ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 34412 B1

(43) Date de publication :
01.08.2013

(51) Cl. internationale :
H04L 29/06; G06Q 10/06; G06F 21/00

(21) N° Dépôt :
34408

(22) Date de Dépôt :
02.12.2011

(71) Demandeur(s) :
NETPEAS, RTE DE NOUACEUR TECHNOPARK BUREAU 345 CASABLANCA (MA)

(72) Inventeur(s) :
Nabil OUCHN ; Rachid HARRANDO

(74) Mandataire :
YOUSSEF LOTFY

(54) Titre : **SYSTEME ET METHODE POUR LA NOTATION L'EVALUATION ET LE CLASSEMENT DES ACTIFS DU SYSTEME D'INFORMATION**

(57) Abrégé : UNE SOLUTION («SCORISK R») INTÉGRÉE DANS LE CONCEPT «PLACE DE MARCHÉ COREVIDENCE R DES TECHNOLOGIES DE L'INFORMATION», DESTINÉE, DANS CET ENVIRONNEMENT, AU CALCUL ET À LA QUANTIFICATION DES NIVEAUX DE RISQUE PENDANT LES SCANS D'ANALYSE OU DE CONFORMITÉ (ASSESSMENT OR COMPLIANCE SCANS), SUR LA BASE DES CRITÈRES STRUCTURÉS SUIVANTS: LA PRÉCISION, C-À-D LES VULNÉRABILITÉS COMMUNES RAPPORTÉES PAR TOUS LES MOTEURS DE SCAN IMPLIQUÉS; LA PONDÉRATION (OU POIDS), BASÉE SUR LA CLASSIFICATION (SCORING) EN MATIÈRE DE SÉVÉRITÉ ET EXPLOITABILITÉ DU SYSTÈME D'ÉVALUATION CVSS V.0; LE REPÉRAGE PRÉDÉTERMINÉ, OU CLASSIFICATION, LORSQUE LA VULNÉRABILITÉ EST REPÉRÉE EN TANT QUE PARTIE D'UNE LISTE DE RISQUES MAJEURS SELON LA LISTE ORDONNÉE CWE/SANS TOP 25; LA PERSISTANCE, CRITÈRE MESURANT LA LONGÉVITÉ DE LA VULNÉRABILITÉ; SOLUTION CONCERNANT UNE APPROCHE INTÉGRÉE ET GLOBALE DE LA SÉCURITÉ DES ACTIFS. (FIGURE 2, FIGURE 3).

ABREGE DESCRIPTIF

« Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information ».

Une solution (« SCORISK ® ») intégrée dans le Concept « Place de Marché COREvidence ® des Technologies de l'Information », destinée, dans cet environnement, au calcul et à la quantification des niveaux de risque pendant les scans d'analyse ou de conformité (*assessment or compliance scans*), sur la base des critères structurés suivants : la Précision, c-à-d les Vulnérabilités Communes rapportées par tous les moteurs de scan impliqués ; la Pondération (ou poids), basée sur la classification (*scoring*) en matière de sévérité et exploitabilité du système d'évaluation *CVSS v2.0* ; le Repérage prédéterminé, ou Classification, lorsque la vulnérabilité est repérée en tant que partie d'une liste de risques majeurs selon la liste ordonnée *CWE/SANS Top 25 ; la* Persistance, critère mesurant la longévité de la vulnérabilité ; solution concernant une approche intégrée et globale de la sécurité des actifs. (Figure 2, Figure 3).

MA 34412B1

01 AOUT 2013

Système et Méthode pour la notation, l'évaluation et le classement des actifs du système d'information

Inventeurs : **Rachid HARRANDO - Nabil OUCHN**

La présente invention a pour objet un système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information des organisations.

La présente invention concerne le domaine de la gestion des vulnérabilités des systèmes informatiques, et se positionne dans un domaine beaucoup plus vaste qui est connu couramment comme « Logiciel en tant que Service » (en anglais *Software as a Service* ou *SaaS*), qui a connu toutes ces dernières années des développements importants, et qui semble vouloir se continuer fortement avec de larges applications telles que la "virtualisation" et le *cloud computing*, et autres développements réseaux et en ligne. La gestion globale des vulnérabilités s'entend dans la présente invention en tant qu'approche nouvelle, homogène et plus complète, voire globale, de la sécurité des systèmes informatiques. Ainsi, la présente invention se classe dans ce qu'il est possible de dénommer « La Sécurité en SaaS ». Une meilleure compréhension de la présente invention est de considérer qu'elle a été conçue pour auditer et analyser la sécurité des systèmes d'information, et apporter une solution ordonnée, systématique, exhaustive, intégrée et en temps réel.

