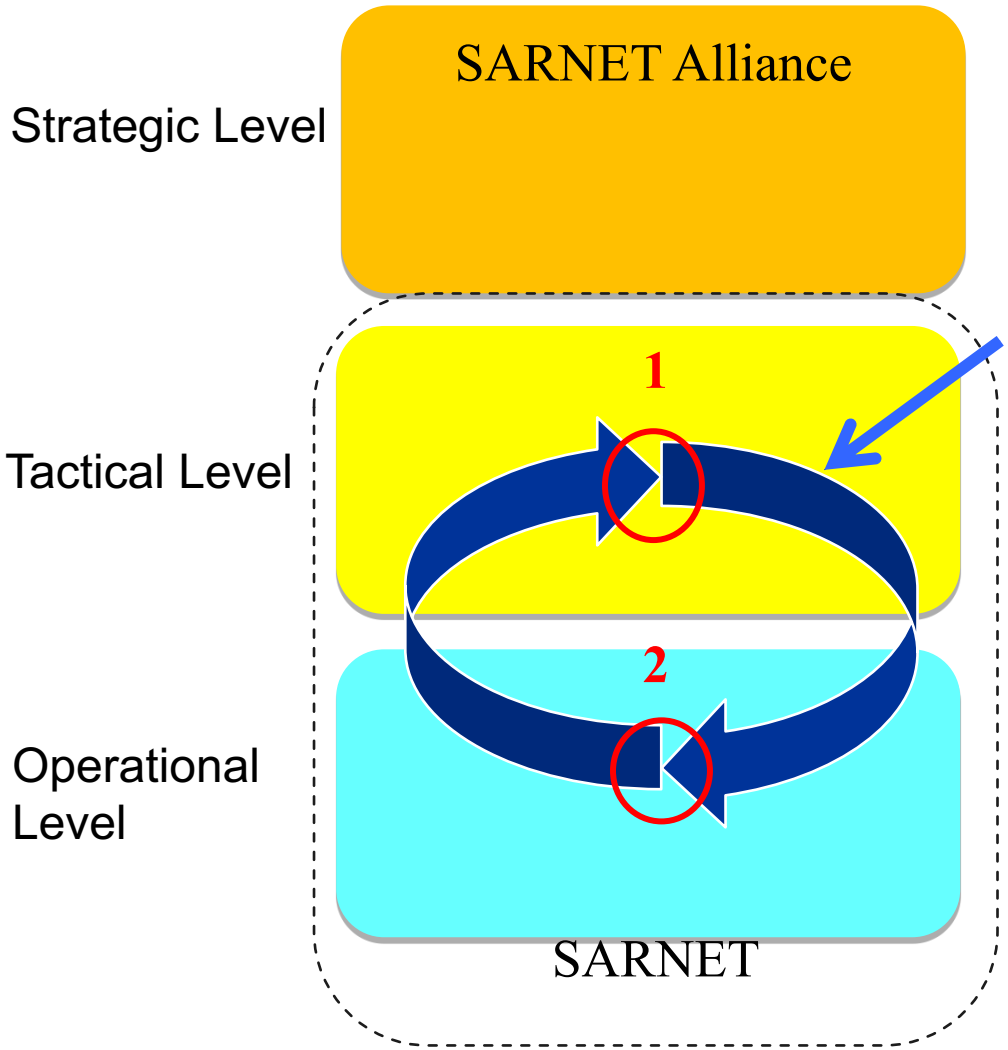
Determining the effectiveness of countermeasures against cyber attacks

