APPROCHE GENERIQUE DE CONTROLE D'ACCES AUX DONNEES ET AUX TRAITEMENTS DANS UNE PLATEFORME D'INTELLIGENCE ECONOMIQUE

Hamid HATIM (**), Anass EL HADDADI (*, **), Hanane EL BAKKALI (**), Bernard DOUSSET (*), Ilham BERRADA (**),
hamidhatim@yahoo.fr ; haddadi@irit.fr ; elbakkali@ensias.ma ; dousset@irit.fr ; iberrada@ensias.ma

(*) IRIT, SIG, Université Paul Sabatier, route de Narbonne, 31062 Toulouse cedex 04
(**) ENSIAS, Equipe Al BIRONI, Université Mohamed V – Souissi, B.P. 713 AGDAL, Rabat - Maroc

Mots clés :
Contrôle d'accès, intelligence économique, sécurité des données, sécurité des procédures.

Keywords:
Access Control, competitive intelligence, data security, Process security.

Palabras clave:
Control de Acceso, inteligencia competitiva, seguridad de los datos, Seguridad del proceso

Résumé:
La concurrence est un concept fondamental de la tradition libérale et de la science économique qui oblige les entreprises à pratiquer l'intelligence économique (IE) pour bien se positionner sur le marché ou tout simplement pour survivre. Sauf que souvent, *ce n'est pas le plus fort de l'espèce qui survit, ni le plus intelligent, mais celui le plus sensible au changement*, qui est le facteur dominant dans la société actuelle. Les changements proviennent de l'extérieur ou naissent au sein même de l'entreprise et peuvent l'affecter plus ou moins durablement. Dès lors, les entreprises sont appelées à rester constamment en veille pour guetter le moindre changement en vue d'y apporter la solution adéquate en temps réel. Cependant, pour une veille réussie, on ne doit pas se contenter uniquement de surveiller les opportunités, mais avant tout, d'anticiper les menaces. Malheureusement, cette veille se déroule en oubliant l'indispensable volet sécurité de l'IE à savoir la sécurité des données manipulées et celle des procédés suivis pour atteindre les objectifs de l'IE.

Dans ce papier, nous présentons une approche de modélisation du contrôle d'accès aux données et aux traitements pour sécuriser toutes les informations et les flux d'interactions dans une plateforme d'intelligence économique durant tout son cycle de vie. Le modèle proposé sera déployé dans la plateforme d'intelligence économique Xplor EveryWhere.

1 Introduction

Les entreprises font face aujourd'hui à une concurrence accrue sur des marchés extrêmement dynamiques et imprévisibles : nouveaux entrants, fusions et acquisitions, baisses tarifaires brutales, évolution rapide des modes de consommation et des valeurs, fragilité des marques et de leur réputation, … Les facteurs de changement et de risques externes n'ont jamais été aussi nombreux, accrus par le contexte de la crise financière actuelle. Pour mieux anticiper ces risques et guetter les opportunités, l'I.E. semble être la seule à l'avant-garde.

Le rapport Henri Martre [1] définit l'IE comme étant l'ensemble des actions coordonnées de recherche, de traitement et la distribution de l'information utile aux acteurs pour permettre l'action et la prise de décision. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de délais et de coûts. L'information utile est celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel. Ces actions, au sein de l'entreprise, s'ordonnent autour d'un cycle ininterrompu, générateur d'une vision partagée des objectifs de l'entreprise.

Pour arriver à ces fins, des plateformes d'IE sont développées dont Xplor EveryWhere [2] pour mettre en ligne ce type de structure en mode client serveur, afin de réaliser une fouille personnalisée via divers outils de restitution graphique des résultats servant comme outil d'aide à la décision.

Le besoin en matière de sécurité dans une plateforme d'IE provient du fait que les informations manipulées sont d'ordre stratégique ayant une valeur assez importante. Une telle sécurité ne doit pas être considérée comme une option supplémentaire qu'offre une plateforme d'IE pour se distinguer d'une autre. D'autant plus que la fuite de ces informations n'est pas le fait de faiblesses inhérentes aux systèmes informatiques des entreprises, mais avant tout, c'est une question organisationnelle.

Dèe lors, les mêmes procédures organisationnelles relatives à l'utilisation des ressources informatiques, visant à assurer la fonction de veille stratégique et concurrentielle dans une plateforme d'IE devraient aussi s'appliquer au domaine du contrôle de l'information : établissement d'une politique de sécurité, sensibilisation des salariés, mise en garde quant au contenu diffusé, et l'adhésion à des bonnes pratiques sont des outils potentiels pour réduire le risque des fuites d'information.

Nous rappelons que l'IE, également connu sous le nom de Business Intelligence, est à la fois un processus et un produit [3]. En tant que processus, l'IE est l'ensemble des méthodes légales et éthiques qu'une entreprise utilise pour mobiliser l'information qui l'aide à réussir dans un environnement mondialisé. En

tant que produit, l'IE est l'ensemble des informations sur les activités des concurrents à partir de sources publiques et privées, et son champ d'application est le comportement présent et futur des concurrents, des fournisseurs, des clients, de la technologie, des acquisitions et fusions, des marchés, des produits et services, et de l'environnement des affaires en général.