Note : Dans ce qui suit, en raison de la prépondérance inévitable des expressions anglaises dans les technologies de l'information (TI), il leur sera le plus souvent référé entre parenthèses, et ces expressions ou abréviations seront en italique.

Parmi les fonctionnalités globales du système décrit ici, il y a lieu d'insister en premier lieu sur le caractère intégré de la solution présentée, par rapport à l'état de la technique antérieure. En effet, les besoins en matière de sécurité des systèmes informatiques sont très variés : Gestion des Vulnérabilités, Evaluation des risques, Suivi/Surveillance (*Monitoring*), Evaluation des applications, Détection et maîtrise/réduction des *Malware*, ...etc. Dans la pratique et sur le marché, chaque Editeur est focalisé sur son domaine plus ou moins délimité. Cependant, comme conséquences, les utilisateurs de telles solutions qui souhaitent couvrir un maximum d'aspects de la sécurité des systèmes informatiques se trouvent dans l'obligation d'acquérir plusieurs solutions. Ce constat fait qu'une vision globale de la sécurité s'avère une tâche très difficile à réaliser pour les raisons ci-après : problèmes d'agrégation des données, compatibilité des rapports due à la multiplicité et à la variété des documents récupérés, différences dans la gestion des équipes de support, tarifications différentes, plans de règlements différents, temps et efforts considérables – et répétitifs - pour comparer les éditeurs de solutions, modalités de classement des rapports, etc. A ces problèmes, il y a encore lieu de rajouter que certaines Solutions ne sont pas en *SaaS*, ce qui a pour résultats de les rendre plus

coûteuses et de mobiliser plus de ressources humaines et matérielles. En synthèse sur l'état actuel de la technique, la vaste hétérogénéité des infrastructures des systèmes d'informations rend complexe une évaluation complète en s'en tenant aux solutions de sécurité existantes sur le marché.

Au-delà des fonctionnalités globales du système décrit ici, qui seront plus détaillées ci-après, il y a lieu d'insister sur ses principaux avantages qui sont un gain de temps et une productivité considérables, en raison du fait qu'en matière d'analyse des données de sécurité, le problème qui se pose est d'arriver rapidement à identifier et isoler les priorités avec la plus grande garantie - techniquement et méthodologiquement possible - que ces priorités sont effectivement pertinentes. La solution qui répond efficacement à cette problématique est à présent disponible et porte la dénomination « COREvidence ® ».

Le résumé suivant de cette solution est fourni à titre d'explication seulement, car elle constitue le cadre de l'invention, qui concerne en effet la solution technique – précisée ci-après – exposée en détail dans le présent descriptif.

La solution « COREvidence » possède donc la particularité d'agréger le contenu de plusieurs API ou moteurs de scan. Le résultat recherché et obtenu est la définition du niveau d'identification de Vulnérabilités communes, encore conçu comme ensemble de Vulnérabilités communes à plusieurs moteurs 'de scan. Ce résultat est en soi une réponse au problème fréquemment posé de la précision des audits et des 'faux-positifs' qui peuvent en résulter. L'importance de la définition de cet environnement lui a valu l'appellation de « Concept de Place de Marché COREvidence des Technologies de l'Information » (*The COREvidence IT Security Marketplace Concept*).

Et c'est à ce niveau qu'intervient la présente invention, en constituant l'élément central de ce concept, qui permet le calcul et la quantification des niveaux de risque pendant les scans d'analyse ou de conformité (*assessment or compliance scans*).

En d'autres termes, la technologie constituante de la présente invention est le concept 'propriétaire' (spécifique) de COREvidence pour l'évaluation méthodologique et quantitative des risques attachés aux actifs, qui fondamentalement est basée sur les critères suivants, comme il sera détaillé plus avant :

Précision : Les Vulnérabilités Communes rapportées par tous les moteurs de scan impliqués. Plus ce ratio est élevé, plus la vulnérabilité est considérée comme sûre.

Pondération (ou poids) : Ceci est basé sur la classification (*scoring*) en matière de sévérité et exploitabilité du système d'évaluation *CVSS v2.0*.

Repérage prédéterminé ou Classification : Marqué lorsque la vulnérabilité est repérée en tant que partie d'une liste de risques majeurs selon la liste ordonnée *CWE/SANS Top 25.*

Persistance : Ce critère mesure la longévité de la vulnérabilité. Ceci signifie que le problème a été trouvé lors d'une session de scan précédente.