Ralph Koning
Ben de Graaff, Paola Grosso, Robert Meijer, Cees de Laat

System and Network Engineering research group
Universiteit van Amsterdam

• Context

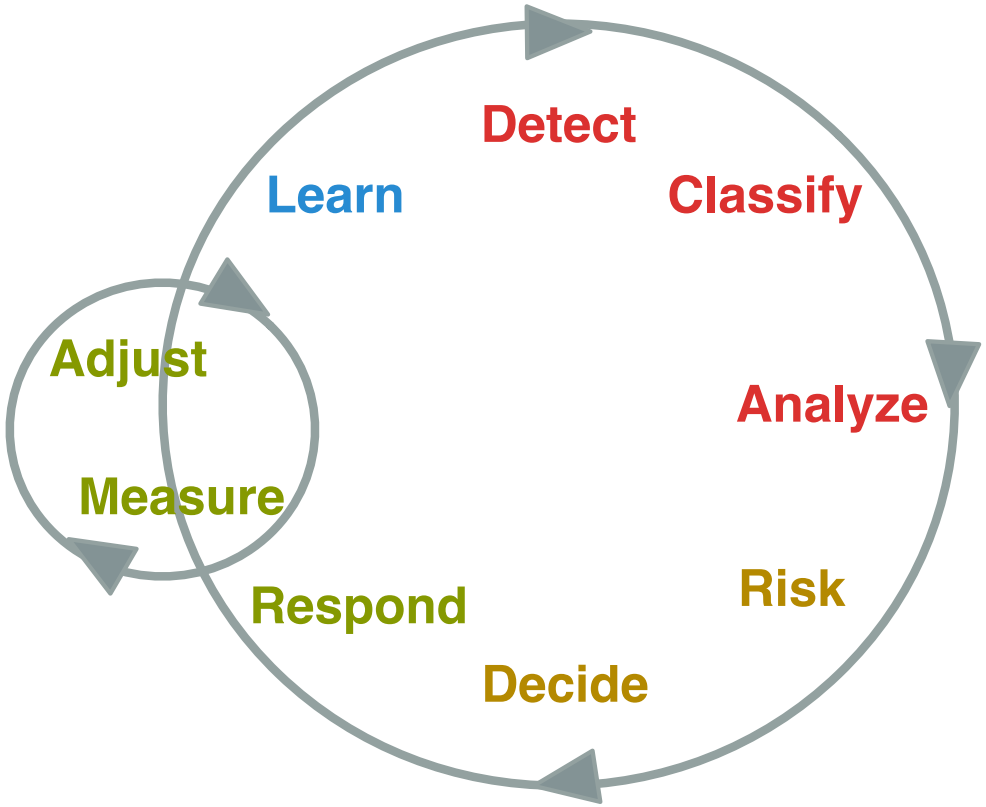


Ameneh Deljoo (PhD):
Why create SARNET Alliances?
Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders

Gleb Polevoy (PD):
Determine best defense scenario against cyberattacks deploying SARNET functions (**1**) based on security state and KPI information (**2**).

Ralph Koning (PhD)
Ben de Graaff (SP):
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g cost)