Il s'agit donc de sécuriser à la fois des données (IE étant un produit) et des procédés (IE en tant que méthode de traitement). De là est partie notre contribution de proposer une approche de contrôle d'accès aux données et aux traitements dans une plateforme d'IE. Il s'agit d'un modèle générique pour intégrer le contrôle d'accès dans le cycle de vie des plateformes d'IE afin que toutes les tâches dans un processus de veille soient exécutées uniquement par les utilisateurs autorisés et habilités. Le reste de l'article est donc organisé comme suit:

Nous commencerons d'abord par décrire dans la section 2 les risques et les vulnérabilités auxquelles sont soumises les plateformes d'IE pour exprimer le besoin d'établir un contrôle d'accès aux données et aux traitements de l'information. Dans la section 3, nous présentons une approche générique pour sécuriser une plateforme d'IE. La section 4 est une mise en œuvre de l'approche proposée dans un cas réel, à savoir la plateforme Xplor EveryWhere. Nos conclusions et perspectives seront formulées à la section 5.

2 Risques de sécurité dans une plateforme d'intelligence économique

L'enquête menée par le CLUSIF en 2008 [4] montre que 73% des entreprises de plus de 200 salariés estiment lourde de conséquence une impossibilité de moins de 24 heures de leurs outils informatiques. Cette dépendance à l'informatique est d'autant plus aiguë dans le domaine d'IE où toute l'activité de veille est complètement automatisée.

Une activité de veille dans une plateforme d'IE, qu'elle soit externalisée via un fournisseur de service ou menée en interne se passe en plusieurs étapes, chacune exigeant une forme de sécurisation spécifique. La première étape, la collecte des données, exige un service de sécurité en matière de disponibilité, d'intégrité et de confidentialité. Toute altération à ce niveau implique des prédictions erronées et c'est tout le sens de l'IE qui est remis en cause. La deuxième étape, celle du traitement des données collectées, exige un service de contrôle d'accès mettent en œuvre des mécanismes d'authentification/autorisation afin de limiter l'accès aux personnes mandatées pour la réalisation des différentes tâches. Cette étape est nécessaire par exemple pour la préservation du secret du métier. Enfin, l'ultime étape, celle de la restitution de l'information jugée 'stratégique' aux clients exige un l'authentification mutuelle (platefome/décideur) et l'intégrité des données.

Les risqué de sécurité sont encore plus importants pour une plateforme collaborative où les veilleurs, organisés en réseaux, peuvent travailler sous forme de forum. La gestion des droits d'accès des utilisateurs distants et accédant à des fonctionnalités réparties est assez laborieuse, car dans la plupart des cas, l'architecture ne reflète pas la politique de sécurité [5].

La solution est de proposer un système de sécurité "transparent", car s'il est compréhensible pour l'attaquant (comprendre un système de sécurité ne signifie pas forcément déceler une faille), il est tout d'abord compréhensible à l'administrateur de sécurité, une condition indispensable pour qu'il puisse monter la garde.
La figure 1 montre quelques problèmes de sécurité pouvant compromettre l'activité de veille dans une plateforme d'IE. Ces problèmes sont à la fois externes à la plateforme (attaque de la part des concurrents par exemple), mais aussi internes à la plateforme (Séparation des tâches entre les différents rôles impliqués, minimum de privilège accordés à chaque utilisateur, éviter les conflits d'intérêt, etc…).

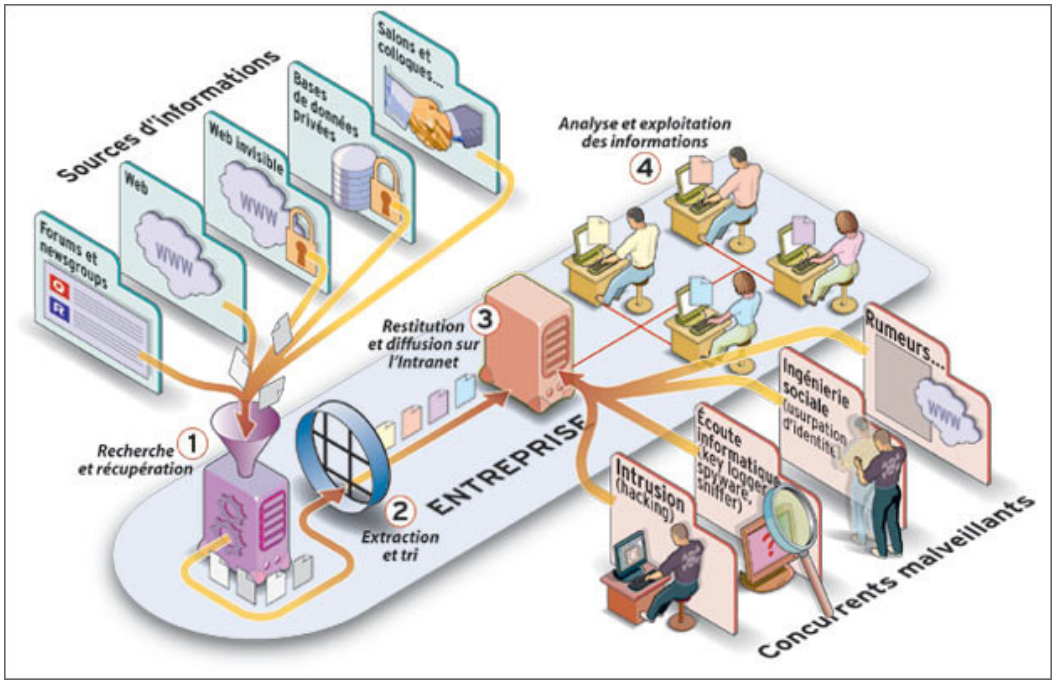

Figure 1 : Interactions dans une plateforme d'IE [6]

2.1 Risques liés à l'importation des données pour le traitement et l'analyse

Les données sont importées via des outils qu'on achète ou qu'on développe chez soi tels que les méta-moteurs de recherche, les web crowlers, etc… pour surveiller tout type d'information sur le Web visible (forums de discussion, newsgroups, blogs, newsletters, Intranets, RSS, Blog, …) et invisible (bases de données en ligne, sites nécessitant une authentification, moteurs de recherche, réseaux sociaux, etc.).

