UNIVERSITÉ DE LORRAINE | UFR MATHÉMATIQUES INFORMATIQUE MÉCANIQUE ET AUTOMATIQUE

Projet M1 UFR MIM :

Graphe d’attaque PHANTOM

Marwin NIMESKERN
Grégory GUGGENBUHL

Sommaire

Table ssdes matières

Etat de l’art 2
Le modèle MULVAL 2
Présentation 2
Avantages Principaux 2
Problèmes Principaux 2
Conclusion 2
Les critères communs 3
Présentation 3
Avantages Principaux : 3
Problèmes Principaux : 3
Conclusion 3
MISP : Malware Information Sharing Platform and Threat 4
Présentation 4
Avantages Principaux 4
Problèmes Principaux : 4
Conclusion 4
Bugyuo Methodology 5
Présentation 5
Avantages Principaux 5
Problèmes Principaux 5
Conclusion 5
Introduction 6
Problématique générale 6
But du graphe d’attaque Phantom 6
Les niveaux du modèle Phantom 7
Représentation des différents modèles : 7
NIVEAU 0 : Optimisation 8
Définition du modèle 8
Représentation 8
Répond aux besoins 8
Passage du niveau 0 au niveau 1 et inversement 9

NIVEAU 1 : Network 10
Définition du modèle 10
Représentation 10
Répond aux besoins 10
NIVEAU 2 : Context 11
Définition du modèle 11
Représentation [Cf. Annexe 1] 11
Répond aux besoins 11
NIVEAU 3 : Standardisation 12
Introduction des types de graphiques 12
Les axiomes 12
Les types d'axiomes 13
Les axiomes Ressources : Les Packages de Ressources 13
Les axiomes Values : Les Packages de valeur 13
Contenant d'un axiome 13
Les interactions possibles entre axiomes 13
Les types d'actions possibles 14
Attack 14
Defense 14
System 14
User 14
Exemples de tactiques d'attaque sur une défense 15
Les attaques Préfixées 15
Les attaques Postfixées 15
Les actionneurs système 16
Le PATH d'un actionneur 16
NIVEAU 3 SB : Scenario BLUE : Defense Policy 17
Définition du modèle 17
Représentation [Cf. Annexe 2] 17
Répond aux besoins 17
NIVEAU 3 SR : Scenario RED : Trying Attack 18
Définition du modèle 18
Représentation [Cf. Annexe 3 / 4] 18
Répond aux besoins 18
Les besoins pour les professionnels 19
L'utilisation de MISP 19

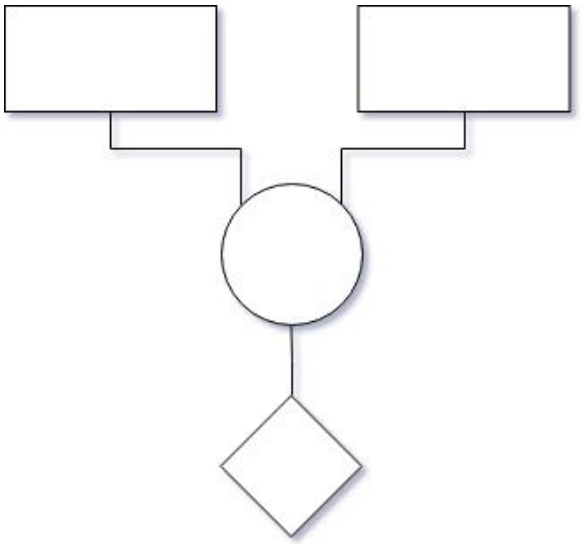
To be continued: 20
Modification Future probable: 20
Le graphe PHANTOM est un graphique Orienté Infrastructure : 20
NIVEAU 0 : Optimisation 20
NIVEAU 1 : Network 20
NIVEAU 2 : Context 20
NIVEAU 3 SB : Scenario BLUE : Defense Policy / SR : Scenario RED : Trying Attack 20
Annexes 21
ANNEXE 1 : Schéma SQL : Entité / Relation 21
..... 21
ANNEXE 2 : Niveau 3 : SB : Exemple d'un schéma de défense : 22
ANNEXE 3 : Niveau 3 : SR : Exemple 1 d'un schéma d'attaque : 23
ANNEXE 4 : Niveau 3 : SR : Exemple 2 d'un schéma d'attaque : 24

Etat de l'art

Le modèle MULVAL

Présentation

Le modèle MULVAL vu en cours est un modèle graphique présentant le déroulement d'une attaque.



- Les prérequis permettent de savoir les conditions nécessaires au bon déroulement de l'attaque
- L'attaque stipule le virus et/ou la faille CVE utilisé.
- Les conséquences* indiquent l'état du système après l'attaque
*Peut servir de prérequis

Avantages Principaux

- Présente efficacement une seule ou plusieurs attaques reliées entre elles
- Possibilité de faire du Prolog dessus

Problèmes Principaux

- Ce modèle ne peut être utilisé que pour décrire un nombre limité d'attaques et ne peut présenter un système complet ainsi que son arborescence.
- Impossibilité de modéliser des contres mesures pour l'attaque (seul l'attaque est modélisée)
- Impossibilité de définir le contexte complet de l'attaque (réseau, utilisateur, disque, etc)

Conclusion

Ce modèle bien qu'incomplet pour définir l'intégralité des failles d'un système est néanmoins efficace pour présenter une attaque seule et inspirera donc fortement notre modèle attaque et défense (cf partie N°3)

Source : Cours de Mme Francine HERRMANN

Les critères communs

Présentation

Les critères communs (CC) sont un ensemble de normes (ISO 15408) internationalement reconnu dont l'objectif est d'évaluer de façon impartiale la sécurité des systèmes et des logiciels informatiques.

L'ISO en mai 2006, va regrouper les différents états pour définir une norme (ISO 15408) reconnue par tous les états signataires de l'accord CC-MRA.

En plus des 17 pays signataires, 9 pays non signataires reconnaissent ces certificats.

Ces certificats définissent différent(e)s :

- Exigences fonctionnelles
- Exigences d'assurance de sécurité
- Niveaux d'assurance EAL

Avantages Principaux :

- Certification reconnue dans le milieu de la sécurité attestant un niveau de sécurité
- Permet d'avoir l'image de sécurité d'une entreprise à un instant T

Problèmes Principaux :

- Pas d'outils propres pour évaluer toute la sécurité
  - *Les entreprises ont tendances à faire leurs propres outils sans aucuns standard*
- Mauvaise mise en œuvre
  - *Les consommateurs ne sont pas en mesure d'indiquer clairement et sans ambiguïté les exigences de sécurité du produit*
- Complexe à mettre en place même pour les experts
  - *Il n'y a pas de norme sur la façon de documenter, de manière concise et systématique, les propriétés de sécurité de systèmes d'information, dans le processus de développement du système*
  - *Les méthodes sont très complexes sur le plan sémantique, et par conséquent, le coût de l'apprentissage est très élevé*
- Trop coûteux
- Ne prennent pas en compte l'audit continu de la sécurité

Conclusion

Les critères communs sont un outil pour assurer la sécurité des réseaux, néanmoins il semble difficiles à l'heure actuelles pour une entreprise de les mettre en œuvre car il n'existe pas d'outils leurs facilitant la tâche.

Notre graphique Phantom essayera donc de répondre le plus exhaustivement possible pour

- La mise en place
- L'évaluation
- La notation

De ces différents critères, afin de répondre à un manque aujourd'hui présent dans le domaine de la sécurité des systèmes et ainsi aider leurs utilisateurs.

Source : Wikipédia / Mr Djamel KHADRAOUI

MISP : Malware Information Sharing Platform and Threat

Présentation

MISP est une organisation gouvernementale luxembourgeoise regroupant une communauté de plus de 6000 entreprises partageant des informations d'attaques, fraudes, ... entre elles.

Les membres du projet :

- David Andre
- Andrzej Dereszowski @deresz666
- Alexandre Dulaunoy @adulau
- Andras Iklody @Iglocska
- Christophe Vandeplas @cvandeplas
- Raphaël Vinot @rafi0t

MISP est un logiciel open source sur GitHub, permettant le partage et la mise en commun des attaques révélés par la communauté entre instances MISP.

Le corps de MISP est une sorte de base de données d'événement, de sous événements et d'attributs interconnectés.

