Les *kill chains*, tout le monde en parle mais personne n'en fait !

Vers une grammaire des *kill chains*

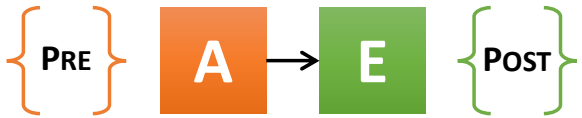
CONIX

LE CHOIX DE L'EXPERTISE

Rappel du volet précédent

Episode précédent : préalables à la constitution de KDB pour élaborer les *kill chains*

- **La *kill chain* n'existe pas** : c'est une succession de séquences « action <> effet »
- Chaque séquence est conditionnée par des **pré-conditions**
- Chaque séquence provoque des **post-conditions** (une transformation de l'espace)



Rappel de la cible

On a besoin :

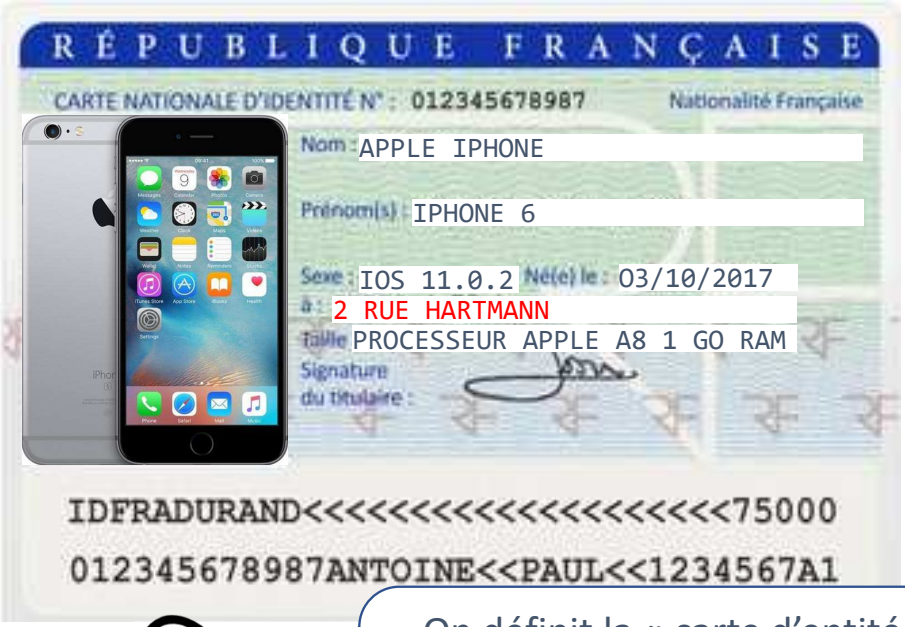
- ➡ D'une rigueur logique
- ➡ De principes pour limiter l'explosion combinatoire

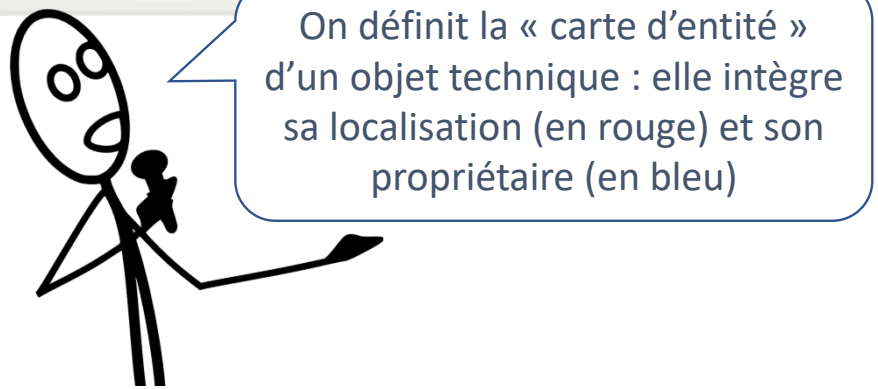
On veut : modéliser les possibilités de progression spatio-temporelle de l'attaquant

