SPIDER
5G CYBER RANGE

A Digital Twin for the 5G Era: the SPIDER Cyber Range

Filippo Rebecchi (THALES), Antonio Pastor (Telefonica), Alberto Mozo (UPM), Chiara Lombardo (CNIT), Roberto Bruschi (CNIT), Ilias Aliferis (UniSystems), Roberto Doriguzzi-Corin (FBK), Panagiotis Gouvas (Ubitech), Antonio Alvarez Romero (ATOS), Anna Angelogianni (UPRC), Ilias Politis (UPRC), Christos Xenakis (UPRC)

Outline

- What is a cyber range
- Why a 5G specific cyber range?
- Guided tour of the SPIDER architecture
- Testbed and Validation activities
- Live demo

Cyber Range definition

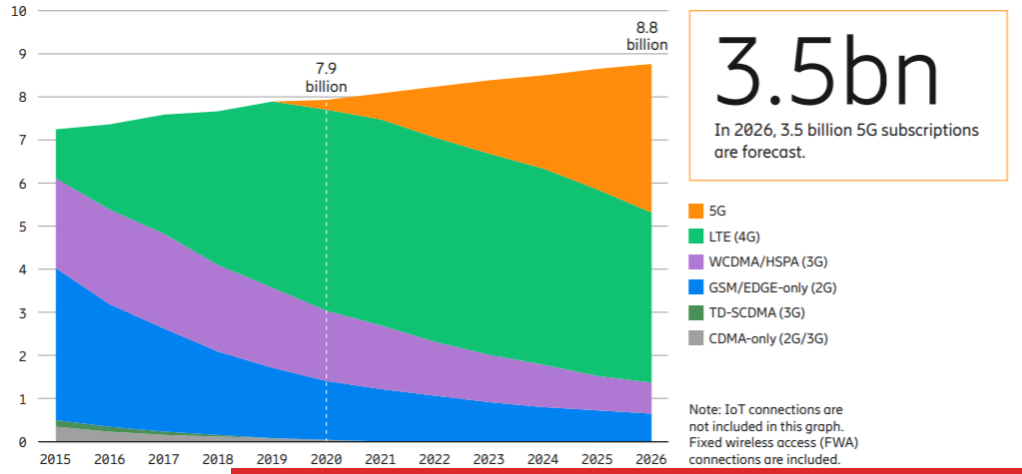
*"Interactive, **simulated representations** of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain **hands-on cyber skills** and a secure environment for product development and security posture testing."*

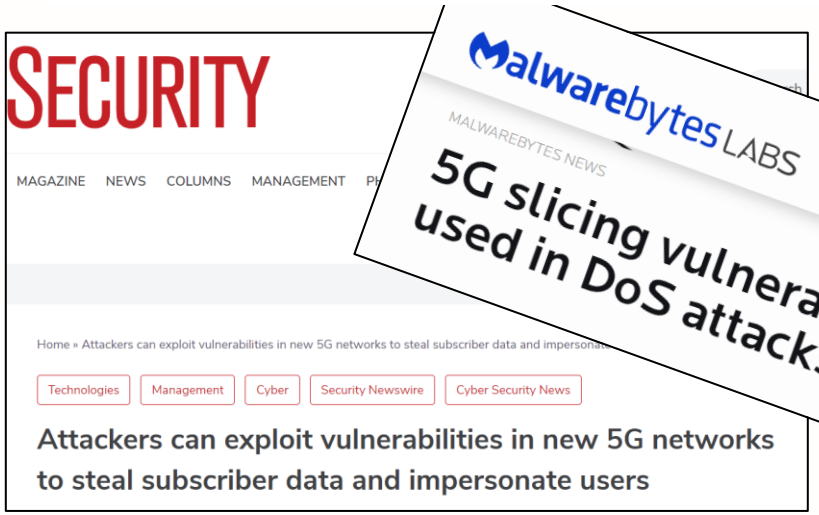
NIST

High market potential & several security concerns

The 5G enterprise market is expected to grow from USD 2.1 billion in 2021 to USD 10.9 billion by 2027, at a CAGR of 31.8%

A few major factors driving the growth of this market are the emergence of Industry 4. 0 paving the way for mMTC, the development of smart infrastructure, and the delivery of differentiated 5G services using network slicing technique.





Train before taking off with 5G

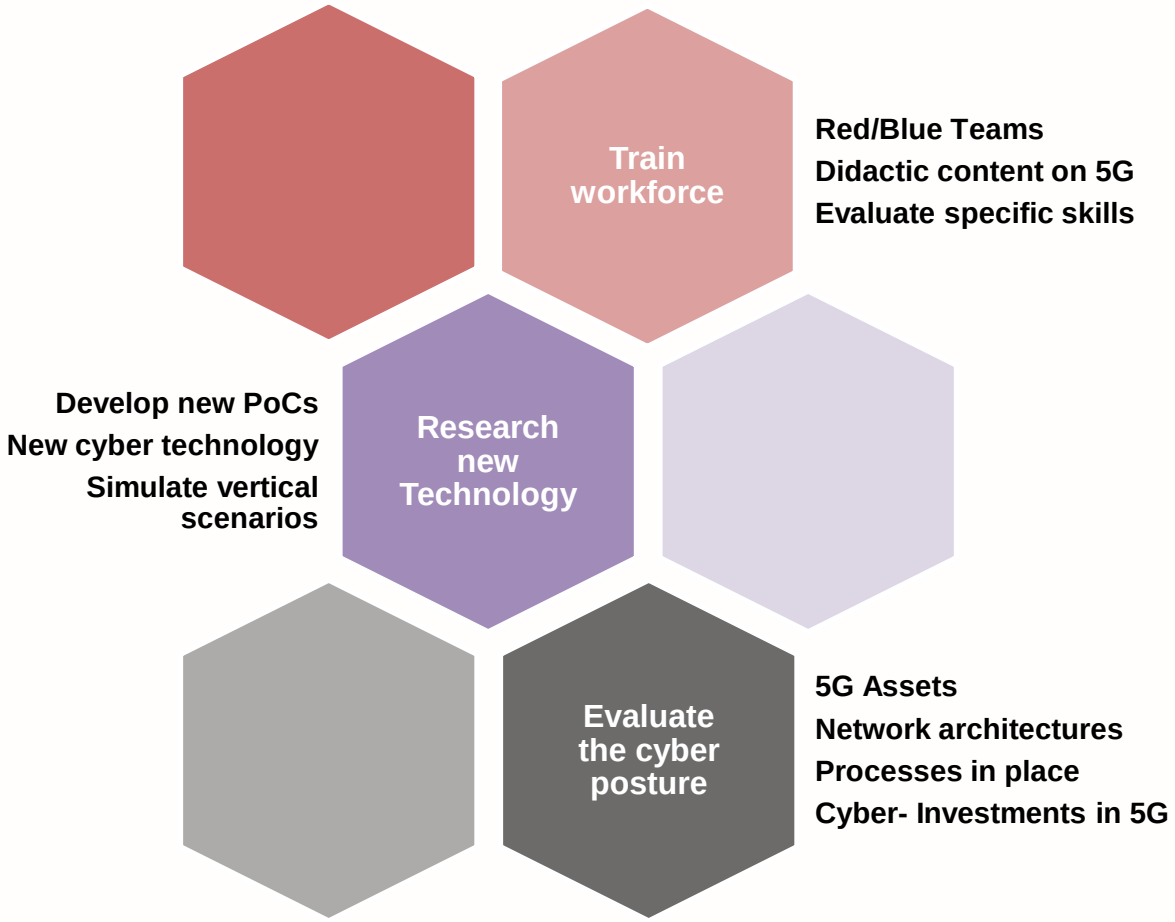
Training

Digital Twin Required

Flight

Before taking off with 5G you want to train and know the « emergency procedures »

