

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1500

(04/2011)

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

Echange d'informations sur la cybersécurité – Aperçu
général de la cybersécurité

Techniques d'échange d'informations sur la cybersécurité

Recommandation UIT-T X.1500

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.1500

Techniques d'échange d'informations sur la cybersécurité

Résumé

La Recommandation UIT-T X.1500 décrit des techniques d'échange d'informations sur la cybersécurité. Utilisables séparément ou de manière combinée, selon les souhaits ou les besoins, ces techniques visent à améliorer la cybersécurité grâce à un échange d'informations cohérent, complet, global, garanti et en temps utile. La présente Recommandation n'entraîne aucune obligation quant à l'échange d'informations, aux moyens d'acquisition ou à l'utilisation finale des informations. Les techniques d'échange d'informations sur la cybersécurité (CYBEX, *cybersecurity information exchange*) sont l'un des éléments qui garantissent la confiance et la sécurité dans l'utilisation des TIC.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1500	2011-04-20	17
1.1	ITU-T X.1500 (2011) Amd. 1	2012-03-02	17

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/>.

© UIT 2012

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1 Domaine d'application	1
2 Références.....	1
3 Définitions	1
3.1 Termes définis ailleurs	1
3.2 Termes définis dans la présente Recommandation	2
4 Abréviations et acronymes	2
5 Conventions	3
6 Concept de base – Echange d'informations sur la cybersécurité (CYBEX).....	3
7 Techniques d'échange structuré d'informations sur la cybersécurité.....	5
7.1 Grappe d'échange – Failles, vulnérabilités et état	6
7.2 Grappe d'échange – Evénements, incidents et heuristiques	6
7.3 Grappe d'échange – Politique d'échange d'informations	6
7.4 Grappe d'identification, de découverte et d'interrogation.....	6
7.5 Grappe d'assurance d'identité	7
7.6 Grappe des protocoles d'échange.....	7
Appendice I – Techniques d'échange structuré d'informations sur la cybersécurité	8
Appendice II – Ontologie d'échange d'informations de cybersécurité.....	19
II.1 Domaines opérationnels	20
II.2 Entités de cybersécurité.....	20
II.3 Informations opérationnelles sur la cybersécurité.....	21
Appendice III – Exemples CYBEX de schémas d'automatisation de la sécurité	24
III.1 Exemple: Configuration de base des postes de travail au niveau fédéral aux Etats-Unis/base de référence de configuration de l'Administration américaine.....	25
III.2 Exemple: Portail japonais d'informations sur la vulnérabilité, JVN	25
Bibliographie.....	29

Introduction

La présente Recommandation a été rédigée de façon à être adaptable, extensible et non prescriptive pour permettre l'application d'une vaste gamme de techniques, dont certaines évoluent en permanence et en sont à divers stades d'achèvement, dans différentes instanciations pour améliorer l'échange d'informations sur la cybersécurité concernant les infrastructures, les dispositifs et les services de télécommunication/TIC. Elle sera révisée régulièrement, à mesure que ces techniques évoluent; les techniques appropriées feront l'objet de Recommandations UIT-T de la série X.1500.

On pense que les techniques intégrées dans la présente Recommandation permettront aux organisations de télécommunication/TIC, y compris aux équipes d'intervention en cas d'incident informatique (CIRT, *computer incident response team*), au sein des juridictions et entre juridictions:

- a) de disposer d'informations leur permettant de prendre des décisions et des mesures afin d'améliorer notablement la confidentialité, l'intégrité et la disponibilité des installations et services de télécommunication/TIC dans le monde;
- b) de disposer d'informations pour faciliter des processus coopératifs sécurisés et des contrôles qui améliorent le niveau de garantie dans les échanges d'informations entre organisations;
- c) d'adopter une approche cohérente pour gérer et échanger des informations sur la cybersécurité sur une base globale;
- d) d'améliorer la sensibilisation à la sécurité et la collaboration afin de lutter contre les cybermenaces, les cyberattaques et les logiciels malveillants.

