SPIDER

a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

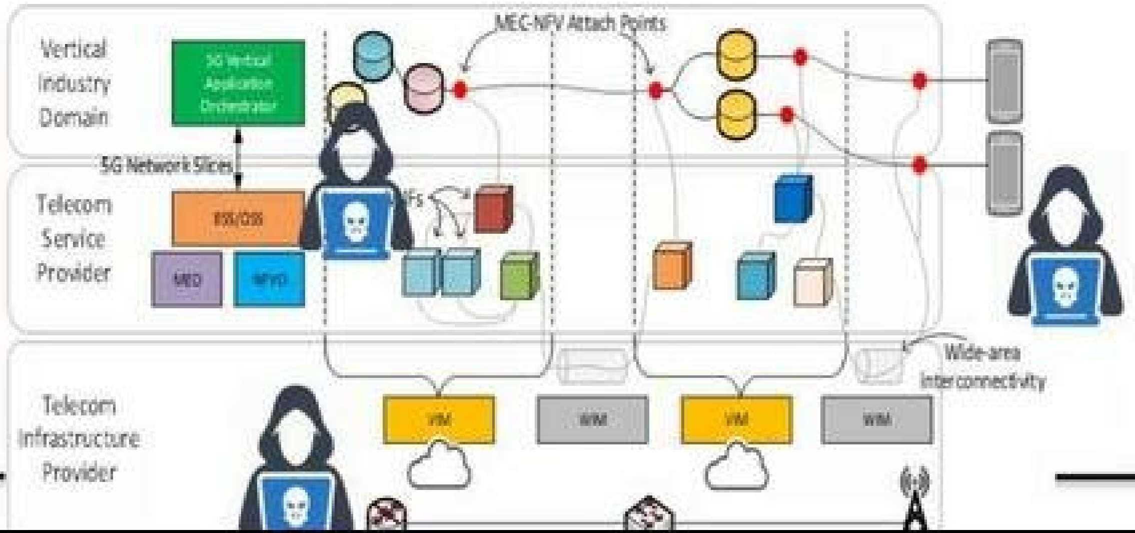
Thursday 26 November 2020

The challenge

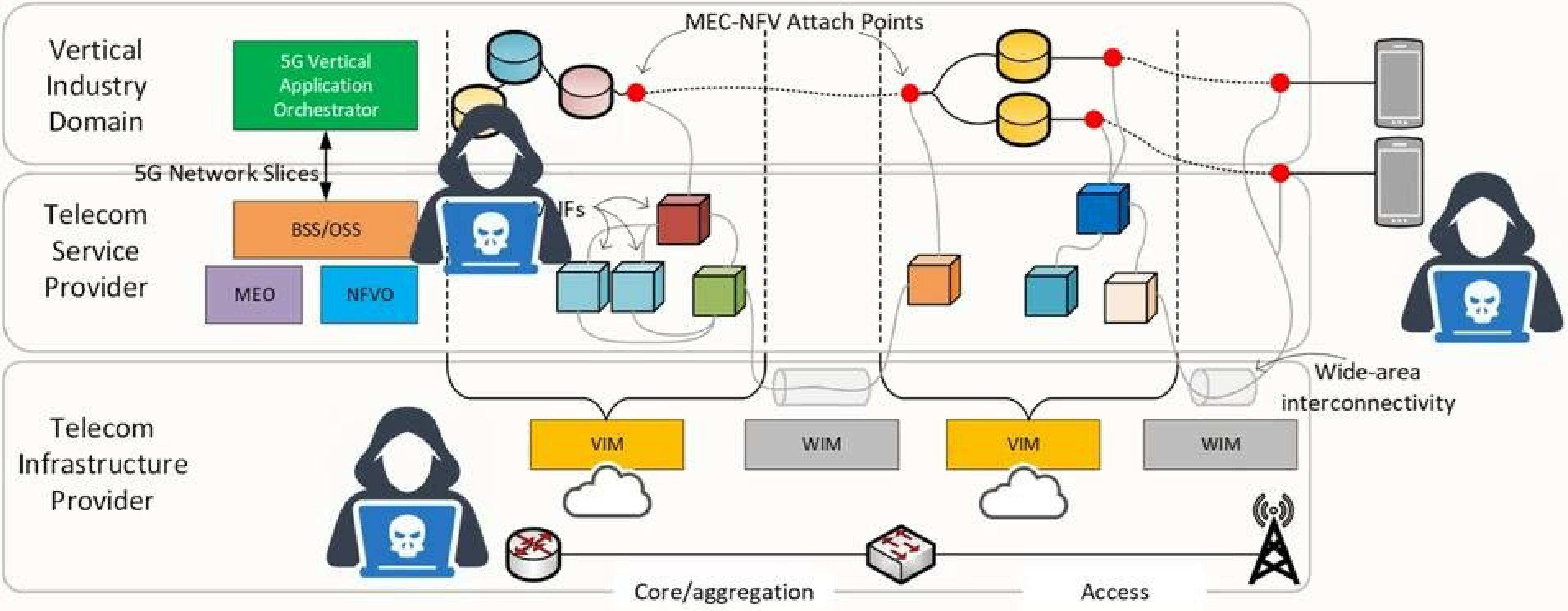
- The emergence of 5G architecture **raised radical changes** in the telco domain
- The **slicing** concept and the **virtualization** of all layers established a **completely new landscape** for both **operators** and application **developers**
- The ‘new operational landscape’ contributes in the **increase of cyber attack surface**
- 5G incorporates many advanced technologies (e.g. SDN, NFV, SDR, Virtualization) each of which **exposes its own attack surface**

The complexity of today’s cybersecurity landscape emphasises the need for **highly competent experts** in securing critical multi-tenant and multi-service environments, such as 5G mobile networks.

5G Threat Landscape



5G Threat Landscape



Concept and approach

Innovative **Cyber Range as a Service platform** that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges with