Avant d'exposer la structure constitutive du système et méthode objets de l'invention, et pour mieux faire comprendre au lecteur l'importance des problèmes techniques que s'attache à résoudre l'invention, il est utile tout d'abord d'examiner l'état de la technique antérieure. Ceci sera fait de préférence de manière synthétique, à travers le Tableau de la Figure 1 / Art Antérieur (*Prior Art*) annexé au présent descriptif.

L'examen de ce tableau, où figure le système de la présente invention sous l'abréviation Netpeas/('Scorisk'), montre clairement qu'il existe plus de dix solutions de notation, évaluation et classement des actifs d'un système d'information, portant différents noms ou abréviations. Pour l'homme de l'art, ces solutions portent aussi un historique, qui explique en grande part pour certaines les lacunes de ces solutions listées, et par voie de conséquence valorisent directement la présente solution technique et son approche plus globale. Ainsi que le montre donc ce tableau comparatif, la plupart des solutions du marché ne couvrent qu'une partie des fonctionnalités que couvre la solution sous la colonne 'Netpeas', tendant vers la globalité et l'unicité de la proposition.

Dans ce qui suit, on verra également que la gestion de la résolution est améliorée grâce à cet outil car elle fournit un environnement multiple-utilisateurs et centralisé, avec un suivi et une traçabilité des actions menées.

Enfin, le coût mutualisé des différentes solutions intégrées dans le système apporte un cout moindre grâce au modèle économique en mode Logiciel en tant que Service, ou *"As a Service" [SaaS].*

Au plan opérationnel, il convient de rappeler également que dans l'état de l'art actuel, les évaluations complètes de systèmes de sécurité informatique sont effectuées par les cabinets de conseil spécialisés, sur une base périodique. La qualité du travail des vérificateurs est tributaire de la capacité de l'auditeur d'avoir connaissance des dernières menaces de sécurité. En outre, une menace pour la sécurité peut se produire immédiatement après l'audit et donc passer inaperçue pendant une longue période – qui peut atteindre des mois. Ces audits sont donc en définitive coûteux, irréguliers, et ne peuvent être exhaustifs ni, malheureusement, sûrs.

Le but ultime de la présente invention est ainsi de résoudre ces problèmes technologiques et méthodologiques par la mise en œuvre d'une seule solution intégrée, dont la structure, les Fonctionnalités et le Mode Opératoire seront plus explicités et illustrés ci-après.

Les explications complémentaires sur l'environnement COREvidence, qui suivent, sont destinées au lecteur pour lui permettre de mieux comprendre l'invention, tout en considérant qu'elles sont fournies pour son information uniquement, et ne sont destinées à limiter la portée de la présente divulgation en aucune manière.

Le système COREvidence est structuré comme suit :

Basé sur une multiplicité de Scanners de vulnérabilité de réseaux

- Scanners automatisés d'Applications et de Services Réseau (*web)*
- Modèles prédéfinis de Scanning Réglementaires et Standards
- Tests de Pénétration et boîte à outils à la demande, de piratage informatique 'éthique'.
- Scanner de sécurité à distance de Voix sur Internet (*VoIP*)
- Questionnaires d'Autoévaluation Techniques et Organisationnels (NIST, CIS, ISO27001, PCI DSS ...)
- Outils de Sécurité et Logiciels malveillants, Exécution de Ressources Frontales
- Scans d'outils (Open Source & Commercial) et Capacités d'importation de sondes
- Service de Vulnérabilité TI et de Surveillance des Outils.

Bénéfices apportés par le Système :

- Flexibilité d'utilisation basée sur Plan de crédit
- Plans de Souscription sur mesure pour les Consultants SMB et Libres (*Freelance*)
- Scans précis utilisant des APIs Multiples et des Moteurs de Scan
- Scans illimités & Suivi (*Monitoring*) d'Actifs Fixes ou Variables
- Interface facile et apte à être personnalisée.
- Rapports Consolidés, Précis et Unifiés

Fonctionnalités :

- Base de Données de Vulnérabilités à Spectre Complet & Capacités d' Exploits basées sur les Ressources CVE, CWE, CVSS, CPE ...
- Scanning d'Application *Web* basée sur OWASP & de Vulnérabilités de

