# Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense

Philippe Lagadec
Philippe.Lagadec(@)nc3a.nato.int

NATO C3 Agency

**Résumé** Cet article présente deux projets de recherche et développement de l'agence NC3A de l'OTAN dans le domaine de la cyber-défense, CIAP (Consolidated Information Assurance Picture) et DRA (Dynamic Risk Assessment). La cyber-défense est aujourd'hui principalement basée sur les outils suivants : systèmes de détection d'intrusion (IDS), scanners de vulnérabilités, antivirus ainsi que systèmes de gestion et corrélation d'événements sécurité (SIEM). Lorsqu'il s'agit de superviser un système informatique à grande échelle réparti sur plusieurs sites, il devient vite très difficile de corréler et analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents suffisamment vite pour réagir efficacement. Cette complexité est due à la quantité d'information générée, au manque d'interopérabilité entre les outils ainsi qu'à leurs lacunes en matière de visualisation.

Le projet CIAP vise à pallier ce manque en étudiant comment toute l'information nécessaire à la cyber-défense peut être consolidée dans un système complet, reposant sur un modèle de donnée commun s'appuyant sur des standards et sur un système de stockage distribué. CIAP fournit également diverses visualisations complémentaires de toutes les données collectées, notamment des vues d'ensemble de la topologie réseau et des vues géographiques.

Un autre problème majeur en cyber-défense est que la tâche de comprendre l'impact réel d'une vulnérabilité ou d'une alerte IDS est généralement dévolue à un analyste humain, qui doit lui- même faire le lien entre toutes les informations techniques et sa connaissance de tous les services ou processus qui dépendent des machines concernées. Le projet DRA est une étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l'impact réel dû à la situation sécurité globale du système et du réseau. Le prototype DRA utilise des outils de génération automatique de graphes d'attaque afin de déterminer quelles vulnérabilités sont réellement exploitables par un attaquant compte tenu de l'architecture du système. Il détermine ensuite en temps réel quels sont les risques induits sur les biens, services et missions de l'organisation, afin de mieux gérer les priorités et suggérer des réponses adaptées.

## 1 Introduction

Cet article présente deux projets de recherche et développement de l'agence NC3A de l'OTAN dans le domaine de la cyber-défense, CIAP (Consolidated Information Assurance Picture) et DRA (Dynamic Risk Assessment). Aujourd'hui les systèmes et réseaux informatiques sont devenus de plus en plus critiques pour de très nombreuses activités, notamment pour la plupart des entreprises et des organisations comme l'OTAN. Cependant, même avec des protections de plus en plus efficaces et des politiques de sécurité bien définies, des incidents et des cyber-attaques se produisent tous les jours. CIAP et DRA visent à pallier certains manques des produits de sécurité actuellement disponibles sur le marché afin d'améliorer les capacités de cyber-défense d'une organisation comme l'OTAN et des Nations qui la composent.

## 2 Cyber-Défense – Les manques des outils actuels

La cyber-défense (ou LID - Lutte Informatique Défensive), qui correspond aux aspects dynamiques et temps réel de la sécurité informatique pour pouvoir détecter les attaques et se défendre, est basée sur de nombreux outils et produits de sécurité comme les systèmes de détection d'intrusion (IDS), les outils de scan de vulnérabilités, les antivirus ainsi que les systèmes de gestion et corrélation d'événements sécurité (SIEM – Security Information and Events Management). Ces outils, bien que très efficaces chacun dans leur domaine, produisent énormément d'informations très techniques, qui requièrent souvent des experts pour pouvoir analyser et exploiter tous leurs résultats. De plus, la plupart de ces outils n'ont pas été conçus pour être interopérables, et leurs résultats sont souvent uniquement destinés à être lus et analysés par un opérateur humain. Lorsqu'il s'agit de superviser un système informatique à grande échelle réparti sur plusieurs sites, il devient donc très difficile de corréler et analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents suffisamment vite pour réagir efficacement. Cette complexité est due à la quantité d'information générée, ainsi qu'à l'hétérogénéité des formats employés.

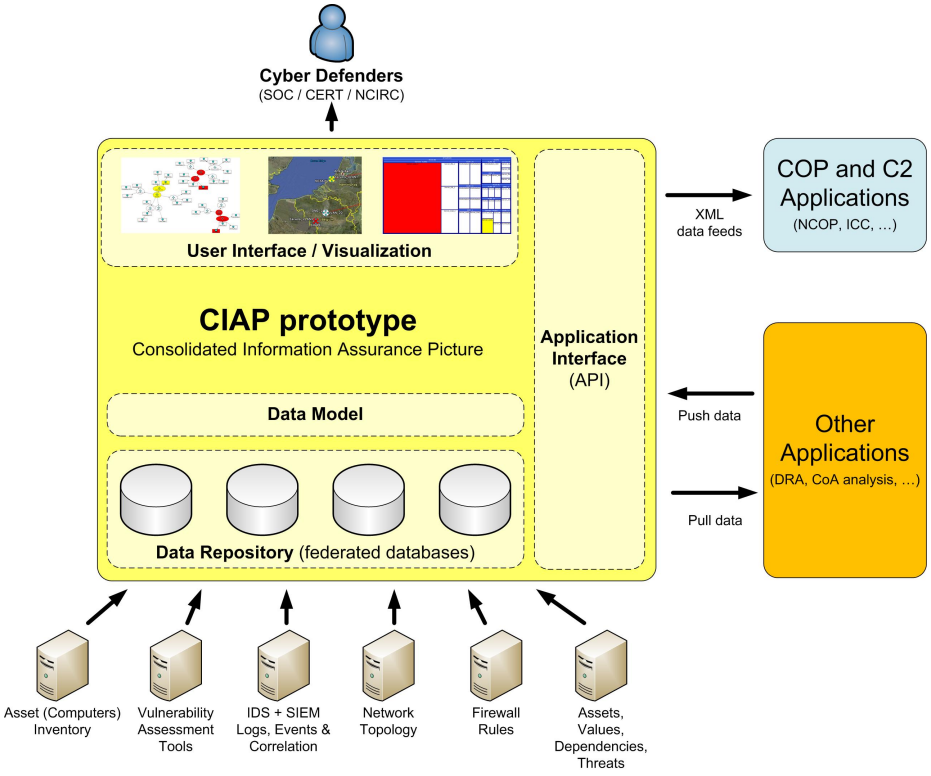
Une autre faiblesse des produits de sécurité actuels est la visualisation de ces informations : par exemple même les outils de corrélation d'événements et de scan de vulnérabilités les plus coûteux ne sont pas encore capables de visualiser leurs résultats sur une carte du réseau afin de fournir une vue d'ensemble de la situation. Il existe aujourd'hui un nombre croissant d'outils utilisables en cyber-défense pour la visualisation (cf. [2,1]), cependant ceux-ci sont pour la plupart destinés à analyser graphiquement le trafic réseau ou un grand nombre d'événements pour y détecter des anomalies ou des tendances. L'emploi de la visualisation pour obtenir une vue d'ensemble de la situation (vulnérabilités, alertes, incidents) est encore peu développé.

Un troisième problème majeur en cyber-défense est que chaque outil de détection ou de supervision ne fournit que des résultats partiels et relativement bas niveau concernant l'infrastructure informatique et réseau. La tâche de comprendre l'impact réel d'une vulnérabilité ou d'une alerte IDS est généralement dévolue à un analyste humain, qui doit lui- même faire le lien entre toutes les informations techniques et sa connaissance de tous les services ou processus qui dépendent des machines concernées. Il est donc nécessaire de développer de nouveaux outils d'analyse de risque dynamique, avec une vue plus globale du problème.

Les projets CIAP et DRA ont pour but d'étudier diverses solutions possibles pour remédier à ces lacunes.

## 3 CIAP – Consolidation et Visualisation

Le projet CIAP (Consolidated Information Assurance Picture) vise à pallier certains manques des produits actuels en étudiant comment toute l'information nécessaire à la cyber-défense peut être consolidée dans un système complet, reposant sur un modèle de donnée commun s'appuyant sur des standards (en partenariat avec MITRE) et sur un système de stockage distribué. CIAP fournit également diverses visualisations complémentaires de toutes les données collectées, notamment des vues d'ensemble de la topologie réseau et des vues géographiques. Un prototype a été développé depuis 2007 en intégrant divers outils comme Nessus, OVALdi et ArcSight ESM, et testé dans des conditions réelles.