- latest technologies in **telecommunications management** and **emulation**

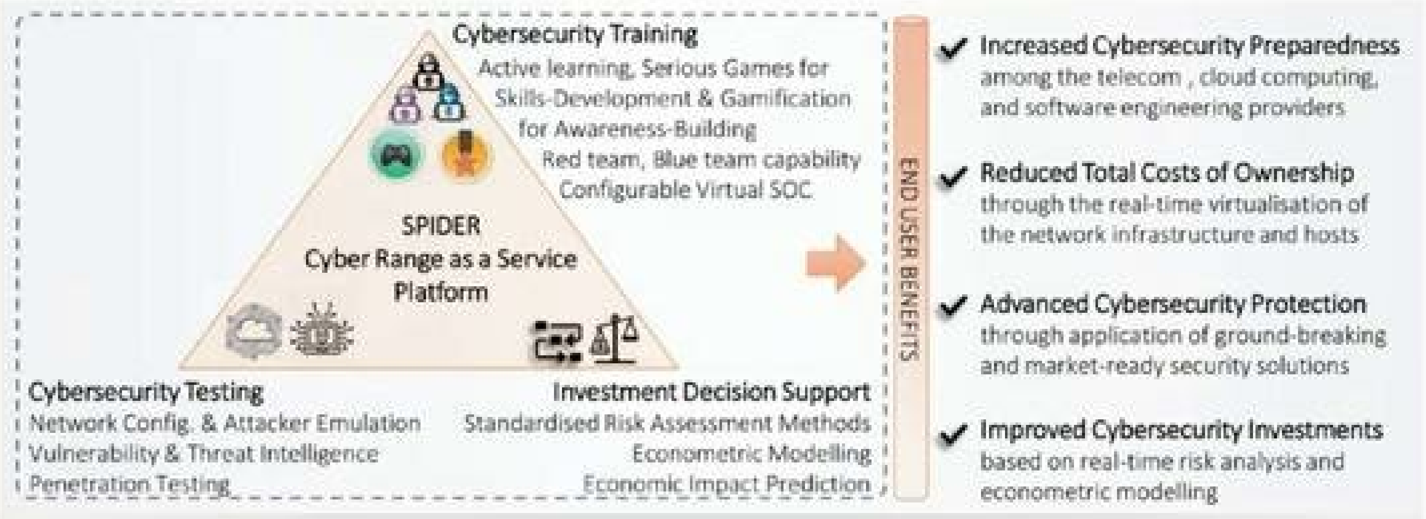
- cyber security training through **gamification and serious games**

- tools for analysing the **economics of cybersecurity solutions**

Uniquely virtualises as **a single and easily accessible solution**

Three major pillars:

- **cybersecurity testing and assessment**, with emphasis on new security technologies;
- **cybersecurity training** in defending against advanced cyber-attacks; and
- **cybersecurity investment decision support**.



Cybersecurity Training
Active learning, Serious Games for Skills-Development & Gamification for Awareness-Building
Red team, Blue team capability
Configurable Virtual SOC

SPIDER
Cyber Range as a Service Platform

Cybersecurity Testing
Network Config. & Attacker Emulation
Vulnerability & Threat Intelligence
Penetration Testing

Investment Decision Support
Standardised Risk Assessment Methods
Econometric Modelling
Economic Impact Prediction

END USER BENEFITS

✓ Increased Cybersecurity Preparedness among the telecom , cloud computing, and software engineering providers

✓ Reduced Total Costs of Ownership through the real-time virtualisation of the network infrastructure and hosts

✓ Advanced Cybersecurity Protection through application of ground-breaking and market-ready security solutions

✓ Improved Cybersecurity Investments based on real-time risk analysis and econometric modelling

Project Information

SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

H2020 Project - Work Programme 2018-2020

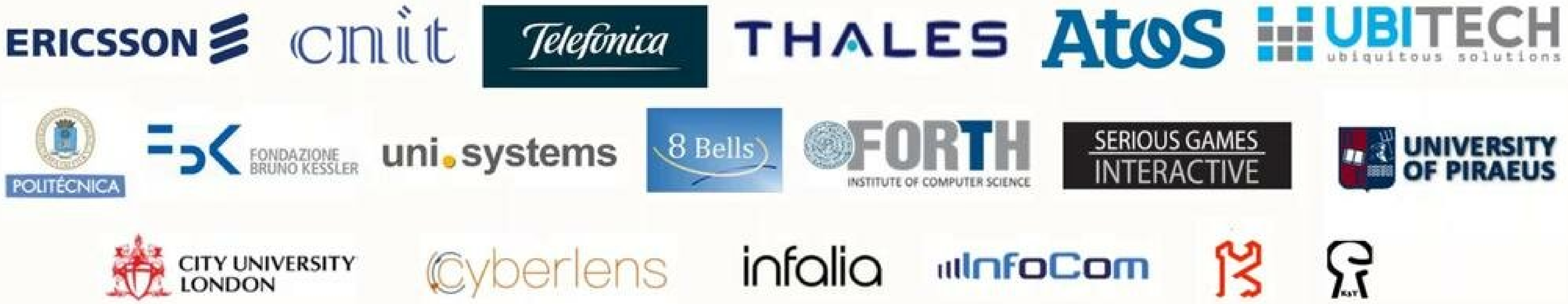
- **Secure societies - Protecting freedom and security of Europe and its citizens**

Call: H2020-SU-DS-2018

- **Topic**: SU-DS01-2018 Cybersecurity preparedness - cyber range, simulation and economics

Duration: 1 July 2019 - 30 June 2022

The Consortium



19 partners from **9 European countries** (high diversity)

- 5 x Large Industries
- 6 x Research Institutes and Universities
- 8 x SMEs

Goals / Objectives of SPIDER

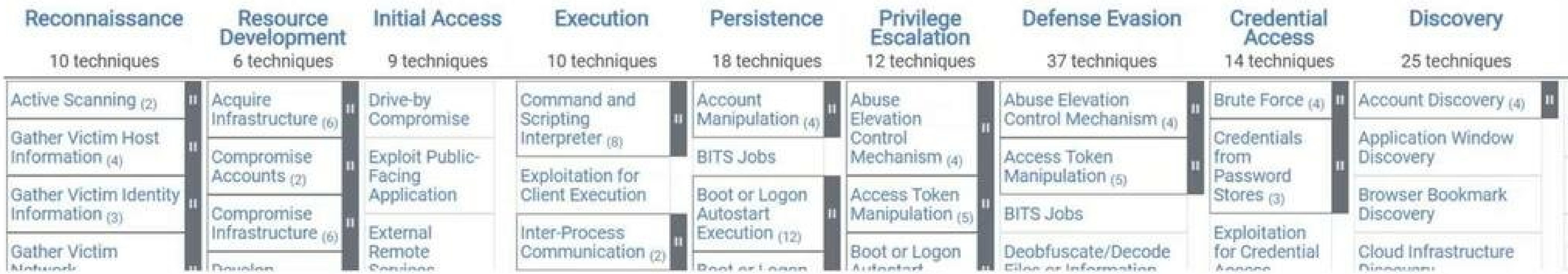
- To **develop** a **Cyber Range as a Service platform** targeting the specifies of **5G infrastructure**
- To **realize** an engine capable of **modelling and emulating** network **services** and **applications** as well as **complex cyber-attacks**
- To **provide active learning strategies** towards increasing the **cybersecurity skills** and **awareness** of **modern cyber defenders**
- To **implement** capabilities for **tracking** the **trainee's activity**
- To **integrate cyber range-driven risk analysis** and **propose econometric modelling tools** capable to forecast the **economic impact of cyber risks**

Target end users & Modalities

- Distinct **Value Proposition** for:
  - **Training Scenario Creators**
  - **Red Team Members**
  - **Blue Team Members**
  - **Infrastructure Providers**
  - **Risk Auditors**
- **Modalities:**
  - **Modality 1: Theoretical Training**
  - **Modality 2: Hands-on Training**
  - **Modality 3: Simulation**

