Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1570

(09/2011)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Identification et découverte

Mécanismes de découverte pour l'échange d'informations de cybersécurité

Recommandation UIT-T X.1570

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	**X.1570–X.1579**
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1570

Mécanismes de découverte pour l'échange d'informations de cybersécurité

Résumé

La Recommandation UIT-T X.1570 décrit un cadre pour la découverte d'informations de cybersécurité et le mécanisme associé. La découverte peut être considérée comme une étape du cycle de vie des informations de cybersécurité, avec la publication et l'acquisition d'informations, qui sont des étapes à part entière et nécessaires pour la découverte. Cela étant, le cadre couvre la façon de publier les informations de cybersécurité, d'obtenir la liste de sources possibles et d'acquérir les informations nécessaires. Un système de découverte peut être implémenté avec des mécanismes arbitraires pour autant qu'ils soient conformes au cadre. Ces mécanismes comprennent notamment la découverte fondée sur l'identificateur d'objet (OID, *object identifier*) et la découverte fondée sur le cadre de description des ressources (RDF, *resource description framework*), qui sont également traitées dans cette Recommandation.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1570	2011-09-02	17

Mots clés

Découverte d'informations, découverte de sources, informations de cybersécurité.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

L'importance accordée à l'échange d'informations de cybersécurité est aujourd'hui plus grande que jamais. A cet égard, une norme internationale relative à l'échange d'informations de cybersécurité, appelée CYBEX, suscite une attention toute particulière. La découverte CYBEX, qui offre un moyen de trouver la source d'informations de cybersécurité, figure au nombre des diverses spécifications techniques CYBEX. Le cadre et les techniques de découverte sont exposés dans la présente Recommandation.

Recommandation UIT-T X.1570

Mécanismes de découverte pour l'échange d'informations de cybersécurité

1 Domaine d'application

La présente Recommandation décrit un cadre pour la découverte d'informations de cybersécurité et le mécanisme associé. La découverte peut être considérée comme une étape du cycle de vie des informations de cybersécurité, avec la publication et l'acquisition d'informations, qui sont des étapes à part entière et nécessaires pour la découverte. Cela étant, le cadre couvre la façon de publier les informations de cybersécurité, d'obtenir la liste de sources possibles et d'acquérir les informations nécessaires. Un système de découverte peut être implémenté avec des mécanismes arbitraires pour autant qu'ils soient conformes au cadre. Ces mécanismes comprennent notamment la découverte fondée sur l'identificateur d'objet (OID, *object identifier*) et la découverte fondée sur le cadre de description des ressources (RDF, *resource description framework*), qui sont également traitées dans la présente Recommandation.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.660] Recommandation UIT-T X.660 (2011) | ISO/CEI 9834-1:2012, *Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet: procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationaux.*

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax.*
<http://www.w3.org/TR/rdf-concepts/>

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants qui sont définis ailleurs:

3.1.1 identificateur d'objet [UIT-T X.660]: suite ordonnée de valeurs entières primaires allant de la racine de l'arbre des identificateurs d'objet internationaux jusqu'à un nœud, et identifiant ledit nœud sans ambiguïté.

3.1.2 ontologie [b-Gruber]: spécification explicite d'une conceptualisation.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 informations de cybersécurité: informations ou connaissances structurées concernant:

1) l'état des équipements, des logiciels ou des systèmes en réseau eu égard à la cybersécurité et en particulier aux vulnérabilités;

2) les investigations relatives aux incidents ou aux événements;

3) les données heuristiques et les signatures provenant d'événements passés;

4) les entités qui implémentent des capacités d'échange d'informations de cybersécurité dans le contexte de ce cadre;

5) les spécifications relatives à l'échange d'informations de cybersécurité, y compris les modules, les schémas, les politiques et les numéros attribués;

6) les identités et les attributs de confiance pour tout ce qui précède;

7) les exigences d'implémentation, les lignes directrices et les pratiques.

NOTE – Cette définition repose sur la description des informations de cybersécurité donnée dans [b-UIT-T X.1500].

3.2.2 échange (d'informations de cybersécurité): transfert d'informations de cybersécurité entre au moins deux entités de cybersécurité. Ce transfert peut être unidirectionnel, bidirectionnel ou multidirectionnel, c'est-à-dire multipoint à multipoint.

3.2.3 découverte: fait de découvrir la cible, c'est-à-dire de prendre connaissance de la cible pour la première fois.

3.2.4 entité effectuant la recherche: entité qui extrait des informations de cybersécurité.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CCE liste des configurations courantes (*common configuration enumeration*)

CERT équipe d'intervention en cas d'urgence informatique (*computer emergency response team*)

CIRT équipe d'intervention en cas d'incident informatique (*computer incident response team*)

CPE liste des plates-formes courantes (*common platform enumeration*)

CVE vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)

CVSS système d'évaluation des vulnérabilités courantes (*common vulnerability scoring system*)

CWE liste des failles courantes (*common weakness enumeration*)

CWSS système d'évaluation des failles courantes (*common weakness scoring system*)

CYBEX échange d'informations de cybersécurité (*cybersecurity information exchange*)

HTTP protocole de transfert d'hypertexte (*hypertext transfer protocol*)

IODEF format d'échange de description d'objet incident (*incident object description exchange format*)

MAEC liste et caractérisation des attributs des logiciels malveillants (*malware attribute enumeration and characterization*)

OID identificateur d'objet (*object identifier*)

OVAL langage ouvert d'évaluation des vulnérabilités (*open vulnerability and assessment language*)

RDF cadre de description des ressources (*resource description framework*)

SCAP protocole d'automatisation des contenus de sécurité (*security content automation protocol*)

SNMP protocole simple de gestion du réseau (*simple network management protocol*)

XCCDF format extensible de description de la liste de points à vérifier dans la configuration (*extensible configuration checklist description format*)

5 Conventions

Sans objet.

6 Cadre pour l'identification et la localisation de la source d'informations de cybersécurité

Différentes organisations s'occupant de cybersécurité implémentent des protocoles communs de cybersécurité pour saisir et échanger des informations sur l'état des systèmes, les vulnérabilités, les investigations relatives aux incidents et les données heuristiques relatives aux incidents, dans des applications opérationnelles. Étant donné que ces informations proviennent de nombreuses sources différentes, les entités chargées de l'implémentation doivent harmoniser la méthode d'identification des organisations s'occupant de cybersécurité, les politiques de confiance et d'échange d'informations, et les informations proprement dites qui sont échangées ou distribuées. A cette fin, le présent paragraphe décrit un cadre permettant d'identifier et de localiser la source d'informations de cybersécurité – le cadre pour la découverte d'informations de cybersécurité.