Avantages Principaux

- Est une des plus grandes bases de données d'attaques au monde
- Est internationalement reconnu
- Les données sont multiples
- Les taxonomies peuvent servirent de typages d'objets
- Open-Source et régulièrement maintenu par une communauté chaleureuse.
- Peut ressembler à du SQL (Entité / Relation)
- Dispose d'un partenariat avec l'université de Lorraine

Problèmes Principaux :

- Peu intuitif au premier plan, nécessite une bonne compréhension du logiciel et de ses modules
- Peu de réutilisabilité à ce jour
- Nécessité de s'adapter au fonctionnement complet et particulier de MISP pour s'en servir comme support sans base de données externe

Conclusion

- Les attributs sont interconnectés ce qui juxtaposer avec un graphe d'attaque peut permettre de révéler les attaques globales des virus et leurs fonctionnements à travers un système donné
- La puissance de MISP couplé à un graphe d'attaque pourrait servir à mieux comprendre les attaquants, le fonctionnement des virus et leurs contre-mesure
- Si le graphique est directement mis en œuvre sur MISP aucune base de données externes ne sera nécessaire (nécessite néanmoins un logiciel pour l'affichage)

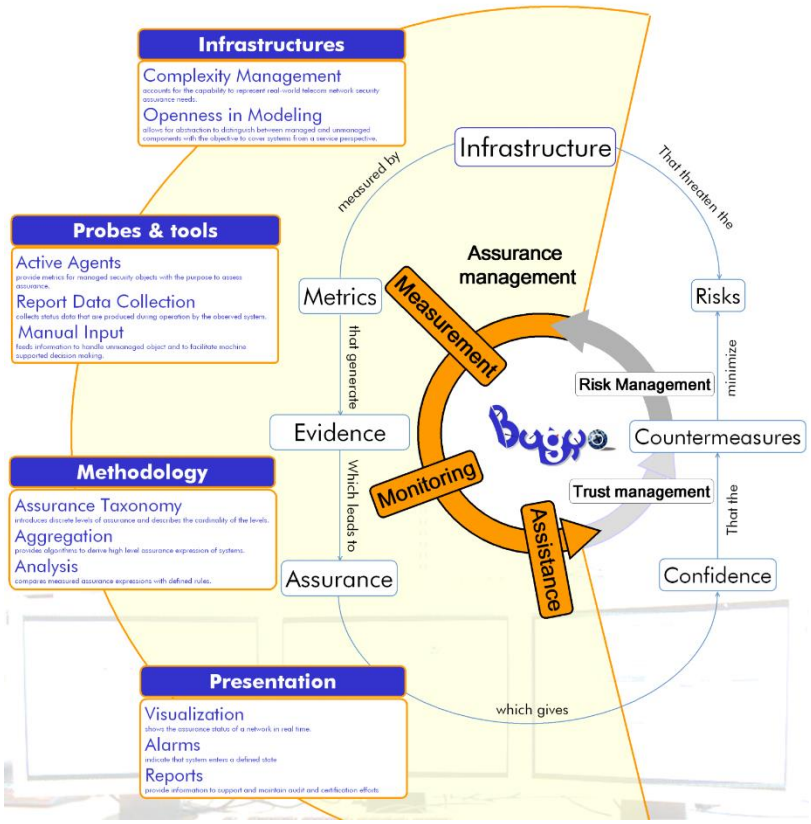
Source : https://www.misp-project.org

Bugyuo Methodology

Présentation

Projet de méthodologie de sécurité des opérateurs télécom

L'infrastructure est générée par des métriques qui génère des évidences qui servent à minimiser les risques qui donnes un niveau de confiance sur les contres mesures qui minimisent les risques.



Avantages Principaux

- Donne une approche intéressante sur la méthodologie d'une politique de sécurité, d'assurance sécurité et leurs différentes mises en place et fonctionnement.
- A été créé avec la collaboration d'un de nos professeurs en sécurité
- Approche parallèle aux critères communs

Problèmes Principaux

- Notion abstraite ne donnants que des indications sur la manière de procéder d'un ingénieur pour la sécurisation d'un système
- Les notions sont très hautes dans la démarche de la méthodologie.

Conclusion

Permettant de mieux comprendre les besoins d'un SSI, cette méthodologie peut nous permettre de voir si nous répondons au mieux à ses besoins.

Comme pour les critères communs, nous nous appuierons dessus pour définir l'utilité du niveau de notre graphique pour cette méthodologie.

Cela servira entre autre à répondre à la question « Quel est l'impact de notre graphique sur la méthodologie vis-à-vis de ses besoins ? »

Source : Mr Djamel KHADRAOUI

Introduction

Problématique générale

Des graphiques d'attaque existant à l'heure actuel aucun d'eux ne peux présenter de façon clair et détaillé l'intégralité d'un système de données avec ses failles, ses utilisateurs et ses contre-mesures.

Il est donc impossible d'avoir graphiquement et de façon précise d'une infrastructure donnée et ainsi de la formaliser.

But du graphe d'attaque Phantom

Le graphe PHANTOM est un graphique Orienté Infrastructure, il permettra donc de :

- Présenter de façon clair l'intégralité des défenses et attaques possible d'un système
- Permettra d'aider les personnes travaillant en forensic à comprendre ce qui s'est passé sur un système et à le présenter graphiquement
- Permettra d'organiser et de vérifier les défenses et ainsi de mettre en place une politique de sécurité dynamique
- Le graphique sera en lien avec MISP, il sera alimenté en temps réel par toutes les entreprises partageant avec eux leurs défenses et attaques d'un même logiciel, cela rendra le graphique dynamique et toujours à jour.
- Il permettra de retracer les actions d'un individu sur un réseau et de connaitre les droits d'un utilisateur sur un système
- Comprendre quels logiciels peuvent poser problème car vulnérable à certaines attaques.
- Anticiper les prochaines attaques
- Simuler des hypothèses d'attaque
- Calculer les pertes, les chemins bipartis et tous autres calculs réalisables avec CPLEX

Les critères communs sont pour les entreprises très complexes à mettre en œuvre et à surveiller.
Ce graphe aura pour objectif d'aider à conceptualiser de façon formelle et normalisé les systèmes et leurs politiques de sécurité.

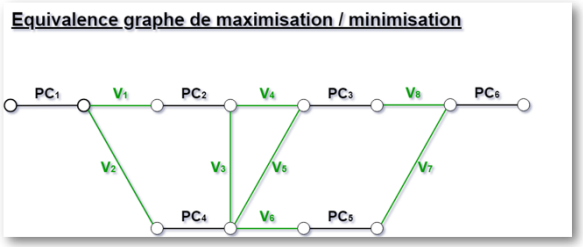
- *Il n'y a pas de norme sur la façon de documenter, de manière concise et systématique, les propriétés de sécurité de systèmes d'information, dans le processus de développement du système*

Des méthodologies de sécurité existant déjà (Cf. Bugyo), il est préférable de les appliquer sur notre graphique pour répondre aux besoins déjà existant des ingénieurs.

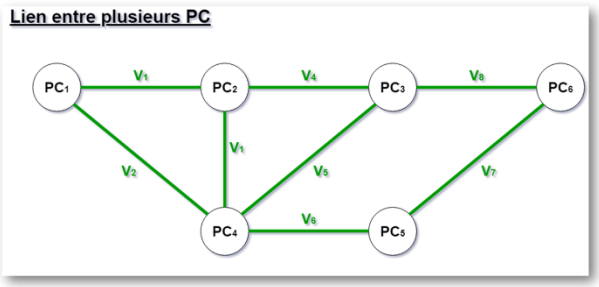
Les niveaux du modèle Phantom

- NIVEAU 0 : Optimisation
- NIVEAU 1 : Network
- NIVEAU 2 : Context
- NIVEAU 3 SB : Scenario BLUE : Defense Policy
- NIVEAU 3 SR : Scenario RED : Trying Attack