## 3.1 Un modèle de données commun

La fonction principale de CIAP est de consolider toutes les informations disponibles relatives à la sécurité du système dans un modèle de données cohérent, afin de pouvoir les analyser, les corréler et obtenir une vue globale de la sécurité. Comme la plupart des outils et produits de sécurité emploient tous des modèles de données différents, il est indispensable de normaliser l'information.

Le modèle de données de CIAP contient entre autres les informations suivantes :

- ordinateurs, équipements réseau, imprimantes, ... (Hosts / Computer assets)
- comptes utilisateur (User accounts)
- applications installées (Installed software)
- processus tournant sur chaque ordinateur (Processes)
- ports ouverts (Open ports)

- vulnérabilités détectées sur chaque ordinateur (Vulnerability instances)
- informations génériques sur chaque vulnérabilité, en provenance de bases comme CVE et NVD (Vulnerability information)
- événements, logs (Events)
- état de sécurité de chaque ordinateur, résultat de la corrélation d'événements d'un SIEM ou d'un IDS (Security status)
- tickets d'incidents (Incidents)
- topologie réseau : réseaux et sous-réseaux, organisés hiérarchiquement (Subnets)
- politique de sécurité du réseau (Firewall rules)
- données pour l'analyse de risque : biens, valeurs, dépendances, menaces (Assets, values, dependencies, threats)

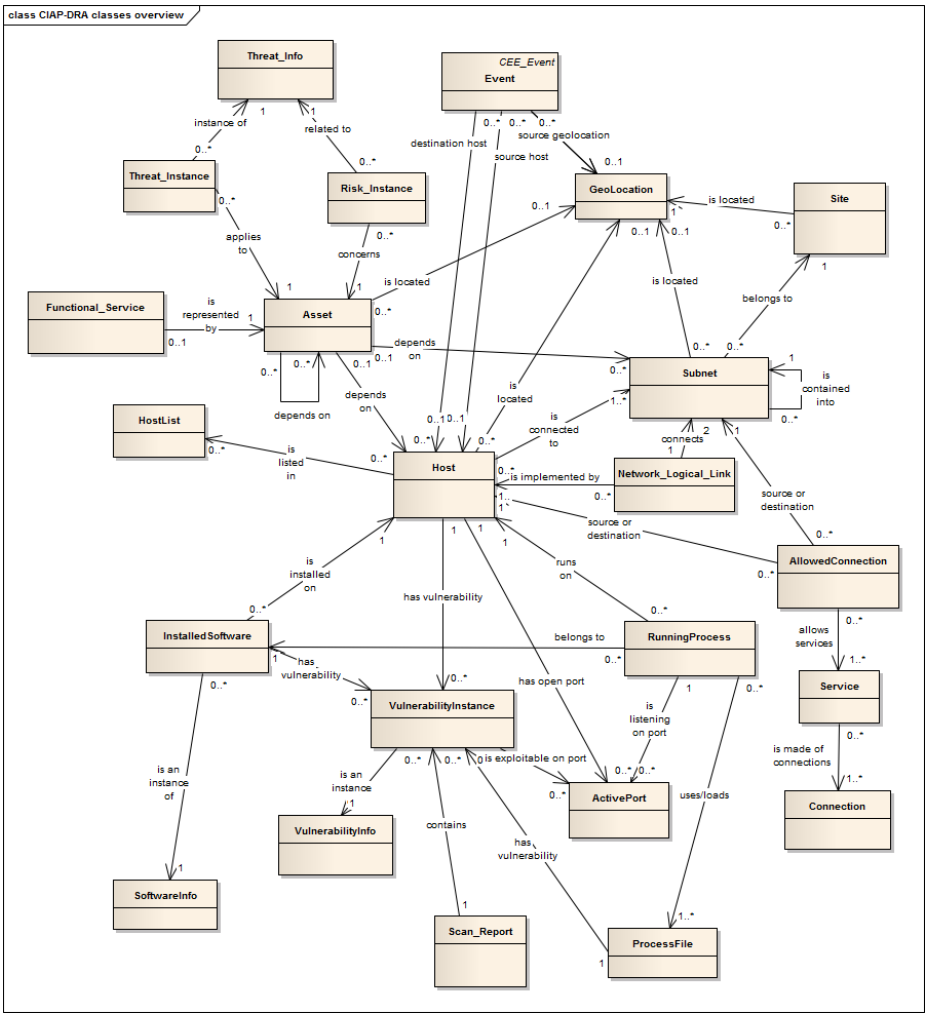
La figure 3.1 montre un aperçu du modèle de données de CIAP.

Dans son principe et les entités qu'il couvre, le modèle de données de CIAP est proche de diverses autres initiatives comme M4D4 [3], NetD (Network Defence) aux Etats-Unis et JNDMS (Joint Network Defence and Management System) au Canada. CIAP évoluera dans le futur pour améliorer son interopérabilité avec ces modèles.

### 3.2 Formats standards pour la cyber-défense

Quand cela est possible, le modèle de données de CIAP utilise ou s'inspire des formats standards ou existants, afin d'être le plus intéropérable possible. Voici quelques formats supportés par la version actuelle de CIAP :

- CVE (Common Vulnerabilities and Exposures) : un identificateur commun pour réferencer les vulnérabilités. [15]
- NVD (National Vulnerability Database) : une base de données fournissant les caractéristiques principales de chaque vulnérabilité connue. [16]
- CPE (Common Platform Enumeration) : une syntaxe commune pour énumérer les versions de systèmes et d'applications. [18]
- OVAL (Open Vulnerability and Assessment Language) : un language pour spécifier les tests et fournir les résultats d'analyse de vulnérabilités. [27]




– KML (Keyhole Markup Language) et NVG (NATO Vector Graphics) : pour décrire des données géo-référencées. [24,23]

Dans le futur, plusieurs autres standards pourraient être mis à profit :

– CVSS (Common Vulnerability Scoring System) : un indice standard de sévérité pour les vulnérabilités. [17]
– CAPEC : pour décrire les étapes d'une attaque et donc potentiellement les éléments d'un graphe d'attaque. [20]
– CEE ou IDMEF : pour stocker les événements et alertes critiques. [33,34]

- CRE, ERD et CCE : pour recommander et stocker les réponses possibles à un incident ou une vulnérabilité. [25,26,19]
- CWE et MAEC : pour décrire les menaces, faiblesses potentielles et codes malicieux.[21,22]
- IODEF ou VerIS : pour décrire les incidents. [31,32]
- ISO 8601 : pour stocker les dates et heures de façon standard. [35]
- XCCDF : pour décrire des tests en complément d'OVAL. [29]

Il faut cependant noter que certains aspects du modèle de CIAP ne sont pas encore couverts par des standards existants, ou que ces standards ne fournissent pas forcément les entités et attributs adaptés aux besoins de CIAP. Par exemple, il existe de nombreux modèles pour décrire une architecture réseau comme le SID (Shared Information Data) du TM Forum ou bien CIM (Common Information Model), qui pourraient être considérés dans CIAP [5,4]. De même, la modélisation générique des règles de filtrage des pare-feu est un domaine ou aucun standard ne s'est encore imposé.

### 3.3 Intégration des outils existants

CIAP est conçu pour collecter des données fournies par diverses sources d'information :

Les informations sur les ordinateurs, processus, ports ouverts et applications installées sont croisées à partir d'outils de gestion de parc, d'agents locaux, d'outils de scan réseau (nmap), et peuvent être complétées manuellement si besoin.

La topologie réseau et les règles de pare-feu sont en général trop complexes pour être configurées manuellement. Un parseur de configuration de pare-feu a donc été développé afin de pouvoir extraire automatiquement les données nécessaires à CIAP.

Les vulnérabilités sont fournies par divers outils de scan. Le prototype CIAP actuel a été testé avec deux outils :

- Nessus, un scanner réseau
- OVALdi, un scanner local [28]

Dans le cas d'OVALdi, un agent a été déployé sur chaque poste surveillé pour lancer un scan de vulnérabilités toutes les 24h, et fournir les résultats au CIAP.

Les événements critiques et alertes générés par des sondes de détection d'intrusion sont centralisés et corrélés dans un SIEM. CIAP extrait les résultats de la corrélation pour en déduire l'état courant de sécurité des ordinateurs du système. Par exemple, le SIEM peut corréler plusieurs événements et en déduire qu'un serveur est compromis ou hostile.