2.1.1 Risques liés à l'utilisation des logiciels de collecte

Il y a des précautions à prendre lorsque ces outils sont des open sources qu'on doit intégrer à la plate forme. On doit s'assurer, et ce, en recompilant soi-même le code avant son intégration pour s'assurer que ces outils ne sont pas en fait des "malwares" destinés à renvoyer en retour le résultat des analyses des données qu'elles importent. "On ne peut avoir totalement confiance dans un code qu'on n'a pas tout à fait développé soi-même" [5].

2.1.2 Risques liés aux sources d'information

Tous les sites web ne sont pas authentiques : certains sont des miroirs qui font rediriger le visiteur vers un site dont les services sont différents de ceux qu'ils affichent. Pour collecter des informations uniquement à partir de sources fiables, il faut se baser sur les certificats de la part d'organisation d'approbation de sites web qui vérifient entre autres, qu'un site Web possède bien une déclaration de confidentialité.

2.1.3 Risques liés aux aspects juridiques

L'IE est complètement distincte de l'espionnage, l'activité de veille doit se faire d'une manière légale et une attention particulière doit être accordée à la préservation de la vie privée. Aux USA, les activités de veilles stratégiques et concurrentielles sont assujetties à des lois fédérales qui expliquent entre autre les modalités sous lesquelles une veille peut être menée [7]. La politique de sécurité au niveau de la plateforme doit donc spécifier à l'avance le contenu 'légalement' accessible pour une activité de veille. Par exemple, le système doit être en mesure de refuser les permissions à un veilleur s'il tente d'importer des données protégées car dans ce cas, les conséquences peuvent aller de la dégradation de la réputation à un procès intenté contre la plateforme. Le mieux c'est d'inviter les utilisateurs à adhérer à un référentiel de bonnes conduits pour encadrer le comportement de chaque usager dans les différentes situations dans l'entreprise.

2.2 Risques liés aux procédures de traitements et d'analyses des données

La perte ou la destruction d'informations sensibles est dans 80 % des cas le fait de maladresses internes [8]. Les dommages peuvent être accidentels ou intentionnels. A la différence des attaques provenant de l'extérieur et opérées par des utilisateurs non autorisés à accéder au système, ces vulnérabilités sont liées à l'utilisation abusive des privilèges par des personnes autorisées et correctement identifiée. Les travaux du projet MITRE [9] concernant l'utilisation abusive des permissions légalement acquis ont proposé des techniques pour palier à ce problème.

2.3 Risques liés à la livraison de l'information

Le résultat des traitements – la fameuse information stratégique – doit être livré au client ayant fait appel à une activité de veille stratégique. Deux méthodes permettent d'arriver à cette fin :

- La stratégie PULL : le client va chercher les informations sur le serveur. Dans ce cas, un portail internet de la plateforme doit fournir les résultats moyennant une authentification de la part du client. L'essor du commerce électronique ces dernières années a fourni des avancées considérables en matière de sécurité qui peuvent être réutilisées dans les portails internet des plateformes d'IE.
- La stratégie PUSH : le serveur envoie l'information sous forme d'alerte au client sous forme de message dans un réseau informatique (ordinateur relié à internet) ou télécom (smart phone).

Notre plateforme d'IE XPlor EveryWhere envoie les résultats au client dans son téléphone portable. Ces équipements (pour la plupart des smart phones), sont autant des ordinateur et doivent donc être équipés de systèmes de protection puissants contre les attaques car désormais, ils ne sont pas seulement des périphériques d'affichage, mais contiennent des informations stratégiques. En effet, c'est grâce à leur faculté d'équipements réseau ouverts, programmable et pouvant fournir divers services de type PC, comme la messagerie, le courrier électronique et la navigation sur le Web qu'ils sont retenus pour la livraison de l'information. [10] décrit les risques encourus par l'utilisation de ces équipements en expliquant le mode d'exécution des processus et présente un Framework qui peut être utilisé pour la sécurité du terminal (téléphone) du client.

3 Approche proposée pour le contrôle d'accès à une plateforme d'IE :

Face aux risques de sécurité énumérés dans la section 3, rares sont les plateformes d'IE qui sont dotées d'un service de sécurité qui s'incère dans un projet digne du nom et qui respecte une politique de sécurité préétablie. Plutôt, les réponses à une attaque de sécurité sont concoctées au grès de leur apparition dans le dysfonctionnement du système [11].

Pour contribuer dans une solution face à cette lacune, nous proposons une approche de contrôle d'accès d'une plateforme d'IE qui s'étale sur tout le cycle de vie de l'IE. Pour respecter l'aspect "générique" de l'approche afin qu'elle puisse être intégrée dans toute plateforme d'IE, nous proposons que la sécurité du traitement des données se base sur le standard de contrôle d'accès RBAC (Role_Based Access Control) [12]. Dans ce qui suit, nous présentons le cycle de vie de l'IE suivie de la formalisation de l'approche proposée.

