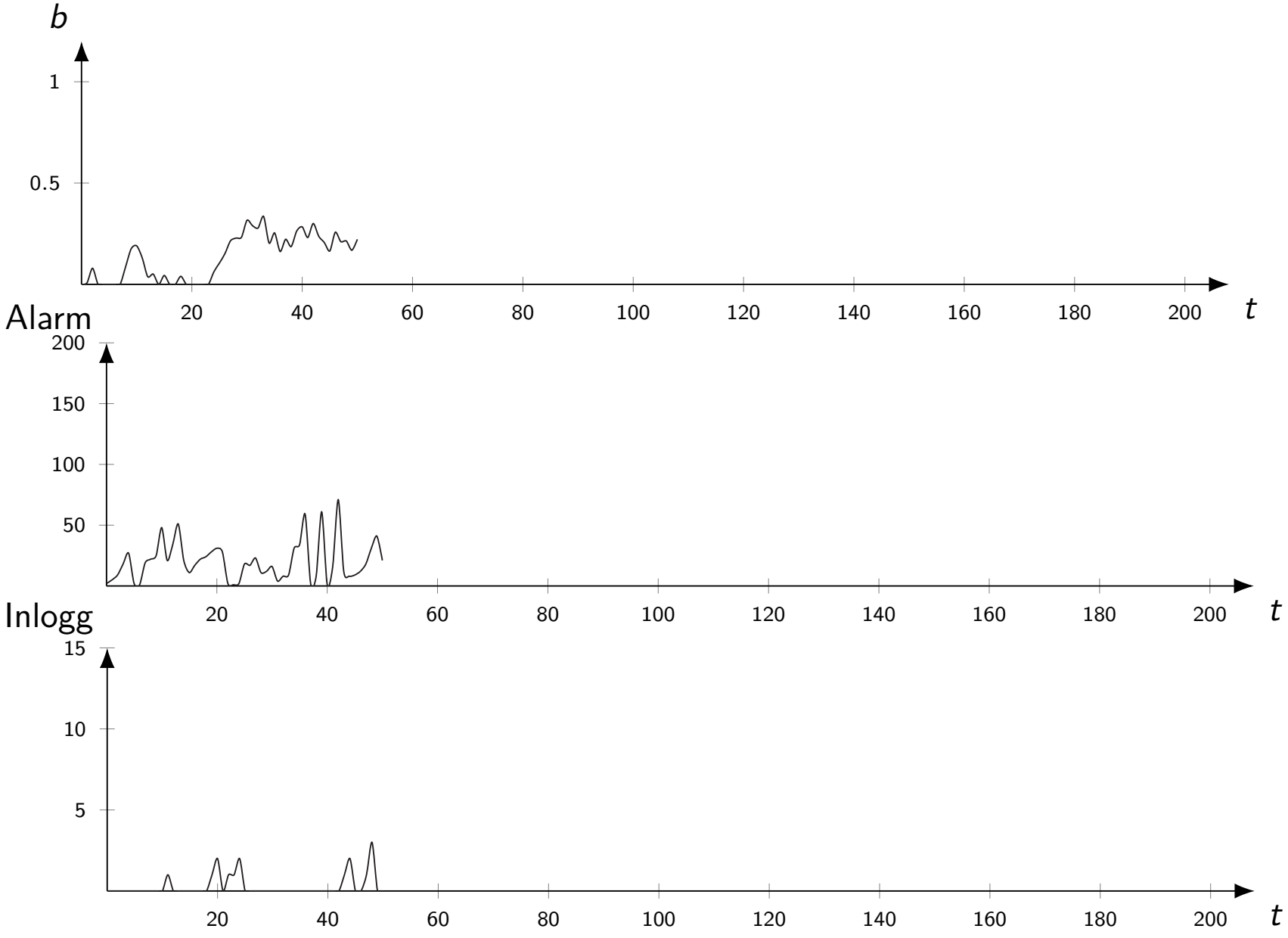
Intrångsmitigeringsproblemet



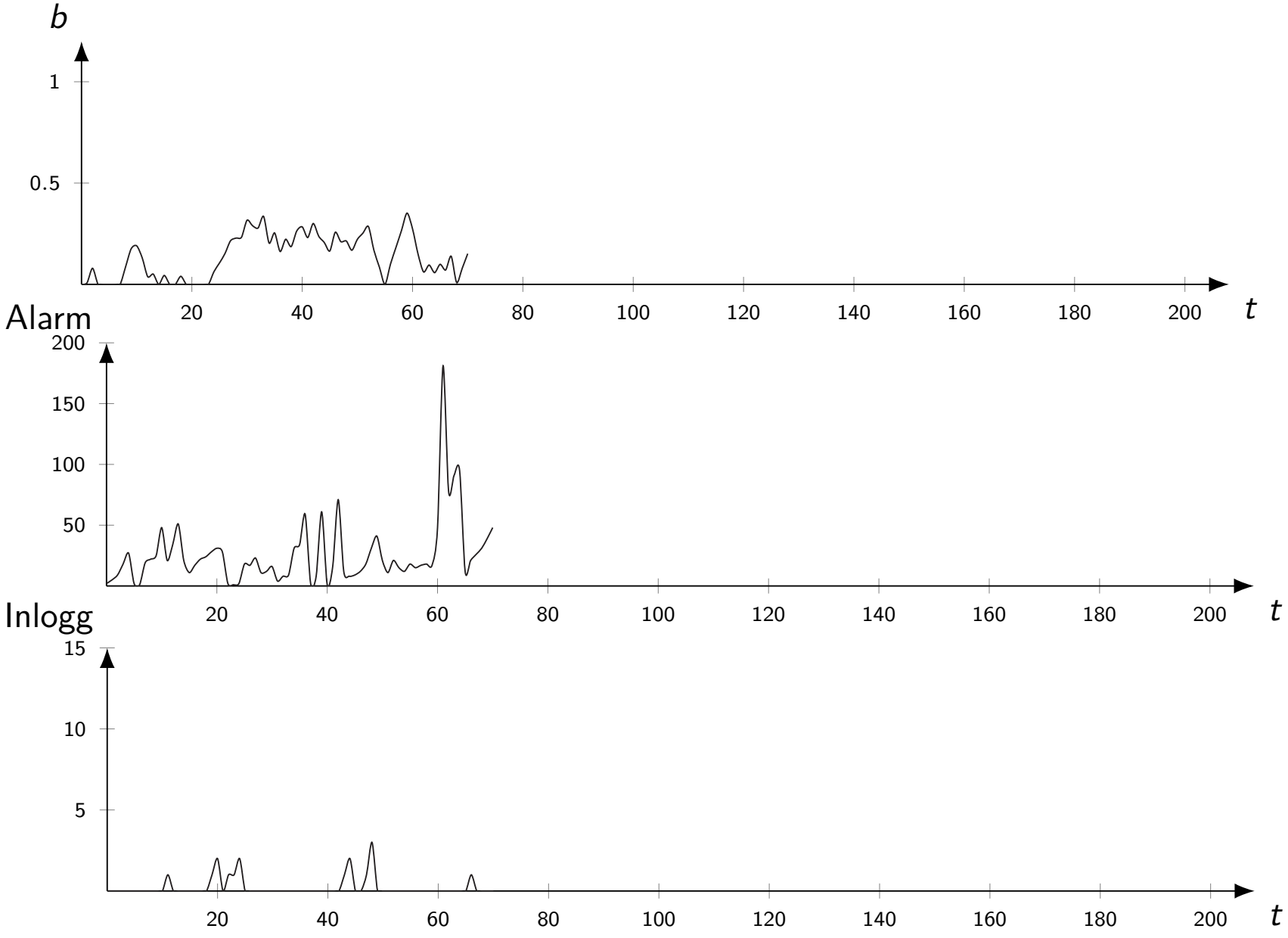
Intrångsmitigeringsproblemet



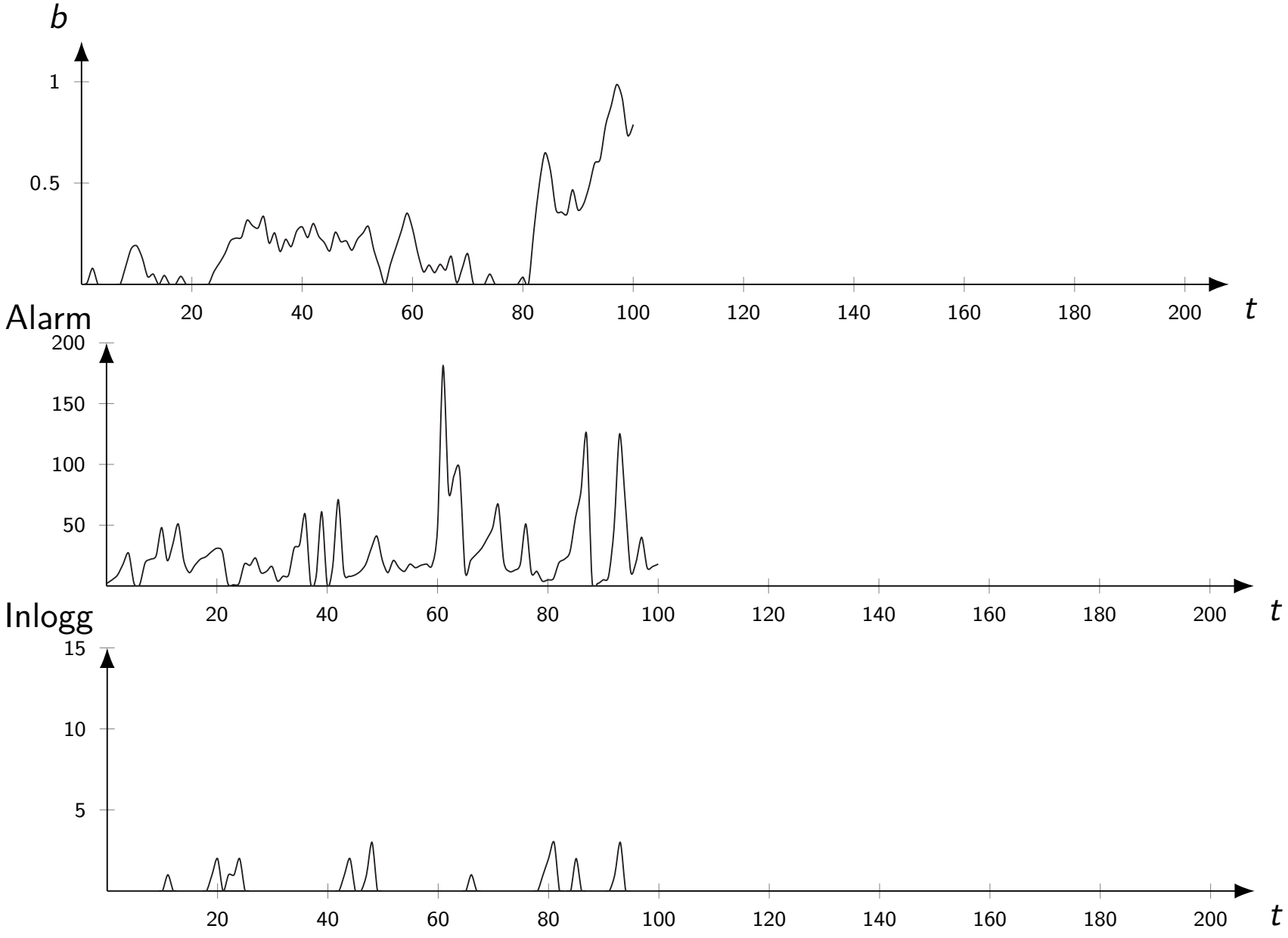
Intrångsmitigeringsproblemet



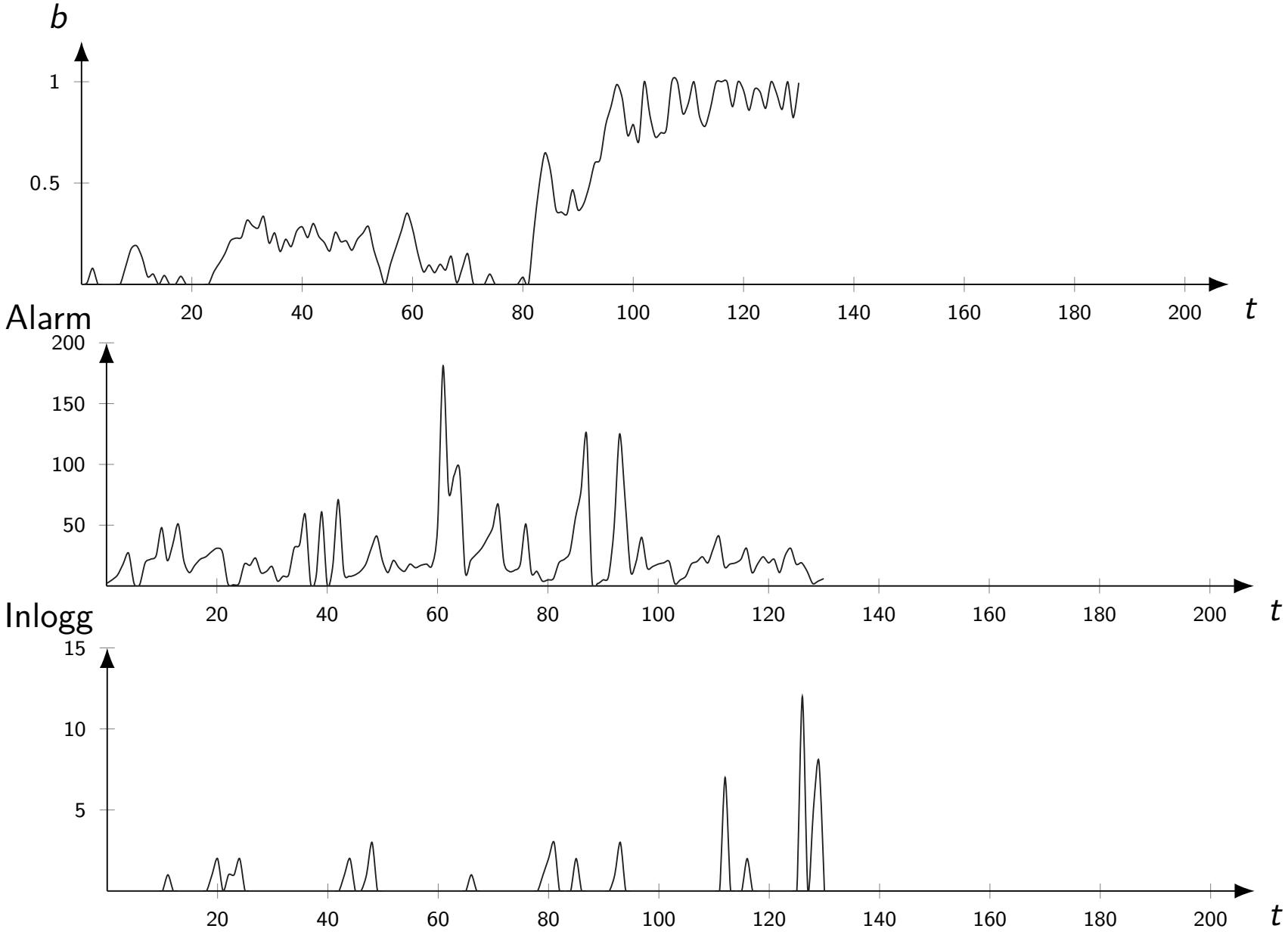
Intrångsmitigeringsproblemet



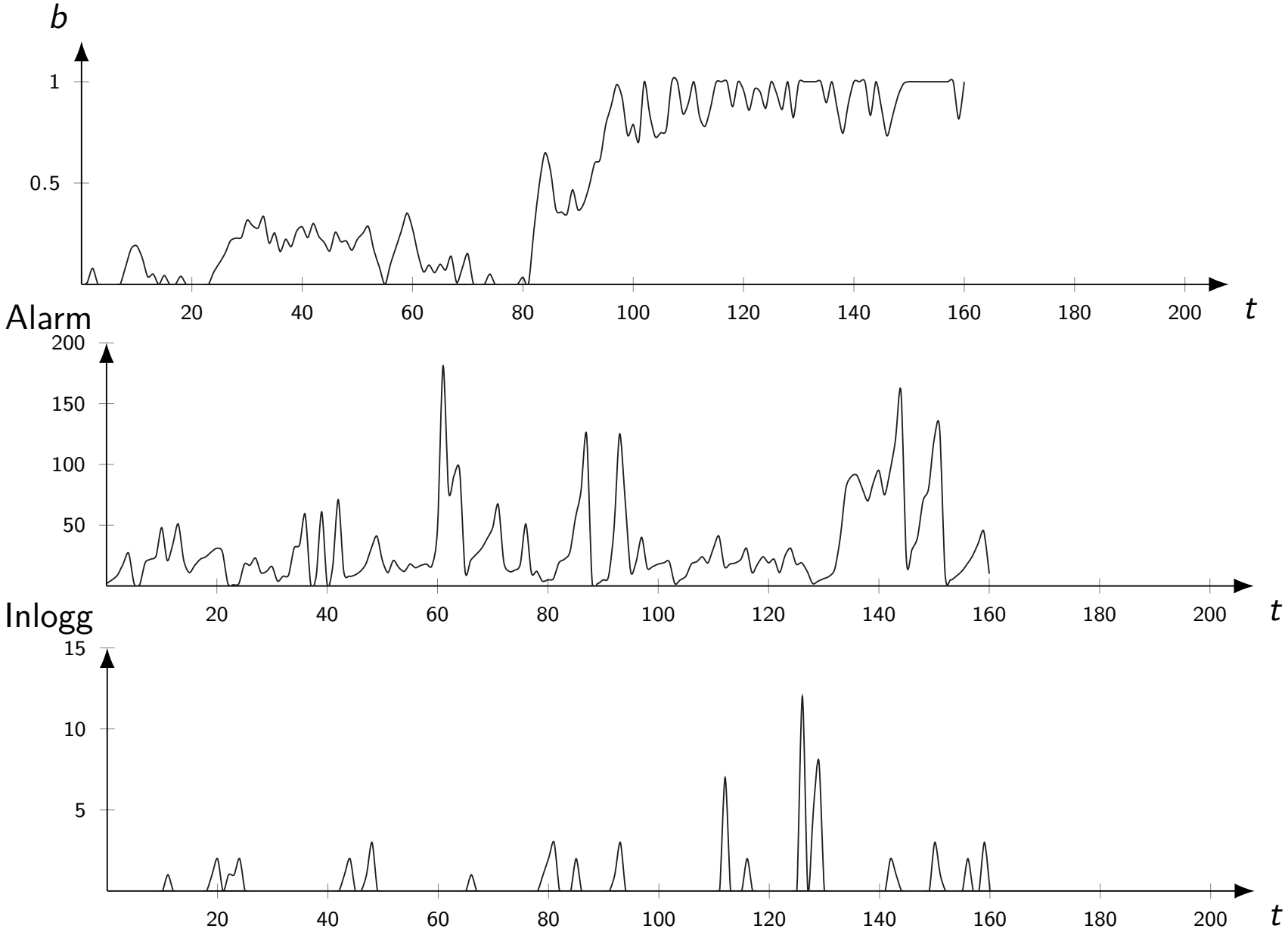
Intrångsmitigeringsproblemet



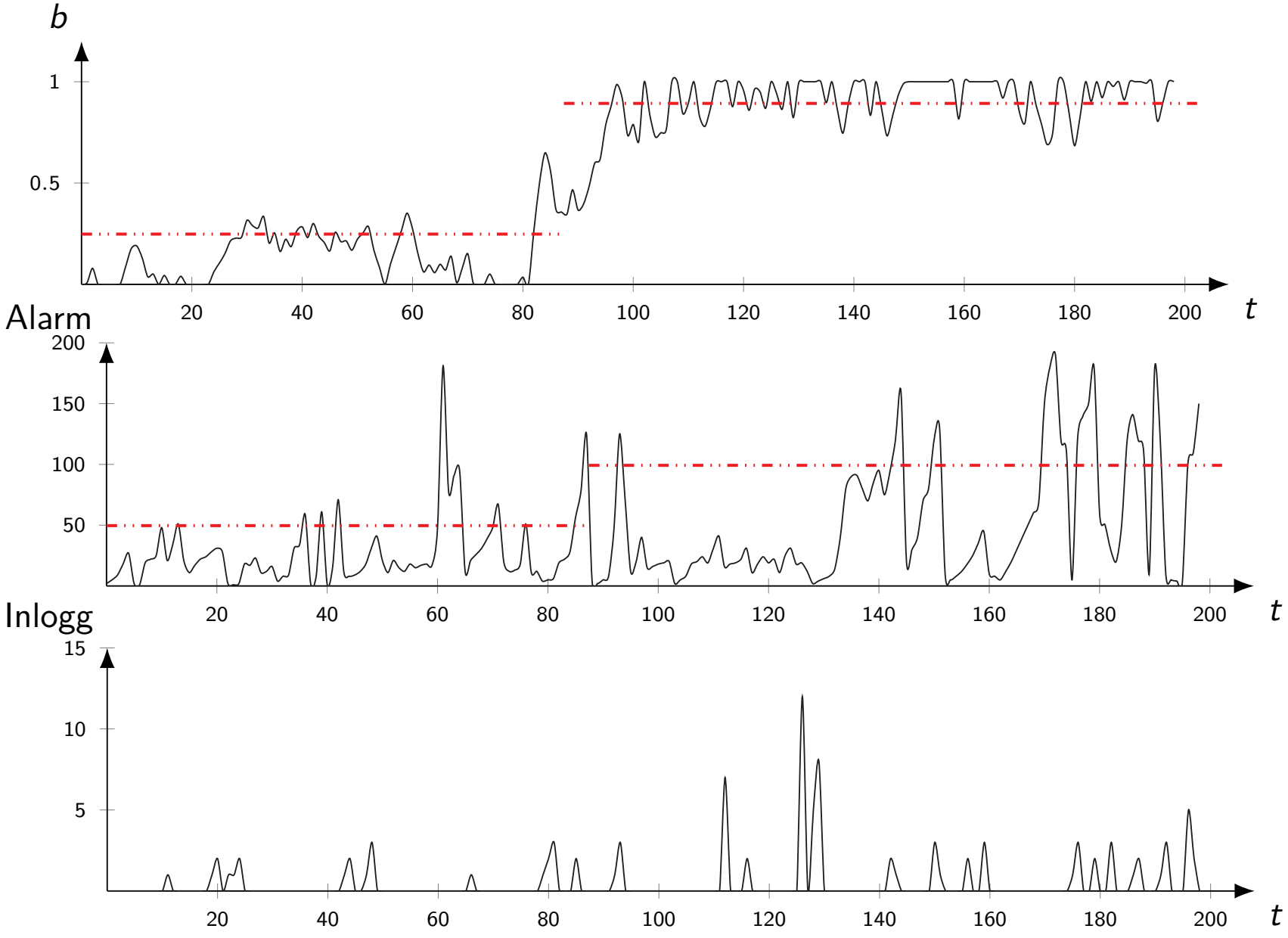
Intrångsmitigeringsproblemet



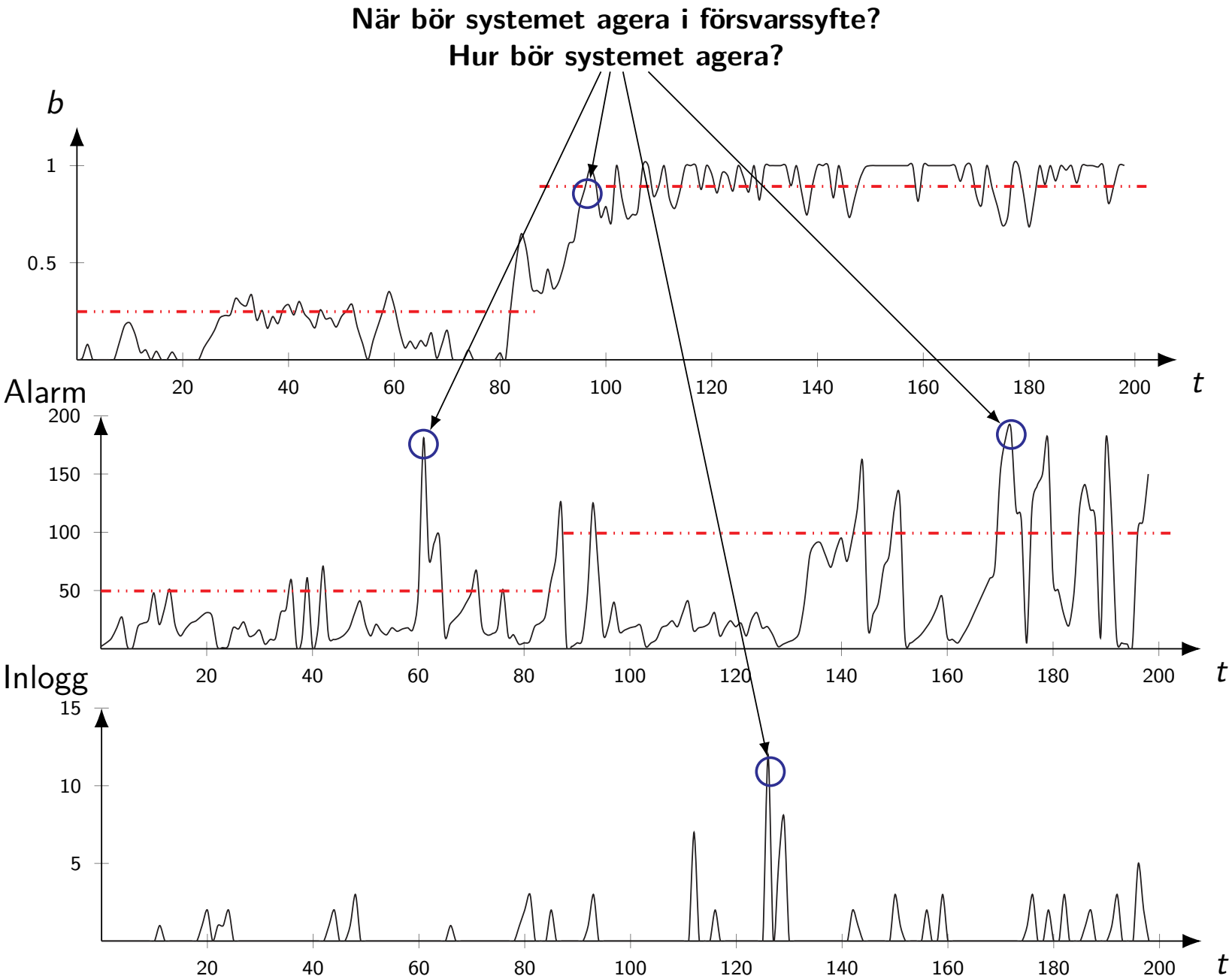
Intrångsmitigeringsproblemet



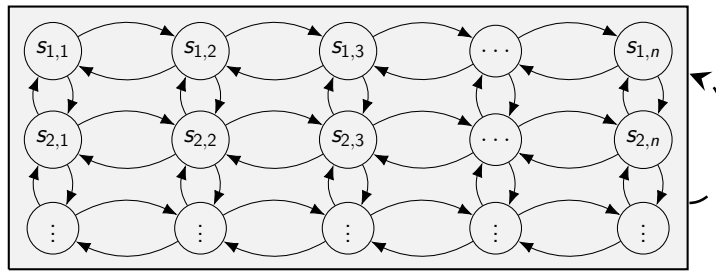
Intrångsmitigeringsproblemet



Intrångsmitigeringsproblemet