Trois entités interviennent dans la recherche d'informations de cybersécurité: l'entité effectuant la recherche, la source et le répertoire. L'entité effectuant la recherche envoie une demande pour extraire des informations, la source fournit les informations demandées, et le répertoire enregistre les métadonnées des informations émanant de la source et aide l'entité effectuant la recherche à trouver une source appropriée.

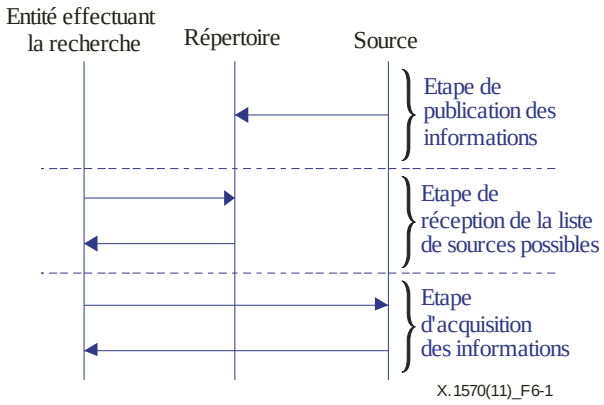
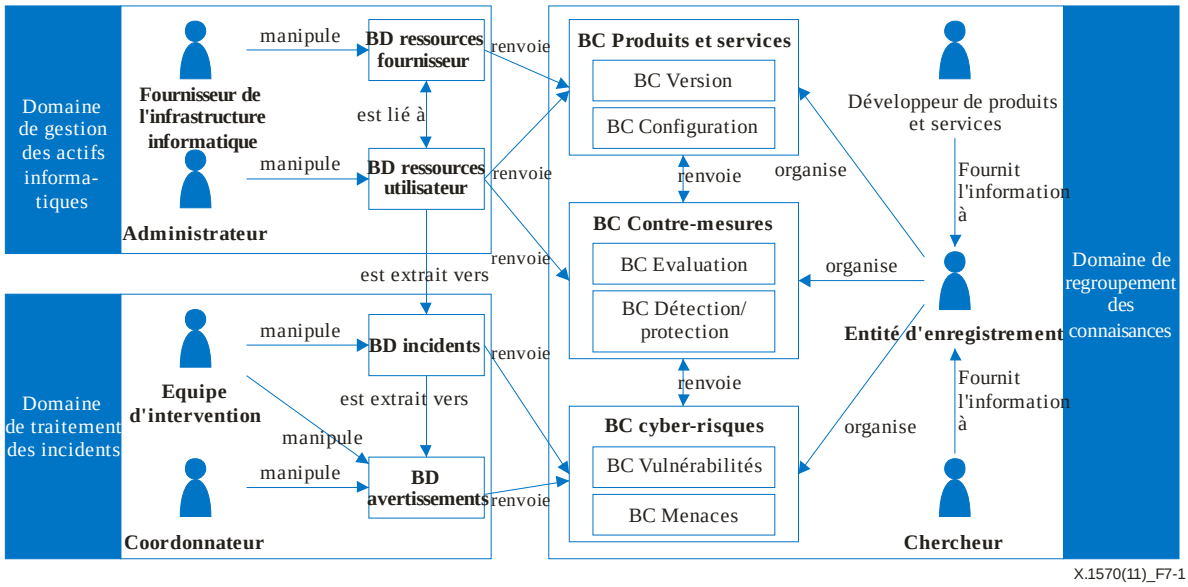


Figure 6-1 – Les trois étapes de la découverte

Le processus de découverte, qui est décrit sur la Figure 6-1, est un processus de communication entre les trois entités. Il comporte trois étapes: publication des informations, réception de la liste de sources possibles et acquisition des informations. La source publie ses informations pour la cybersociété en les enregistrant dans le répertoire au stade de la publication des informations. L'entité effectuant la recherche demande à un répertoire la liste de sources possibles au stade de la réception de la liste de sources possibles. Elle choisit alors dans la liste la source qui lui paraît la mieux adaptée et reçoit les informations émanant de la source au stade de la sélection de la source.

7 Types et niveau de précision des informations de cybersécurité découvertes

Les mécanismes de découverte permettent de découvrir des informations de cybersécurité. Le mécanisme considéré vise à découvrir les sept types d'informations suivants: base de données sur les ressources de l'utilisateur, base de données sur les ressources du fournisseur, base de données sur les incidents, base de données sur les avertissements, base de connaissances sur les produits et services, base de connaissances sur les cyberrisques et base de connaissances sur les contre-mesures. La Figure 7-1 présente le modèle d'ontologie utilisé dans la présente Recommandation et montre les relations entre les types d'informations utilisés dans le modèle.



BD: Base de données BC: Base de connaissances

Figure 7-1 – Ontologie des informations opérationnelles de cybersécurité

Cette ontologie est un modèle utilisé pour décrire l'acquisition, le regroupement et l'utilisation des connaissances sur les informations de cybersécurité, qui se compose d'un ensemble de domaines d'opérations, de rôles et de types d'informations. Les rôles, représentés sous forme d'icônes humaines sur la figure, sont génériques et des entités comme les CIRT peuvent englober une ou plusieurs de ces fonctions. On utilise ce modèle pour définir des domaines d'opérations de cybersécurité, puis pour identifier les entités de cybersécurité requises pour prendre en charge les opérations dans chaque domaine. L'ontologie est décrite de manière détaillée dans l'Appendice I.

Le Tableau II.1 indique les spécifications relatives à la cybersécurité qui peuvent être utilisées pour les sept types d'informations décrits dans ce modèle d'ontologie. Le niveau de précision des informations de cybersécurité découvertes sera conforme au niveau de précision des normes. Cela étant, le niveau de précision est souple et différentes normes pourraient donc être créées à des fins précises.

8 Identificateur d'informations de cybersécurité

Un identificateur unique est nécessaire pour identifier les informations de cybersécurité. Tout identificateur unique à l'échelle mondiale utilisé pour l'échange mondial d'informations de cybersécurité doit présenter les caractéristiques suivantes:

- simplicité, utilisabilité, souplesse, extensibilité, évolutivité et déployabilité;
- gestion répartie des divers schémas d'identificateurs;
- fiabilité à long terme des entités d'enregistrement des identificateurs et disponibilité d'outils performants pour la découverte des informations associées à tout identificateur donné.

Deux identificateurs uniques remplissent les conditions précitées: l'identificateur d'objet (OID) et le cadre de description des ressources (RDF). Ces identificateurs représentent deux paradigmes essentiels pour assurer un service commun et permettre la découverte d'informations, comme examiné au paragraphe 9.