3.1 Cycle de vie de l'IE

L'analyse stratégique et la veille constituent les bases méthodologiques du processus d'IE. Sa mise en place doit s'instaurer dans un climat de sécurité globale. Dans ce contexte, nous regroupons les étapes du processus en trois phases distinctes mais complémentaires : l'analyse stratégique, la veille et la protection de l'information.

Le processus d'IE est alors une coordination des processus d'analyse stratégique et de veille basée sur les systèmes d'informations. Nous le présentons dans la figure 2. On retrouve dans cette présentation schématique, les quatre étapes essentielles du cycle du renseignement à savoir :

- Compréhension du besoin,
- La recherche et la collecte d'information,
- Le traitement de l'information,
- La diffusion de l'information.

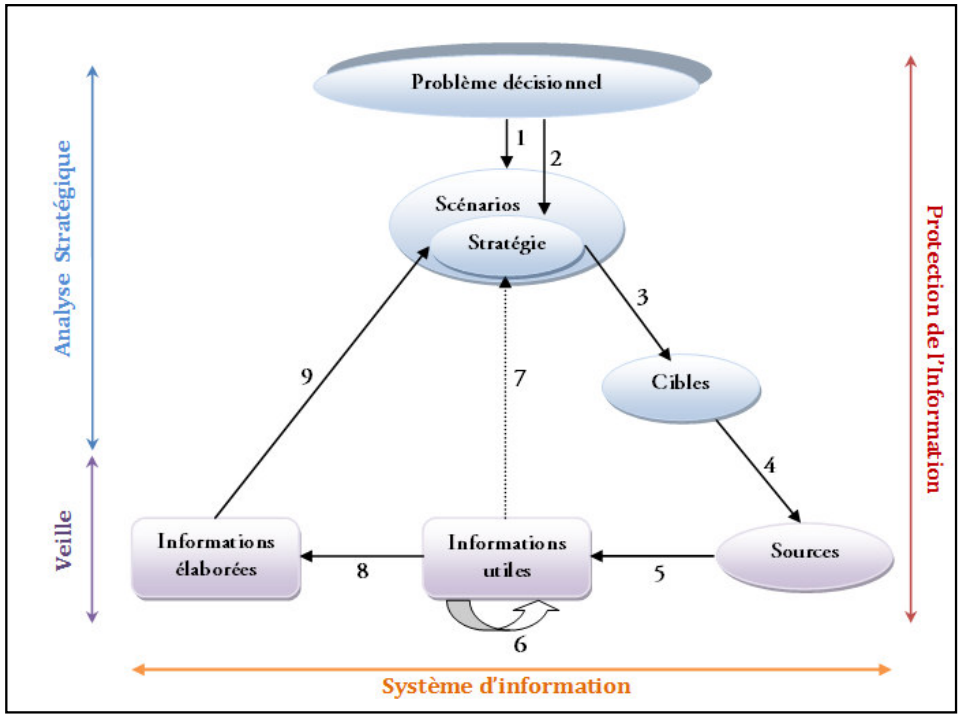

Figure 1 : Cycle de vie de l'IE

3.2 Politique de sécurité dans une plateforme d'IE

La politique de sécurité décrit d'une manière exhaustive l'ensemble des dispositifs et des procédures techniques, administratives, juridiques qui doivent être mis en place pour travailler en toute confiance aussi bien au sein de la plateforme qu'avec les collaborateurs. Le Service de Coordination à l'Intelligence Economique (SCIE) [9], rattaché aux ministères français de l'Economie et du Budget a élaboré un guide de bonnes pratiques en matière d'IE sur lequel nous

nous basons, - en y introduisant les principes de contrôle d'accès les plus indispensables - pour formuler une politique de sécurité applicable à une plateforme d'IE. Nous l'exprimons d'une manière formelle dans ce papier (des travaux antérieurs que nous avons menés donnent une idée sur la formalisation d'une telle politique [13]). Un administrateur de sécurité est chargé de sa mise en œuvre et de l'observance des modalités selon lesquelles chaque étape du cycle de l'IE est réalisée conformément à ses dispositions.

3.2.1 Au niveau de la collecte et de l'importation des données

- Application du principe SOD (Separation of Duty ou Séparation des tâches) [14] pour éviter le conflit d'intérêt:
- Application de la cardinalité : Pour les sujets particulièrement sensibles à diffusion restreinte, limiter le nombre de collaborateurs impliqués dans la collecte.
- Pour la collecte d'informations qui ne doivent en aucun cas être divulguées (même pour obtenir une information en retour), il faut les scinder en plusieurs sujets et diversifier les contacts.
- Après la collecte, supprimer régulièrement les cookies de l'ordinateur et déconnecter la messagerie.

3.2.2 Au niveau du traitement et de l'analyse des données

- Identification des personnes qui doivent avoir accès à l'information
- Identification des rôles joués par chaque utilisateur.
- Identification des permissions associées à chaque rôle.
- Identification de chaque tâche associée à chaque rôle
- Identification des conflits entre les entités (rôles, utilisateurs, tâches)
- Identification des ressources
- Protection du corpus
- Respect du principe LP (Least Privilege ou minimum de privilège) [15] pour accorder à un utilisateur le plus petit ensemble de privilèges (ou permissions) qui lui sont nécessaires dans l'accomplissement de la tâche qu'il s'apprête à exécuter et non tous les privilèges liés à son rôle dans l'entreprise.
- Etablissement d'un référentiel d'historique des accès de tous les rôles, utilisateurs et tâches.