Services *Web*

- Réalise les compatibilités avec les Règlements et Standards Internationaux (COBIT, ISO 27001, SOX, PCI DSS, HIPAA, GLBA, FISMA, SCAP, FDCC, NERC ...etc.).
- Importe, corrèle et affiche vers des tableaux de bord tous les résultats bruts *'IT Friendly-Probes'* tels que OVAL, OpenVAS, Nessus, Nmap, Open SCAP ...etc.
- Questionnaires d'Auto-évaluation et listes de contrôle pour ISO 27001, PCI DSS v2.0, iSeries AS/400, CIS Benchmarks, NIST SCAP ...
- Canal de Communication Collaborative pour interagir entre toutes les Parties prenantes
- Interprétation facile de l'Information à travers de puissant tableaux de Bord, Graphiques et les tableaux d'affichage propriété de la Société NETpeas. Les Métriques sont compatibles avec *CIS Security Metrics*

A titre complémentaire, il convient d'indiquer à l'intention de l'homme de l'art que, outre COREvidence, la mise en œuvre de tout le système - et par voie de conséquence l'invention objet des présentes - est supportée par le développement de programmes complémentaires *ad hoc,* spécialement :

- Interface graphique
- Interface Homme-Machine simplifiée de gestion des vulnérabilités
- Table d'analogie avec les tables d'exploits

En résumé, substantiellement, la présente invention présente un Système complet d'évaluation quantitative qui procure un classement sur ce critère, des actifs du système d'information.

Dans la pratique opérationnelle, nous avons adopté une notation graduelle à cinq niveaux (A à E), avec des niveaux de couleurs depuis le vert jusqu'au rouge, pour signifier le niveau de vulnérabilité de l'actif.

Illustrations

Nous illustrerons le concept de l'invention au moyen de formules, de tableaux et de graphismes spécifiques, qui ne sont en aucun cas restrictifs de l'expression ou de la portée de l'invention. Ces éléments sont prioritairement fournis pour établir définitivement le caractère opérationnel du système et faire comprendre globalement la solution apportée à la problématique technique et méthodologique de l'évaluation des actifs au regard des risques.

La Figure 1, déjà citée, représente l'état de l'art antérieur.

La Figure 2 est une représentation schématique de la **structure** du Système « Scorisk », montrant les quatre pôles constituant la base du système et leurs interrelations, ainsi que les principales fonctionnalités assurées par cette disposition spéciale.

La Figure 3 représente en synthèse l'évaluation de types d'actifs, telle qu'elle découle de l'application de l'invention. Sont représentés trois cas illustratifs, comme suit :

- Figure 3.1: ScoRisk montrant un actif avec rang C (abaissé de B à C)
- Figure 3.2: ScoRisk montrant un actif avec rang A (amélioré de D à A)
- Figure 3.3: Une autre représentation possible de ScoRisk montrant un actif avec Rang C

Ce cadre étant établi, l'expression de l'invention se décline en étapes et procédures spécifiques qui sont décrites ci-après, essentiellement en tant qu'exemples concrets de l'application du système, qui par ailleurs révèlent une méthodologie et des modes opératoires précis. On procède donc comme suit ou de manière similaire aux étapes ci-après exposées.

On suppose un nombre 'n' de Moteurs de Scan ou (n APIs), impliqués dans un processus de scan (comme on pourrait s'y référer dans COREvidence) et nous considérons les formules suivantes :

Niveau 1 Vulnérabilités Communes (VC) = VC identifiées avec 'n' APIs

Niveau 2 Vulnérabilités Communes (VC) = VC identifiées avec (n-1) APIs ...

Niveau 'N' Vulnérabilités Communes (VC) = VC rapportées avec chaque API

L'exemple suivant schématise le concept :

API 1	API 2	API 3
Bug A	Bug B	Bug B
Bug C	Bug C	Bug D
Bug E	Bug Z	Bug E
Bug I	Bug M	Bug N

Tableau 1 : Vulnérabilités rapportées par chaque Moteur de Scan

Par l'application de la formule, trois niveaux seront déterminés (du fait de 3 APIs dans cet exemple) :

Niveau 1 Vulnérabilités Communes
Bug F (API 1 & 2 & 3)
Bug W (API 1 & 2 & 3)
Niveau 2 Vulnérabilités Communes
Bug B (API 2 & 3)
Bug C (API 1 & 2)
Bug E (API 1 & 3)
Niveau 3 Vulnérabilités Communes
Bug A (API 1)
Bug I (API 1)
Bug Z (API 2)
Bug M (API 2)
Bug D (API 3)
Bug N (API 3)

Tableau 2 : Les différents niveaux de corrélation

On définit par convention dans ce qui suit les éléments ci-après :

v: Vulnérabilité
n : le nombre d'APIs
L : est le niveau = (Nb (API) - 1) (3 APIs si le nombre de niveaux est 2)
Occurrence : le Nombre de fois que la Vulnérabilité est détectée par les APIs. Une vulnérabilité est détectée *n* fois (par tous les APIs impliqués) jusqu'à 1 fois (par 1 API).

