SARNET
Secure Autonomous Response NETworks

Ralph Koning,
SNE Research Group | University of Amsterdam

e-mail: r.koning _at_ uva.nl
web: https://staff.fnwi.uva.nl/r.koning/
Ameneh Deljoo (PhD): Why create SARNET Alliances? Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders.

Stojan Trajanovski (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).
SARNET control loop

Detect
Classify
Analyze
Risk
Decide
Respond
Measure
Adjust
Learn
Example observables:

Services request to service $x$ is only allowed from $y$
Response time of the application should be $< 30$ms
CPU load of system $x$ should not exceed $y$
Network bandwidth on link $x$ cannot exceed $1$ gb/s
Traffic to service provider $x$ must pass via link $y$
SARNET patterns

Nesting

Intersecting

Security Observable

SO

SO

SO

SO
Objective

• To get a better understanding for cyber attack complexity by visually defend a network suffering from basic volumetric attacks.
• To find a way to visualize future research in automated response.

Demo highlights

• Pre-programmed attack scenarios that are able to show defense functions.
• Virtual sales + income from web services
• Defense cost

DDoS Defence functions.

• Filtering
• Blocking
• Resource Scaling
VNET demo prototype

Multitouch Table or Web browser

VNET-visualization UI

UI controller

VNET

Infrastructure controller
Monitoring system
Network controller

uva-nl
ExoGENI rack

VNET-agent
Network Functions

Virtual machines
Touch table demo
Solution cost vs revenue

The graph shows the relationship between solution costs and revenue compared to a baseline, with two scenarios distinguished by different markers (scenario 1 and scenario 2). The costs are compared to the baseline in percentage terms, indicating a range from 90% to 170%. The revenue is also expressed as a percentage compared to the baseline, with values ranging from 20% to 180%. The distribution of data points suggests a trend where higher revenue is associated with a wider range of costs for both scenarios.
Solution cost vs revenue

Revenue gain!
Solution cost vs revenue

Full revenue recovery without (much) extra costs
https://sarnet.uvalight.net/