The SPIDER Cyber Security Investment Component (CIC)

Maria Tsiodra
Michalis Chronopoulos
City, University of London

Matthias Ghering
Eirini Karapistoli
CyberLens

Neofytos Gerosavva
Nicolas Kylilis
8Bells

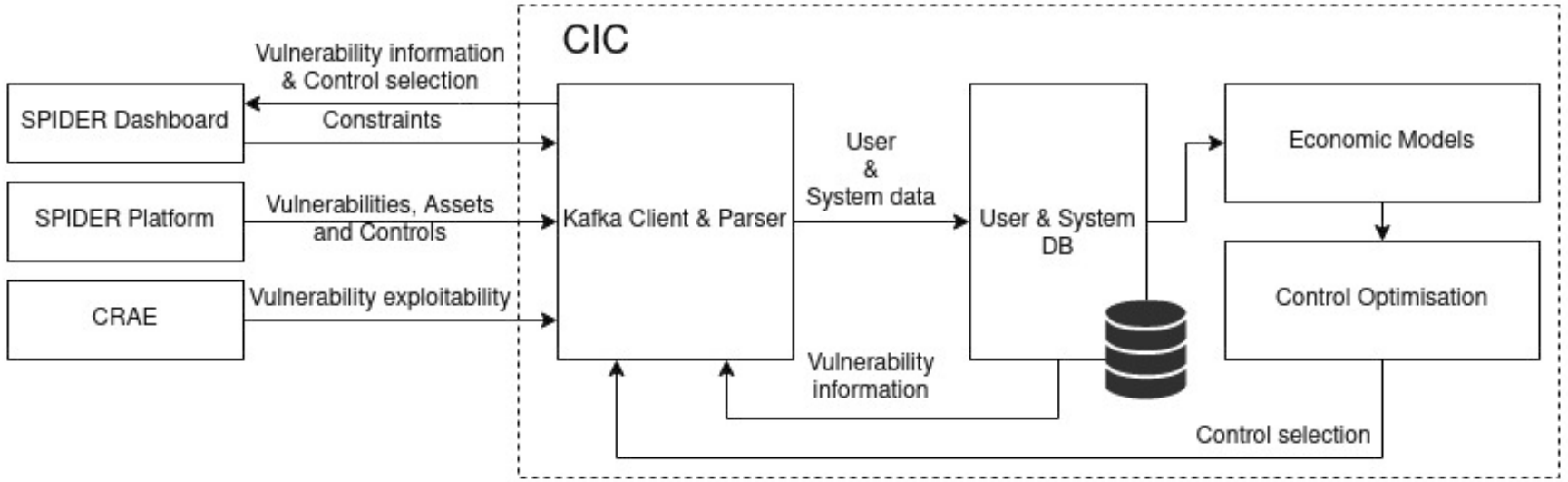
Introduction to SPIDER

SPIDER delivers an innovative Cyber Range-as-a-Service (CRaaS) platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges (TID's Mouseworld and 5Tonic testbeds and Thales's Cyber Range platform) with the most recent advances in telecommunications management and emulation, gamification and serious games training as well as economics of cybersecurity, into a single and easily accessible solution.

Introduction to Cyber security Investment Component

The Cyber security Investment Component (CIC) aim is to provide system administrators with actionable decision support. The CIC leverages economic models and data provided by the other SPIDER components to compute the most optimal binary selection of controls given the system administrator's constraints (e.g., budget, rules, policies).