3.2.3 Au niveau de la restitution de l'information aux décideurs

- Classification de l'information en fonction de son degré de sensibilité (générale, restreinte, confidentielle, etc…). Les informations confidentielles sont celles dont la divulgation procurerait un avantage à la concurrence ou aux partenaires ou réduirait l'avantage dont dispose l'entreprise (R&D, travaux d'innovation, savoir-faire technologique, contenu d'offres commerciales, structure des comptes, fichiers clients projets de développement, fonctionnement de l'entreprise…)
- Définir les supports de diffusion de l'information (réunions, compte-rendu, messagerie électronique, etc…)
- Identification des clients qui doivent avoir accès à l'information.

4 Mise en œuvre dans un cas pratique : Sécurisation de la plateforme Xplor EveryWhere

4.1 Description de la plateforme Xplor EveryWhere

Le prototype Xplor Evry Where est alimenté par des données relationnelles issues de la plateforme Tétralogie. Cette dernière permet d'effectuer des analyses stratégiques globales sur des données textuelles ou factuelles provenant de bases bibliographiques en ligne, sur CD/Rom, d'Internet ou de toute autre source informatisée, presse etc. Par l'intermédiaire de méthodes statistiques descriptives et exploratoire des données, Xplor Evry Where fait apparaître, dans des temps très courts, de nouvelles connaissances stratégiques comme : l'identité des acteurs, leur notoriété, leurs relations, leurs lieux d'action, leur mobilité, l'émergence et l'évolution des sujets et des concepts, la terminologie, les domaines porteurs.

L'approche adoptée, pour le développement du prototype Xplor Evry Where, permet de combiner les techniques d'extraction de connaissance à partir des données textuelles et les techniques de stockage, d'analyse et de visualisation des données relationnelles. Chacune de ces techniques est vue comme un composant aux fonctionnalités précises et délimitées. Plus simples à développer, plus robustes et testés dans des contextes différents, ces composants peuvent s'assembler de plusieurs manières pour créer ainsi des applications variées et adaptées aux besoins des utilisateurs.

Notre approche pour le développement du système Xplor Every Where repose sur une architecture décisionnelle à trois niveaux, en se basant sur les travaux de l'équipe SIG-EVI pour le développement du prototype Xplor [16] :

- Sources et traitement, ce niveau permet d'alimenter l'entrepôt de donnée, à partir des corpus de données textuelles. Il permet le passage de la représentation des documents textuels (données qualitatives) sous forme de données quantitatives. Il concerne le traitement de l'hétérogénéité des informations, d'un point de vue : contenu sémantique : scientifique, technique, etc., structurel : fortement structuré (brevet) à non structuré (e-mails), linguistique (multilinguisme) : chinois, arabe, format du support : Word, html, pdf, etc., taille : définition de l'unité d'information à analyser (granularité de l'information). Pour cette partie du traitement, les techniques employées

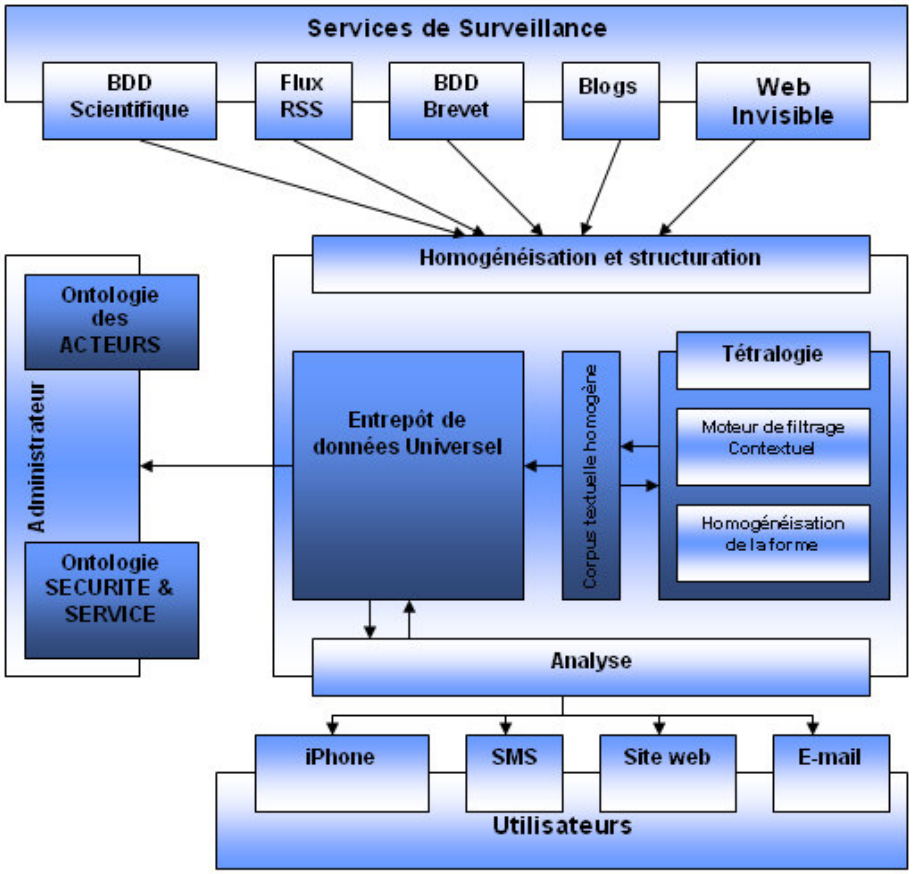

Figure 3 : Architecture de la plate-forme d'IE

s'appuient sur les fonctionnalités du système Tétralogie développé antérieurement par les membres de l'équipe SIG-EVI. Ces composantes permettent de répondre au problème d'hétérogénéité des documents à analyser.