Ces techniques incluent:

- la structuration des informations sur la cybersécurité à des fins d'échanges;
- l'identification et la découverte d'informations sur la cybersécurité et d'entités;
- l'établissement d'accords de confiance et de politique entre entités échangeant des informations;
- la demande d'informations sur la cybersécurité et la réponse;
- l'assurance de l'intégrité des échanges d'informations sur la cybersécurité;

et sont organisées en "grappes":

- failles, vulnérabilités et état;
- événement, incident et heuristique;
- politique d'échange d'informations;
- identification, découverte et interrogations;
- assurance d'identité;
- protocoles d'échange.

Recommandation UIT-T X.1500

Techniques d'échange d'informations sur la cybersécurité

1 Domaine d'application

La présente Recommandation donne un modèle d'échange d'informations sur la cybersécurité (CYBEX) et porte sur les techniques qui peuvent être utilisées pour faciliter les échanges d'informations sur la cybersécurité. Utilisables séparément ou de manière combinée, selon les souhaits où les besoins, ces techniques visent à améliorer la cybersécurité grâce à un échange d'informations cohérent, complet, global, garanti et en temps utile. La présente Recommandation n'entraîne aucune obligation quant à l'échange d'informations, aux moyens d'acquisition ou à l'utilisation finale des informations. Ces techniques incluent la découverte globale structurée et l'interopérabilité d'informations sur la cybersécurité, qui permettent une évolution permanente, afin de s'adapter aux évolutions significatives des activités et des spécifications définies dans les nombreux groupes s'occupant de cybersécurité. Les spécifications CYBEX sont l'un des éléments qui garantissent la confiance et la sécurité dans l'utilisation des TIC.

La présente Recommandation englobe les fonctions de base suivantes qui peuvent être utilisées séparément ou ensemble, selon qu'il conviendra:

- structuration des informations sur la cybersécurité à des fins d'échange;
- identification et découverte des informations sur la cybersécurité et des entités;
- établissement d'accords de confiance et de politique entre entités échangeant des informations;
- demandes d'informations sur la cybersécurité et réponses;
- assurance de l'intégrité des échanges d'informations sur la cybersécurité.

Sous réserve des politiques convenues ainsi que des lois et des réglementations applicables, les moyens d'acquisition des informations ainsi que l'usage de ces informations ne sont ni couverts ni traités par la présente Recommandation. Certaines réglementations et lois spécifiques nationales et régionales peuvent nécessiter la mise en oeuvre de mécanismes de protection des informations d'identification personnelles. Ni les techniques décrites dans la présente Recommandation ni l'échange d'informations sur la cybersécurité connexes ne sont rendus obligatoires par la présente Recommandation.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 cybersécurité [b-UIT-T X.1205]: ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par

rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont la disponibilité, l'intégrité (qui peut englober l'authenticité et la non-répudiation) et la confidentialité.

NOTE – Certaines réglementations et lois nationales spécifiques peuvent exiger la mise en oeuvre de mécanismes de protection d'informations d'identification personnelles.

3.1.2 atteinte à la sécurité [b-UIT-T E.409]: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 assurance: degré de confiance dans le fait que le processus ou l'élément à livrer est conforme à des caractéristiques ou à des objectifs définis.

3.2.2 protocole d'échange: ensemble de règles techniques et de formats régissant l'échange d'informations entre deux ou plusieurs entités.

3.2.3 politique d'échange d'informations: termes et conditions associés à l'usage et au partage d'informations sur la cybersécurité.

3.2.4 état d'un système: état courant d'un système ou d'une entité, incluant les informations comme sa configuration, l'utilisation de la mémoire et d'autres données pertinentes pour la cybersécurité.

3.2.5 vulnérabilité: (alignée sur [b-UIT-T X.800]): toute faille qui pourrait être exploitée pour violer un système ou les informations qu'il contient.