Ratio (v) = Occurrence (v) / n * 100

GR (Global Ratio) = Somme (Ratio (v)) i / (Total des Ratios sauf Niveau 1) * 100

(i allant de n à L). En fait, nous ne calculons pas les vulnérabilités de niveau 1. Ce qui est normal, puisque nous recherchons celles trouvées par plusieurs APIs.

Score +2 si Global Ratio >= 80 %

Score + 1 si Global Ratio <50 < 70 %

Score +0 si pas de commune vulnérabilité

Le tableau qui suit montre comment le Ratio et le Global Ratio sont calculés en utilisant l'exemple montré au Tableau 1 immédiatement ci-dessus.

Vulnérabilité Trouvée	Occurrence	Ratio(v)
A	1	(1/3) * 100 = 33,3 %
B	**2**	**66,6 %**
C	**2**	**66,6 %**
D	1	33,3 %
E	**2**	**66,6 %**
F	**3**	**100 %**
W	**3**	**100 %**
I	1	33,3 %
Z	1	33,3 %
M	1	33,3 %
GR (Global Ratio)	(66,6 % + 66,6 % + 66,6 % + 100 % + 100 %) / 5 * 100 **GR = 80 %**	
Score Global	**+ 2 (du fait que GR >= 75 %)**	

- **Notes**
- *Max Occurrence = n et Minimum = 1*
- *Vulnérabilités Ratio(v) avec occurrence = 1 ne sont pas tenues en considération pour le calcul*
- *5 est le nombre de vulnérabilités uniques identifiées dans le niveau (L) ; (L est n - 1) (Dans cet exemple.).*

Par application des éléments fondamentaux du Système on obtient :

- **Poids de la Vulnérabilité.** Ce critère est basé sur le système de '*scoring*' CVSS v2.0. L'exception étant l'exploit CVSS égal à 10.

- **Repérage :** Si l'une quelconque des vulnérabilités identifiée par un API fait partie de la liste publiée par le SANS / CWE Top 25

- **Persistance**: La loi décrite dans ' QUALYS - Les lois de vulnérabilités 2.0' permet de mesurer la longévité d'une vulnérabilité. Cela est, si l'une des vulnérabilités appartenant au niveau le plus haut (identifiée comme exacte) est détectée lors d'une nouvelle session.

La Table qui suit résume les calculs de score ('Guide de Notation de ScorRisk' (*ScoRISK Rating Guide*)) :

Guide de Notation ScoRISK (*Rating Guide*)			
Précision / Exactitude	GR >= 75 %		**+ 2**
	50 < GR < 74 %		**+ 1**
	Pas de Vulnérabilités Communes		**+ 0**
Poids	Sévérité	Moyenne (base CVSS) > 8	**+ 2**
		Moyenne (base CVSS) > 5	**+ 1**
		Moyenne (base CVSS) < 3	**+ 0**
	Exploitabilité	Exception : exploit score CVSS = 10	**+ 2**
		Moyenne (exploit CVSS) > 8	**+ 2**
		Moyenne (exploit CVSS) > 5	**+ 1**
		Moyenne (exploit CVSS) < 3	**+ 0**
Repérage / Positionnement	Oui (base liste CWE/SANS)		**+ 2**
	Non		**+ 0**
Persistance	Oui - si fenêtre d'exposition >= 90 jours		**+ 2**
	Oui - si fenêtre d'exposition >= 30 jours		**+ 1**
	Non		**+ 0**

La Table qui suit résume les Grades de Qualité ScoRISK (*ScoRISK Quality Grades*) utilisés pour marquer un actif :

Grades de Qualité ScoRISK (*Quality Grades*)		
A	**Excellent Classement** Position entre 0 et 2. **Exception** : *CVSS exploit score* égal à 10. L'actif est dégradé au Grade B.	Convient pour pare-feux, (*Firewalls*), dispositifs de filtrage, appareils de sécurité, serveurs hautement blindés, services de banque et de paiement.
B	**Bon Classement** Position entre 3 et 4.	Convient pour services web frontaux.

		Quelques serveurs communs (messagerie web, serveurs web de sociétés)
C	**Faible Classement** Position entre 5 et 7.	
D	**Mauvais Classement** Position entre 8 et 9.	
E	**Très Mauvais Classement** Position > 10	

En conclusion, ce système mène bien à la notation, l'évaluation et le classement des actifs comme proposé, avec essentiellement une expression très simple et condensée des résultats, résolvant par là même la problématique identifiée et susmentionnée, et permettant donc de positionner la présente invention au-devant de l'état de l'art antérieur tel que schématisé et résumé dans le Tableau Figure 1.