9 Types de mécanismes de découverte

Les systèmes de découverte peuvent être implémentés avec des mécanismes arbitraires pour autant que ceux-ci soient conformes au cadre. On en distingue deux types – centralisés et décentralisés – selon la manière dont les informations de cybersécurité sont enregistrées et dont les registres d'informations de cybersécurité sont gérés.

Dans le cas d'un mécanisme centralisé, les répertoires gèrent un ou plusieurs "registres" centraux, ce qui permet de localiser aisément et de découvrir rapidement les informations recherchées (on peut omettre l'étape de réception de la liste de sources possibles dans certains cas). Toutefois, l'entité effectuant la recherche doit en premier lieu connaître l'existence d'un registre donné avant de pouvoir l'utiliser. De plus, les différentes ressources et les coûts associés à la tenue à jour de registres centraux peuvent être trop importants pour ceux qui disposent de ressources limitées. La découverte fondée sur l'identificateur OID représente en l'espèce un mécanisme type.

Dans le cas d'un mécanisme décentralisé, les répertoires gèrent plusieurs registres "répartis", ce qui présente l'avantage de nécessiter très peu de ressources et d'entraîner très peu de coûts pour mettre à disposition les informations, et ceux qui fournissent et recherchent des informations n'ont pas à connaître au préalable l'existence de chacun d'eux. Cependant, pour trouver des informations en ne disposant au départ d'aucune connaissance, l'entité qui effectue la recherche doit littéralement naviguer sur tout l'Internet. La découverte fondée sur le cadre RDF représente en l'espèce un mécanisme type.

9.1 Mécanismes de découverte fondés sur l'identificateur OID pour l'échange d'informations de cybersécurité

Un mécanisme de découverte fondé sur l'identificateur OID identifie et localise des sources d'informations de cybersécurité au moyen d'identificateurs OID, dans une structure arborescente hiérarchique dont les feuilles identifient des objets. Les identificateurs OID constituent des noms hiérarchiques, c'est-à-dire des concaténations de valeurs d'arcs allant de la racine de l'arborescence jusqu'à l'une de ses feuilles. On peut accéder aux informations de cybersécurité enregistrées en suivant l'arborescence depuis sa racine jusqu'à l'une des feuilles. Il est à noter que les informations de cybersécurité sont enregistrées sous l'arc d'identificateur d'objet relatif à l'échange d'informations de cybersécurité {joint-iso-itu-t(2) cybersecurity(48)} [b-UIT-T X.1500.1].

Les étapes de la découverte présentées au paragraphe 6 sont décrites en détail aux paragraphes 9.1.1 à 9.1.3.

9.1.1 Etape de publication des informations

Lorsqu'elle enregistre des informations, une source fournit plusieurs types d'informations de métadonnées, dont les principales catégories sont le pays/la région, l'identification de l'organisation, le type d'informations et le format de description des informations. Le pays/la région indique le pays de l'organisation, ou la région de l'organisation si la source est une organisation transnationale telle que l'UIT. L'identification de l'organisation désigne l'organisation et peut être décrite par exemple au moyen d'un code mnémonique ou d'un nom de société unique. Le type d'informations désigne le type d'informations décrit au paragraphe 7. Le format de description des informations indique le format, par exemple un format compatible CVE [b-UIT-T X.1520] ou ARF [b-ARF].

Dès réception de la demande d'enregistrement provenant de la source, le répertoire enregistre et stocke les informations à partir des métadonnées et construit des sous-arborescences d'identificateurs OID. Bien que la présente Recommandation ne spécifie aucune structure normative pour l'arborescence, certaines possibilités sont décrites dans les Appendices I et II.

9.1.2 Etape de réception de la liste de sources possibles

L'entité effectuant la recherche n'envoie pas nécessairement une demande au répertoire qui possède le seul registre cohérent de l'arborescence des identificateurs OID. Elle peut connaître au préalable la structure de l'arborescence et, en la suivant, identifier les informations nécessaires sans envoyer de demande.

Le répertoire peut accepter une demande arbitraire (y compris une demande de recherche de texte) et répondre en fournissant une liste de sources possibles.

9.1.3 Etape d'acquisition des informations

A partir de la liste de sources possibles ou en suivant l'arborescence des identificateurs OID de la racine vers une feuille, une entité effectuant la recherche choisit une source puis envoie une demande à cette source, laquelle fournit en retour les informations de cybersécurité.

Pour la découverte fondée sur l'identificateur OID, on pourrait dire que les étapes de réception de la liste de sources possibles et d'acquisition des informations sont inséparables, puisque le fait de restreindre le nombre de sources possibles en suivant l'arborescence aboutit à la sélection d'une seule source.

9.2 Mécanismes de découverte fondés sur le cadre RDF pour l'échange d'informations de cybersécurité

Un mécanisme de découverte fondé sur le cadre RDF identifie et localise des sources d'informations de cybersécurité sur la base du cadre RDF. La Figure 9-1 décrit le concept de ce mécanisme. La source peut s'enregistrer auprès d'un ou de plusieurs répertoires (contenant des registres), ce qui aide les entités effectuant des recherches à extraire les informations. Les informations sur les identités et les capacités des entités de cybersécurité sont échangées entre les entités pendant le processus de découverte. Les entités de cybersécurité envoient des demandes de découverte à un répertoire, dont chacun a des sources différentes, constituant la plage de recherche du moteur de recherche.

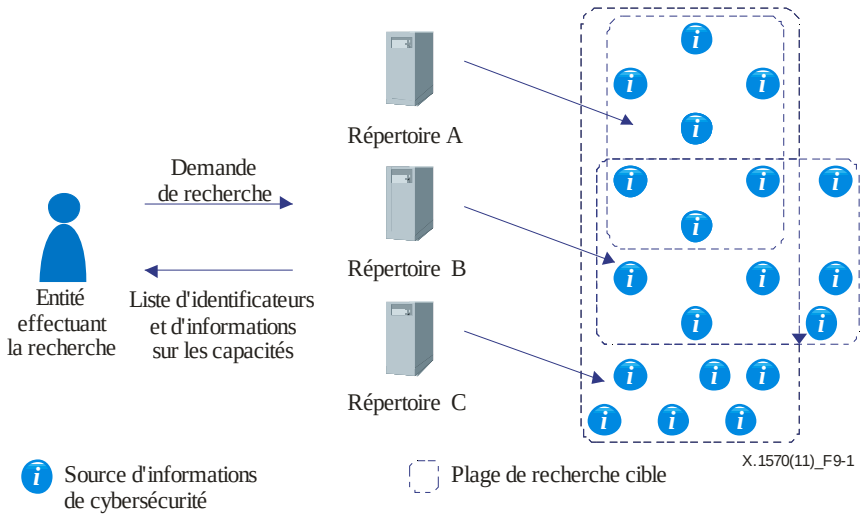


Figure 9-1 – Concept de la découverte fondée sur le cadre RDF

Contrairement à la découverte fondée sur l'identificateur OID, la découverte fondée sur le cadre RDF a des répertoires composés d'entités multiples (voir la Figure 9-2). D'un point de vue fonctionnel, un répertoire comprend un agent de découverte et un agent d'enregistrement. L'agent de découverte communique avec l'entité effectuant la recherche (interface pour le destinataire) et l'agent d'enregistrement communique avec la source (interface pour la source). Dans certains cas, l'agent de découverte et l'agent d'enregistrement peuvent résider dans un même ordinateur. Des informations sur les capacités et les identificateurs sont échangées entre les quatre entités.