3.2.6 faille: insuffisance ou imperfection qui, bien qu'elle ne soit pas reconnue comme étant une vulnérabilité en soi, pourrait à un certain moment devenir une vulnérabilité ou contribuer à l'apparition d'autres vulnérabilités.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ARF	format des résultats d'évaluation (<i>assessment results format</i>) ou format de rapport sur les actifs (<i>asset reporting format</i>) (selon le contexte)
BEEP	protocole d'échange extensible de blocs (<i>blocks extensible exchange protocol</i>)
CA	autorité de certification (<i>certification authority</i>)
CAPEC	liste et classification des schémas d'attaque courants (<i>common attack pattern enumeration and classification</i>)
CCE	liste des configurations courantes (<i>common configuration enumeration</i>)
CEE	expression d'événements courants (<i>common event expression</i>)
CEEE	échange d'expression d'événements courants (<i>common event expression exchange</i>)
CIRT	équipe d'intervention en cas d'incident informatique (<i>computer incident response team</i>)
CPE	système commun d'énumération des éléments d'une plate-forme (<i>common platform enumeration</i>)
CVE	vulnérabilités et expositions courantes (<i>common vulnerabilities and exposures</i>)
CVSS	système d'évaluation des vulnérabilités courantes (<i>common vulnerability scoring system</i>)
CWE	liste des failles courantes (<i>common weakness enumeration</i>)

CWSS	système d'évaluation des failles courantes (<i>common weakness scoring system</i>)
CYBEX	échange d'informations sur la cybersécurité (<i>cybersecurity information exchange</i>)
CYIQL	langage d'interrogation d'informations de cybersécurité (<i>cybersecurity information query language</i>)
DDoS	déni de service distribué (<i>distributed denial of service</i>)
EVC	certificats de validation étendue (<i>extended validation certificates</i>)
EVCERT	certificat de validation étendu (<i>extended validation certificate</i>)
HTTP	protocole de transfert d'hypertexte (<i>hypertext transfer protocol</i>)
IC	circuit intégré (<i>integrated circuit</i>)
IDS	système de détection des intrusions (<i>intrusion detection system</i>)
IODEF	format d'échange de description d'objet incident (<i>incident object description exchange format</i>)
IPS	système de prévention des intrusions (<i>intrusion prevention system</i>)
IT	technologie de l'information (<i>information technology</i>)
MAEC	liste et caractérisation des attributs de logiciels malveillants (<i>malware attribute enumeration and characterization</i>)
OID	identificateur d'objet (<i>object identifier</i>)
OS	système d'exploitation (<i>operating system</i>)
OVAL	langage ouvert d'évaluation des vulnérabilités (<i>open vulnerability and assessment language</i>)
RID	défense en temps réel interréseaux (<i>real-time inter-network defense</i>)
SCAP	protocole d'automatisation du contenu de sécurité (<i>security content automation protocol</i>)
SOAP	protocole simple d'accès aux objets (<i>simple object access protocol</i>)
TIC	technologies de l'information et de la communication
TLP	protocole léger de trafic (<i>traffic light protocol</i>)
TLS	sécurité de la couche transport (<i>transport layer security</i>)
TNC	connexion avec un réseau de confiance (<i>trusted network connect</i>)
TPM	module de plate-forme de confiance (<i>trusted platform module</i>)
XCCDF	format de description extensible de la liste de contrôle de la configuration (<i>eXtensible configuration checklist description format</i>)

5 Conventions

Lorsque le terme "norme" ou "normes" est utilisé dans la présente Recommandation dans son sens générique, il doit être interprété comme comprenant les normes, spécifications et Recommandations.

6 Concept de base – Échange d'informations sur la cybersécurité (CYBEX)

La présente Recommandation relative à l'échange d'informations sur la cybersécurité (CYBEX) a un objectif simple et limité qui est de décrire des techniques permettant à des entités de cybersécurité d'échanger des informations sur la cybersécurité selon des méthodes offrant un niveau de garantie convenable. Généralement, ces entités sont des organisations, des personnes, des dispositifs ou des processus possédant ou cherchant des informations sur la cybersécurité. Le plus

souvent, ces entités sont des équipes CIRT et les opérateurs ou fabricants d'équipements, de logiciels et de systèmes réseaux.

L'échange d'informations sur la cybersécurité est très important pour renforcer la cybersécurité et la protection des infrastructures et pour contribuer aux fonctions principales effectuées par les équipes CIRT.