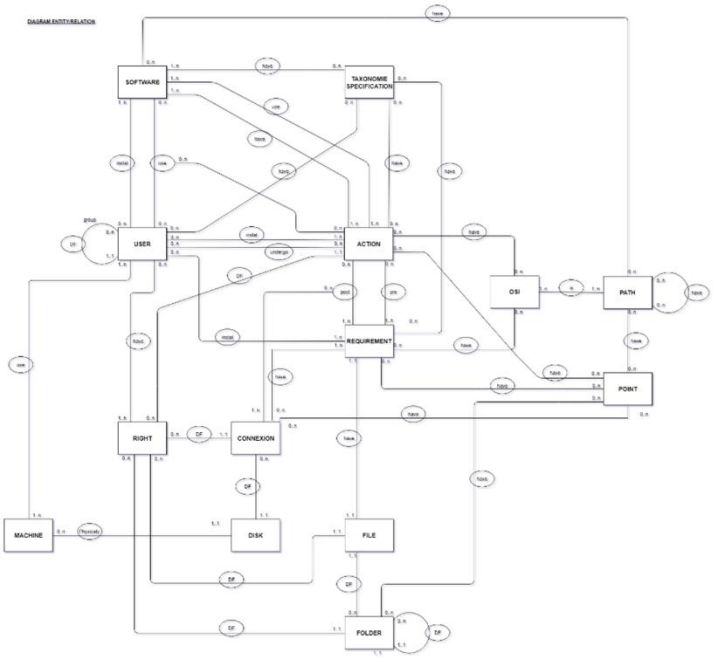
Représentation des différents modèles :



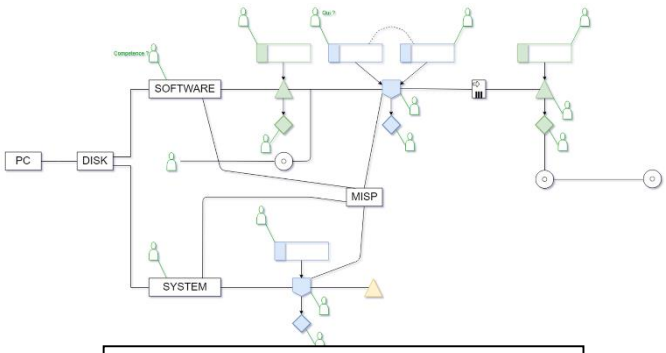
NIVEAU 0 : Optimisation



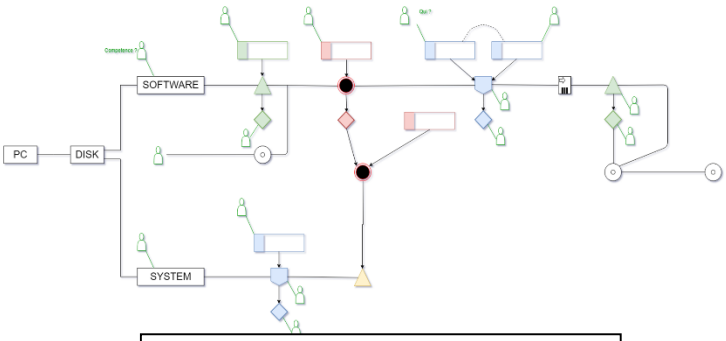
NIVEAU 1 : Network



NIVEAU 2 : Context



NIVEAU 3 SB



NIVEAU 3 SR

Le graphique général se découpe ainsi en plusieurs sous couches, chacune d'elles détenant sa propre utilité.

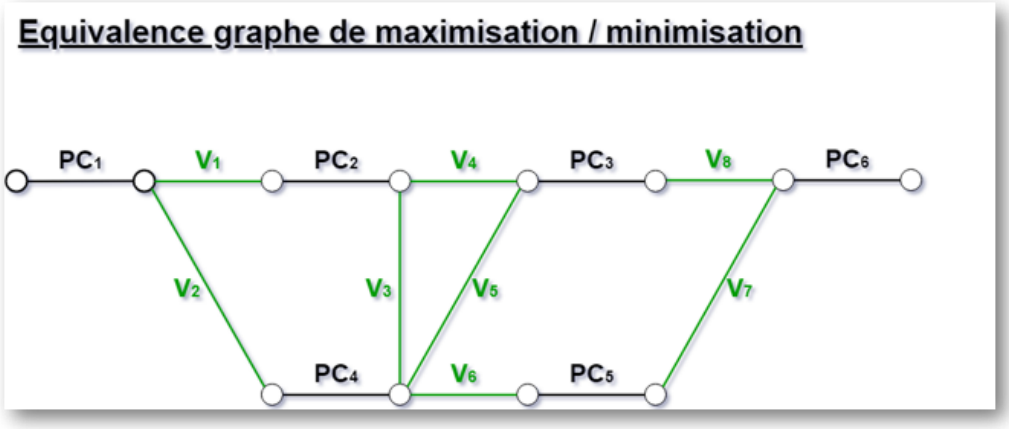
Chaque couche N est dépendante de sa couche N+1, cette dernière étant un « zoom » de la couche précédente.

NIVEAU 0 : Optimisation

Définition du modèle

Représentation la plus haute des parties du graphique. Cette figure rend possible tous les différents calculs d'optimisation vu en cours avec Monsieur Nagih sur le logiciel Cplex dans le domaine des graphes d'attaques.

Représentation



Exemple d'une représentation graphique du niveau 0 partie Optimisation

Répond aux besoins

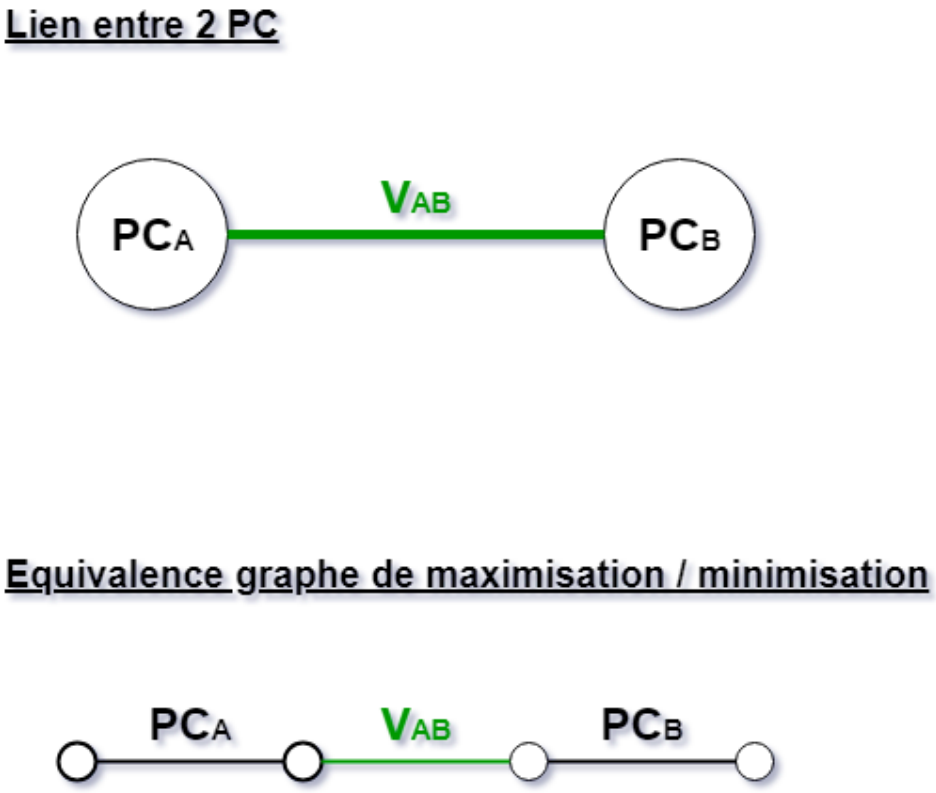
Ce graphique étant compatible pour une modélisation sur le logiciel Cplex d'IBM, ce dernier étant souvent utilisé dans le domaine de la sécurité, cette modélisation permettra notamment :

- Calculer leurs canaux de confiances
  - Exigence fonctionnelle FTP des critères communs
  - Pour connaître le niveau de confiance des différents chemins
    - Utilisation d'une notation établie dans les niveaux plus haut du graphique
      - Ratio d'attaque (fréquence d'attaque)
      - Dangerosité (Importance des CVE utilisés)
      - Vitesse d'attaque (moyenne de la vitesse d'attaque réussi du pc)
      - Ratio de confiance (calcul d'un GAP bugyo)
- Calculer les tolérances aux pannes, les coûts, l'allocation de ressources et la priorité des services
  - Exigence fonctionnelle FRU des critères communs
  - Le calcul des chemins bipartie permettant de connaître différents chemins de secours
- Calculer le niveau de criticité et d'importance d'un système
  - Coût du système dans le réseau (flux d'argent traité par ce système)
  - Point critique du réseau (calcul déterminé par Cplex)

Passage du niveau 0 au niveau 1 et inversement

Cplex ne permettant pas de gérer des graphiques avec des sommets disposant d'attributs, il convient de passer d'une modélisation à sommets pondérés à une modélisation avec arcs pondérés.