Control loop



Detection phase: Detect, Classify, Analyze

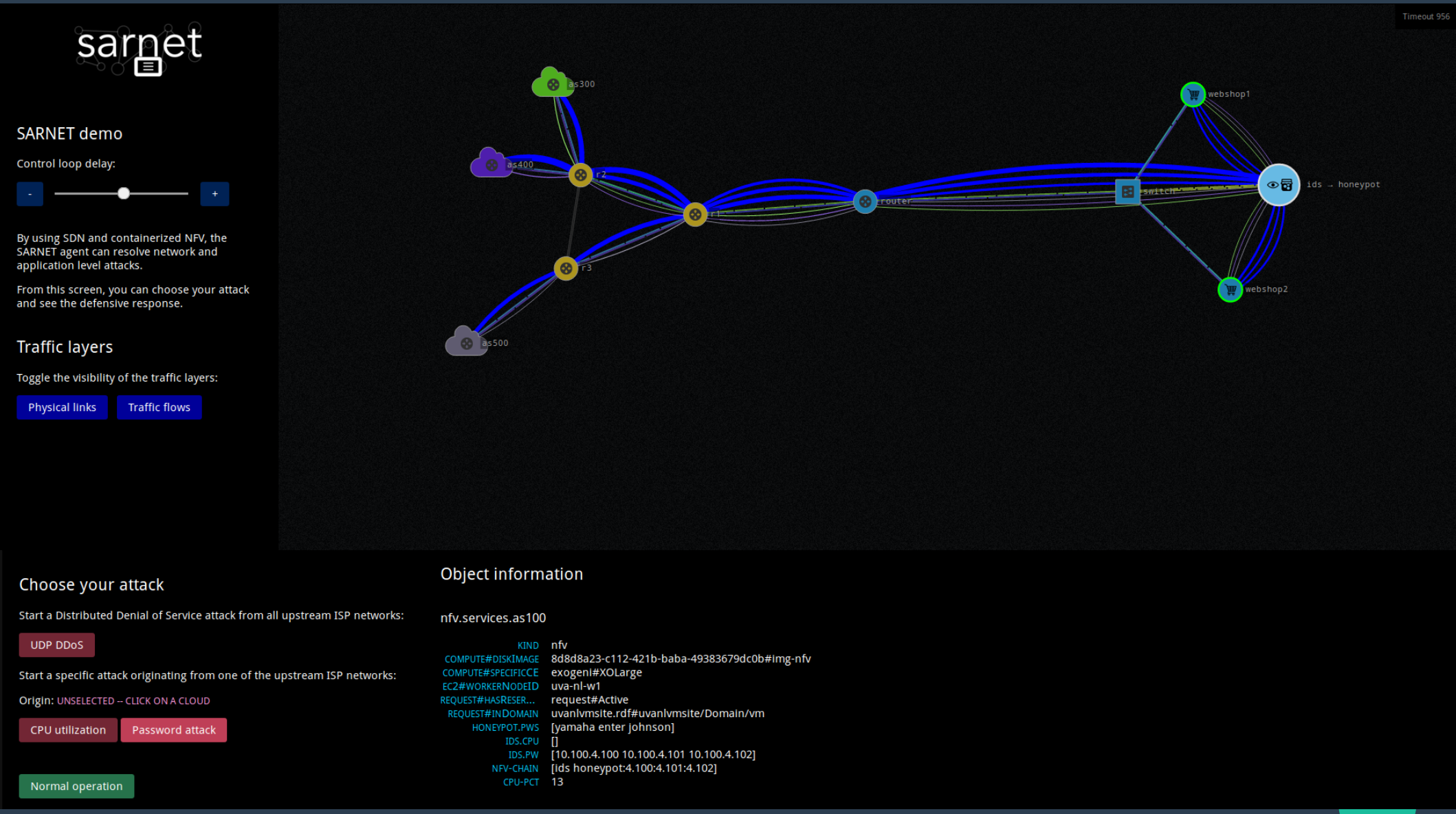
Decision phase: Risk, Decide

Response phase: Respond, Adjust, Measure

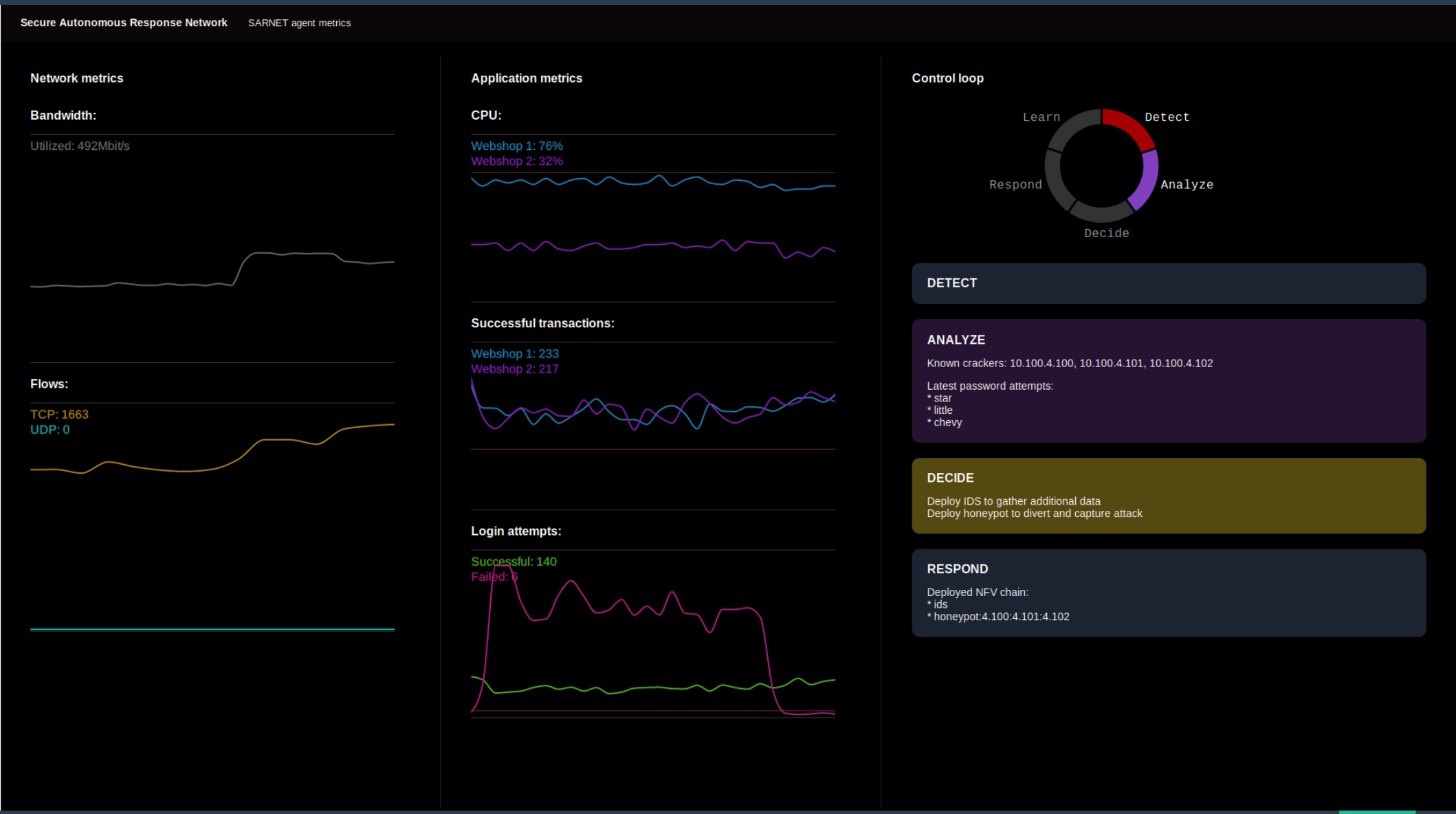
Learn phase: Learn (with input form other phases)

Environment

• Scenario


sarnet
SARNET demo
Control loop delay:
-
+
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.
From this screen, you can choose your attack and see the defensive response.
Traffic layers
Toggle the visibility of the traffic layers:
Physical links
Traffic flows
Timeout 956
as300
as400
as500
r1
r2
r3
router
switch
webshop1
webshop2
ids → honeypot
Choose your attack
Start a Distributed Denial of Service attack from all upstream ISP networks:
UDP DDoS
Start a specific attack originating from one of the upstream ISP networks:
Origin: UNSELECTED -- CLICK ON A CLOUD
CPU utilization
Password attack
Normal operation
