GÉNÉRATION DE GRAPHES DE REMÉDIATION BASÉ SUR DES ONTOLOGIES

Auteurs

Kéren Saint-Hilaire

Frédéric Cuppens

Nora Cuppens

Joaquin Garcia-Alfaro

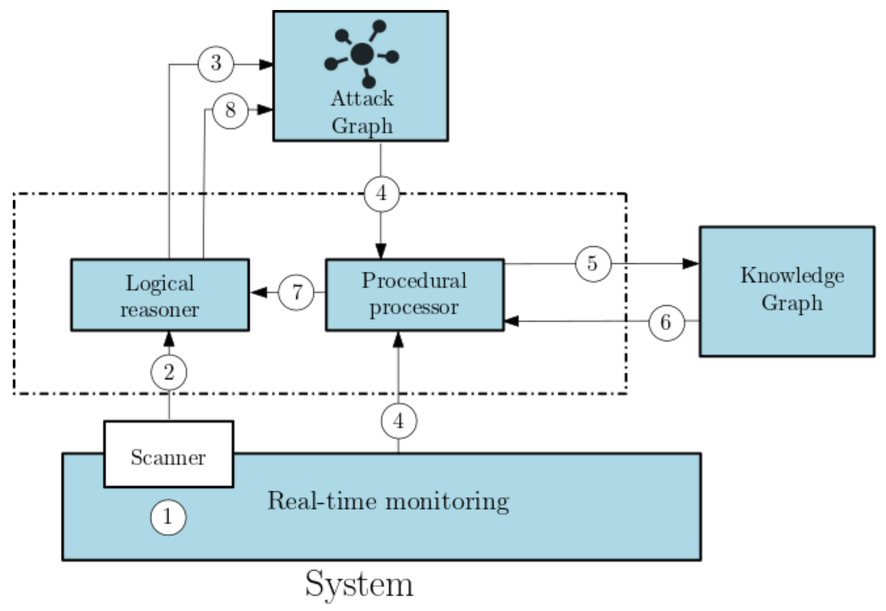
Partenaires

1. CONTEXTE

- Automatisation de la gestion de risque
- Sélection en temps réel de contremesures
- Enrichissement ontologique des graphes d'attaque
- Dérivation des plans de remédiation

2. REVUE DE LITTÉRATURE

- L'analyse des vulnérabilités ne tient pas compte de la topologie du système, de la position de l'attaquant et de ses potentielles actions
- Les graphes d'attaque logiques [1] offrent ...
  - Topologie, position et actions de l'attaquant
  - Déduction de nouvelles connaissances
  - Sélection de contremesures & remédiation