CIC Architecture



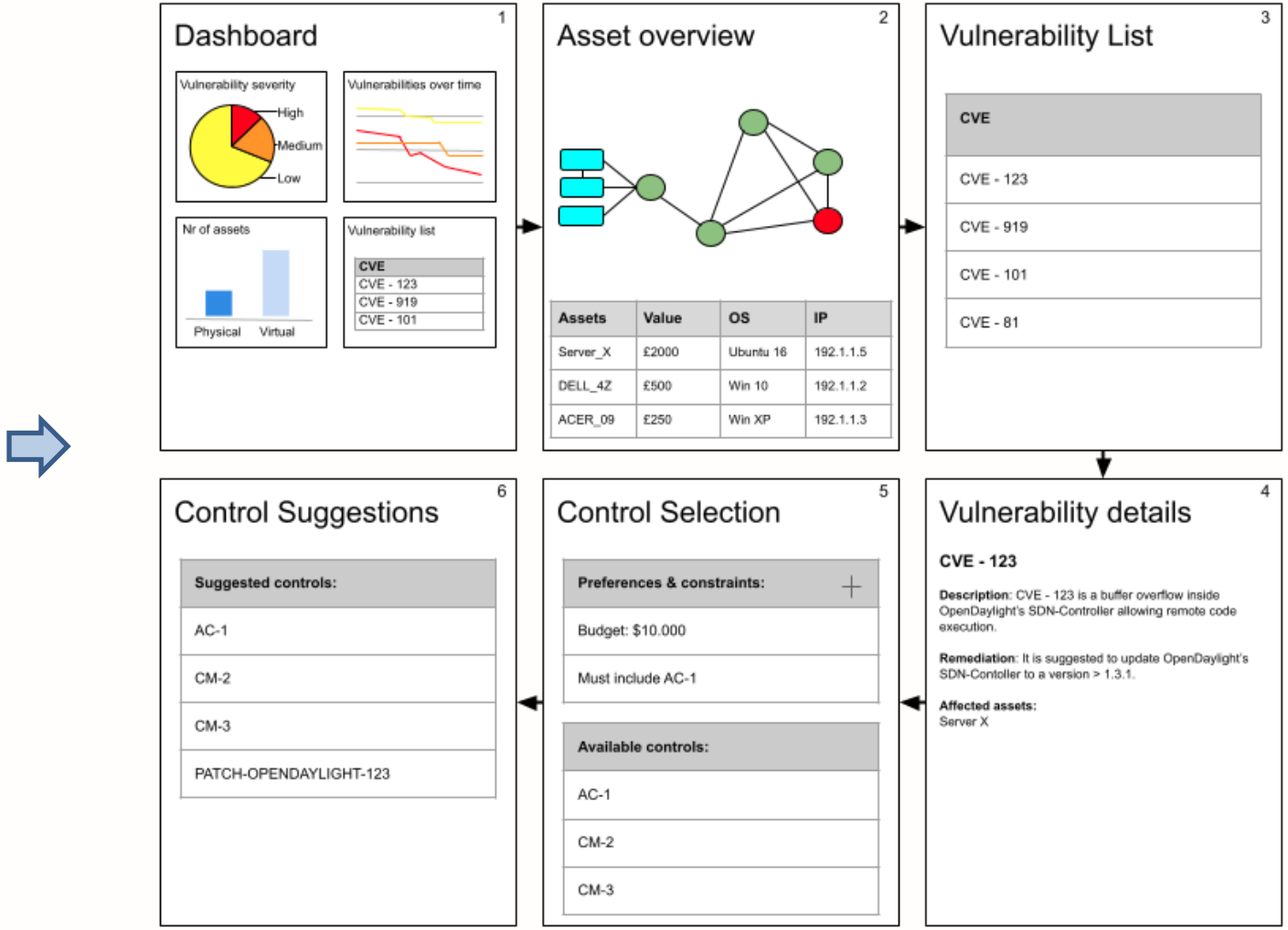
- **Input #1:** Assets at Risk & Impact
  - Identified assets
  - Asset value
- **Input #2:** Threats and vulnerabilities
  - Likelihood & Severity of attacks
  - Impact metrics (e.g., CVE impact metrics)
- **Input #3:** Existing cyber security controls
  - Control suggestions to mitigate threats & vulnerabilities
  - Efficacy and cost of implementing specific controls

- **Output #1**: Optimal binary investment portfolio (including decision & possible variations)
- **Output #2**: Vulnerability and Asset information