Vår metod för att automatiskt beräkna säkerhetsstrategier

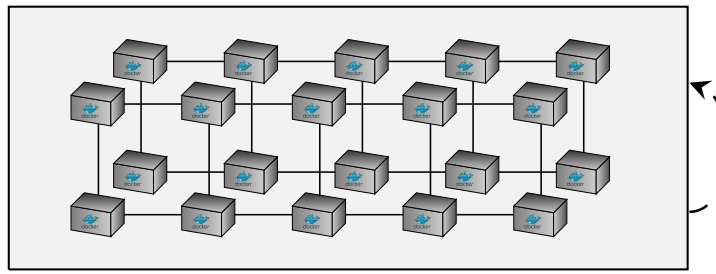


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

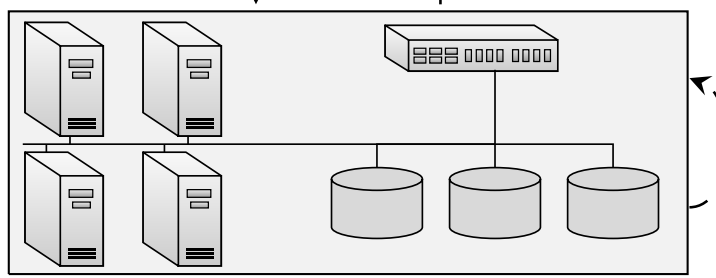


EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

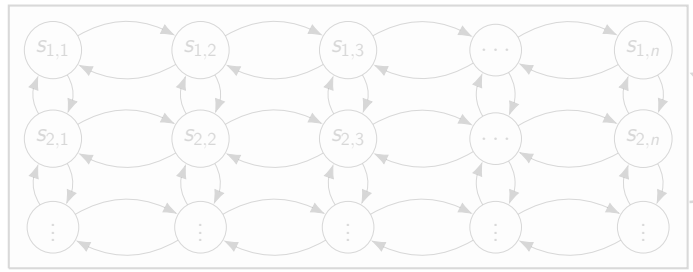
Selektiv replikering



IT INFRASTRUKTUR

Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier

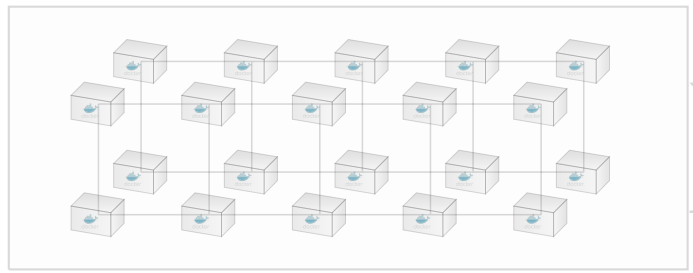


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering



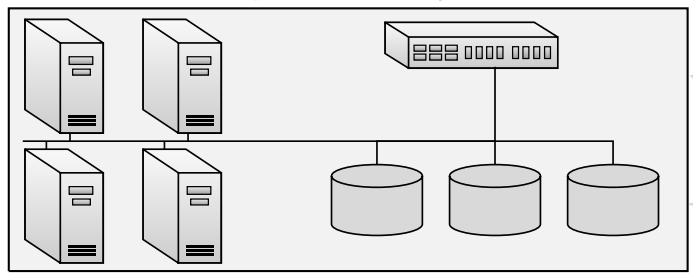
EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

