Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

sdw
Stiftung der Deutschen Wirtschaft

Descartes
research

The Vision of Self-aware Reordering of Security Network Function Chains

ICPE 2018, Berlin

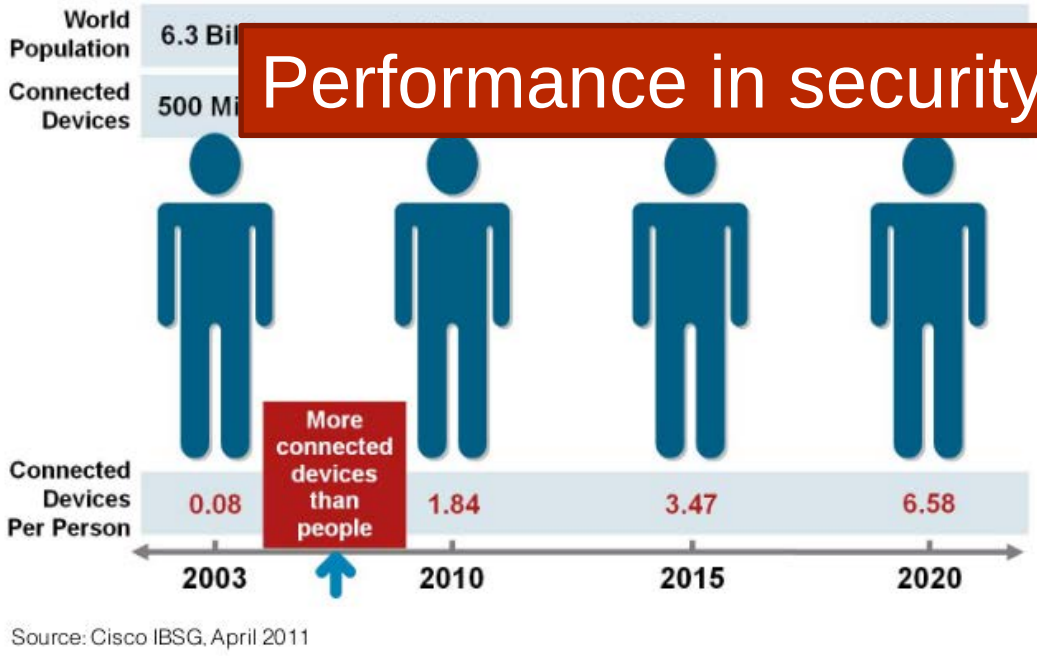
Lukas Iffländer, Jürgen Walter, Simon Eismann and Samuel Kounev

http://se.informatik.uni-wuerzburg.de/

MOTIVATION

New Challenges

- Exponentially increasing number of hackable devices in the IoT
- End of Moore‘s Law
- Attacks become easier (DDoSaaS)
- Frequency of attacks and range of targets increases