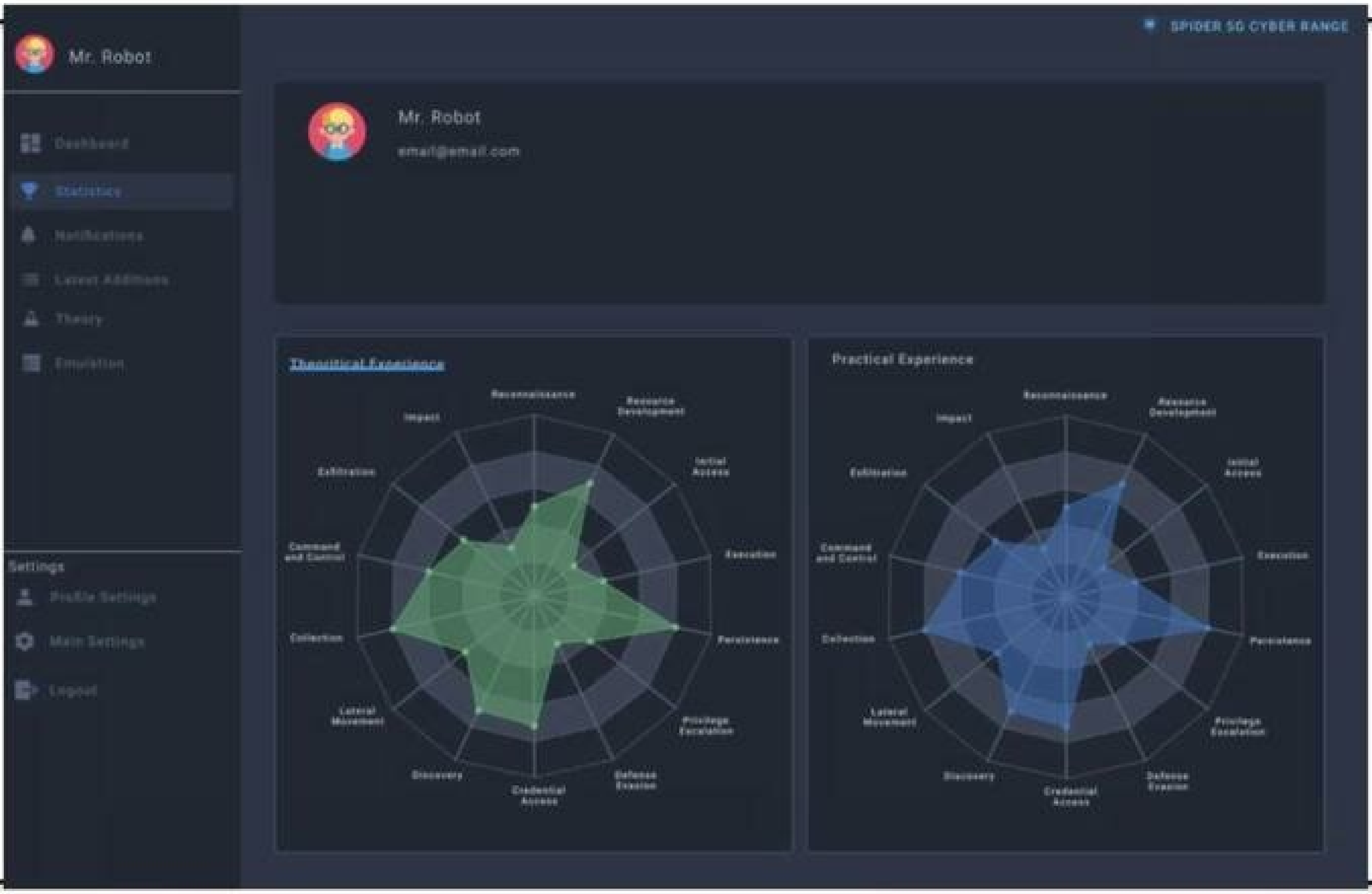
Modality 1: Theoretical Training

- **Goal**: Leverage the theoretical background of trainees
- **Medium** : Interactive Tests that aim to infer the level of the trainee regarding Hacking Tactics and Techniques
- **Model-Adherence**: MITRE ATT&CK



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery
Gather Victim Network	Develop			Boot or Logon		Deobfuscate/Decode Files or Information		Cloud Infrastructure Discovery

Theoretical / Pracitcal Skill Level



Mr. Robot

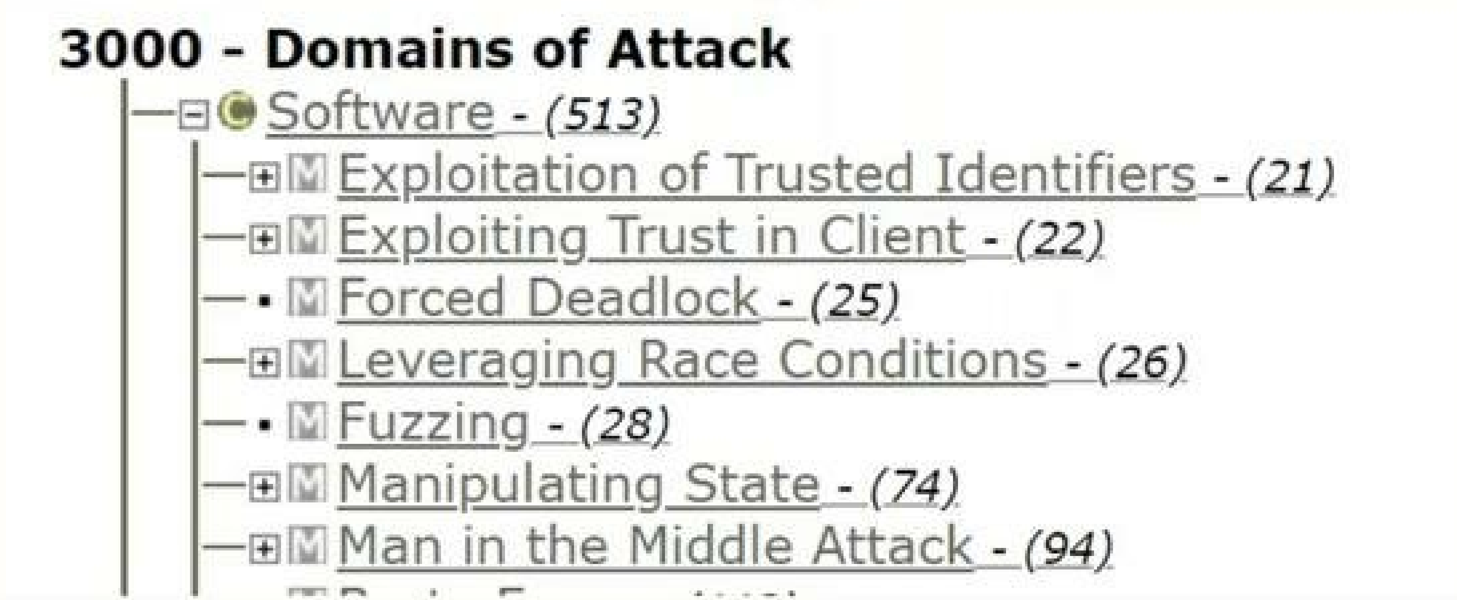
email@email.com

Theoretical Experience

Practical Experience

Modality 2: Hands-on Training

- **Goal**: Leverage the practical skills of trainees
- **Medium** : Setup of a Virtual Infrastructure that covers 5G assets
- **Model-Adherence**: MITRE CAPEC