REVENDICATIONS

1 - Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information, constituant l'élément central du concept de « Place de Marché COREvidence® des Technologies de l'Information », une solution qui possède la particularité d'agréger le contenu de plusieurs API ou moteurs de scan, et approche-cadre dont le but premier est la définition du niveau d'identification de Vulnérabilités communes, encore conçu comme ensemble de Vulnérabilités communes à plusieurs moteurs de scan, et résultat constituant en soi une réponse au problème fréquemment posé de la précision des audits et des 'faux-positifs' qui peuvent en résulter, ayant comme principaux avantages un gain de temps et une productivité considérables, en raison du fait qu'en matière d'analyse des données de sécurité, le problème qui se pose est d'arriver rapidement à identifier et isoler les priorités avec la plus grande garantie techniquement et méthodologiquement possible, que ces priorités sont effectivement pertinentes ; solution dans le cadre ainsi décrit, caractérisée par la possibilité de calcul et de quantification des niveaux de risque pendant les scans d'analyse ou de conformité (*assessment or compliance scans*), sur la base au moins des critères structurés suivants : la Précision, c-à-d les Vulnérabilités Communes rapportées par tous les moteurs de scan impliqués ; la Pondération (ou poids), basée sur la classification (*scoring*) en matière de sévérité et exploitabilité du système d'évaluation *CVSS v2.0* ; le Repérage prédéterminé, ou Classification, lorsque la vulnérabilité est repérée en tant que partie d'une liste de risques majeurs selon la liste ordonnée *CWE/SANS Top 25 ; la* Persistance, critère mesurant la longévité de la vulnérabilité. (Figures 1 à 3).

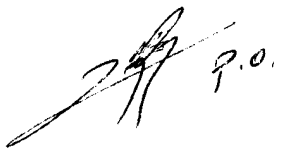
2 - Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information, selon Revendication 1, caractérisé en ce que, au titre d'une solution intégrée, répondant à des besoins en matière de sécurité des systèmes informatiques très variés elle résout notamment les problèmes suivants: gestion des Vulnérabilités, évaluation des risques, suivi/surveillance (*Monitoring*), évaluation des applications, détection et maîtrise et réduction des Logiciels Malveillants (*Malware)*, ...etc.

3 - Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information, selon Revendications 1 et 2, caractérisé en ce que - étant donné que dans la pratique et sur le marché, chaque Editeur est focalisé sur son domaine plus ou moins délimité - avec comme conséquences que les utilisateurs de telles solutions qui souhaitent couvrir un maximum d'aspects de la sécurité des systèmes informatiques se trouvent dans l'obligation d'acquérir plusieurs solutions - cette solution apporte une vision globale de la sécurité, évitant notamment aux exploitants les problèmes de : agrégation des données, difficile compatibilité des rapports due à la multiplicité et à la variété des documents récupérés, différences dans la gestion des équipes de support, tarifications différentes, plans de règlements différents, temps et efforts considérables et répétitifs, pour comparer les éditeurs de solutions, et modalités disparates de classement des rapports.

4 - Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information, selon Revendications 1 à 3, caractérisé en ce que, dans le but pour le client de minimiser le coût de la Solution, notamment en termes de ressources humaines matérielles et méthodologiques, ladite solution est prodiguée en mode SaaS, ou Logiciel en tant que Service.