Source: Cisco IBSG, April 2011

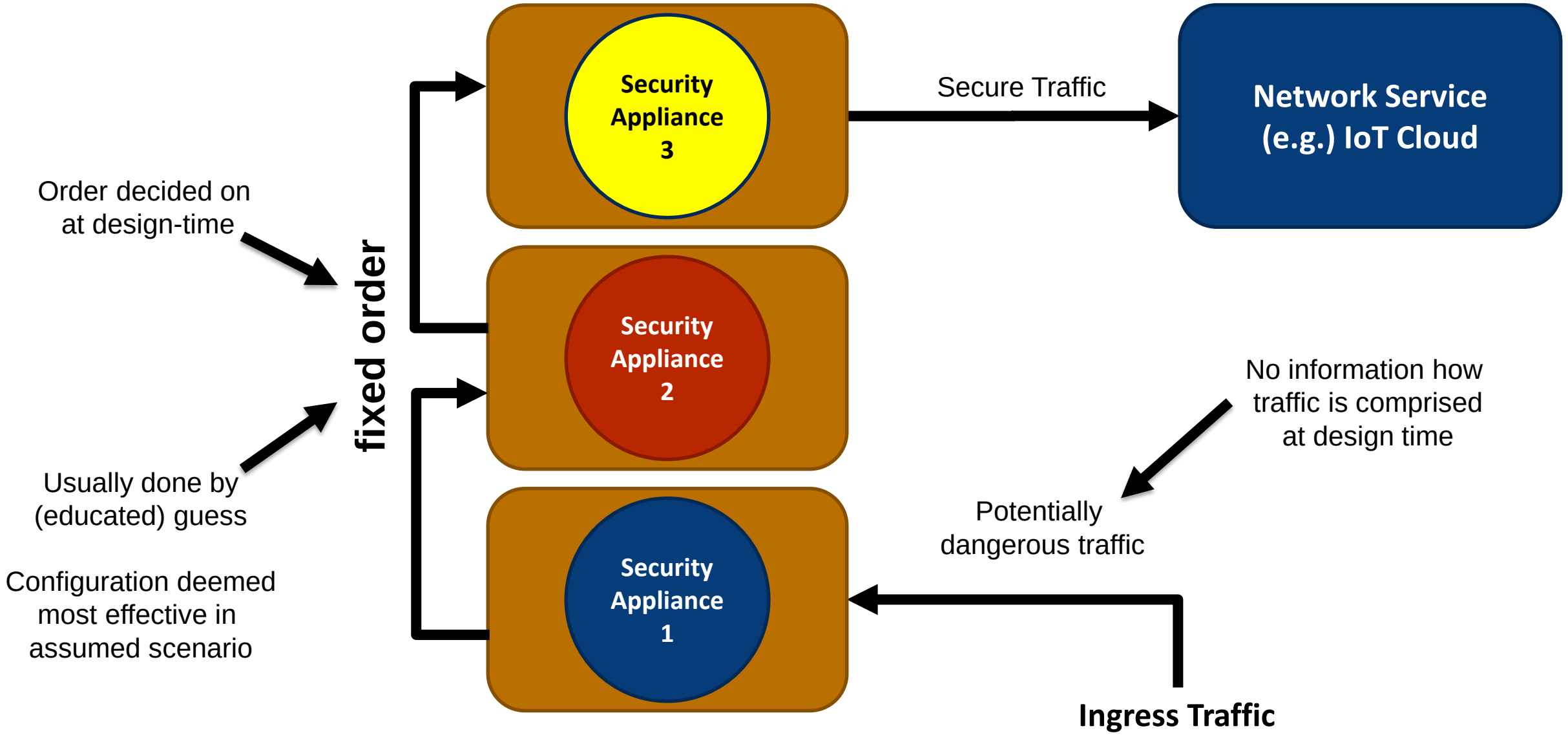
Performance in security becoming more important