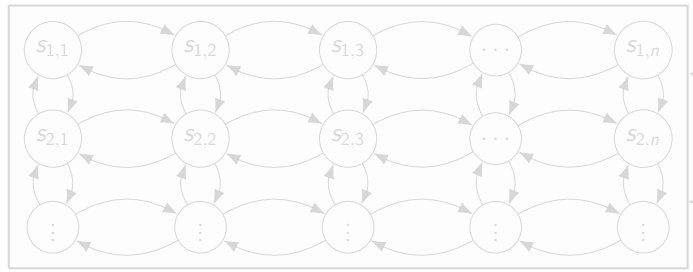
Selektiv replikering

IT INFRASTRUKTUR



Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier

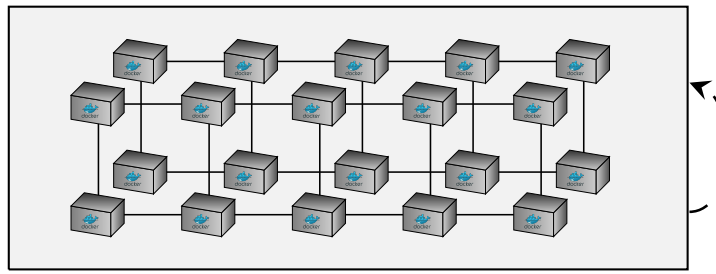


Simuleringssystem

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering



Emuleringssystem

Utvärdering & skattning av modeller

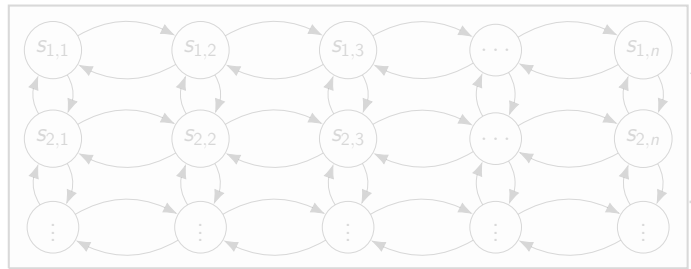
Implementation av säkerhetsstrategi π

Selektiv replikering

IT infrastruktur

Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier

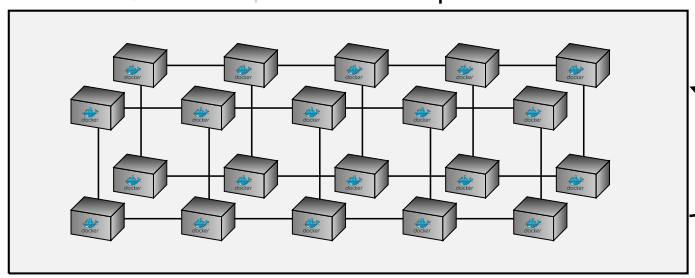


Simuleringssystem

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

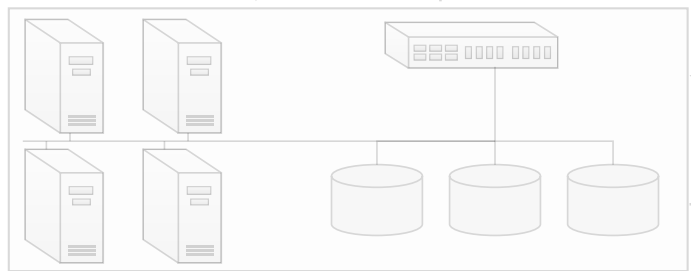


Emuleringssystem

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

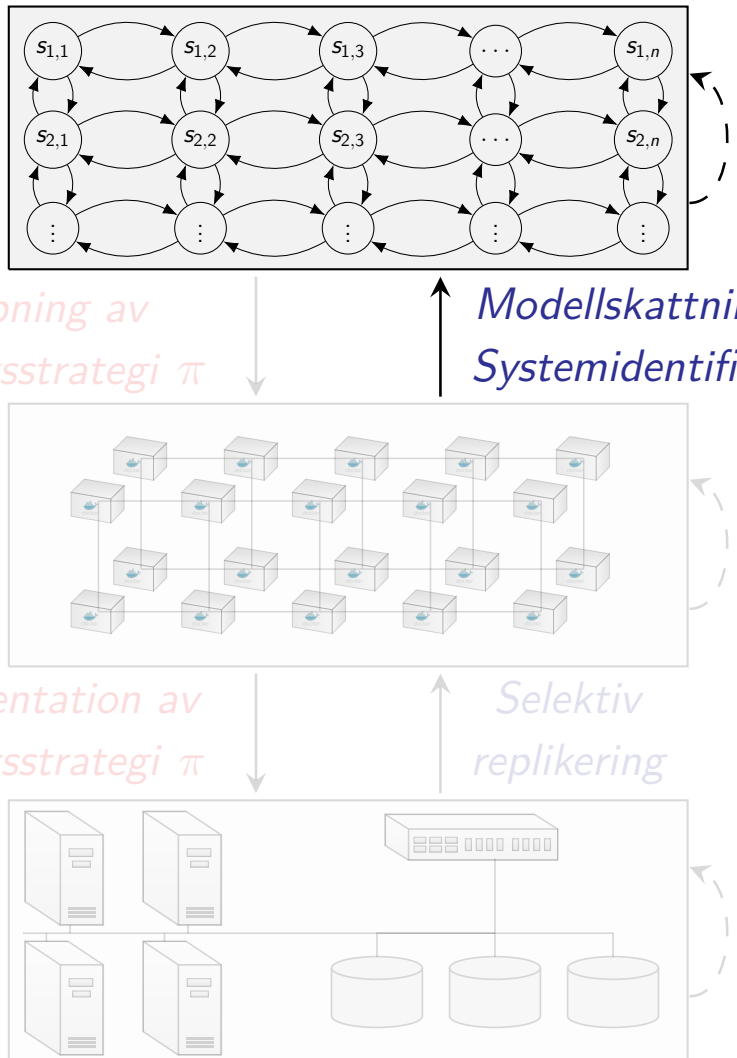
Selektiv replikering



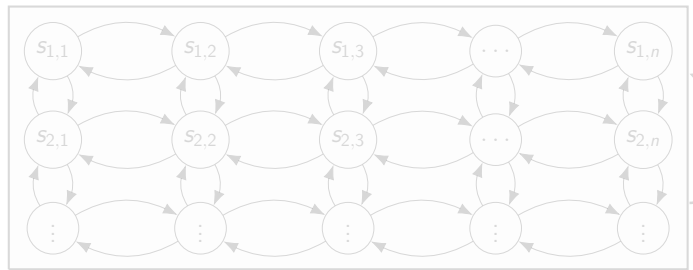
IT infrastruktur

Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier



Vår metod för att automatiskt beräkna säkerhetsstrategier

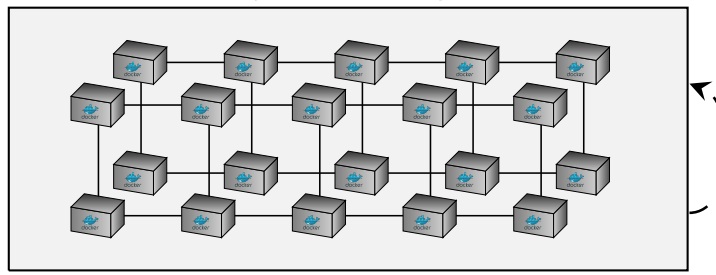


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

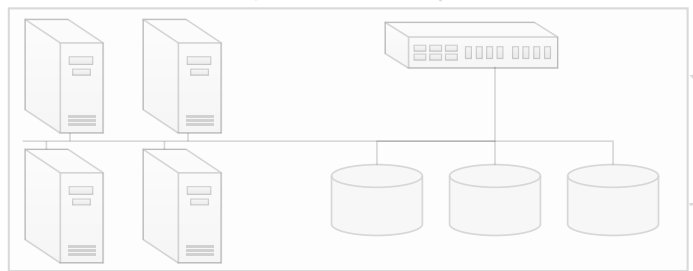


EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

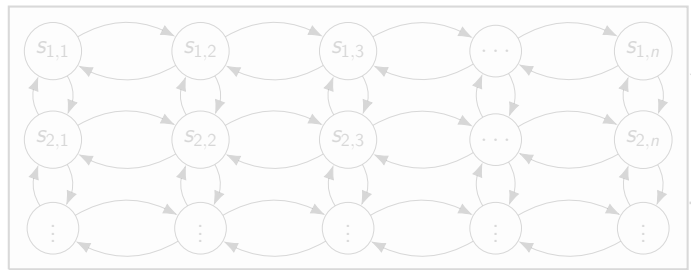
Selektiv replikering



IT INFRASTRUKTUR

Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier

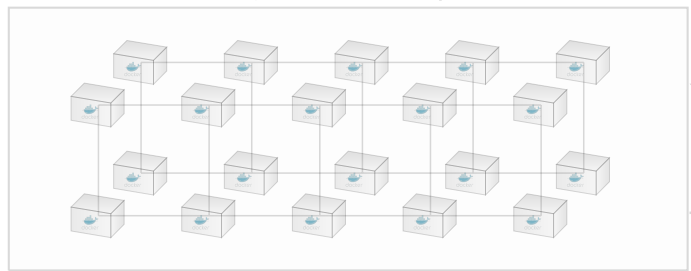


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

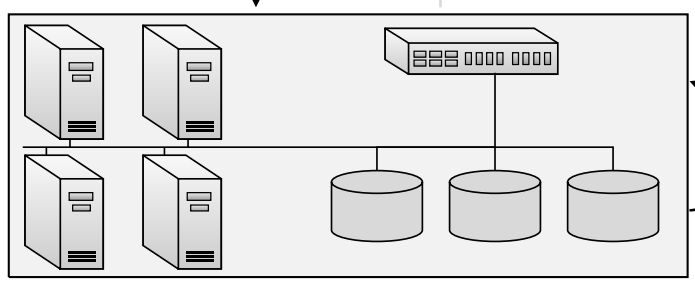


EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

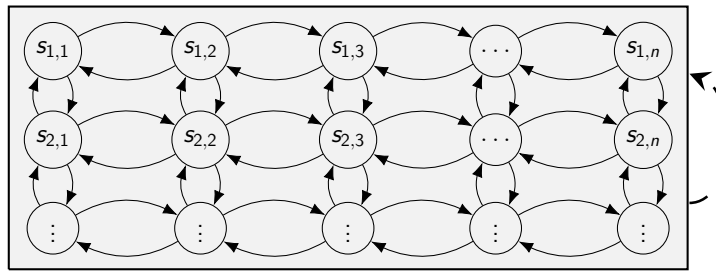
Selektiv replikering



IT INFRASTRUKTUR

Automatiserad säkerhet & självlärande system

Vår metod för att automatiskt beräkna säkerhetsstrategier

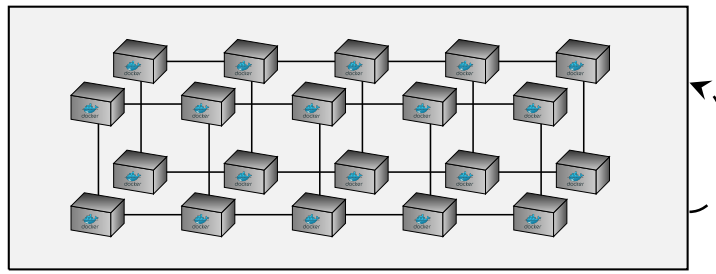


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

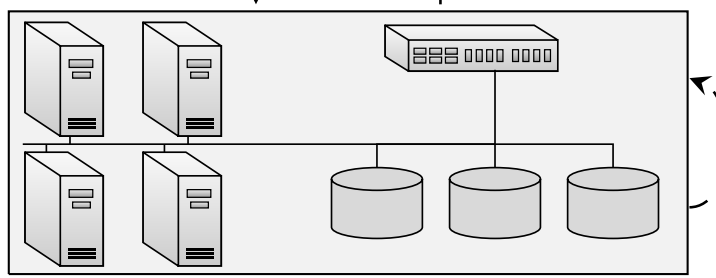


EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

Selektiv replikering

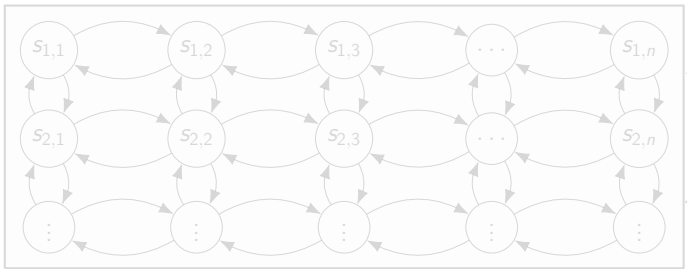


IT INFRASTRUKTUR

Automatiserad säkerhet & självlärande system

Emuleringssystemet

Simuleringssystem

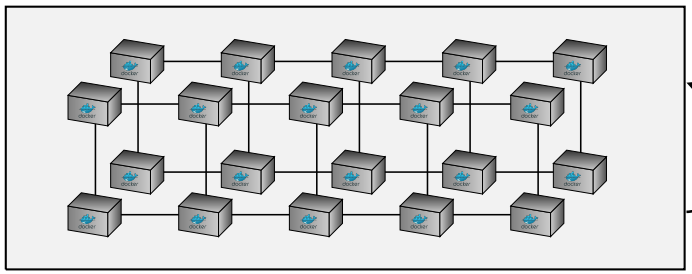


Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

Emuleringssystem

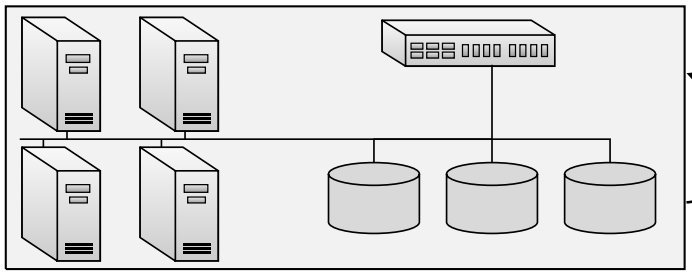


Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

Selektiv replikering

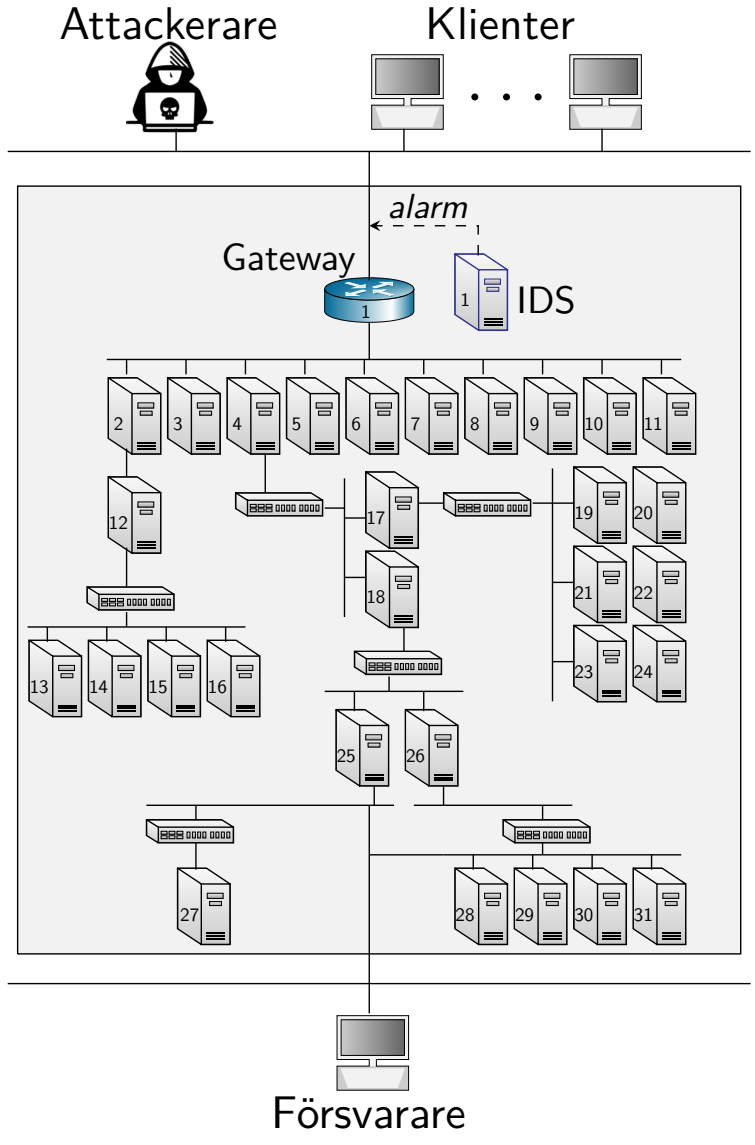
IT infrastruktur



Automatiserad säkerhet & självlärande system

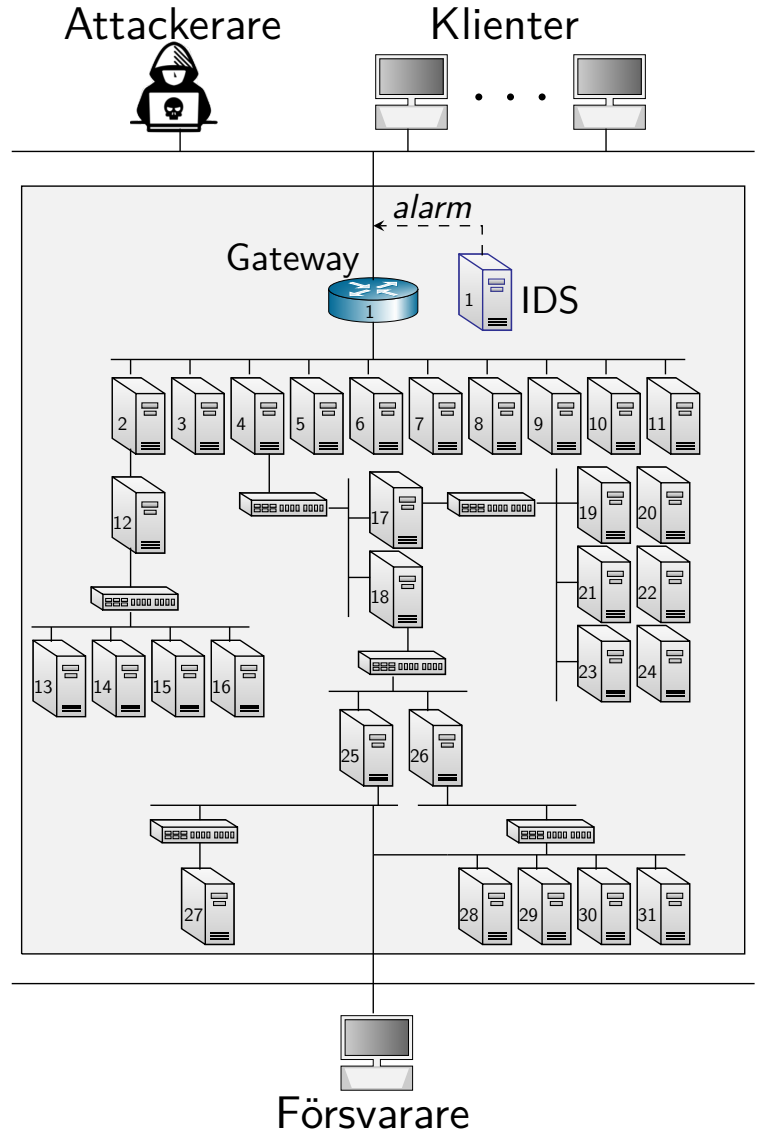
Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.



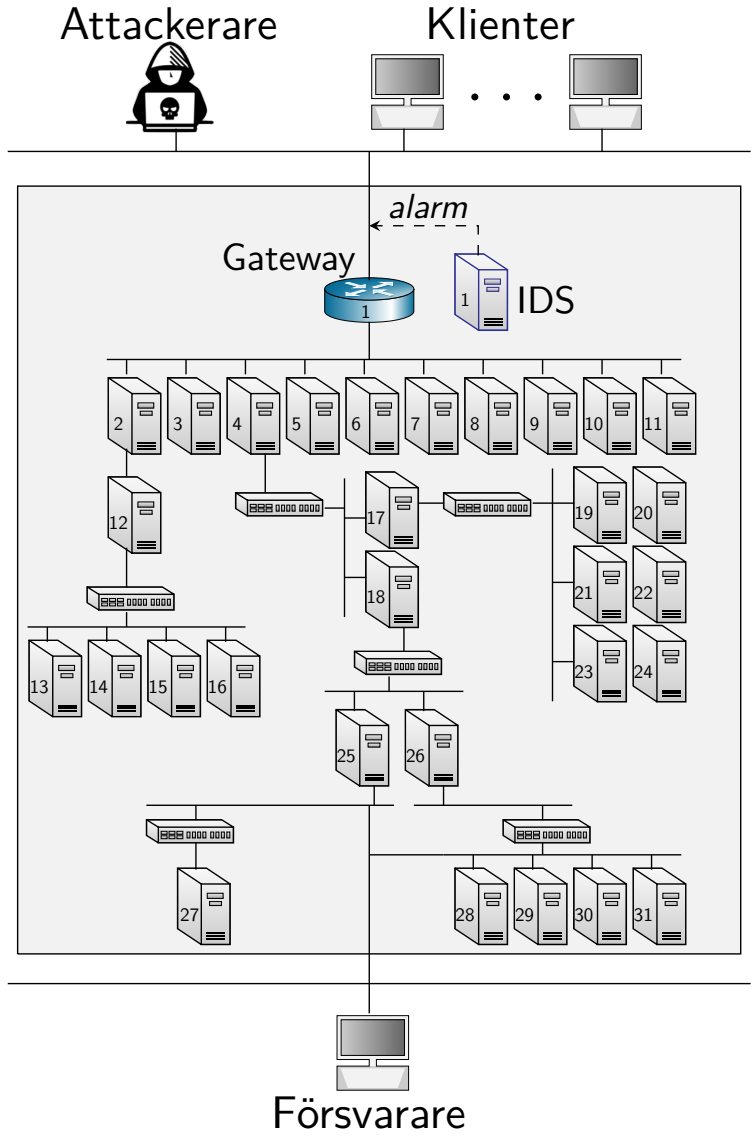
Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.