CIAP est donc capable de maintenir à jour une vision complète du système en consolidant automatiquement toutes les sources de données disponibles.

### 3.4 Système de stockage fédéré

Bien qu'il soit possible de stocker toute l'information dans une seule base de données, il est plus efficace de tirer parti de toutes les bases de données déjà fournies par les outils de sécurité employés comme sources d'information. Lorsque cela est possible, les informations sont obtenues à la demande en requêtant les bases de données correspondantes : SIEM, outil de scan de vulnérabilités, outil de gestion de parc, etc... Cela permet d'éviter des informations redondantes et potentiellement désynchronisées.

### 3.5 Visualisation

Dans le domaine de la cyber-défense, la visualisation peut servir à deux objectifs différents :

1. Analyser visuellement une grande quantité de données pour y détecter des anomalies, activités suspectes ou des tendances.
2. Afficher graphiquement les données existantes pour obtenir une meilleure vue d'ensemble.

Le cas 1 est déjà couvert par de nombreux outils et publications (cf. [2,1]). CIAP concerne essentiellement le cas 2.

En tirant parti de toutes les données consolidées dans CIAP, il est possible de bâtir de nouvelles vues afin d'obtenir une meilleure perception globale de la situation.

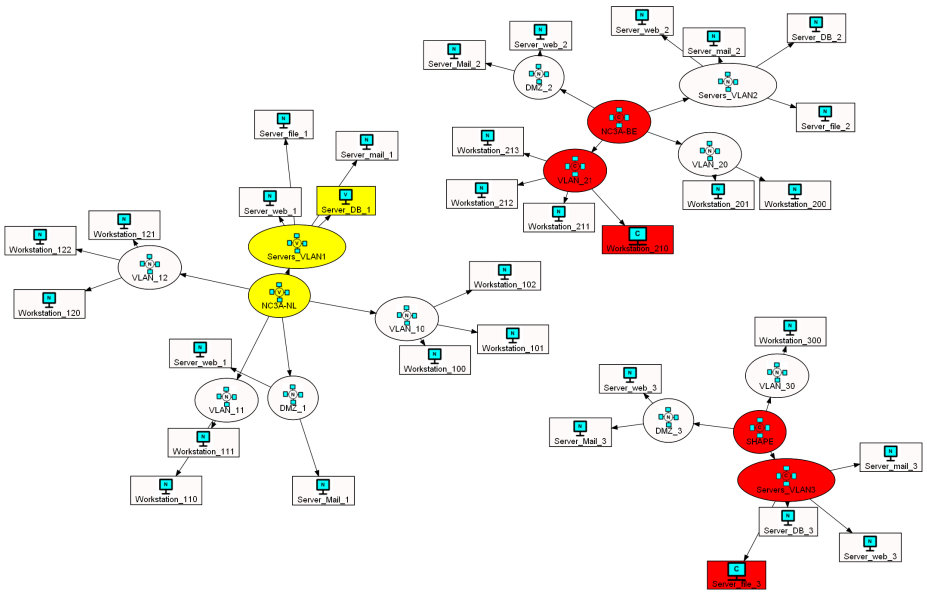
La principale métrique employée dans la version actuelle de CIAP est l'état de sécurité des postes et des réseaux, qui peut prendre quatre valeurs. Dans la plupart des vues développées pour le prototype, les couleurs suivantes sont employées pour ces quatre valeurs :

| Etat de sécurité | Couleur | Signification |
|---|---|---|
| Normal | Blanc | Aucune vulnérabilité ou attaque n'a été détectée |
| Vulnérable | Jaune | Des vulnérabilités ont été détectées, mais elles ne semblent pas exploitables par un attaquant (pas de chemin identifié dans le graphe d'attaque) |
| Exposé | Orange | Des vulnérabilités ont été détectées, et elles semblent exploitables par un attaquant (chemin identifié dans le graphe d'attaque) |
| Compromis | Rouge | Une attaque réussie a été détectée (alerte IDS ou corrélation d'événements), ou bien des informations montrent qu'un attaquant contrôle la machine. |

Ce jeu de couleurs initial est très simple et limité, cependant il permet déjà d'obtenir une bonne vue d'ensemble des principaux problèmes de sécurité remontés par les outils d'analyse de vulnérabilités et de détection d'intrusion.

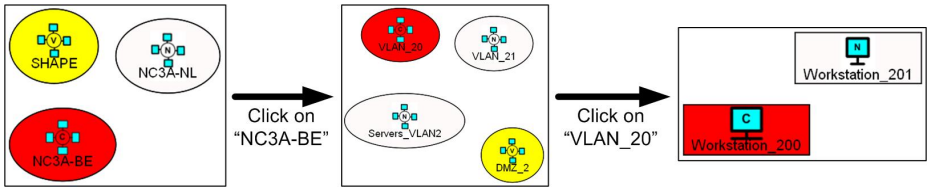
Diverses vues ont été expérimentées à partir de plusieurs outils, dont voici quelques exemples :

**Vue réseau à plat (GraphViz fdp)** Cette vue fournit un aperçu complet de l'organisation du réseau sous forme de graphe, et met en évidence les machines et sous-réseaux où des vulnérabilités ou des compromissions ont été détectés. Les fonctionnalités de GraphViz permettent de générer une image bitmap facilement utilisable dans une application web, avec la possibilité de cliquer sur chaque objet pour déplier/replier des branches du graphe ou bien pour obtenir des détails sur une machine.




Les tests menés avec GraphViz ont cependant montré que cet outil n'est pas adapté à la visualisation d'un réseau informatique de grande taille. Par exemple, le manque de fonctions "pan&zoom" efficaces rend difficile la navigation dans un grand graphe. De plus, les algorithmes de placement des nœuds du graphe aboutissent à des résultats complètement différents et aléatoires dès qu'un objet est ajouté ou retiré. D'autres outils et algorithmes seront testés dans les futures versions du prototype pour pallier ces problèmes.

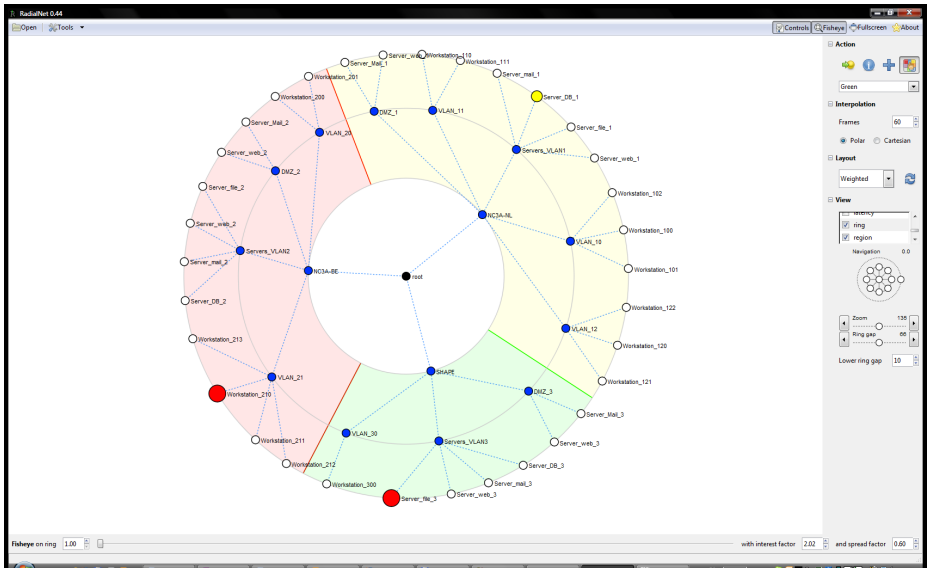
**Vue réseau hiérarchique (GraphViz)** Cette vue fournit également un aperçu du réseau, mais de façon plus compacte, en ne montrant qu'un niveau de sous-réseaux à la fois. La vue initiale montre les sous-réseaux de plus haut niveau. Si l'un de ces réseaux contient au moins une machine vulnérable ou compromise, il est mis en évidence avec la couleur correspondante. En cliquant sur un sous-réseau, il est possible de zoomer pour afficher les sous-réseaux et machines contenus à l'intérieur, et ainsi de suite.