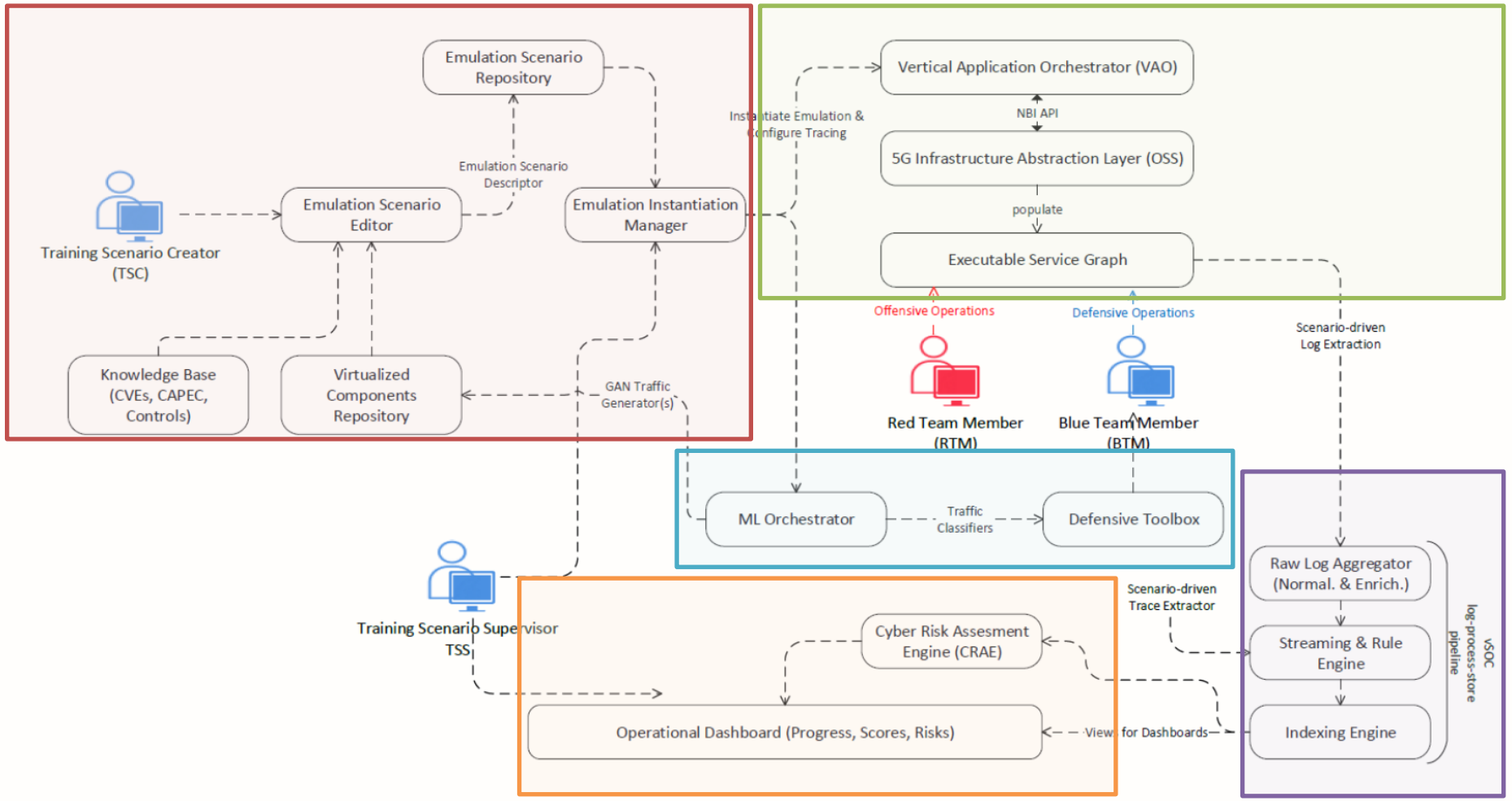
The need for a Cyber range 5G



Identified stakeholders

- Mobile network operators
- ICT providers
- CERTs/CSIRTs
- Cyber Training Firms
- Cyber insurances
- Cyber and 5G Regulators
- Academics & Researchers
- Governments (MoDs, MoIs)
- Vertical Service Operators
- General public

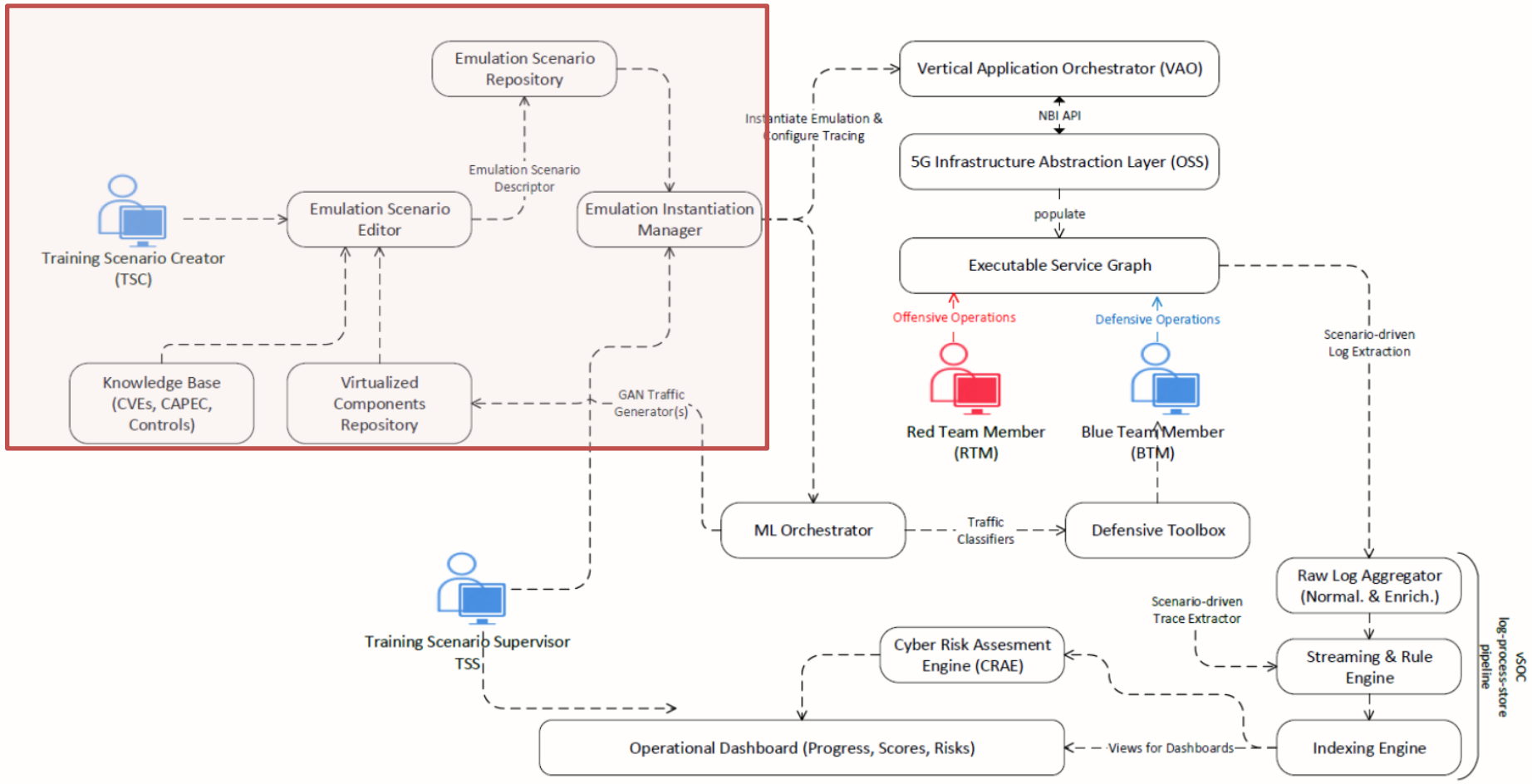
SPIDER Architecture (condensed)