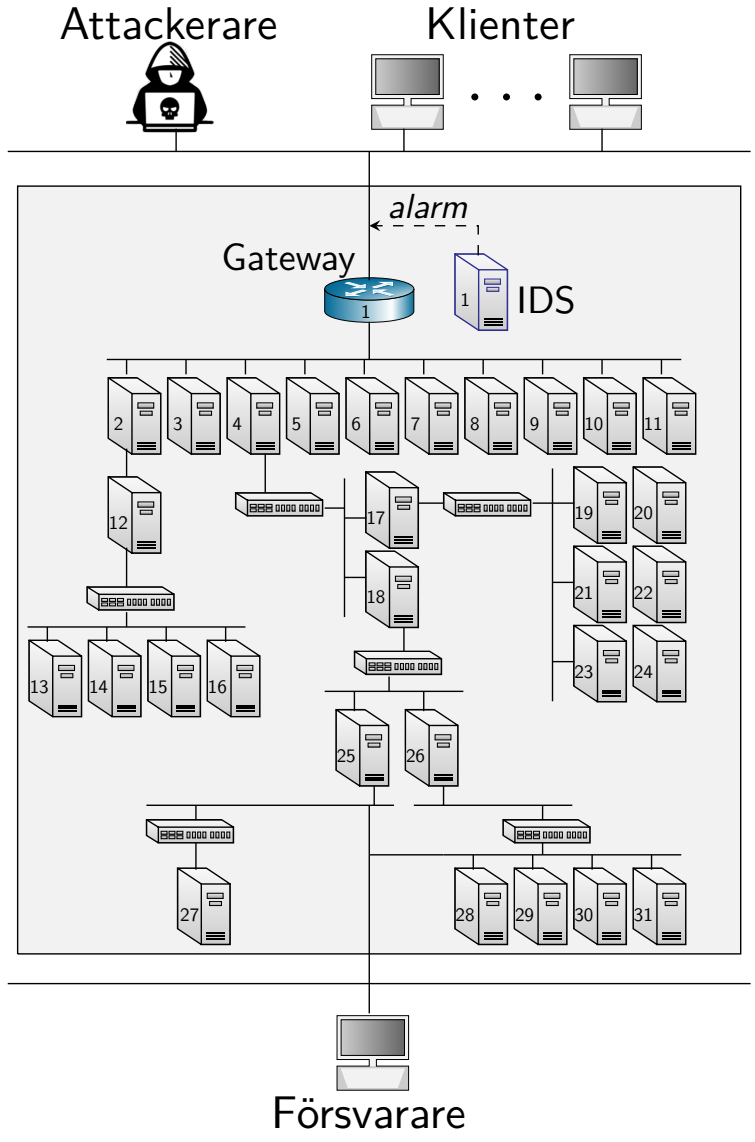
Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.



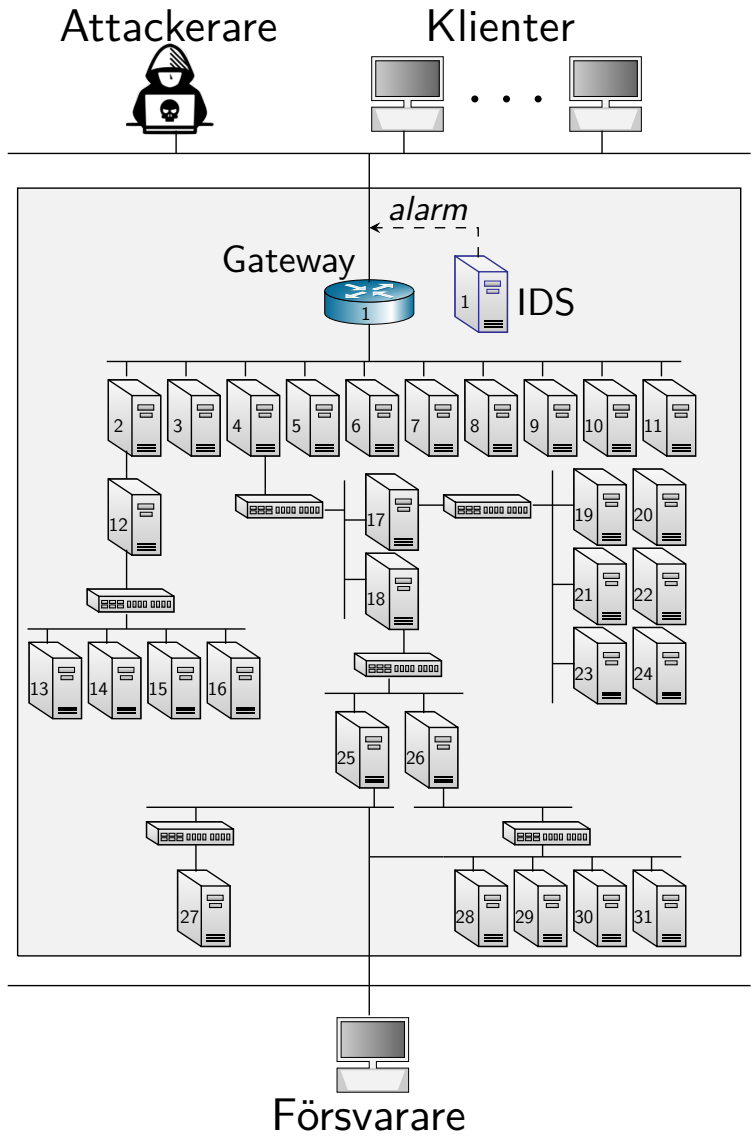
Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.



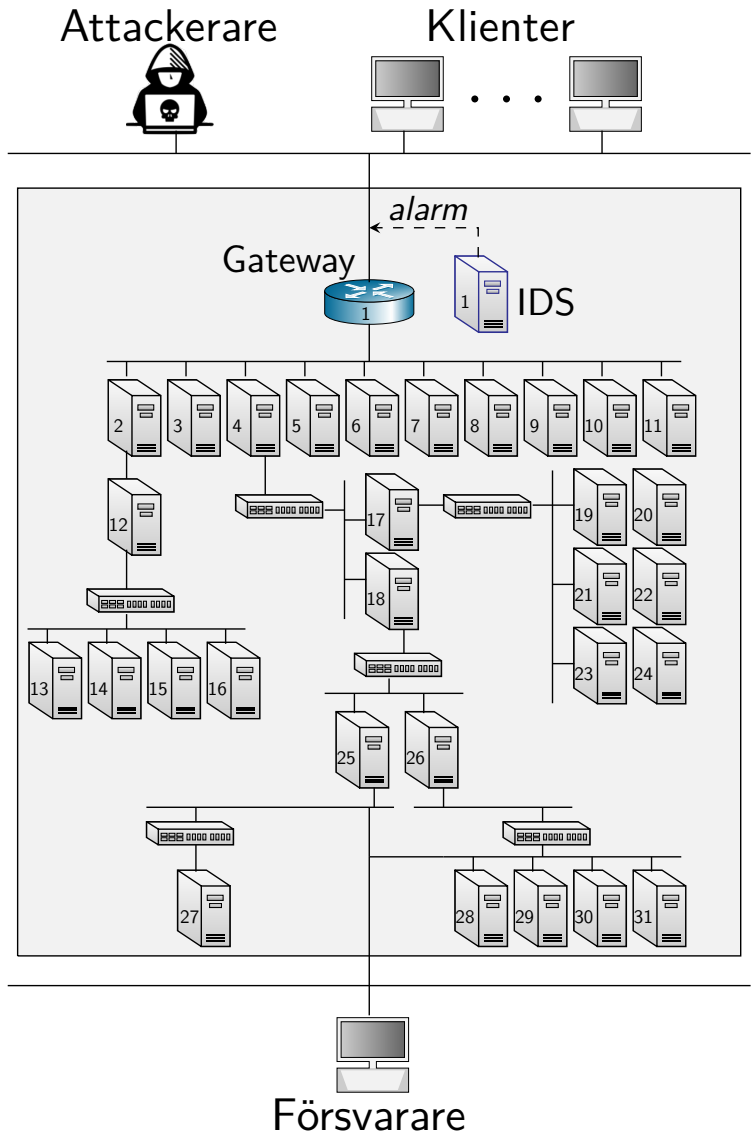
Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.

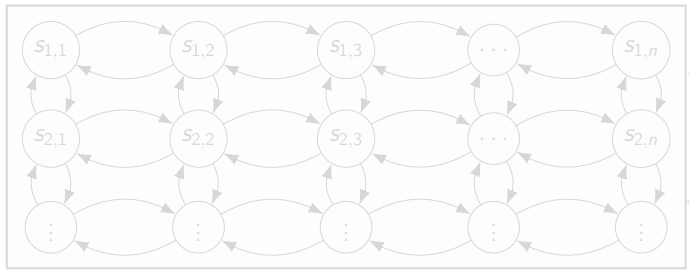


Emuleringssystemet

- Emulerar **nätnoder** med Docker containrar
- Emulerar **IPS och sårbarheter** med mjukvara
- Nätverksisolering och **trafikformning** genom NetEm i Linuxkärnan
- Resursregler definieras med cgroups.
- Emulerar ankommande klienter med en Poisson process.
- **Interna kommunikationslänkar** är full-duplex med kapacitet 1000 Mbit/s
- **Externa kommunikationslänkar** är full-duplex med kapacitet 100 Mbit/s & 0.1% paketförlust i normal operation samt slumpmässiga burstar med 1% paketförlust.



Systemidentifiering

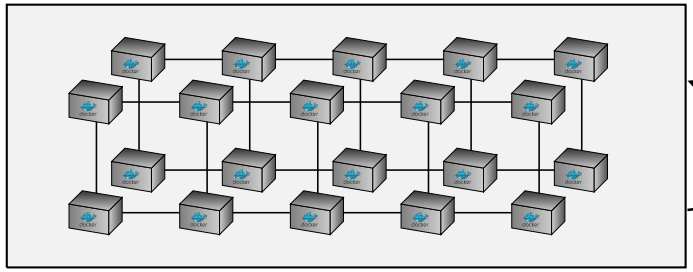


Simuleringssystem

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering



Emuleringssystem

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

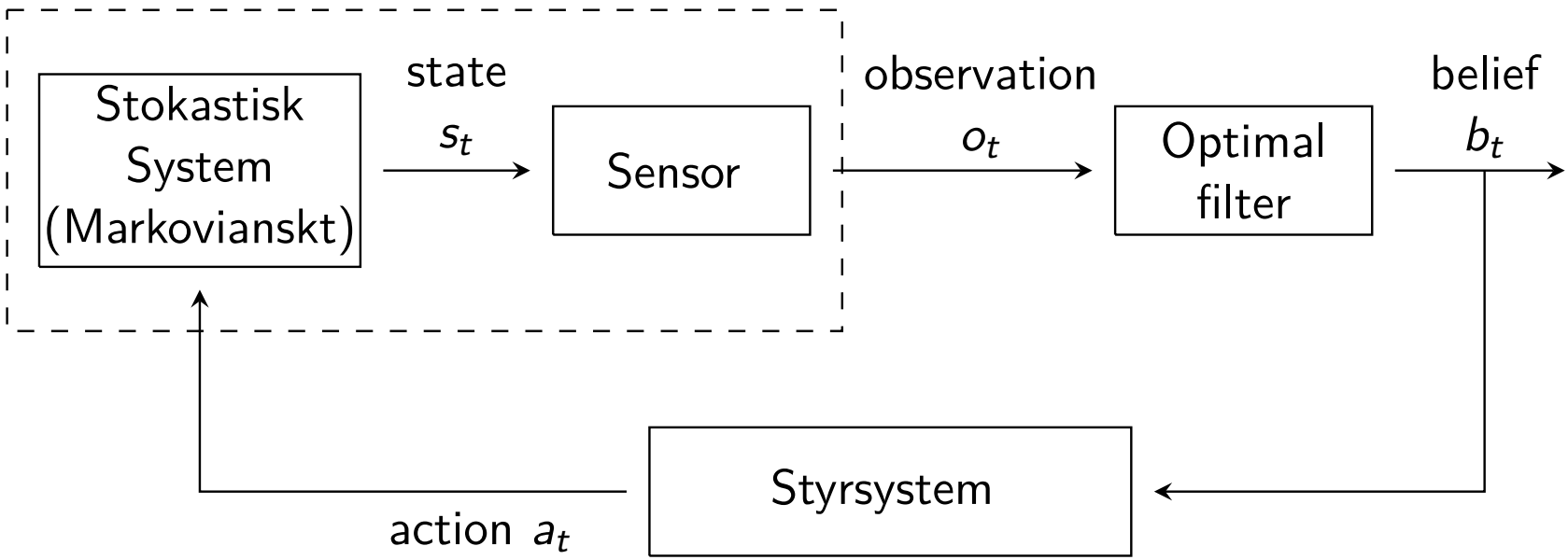
Selektiv replikering

IT infrastruktur

Automatiserad säkerhet & självlärande system

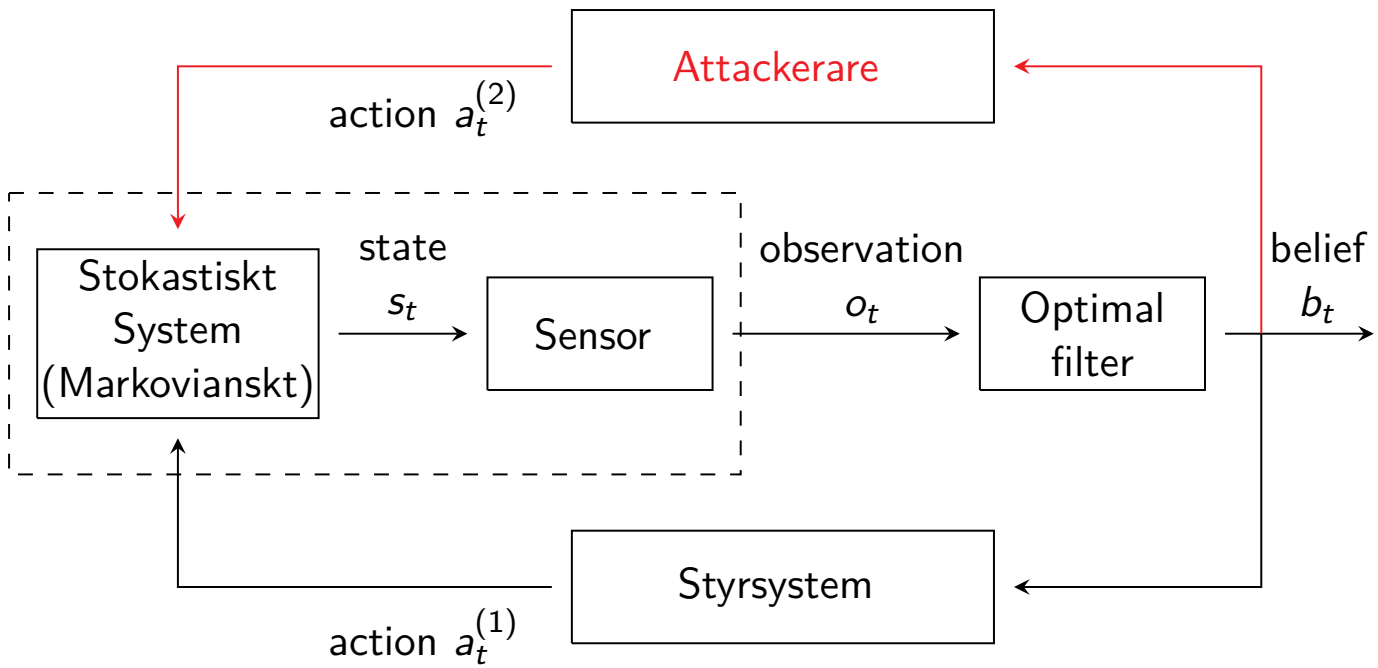
Systemmodell

- Vi modellerar systemets evolution med ett diskret dynamiskt system.
- Vi antar ett Markovianskt system med stokastisk dynamik och partiell observerbarhet.