Ce type de vue fournit de meilleurs résultats que la précédente pour l'affichage de réseaux de grande taille. Cependant, là-aussi le placement des objets est aléatoire car l'algorithme employé dans GraphViz n'est pas adapté.

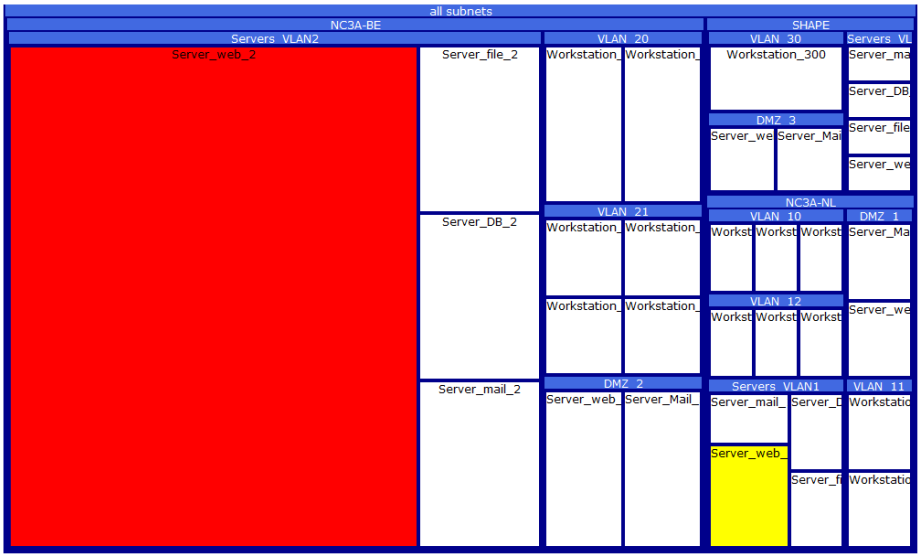
**Vue réseau radiale (RadialNet)** Cette vue montre également une vue d'ensemble du réseau, mais avec un placement des objets sur des cercles concentriques, ce qui permet d'obtenir un graphe plus compact et moins aléatoire. L'outil employé est une version légèrement modifiée de RadialNet, une interface fournie avec l'outil de scan de ports Nmap.

Les résultats obtenus sont plus satisfaisants qu'avec GraphViz, en particulier pour de grands réseaux.



**Vue réseau treemap (thejit.org)** Cette vue montre une vue d'ensemble du réseau sous forme de "treemap" [14]. Cela permet d'obtenir un affichage compact, même pour de très grands réseaux. L'intérêt principal des treemaps est de pouvoir mettre en évidence les problèmes, en affichant des rectangles plus ou moins grands suivant une métrique choisie. Dans notre cas, les rectangles des ma-

chines compromises (rouge) ou vulnérables (jaune) ont une taille plus grande que les machines normales, ce qui permet de les voir rapidement même si la structure du réseau est complexe.




**Vue géographique (Google Earth, OpenLayers)** Pour apprécier la situation, il est parfois utile de montrer les mêmes informations sur une carte géographique plutôt que sur un schéma du réseau. Dans ce cas, CIAP montre des icônes pour chaque site géographique, dont la couleur indique l'état de sécurité global. Les incidents en cours peuvent aussi être visualisés sous forme d'icônes. D'autres symboles comme les lignes sont utilisés pour afficher les alertes IDS correspondant à des attaques.

Pour ce faire CIAP fournit deux flux de données XML via HTTP, un au format KML et l'autre au format NVG [24,23]. KML est supporté par de nombreuses applications comme Google Earth, Google Maps ou OpenLayers. NVG est un nouveau format OTAN employé par des applications de commandement et contrôle miltaires. Toutes ces applications sont capables d'afficher simultanément plusieurs sources de données sur une même carte, afin de corréler visuellement les informations.


**Figure 1.** Exemple 1 : Vue géographique dans Google Earth

**Figure 2.** Exemple 2 : Vue géographique dans OpenLayers

### 3.6 Résultats actuels et futures étapes

Le prototype actuel de CIAP a permis de montrer la faisabilité technique du concept, et d'expérimenter divers modes de visualisation non disponibles dans les produits de sécurité actuels.

Plusieurs limitations ont été identifiées dans les outils testés : par exemple les algorithmes proposés par GraphViz pour représenter des graphes ne sont pas adaptés aux réseaux informatiques, et l'outil ne permet pas de visualiser de grands graphes aisément. Il est donc nécessaire de continuer le développement et de trouver des outils mieux adaptés.

Les prochaines étapes du projet consisteront à :

- Améliorer le modèle de données, pour couvrir plus de données utiles et employer plus de standards,
- Améliorer les vues existantes, à la fois en termes d'outils et en vues adaptées aux besoins des utilisateurs,
- Développer de nouvelles vues pour fournir une vision plus complète de la situation (incidents, topologie réseau physique, risques, vues fonctionnelles, etc),
- Identifier les métriques utiles pour développer des vues globales,
- Fournir une API (Application Programming Interface) plus complète pour les applications tierces basées sur CIAP (DRA, détection d'intrusion avancée, recommandation de réponses, etc),
- Implémenter une version opérationnelle de CIAP.

## 4 DRA – Analyse de Risque Dynamique

Le projet DRA (Dynamic Risk Assessment) est une étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l'impact réel dû à la situation sécurité globale du système et du réseau. Pour cela diverses techniques et outils ont été testés dans un prototype depuis 2007. Une nouvelle méthodologie innovante a été développée en combinant un générateur automatique d'arbres d'attaque (attack trees/graphs) et un moteur d'analyse de risque « traditionnel » similaire à EBIOS.

Cette méthodologie permet d'analyser en temps réel les vulnérabilités et alertes IDS détectées vis-à-vis de la topologie réseau, puis d'en déduire l'impact et les risques sur les biens (assets), services et missions de plus haut niveau de l'organisation ou de l'entreprise. Le prototype DRA est également capable de suggérer différentes réponses possibles à chaque incident, en fonction de la topologie réseau et des risques associés.

## 4.1 Objectifs

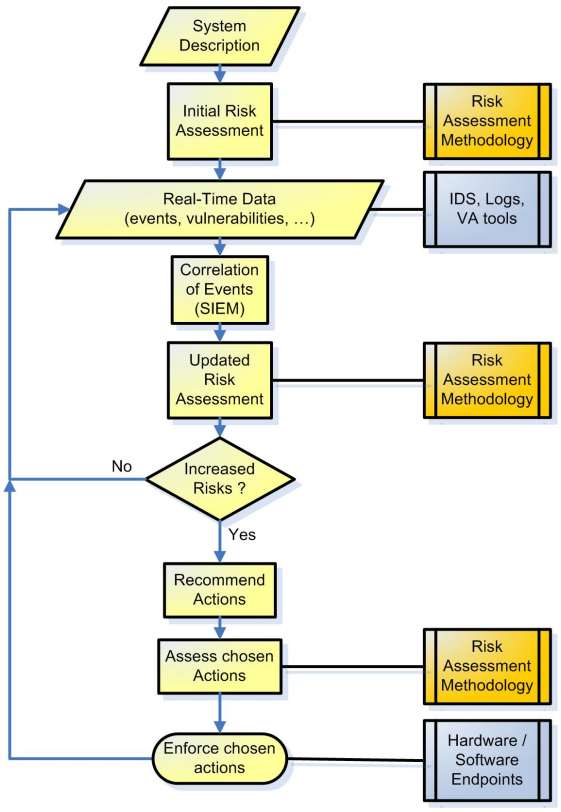
Puisque les menaces, vulnérabilités et configurations évoluent continuellement dans les systèmes d'information, il est très difficile d'effectuer une analyse de risque à un moment donné, en garantissant que les résultats seront toujours valables à moyen et long terme. Le concept d'analyse de risque dynamique (DRA, Dynamic Risk Assessment) a pour but de s'adapter à ces changements en quasi temps réel, afin de déterminer les risques en permanence pour prendre les bonnes décisions.

Un autre objectif du projet DRA est de pouvoir recommander automatiquement des réponses possibles pour réduire les risques qui ont augmenté.

## 4.2 Principe global

Le prototype de DRA actuel est basé sur un outil d'analyse de risque statique "classique", employé dans une boucle de calcul dynamique. La figure 4.2 montre un aperçu de cette méthodologie dans DRA.