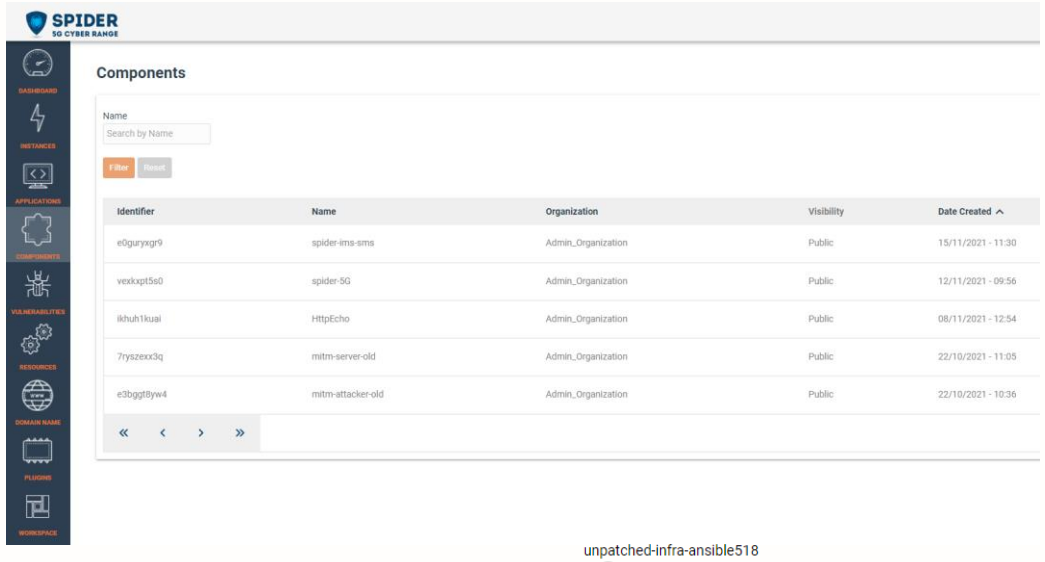
- 4 learning modalities
  - Theoretical quizzes
  - **Hands-on (emulation)**
  - Simulation
  - Serious games

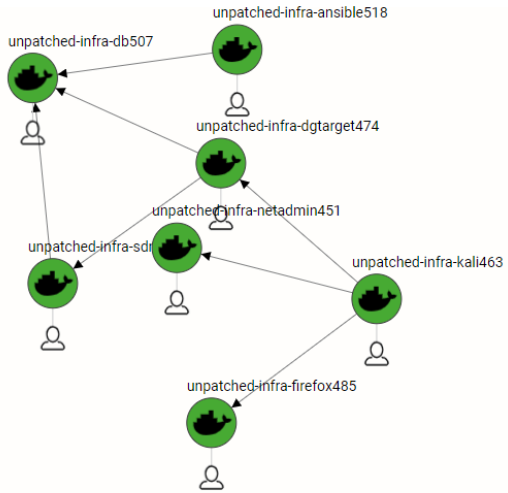
- For the full architecture go here: https://go.gliffy.com/go/publish/13219314

Scenario Definition



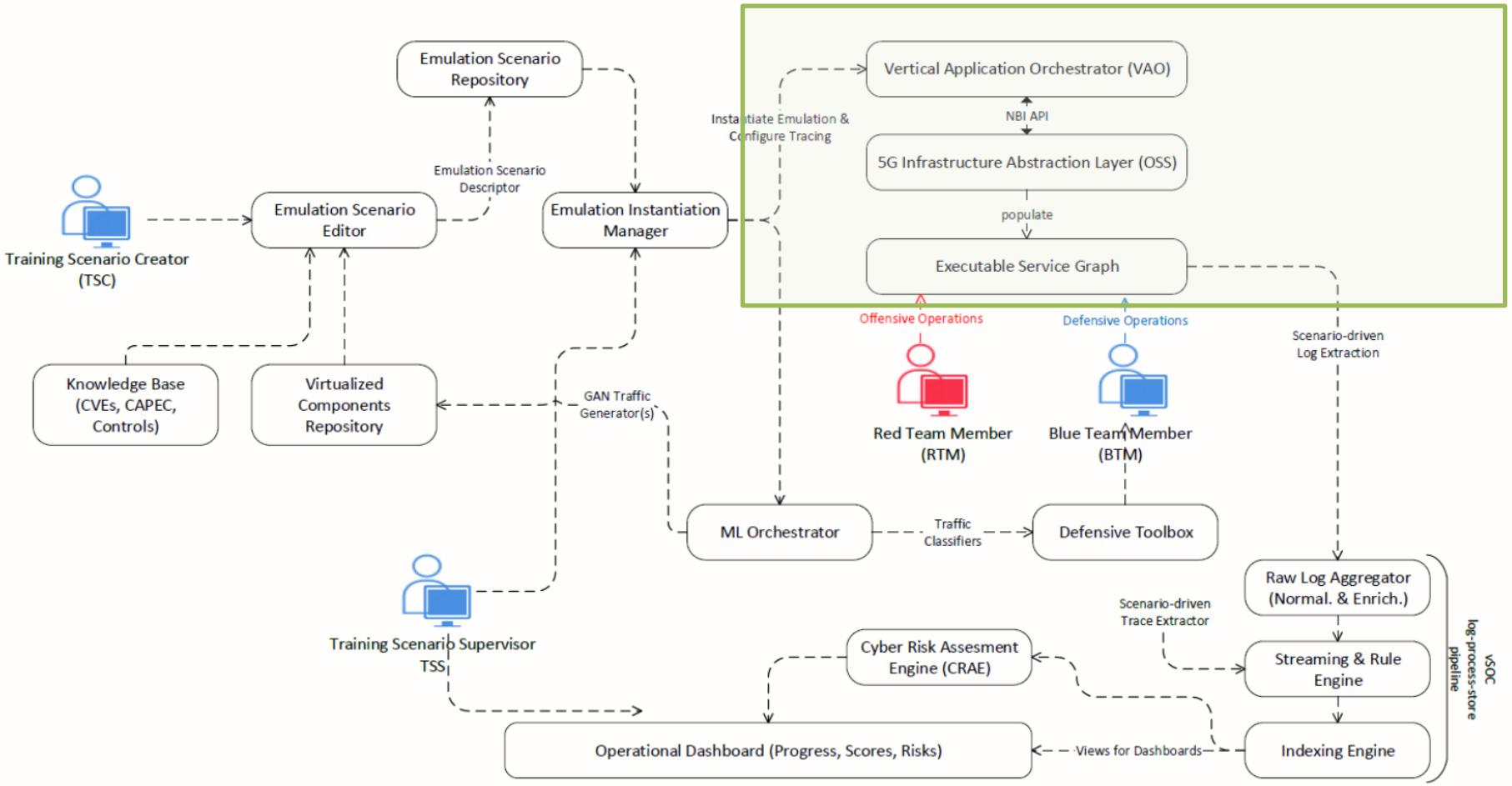
Scenario Definition





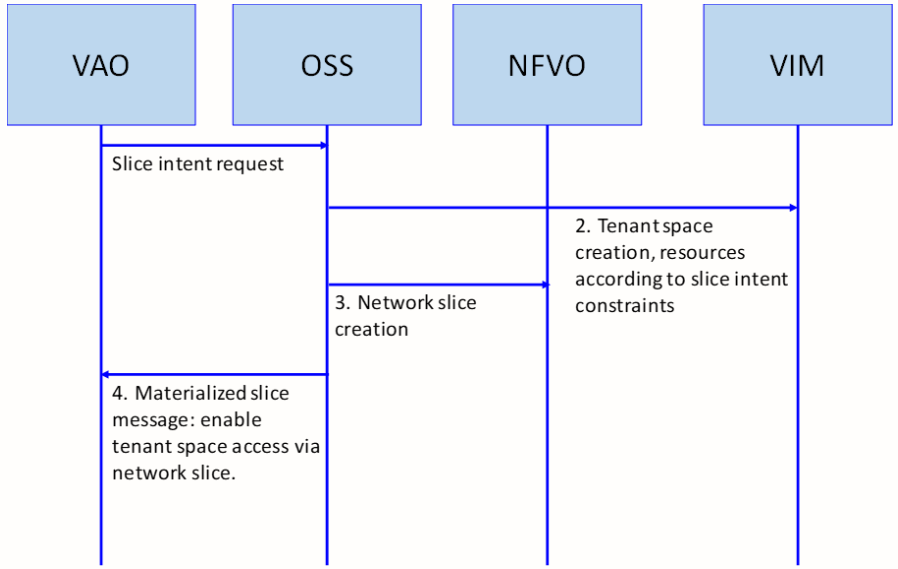
- Select the assets
  - VNFs, PNFs, UEs, vertical applications stored in a specific repository
- Select the vulnerabilities of
  - Ranked by CVSS
- Create a Directed Acyclic Graph (DAG) with drag and drop GUI
- Expose it as Emulation Scenario Descriptor in JSON
  - Stored in a scenario repository