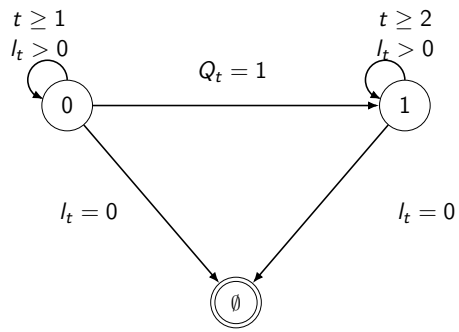
Systemmodell

- Vi modellerar systemets evolution med ett diskret dynamiskt system.
- Vi antar ett Markovianskt system med stokastisk dynamik och partiell observerbarhet.
- En Partiellt Observerbar Markoviansk Beslutprocess (POMDP)
  - Om attackeraren är statisk.
- Ett Partiellt Observerbart Stokastiskt Spel (POSG)
  - Om attackeraren är dynamisk.

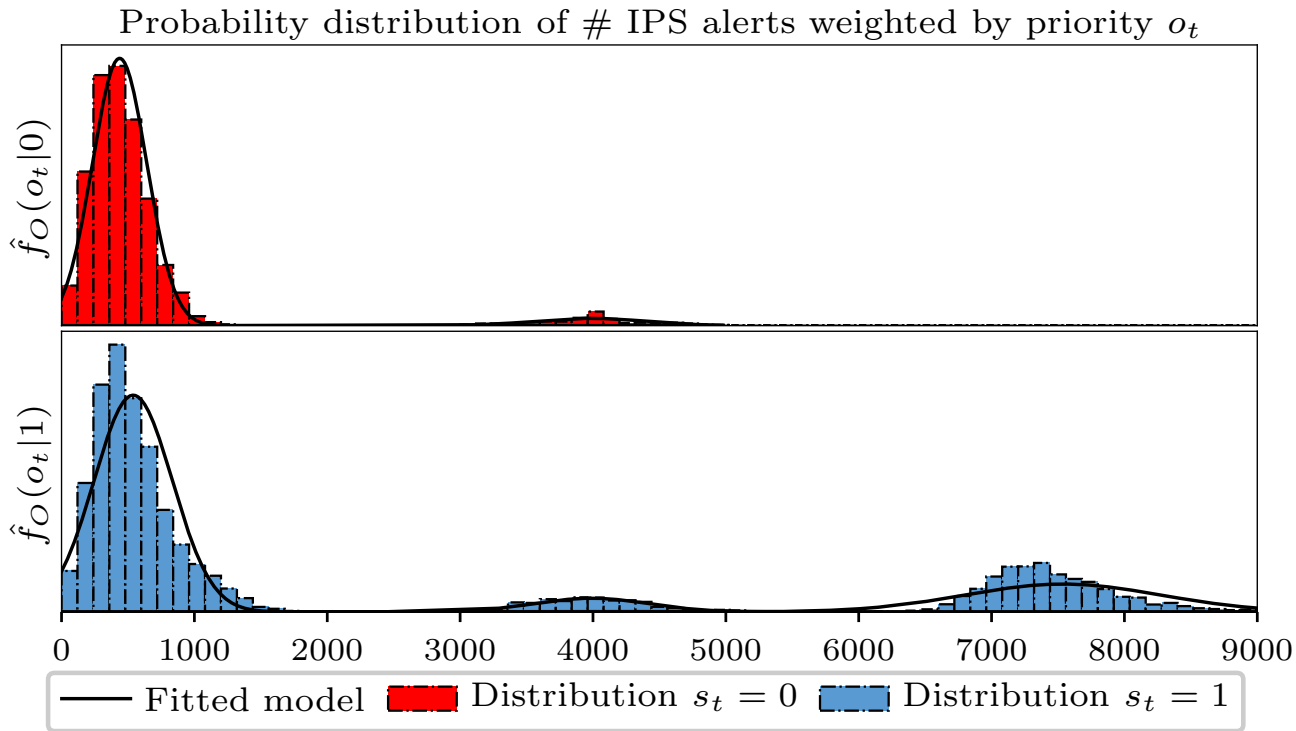


Systemmodell

- Modeller:
  - **POMDP:** $\langle \mathcal{S}, \mathcal{A}, \mathcal{P}^{a_t}_{s_t,s_{t+1}}, \mathcal{R}^{a_t}_{s_t,s_{t+1}}, \gamma, \rho_1, T, \mathcal{O}, \mathcal{Z} \rangle$
  - **POSG:** $\langle \mathcal{N}, \mathcal{S}, (\mathcal{A}_i)_{i \in \mathcal{N}}, \mathcal{T}, (\mathcal{R}_i)_{i \in \mathcal{N}}, \gamma, \rho_1, T, (\mathcal{O}_i)_{i \in \mathcal{N}}, \mathcal{Z} \rangle$
- **Tillstånd (states) och transitionssannolikheter**
  - Exempelvis intrång/icke intrång, systembelastning, osv.
  - Sannolikhet att systemet ändrar tillstånd?
- **Observationer:**
  - Exempelvis alarm från ett intrångsdetekteringssystem.
  - Observationsfördelningar?
- **Aktioner:**
  - Exempelvis: uppdatera brandvägg, uppdatera behörigheter, osv.
- **Utilitet:**
  - Exempelvis utilitet för säkerhet och för att bibehålla tjänster



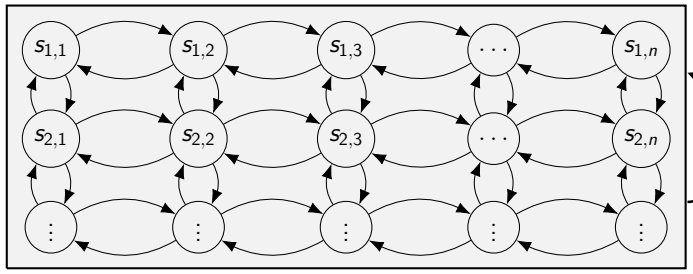
Systemidentifiering



- Observationsfördelningen f_O av försvarsobservationer (ex. IDS alarm) är inte känd.
- Vi beräknar en Gaussiansk blandningsfördelning $\hat{f}_O$ som skattning av f_O i målinfrastrukturen.
- För varje modelltillstånd s skattar vi den betingade fördelningen $\hat{f}_{O|s}$ genom expectation-maximization algoritmen.

Optimering och inlärning av försvarsstrategier

SIMULERINGSSYSTEM

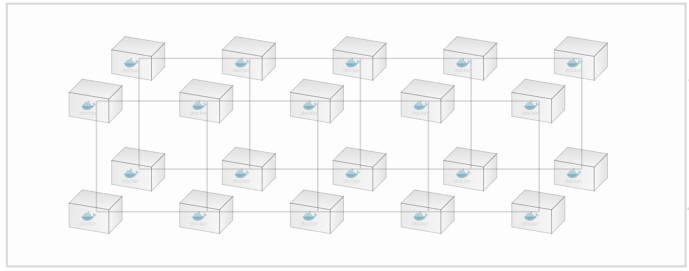


Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

EMULERINGSSYSTEM



Utvärdering & skattning av modeller

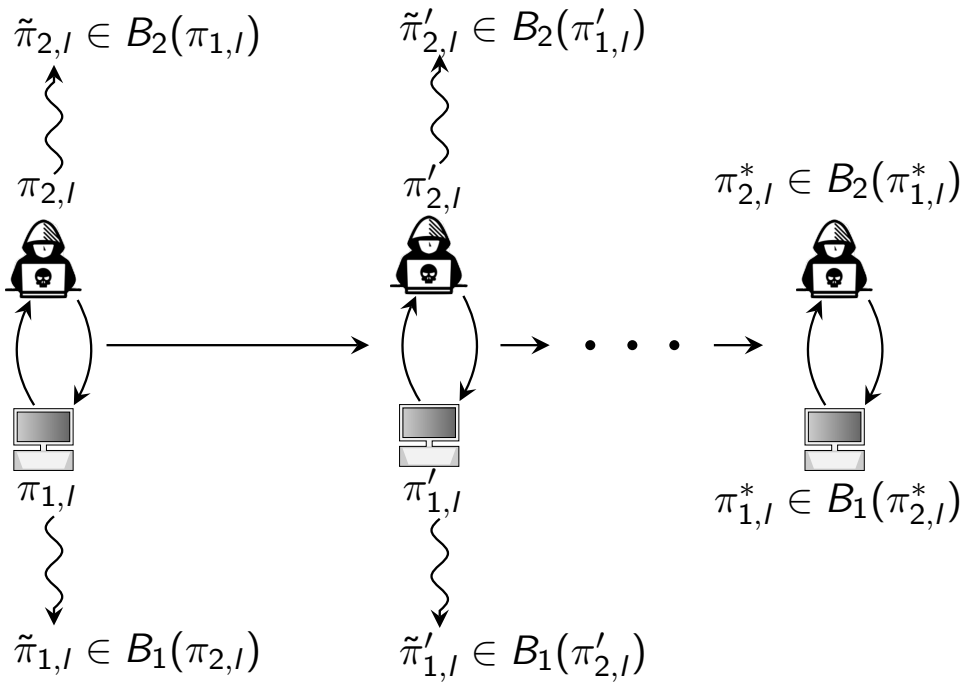
Implementation av säkerhetsstrategi π

Selektiv replikering

IT INFRASTRUKTUR

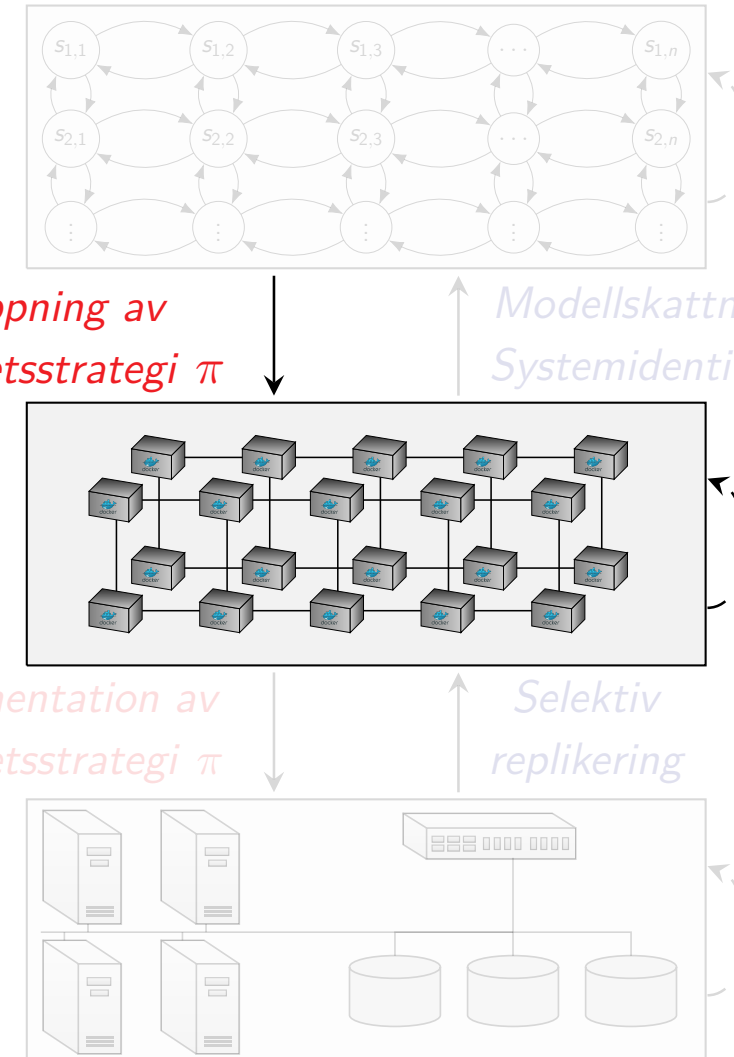
Automatiserad säkerhet & självlärande system

Optimering och inlärning av försvarsstrategier



- Simulering av den formella modellen.
- Spelarna uppdaterar sina strategier kontinuerligt.
- Beräkningsmetoder som används för att uppdatera strategier:
  - Stokastisk approximering (förstärkningsinlärning).
  - Beräkningsmässig spelteori.
  - Dynamisk/Linjär programmering.