Les étapes de découverte présentées au paragraphe 6 sont décrites en détail aux paragraphes 9.2.1 à 9.2.3.

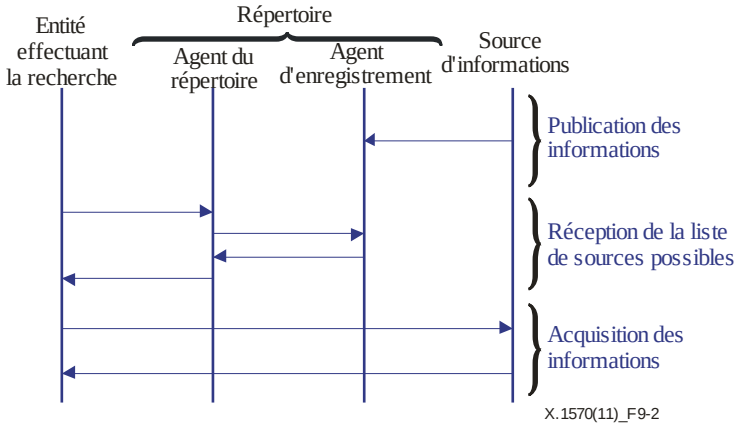


Figure 9-2 – Diagramme de séquence de la découverte fondée sur le cadre RDF

9.2.1 Etape de publication des informations

Une source enregistre ses informations auprès d'un agent d'enregistrement, qui crée et organise des métadonnées appropriées pour les données au stade de la publication des informations. Comme pour la découverte fondée sur l'identificateur OID, la source fournit plusieurs types d'informations de métadonnées lorsqu'elle enregistre des informations de cybersécurité, dont les principales catégories sont le pays/la région, l'identification de l'organisation, le type d'informations et le format de description des informations. Le pays/la région indique le pays de l'organisation, ou la région de l'organisation si la source est une organisation transnationale telle que l'UIT. L'identification de l'organisation désigne l'organisation et peut être décrit par exemple au moyen d'un code mnémonique ou d'un nom de société unique. Le type d'informations désigne le type d'informations décrit au paragraphe 7. Le format de description des informations indique le format, par exemple un format compatible CVE ou ARF.

Dès réception de la demande d'enregistrement émanant de la source, le répertoire enregistre et stocke les informations à partir des métadonnées et met à jour la base de données RDF. Etant donné que les agents d'enregistrement utilisent souvent des registres hiérarchiquement répartis, l'agent d'enregistrement doit déterminer dans quel registre il y a lieu de stocker les données.

Bien que la présente Recommandation ne spécifie aucune structure normative pour le format des métadonnées RDF, certaines possibilités sont décrites dans les Appendices I et II.

9.2.2 Etape de réception de la liste de sources possibles

L'entité effectuant la recherche envoie des demandes à un agent de découverte, qui les retransmet à un ou plusieurs agents d'enregistrement. Ceux-ci font une recherche dans leur base de données de métadonnées et répondent en fournissant une liste de sources possibles au stade de la réception de la liste de sources possibles. L'agent de découverte rassemble les informations reçues de la part de plusieurs agents d'enregistrement et les envoie à l'entité effectuant la recherche.

9.2.3 Etape d'acquisition des informations

L'entité effectuant la recherche choisit la source la mieux adaptée parmi les sources de la liste au stade d'acquisition des informations.

10 Méthodes permettant d'accéder aux informations découvertes

On peut utiliser divers protocoles de communication pour échanger des informations de cybersécurité, en particulier les protocoles HTTP (qui utilise le cadre RDF) et SNMP (qui utilise l'identificateur OID).

Certaines parties voudront peut-être restreindre le nombre de parties pouvant avoir accès à des informations découvertes en élaborant des politiques de contrôle d'accès. Les principaux critères de ces politiques sont l'adresse IP, le domaine, le protocole de communication, l'identifiant et le mot de passe et le certificat d'identification.

Toute partie recherchant des informations de cybersécurité échange plusieurs messages, dont des messages de demande. Ces méthodes seront définies dans les Recommandations UIT-T de la série X.1500.

Appendice I

Ontologie des informations opérationnelles de cybersécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le paragraphe 7 de la présente Recommandation utilise une ontologie des informations opérationnelles de cybersécurité, qui est décrite sur la Figure 7-1. Le présent appendice décrit en détail l'ontologie.

L'ontologie se compose de domaines d'opérations de cybersécurité, des rôles requis pour exécuter les opérations dans les domaines, et des informations de cybersécurité associées aux rôles, qui sont décrits en détail ci-après.

I.1 Domaines d'opérations de cybersécurité

L'expression "opérations de cybersécurité" désigne un ensemble d'opérations de sécurité dans la cybersociété, mais dans cette ontologie, on s'intéresse plus particulièrement aux opérations de cybersécurité qui préservent la sécurité des informations dans les cybersociétés. Par sécurité des informations, on entend la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations, ainsi que, parfois, la responsabilité, l'authenticité et la fiabilité des informations.

Dans cette ontologie, on définit trois domaines d'opérations de cybersécurité: gestion des actifs informatiques, traitement des incidents et regroupement des connaissances.

Gestion des actifs informatiques: ce domaine exécute des opérations de cybersécurité à l'intérieur des organisations d'utilisateur (par exemple installation, configuration et gestion des actifs informatiques) et comporte à la fois des opérations de prévention des incidents et des opérations de contrôle des dommages. Les actifs informatiques incluent non seulement les propres actifs informatiques de l'utilisateur mais aussi la connectivité au réseau, les services en nuage et les services d'identité fournis à l'utilisateur par des entités externes.