La réalisation de cette modification se présentera comme sur l'image ci-dessous



PC_A et PC_B sont des ratios, notations et attributs octroyés à un pc donné via le nouveau supérieur du graphique ou donné arbitrairement par l'utilisateur du graphique.

Note : Chacun des PCs gardera ses attributs quelques soit le niveau du graphique en cours.

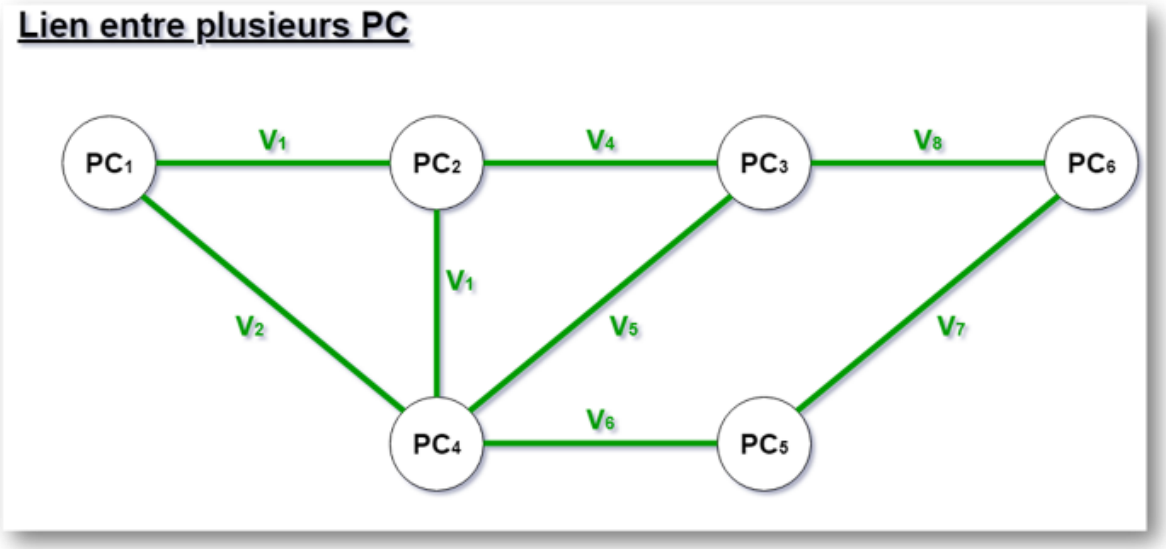
V_{AB} sera la vitesse de connexion entre 2 PC du réseau, permettant ainsi les calculs de débit.

NIVEAU 1 : Network

Définition du modèle

Modèle présentant les interconnexions entre les différents PC du réseau

Représentation



Répond aux besoins

Permet d'avoir la carte du réseau dévoilant les différentes connexions des PCs entre eux.

- Cette carte permet de savoir quel pc répond favorablement ou défavorablement à la politique de sécurité de l'entreprise
  - Permettra pour l'assurance sécurité de savoir si tous les systèmes sont à jour au niveau de leur politique de sécurité.
- Permet de savoir quel pc réviser et éviter dans le réseau lors du passage d'informations sensibles

Permet le monitoring dynamique des PCs

- Répond aux besoins de sécurité de la méthodologie Bugyo
  - Permettra de savoir quel système est sensible à des attaques

NIVEAU 2 : Context

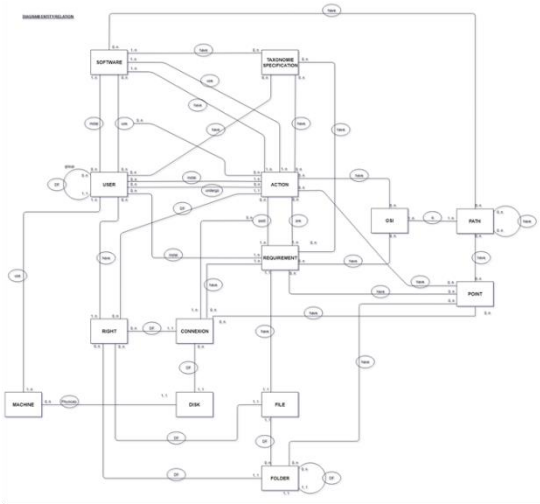
Définition du modèle

Pour définir l'intégralité du contexte d'une infrastructure un schéma SQL a été réalisé.

La nécessité d'utiliser MISP comme base de données principale obligera une conversion de ce schéma dans le format de données propre à MISP.

Toutefois ce format étant relativement proche de SQL, cette conversion pourra se faire aisément. Cependant, il reste à trouver une formalisation de cette conversion pour faciliter les modifications future .

Représentation [Cf. Annexe 1]



Répond aux besoins

Ce schéma a pour but de décrire le fonctionnement d'une infrastructure d'un système sans omettre de données.

La liste des utilisateurs ainsi que leurs droits et rôles dans le système répond favorablement aux exigences fonctionnelles des critères communs suivant :

- FDP : Manipulation des données de l'utilisateur
  - Connaissant les droits des utilisateurs sur les fichiers, il est possible de savoir qui peut les modifier
- FIA : Identifier, authentifier et gérer les droits d'accès

Le logiciel MISP disposant de normes différentes, propre à lui-même, il est impossible de faire un schéma de généralisation directement traduit en MISP, car de connaissances, aucunes normes schématiques n'ont été établie pour ça, le passage par un schéma SQL pour retraduction en MISP a donc été obligatoire dans cette étape.

NIVEAU 3 : Standardisation

Introduction des types de graphiques

Ce niveau est celui qui se rapproche le plus du graphique d'attaque Mulval.

Il se présente en 2 catégories :

- NIVEAU 3 SB : Scenario BLUE : Defense Policy
- NIVEAU 3 SR : Scenario RED : Trying Attack

L'une présentant la politique de défense d'un logiciel installé sur le système étudié. L'autre présentant les différentes attaques possible sur le logiciel et/ou système.

Les axiomes

Comme dans le graphique Mulval, pour qu'une action se fasse il lui faut des axiomes en prérequis.

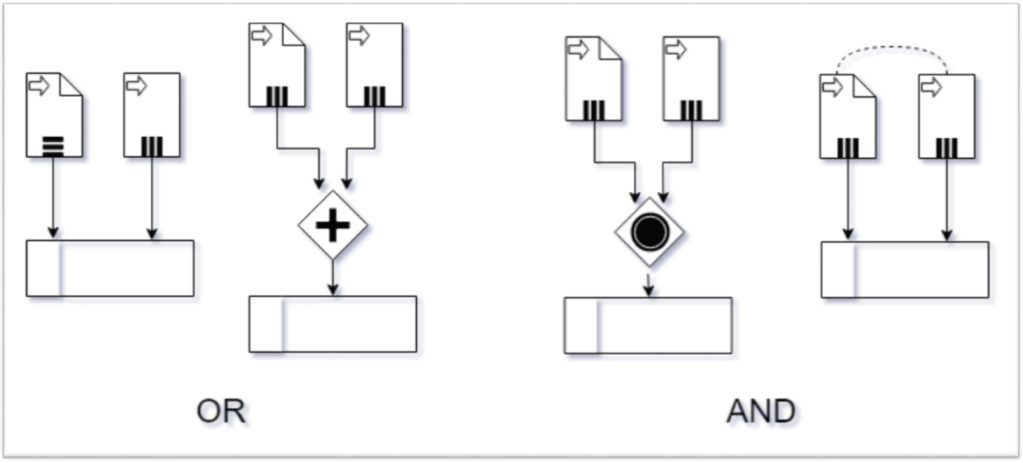
Un axiome dépendra :

- Soit d'un ou plusieurs fichiers atteignables sur le système
- Soit nécessitera obligatoirement la présence d'une série de fichiers

Règles logique d'un axiome

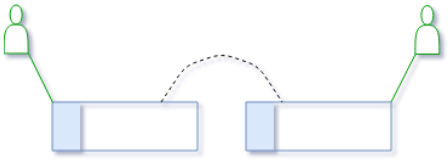
Si un axiome nécessite 2 fichiers :

- Dans le cas du OR, la compromission d'un seul fichier n'entravera en rien l'axiome impacté
  - Tous les fichiers doivent être impacté pour annuler l'axiome (OU logique)
- Dans le cas du AND, la compromission d'un seul fichier entravera l'axiome impacté
  - Un seul fichier entravé impactera l'axiome (ET logique)

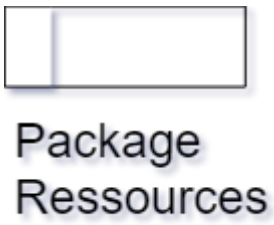


Note :

Ces portes OR et AND logique peuvent aussi être utilisées avec l'utilisation de ces mêmes axiomes.