Utvärdering av beräknade säkerhetsstrategier



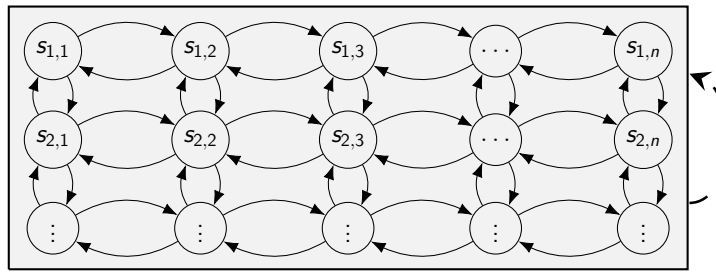
Utvärdering av beräknade säkerhetsstrategier

Type	*Actions*
Reconnaissance	TCP-SYN scan, UDP port scan, TCP Null scan, TCP Xmas scan, TCP FIN scan, ping-scan, TCP connection scan, "Vulscan" vulnerability scanner
Brute-force attack	Telnet, SSH, FTP, Cassandra, IRC, MongoDB, MySQL, SMTP, Postgres
Exploit	CVE-2017-7494, CVE-2015-3306, CVE-2010-0426, CVE-2015-5602, CVE-2014-6271, CVE-2016-10033 CVE-2015-1427, SQL Injection

Table 1: Attacker commands to emulate intrusions.

- **Utvärdering av beräknade säkerhetsstrategier:**
  1. Implementera strategierna i emuleringssystemet.
  2. Exekvera en stor mängd cyberattacker mot systemet.
  3. Granska säkerhetsstrategiernas respons.

Vår metod för att automatiskt beräkna säkerhetsstrategier

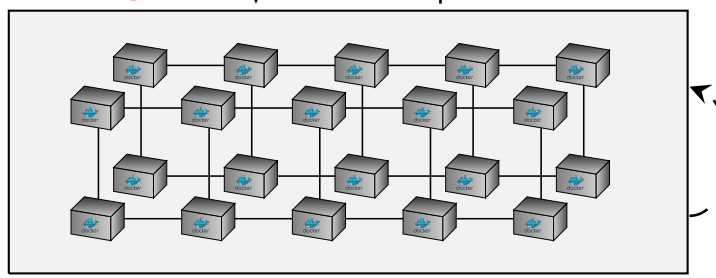


SIMULERINGSSYSTEM

Förstärkningsinlärning & optimering

Mappning av säkerhetsstrategi π

Modellskattning & Systemidentifiering

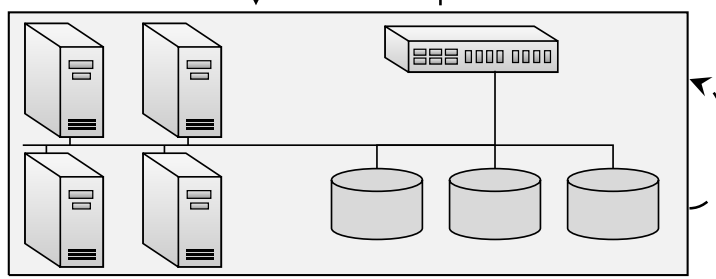


EMULERINGSSYSTEM

Utvärdering & skattning av modeller

Implementation av säkerhetsstrategi π

Selektiv replikering

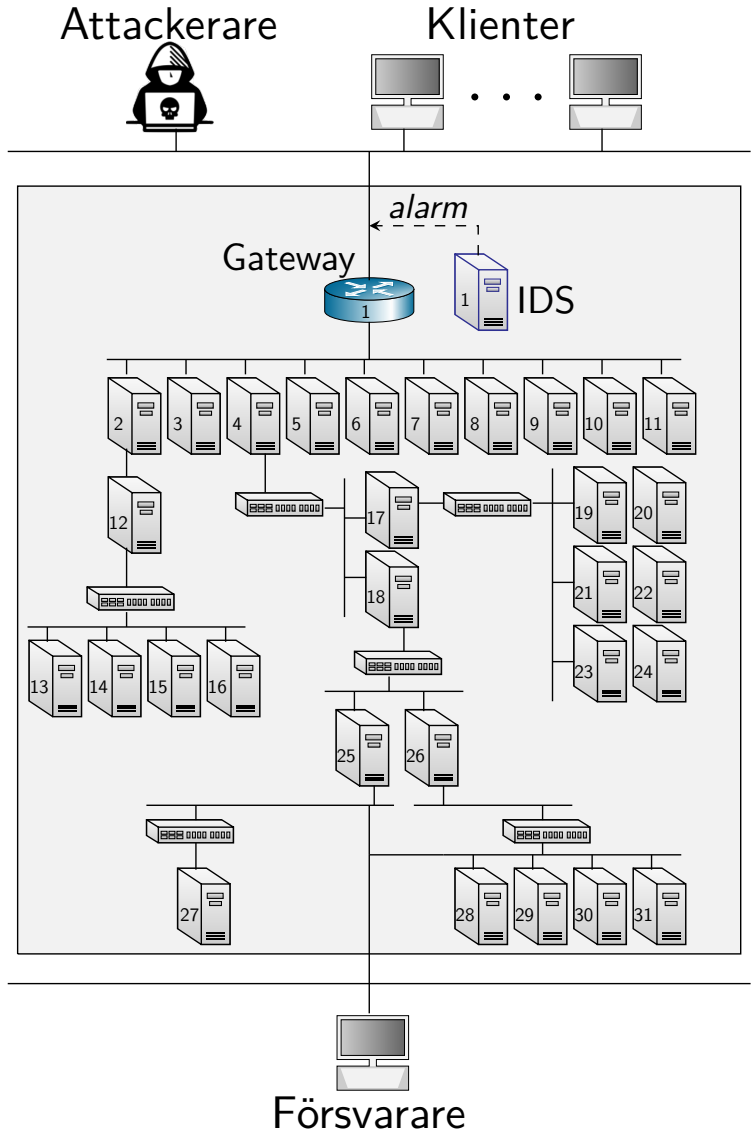


IT INFRASTRUKTUR

Automatiserad säkerhet & självlärande system

Scenario: Intrångsmitigering

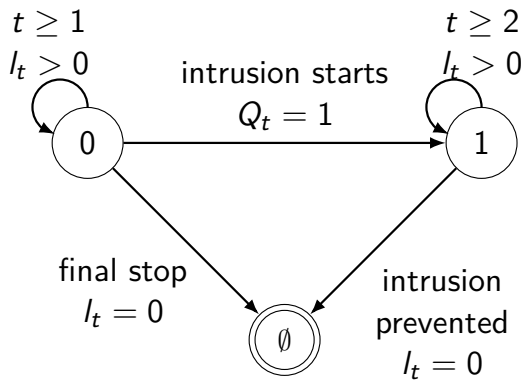
- En **försvarare** administrerar en IT-infrastruktur
  - Består av sammankopplade komponenter
  - Komponenter exekverar nätverkstjänster
  - Försvararen försvarar infrastrukturen genom övervakning och aktivt försvar.
  - Har partiell observerbarhet
- En **attackerare** har som mål att göra ett intrång på infrastrukturen
  - Har en partiell vy av infrastrukturen
  - Vill ta över specifika komponenter
  - Attackerar genom rekognisering och exploatering



Intrångsmitigering genom Optimal Multiple Stopping[1]

- **Intrångsmitigering genom Multiple Optimal Stopping:**
  - Maximera utilitet av stopptider $\tau_L, \tau_{L-1}, \ldots, \tau_1$:

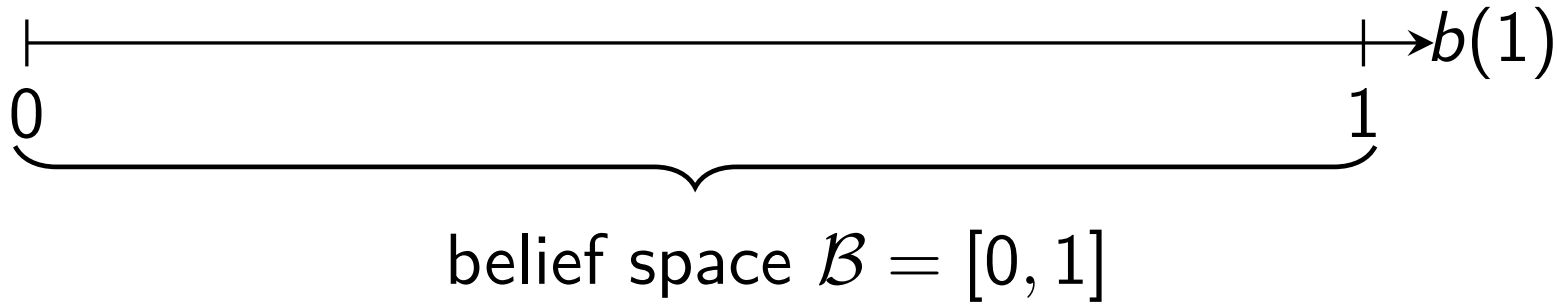
$$\pi_l^* \in \arg\max_{\pi_l} \mathbb{E}_{\pi_l} \Bigg[\sum_{t=1}^{\tau_L - 1} \gamma^{t-1} \mathcal{R}^C_{s_t, s_{t+1}, L} + \gamma^{\tau_L - 1} \mathcal{R}^S_{s_{\tau_L}, s_{\tau_L+1}, L} + \ldots + \sum_{t=\tau_2+1}^{\tau_1 - 1} \gamma^{t-1} \mathcal{R}^C_{s_t, s_{t+1}, 1} + \gamma^{\tau_1 - 1} \mathcal{R}^S_{s_{\tau_1}, s_{\tau_1+1}, 1} \Bigg]$$



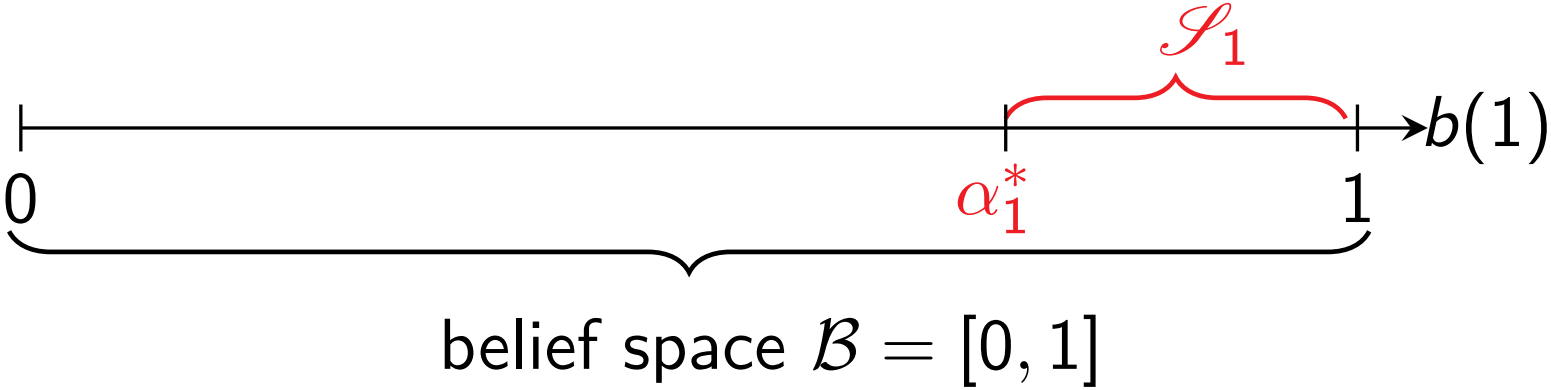
- Varje stopptid = en defensiv aktion

[1] Kim Hammar and Rolf Stadler. "Intrusion Prevention Through Optimal Stopping". In: *IEEE Transactions on Network and Service Management* 19.3 (2022), pp. 2333–2348. DOI: 10.1109/TNSM.2022.3176781.