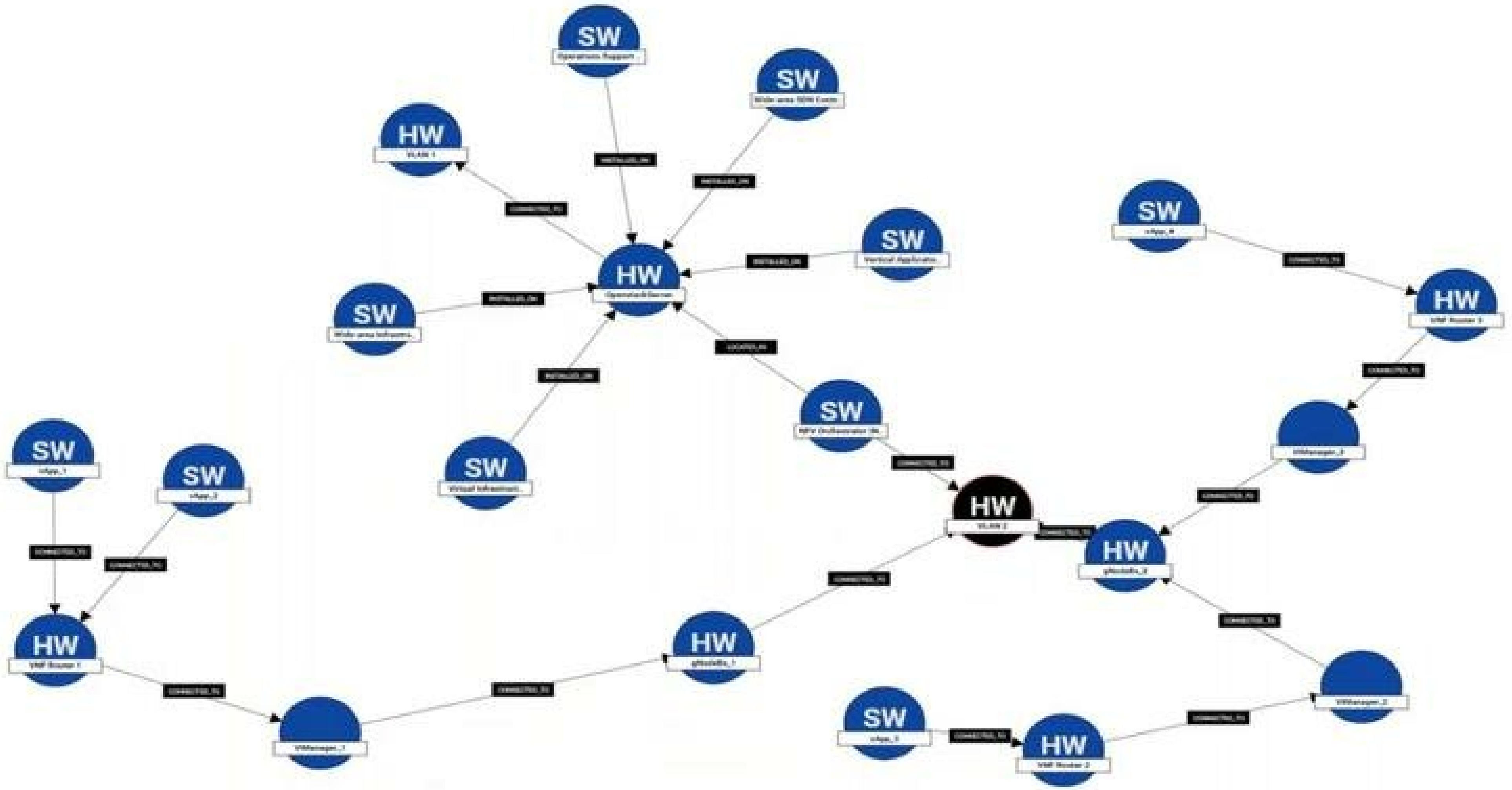


3000 - Domains of Attack

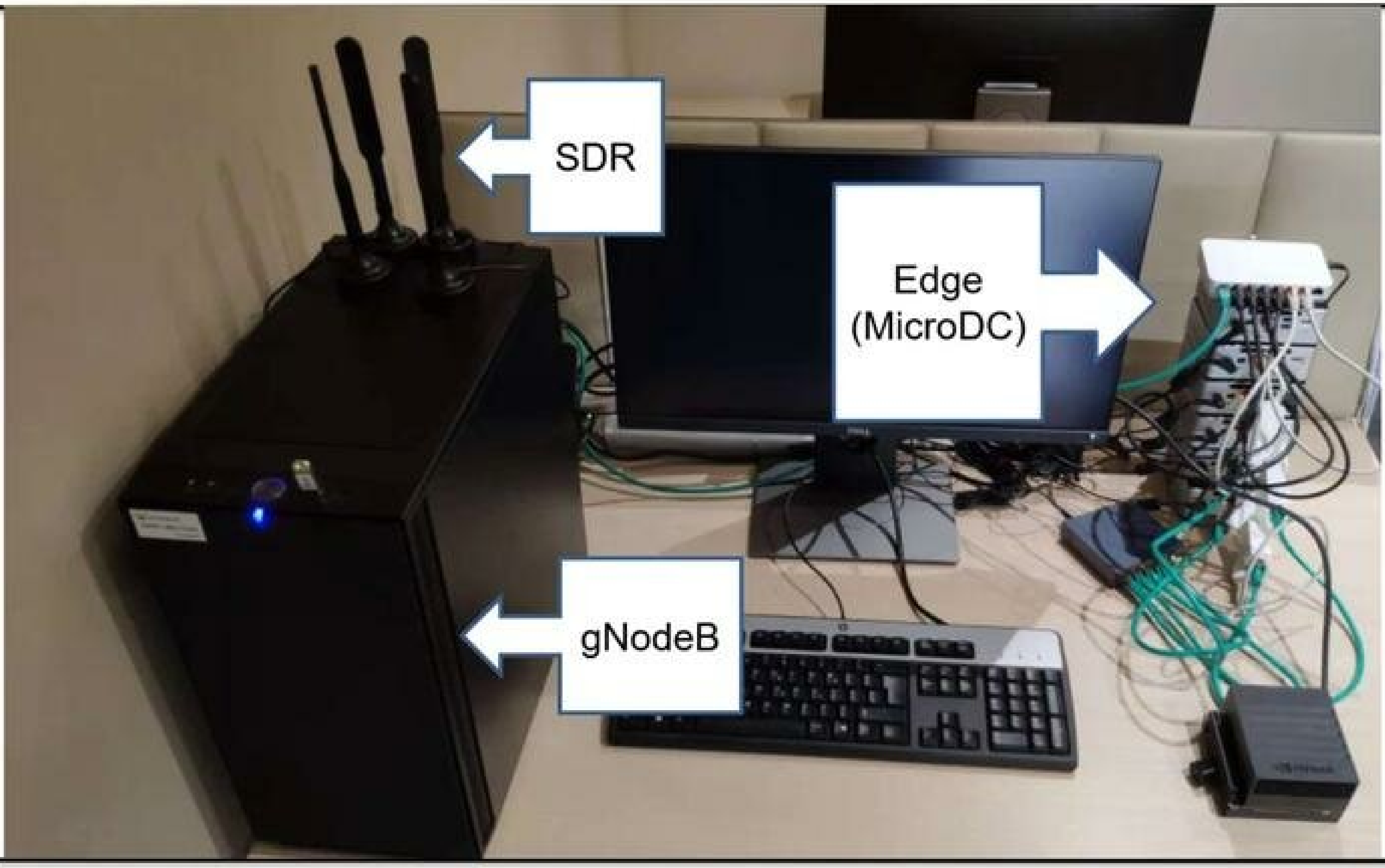
- ⊟ Software - *(513)*
  - ⊞ Exploitation of Trusted Identifiers - *(21)*
  - ⊞ Exploiting Trust in Client - *(22)*
  - ▪ Forced Deadlock - *(25)*
  - ⊞ Leveraging Race Conditions - *(26)*
  - ▪ Fuzzing - *(28)*
  - ⊞ Manipulating State - *(74)*
  - ⊞ Man in the Middle Attack - *(94)*