Management and Orchestration

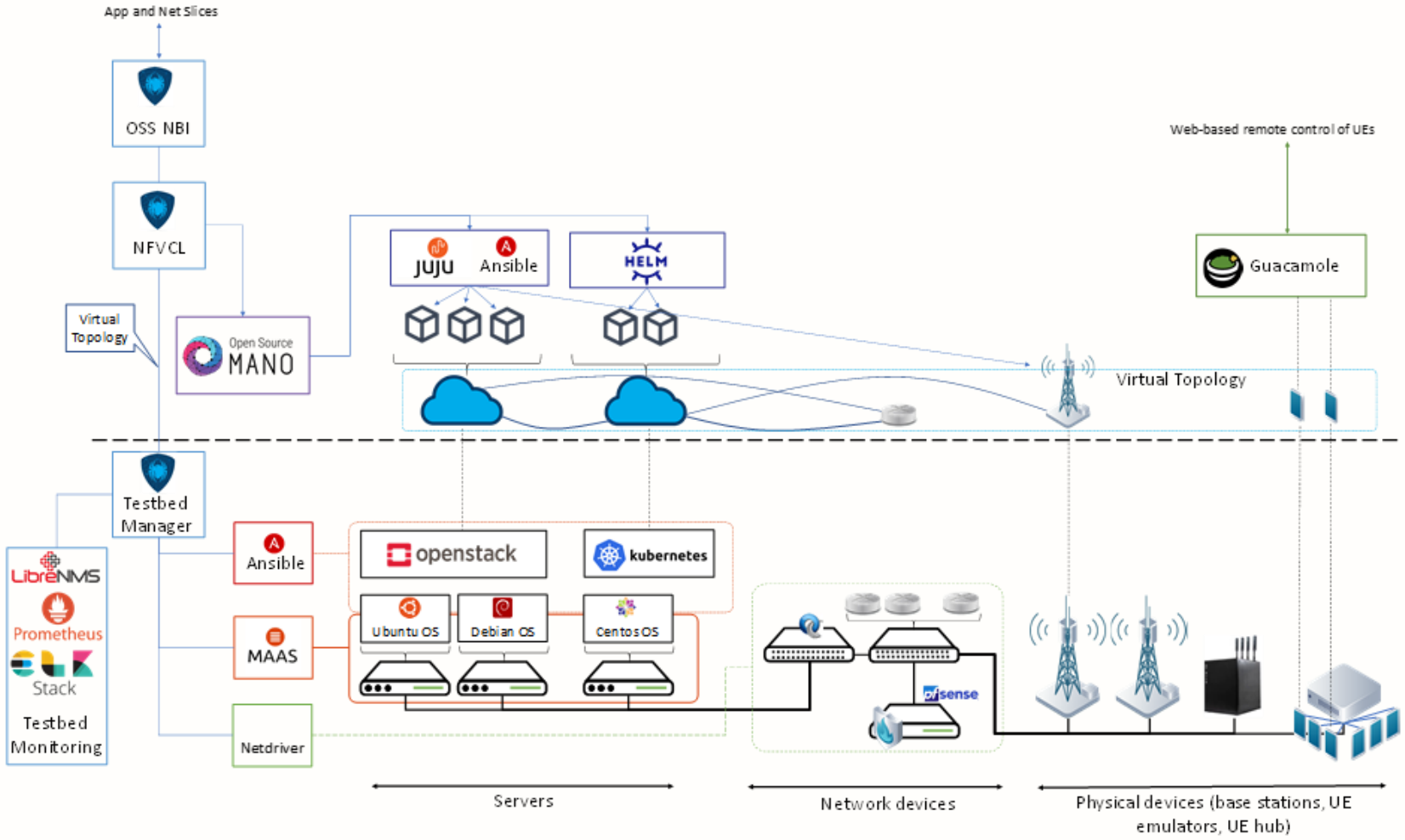


Management and Orchestration

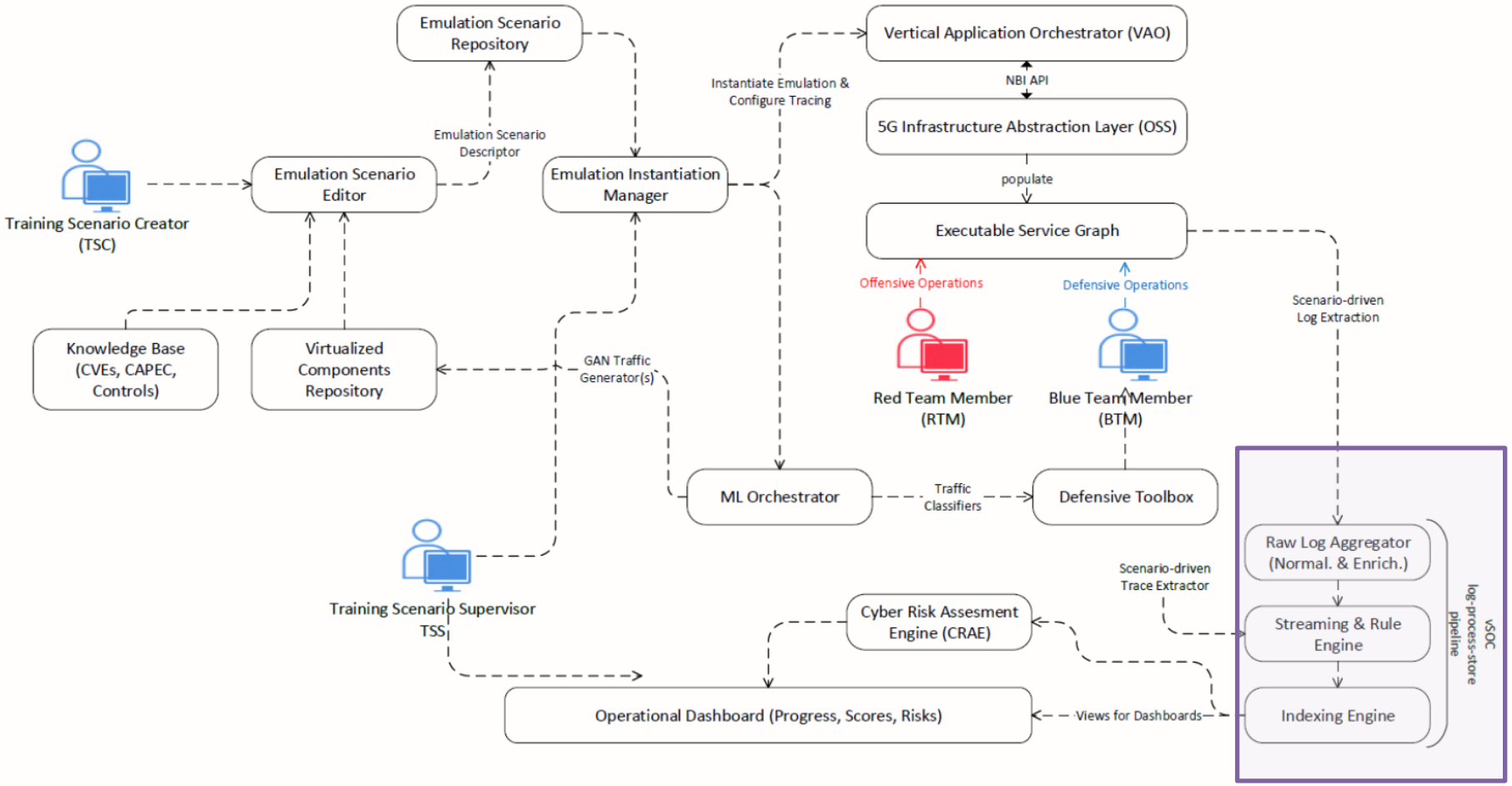
- From the Scenario Request to the Executable Service Graph
- Choreography between the OSS and the VAO
  - 5G infra and vertical apps are managed by independent entities
  - VAO in charge of setting up vertical apps and requesting a slice through a slice intent (JSON) via the NBI
  - OSS in charge of materializing the slice
- Day 2 operations key for the cyber range configuration
  - Programmable log extraction shippers based on eBPF and Beats
  - Scenario related
  - Configured through specific Ansible and charms