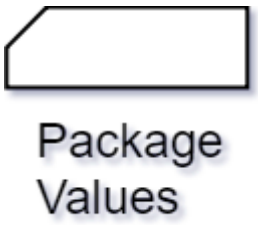


Les types d'axiomes



Les axiomes Ressources : Les Packages de Ressources

Représente tout axiome nécessaire au bon fonctionnement d'une action quelconque.



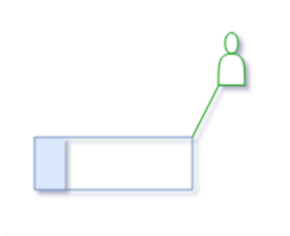
Les axiomes Values : Les Packages de valeur

Représente une ou plusieurs données de valeur à protéger.

Disposera d'une notation évaluant la valeur du package

Est l'une des raisons d'être de la défense.

Contenant d'un axiome

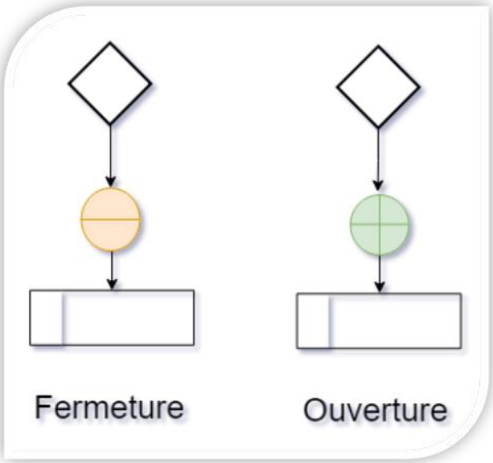


Un axiome contiendra

- Celui qui l'a mis en place (dernier à l'avoir configuré)
- Les compétences recommandées pour le mettre en place

Les interactions possibles entre axiomes

Il peut arriver que des axiomes aient à interagir entre eux, nous discernons 2 catégories d'actions possible :



- La fermeture : Neutralisation de l'axiome concerné
- L'ouverture : Activation de l'axiome concerné

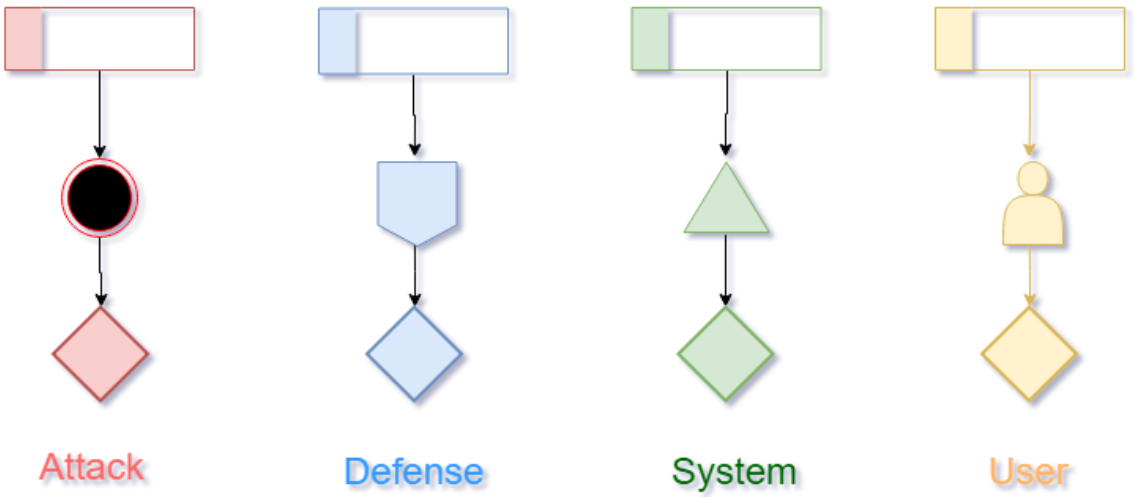
Un axiome neutralisé ne pourra plus servir à une action.

Un axiome activé sera lui susceptible d'activé l'action reliée à lui.

Ces interactions ne sont pas des actions à part entière, elles ont besoins d'actions pour se déclencher.

Les types d'actions possibles

Chacune de ces actions à au moins besoin d'un ou plusieurs axiomes pour fonctionner.
Si une défense est effective, elle pourra activer un ou plusieurs effets qui seront eux aussi des axiomes.



Attack

- Représente une action de l'attaquant :
  - Virus
  - Exploit
  - Malware

Defense

- Représente une action de la défense :
  - Contre mesure
  - Mise à jour
  - Patch

System

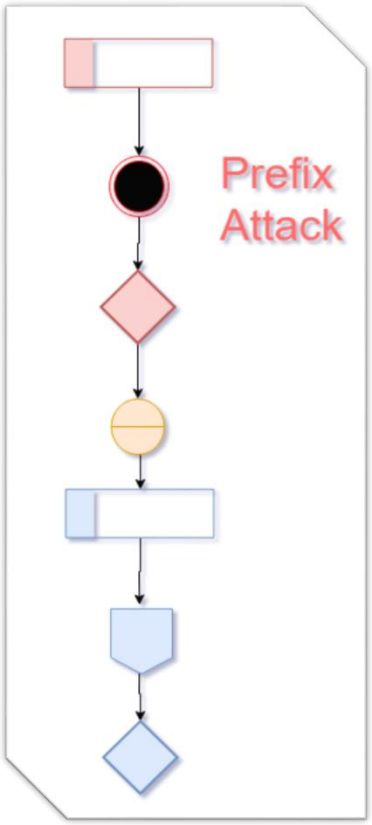
- Représente une action de la défense :
  - Routine
  - Action d'un programme

User

- Représente d'une action utilisateur :
  - Lancement d'un programme
  - Commande Shell
  - Est un utilisateur autorisé ou non du système

Exemples de tactiques d'attaque sur une défense

Les attaques Préfixées



Les attaques préfixées vont s'attaquer aux axiomes composants une action à annuler.

Elles vont pour ainsi dire « saboter » ce qui compose l'axiome.

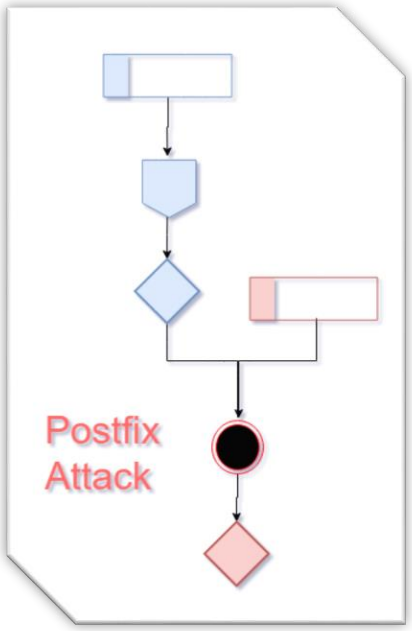
Une défense ne disposant plus d'assez d'axiomes pour se lancer sera considérée comme brisée.

Une défense une fois brisée est considérée comme nulle. Elle pourra être dépassée par l'attaquant sans activer aucuns de ses effets.

Exemple :

Sabotage d'un fichier indispensable au bon fonctionnement d'un anti-virus

Les attaques Postfixées



Les attaques postfixées d'une défense vont s'attaquer aux effets de cette même défense.

L'attaque va utiliser les effets d'une défense pour s'activer et/ou annuler les effets défensifs.

Exemple :

Faire en sorte qu'un fichier système reçoivent du code malicieux pour qu'il soit supprimé par la défense.

Les actionneurs système

Est considéré comme actionneur tout objet du système disposant d'un environnement.

Un environnement est composé d'un ou plusieurs path.