1. Tout d'abord, une description complète du système à protéger doit être établie, incluant tous les biens (assets) importants, leurs valeurs et interdépendances, les menaces estimées, les machines du système, les logiciels installés, la topologie et la politique de sécurité du réseau. Cette information est stockée dans CIAP.
2. Une analyse de risque initiale est calculée. A cette étape, on suppose que le système est dans un état "sain", sans vulnérabilités et sans attaques. Le résultat est stocké comme analyse de risque de référence. C'est le niveau de risque accepté pour le déploiement opérationnel du système.




3. La description du système est mise à jour continuellement en fonction des sources de données disponibles, notamment :
   - tout changement dans le système (machines, logiciels, réseau) ou les données d'analyse de risque (biens, valeurs, dépendances, menaces)
   - nouvelles vulnérabilités détectées par des outils de scan
   - alertes et événements critiques rapportés par des IDS
   - état de sécurité des machines rapporté par un SIEM d'après la corrélation d'événements.

4. Quand un changement survient, une nouvelle analyse de risque est calculée, puis stockée en tant qu'analyse de risque courante.

5. Ces résultats sont comparés avec l'analyse de risque de référence. Certains niveaux de risque peuvent avoir augmenté, diminué, apparu ou disparu.

6. Si certains risques ont augmenté ou apparu, l'utilisateur de DRA est alerté. Sinon retour à l'étape 3.
7. DRA peut suggérer des réponses potentielles pour réduire les risques identifiés. Par exemple si une vulnérabilité critique est détectée sur un serveur web public, les réponses possibles sont d'appliquer le correctif de sécurité correspondant, de stopper l'application vulnérable, de bloquer les flux HTTP vers ce serveur en reconfigurant le pare-feu, ou bien de déconnecter le serveur du réseau.
8. L'utilisateur de DRA peut sélectionner une ou plusieurs réponses.
9. DRA peut ensuite recalculer le risque résiduel en fonctions des réponses choisies, pour confirmer si l'effet est globalement positif. En effet, certaines réponses peuvent avoir un impact négatif sur d'autres biens ou services. Par exemple, il se peut que la disponibilité d'un serveur soit critique pour l'organisation, ce qui exclut certaines réponses.
10. Lorsque des réponses satisfaisantes ont été choisies, elles peuvent être mises en oeuvre par les moyens appropriés (par exemple contacter l'administrateur d'un serveur pour installer un correctif ou changer la configuration du pare-feu).
11. Retour à l'étape 3.

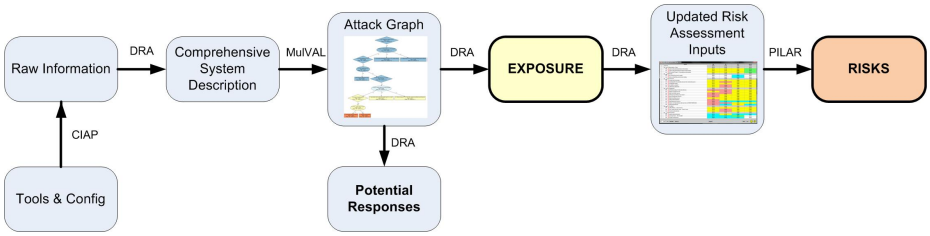
Les étapes 8 à 10 ne sont pas encore implémentées dans le prototype DRA actuel. Elles ont été testées dans le prototype initial en 2007, mais demanderont des efforts supplémentaires pour être ajoutées au prototype actuel dans de futures étapes du projet.

### 4.3 Méthodologie hybride

Plusieurs solutions d'analyse de risque ont été testées dans le prototype DRA depuis 2007. Les meilleurs résultats ont été obtenus grâce à une méthodologie hybride, combinant graphes d'attaque et analyse de risque "classique" :

1. A partir de la description du système, un graphe d'attaque est généré automatiquement. A partir de ce graphe, DRA détermine "l'exposition" (exposure) du système, autrement dit quelles sont les machines dont les vulnérabilités sont réellement exploitables par un attaquant, et les chemins d'attaque correspondants.

2. DRA utilise également le graphe d'attaque pour proposer des réponses potentielles, afin de couper les chemins d'attaque identifiés.
3. Les données d'entrées du moteur d'analyse de risque sont mises à jour en fonction de l'exposition, et les niveaux de risque sont recalculés.




## 4.4 Génération automatique d'arbres d'attaque

Le prototype DRA s'appuie sur plusieurs outils tiers pour générer les graphes d'attaque automatiquement :

**MulVAL** MulVAL est un outil expérimental développé par Kansas State University [6]. Son but est de générer automatiquement des graphes d'attaque à partir d'une base de connaissances contenant des faits et règles logiques. MulVAL utilise le langage Datalog, un dérivé de Prolog, pour exprimer ces faits et règles.

Les faits Datalog sont employés pour décrire l'ensemble du système : machines, topologie réseau, règles de pare-feu, applications installées, vulnérabilités, emplacement de l'attaquant, etc.

Les règles décrivent de façon générique les étapes des attaques connues, sous forme de conditions logiques. MulVAL est fourni avec un ensemble de règles de base qui peut être étendu au cours du temps pour ajouter de nouvelles connaissances.

MulVAL emploie toutes ces informations pour déterminer tous les chemins d'attaque possibles depuis l'attaquant jusqu'aux cibles. Le résultat est un graphe d'attaque qui est logiquement complet et exhaustif par rapport aux données fournies.

**AssetRank** AssetRank [10] est un outil développé par Defence Research and Development Canada (DRDC) pour ajouter des métriques

aux résultats de MulVAL, afin de les trier par priorité et mettre en évidence les noeuds les plus critiques du graphe d'attaque.

L'algorithme d'AssetRank est inspiré de PageRank, employé par Google pour trier les résultats de son moteur de recherche par priorité. AssetRank permet d'identifier quels sont les chemins d'attaque les plus probables du point de vue de l'attaquant en fonction de divers critères (facilité d'exploitation, furtivité, criticalité des cibles, etc).

**Génération d'un graphe d'attaque** Pour produire un graphe d'attaque, DRA doit fournir à MulVAL une description complète du système en utilisant des prédicats spécifiques en langage Datalog, comme décrit dans [7] et [8]. Le prototype DRA actuel n'exploite pas encore toutes les possibilités de MulVAL. La figure 4.4 résume les prédicats employés par DRA :

Par exemple, voici la description simple d'un système contenant uniquement un serveur web connecté à Internet avec une vulnérabilité connue exploitable sur le port 80, avec un attaquant potentiel situé sur Internet :

```
attackerLocated('internet').
hacl('internet', 'webServer', 'tcp', 80).
networkServiceInfo('webServer', 'iis', 'tcp', 80, 'unknown').
networkServiceInfo('webServer', 'system', 'tcp', 445, 'unknown
    ').
vulExists('webServer', 'CVE-2008-0075', 'iis').
vulProperty('CVE-2008-0075', remoteExploit, privEscalation).
```

La règle suivante (qui fait partie de la base de connaissances de MulVAL) décrit les conditions nécessaires pour qu'une vulnérabilité dans une application serveur soit exploitable :

```
execCode(H, Perm) :-
vulExists(H, \_, Software, remoteExploit, privEscalation),
networkServiceInfo(H, Software, Protocol, Port, Perm),
netAccess(H, Protocol, Port)
```

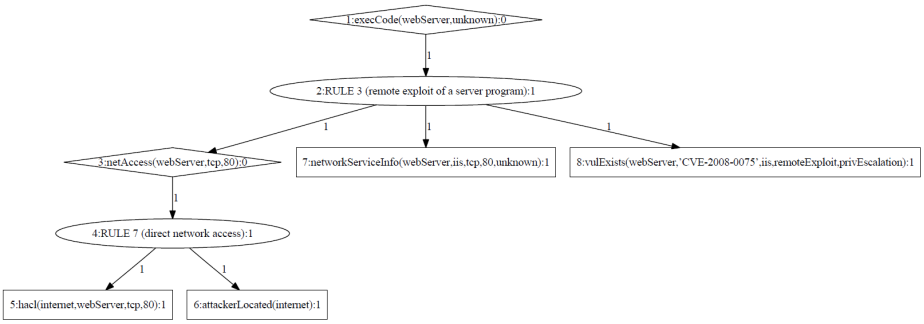
Autrement dit, s'il existe une vulnérabilité sur l'application "Software" de la machine H avec les caractéristiques "remote exploit" et "privilege escalation", que cette application est en écoute sur le port "Port" du protocole "Protocol", et que l'attaquant a accès à ce port via le réseau, alors il peut exécuter du code sur cette machine avec les privilèges de l'application.