Structure

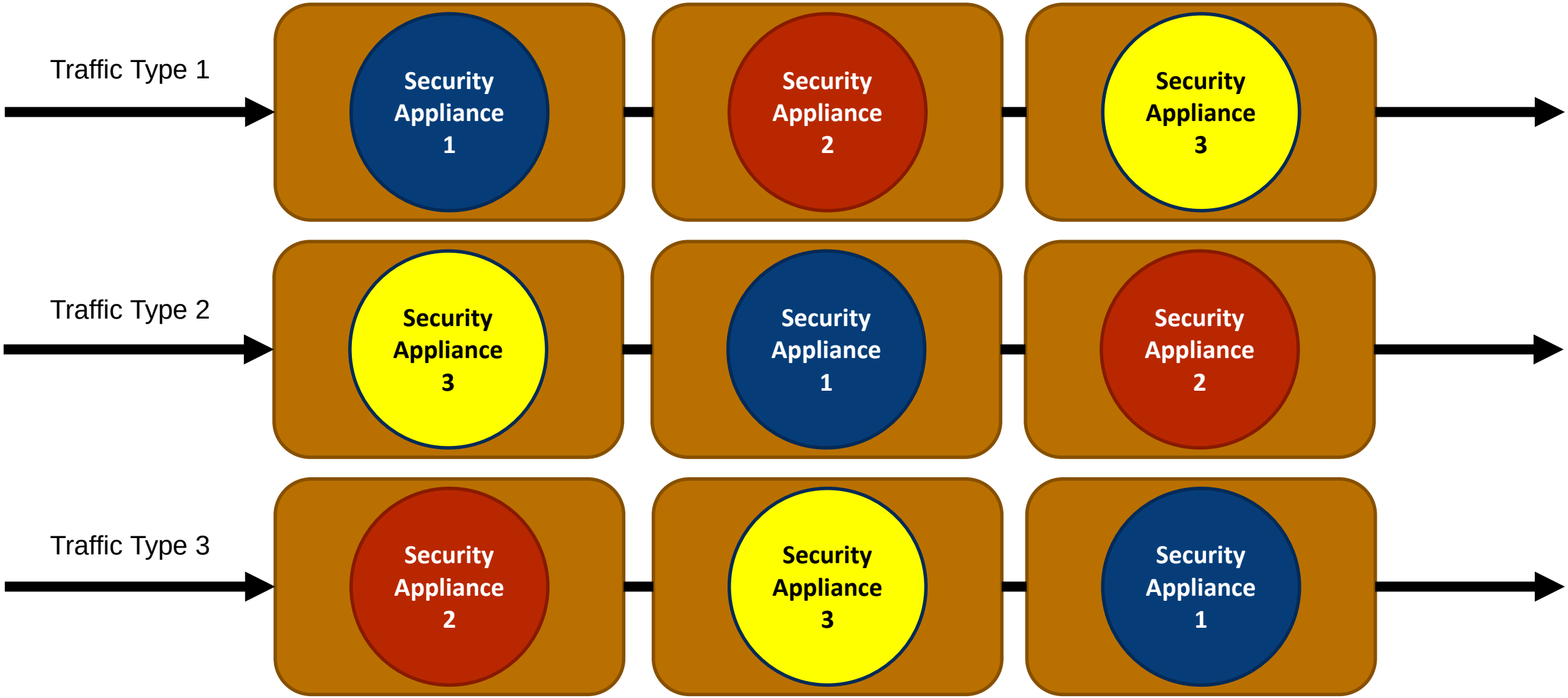
- Motivation
- Problem Formulation
- Approach
- Conclusion & Future Work