L'échange d'informations sur la cybersécurité peut se faire au sein de communautés de confiance et très compartimentées respectant les principes du besoin de savoir basés sur des politiques convenues au préalable, ainsi qu'au sein du domaine public. La connaissance des menaces, des vulnérabilités, des incidents et des risques, ainsi que des mesures permettant de les atténuer ou d'y remédier sont des exemples types des informations sur la cybersécurité échangées entre entités. Les techniques associées décrites dans la présente Recommandation ont pour objet de faciliter cet échange d'informations et donc d'améliorer la cybersécurité.

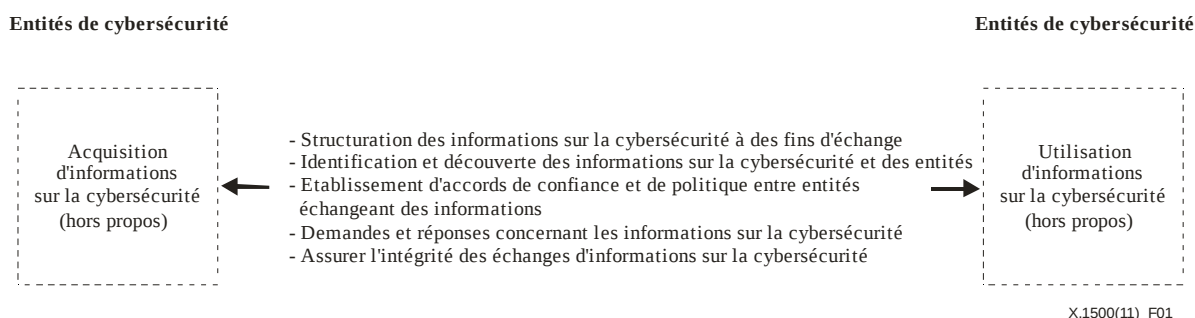


Figure 1 – Modèle de CYBEX

Le modèle général d'échange d'informations sur la cybersécurité utilisé dans la présente Recommandation (Figure 1) est composé de fonctions de base pouvant être utilisées séparément ou ensemble, selon qu'il conviendra et étendues en fonction des besoins afin de faciliter les échanges d'informations assurées sur la cybersécurité. Ces fonctions sont les suivantes :

- structuration des informations sur la cybersécurité à des fins d'échange;
- identification et découverte d'informations sur la cybersécurité et d'entités;
- établissement d'accords de confiance et de politiques d'échange d'informations entre entités échangeant de telles informations;
- demandes et réponses concernant les informations sur la cybersécurité;
- assurer l'intégrité des échanges d'informations sur la cybersécurité.

Le paragraphe 7 décrit des techniques relatives à l'exécution de ces fonctions.

L'échange d'informations sur la cybersécurité peut être bidirectionnel, ce qui permet de tenir compte de demandes et de réponses concernant des informations vérifiées pour assurer les niveaux de garantie requis entre les parties ou de fournir une attestation de fourniture.

Sous réserve des politiques agréées ainsi que des lois et réglementations applicables, les moyens d'acquisition d'informations ainsi que l'usage de ces informations ne sont ni couverts ni traités par la présente Recommandation. Par exemple, certaines applications spécialisées d'échange d'informations sur la cybersécurité, comme le retraçage de l'origine d'une attaque, peuvent nécessiter des mécanismes propres à l'application qui tiennent compte d'une série récursive de demandes et de réponses pour obtenir les informations requises. Toutefois, d'autres applications comme l'utilisation de capacités pour pouvoir mesurer et gérer la cybersécurité relèvent de la présente Recommandation. Ces applications et d'autres types d'utilisation peuvent être facilités par les techniques décrites dans la présente Recommandation. Ni les techniques décrites ni l'échange

d'informations sur la cybersécurité qui y sont associées ne sont rendues obligatoires par la présente Recommandation et d'autres techniques peuvent être appropriées.

7 Techniques d'échange structuré d'informations sur la cybersécurité

Pour que deux entités puissent échanger des informations sur la cybersécurité, l'échange doit être structuré et décrit de manière cohérente, compréhensible par ces deux entités. L'objectif des spécifications CYBEX est de faciliter le partage d'informations sur la cybersécurité qui comprennent des "listes courantes", c'est-à-dire, des listes organisées de valeurs d'information bien établies pour le même type de données. Les listes courantes permettent d'établir un lien entre des bases de données distribuées et d'autres capacités et facilitent les comparaisons en matière de cybersécurité.