Le PATH d'un actionneur

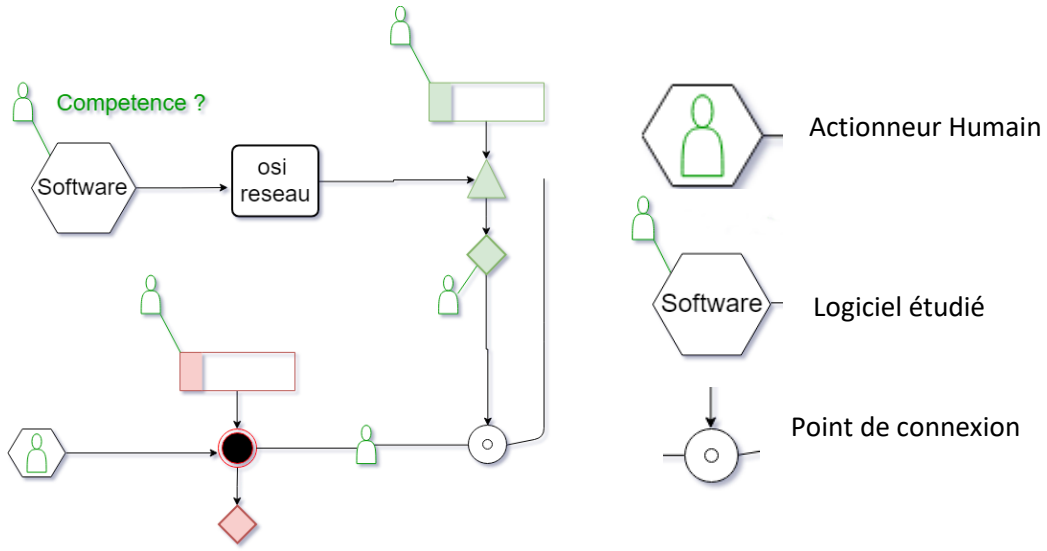
Un path est un chemin à travers l'actionneur.

Son premier élément décrit le type de path traversé (décrit la couche OSI traversée par le path).

Si aucun type n'est décrit, un seul type de path est admis par l'actionneur.

Le chemin path est une variable d'environnement dévoilant les possibilités d'action d'un utilisateur sur un système à partir d'un point de connexion.

Un point de connexion peut être lancé par une action et relié à un path :



Sauf indication contraire (défense, conteneur), un path n'est pas cloisonné au seul programme visité. Une attaque pourra utiliser un programme pour en attaquer un autre, comme le système.

Un path au départ d'un actionneur :

- Utilisateur :
  - Social engineering
  - Erreur humaine (paresse, méprise d'une politique de sécurité)
- Programme :
  - Possibilité d'actions au travers d'un programme
- Système :
  - Recherche de privilèges

Attention :

On distinguera l'arborescence des fichiers du PATH. De ce fait, un fichier ne pourra pas être sur le PATH.

Un path ne contiendra que des actions ; leurs packages et des points de connexion.

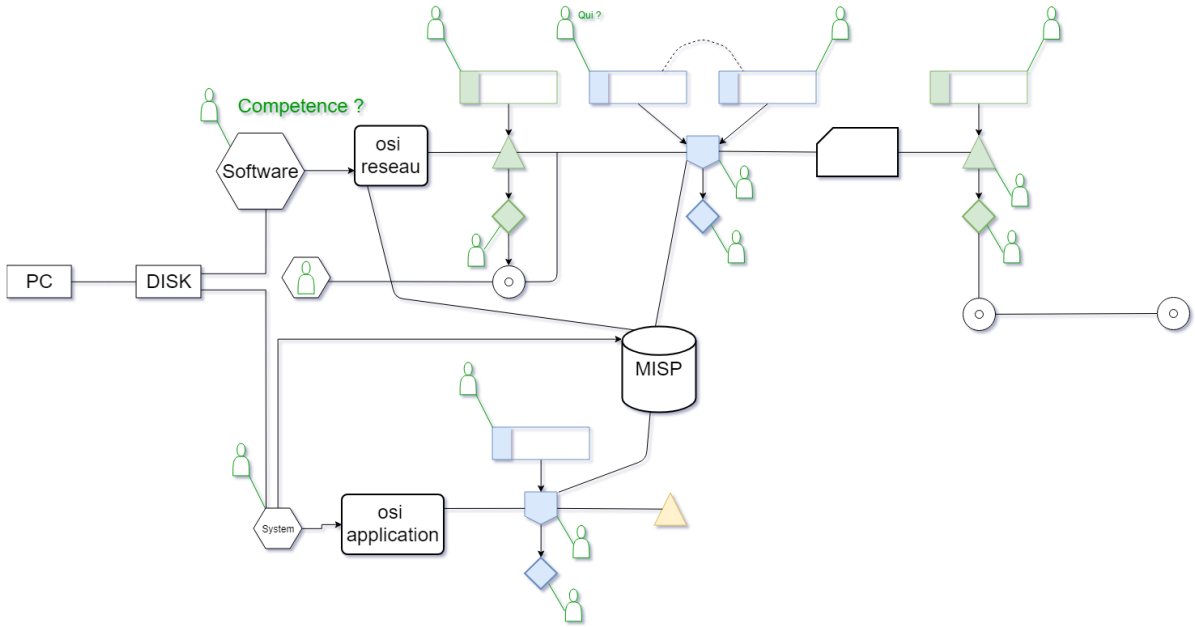
NIVEAU 3 SB : Scenario BLUE : Defense Policy

Définition du modèle

Ce niveau servira à mettre en place la politique de sécurité du système.

Ici, seule la défense du système sera représentée.

Représentation [Cf. Annexe 2]



Répond aux besoins

Peut présenter une description détaillée des composants d'une infrastructure ainsi que son environnement de fonctionnement et ses exigences de sécurité du produit.

- Nécessaire pour une certification des critères communs

La description détaillé d'un graphique de défense répond favorablement aux critères communs :

Exigence fonctionnelle :

- FMT : Administration de la sécurité
- FPT : Exige une sécurisation de la connexion de l'utilisateur à son produit.
- TOE FPT : Double de la FPT, exige une sécurisation de la connexion de l'entreprise
- FTA : Contrôle l'établissement d'une connexion de l'utilisateur

La connexion au serveur MISP permettra de générer dynamiquement le graphique le plus sécurisé si un partage de la meilleure défense évaluée est fait pour le logiciel étudié.

Sera utilisé comme graphique template pour le niveau 3 SR, différents scénarios d'attaque qui pourront ainsi être appliqués sur une même défense.

NIVEAU 3 SR : Scenario RED : Trying Attack

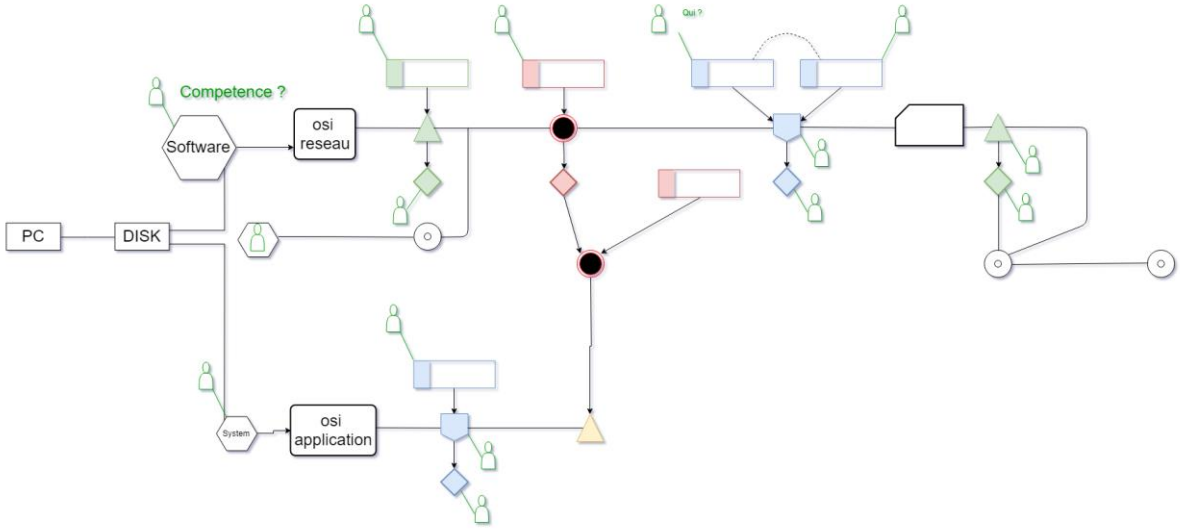
Définition du modèle

Utilisera la partie défense comme template pour lancer différents scénarios d'attaques.