Reference implementation

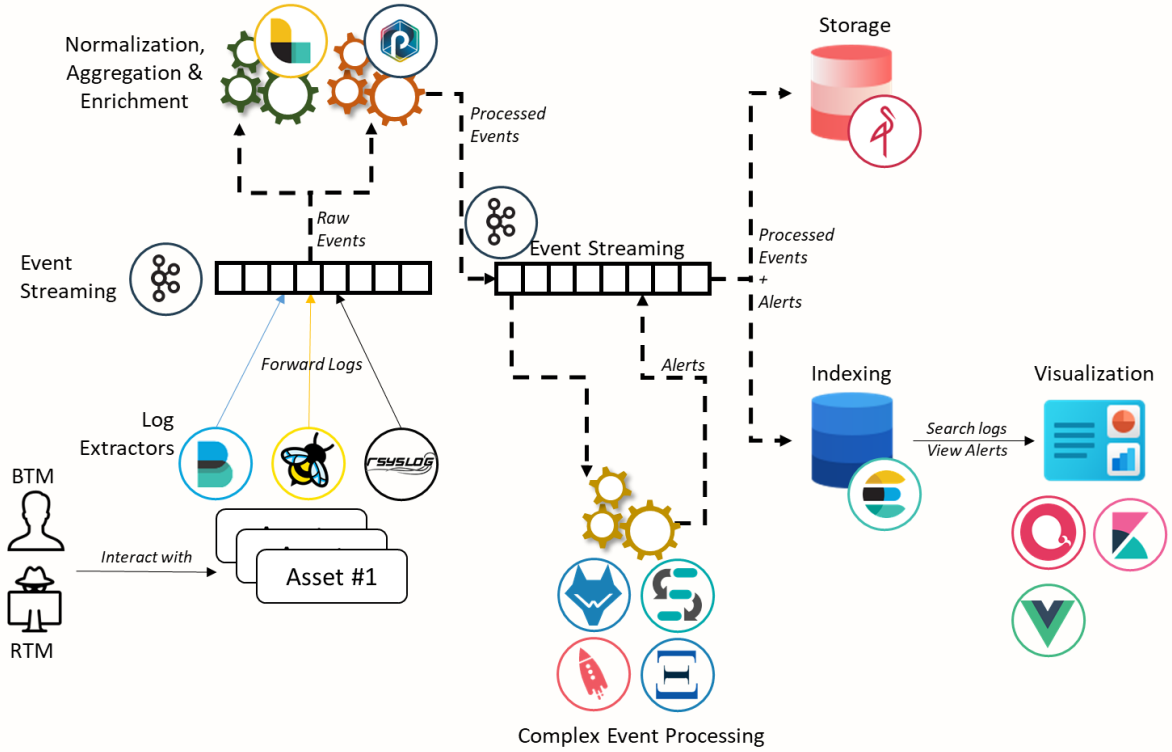


Virtual SOC

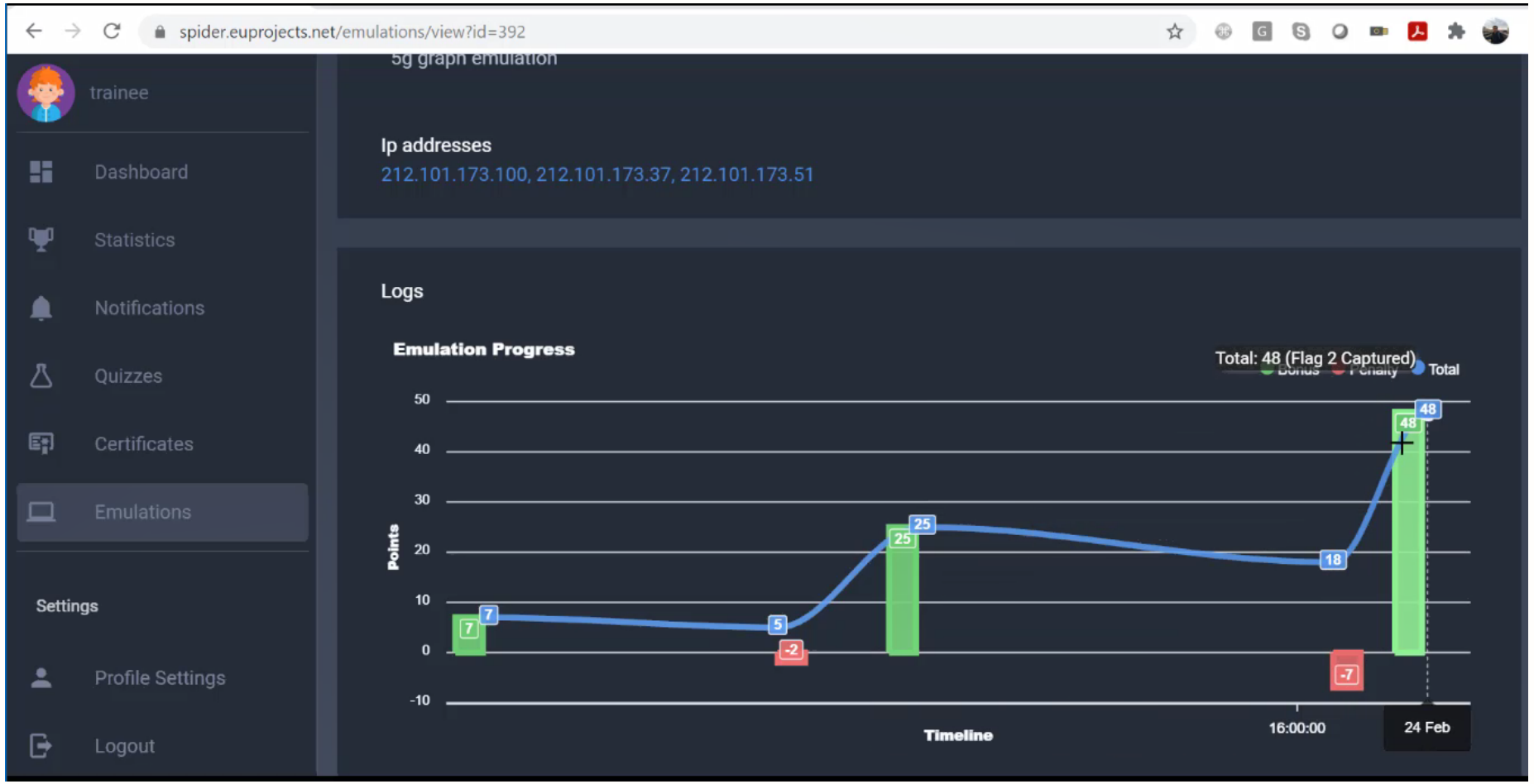

Emulation Scenario Repository
Vertical Application Orchestrator (VAO)
Instantiate Emulation & Configure Tracing
NBI API
5G Infrastructure Abstraction Layer (OSS)
Emulation Scenario Descriptor
Training Scenario Creator (TSC)
Emulation Scenario Editor
Emulation Instantiation Manager
populate
Executable Service Graph
Offensive Operations
Defensive Operations
Scenario-driven Log Extraction
Knowledge Base (CVEs, CAPEC, Controls)
Virtualized Components Repository
GAN Traffic Generator(s)
Red Team Member (RTM)
Blue Team Member (BTM)
ML Orchestrator
Traffic Classifiers
Defensive Toolbox
Raw Log Aggregator (Normal. & Enrich.)
Scenario-driven Trace Extractor
Training Scenario Supervisor TSS
Cyber Risk Assesment Engine (CRAE)
Streaming & Rule Engine
vSOC log-process-store pipeline
Indexing Engine
Operational Dashboard (Progress, Scores, Risks)
Views for Dashboards