PROBLEM FORMULATION

Current Approach to Network Security

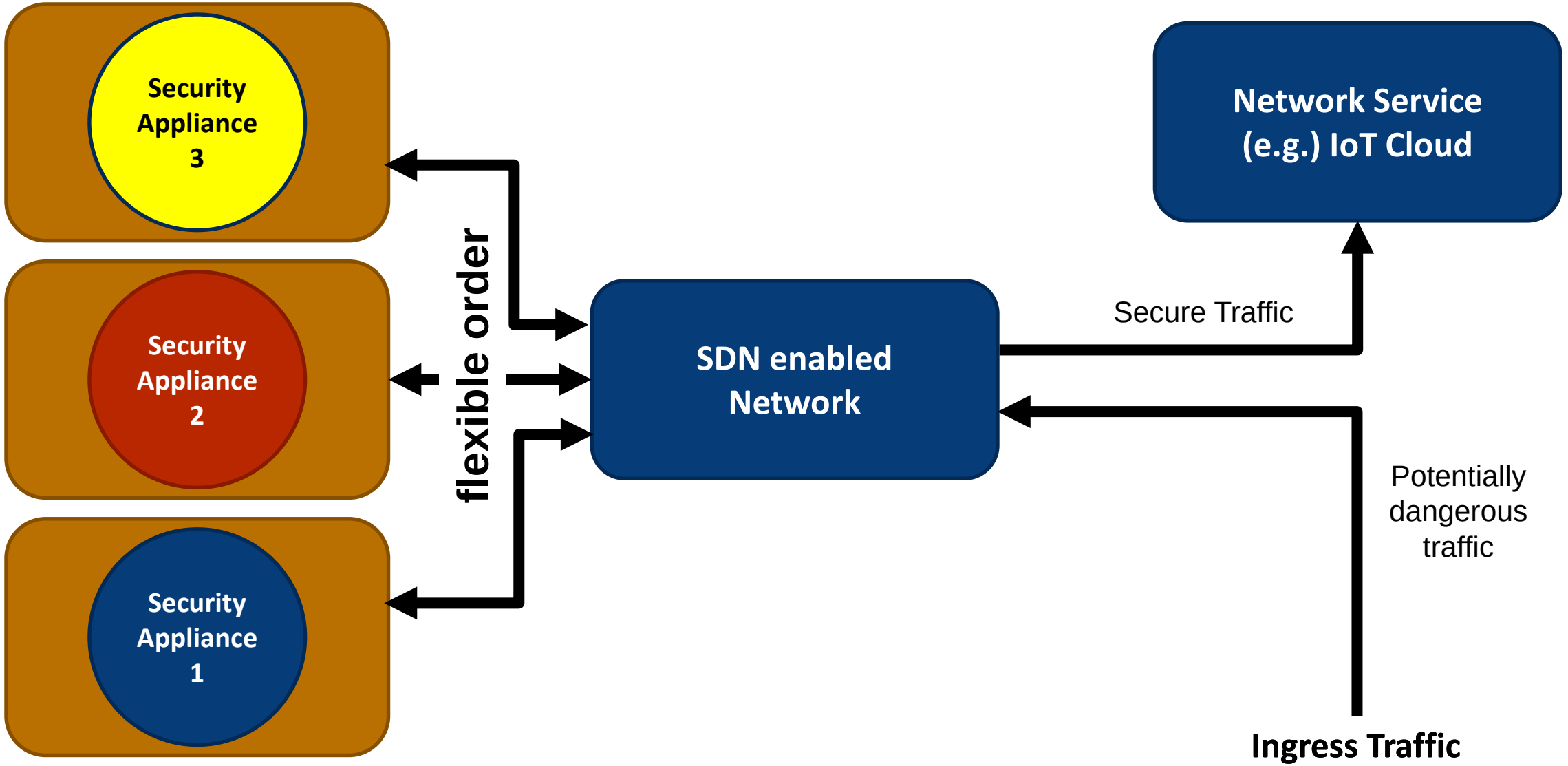


Different Optimal Order



APPROACH

Requirement: Flexible Order



Knowledge – The Road to Victory

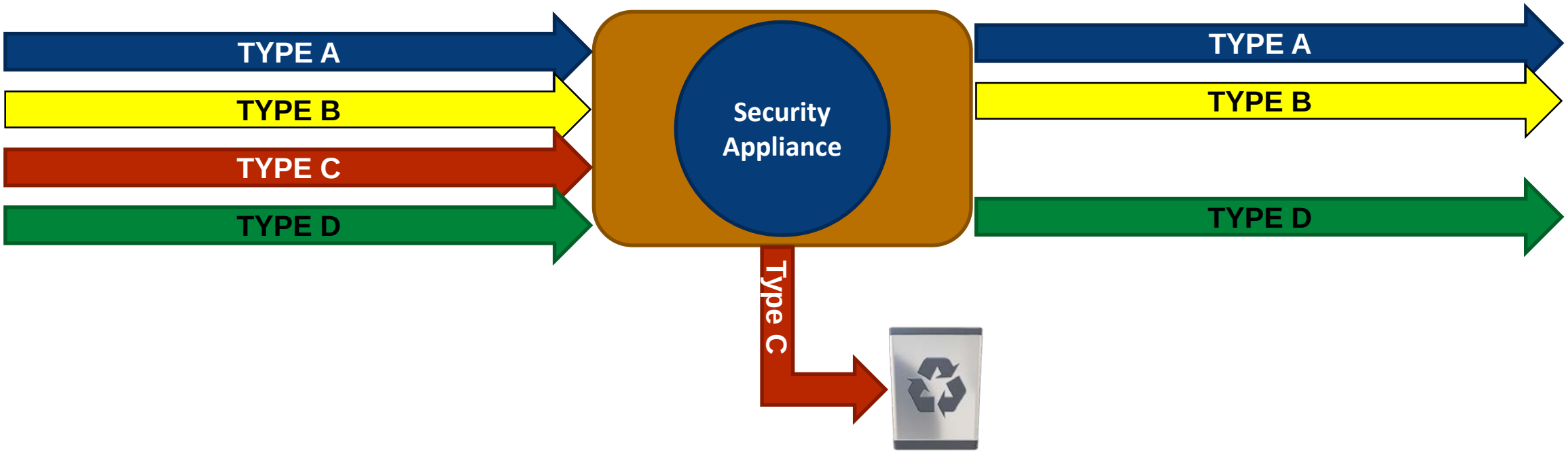
- If you know the enemy and know yourself, you need not fear the result of a hundred battles.