- Entrepôt de données, est un espace de stockage qui à premier niveau permet d'offrir une vue unifié du corpus cible, et au deuxième niveau permet l'extraction et le stockage des données sources structurées sous forme d'une représentation multidimensionnelle. Le second niveau porte sur les traitements de création de l'entrepôt de données. Il repose sur la création des matrices à deux et trois dimensions (contingences, cooccurrences, présence absence) à partir de la vue unifiée. Notre approche consiste à utiliser les composantes du système Tétralogie pour la création des matrices à deux dimensions et réajuster la structure des résultats obtenus pour faciliter le transfert des données dans l'entrepôt de données du prototype. Cet entrepôt ne contiendra que les données sous forme relationnelles tel que : N°doc-Auteur, Auteur-Auteur-Date, etc. Cette représentation permet de synthétiser toutes les relations existantes entre les différents attributs constituant les documents à analyser. La base de données est interfacée grâce au système Xplor sur Intranet ou Internet, afin que l'utilisateur puisse lui même mener ses propres investigations.
- Analyse et restitution, ce niveau permet d'effectuer des analyses multidimensionnelles en ligne sur les données issues de l'entrepôt et restituer les résultats à l'utilisateur par des fonctions de reporting. Il comporte les fonctionnalités de navigation et d'analyse en ligne. Ces fonctions sont: administration des données, exploration des données relationnelles et visualisation des résultats. Chaque attribut peut être filtré au moyen de fonctions relationnelles prédéfinies en se servant des liens complexes qu'il possède avec lui même et les autres attributs de la base. Des statistiques descriptives interactives sont alors disponibles pour chaque extrait (fréquences, équivalences, etc.) ainsi que sur l'évolution de leurs relations. Des fonctions de reporting sont prédéfinies pour permettre la visualisation des résultats.

Les différents utilisateurs qui interagissent avec notre plateforme, sont représente dans le diagramme de contexte suivant :

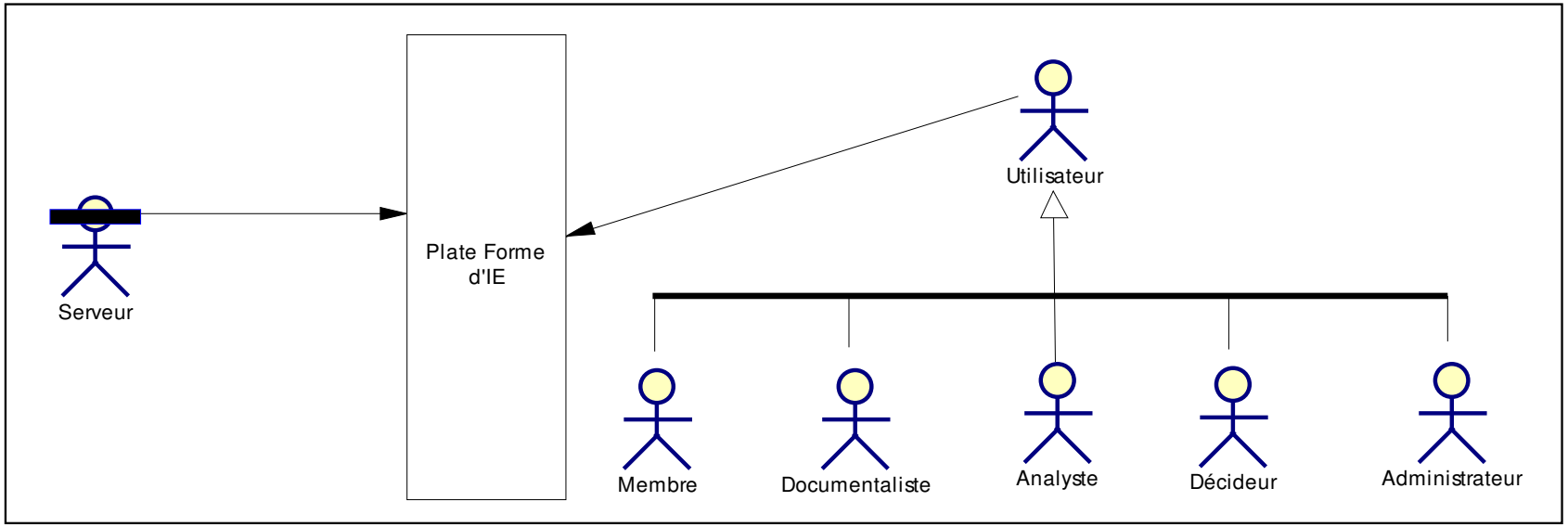

Figure 4 : Diagramme de contexte de la plateforme d'IE

4.2 Contrôle d'accès aux données et aux traitements dans Xplor EveryWhere

Nous adaptons le standard RBAC (Role-Based Access Control) pour mettre en œuvre la politique de contrôle d'accès. Ceci est nécessaire pour une éventuelle extension en cas de collaboration avec d'autres plateformes d'IE qui respectent ce standard : le modèle de contrôle d'accès n'a pas besoin d'être remis de fond en comble. Un framework construit autour des concepts de ce standard assure la gestion de tous les accès à la plateforme.

4.2.1 4.2.1. Modélisation des processus de la plateforme Xplor

Pour une visibilité complète et une meilleure maîtrise des flux d'information pour l'administrateur de sécurité, nous représentons dans la figure 5 tous les processus métiers de Xplor par un workflow (un ensemble de tâches reliées par une relation de dépendances et de succession).