Traitement des incidents: ce domaine détecte les incidents se produisant dans les cybersociétés et intervient, à partir de la surveillance des événements informatiques, des incidents comportant plusieurs événements informatiques et des attaques à l'origine des incidents. Plus précisément, il surveille les événements informatiques, et lorsqu'une anomalie est détectée, il produit un rapport d'incident. A partir du rapport, il analyse l'incident en détail afin de pouvoir déterminer le type d'attaque et les contre-mesures associées. A partir de l'analyse de l'incident, il peut fournir des alertes et des conseils (par exemples des mises en garde avancées contre des menaces potentielles) aux organisations d'utilisateurs.

Regroupement des connaissances: ce domaine collecte et génère des informations de cybersécurité et extrait les connaissances réutilisables par d'autres organisations. Pour faciliter la réutilisabilité, il définit un nommage et une taxonomie communs, à partir desquels il organise et regroupe les connaissances. Ce domaine sert de base à la collaboration mondiale au-delà des frontières des organisations.

I.2 Rôles

A partir des domaines d'opérations de cybersécurité définis ci-dessus, le présent paragraphe définit les rôles nécessaires à l'exécution des opérations de cybersécurité dans chaque domaine. Le domaine de gestion des actifs informatiques a un administrateur et un fournisseur de l'infrastructure informatique, le domaine de traitement des incidents a une équipe d'intervention et un coordonnateur, et le domaine de regroupement des connaissances a un chercheur, un développeur de produits et services, et une entité d'enregistrement pour les opérations associées. Il est à noter

que les rôles sont définis du point de vue des fonctions, si bien qu'une même entité peut assumer plusieurs rôles en fonction du contexte.

Administrateur: ce rôle administre le système de son organisation et maintient sa fonctionnalité. A cette fin, il surveille l'utilisation du système, effectue sur le système des contrôles d'intégrité, des analyses de vulnérabilité et des tests de pénétration pour poser des diagnostics, puis évalue le niveau de sécurité du système. Un administrateur de système dans chaque organisation constitue une instance type. Un fournisseur de services de sécurité gérés (MSSP, *managed security service provider*) fait aussi office d'administrateur si une organisation lui sous-traite une partie des opérations ci-dessus.

Fournisseur de l'infrastructure informatique: ce rôle fournit l'infrastructure informatique pour une organisation. L'infrastructure inclut la connectivité au réseau et les services en nuage comme le service de logiciels (SaaS, *software as a service*), le service de plate-forme (PaaS, *platform as a service*) et le service d'infrastructure (IaaS, *infrastructure as a service*). Le fournisseur de l'infrastructure informatique possède des informations sur les réseaux inter-organisations (par exemple des informations sur la topologie de réseau et les spécifications des services en nuage). Un fournisseur de services Internet (ISP, *Internet service provider*), un fournisseur de services d'application (ASP, *application service provider*) et un fournisseur de services en nuage (CSP, *cloud service provider*) constituent des instances types.

Equipe d'intervention: ce rôle surveille et analyse des incidents variés dans les cybersociétés, par exemple l'accès non autorisé, les attaques par déni de service réparti (DDoS) et l'hameçonnage, et regroupe des informations sur les incidents. A partir de ces informations, il peut mettre en place des contremesures, par exemple bloquer le trafic ou enregistrer les adresses des sites d'hameçonnage sur des listes noires. L'équipe d'intervention en cas d'incident d'un fournisseur MSSP constitue une instance type.

Coordonnateur: ce rôle assure la coordination avec les autres rôles et examine les menaces potentielles à partir des informations relatives aux incidents connus. Il envoie des avertissements aux autres organisations et, parfois, dirige les efforts menés en collaboration pour atténuer les effets d'attaques dévastatrices à grande échelle telles que les attaques DDoS. Le centre de coordination de l'équipe CERT (CERT/CC), qui peut être une entité commerciale ou non, constitue une instance type.

Chercheur: ce rôle mène des recherches sur les problèmes de cybersécurité, y compris les vulnérabilités et les attaques, extrait des connaissances des travaux de recherche, et les regroupe. Il publie une grande partie des informations réutilisables par l'intermédiaire de l'entité d'enregistrement afin que les différentes organisations puissent mettre en place les contremesures nécessaires. Le groupe X-force de l'International Business Machines Corp. (IBM), le Risk Research Institute of Cyber Space (RRICS) de Little eArth Corporation Co., Ltd. (LAC) et le McAfee Lab de McAfee Inc. constituent des instances types.

Développeur de produits et services: ce rôle développe des produits et des services et regroupe des informations les concernant, par exemple leurs versions, configurations, vulnérabilités et correctifs. Il publie une grande partie des informations réutilisables par l'intermédiaire de l'entité d'enregistrement afin que, comme dans le cas du chercheur, les différentes organisations puissent mettre en place les contremesures nécessaires. Un vendeur de logiciels et un développeur particulier de logiciels constituent des instances types.

Entité d'enregistrement: ce rôle classe, organise et regroupe les connaissances sur la cybersécurité fournies par le chercheur et le développeur de produits et services afin que ces connaissances puissent être réutilisées par d'autres organisations. NIST et l'Information-Technology Promotion Agency (Japon) constituent des instances types. Dans certains cas, une entité faisant office de chercheur ou de développeur de produits et services peut aussi faire office d'entité d'enregistrement et publier les informations.

I.3 Informations de cybersécurité

A partir des domaines d'opération et des rôles, le présent paragraphe définit les informations de cybersécurité nécessaires pour les opérations. Compte tenu des informations traitées par chacun des rôles, cette ontologie définit quatre bases de données (ressources de l'utilisateur, ressources du fournisseur, incidents, avertissements) et trois bases de connaissances (produits et services, contremesures, cyber-risques).

I.3.1 Base de données sur les ressources de l'utilisateur

La base de données sur les ressources de l'utilisateur regroupe des informations sur les actifs à l'intérieur de chaque organisation et contient des informations telles que les listes de logiciels/matériels, leurs configurations, l'état d'utilisation des ressources, les politiques de sécurité y compris les politiques de contrôle d'accès, les résultats d'évaluation du niveau de sécurité, et la topologie de l'intranet. Elle contient aussi des informations sur les ressources externes que chaque organisation d'utilisateur utilise, par exemple les listes des services en nuage souscrits (par exemple centres de données et service SaaS) et les relevés d'utilisation associés. Ces informations sont manipulées par l'administrateur. On peut utiliser les formats ARF et CRF pour décrire les résultats d'évaluation des actifs informatiques, et utiliser les notes CVSS et CWSS pour noter le niveau de sécurité des actifs informatiques. Les notes sont utiles aux administrateurs pour classer par ordre de priorité les opérations de sécurité à effectuer sur les actifs informatiques.