⇨ The output of the CIC component is exposed to the **SPIDER Dashboard.**

CIC Dashboard capabilities

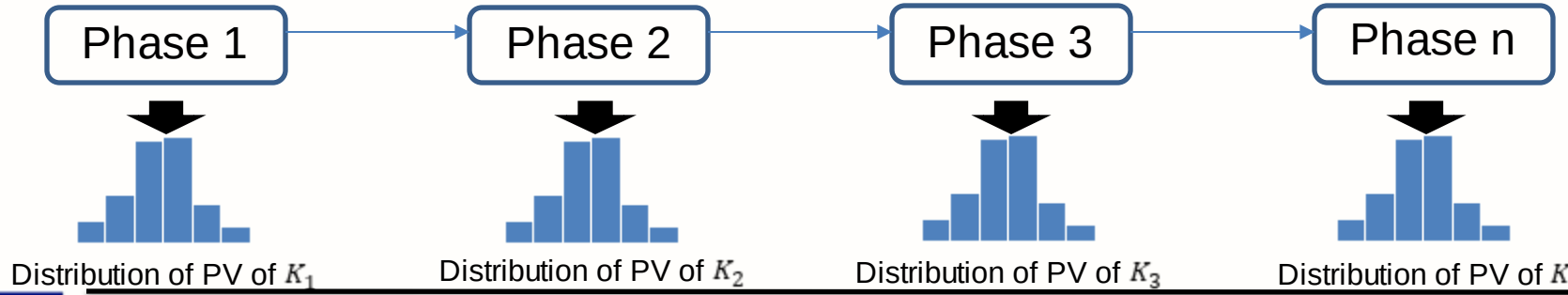
Sketches of the CIC pages to be considered in the SPIDER Dashboard



Economic Models

- **Assumptions**
  - We consider a security breach as a **multi-staged** process
  - Each stage reflects the exploitation of an asset, $i = 1, 2, \dots, n$, with $j = 1, 2, \dots, m_i$ vulnerabilities (V_{ij})
  - At the end of each stage there is a cost K_i for the organisation, such that: $K_i = A_i \langle R_i, S_i \rangle$
  - A_i is the asset value; R_i is the probability that a vulnerability is attacked; and S_i is the probability that the attack is successful.
  - Both the **time** (T_i) required to exploit an asset and the associated **cost** (K_i) vary randomly.
- **Objective:** Gauge the risk associated with the financial impact of the cyber attack.

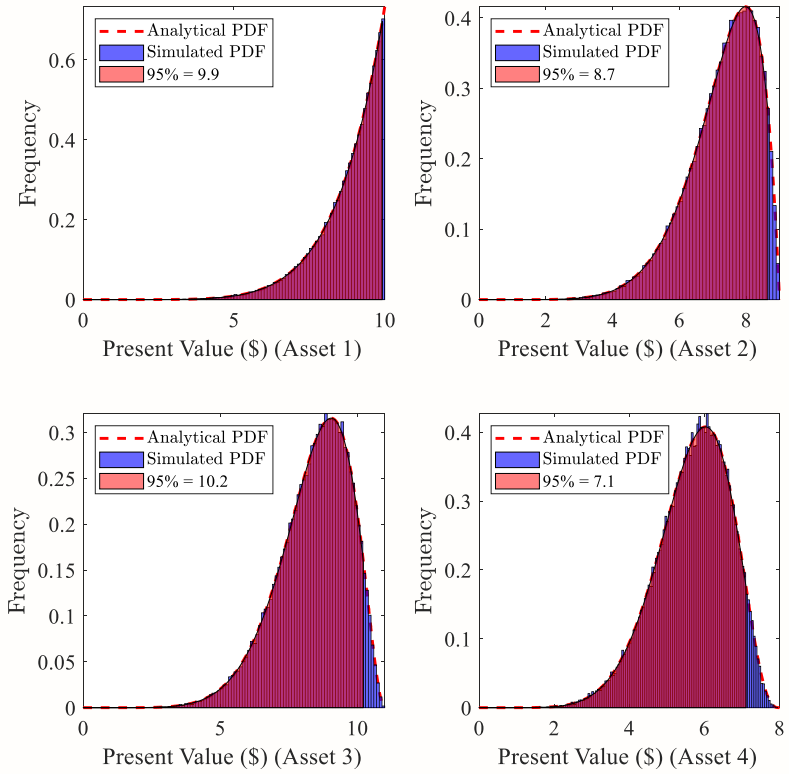
$$Z_n = K_1 e^{-\rho W_1} + K_2 e^{-\rho W_2} + K_3 e^{-\rho W_3} + \dots + K_n e^{-\rho W_n}, W_i = \sum T_i$$