Etape suivante : construire les outils méthodologiques pour…

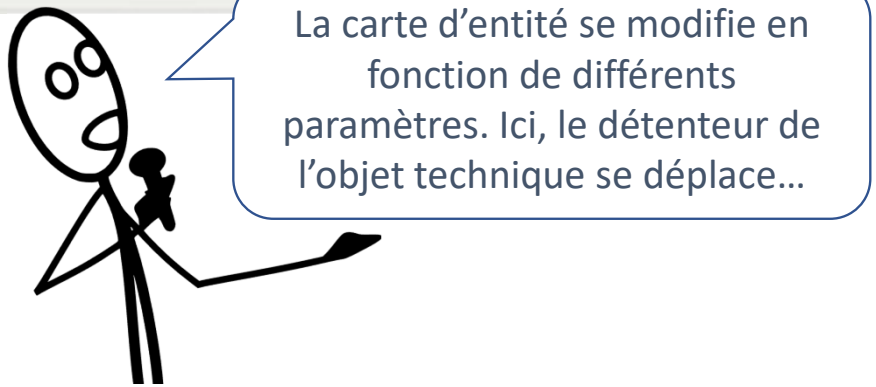
- ➡ Donner du sens aux pré-conditions et aux post-conditions
- ➡ Introduire les KDB interdépendantes : on travaille avec celles du MITRE / du NIST
- ➡ Spécifier les règles qui permettent d'utiliser ces KDB