Afin de mener à bien ces échanges, les informations sur la cybersécurité incluent des informations et des connaissances structurées concernant:

- l'état de l'équipement du logiciel ou des systèmes réseaux sur le plan de la cybersécurité et en particulier des vulnérabilités;
- les rapports d'incidents ou d'événements;
- les heuristiques et les signatures dérivées d'événements passés;
- les entités de cybersécurité impliquées;
- les spécifications pour l'échange d'informations sur la cybersécurité, y compris les modules, les schémas, les termes et conditions et les numéros assignés;
- les identités et les attributs fiables de toutes les informations sur la cybersécurité;
- les prescriptions, lignes directrices et pratiques d'implémentation.

Pour décrire à un niveau général les attributs souhaités pour l'échange d'informations sur la cybersécurité, les capacités d'échange structuré d'informations sont organisées en six "grappes" de techniques pour des groupes distincts d'échange d'informations sur la cybersécurité. Ces grappes sont les suivantes:

- Failles, vulnérabilités et état.
- Événements, incidents et heuristiques.
- Politique d'échange d'informations.
- Identification, découverte et interrogation.
- Assurance de l'identité.
- Protocole d'échange.

Ces grappes sont des classifications larges et les capacités d'une grappe peuvent en fait être utilisées dans une ou plusieurs autres grappes, en fonction de l'application.

Chacune des grappes énumérées ci-dessus est décrite en détail dans les paragraphes ci-après. Ils donnent pour chaque grappe un aperçu du rôle dans les spécifications CYBEX et une liste des techniques de mise en oeuvre. Les techniques identifiées ne sont en aucun cas prescriptives et illustrent simplement des techniques considérées comme étant cohérentes avec les objectifs de la grappe concernée. Le choix du traitement dépend avant tout du degré de spécialisation de la communauté d'utilisateurs "propriétaire" et avec les avantages généraux dérivés de l'importation.

Les techniques CYBEX décrites dans la présente Recommandation identifient une panoplie de techniques complémentaires qui permettent et facilitent ces instanciations et d'autres.

Le reste de cette partie et l'Appendice I associé décrivent chaque grappe, et donnent un aperçu de leur rôle dans les techniques CYBEX ainsi qu'une liste des techniques de mise en oeuvre pour chaque grappe. Les références ne sont pas normatives et sont détaillées dans la bibliographie.

Les entités chargées de la mise en oeuvre et les utilisateurs des techniques de grappe se conformeront à toutes les législations, réglementations et politiques nationales et régionales applicables.

7.1 Grappe d'échange – Failles, vulnérabilités et état

Les fonctionnalités associées à la grappe d'échange d'informations sur les failles, les vulnérabilités et l'état prennent en charge l'échange d'informations sur les failles et les vulnérabilités et l'évaluation de l'état des systèmes et des applications.

Le Tableau I.1 donne une liste de fonctionnalités qui sont représentatives des types qui peuvent faciliter la prise en charge de l'échange d'informations sur les failles, les vulnérabilités et l'état.

7.2 Grappe d'échange – Événements, incidents et heuristiques

Les fonctionnalités associées à la grappe d'échange d'informations sur les événements, les incidents et les heuristiques prennent en charge l'échange d'informations se rapportant à des événements, incidents ou heuristiques observés.

Le Tableau I.2 donne une liste de fonctionnalités qui sont représentatives des types qui peuvent faciliter la prise en charge de l'échange d'informations sur les événements, les incidents ou les heuristiques observés, de manière structurée entre des équipes CIRT et d'autres entités. Ces informations échangées pourront servir à élaborer une réponse globale aux attaques et à réduire les failles et les vulnérabilités existantes.

7.3 Grappe d'échange – Politique d'échange d'informations

Les fonctionnalités associées à la grappe d'échange d'information sur la politique d'échange d'informations permettent à des entités d'échanger et d'utiliser des informations sur la cybersécurité en ce qui concerne les termes et conditions associés aux informations partagées. Ces conditions peuvent être liées aux informations spécifiques partagées ou à la classe large d'informations à laquelle elle appartient ou encore être associées aux entités impliquées. Si les circonstances l'exigent, il est souhaitable de fournir aux entités concernées une notification de ces politiques. Cette notification peut prendre de nombreuses façons et être acheminée avec l'information ou fournie de manière indépendante par un mécanisme de questions-réponses.