Virtual SOC

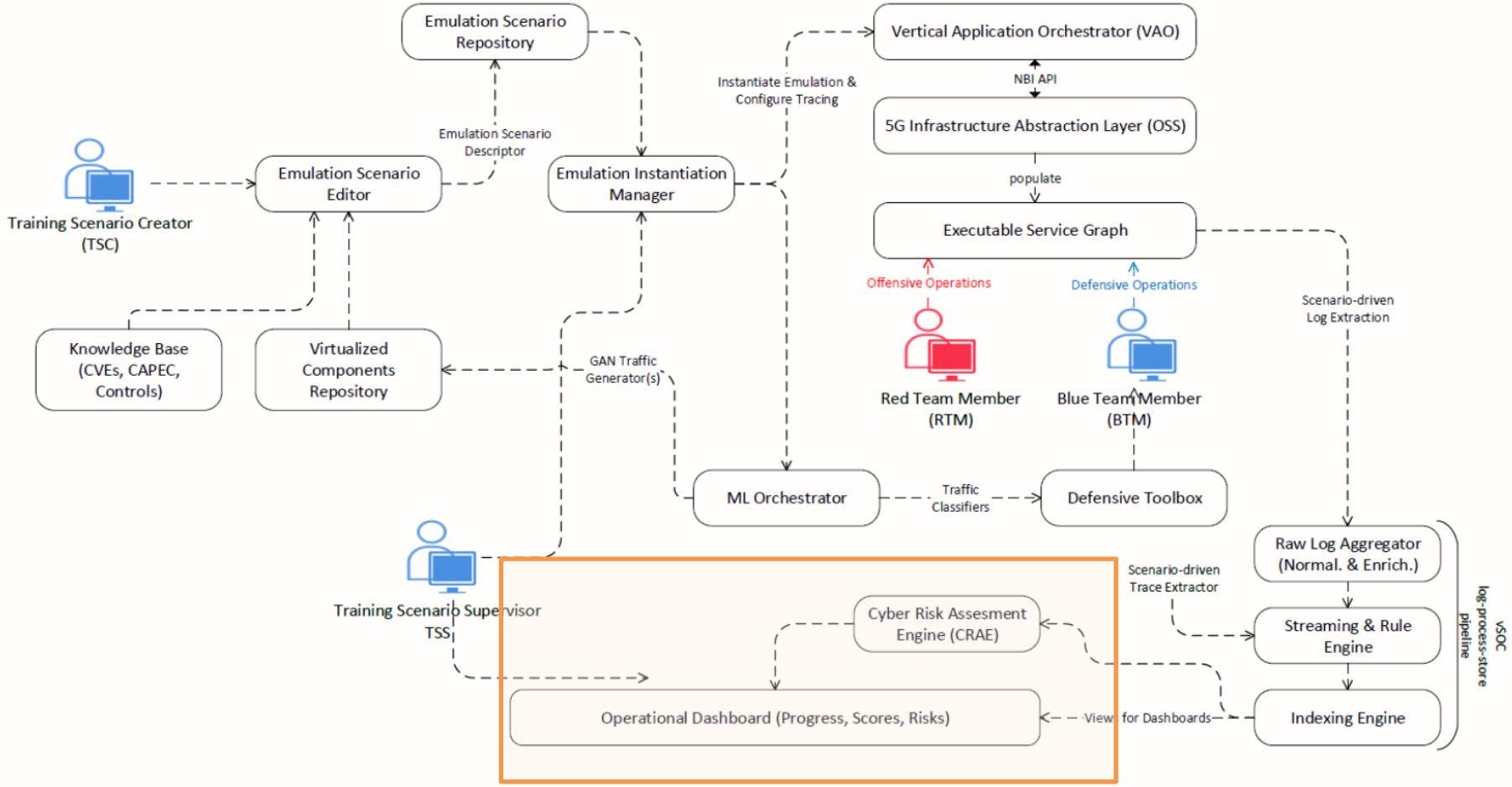
- Performance inference through log analysis (events, actions)
  - Has learning value
  - No trainer intervention required
  - Require a log-process-store data analysis pipeline
- Trace extractor configuration added to the Emulation Scenario Descriptor
  - Match action rules in CEP language



Trainer dashboard



Cyber Risk Assesment

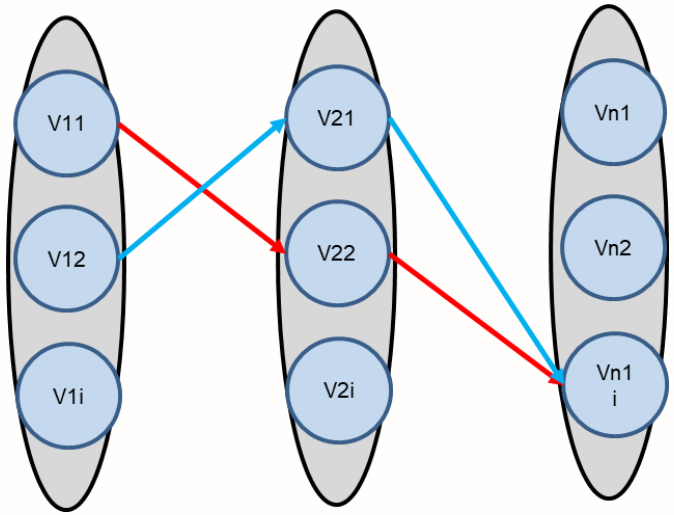


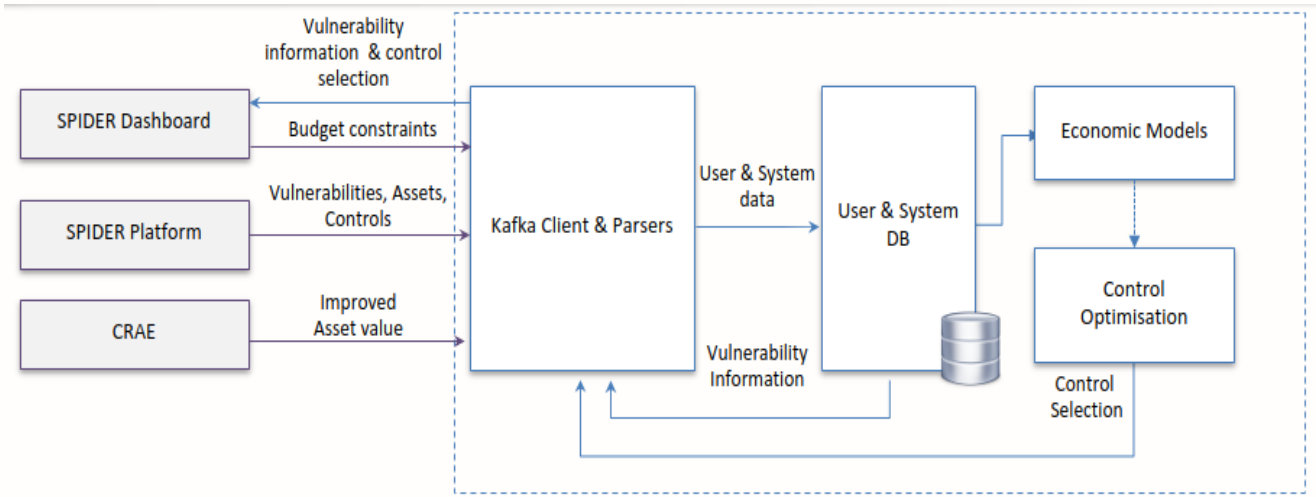
Cyber risk assessment

- Calculation of the economic Cyber risk exposure of a 5G infrastructure
  - Based on the CORAS model, based on ISO 27005
    - Graphic model of relationships among threats, vulnerabilities, incidents, assets, indicators, and mitigations, as well as the existing relations among them
  - Typically done statically
  - Allow a quantitative evaluation of the impact of the measures and the actions taken by trainees in real time.
    - From score to $$$