Carte d’entité

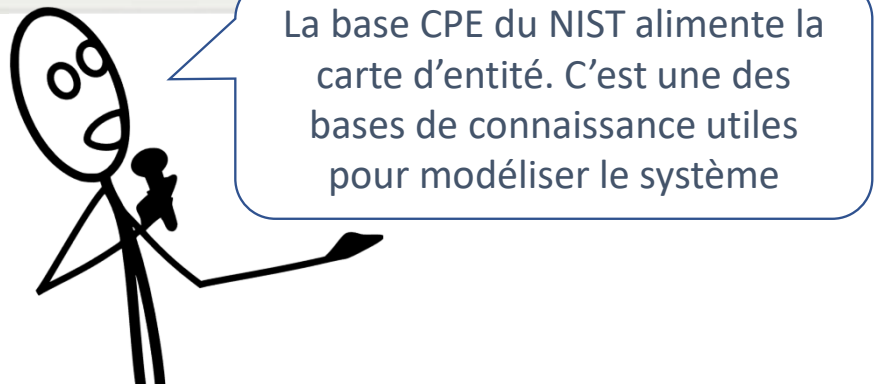




Carte d’entité

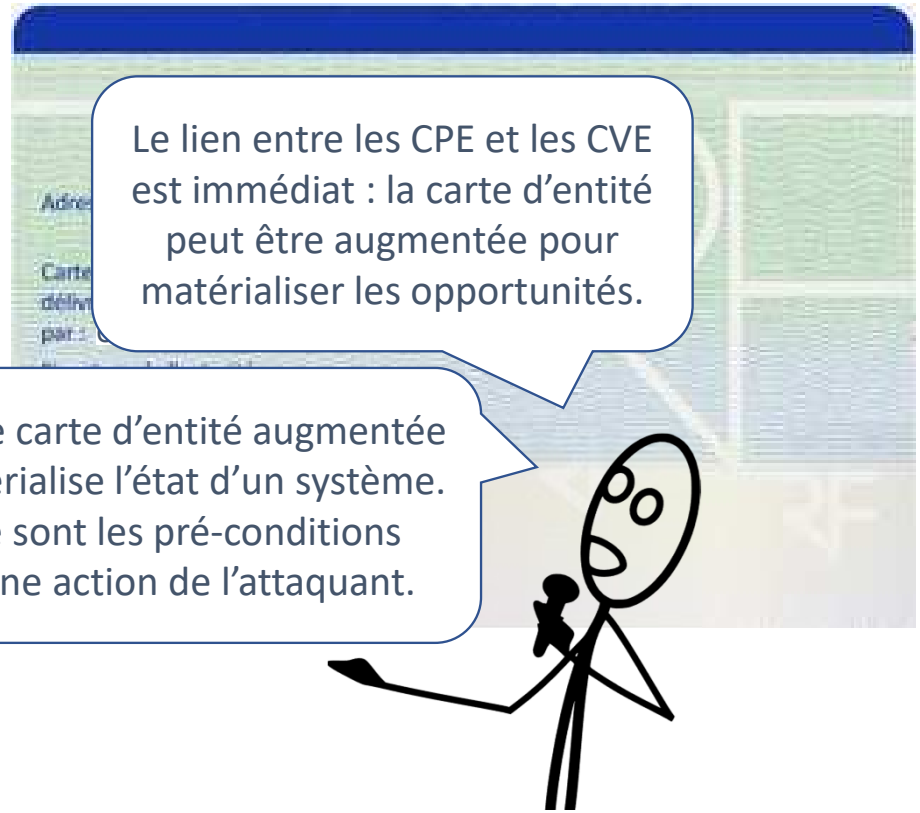


Carte d'entité

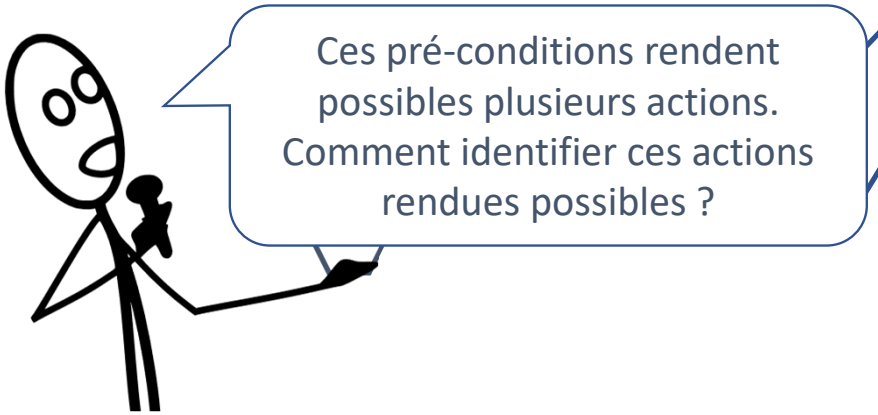


Carte d'entité (augmentée)

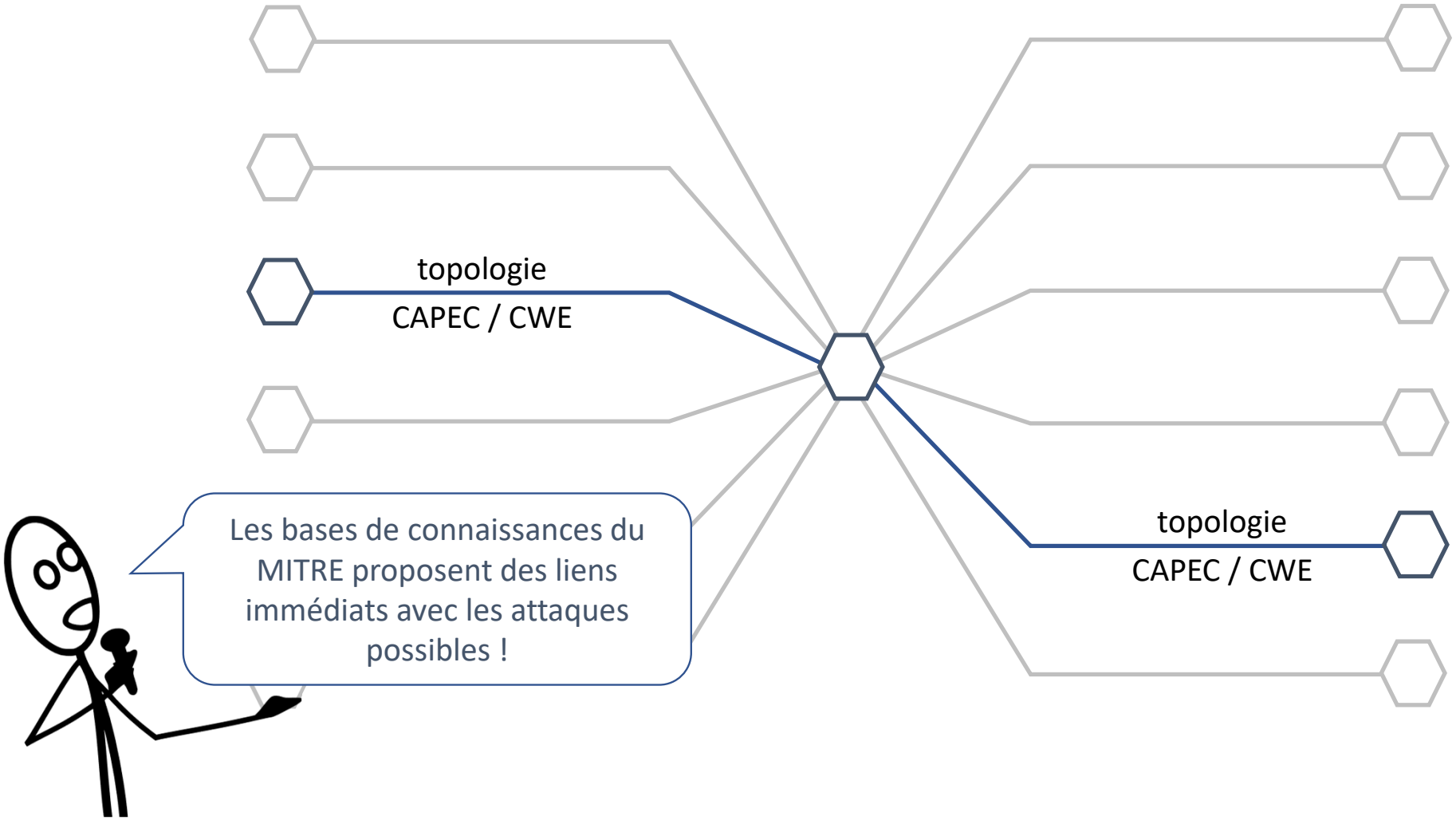
CVE-2018-4465
CVE-2018-4464
CVE-2018-4461
[…]