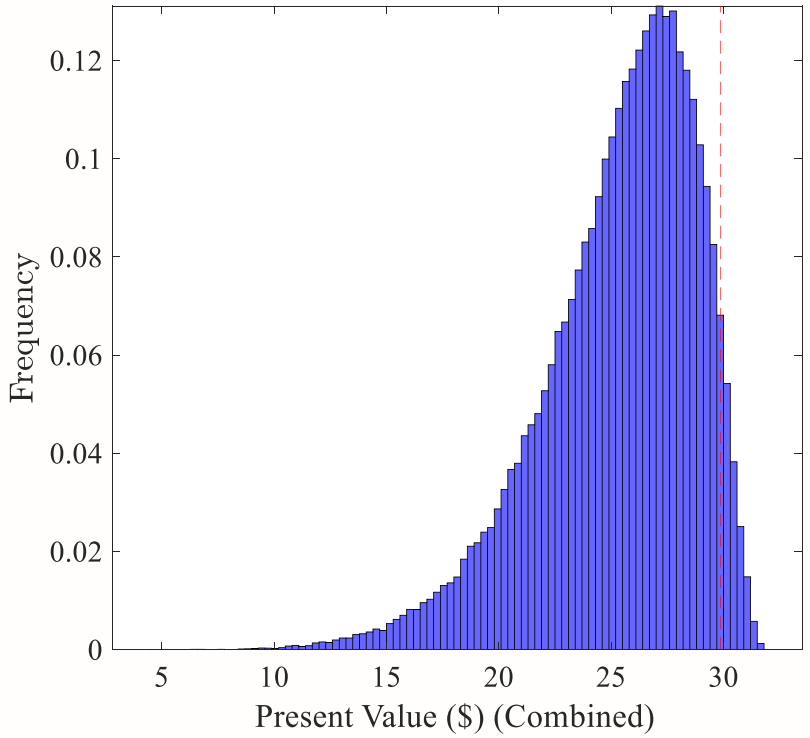
- Distribution of the PV of the overall impact
- Risk Measures
  - Expectation
  - Variance
  - VaR
  - CVaR

Results

Distribution of PV per Asset



Combined PV Distribution

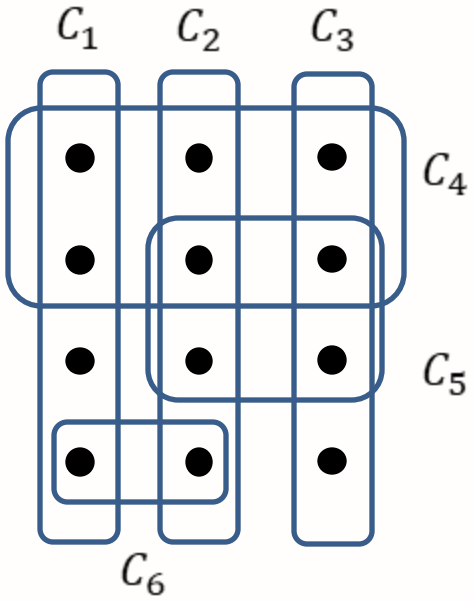


Risk Metrics $(n = 4)$

	Asset 1	Asset 2	Asset 3	Asset 4	Total
Mean ($)	8.8	7.29	8.4	5.69	25.32
SD ($)	1.13	1.11	1.71	0.94	12.15
95% Percentile ($)	9.93	8.66	10.22	7.11	29.85

Optimisation Models (Set Cover)

- Cast the optimal selection of controls as a **set cover problem**.
  - Available controls $\{C_1, C_2, \dots, C_\ell\}$
  - x_l: Binary variable indicating the inclusion or not of a control $l = 1, 2, \dots, \ell$
  - y_l: Cost of implementing control $l = 1, 2, \dots, \ell$
  - B: Available budget.
  - Determine the minimum set of controls that achieves a complete coverage of the systems vulnerabilities.