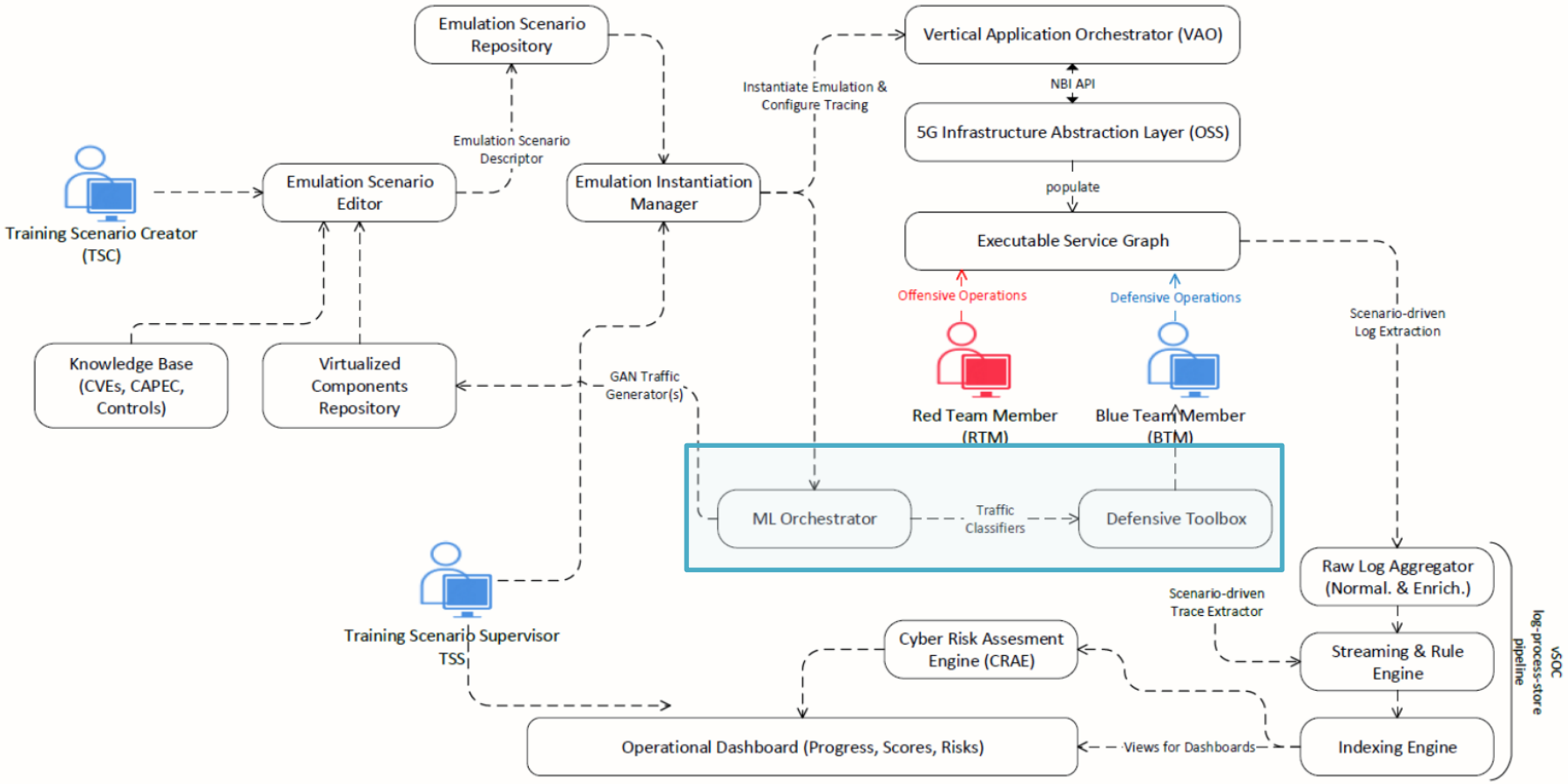
Calculation Model

- When Assets are connected model is bound to the Direct Acyclic Graph
  - Individual Risk Level IRL
  - Propagated/Cumulative Risk Level PRL/CRL
- Both PRL and CRL are dependent to Attack Paths





Synthetic Attack Generation



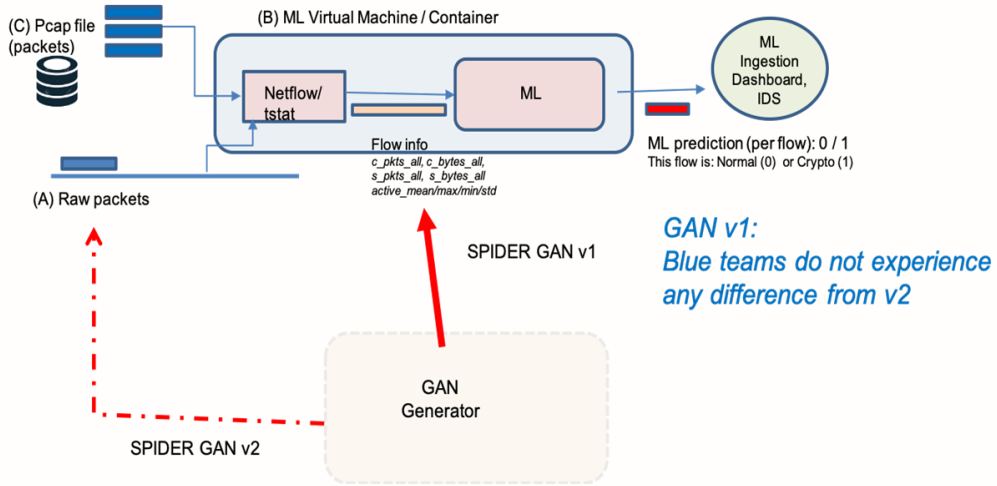
Synthetic attack generation

- Offer automated offensive synthetic traffic to test/train detection mechanisms for cyber attack
- Based on Generative Adversarial Network (GAN) for data generation
- Common issues:
  - Lack of labelled data for supervised ML
  - Data privacy / legal regulations
  - Reduced need for a Red Team

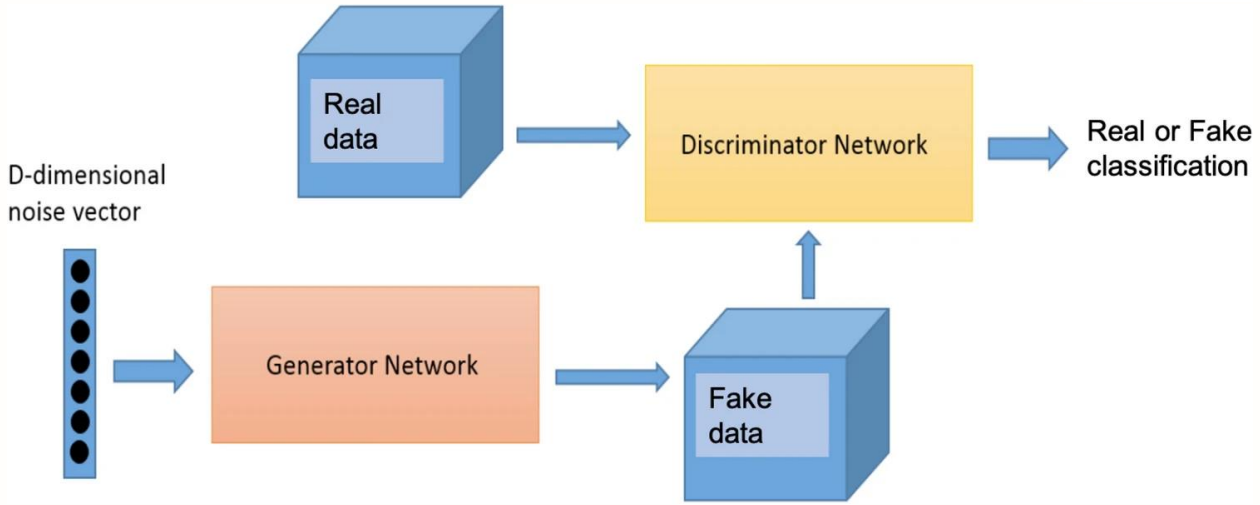
Telecom/Cybersecurity industry requires novel methods to generate labelled data sets