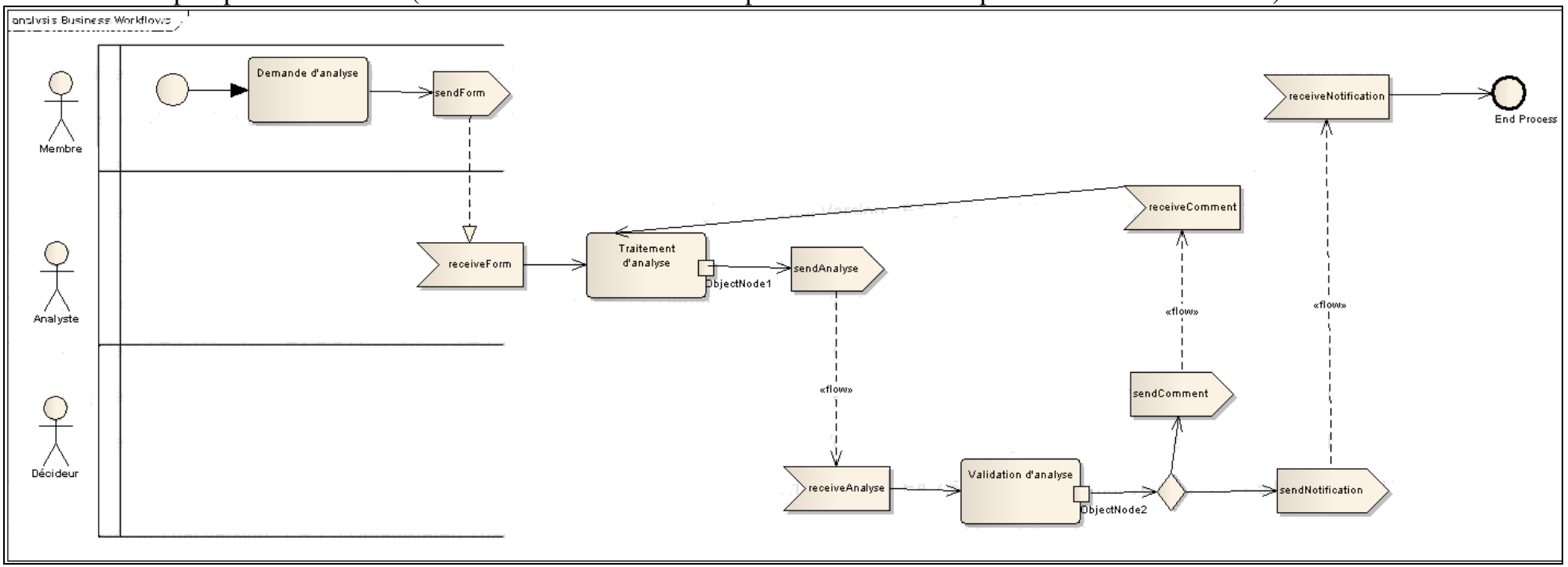

Figure 5 : Représentation du workflow Xplor

4.2.2 Application du modèle de contrôle d'accès RBAC.

Adopté comme une norme ANSI / INCITS en 2004, RBAC (Role-Based Access Control) est le modèle de contrôle d'accès le plus rependu dans les systèmes informatiques [12]. Dans ce modèle, les permissions sont accordées aux rôles joués par les utilisateurs plutôt qu'aux utilistaeurs eux-mêmes. Vu que dans une entreprise on dénombre quelques roles alors qu'on a plusieurs milliers d'employés, l'administration de la sécurité se trouve largement facilitée.

a. Etablissement des différents rôles et les tâches associées

Concept central du standard RBAC, les rôles décrivent les positions administratives et opérationnelles que remplissent les acteurs impliqués dans le fonctionnement d'une plateforme d'IE. Ces rôles auxquels on associe les privilèges d'accès aux ressources sont établis en fonction des besoins du métier de l'IE et les utilisateurs les utilisent pour accéder à la plateforme. Il faut noter que l'accès au système n'est possible que sur la base du rôle joué pour exécuter une tâche. Le tableau 1 répertorie les différents rôles dans Xplor ainsi que les tâches correspondantes.

Rôle	Tâche
Administrateur sécurité	Protéger le système informatique et les données sensibles
Collecteur-Veilleur	Collecter les données au moyen de : - Flux Rss : S'informer de l'actualité sur les sites sélectionnés sans avoir à se connecter en utilisant des lecteurs de flux Rss - Les agents d'alerte : Détection de changements sur une page web - Les requêtes : Recherche à partir de mots clés dans les moteurs de recherche - Les newsletters
Analyste-Veilleur	- Trier les informations et ne retenir que celles qui sont pertinentes - Appliquer les techniques de data-mining pour extraire des informations utiles - Organiser, structurer, hiérarchiser et rapprocher les informations - Interpréter et synthétiser les principaux résultats de l'analyse
Administrateur	- Valider la crédibilité de la source d'information de la part du collecteur - Valider les informations retenues : évaluer leur exactitude et leur fiabilité
Auditeur	- S'interroger sur la conformité des procedures suivies dans les différentes activités avec la politique de sécurité - Tester les résultats
Stagiaire	Remplit l'une des tâches du rôle auprès duquel il est admis

b. Les permissions aux objets à protéger

D'une manière logique, un rôle n'est rien d'autre qu'un ensemble de permissions. Les permissions accordées à un rôle sont opérations portant sur des objets. Concernant la plateforme Xplor EveryWhere, les objets à protéger sont les suivants