Example Instantiated Topology

SPIDER
5G CYBER RANGE

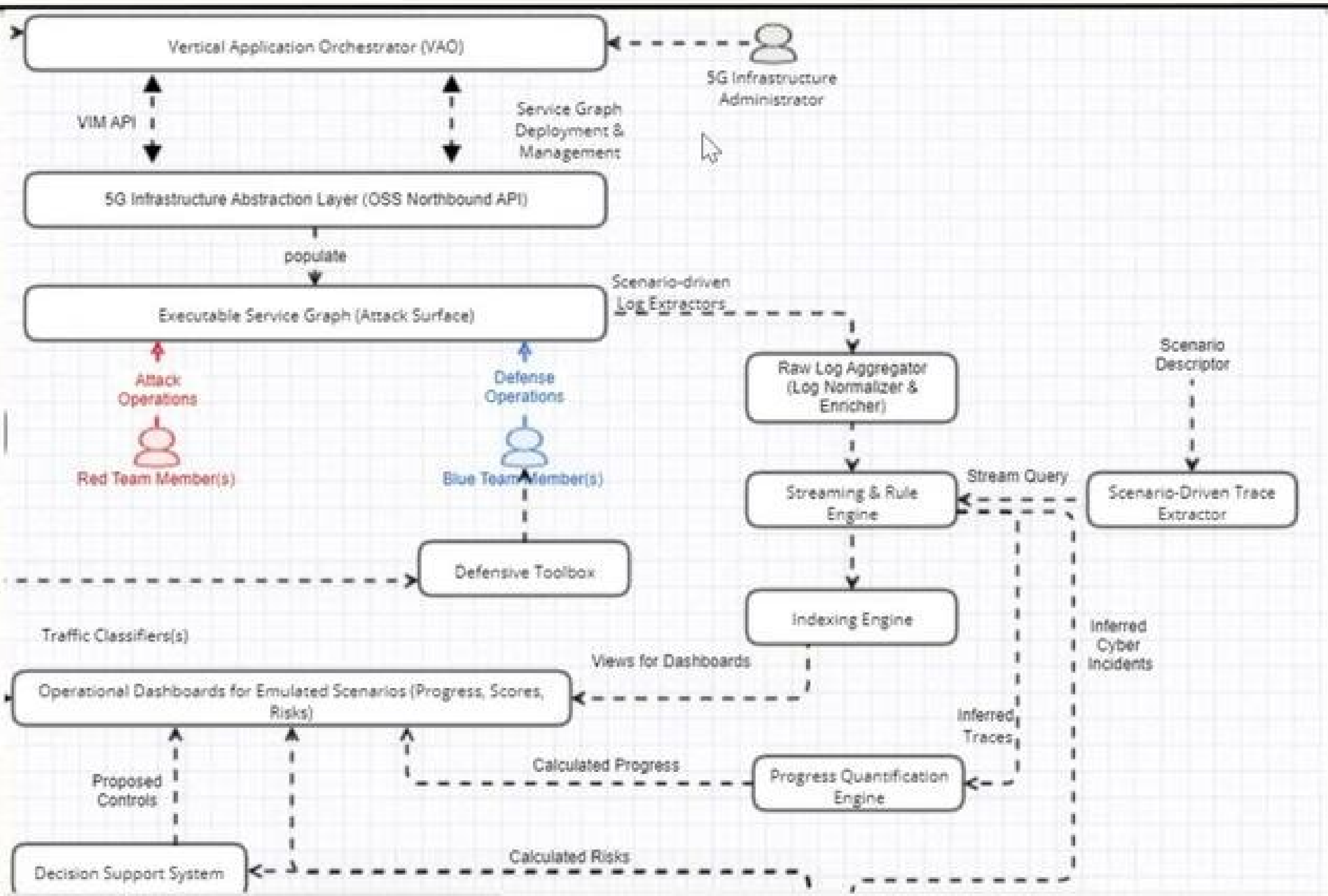


VNFs & PNFs used (4G/5G in a box)



VSOC & Scoring Model

SPIDER
5G CYBER RANGE



Vertical Application Orchestrator (VAO)

5G Infrastructure Administrator

VIM API

Service Graph Deployment & Management

5G Infrastructure Abstraction Layer (OSS Northbound API)

populate

Executable Service Graph (Attack Surface)

Scenario-driven Log Extractors

Attack Operations

Red Team Member(s)

Defense Operations

Blue Team Member(s)

Raw Log Aggregator (Log Normalizer & Enricher)

Scenario Descriptor

Streaming & Rule Engine

Stream Query

Scenario-Driven Trace Extractor

Defensive Toolbox

Indexing Engine

Traffic Classifiers(s)

Views for Dashboards

Inferred Cyber Incidents

Operational Dashboards for Emulated Scenarios (Progress, Scores, Risks)