L'attaquant cherchera

- Soit à prendre le triangle du système général (privilege escalation)
- Soit à voler les données du programme.

Représentation [Cf. Annexe 3 / 4]



Répond aux besoins

Le fait de pouvoir exécuter un nombre infinis d'attaques en continu sur un même système, répond quasiment aux exigences des critères communs de l'assurance sécurité d'un point de vue infrastructure :

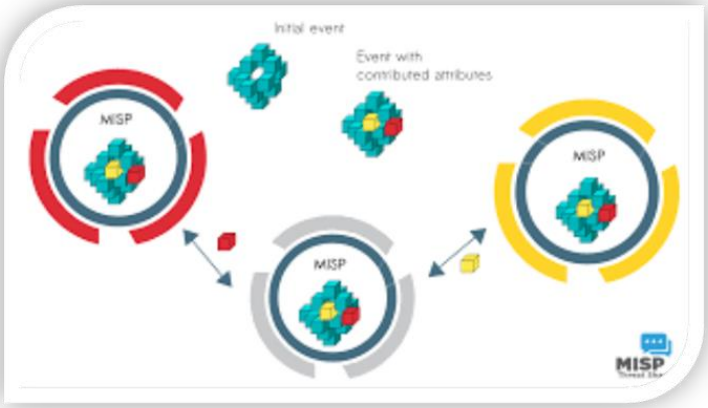
- ADV : Spécification du programme jusqu'à son implémentation
  - Décrit les actions et l'environnement d'un programme
- ACO : Respect de la sécurité avec les fonctions systèmes
  - Permet de voir si le système est impacté ou non
- AGD : Documentation complète permettant d'utiliser efficacement la sécurité
  - C'est une documentation à part entière en plus d'un graphique
- APE : S'assure que le profil de protection est complet
  - Les multiples attaques peuvent permettre de discerner une faille
- ASE : Démontre que l'évaluation de la cible est saine techniquement
  - Si toute attaque lancée échoue, la cible peut être considérée comme sûre
- ATE : Test détaillé et complet
  - Seule manque la partie sur les datas répondant à la partie infrastructures
- AVA : Identification des vulnérabilités lors des phases de développement/ configuration / exploitation
  - Seule manque la partie exploitation des données répondant favorablement à la partie développement et configuration

Les besoins pour les professionnels

Le graphique d’attaque rouge peut servir aux pentesters pour expliquer clairement et en détail leurs façons de procéder pour attaquer la structure défensive du réseau.

Le graphique d’attaque bleu sera très utile en forensic pour aider les ingénieurs à identifier les défenses et l’infrastructure du système tombé. Ce qui leur permettra de reconnaître les failles probablement exploitées.

L’utilisation de MISP



MISP est un logiciel open source favorisant le partage des données entre ses différentes instances.

Un graphe PHANTOM sur une instance privée MISP d’une entreprise

On peut imaginer une entreprise mettant l’intégralité de son infrastructure sur une instance MISP d’une zone DMZ cryptée.

Note : ces données pouvant être à caractère critique, le partage complet de l’infrastructure est à éviter

Elle pourra à sa guise partager les attaques trouvées sur tel logiciel et/ou ses contre-mesure prise.

Ainsi un logiciel, sera de plus en plus détaillé de façon :

- Défensive : Contre-mesure partagée à l’ensemble de la communauté
- Offensive : Attaque / Faille trouvée et partagée à l’ensemble de la communauté

Une IA sur MISP ?

Avec ces paramètres cités plus haut, une IA pourra identifier les attaques les plus fréquemment utilisées pour un logiciel donné et ainsi déduire le meilleur schéma d’attaque et de défense de tel ou tel logiciel.

To be continued:

Ce modèle nécessite-t-il des améliorations? Oui, des modifications sont encore nécessaires pour s'approcher de l'objectif fixé.

Modification Future probable:

Le graphe PHANTOM est un graphique Orienté Infrastructure :

- Il n'est donc pas assez orienté Service.
- Il n'a pas de modélisation de traitement de données.

NIVEAU 0 : Optimisation

- Nécessite une bonne compréhension dans le domaine de l'optimisation des graphes d'attaques sur le logiciel Cplex enseigné par Monsieur Nagih à l'UFR MIM.

NIVEAU 1 : Network

- Nécessite de déduire exactement les différents ratios à traiter dynamiquement par le graphe.

NIVEAU 2 : Context

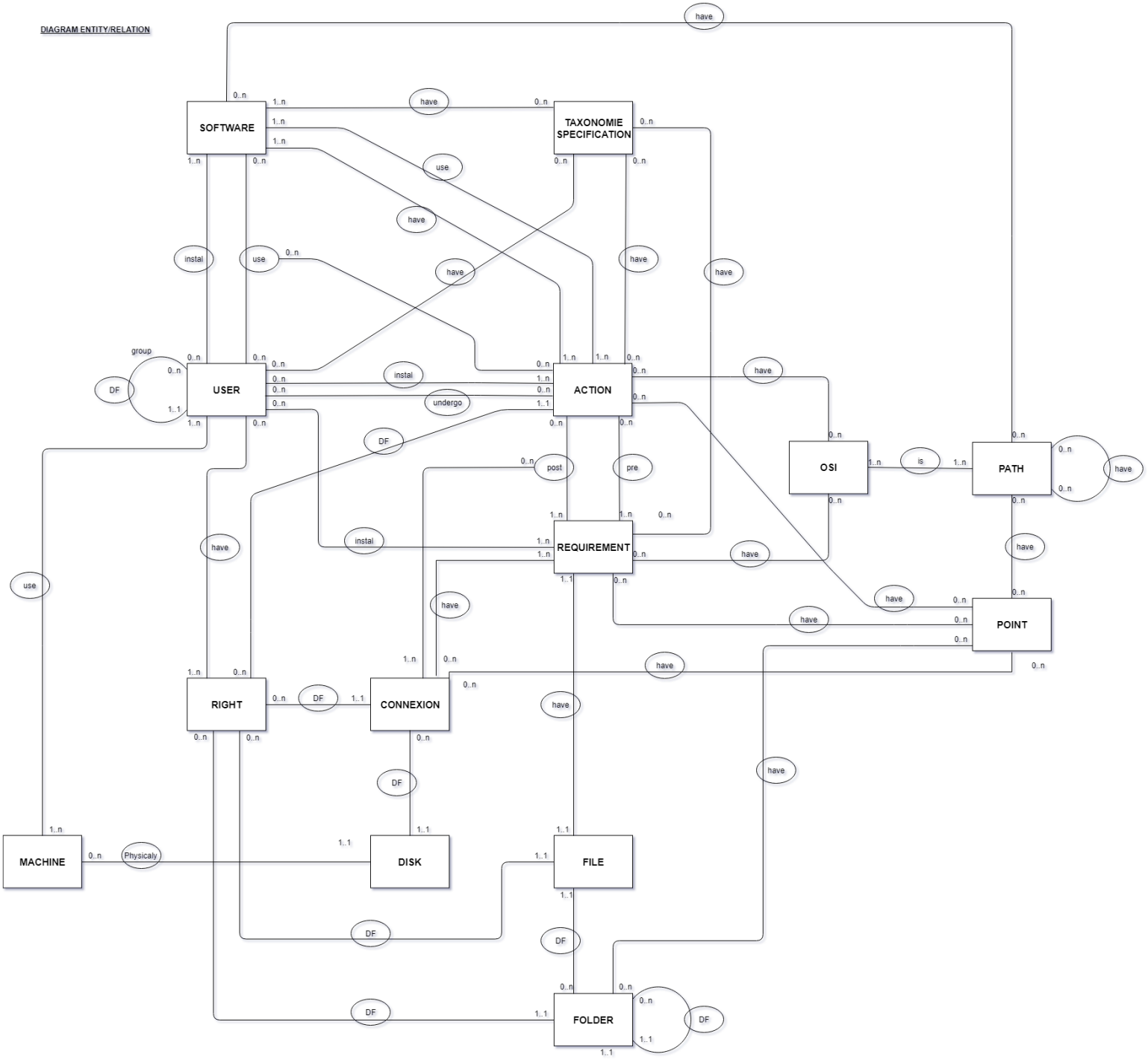
- Nécessite plus d'abstraction pour gérer plus de problèmes génériques pouvant correspondre à la forme de notre graphique.
- Une plus grande abstraction simplifierait sa mise en place dans MISP.