  - Sun Tzu “The Art of War”

- Enemy
  - Type of attacks incoming
  - Composition of incoming traffic
- Ourselves
  - Computation requirements
  - Output and input traffic

Getting to know yourself

- Model security appliances as software components:
  - Output traffic as a function of input traffic



- Model function chains by putting models for every used type in right order

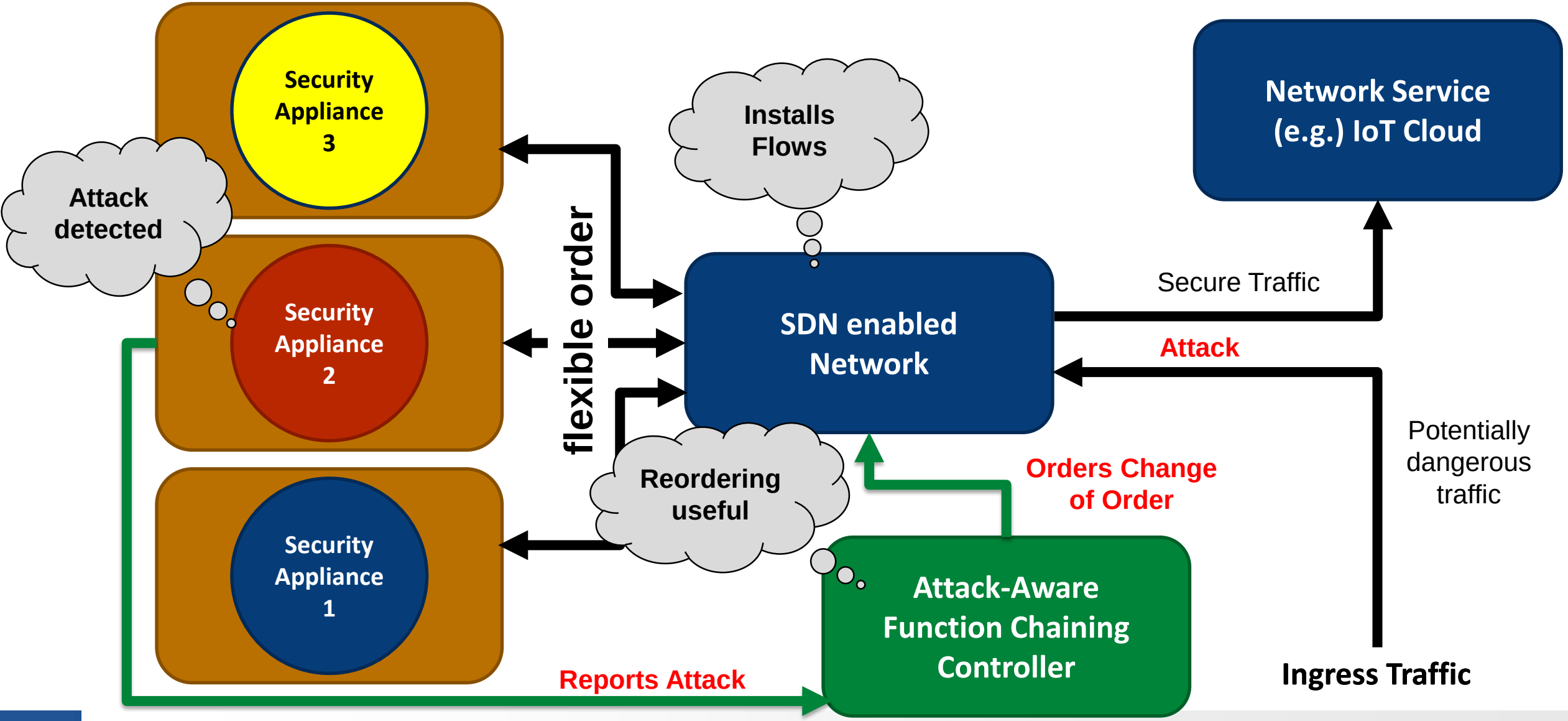
Getting to know your enemy

- Distribution of attack traffic required
- Local distribution available at each SA
  - Traffic runs through the chain until it hits first SA capable of defense
  - Benign traffic runs through all stages
  - SAs have number of alerts
- Put global distribution together
  - SAs report alerts to a central instance
  - Central instance aggregates data
  - Central instance infers distribution