| Category | Predicate and parameters | Description |
|---|---|---|
| **Network topology and security policy** | **inSubnet** (HS, S). | The host or subnet HS is connected to the subnet S.<br>Example: inSubnet('webServer', 'DMZ'). |
| | **hacl**(HS1, HS2, Protocol, Destport). | The host or subnet HS1 is allowed to connect to the host or subnet HS2, using protocol name Protocol, with destination port Destport.<br>Example: hacl('internet', 'webServer', 'tcp', 80). |
| **Server software** | **networkServiceInfo**(Host, Software, Protocol, Port, Account). | Software is running on Host with the user privileges of Account, listening on Port with Protocol.<br>Example: networkServiceInfo('webServer', 'iis', 'tcp', 80, 'iis-account'). |
| | **isEmailServer**(Software). | Software is an e-mail server.<br>Example: isEmailServer('exchange'). |
| **Client Software** | **installed**(Host, Software). | Software is installed on Host.<br>Example: installed('workstation', 'ie6'). |
| | **clientProgram**(Host, Software). | Software on Host is a client program.<br>Example: clientProgram('workstation', 'ie6'). |
| | **isWebBrowser**(Software). | Software is a web browser.<br>Example: isWebBrowser('ie6'). |
| | **isEmailClient**(Software). | Software is an e-mail client.<br>Example: isEmailClient('outlook'). |
| **User information** | **hasAccount**(Person, Host, Account). | The person "Person" has a user account named "Account" on Host.<br>Example: hasAccount('John', 'workstation', 'user'). |
| | **inCompetent**(Person). | The person "Person" is not incompetent, but it may be fooled by an attacker to click on a malicious link or to open a malicious attachment. |
| **Vulnerability information** | **vulProperty**(VulnID, ExploitRange, ExploitConsequence). | General information about vulnerability identified by the identifier "VulnID" (usually its CVE reference). ExploitRange indicates if the vulnerability is locally exploitable or remotely exploitable: the value may be either "localExploit" or "remoteExploit". ExploitConsequence indicates the consequence if the vulnerability is exploited: possible values are either "privEscalation", meaning a successful exploit would enable an attacker to execute arbitrary code, and "dos" (denial of service), meaning the attacker can crash or block the program.<br>Example: vulProperty('CVE-2008-0075', remoteExploit, privEscalation). |
| **Vulnerability instance** | **vulExists**(Host, VulnID, Software). | Software running on Host has a vulnerability identified by VulnID.<br>Example: vulExists('webServer', 'CVE-2008-0075', 'iis'). |
| **Attacker location** | **attackerLocated**(HS). | A potential attacker is located on the host or subnet HS.<br>Example: attackerLocated('internet'). |

D'autre règles de la base de connaissances de MulVAL permettent de modéliser différentes attaques comme celles des applications

clientes (navigateur, messagerie) ou encore les attaques locales sur des fichiers.

Le résultat de MulVAL pour cet exemple est le graphe d'attaque de la figure 4.4.




Dans les graphes produits par MulVAL, les rectangles sont des faits (prédicats primitifs) provenant de la description du système, les ellipses sont des règles décrivant une étape d'attaque, et les losanges sont le résultat d'une règle.

Dans cet exemple, le noeud supérieur "execCode(webServer,unknown)" signifie que l'attaquant a la possibilité d'exécuter du code sur le serveur web. Cette machine est donc exposée à cause de la politique de sécurité du réseau qui rend la vulnérabilité exploitable, et non plus seulement vulnérable.

Suivant le même principe, MulVAL est capable de mettre bout à bout plusieurs vulnérabilités pour déterminer des chemins d'attaque en plusieurs étapes et bâtir automatiquement des graphes d'attaque complets.

**Sources de données** Pour obtenir des résultats corrects avec MulVAL, il est donc nécessaire de lui fournir au minimum des informations complètes et détaillées sur :

- La topologie et la politique de sécurité du réseau (règles de pare-feu), afin de connaître quelles machines sont joignables à travers le réseau,
- Les applications installées sur chaque machines, et les processus serveur qui écoutent sur des ports spécifiques,

- Les vulnérabilités actuelles sur chaque machine, détaillant quelles applications ou processus sont vulnérables,
- Les caractéristiques génerales de chaque vulnérabilité (exploitable via réseau ou non).

Dans le prototype DRA, ces informations doivent être collectées automatiquement depuis diverses sources de données et outils employant des formats variés. Le prototype CIAP est chargé de collecter, normaliser, stocker et fournir les informations à DRA.

**Exploitation des graphes d'attaque dans DRA** A partir du graphe d'attaque, DRA extrait la liste :

- des vulnérabilités exploitables par l'attaquant,
- des machines exposées (ayant une vulnérabilité exploitable ou bien déjà compromises),
- des applications exposées,
- des connections réseau utilisables par les chemins d'attaque.

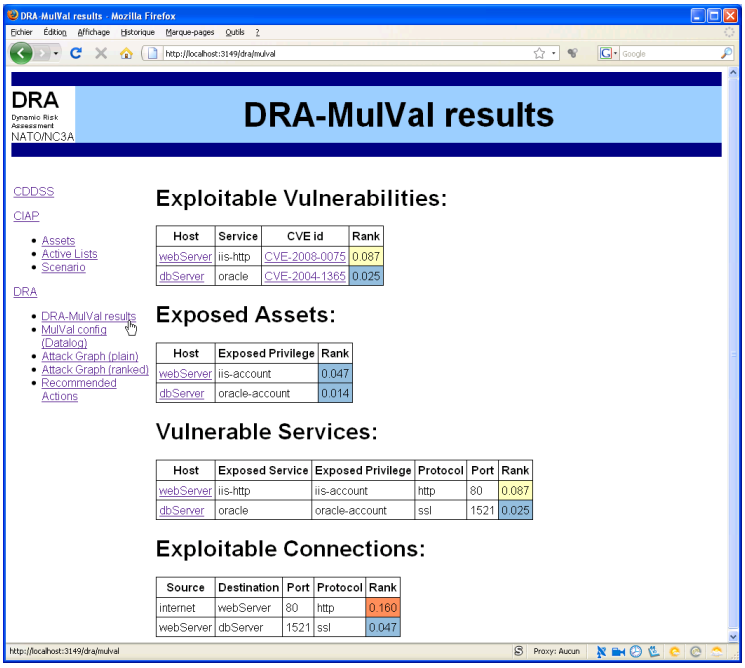
Ces informations sont fournies à l'utilisateur, triées suivant la métrique calculée par AssetRank, ce qui permet de lister en premier les problèmes les plus critiques :

## 4.5 Analyse de risque dynamique

DRA utilise PILAR, un outil d'analyse de risque tierce-partie, pour calculer les risques induits sur les biens, services et missions de plus haut niveau du système [11]. Cet outil se base sur une description des biens (assets), leurs interdépendances, leurs valeurs et les menaces associées, pour calculer les risques suivant les principes "classique" d'une analyse de risque comme decrit dans [12] ou [13].

CIAP fournit déjà des informations sur les machines vulnérables et compromises. Les arbres d'attaques générés par MulVAL permettent de déterminer plus précisément quelles vulnérabilités sont réellement exploitables par un attaquant externe. DRA synthétise toutes ces informations pour déterminer l'état de sécurité de chaque machine (normal, vulnérable, exposé ou compromis), comme indiqué plus haut dans la section "Visualisation" de CIAP.