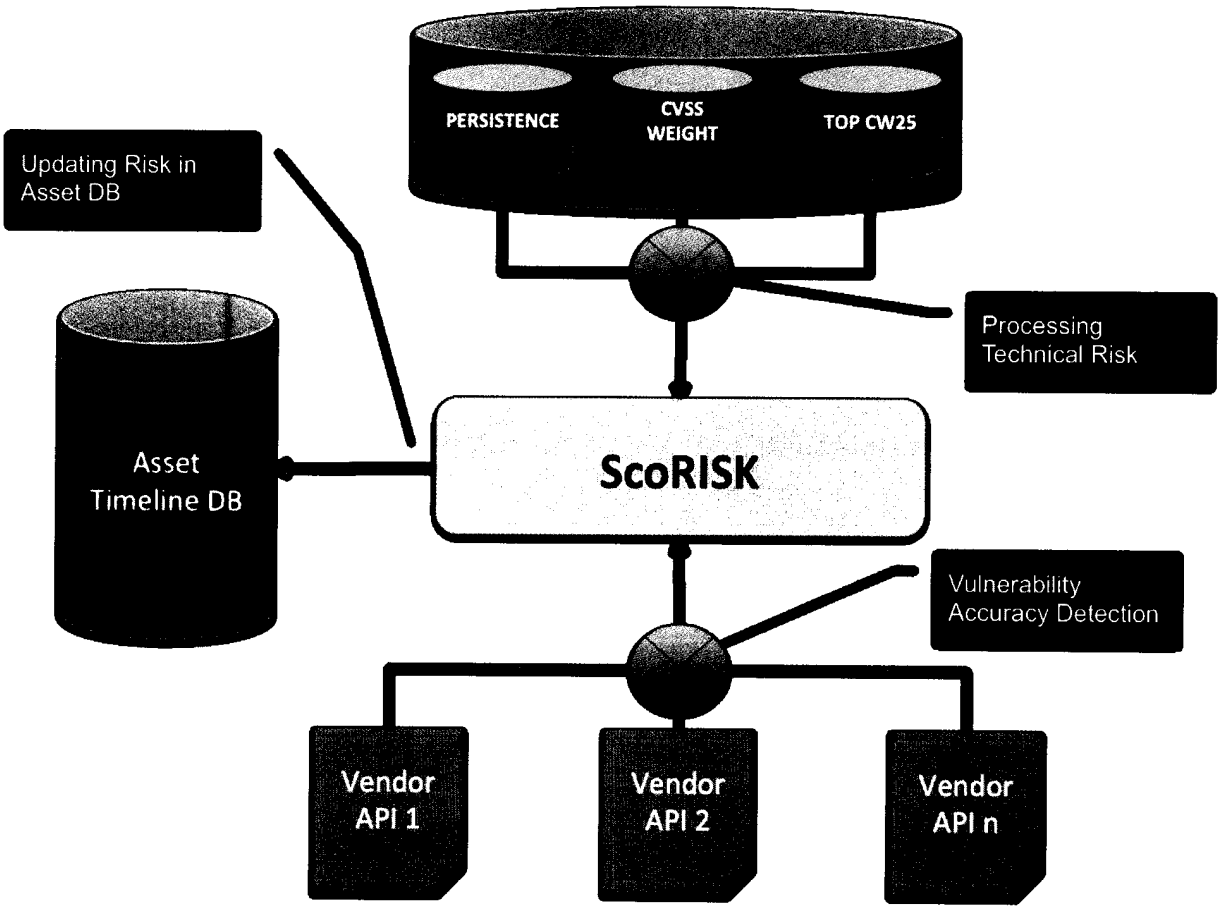
5 - Système et méthode pour la notation, l'évaluation et le classement des actifs du système d'information, selon Revendications 1 à 4, caractérisé en ce que cette Solution est déployée pour pallier à la vaste hétérogénéité des infrastructures des systèmes d'informations, qui dans l'état actuel de la technique rend complexe une évaluation complète en s'en tenant aux solutions disparates de sécurité existantes sur le marché, en constituant une solution unique, exhaustive et intégrée.

Rachid HARRANDO ***Nabil OUCHN***



In Green means integrated Inside COREvidence	[redacted]	HackersLocker	HackerTarget	WhiteHAT Sentinel	Symantec VSS	Qualys	Rapid7	Auditor	Saint SaaS	Nessus SaaS	NOPSEC	Risk I/O	T
Marketplace position	YES	NO	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	
Complete VM Engine	YES	?	?	YES	Yes	yes	yes	YES	YES	YES	YES	NO	
WAS Engine	YES		Equivalent to their 40	YES	Yes	YES	not good	YES	NO	YES	YES	NO	
Malware Analysis Scanner	YES	NO	NO	NO	YES	YES	NO	YES	NO	NO	YES	NO	
VOIP Engine	YES	NO	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	
Checklist	in Plan	NO	NO	NO	NO	YES	YES	YES	NO	NO	NO	NO	
Import	in Plan	NO	NO	NO	NO	NO	YES	YES	NO	NO	NO	YES	
Vellis	YES	NO	NO	YES	NO	YES	YES	YES	NO	NO	NO	NO	
Price per IP Unlimited/month	500 $	55$, web site ON	89$ (not even co	NO	YES	YES	YES	NO	YES.1500	[redacted]	YES	900 $	
Price for complete 1VM	300 $	NO	NO	NO	NO	YEs	NO	YES	YES	YES	YES	NO	
Monitoring	YES	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	NO	
Pay Online	YES	?	YES, Paypal C	NO	NO	NO	NO	NO	YES	YES	NO	NO	
White Label	In Plan	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	
FREE trial	YES	NO	YES	YES	NO	YES	NO	NO	NO	NO	NO	YES	
Compliance Templates ready	NO. In pl	[redacted]	NO	YES	YES	YES	YES	YES	YES	YES	NO	YES	
Multi-users/Collaborative	YES	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	YES	
Agregation, Correlation	YES	NO	NO	No	NO	NO	NO	YES	NO	NO	NO	YES	
Commercial tools	YES	NO	NO	YES	YES	YES	YES	NO	YES	YES	NO	YES	
NETwork discovery	YES	NO	YES	YES	YES	YES	YEs	YES	YES	YES	NO	NO	
Ticketing system	YES	[redacted]	NO	NO	NO	YES	NO	NO	NO	YES	NO	YES	
RACI model	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	
Integrated FREE scanners	YES	YES	YES	NO	NO	NO	NO	YES	NO	YES	YES	NO	
TREND	In Plan (V	YES	?	YES	YES	YES	YES	YES	NO		YES	YES	
Exploit/PENTEST	YES	NO	NO	NO	NO	NO	YES	YES	YES	YES	NO	NO	