Inferred Traces

Calculated Progress

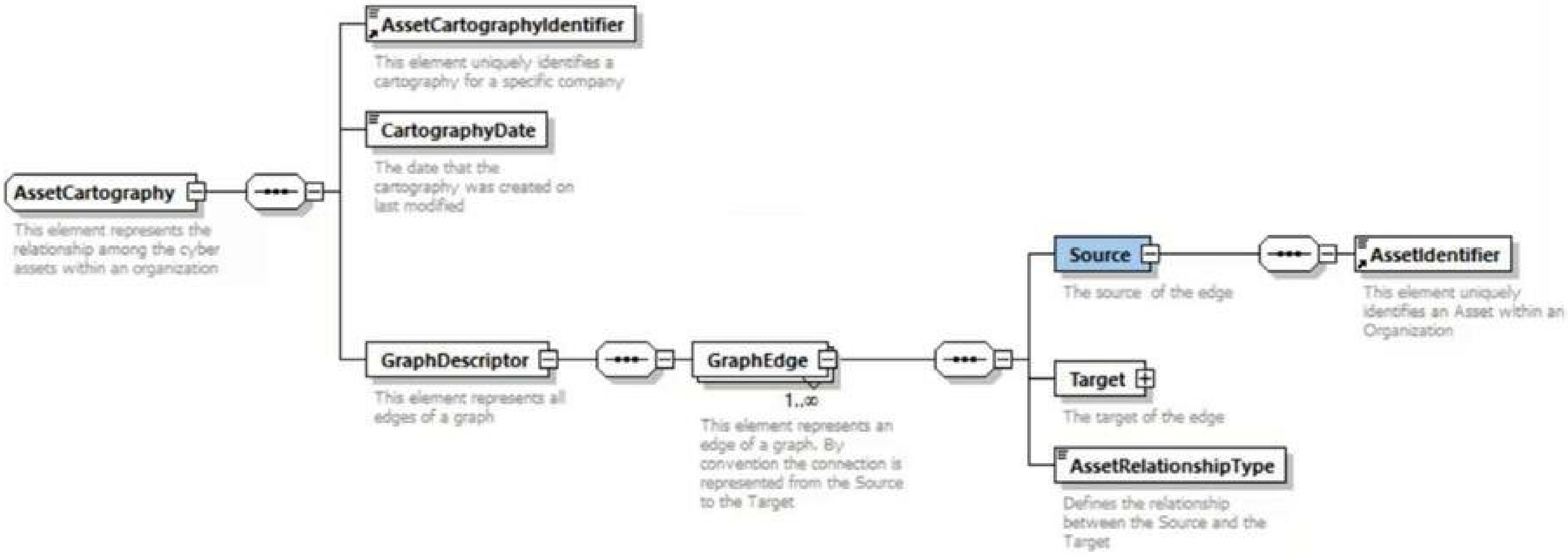
Progress Quantification Engine

Proposed Controls

Calculated Risks

Decision Support System

Normative Models



AssetCartography

This element represents the relationship among the cyber assets within an organization

AssetCartographyIdentifier

This element uniquely identifies a cartography for a specific company

CartographyDate

The date that the cartography was created on last modified

GraphDescriptor

This element represents all edges of a graph

GraphEdge

1..∞

This element represents an edge of a graph. By convention the connection is represented from the Source to the Target

Source

The source of the edge

AssetIdentifier

This element uniquely identifies an Asset within an Organization

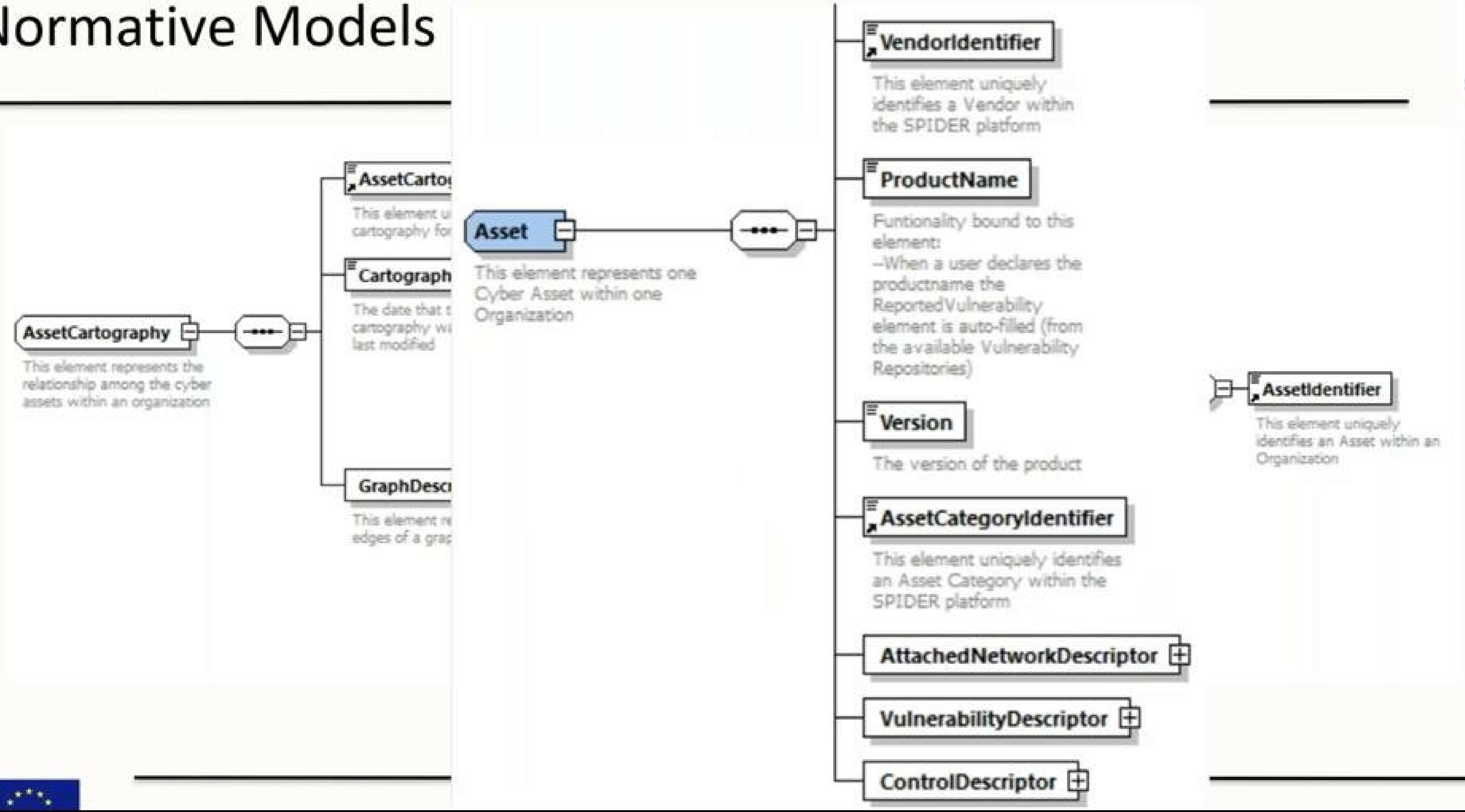
Target

The target of the edge

AssetRelationshipType

Defines the relationship between the Source and the Target

Normative Models



AssetCartography: This element represents the relationship among the cyber assets within an organization

AssetCarto: This element u cartography for

Cartograph: The date that t cartography wa last modified

GraphDesc: This element re edges of a grap

Asset: This element represents one Cyber Asset within one Organization

VendorIdentifier: This element uniquely identifies a Vendor within the SPIDER platform