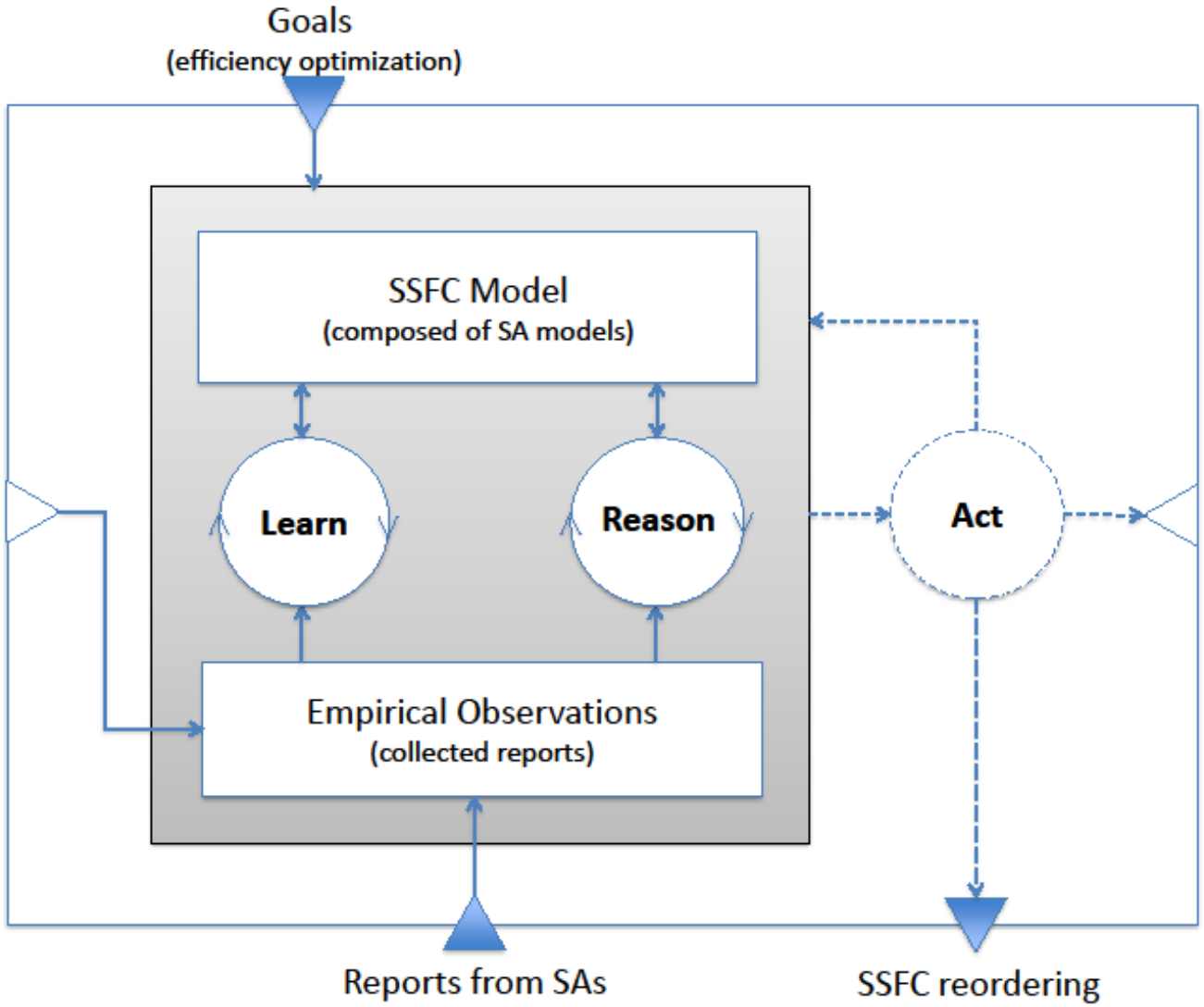
Using our new Knowledge

- Inferred distribution can be fed into function chain model
- Throughput / required computational resources computed from model
- Optimal configuration can be deduced by feeding possible configurations into model
- Optimal configuration gives
  - Optimal performance
  - Minimal computational resources required

Suggest Solution



Integration in LRA-M Loop



CONCLUSION AND FUTURE WORK

Conclusion and Future Work

- Vision of self-aware security network function chains
- Situation-aware reordering of the function chains based on models
  - Modelling security appliances as functions on the traffic distribution
  - Modelling traffic composition based on feedback from security appliances
  - Determine best configuration from the model
- Next steps
  - Realize our approach (many parts already at prototype stage)
  - Extend for further parameters (e.g. behavior under overload)

Thank you for your attention!

Phone: +49 (931) 31 89947
Mail: lukas.ifflaender@uni-wuerzburg.de
Web: https://go.uniwue.de/ifflaender