Figure 1 Art Antérieur (*Prior Art*)



LEGENDE :

- **SCORISK : Système Solution exposé**
- **Vendor API : Fournisseur Moteur de scan**
- **Asset Timeline DB : Base de Données des mises à jour**
- **Updating Risk in Asset DB : (Process)Mises à jour des Risques dans la BD**
- **Processing Technical Risk : (Process)Traitement des Risques Techniques**
- **Vulnerability Accuracy detection : (Process) Detection de l'Exactitude des Vulnérabilités**

Figure 2

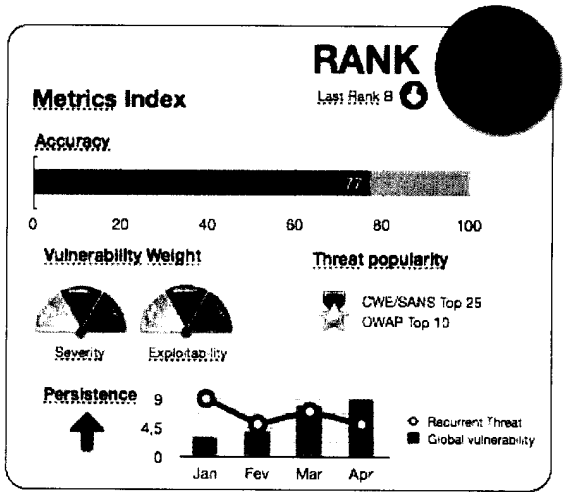


Fig 3.1

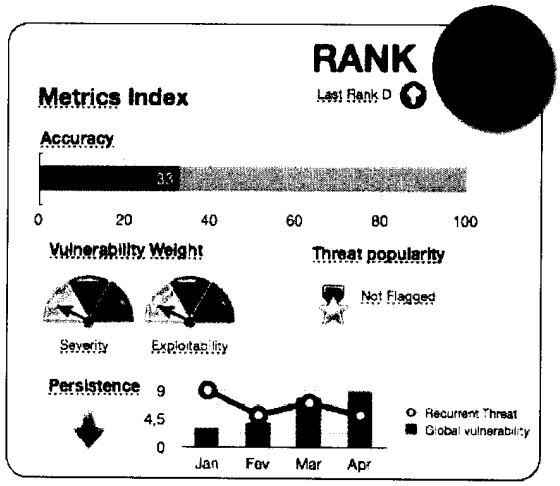


Fig 3.2

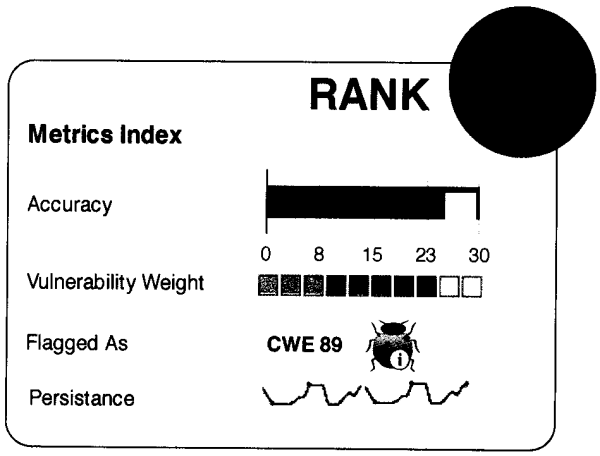


Fig 3.3

Figure 3