Carte d’entité (augmentée)



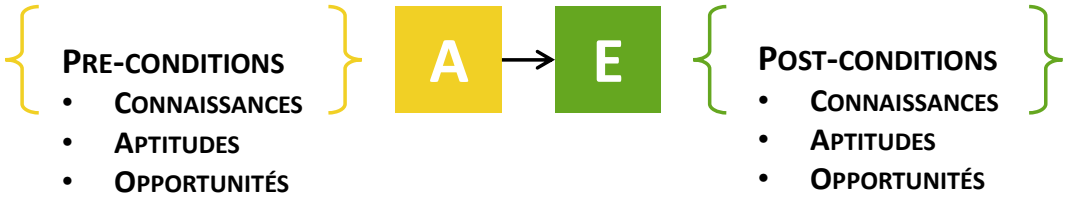
Carte d’entité (augmentée)

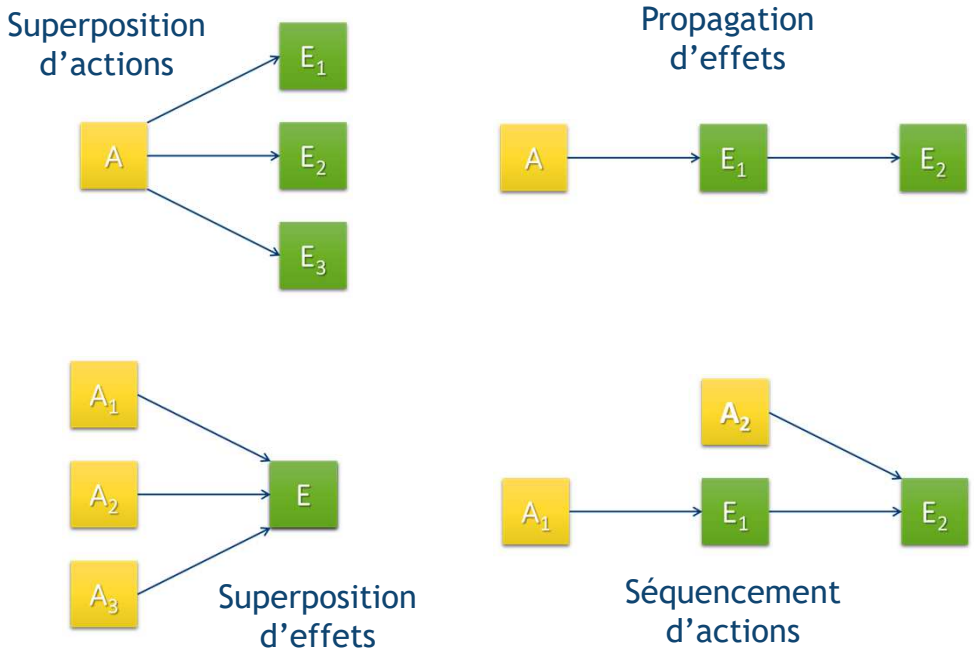


Règles d'utilisation de CAPEC

Principes (tempo)-logiques :

Règles d'inférence qui régissent l'évolution d'une entité soumise à des actions.