- Le portail web de la plateforme
- Les documents internes : tableaux de bord, documents de gestion, guides de procédure interne, compte rendu de réunion, de visites, les bilans …

- Les documents externes : courriers et courriels reçus, CV, etc…
- Les logiciels et applications : méta-moteur de recherche, explorateur de web, outil de data-mining, etc …
- Le corpus

Le corpus est l'ensemble des données collectées pour une l'activité de veille au sein de la plateforme. Les données peuvent provenir de la presse en ligne, des sites internet des clients et des fournisseurs, des forums et des blogs bases de données gratuites ou payantes, des réseaux sociaux sur Internet etc …

c. L'infrastructure de sécurité

- Outils cryptographiques : Pour chiffrer les données sensibles lors des échanges, notamment lors de laivraison des informations aux décideurs
- Référentiel des historiques des accès : Pour la traçabilité de toutes les activités menées. A tout moment, pour un utilisateur donné, ce référentiel renseigne sur les rôles activés, les tâches exécutées, ainsi que les durées nécessaires.
- Gestionnaire de worklist : Pour une session donnée (chaque fois qu'un utilisateur active un rôle pour exercer une tâche donnée), une worklist correspondante est générée conformément à la politique de sécurité et sur la base du référentiel des historiques. Elle comporte la succession de toutes les actions possibles pour l'utilisateur en question et permet ainsi à l'administrateur d'octroyer ou de refuser l'accès à chaque étape.
- Référentiels.

5 Conclusion

Sécuriser un système informatique est un problème indécidable : On ne peut pas conclure d'une manière définitive que le système est déjà sécurisé. Dans cet article, nous avons fait ressortir les risques de sécurité dans les plateformes d'IE et le besoin d'avoir en leur sein un service de contrôle d'accès. Sur la base de ces vulnérabilités, Les bases d'une approche générique de sécurité sont proposées et mises en pratique dans la palteforme d'IE Xplor EveryWhere. Toutefois, le contrôle d'accès est un projet graduel, qui évolue en fonction des disfonctionnements qui se produisent de temps à autre et qui sont malheureusement imprévisibles. Une étude par scénarios permet de recenser les disfonctionnement sous formes de patterns à fin de raffiner continuellement l'approche de sécurisation d'une plateforme d'IE : telles sont nos travaux pour un futur proche

6 Bibliographie

[1] **H. MARTRE, P. CLERC, C. HARBULOT, P. BAUMARD, B. FLEURY, D. VIOLLE**, *Rapport du Groupe «Intelligence économique et stratégie des entreprises»*, Commissariat général du Plan, France, February 1994.

[2] **A. EL HADDADI,** *Portail Web de Veille stratégique pour Mobile*. XXVII° congrès INFORSID, pp. 459-460, Toulouse, mai 2009.

[3] **J-P BICHARD**, *De la veille stratégique à la sécurité de l'information,* Décision Informatique, N° 625, Mars 2005

[4] **CLUSIF**. Club de la Sécurité de l'Information Français, *Menaces informatiques et pratiques de sécurité en France*, edition 2008.

[5] **E. B. TALBOT, D. FRINCKE, M. BISHOP,** *Demythifying Cybersecurity*, IEEE Security & Privacy, Vol 8, N° 3, May/Juin 2010

[6] **J-P BICHARD**, *De la veille stratégique à la sécurité de l'information*, Décision Informatique, N° 625, Mars 2005

[7] **I. P. COOK,** S. L. Pfleeger, "Security Decision Support Challenges in Data Collection and Use", IEEE Security & Privacy, Vol 8, N° 3, May/Juin 2010

[8] **SCIE Service de Coordination à l'Intelligence Economique**, *Guide des bonnes pratiques en matière d'intelligence économique*, Base de Connaissance AEGE, France, Février 2009. http://www.bdc.aege.fr

[9] **D. D. CAPUTO, G. D. STEPHENS, M. A. MALOOF**, *Detecting Insider Theft of Trade Secrets*, IEEE Security & Privacy, Vol 7, N° 6, November/December 2009

[10] **A. SHABTAL, Y. FLEDEL, Y. ELOVICI,** *Securing Android-Powered Mobile Devices Using SELinux*, IEEE Security & Privacy, Vol 8, N° 3, May/Juin 2010

[11] **K. J. HOLE, L-H. NETLAND,** *Toward Risk Assessment of Large-Impact and Rare Events*, IEEE Security & Privacy, Vol 8, N° 3, May/Juin 2010

[12] **ANSI**. American national standard for information technology – Role based access control. ANSI INCITS 359-2004, February 2004

[13] **H. EL BAKKALI, H. HATIM,** *RB-WAC: New approach for access control in workflows*, The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA'09), May 10-13, 2009 (pp 637-640).

[14] **R. A. BOTHA, J. H. P. ELOFF,** *Separation of duties for access control enforcement in workflow environments*, IBM Systems Journal, vol 40, n° 3, 2001 (pp 666-682).

[15] **K. BUYENS, B. D. WIN, W. JOOSEN,** *Resolving least privilege violations in software architectures*, In Proceedings of the ICSE Workshop on Software Engineering for Secure Systems (ICSE/SESS'09), May 19, 2009 (pp 9-16).

[16] **GHALAMALLAH I ,** Proposition d'un modèle d'analyse exploratoire multidimensionnelle dans un contexte d'intelligence economique, doctorat de l'université de toulouse, 18 décembre (2009).