I.3.2 Base de données sur les ressources du fournisseur

La base de données sur les ressources du fournisseur regroupe des informations sur les actifs à l'extérieur de chaque organisation. Pour pouvoir exécuter des opérations de cybersécurité efficaces et efficientes, la base de données doit être reliée à la base de données sur les ressources de l'utilisateur étant donné que la frontière entre actifs informatiques internes et actifs informatiques externes est de plus en plus floue, en particulier pour l'informatique en nuage. Ces informations sont manipulées par le fournisseur de l'infrastructure informatique. La base de données contient principalement des informations sur les réseaux de fournisseur et les services en nuage. Les informations sur les réseaux de fournisseur concernent les réseaux par lesquels chaque organisation est connectée à d'autres organisations (par exemple topologie, informations de routage, politiques de contrôle d'accès, état du trafic et niveaux de sécurité). Les informations sur les services en nuage incluent les spécifications des services, des informations sur les tâches et des informations sur les politiques de sécurité pour chaque service en nuage. Il est à noter que les informations propres à chaque organisation d'utilisateur (par exemple la configuration locale de chaque service en nuage) sont stockées dans la base de données sur les ressources de l'utilisateur.

I.3.3 Base de données sur les incidents

La base de données sur les incidents contient des informations sur les incidents, qui sont générées à partir d'une analyse des informations contenues dans la base de données sur les ressources de l'utilisateur. Ces informations sont manipulées par l'équipe d'intervention. Cette base de données inclut trois relevés: le relevé des événements, le relevé des incidents et le relevé des attaques.

Le relevé des événements contient des informations sur les événements informatiques, en particulier concernant les paquets, les fichiers et les transactions associées. En règle générale, les ordinateurs fournissent automatiquement la plupart des relevés sous forme de journaux (par exemple date et heure de connexion, informations terminales fournies lorsqu'un utilisateur racine se connecte à un système). Les journaux sont des instances de ce relevé. On peut utiliser le format CEE pour décrire ce relevé.

Le relevé des incidents contient des informations sur les incidents de sécurité et fournit des informations telles que l'état actuel des systèmes d'utilisateur et les risques potentiels. Il est obtenu à partir d'analyses de plusieurs relevés des événements et des conséquences possibles, qui sont créées automatiquement ou manuellement. Par exemple, en cas de détection d'un accès excessif à un

ordinateur, l'état de l'ordinateur (accès excessif à un ordinateur) et la conséquence attendue (déni de service) doivent être enregistrés dans le relevé des incidents. La nocivité de l'incident ainsi que le besoin de contremesures peuvent être estimés à partir de ce relevé. Il est à noter qu'un relevé des incidents peut enregistrer de faux incidents, qui s'avèrent ne pas être des incidents après investigation. On peut utiliser le format d'échange de description d'objet incident (IODEF) pour décrire ce relevé.

Le relevé des attaques contient des informations sur les attaques, qui sont obtenues à partir d'analyses des relevés des incidents. Il décrit la séquence de chaque attaque, par exemple comment l'attaque a été déclenchée, quelle partie des actifs informatiques a été ciblée, et comment les dommages causés par l'attaque se sont propagés. Il est à noter que ce relevé doit être relié au relevé des incidents.

I.3.4 Base de données sur les avertissements

La base de données sur les avertissements contient des informations sur les avertissements de cybersécurité. Les informations sont destinées soit au grand public soit à une organisation particulière. Celles destinées au grand public contiennent généralement des informations statistiques et des alertes tandis que celles destinées à une organisation particulière contiennent des avis de sécurité formulés en fonction de chaque organisation. Les informations sont générées à partir des informations contenues dans la base de données sur les incidents et dans la base de connaissances sur les cyber-risques. Ces informations sont manipulées par le coordonnateur et l'équipe d'intervention. A partir des avertissements concernant des risques de cybersécurité, les organisations d'utilisateur peuvent mettre en place des contre-mesures.

I.3.5 Base de connaissances sur les cyber-risques

La base de connaissances sur les cyber-risques regroupe des informations sur les risques de cybersécurité. Ces informations sont fournies par le chercheur et le développeur de produits et services, puis organisées et classées par l'entité d'enregistrement. Cette base de connaissances comporte une base de connaissances sur les vulnérabilités et une base de connaissances sur les menaces.

Base de connaissances sur les vulnérabilités: cette base de connaissances regroupe des informations sur les vulnérabilités connues (nommage, taxonomie, et liste des vulnérabilités connues dans les logiciels et les systèmes). Elle inclut aussi des informations sur les vulnérabilités humaines, qui sont les vulnérabilités auxquelles les utilisateurs humains de l'informatique sont exposés. La base de données nationale sur les vulnérabilités (NVD) et la base de données sur les vulnérabilités dans le code source ouvert (OSVDB) sont des instances concrètes de cette base de données, et on peut utiliser les formats CVE et CWE pour décrire le contenu de la base de connaissances.

Base de connaissances sur les menaces: cette base de connaissances regroupe des informations sur les menaces de cybersécurité connues. Elle comporte une base de connaissances sur les attaques et une base de connaissances sur les utilisations abusives. La base de connaissances sur les attaques regroupe des informations sur les attaques comme les types d'attaque, les outils utilisés pour les attaques (par exemple des logiciels malveillants), et les tendances associées. Les informations sur les tendances visent par exemple à renseigner sur les tendances des attaques passées en termes de lieu géographique et de cibles des attaques, et à donner des informations statistiques sur les attaques passées. On peut utiliser les formats CAPEC et MAEC pour décrire le contenu de la base de connaissances.

La base de connaissances sur les utilisations abusives regroupe des informations sur les utilisations abusives découlant d'utilisations inappropriées par les utilisateurs, qui peuvent être involontaires ou malveillantes. Parmi les utilisations involontaires, on peut citer les erreurs de frappe, les erreurs de reconnaissance par inattention, les erreurs de compréhension, et la prise dans des pièges d'hameçonnage. Parmi les utilisations malveillantes, on peut citer les transgressions comme

l'utilisation d'un service sans autorisation et l'accès à des contenus inappropriés. Il est à noter que les bases de connaissances sur les attaques et sur les utilisations abusives ne sont pas représentées sur la Figure 7-1 dans un souci de simplicité.

I.3.6 Base de connaissances sur les contremesures

La base de connaissances sur les contremesures regroupe des informations sur les contremesures applicables face aux risques de cybersécurité. Ces informations sont fournies par le chercheur et le développeur de produits et services, puis organisées et classées par l'entité d'enregistrement. Cette base de connaissances comporte une base de connaissances sur l'évaluation et une base de connaissances sur la détection/protection.