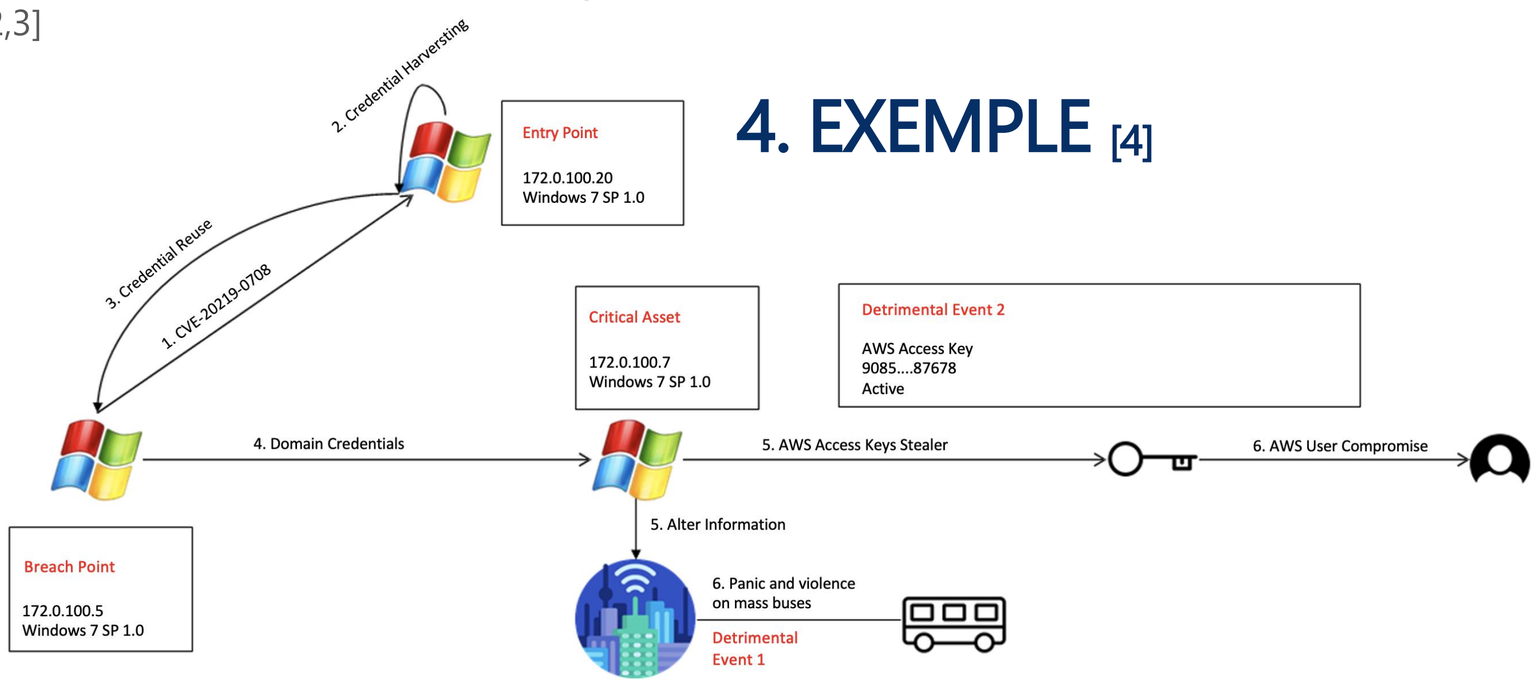


3. APPROCHE PROPOSÉE

- Génération de graphes d'attaque logiques
  - Utilisation d'un raisonneur logique
    - Programme logique
    - Ensemble fixe de règles
    - Hypothèse du monde fermé
      - pas connu ⇝ faux
  - Information provenant du système à l'aide du monitoring & conséquences logiques

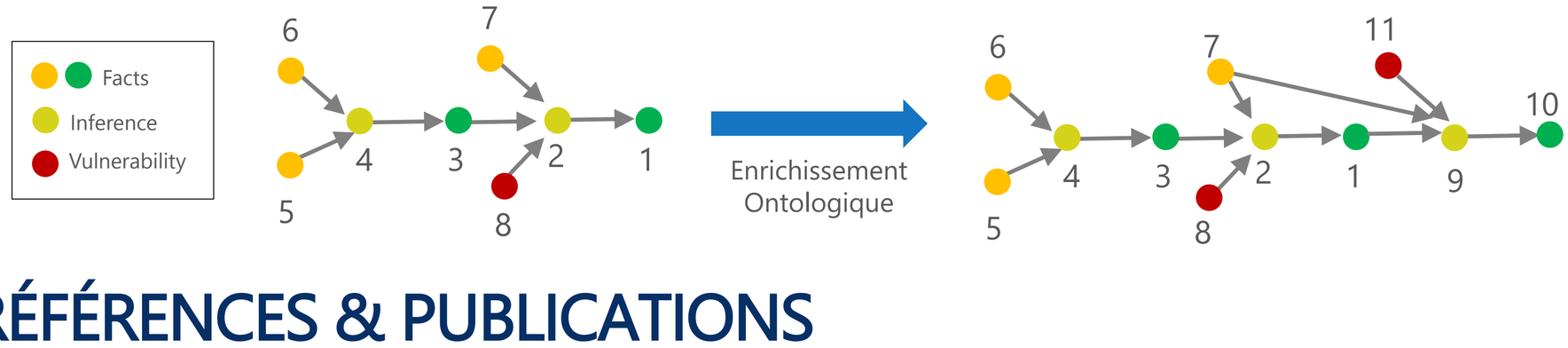
- Le graphe de connaissances permet
  - Enrichir le graphe d'attaque en déduisant de nouvelles connaissances à base d'ontologies existantes [2,3]

4. EXEMPLE [4]



- Déduction logique de nouvelles conséquences suite à l'exploitation d'une vulnérabilité
  - De nouvelles règles logiques alimentent la base de connaissance du raisonneur logique, e.g. [4,5] :

```
execCode(_host, _username) :- vulExists(_host, _CVE, _product, remoteExploit, privEscalation),
                              execCode(_host, _username), networkServiceInfo(_host, _product, _protocol, _, _username).
```



RÉFÉRENCES & PUBLICATIONS

[1] Ou *et al.* MulVAL: A logic-based network security analyzer. USENIX Security Symposium, 2005 & https://github.com/risksense/mulval

[2] NIST. Vulnerability Description Ontology (VDO), 2016. [3] MITRE. Digital Artifact Ontology (DAO) & DEFEND Knowledge Graph of Cybersecurity Countermeasures. 2012-2022.

[4] Saint-Hilaire *et al.* Ontology-based Attack Graph Enrichment, *2021 TIEMS Annual Conference*, Paris, France & https://arxiv.org/abs/2202.04016

[5] Saint-Hilaire *et al.* Enrichment of Defense Graphs using Ontologies, *submitted, under evaluation, 2022-2023*.

Contact keren.saint-hilaire@telecom-sudparis.eu https://scn.telecom-sudparis.eu/

SAMOVAR PhD Day March 2023