Cet état de sécurité est alors pris en compte pour changer les paramètres d'entrée du moteur d'analyse de risque, en modifiant le niveau des menaces associées. Pour cela, il est nécessaire de décrire

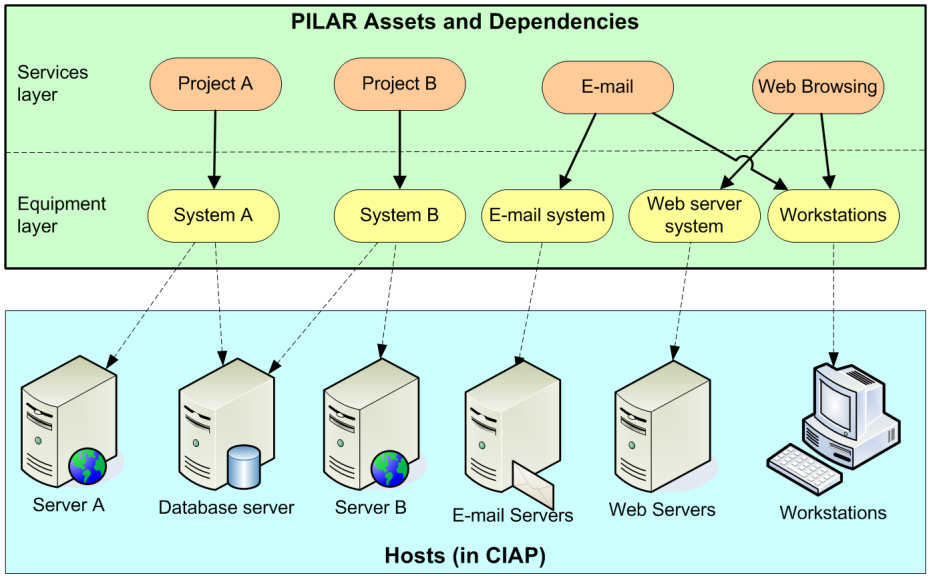


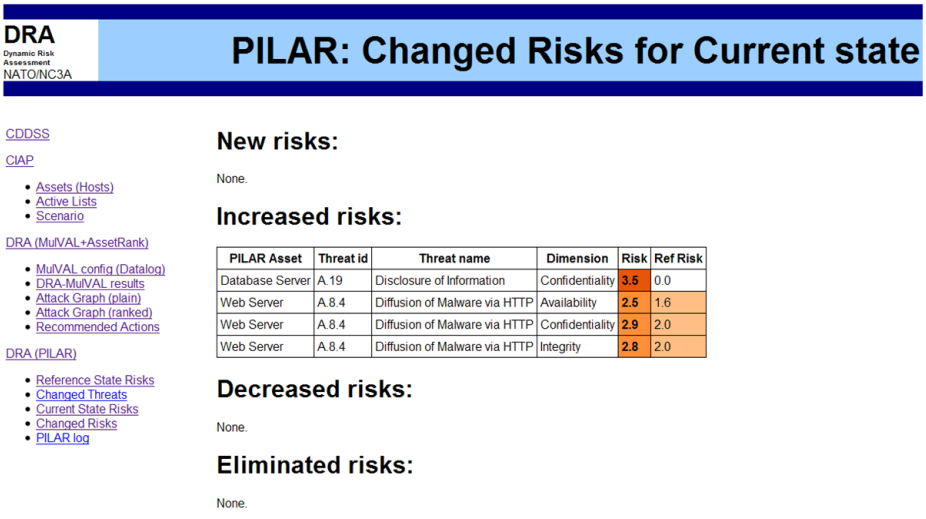

les dépendances des biens de l'analyse de risque par rapport aux machines du système. Cela se fait généralement en groupant les machines similaires ou par fonctions (par exemple, tous les postes utilisateurs normaux, tous les serveurs web internes, etc). La figure 4.5 montre un exemple de ce type de dépendances :

L'analyse de risque est recalculée à chaque changement, puis comparée avec l'analyse de référence en suivant l'algorithme détaillé précédemment dans la section "principe global". L'utilisateur est alors averti si certains risques ont augmenté par rapport à la situation normale, comme le montre la figure 4.5.

Les résultats obtenus montrent que cette approche permet d'analyser dynamiquement les risques sur les biens de haut niveau de l'organisation, en tenant compte des informations techniques fournies par les outils de sécurité, le tout de façon automatisée. Par exemple, cela permet de trier par priorité les vulnérabilités identifiées en fonction de leur impact sur les services critiques et missions de l'organisation.

Bien sûr, les résultats dépendent énormément de la qualité de l'analyse de risque initiale, et de l'arbre des dépendances entre biens,




services, missions et machines du système. L'intérêt d'employer un outil existant d'analyse de risque comme PILAR ou EBIOS est qu'il est possible de réutiliser une analyse de risque déjà effectuée avant déploiement du système, comme cela est courant pour les systèmes militaires ou gouvernementaux.

### 4.6 Suggestion de réponses

Recommander des réponses adaptées pour réduire les risques identifiés est une des fonctionnalités les plus importantes d'un système d'analyse de risque dynamique. Le prototype DRA actuel ne fournit pour l'instant que des suggestions simples, en fonction des chemins d'attaque identifiés par MulVAL :

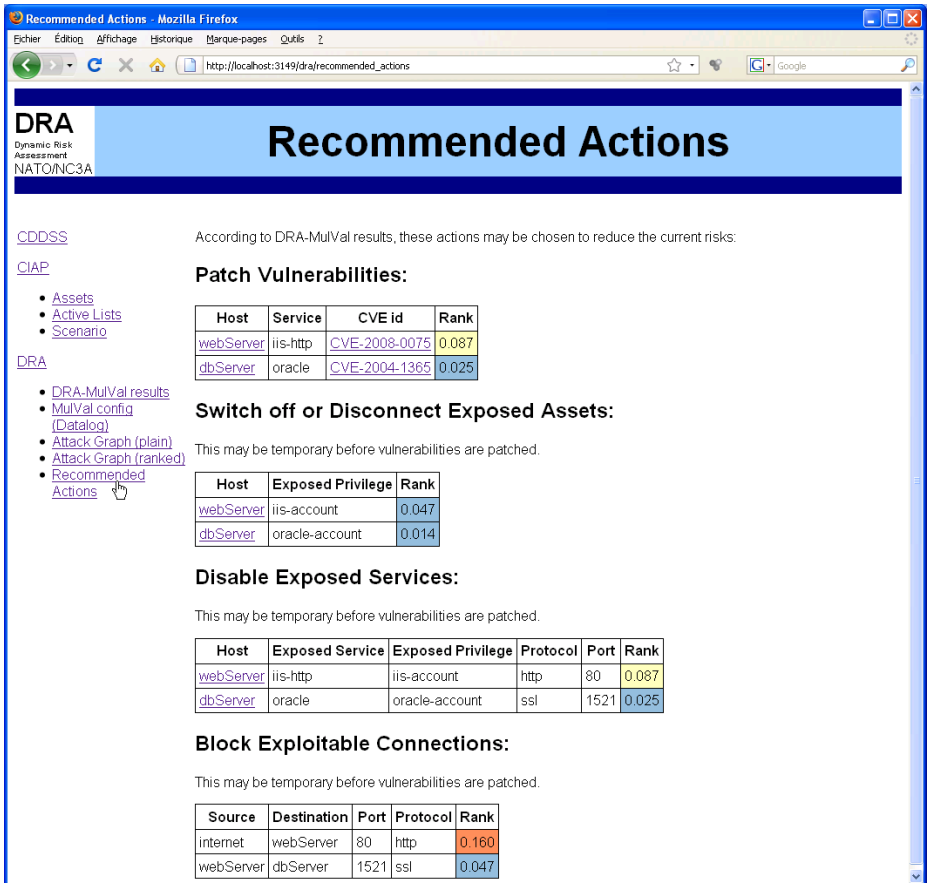
- Appliquer un correctif de sécurité : pour corriger une vulnérabilité exploitable.
- Déconnecter, éteindre ou mettre en quarantaine une machine compromise ou ayant une vulnérabilité exploitable.
- Arrêter, désactiver ou désinstaller une application ayant une vulnérabilité exploitable.
- Bloquer une connexion réseau correspondant à un chemin d'attaque, par exemple en ajoutant une règle "deny" sur un pare-feu ou un routeur.

Ces réponses possibles sont fournies à l'utilisateur de DRA, triées par ordre décroissant suivant la métrique calculée par AssetRank, comme le montre la capture d'écran ci-dessous. En pratique, cela correspond généralement à "couper" les chemins d'attaque identifiés au plus près de l'attaquant, ce qui est souvent le choix le plus efficace.

Cependant, certaines de ces réponses peuvent avoir un impact négatif sur le système, car des services critiques peuvent dépendre des machines, applications et connexions réseau listées. Dans de futures versions de DRA, l'analyse de risque sera combinée avec ces réponses pour identifier quels sont les meilleurs compromis entre disponibilité et vulnérabilités, pour recommander les solutions optimales.