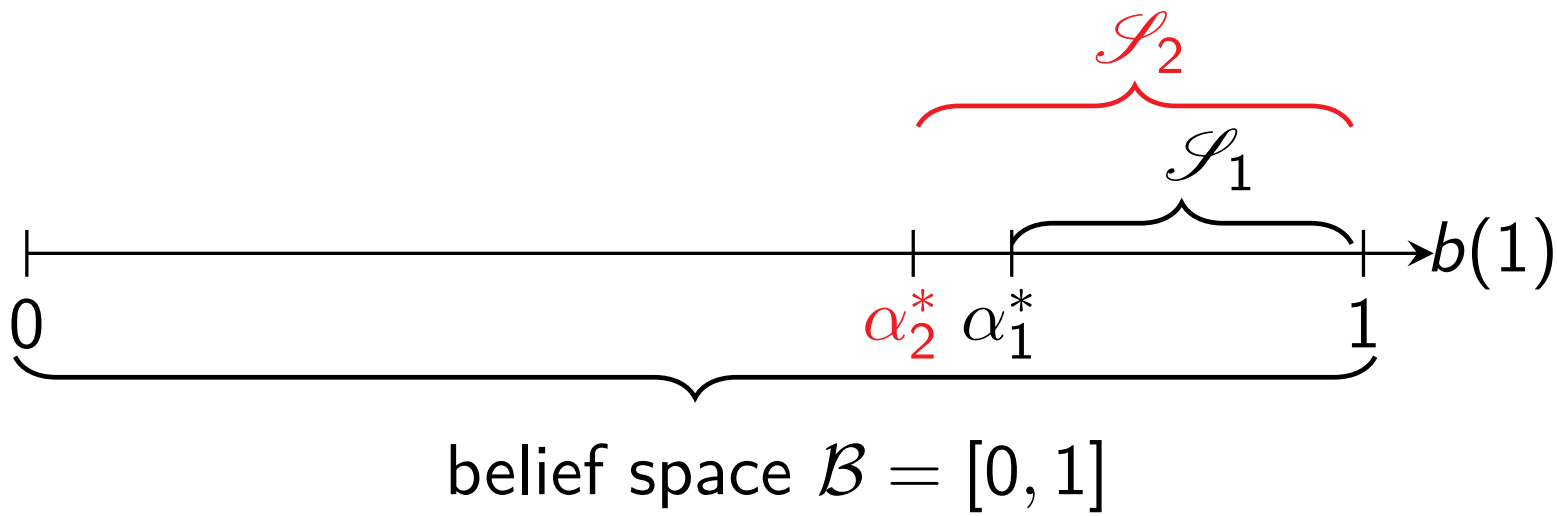
Strukturellt Resultat: Optimal Multi-Tröskel Policy & Nästlade Stoppingmängder



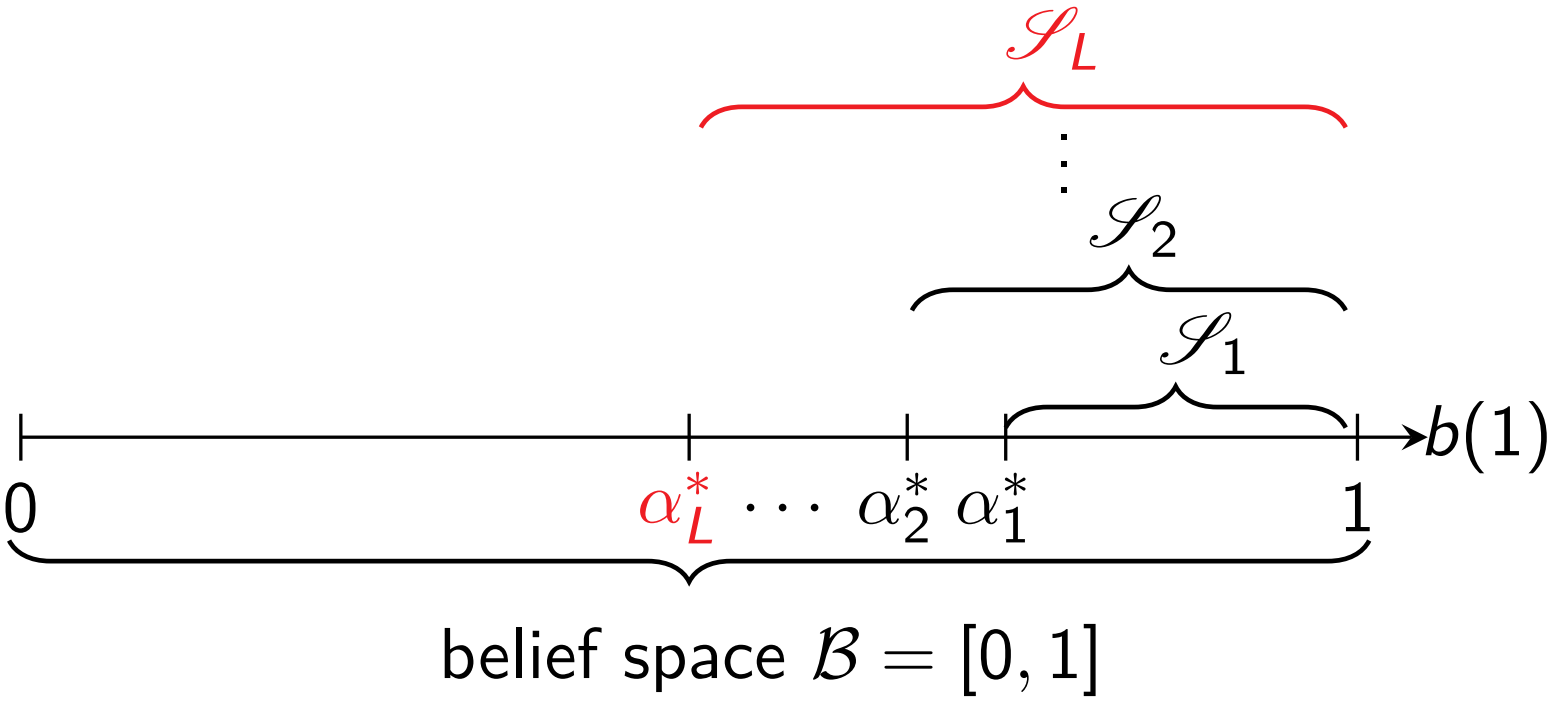
Strukturellt Resultat: Optimal Multi-Tröskel Policy & Nästlade Stoppingmängder



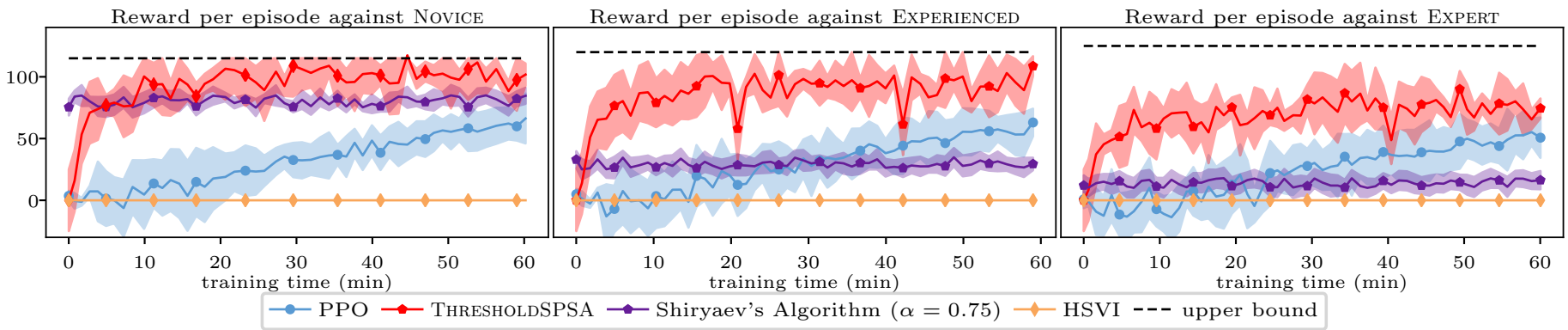
Strukturellt Resultat: Optimal Multi-Tröskel Policy & Nästlade Stoppingmängder



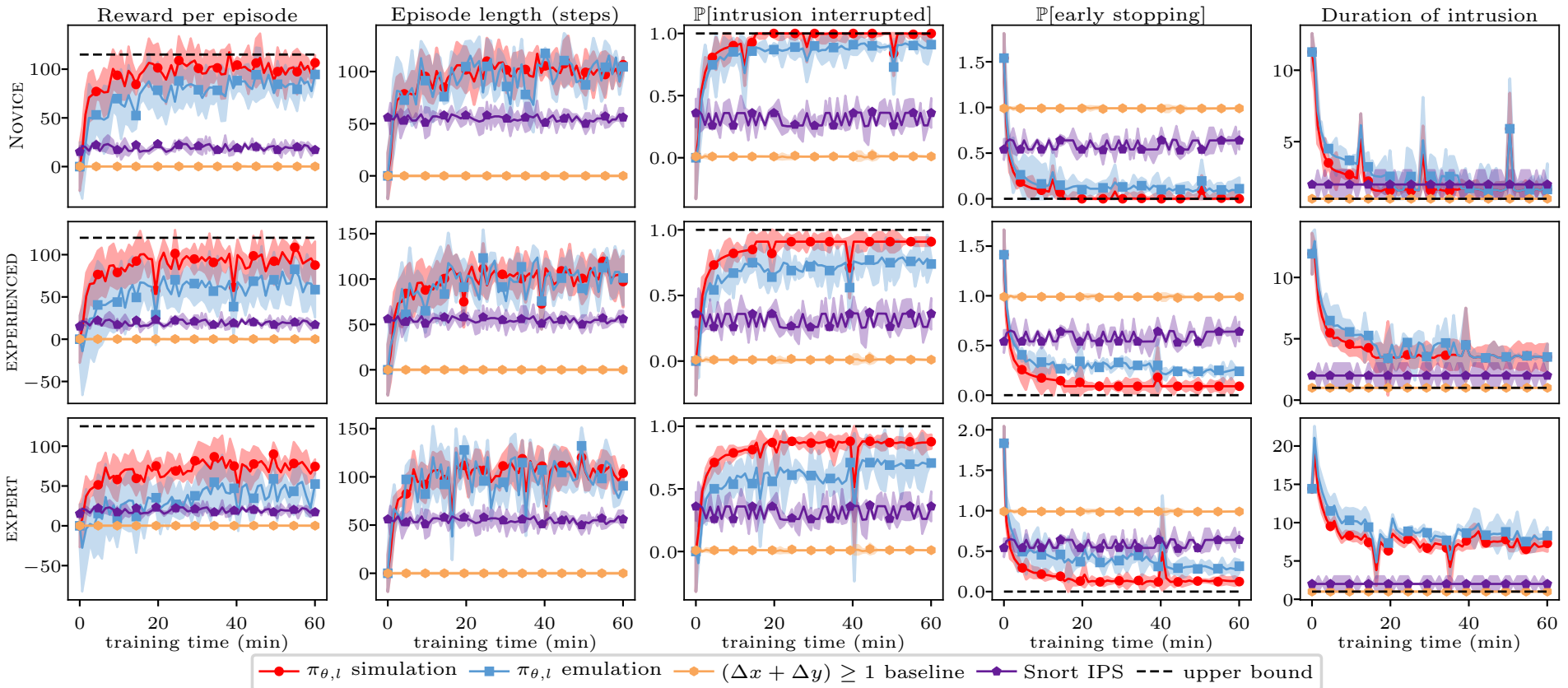
Strukturellt Resultat: Optimal Multi-Tröskel Policy & Nästlade Stoppingmängder



Jämförelse med State-of-the-art Algoritmer

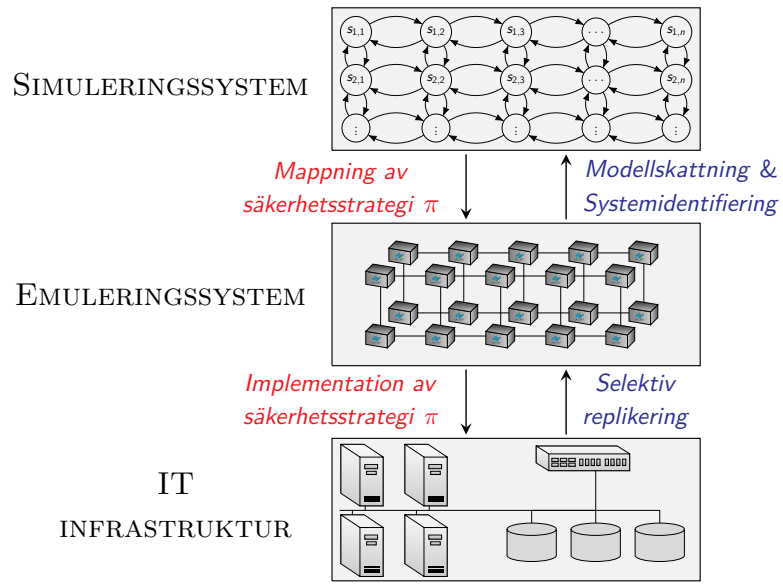


Inlärningskurvor i simuleringsmiljön och emuleringsmiljön



Sammanfattning

- We utvecklar en *metod* för automatisk inlärning av säkerhetsstrategier.
- We har applicerarat metoden på ett **intrångsmitigeringsscenario**.
- We har designat ett teoretiskt ramverk baserat på optimal-stopping teori.
- We har presenterat flera teoretiska egenskaper av den optimala säkerhetsstrategin.
- We har visat numeriska resultat från en realistisk utvärderingsmiljö.



Referenser

- *Finding Effective Security Strategies through Reinforcement Learning and Self-Play*[2]
- *Learning Intrusion Prevention Policies through Optimal Stopping*[3]
- *A System for Interactive Examination of Learned Security Policies*[4]
- *Intrusion Prevention Through Optimal Stopping*[5]
- *Learning Security Strategies through Game Play and Optimal Stopping*[6]

---

[2] Kim Hammar and Rolf Stadler. "Finding Effective Security Strategies through Reinforcement Learning and Self-Play". In: *International Conference on Network and Service Management (CNSM 2020)*. Izmir, Turkey, 2020.

[3] Kim Hammar and Rolf Stadler. "Learning Intrusion Prevention Policies through Optimal Stopping". In: *International Conference on Network and Service Management (CNSM 2021)*. http://dl.ifip.org/db/conf/cnsm/cnsm2021/1570732932.pdf. Izmir, Turkey, 2021.

[4] Kim Hammar and Rolf Stadler. "A System for Interactive Examination of Learned Security Policies". In: *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. 2022, pp. 1–3. DOI: 10.1109/NOMS54207.2022.9789707.

[5] Kim Hammar and Rolf Stadler. "Intrusion Prevention Through Optimal Stopping". In: *IEEE Transactions on Network and Service Management* 19.3 (2022), pp. 2333–2348. DOI: 10.1109/TNSM.2022.3176781.

[6] Kim Hammar and Rolf Stadler. "Learning Security Strategies through Game Play and Optimal Stopping". In: *Proceedings of the ML4Cyber workshop, ICML 2022, Baltimore, USA, July 17-23, 2022*. PMLR, 2022.