Mathematical Formulation

$$\min \sum_{l=1}^{\ell} x_l$$

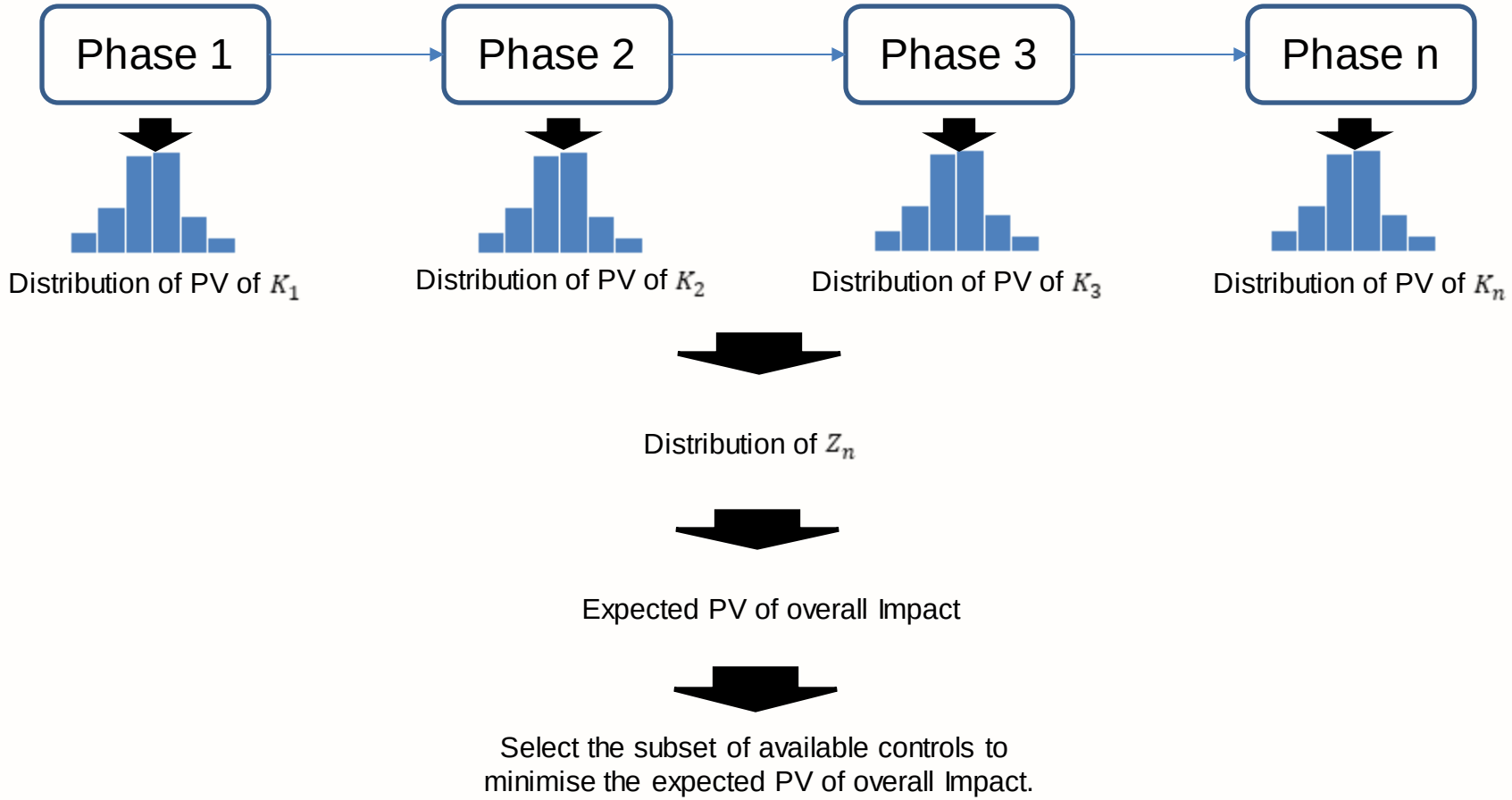
$$\sum_{l:V_{ij} \in C_l} x_l \geq 1, \quad \forall V_{ij} \in \mathcal{V}$$