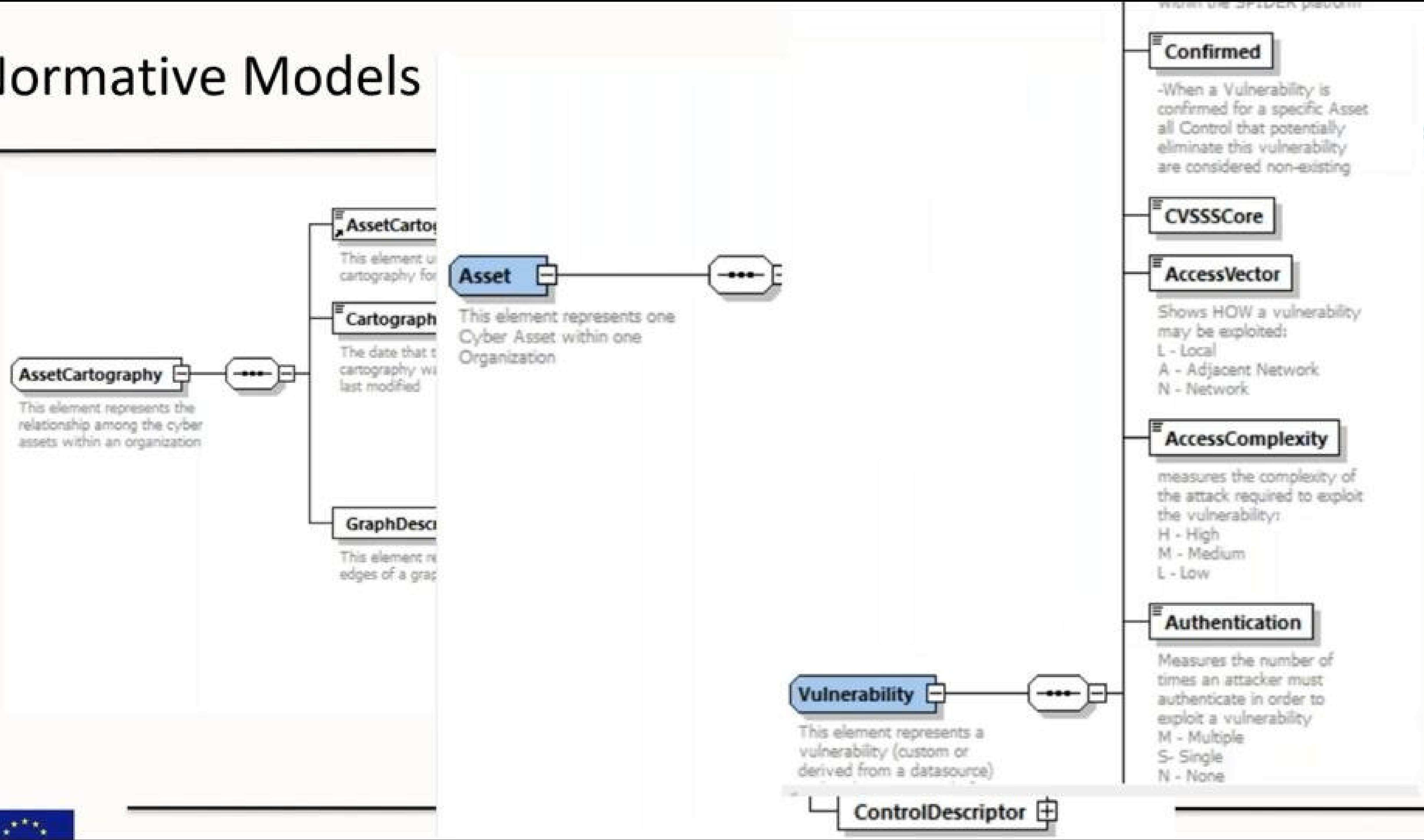
ProductName: Funtionality bound to this element:
–When a user declares the productname the ReportedVulnerability element is auto-filled (from the available Vulnerability Repositories)

Version: The version of the product

AssetCategoryIdentifier: This element uniquely identifies an Asset Category within the SPIDER platform

AssetIdentifier: This element uniquely identifies an Asset within an Organization

Normative Models



AssetCartography

This element represents the relationship among the cyber assets within an organization

AssetCartog

This element u
cartography for

Cartograph

The date that t
cartography wa
last modified

GraphDescr

This element re
edges of a grap

Asset

This element represents one Cyber Asset within one Organization

within the SPIDER platform

Confirmed

-When a Vulnerability is confirmed for a specific Asset all Control that potentially eliminate this vulnerability are considered non-existing

CVSSSCore

AccessVector

Shows HOW a vulnerability may be exploited:
L - Local
A - Adjacent Network
N - Network

AccessComplexity

measures the complexity of the attack required to exploit the vulnerability:
H - High
M - Medium
L - Low

Authentication

Measures the number of times an attacker must authenticate in order to exploit a vulnerability
M - Multiple
S- Single
N - None

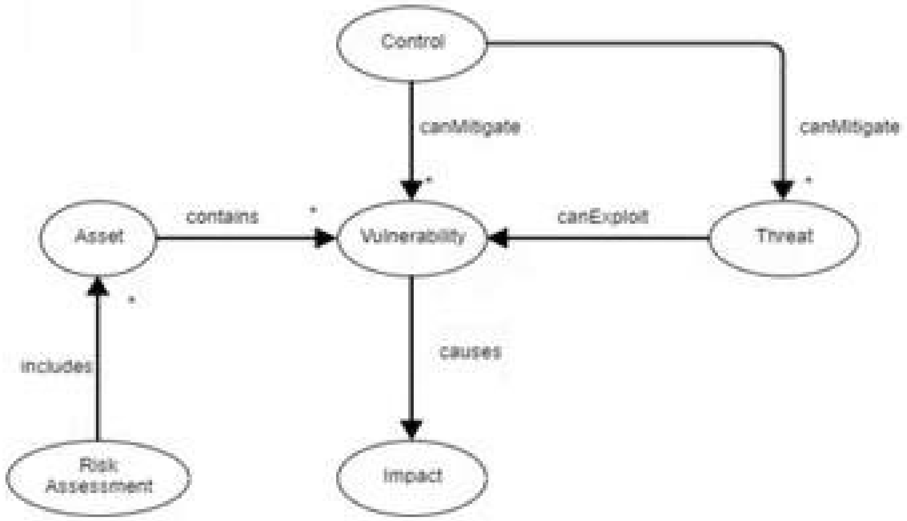
Vulnerability

This element represents a vulnerability (custom or derived from a datasource)

ControlDescriptor

Modality 3: Simulation Training

- **Goal**: Leverage the Risk Assessment skills of auditors/assessors
- **Medium** : Setup of a logical Infrastructure with hypothetical assets and controls
- **Model-Adherence**: NIST Models, CVE, CWE,CPE, ISO-27001