Object information
nfv.services.as100
KIND nfv
COMPUTE#DISKIMAGE 8d8d8a23-c112-421b-baba-49383679dc0b#img-nfv
COMPUTE#SPECIFICCE exogeni#XOLarge
EC2#WORKERNODEID uva-nl-w1
REQUEST#HASRESER... request#Active
REQUEST#INDOMAIN uvanlvmsite.rdf#uvanlvmsite/Domain/vm
HONEYPOT.PWS [yamaha enter johnson]
IDS.CPU []
IDS.PW [10.100.4.100 10.100.4.101 10.100.4.102]
NFV-CHAIN [ids honeypot:4.100:4.101:4.102]
CPU-PCT 13

• Observables

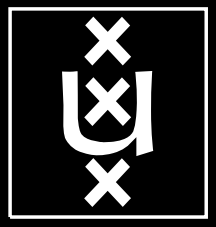


Effectiveness and Impact

Effectiveness and Impact (2)

Future work

- **Metrics**
  - Cost
    - –
- **Learning**
  - Dynamic baseline
  - Adaptive observable thresholds
- **Multi domain**
  - Cooperative vs non-cooperative domains



University of Amsterdam

https://sarnet.uvalight.net/

mailto: r.koning at uva.nl

TNO innovation for life

NWO
Netherlands Organisation for Scientific Research

COMMIT/

AIRFRANCE KLM

ciena