NIVEAU 3 SB : Scenario BLUE : Defense Policy / SR : Scenario RED : Trying Attack

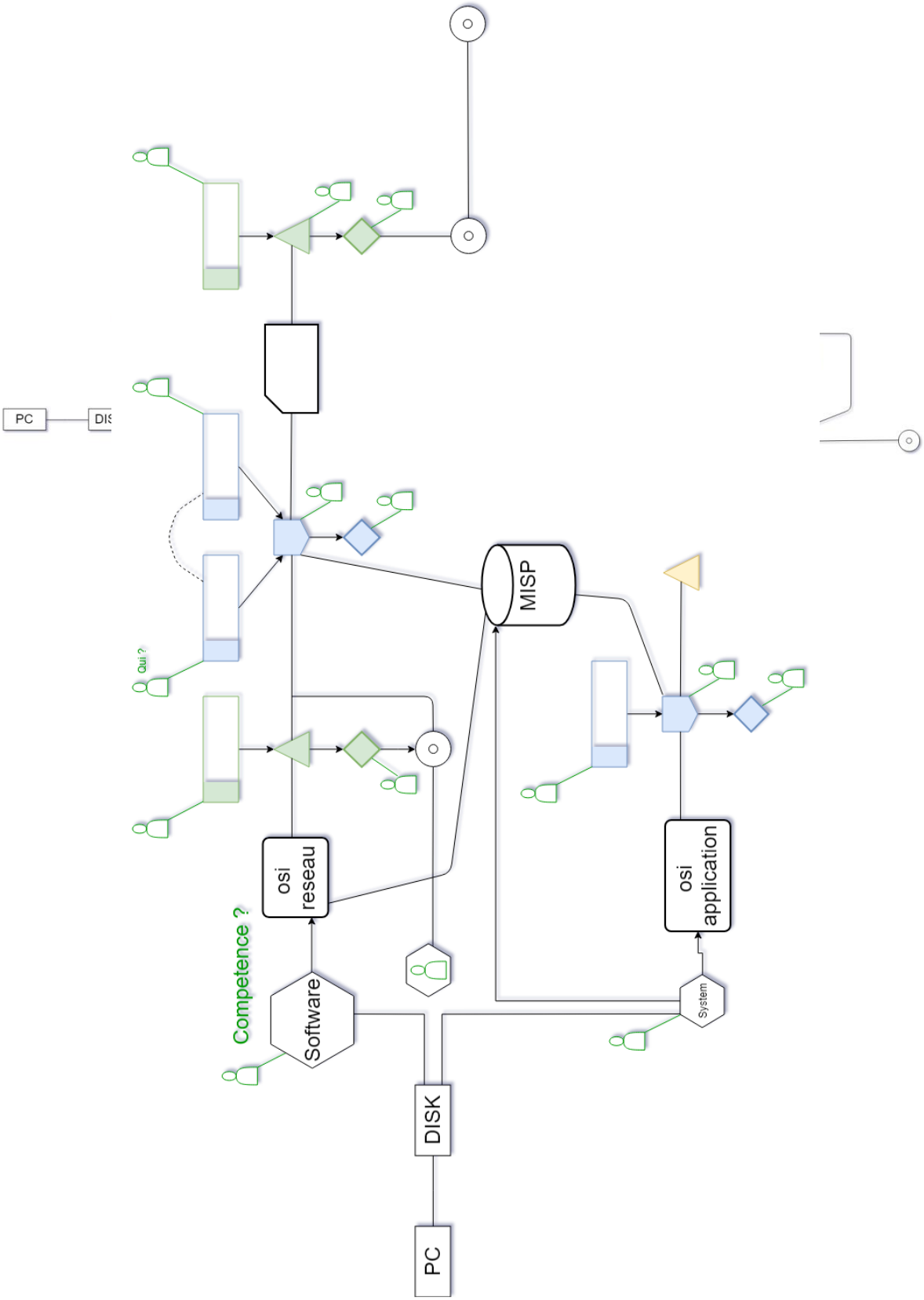
- La standardisation est à réévaluer avec des experts du domaine.
- Reste à formaliser en détail les conteneurs et actionneurs pour l'abstraction de la partie 2.
- Les points de connexion et leurs détections dans le système sont à revoir (Nmap).
- Les attaques « parasites » sont en cours de recherches (attaque installant un rootkit / virus) de façon permanent sur le système tombé et l'utilisant.
- L'ordonnancement des actions entre elles peut poser quelques problèmes à l'activation / désactivation d'un même axiome

Annexes

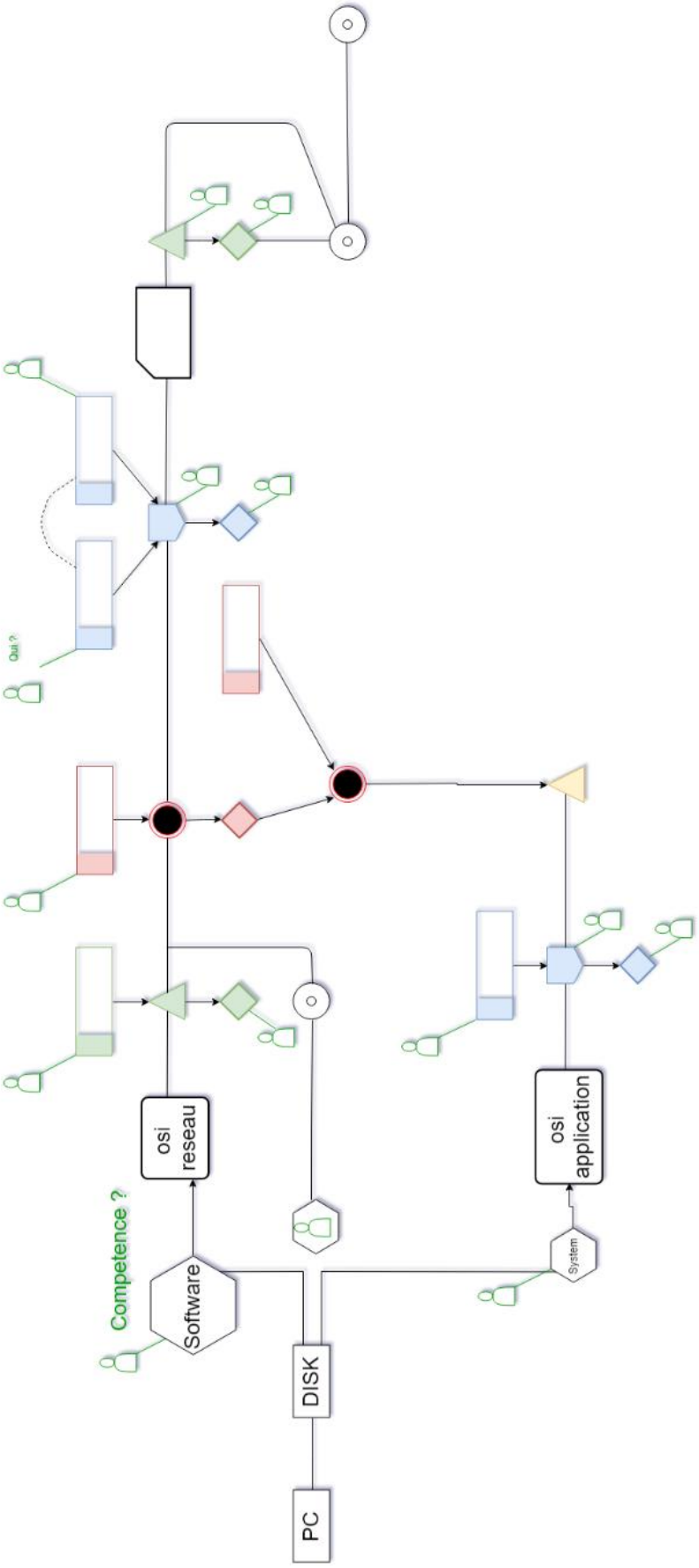
ANNEXE 1 : Schéma SQL : Entité / Relation



ANNEXE 2 : Niveau 3 : SB : Exemple d’un schéma de défense :



ANNEXE 3 : Niveau 3 : SR : Exemple 1 d’un schéma d’attaque :



ANNEXE 4 : Niveau 3 : SR : Exemple 2 d’un schéma d’attaque :