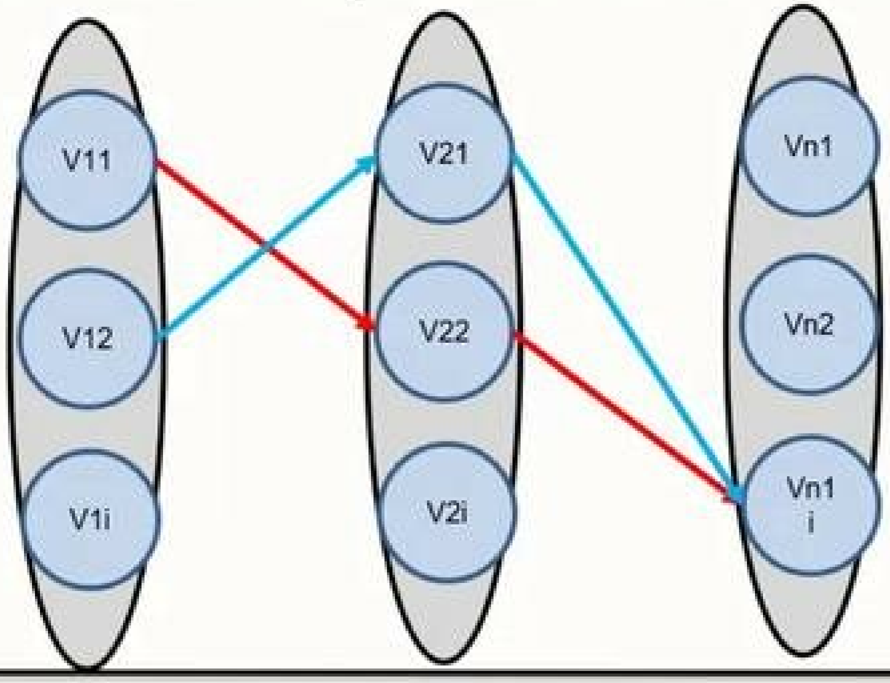


Calculation Model (non Graph-based)

- Individual_Risk = f(VL , IL , TL)
  - TL = f(AV , AC , AUTH)
  - IL = f(C , I , A)
  - TL = subjective
- In traditional models TL is hypothetical
  - Also known as Risk Appetite
- SPIDER provides TL quantification

Calculation Model (Graph Based)

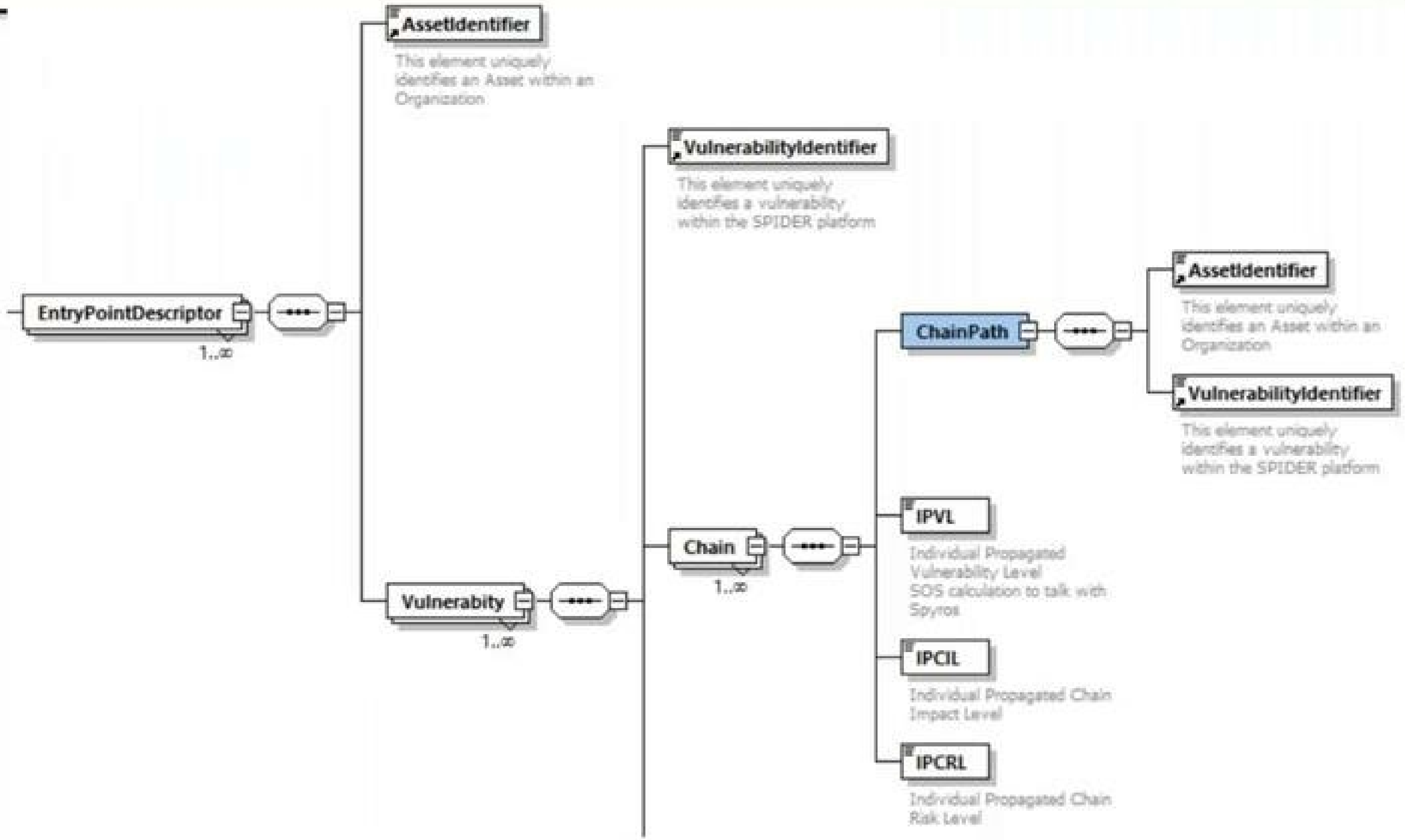
- When Assets are connected model is bound to the Direct Acyclic Graph;
  - Individual Risk Level **IRL**
  - Propagated Risk Level **PRL**
  - Cumulative Risk Level **CRL**
- Both PRL and CRL are dependent to Attack Paths



Game Definition

- What is defensive strategy that has to be followed with given:
  - Asset (vulnerable) topology
  - Likelihood per Attack
  - Acceptable Risk
- Defensive strategy is set of **controls** under a given “cost”

Normative Models



EntryPointDescriptor

1..∞

AssetIdentifier

This element uniquely identifies an Asset within an Organization

Vulnerabity

1..∞

VulnerabilityIdentifier

This element uniquely identifies a vulnerability within the SPIDER platform

Chain

1..∞

ChainPath

AssetIdentifier

This element uniquely identifies an Asset within an Organization

VulnerabilityIdentifier

This element uniquely identifies a vulnerability within the SPIDER platform

IPVL

Individual Propagated Vulnerability Level SOS calculation to talk with Spyros

IPCIL

Individual Propagated Chain Impact Level

IPCRL

Individual Propagated Chain Risk Level

Takeaways

- SPIDER is a “niche” Cyber Range platform targeting the specificities of the 5G telco domain
- It offers three distinct learning-modalities
- It follows de-facto standards
- It exposes normative APIs and structures for its artefacts

Major Challenges

- Syntactic Interoperability of Scenarios
- Model alignment (skills, topologies)
- Scoring models

Thank you!