GAN integration in SPIDER

- ML integration (detectors)
  + evaluation in 5G environment
  - Real traffic: Encrypted traffic, DDoS
  - Synthetic traffic: Encrypted traffic Botnet



GAN v1:
Blue teams do not experience any difference from v2



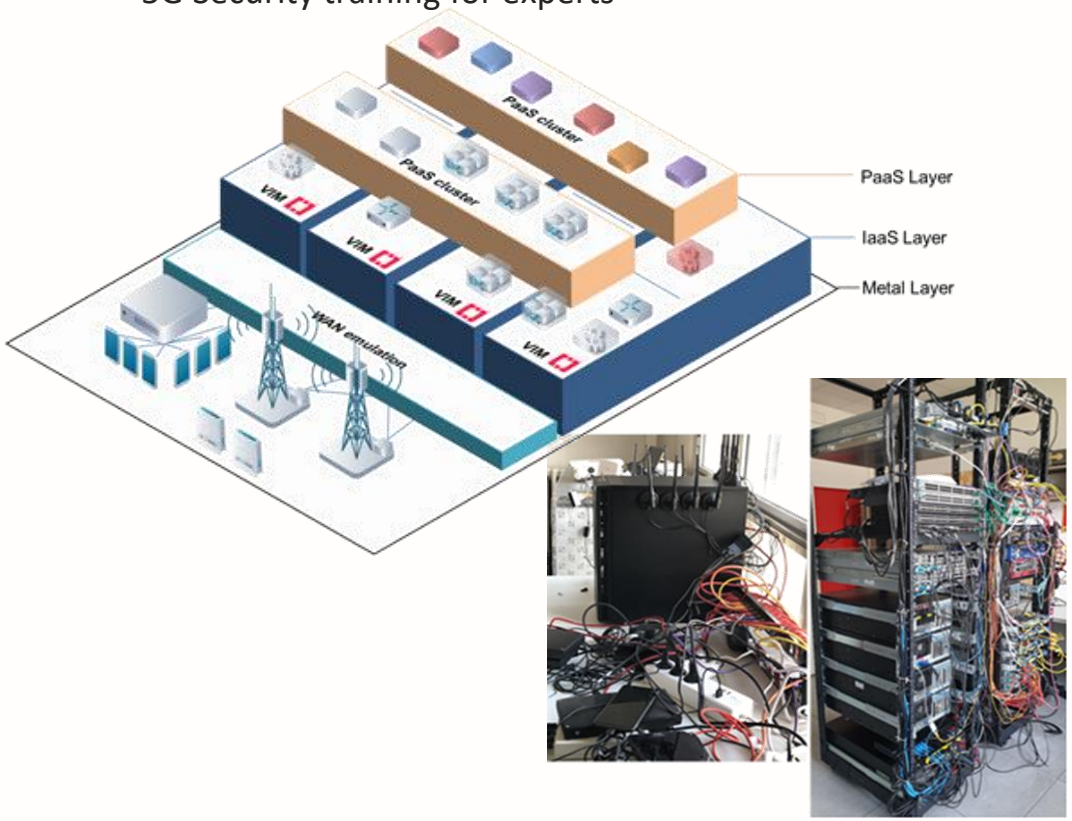
- *Wasserstein GAN + GC/GP: to optimize convergence.*
- *One GAN per type of traffic*
- *Custom activation functions at the last layer of Generator to bend data distribution*
- *Rich set of hyperparameters*
- *Design of 2 novel **distance functions** to **measure the similarity of synthetic vs real data** (L1 and Jaccard index)*

Mozo, A., González-Prieto, Á., Pastor, A. *et al. Synthetic flow-based cryptomining attack generation through Generative Adversarial Networks. Sci Rep* **12**, 2091 (2022). https://doi.org/10.1038/s41598-022-06057-2

Testbeds

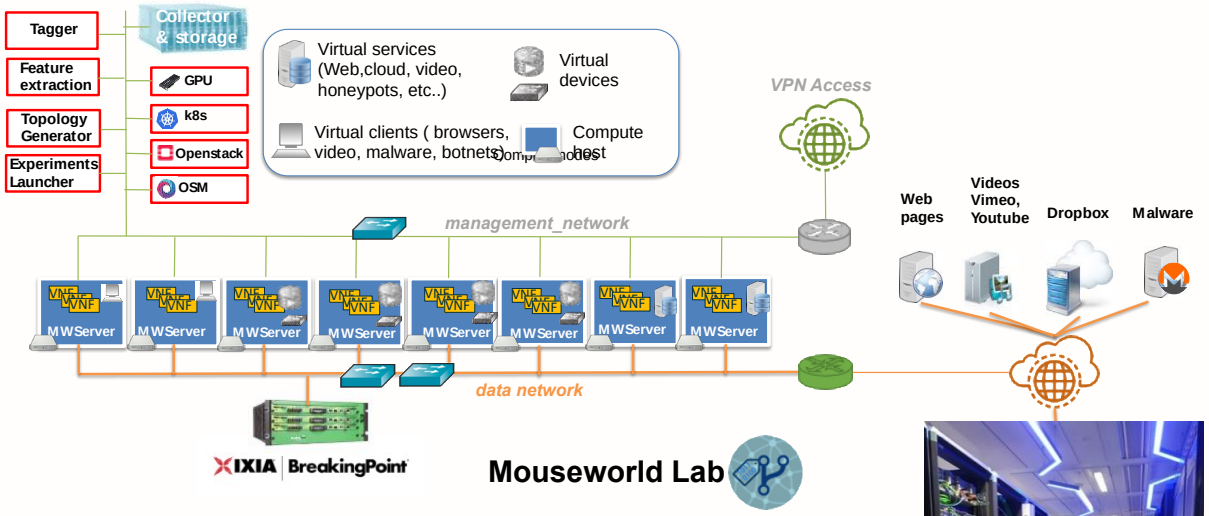
MATILDA (Genoa – Italy)

- Cybersecurity testing of 5G ready applications and network services
- 5G Security training for experts



MOUSEWORLD (Madrid - Spain)

- Cybersecurity of next generation mobile core SBA



Validation and KPIs

- Validation activities with real users ongoing
  - Pilots
  - CTFs
- Some KPIs
  - Technical (measured)
    - Time required to deploy/undeploy a service graph (OSS-VAO)
    - Supported number of virtualized components per scenario (
    - Delay between action and inference (vSOC)
    - Time required for risk calculation (CRAE)
  - Non-technical (questionnaire)
    - Acceptance
    - Usefulness
    - Ease of use
    - Effectiveness
    - Satisfaction

Conclusion and take away

- Major Achievements
  - Cyber Range as a Service platform targeting the specificities of 5G
  - Modelling and emulating of network services and applications as well as complex cyber-attacks
  - Capabilities for tracking the trainee's activity
  - Integrate cyber range-driven risk analysis and propose econometric modelling tools capable to forecast the economic impact of cyber risks

- Next Steps
  - Finalize pilot validation
  - Open Source

Stable Release

2 complementary environments

- spider.euprojects.net := Educational environment
- spider-os.euprojects.net := Administration environment

SPIDER
5G CYBER RANGE

ERICSSON cnit Telefonica THALES Atos UBITECH ubiquitous solutions

POLITÉCNICA FONDAZIONE BRUNO KESSLER uni.systems 8 Bells FORTH INSTITUTE OF COMPUTER SCIENCE SERIOUS GAMES INTERACTIVE UNIVERSITY OF PIRAEUS

CITY UNIVERSITY LONDON EXALENS® infalia InfoCom Sphynx Technology Solutions KEY

Thank you

https://spider-h2020.eu

SPIDER.H2020

@spiderh2020_eu

spider-h2020-funded-project/