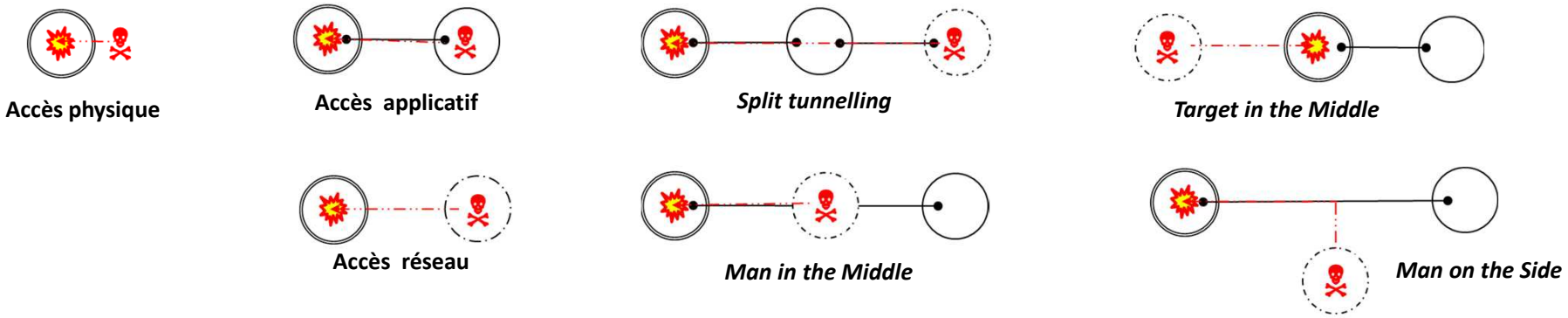




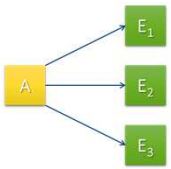
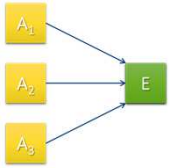
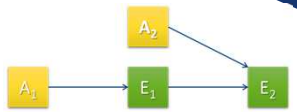
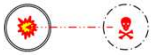
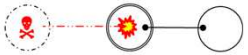
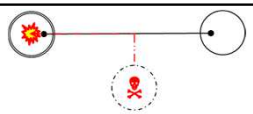
Règles d’utilisation de CAPEC

Principes (topo)-logiques :

Règles structurelles qui définissent les opportunités d’action en fonction des positions relatives des acteurs (hostile, cible, neutre) dans le système

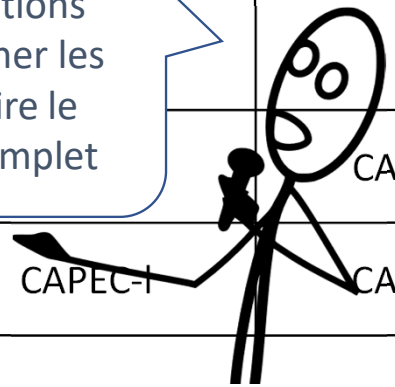


Règles d'utilisation de CAPEC

					
	CAPEC-a	∅	CAPEC-g	∅	CAPEC-m
	CAPEC-b	CAPEC-d	∅		∅
	CAPEC-c	∅	∅		∅
	∅	CAPEC-e			∅
	∅	CAPEC-f			
	∅	∅			CAPEC-n
	∅		CAPEC-h	CAPEC-i	CAPEC-o

Les attaques du modèle CAPEC sont l'application d'une action dans une configuration donnée (forme topologique)

Les Pré et Post-conditions permettront d'enchaîner les CAPEC pour construire le scénario d'attaque complet



Pour en savoir plus

contact_securite@conix.fr

CONIX