$$\sum_{l=1}^{\ell} x_l y_l \leq B$$

$$x_l \in \{0, 1\}$$

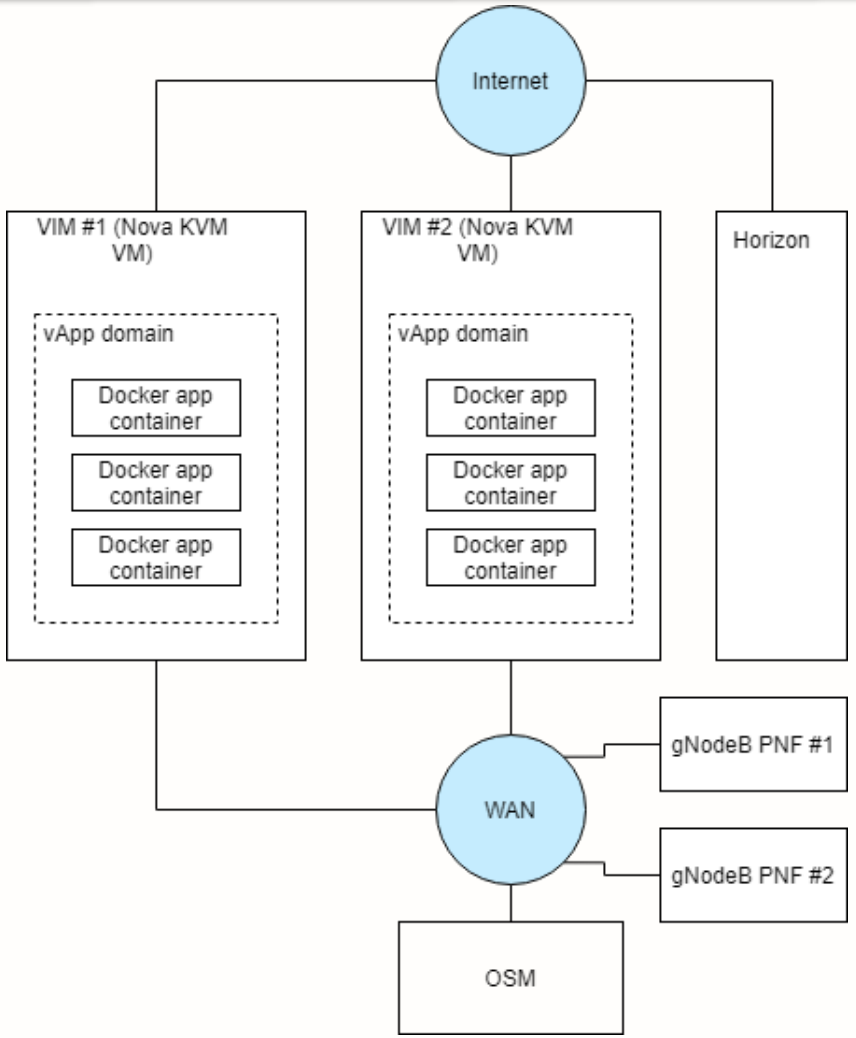
Optimisation Models (Knapsack)

- **Model II**: Determine the set of controls to **<u>minimise the expected impact of the cyber attack</u>**.