Base de connaissances sur l'évaluation: cette base de connaissances regroupe des règles et des critères connus pour évaluer le niveau de sécurité des actifs informatiques, des listes de points à vérifier dans les configurations, des données heuristiques et des bonnes pratiques. Parmi les bonnes pratiques d'évaluation des niveaux de sécurité, on peut citer les formules CVSS/CWSS, qui figurent dans cette base de connaissances. Cela étant, on peut utiliser les formats XCCDF et OVAL pour décrire les règles et fournir les listes de points à vérifier.

Base de connaissances sur la détection/protection: cette base de connaissances regroupe des règles et des critères connus pour détecter les menaces de sécurité et assurer la protection contre ces menaces. Elle regroupe aussi des données heuristiques et des bonnes pratiques.

I.3.7 Base de connaissances sur les produits et services

La base de connaissances sur les produits et services regroupe des informations sur les produits et services. Ces informations sont fournies par le chercheur et le développeur de produits et services, puis organisées et classées par l'entité d'enregistrement. Cette base de connaissances comporte une base de connaissances sur la version et une base de connaissances sur la configuration.

Base de connaissances sur la version: cette base de connaissances regroupe des informations sur la version des produits et services, avec nommage et liste des versions. En ce qui concerne les produits, elle renseigne aussi sur les correctifs de sécurité. On peut utiliser le format CPE pour faire la liste des plates-formes courantes.

Base de connaissances sur la configuration: cette base de connaissances regroupe des informations sur la configuration des produits et services, avec nommage, taxonomie et liste des configurations connues des produits et services. En ce qui concerne la configuration des services, elle contient aussi des lignes directrices sur les utilisations des services. On peut utiliser le format CCE pour faire la liste des configurations courantes des produits.

On trouvera des informations complémentaires sur cette ontologie dans le document [b-Ontology] et dans l'Appendice II de [b-UIT-T X.1500].

Appendice II

Spécifications décrivant les bases de données et les bases de connaissances

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Les sept types d'informations présentés au paragraphe 7 sont décrits au moyen de diverses spécifications relatives à la cybersécurité, en particulier les spécifications compatibles avec la Recommandation UIT-T X.1500 (par exemple CVE et IODEF), comme il ressort du Tableau II.1. En conséquence, le niveau de précision des informations de cybersécurité découvertes sera conforme au niveau de précision des spécifications. Cela étant, le niveau de précision est souple et différentes spécifications pourraient donc être créées à des fins précises.

Tableau II.1 – Spécifications utilisables pour l'ontologie

Domaines	**BC/BD**		**Spécifications**
Gestion des actifs informatiques	BD ressources de l'utilisateur		Notes ARF, AI, CVSS/CWSS
	BD ressources du fournisseur		–
Traitement des incidents	BD incidents		CEE, IODEF
	BD avertissements		IODEF
Regroupement des connaissances	BC cyber-risques	BC vulnérabilités	CVE, CWE, CVRF
		BC menaces	CAPEC, MAEC
	BC contre-mesures	BC évaluation	Formule CVSS/CWSS
		BC détection/protection	OVAL, XCCDF
	BC produits et services	BC version	CPE
		BC configuration	CCE
NOTE – BD: base de données; BC: base de connaissances.			

Appendice III

Illustration de l'implémentation de la découverte fondée sur le cadre RDF

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

III.1 Exemple d'implémentation de la découverte fondée sur le cadre RDF

Le concept illustré sur la Figure 9-1 pourrait être concrétisé par le rassemblement des agents de découverte et des agents d'enregistrement dans des moteurs de recherche RDF. Les entités de cybersécurité envoient une demande de découverte à un moteur de recherche RDF, qui renvoie une liste d'identités et de leurs capacités. Il est à noter que chaque moteur de recherche dispose de sources différentes, qui constituent leur plage de recherche.

Dans la pratique, pour assurer une certaine évolutivité, la source peut être enregistrée et gérée de manière hiérarchique, comme indiqué sur la Figure III.1. Le niveau 1 peut être un moteur de recherche RDF individuel qui fait fonction d'agent de découverte, le niveau 2 pourrait être une entité enregistrée conformément aux règles de fonctionnement d'un registre régional, tel que l'ARIN (American Registry for Internet Numbers), le RIPE (Réseaux IP européens), ou l'APNIC (Asia Pacific Network Information Centre), et d'autres niveaux hiérarchiques pourront être créés selon l'implémentation. Une source peut être une équipe CERT ou toute autre entité de cybersécurité.

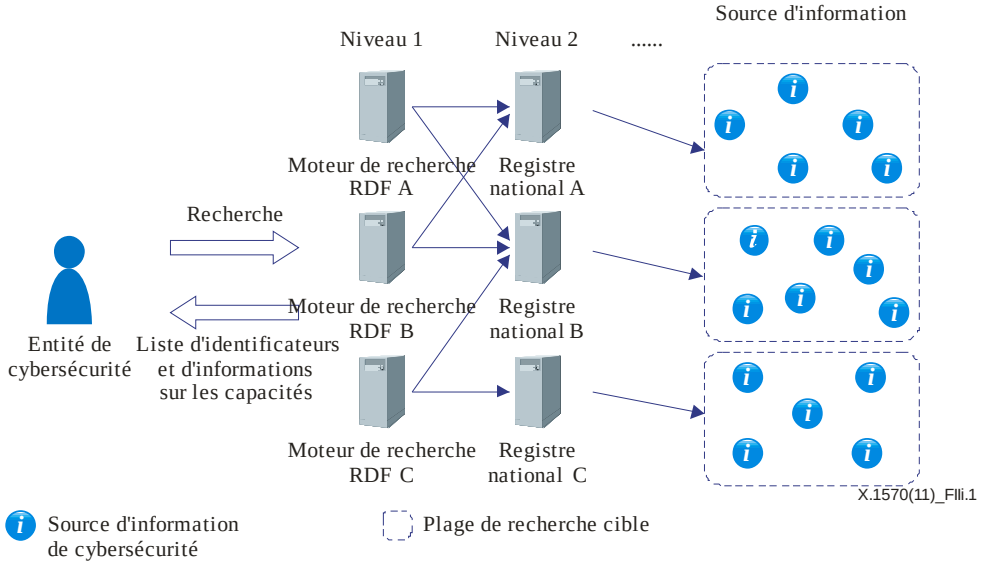


Figure III.1 – Hiérarchie du registre de sources

III.2 Hiérarchie des classes d'informations de cybersécurité

La Figure III.2 représente la hiérarchie des classes du mécanisme de découverte. Chaque classe représente la catégorie présentée dans l'Appendice II de [b-UIT-T X.1500]. Pour plus de précisions sur chaque catégorie, voir cette Recommandation. Il est à noter que l'espace de noms XML défini par l'UIT-T est utilisé [b-UIT-T X.1500].