### 4.7 Résultats actuels et futures étapes

Une expérimentation menée en 2009 sur des machines opérationnelles et en se basant sur les données d'une analyse de risques réelle a montré que le prototype DRA fournissait des résultats probants. Les indicateurs de risque obtenus augmentent effectivement lorsque de nouvelles vulnérabilités sont détectées ou lorsqu'une compromission est signalée par un SIEM après corrélation d'alertes IDS. De plus le risque augmente lorsque des vulnérabilités sont effectivement exploitables ou lors d'une compromission.




Cependant, l'expérimentation a montré qu'il est nécessaire de collecter un très grand nombre d'informations provenant de diverses sources pour obtenir des résultats satisfaisants. Il est par exemple très difficile d'obtenir la topologie complète d'un réseau ainsi que les règles de filtrage des pare-feux sous une forme simple à analyser, pour ensuite générer la description du système pour MulVAL.

Un autre problème critique est que les différentes sources d'information ne sont pas toujours aussi complètes et rigoureuses qu'espéré. Par exemple, l'outil OVALdi détecte bien les vulnérabilités, mais ne permet pas de déterminer sur quel port réseau elles sont exploitables. A l'inverse, Nessus fournit bien cette information, mais n'indique pas clairement la référence CVE de chaque vulnérabilité. Tous les

scanners de vulnérabilités ne sont donc pas forcément adaptés à la génération automatique de graphes d'attaque.

Le modèle de données et les sources de CIAP sont donc extrêmement importantes pour permettre à un système tel que DRA de fonctionner.

De plus, cette expérimentation initiale n'a porté que sur une dizaine de machines. Il serait donc nécessaire de faire des tests similaires à plus grande échelle pour vérifier les performances effectives de DRA. Des études précédentes sur MulVAL ont cependant montré que l'outil est capable de générer des graphes d'attaque pour un millier de machines dans un temps acceptable (quelques minutes) [9]. De plus, la possibilité de distribuer les calculs d'analyse de risque de PILAR sur chaque site a été proposée dans une étude préliminaire.

Les prochaines étapes du projet consisteront à :

- Améliorer le modèle de données de CIAP pour DRA
- Améliorer la méthodologie d'analyse de risques dynamique
- Expérimenter d'autres méthodes d'analyse
- Tester DRA avec un système de grande taille
- Améliorer l'algorithme de suggestion de réponses, en analysant le niveau de risque obtenu pour chaque suggestion
- Continuer à développer le concept de DRA en concertation avec les utilisateurs
- Implémenter tout ou partie du concept DRA dans un système opérationnel

## 5 Conclusion

Cet article a présenté les résultats actuels de deux projets de recherche et développement de l'agence NC3A de l'OTAN, CIAP et DRA. Ces deux projets visent à étudier des solutions techniques pour pallier certains manques actuels des produits de sécurité.

Le prototype CIAP permet de consolider toutes les données générées par les nombreux outils employés en cyber-défense dans un modèle de données commun et basé sur des standards pour favoriser l'interopérabilité. Une interface de visualisation innovante permet d'obtenir une meilleure vue d'ensemble de la situation, avec divers points de vue (réseau, géographique, risques, etc) suivant les besoins.

Le prototype DRA utilise des outils de génération automatique de graphes d'attaque afin de déterminer quelles vulnérabilités sont réellement exploitables par un attaquant compte tenu de l'architecture du système. Il détermine ensuite en temps réel quels sont les risques induits sur les biens, services et missions de l'organisation, afin de mieux gérer les priorités et suggérer des réponses adaptées.

Ces deux projets CIAP et DRA seront bientôt implémentés dans des systèmes opérationnels afin d'améliorer l'efficacité des moyens de cyber-défense.

## Références

1. R. Marty, "Applied Security Visualization", Addison Wesley, August 2008 (book), http ://secviz.org/content/applied-security-visualization.
2. The DAVIX Live CD, http ://www.secviz.org/node/89
3. A logic-based model to support alert correlation in intrusion detection, B. Morin, L. Mé, H. Debar, M. Ducassé, 2009, http ://dx.doi.org/10.1016/j.inffus.2009.01.005, http ://www.rennes.supelec.fr/aces/PUBLIS/aces-l2.3.pdf
4. Distributed Management Task Force. (2009). Common Information Model (CIM) Infrastructure Version 2.5.0. DMTF Standard Specification, Distributed Management Task Force.
5. TM Forum. (2009). Shared Information/Data (SID) Model.
6. Multi-host, Multi-stage Vulnerability Analysis Language, http ://people.cis.ksu.edu/~xou/mulval/
7. X. Ou, "A Logic-programming approach to network security analysis", Ph.D. thesis, Princeton University, Princeton, New Jersey, USA, November 2005.
8. X. Ou, S. Govindavajhala, A. Appel, "MulVAL : a logic-based network security analyzer", in proceedings of the 14th USENIX Security Symposium, held 31 July – 5 August 2005 in Baltimore, Maryland, USA, Vol. 14, pp. 113-128, USENIX Association, Berkeley, California, USA, August 2005.
9. A scalable approach to attack graph generation. Xinming Ou, Wayne F. Boyer, and Miles A. McQueen. In 13th ACM Conference on Computer and Communications Security (CCS 2006), Alexandria, VA, U.S.A., October 2006.
10. Identifying critical attack assets in dependency attack graphs, Reginald Sawilla and Xinming Ou, 2008, http ://people.cis.ksu.edu/~xou/publications/esorics08.pdf
11. EAR / PILAR - Environment for the Analysis of Risk, http ://www.artools.com/en/index.html
12. International Organization for Standardization/International Electrotechnical Commission international standard 27005 :2008, "Information Technology – Security techniques – Information security risk management", ISO, Geneva, Switzerland, 15 June 2008.
13. EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, http ://www.ssi.gouv.fr/site_article45.html.

14. Treemapping, Wikipedia, http ://en.wikipedia.org/wiki/Treemapping
15. CVE, Common Vulnerabilities and Exposures, http ://cve.mitre.org/
16. NVD, National Vulnerability Database, http ://nvd.nist.gov/
17. CVSS, Common Vulnerability Scoring System, http ://www.first.org/cvss/
18. CPE, Common Platform Enumeration, http ://cpe.mitre.org/
19. CCE, Common Configuration Enumeration, http ://cce.mitre.org/
20. CAPEC, Common Attack Pattern Enumeration and Classification, http ://-capec.mitre.org/
21. CWE, Common Weakness Enumeration, http ://cwe.mitre.org/
22. MAEC, Malware Attribute Enumeration and Characterization, http ://-maec.mitre.org/
23. NVG, NATO Vector Graphics (internal publication).
24. KML, Keyhole Markup Language, http ://en.wikipedia.org/wiki/Keyhole_Markup_Language.
25. CRE, Common Remediation Enumeration, http ://scap.nist.gov/events/2009/ itsac/presentations/day4/Day4_SCAP_Wojcik.pdf
26. ERD, Extended Remediation Data, http ://scap.nist.gov/events/2009/ itsac/presentations/day3/Day3_DoD_Wojcik.pdf
27. OVAL, Open Vulnerability and Assessment Language, http ://oval.mitre.org/
28. OVALdi, "OVAL Interpreter", http ://oval.mitre.org/language/download/interpreter
29. XCCDF, The eXtensible Configuration Checklist Description Format, http ://s-cap.nist.gov/specifications/xccdf/
30. CRF, Common Result Format : http ://makingsecuritymeasurable.mitre.org/crf/
31. IODEF, Incident Object Description and Exchange Format, http ://xml.coverpages.org/iodef.html
32. VerIS, The Verizon Incident Sharing Framework, http ://securityblog.verizonbusiness.com/ wp-content/uploads/2010/03/VerIS_Framework_Beta_1.pdf
33. CEE, Common Event Expression, http ://cee.mitre.org/
34. H. Debar, D. Curry, B. Feinstein, The Intrusion Detection Message Exchange Format (IDMEF), IETF RFC 4765, 2007.
35. ISO 8601 :2004, Data elements and interchange formats - Information interchange - Representation of dates and times, http ://www.iso.org, http ://en.wikipedia.org/wiki/ISO_8601.