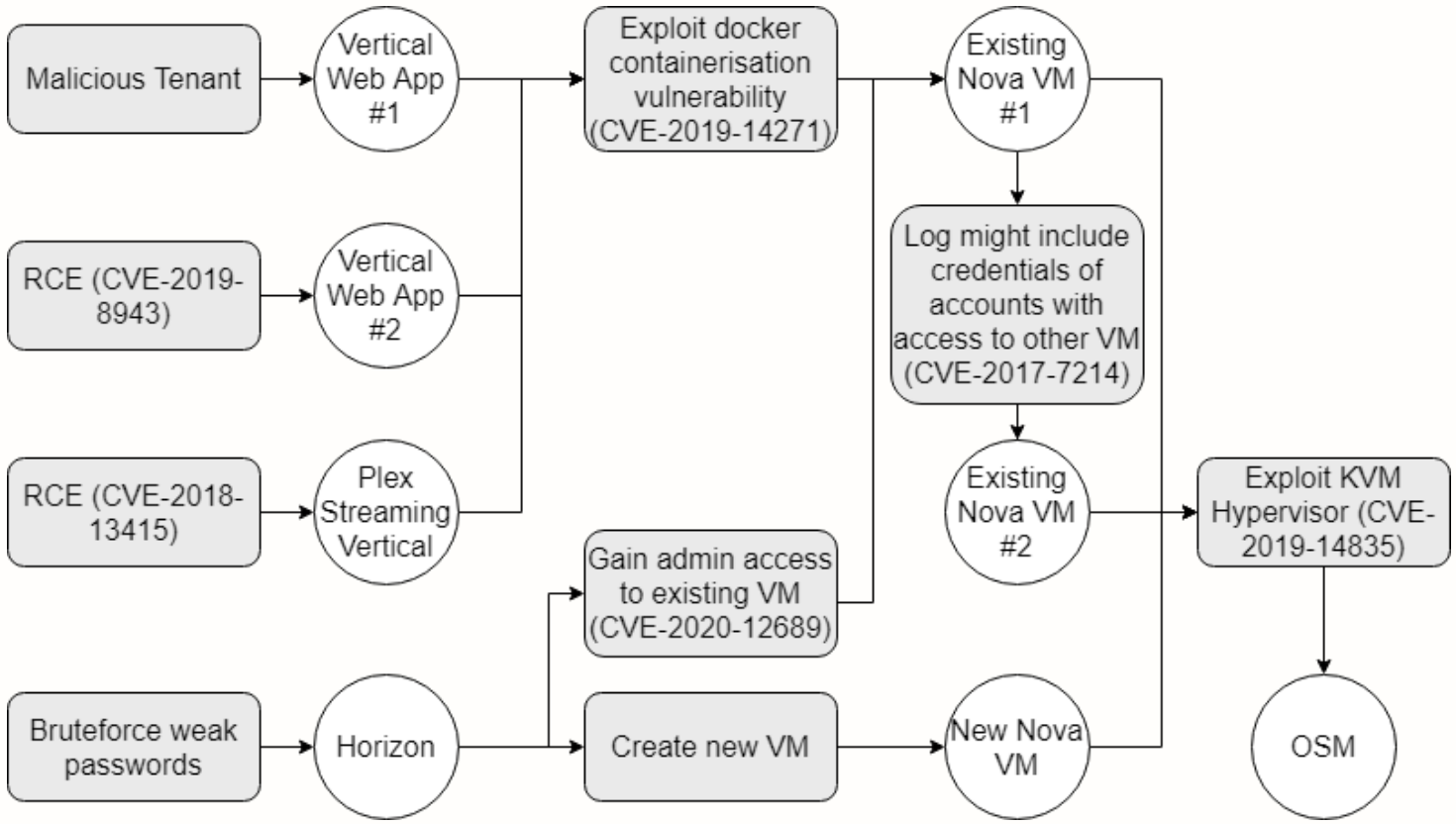
5G Scenario

Infrastructure overview

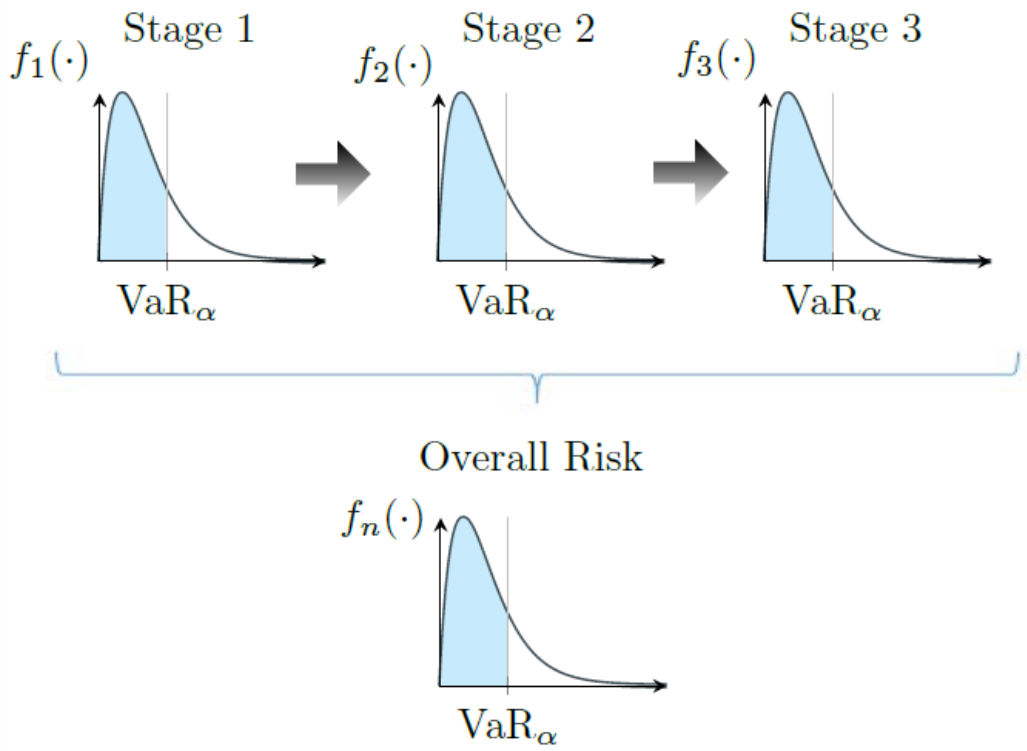


5G Scenario

Attack tree



5G Scenario conclusion



The SPIDER Cyber Security Investment Component (CIC)

Questions