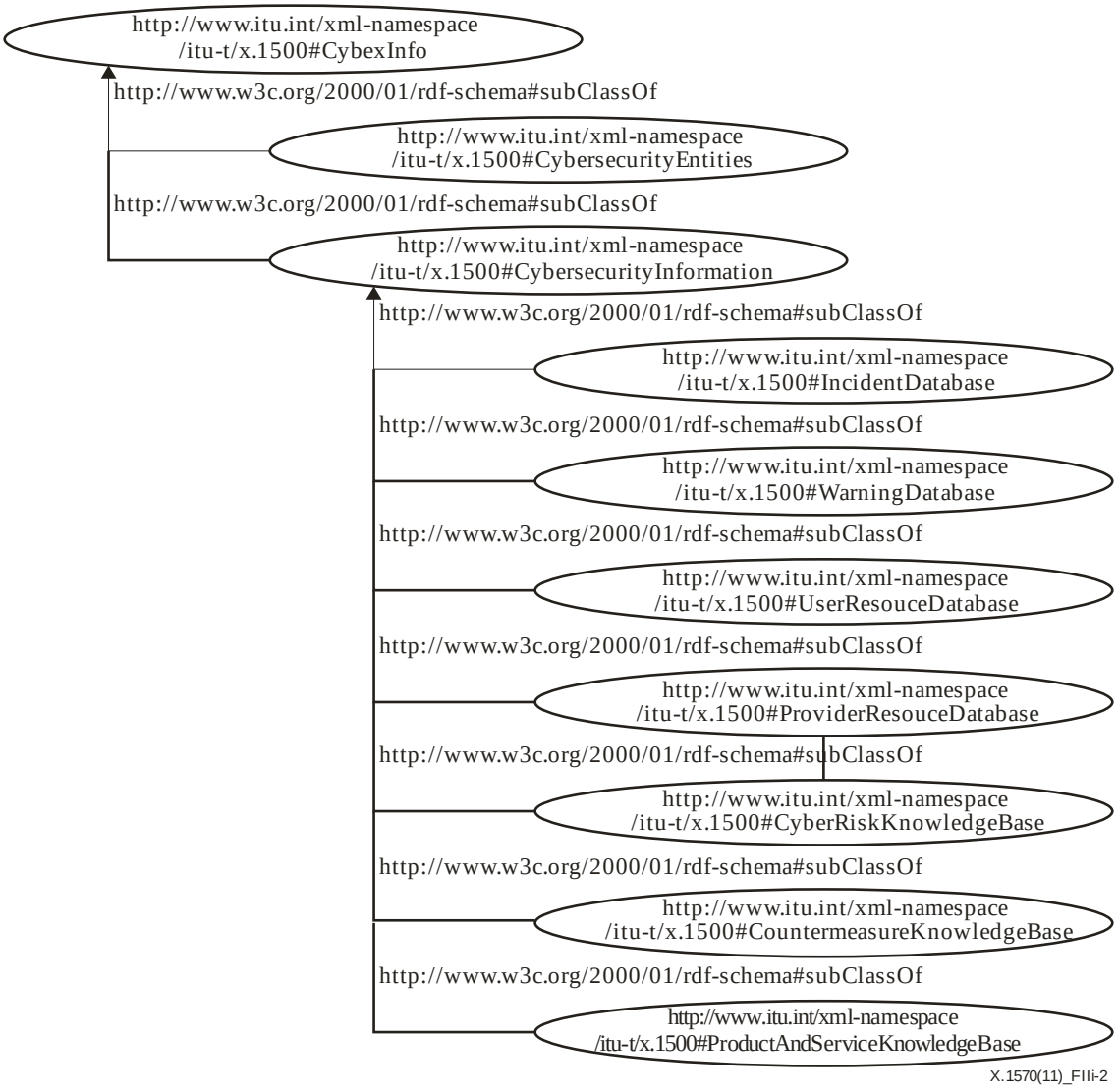


Figure III.2 – Hiérarchie des classes d'informations de cybersécurité

NOTE 1 – L'utilisation de la désignation **.int** dans le nom de domaine de premier niveau est indiquée à titre d'exemple sur la Figure III.3 et n'est pas destinée à être utilisée dans la pratique.

Chaque classe de cybersécurité comprend généralement les attributs suivants:

- entry_date: stocke la date d'entrée/de modification des données;
- issuer_name: stocke le nom de l'émetteur (celui-ci peut être un particulier ou une entreprise);
- contact_email: stocke l'adresse électronique de la partie à contacter;
- resources: stocke les identificateurs, par exemple les adresses web, vers d'autres ressources;
- Info_type: stocke le type d'informations, par exemple CVE, CWSS [b-CWSS], CVSS [b-UIT-T X.1521], OVAL [b-OVAL], SCAP [b-SCAP], XCCDF [b-XCCDF], CPE [b-CPE], CCE [b-CCE] et ARF.

Toute partie recherchant des informations de cybersécurité peut demander des données dans une unité d'une classe donnée. Les informations peuvent être recherchées au moyen de critères tels que le nom de la classe, un attribut de la classe et la date et l'heure de la dernière modification.

L'implémentation test du système de découverte est accessible en ligne à l'adresse: http://cybiet.sourceforge.net/.

NOTE 2 – L'implémentation découvre les informations de sécurité qui sont structurées conformément à l'ontologie décrite sur la Figure 7-1.

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

[b-UIT-T X.1500.1] Recommandation UIT-T X.1500.1 (2012), *Procédures d'enregistrement d'arcs sous l'arc d'identificateur d'objet aux fins de l'échange d'informations de cybersécurité*.

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2011), *Vulnérabilités et expositions courantes (CVE)*.

[b-UIT-T X.1521] Recommandation UIT-T X.1521 (2011), *Système d'évaluation des vulnérabilités courantes (CVSS)*.

[b-AI] NIST, *The Asset Identification.*
<http://scap.nist.gov/specifications/ai/>

[b-ARF] *Assessment Results Format*
<https://measurablesecurity.mitre.org/incubator/arf/>

[b-CCE] *Common Configuration Enumeration.*
<https://cce.mitre.org/>

[b-CPE] *Common Platform Enumeration.*
<https://cpe.mitre.org/>

[b-CWSS] *Common Weakness Scoring System.*
<https://cwe.mitre.org/cwss/>

[b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, novembre 1995, pages 907 à 928.

[b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), septembre 2010.

[b-OVAL] *Oval – Open Vulnerability and Assessment Language.*
<https://oval.mitre.org/>

[b-SCAP] *Security Content Automation Protocol (SCAP).*
<http://scap.nist.gov/>

[b-XCCDF] *XCCDF – The Extensible Configuration Checklist Description Format.*
<http://scap.nist.gov/specifications/xccdf/>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2012