Le Tableau I.3 donne une liste de fonctionnalités qui sont représentatives des types qui peuvent faciliter la prise en charge de l'échange d'informations de politique entre des entités de cybersécurité. Il est à noter que les exigences et les protocoles concernant l'échange d'informations de politique continuent d'être mis au point dans le cadre des groupes sur l'échange sur la sécurité des informations et il faut veiller à s'assurer de leur bonne mise en oeuvre.

7.4 Grappe d'identification, de découverte et d'interrogation

Les fonctionnalités associées à la grappe d'identification, de découverte et d'interrogation prennent en charge les processus d'identification, de découverte et d'interrogation.

Les communautés de la cybersécurité s'intéressent souvent à des questions concernant les identificateurs de cybersécurité ainsi que leur création, leur administration, leur découverte, leur vérification et leur utilisation, notamment:

- Accroître la valeur des informations de cybersécurité en échange de l'information sur l'événement connexe et l'analyse des événements sur de longues périodes.
- Renforcer la sécurité des échanges d'informations sur la cybersécurité en permettant l'obtention des informations concernant les identificateurs à des fins de vérification et la connaissance de politiques associées.

- Accroître la souplesse des échanges d'informations sur la cybersécurité en permettant l'obtention d'informations nouvelles ou complémentaires associées au message, par exemple, état de l'information.

Différentes organisations de cybersécurité souhaiteront peut-être mettre en oeuvre des protocoles communs de cybersécurité pour saisir et échanger des informations sur l'état du système, les vulnérabilités, les rapports d'incident et l'heuristique des incidents dans des applications opérationnelles. Etant donné que ces informations peuvent être fournies par des sources nombreuses et différentes, les responsables de la mise en oeuvre devraient harmoniser la méthode d'identification des organisations de cybersécurité, les politiques de confiance et d'échange d'informations et les informations proprement dites qui sont échangées ou distribuées. Le fait qu'un identificateur unique non ambigu utilisé pour les échanges d'informations de cybersécurité peut exister implique nécessairement qu'il présente les caractéristiques suivantes:

- simplicité, facilité d'utilisation, souplesse, extensibilité, modularité et facilité de déploiement;
- gestion répartie des différents schémas d'identificateurs;
- fiabilité à long terme des registres d'identificateurs et disponibilité d'outils très performants pour découvrir les informations associées à un identificateur donné.

Le Tableau I.4 donne une liste de fonctionnalités qui sont représentatives des types qui peuvent faciliter l'identification des organisations de cybersécurité, ainsi que les processus de découverte et de demande d'informations sur la cybersécurité.

7.5 Grappe d'assurance d'identité

Les fonctionnalités associées à la grappe d'assurance d'identité prennent en charge l'assurance d'identité.

Dans le cadre des spécifications CYBEX, l'échange proprement dit d'informations structurées peut se faire de différentes façons, via un réseau ou par transport physique. Un élément clé de l'échange est la confiance, c'est-à-dire la confiance dans l'identité des parties et dans les informations transmises.

Le Tableau I.5 donne une liste de fonctionnalités qui sont représentatives des types qui peuvent prendre en charge l'assurance d'identité.

7.6 Grappe des protocoles d'échange

Les fonctionnalités associées à la grappe des protocoles d'échange comprennent les protocoles d'échange susceptibles d'être utilisés dans différents contextes d'échange d'informations sur la cybersécurité. L'échange sécurisé d'informations suppose d'associer certains des protocoles énumérés ci-après. Le système de défense en temps réel interréseaux (RID) offre un cadre d'échange de messages permettant de communiquer des informations sur les incidents et les politiques associées à cette information. Le protocole de transport des messages RID encapsulant les documents d'incident au format IODEF (ainsi que toute extension du format IODEF) comprend les options de transport SOAP, BEEP et HTTPS énumérées ci-après. Le protocole de transport des messages RID (c'est-à-dire le premier protocole de transport mis au point pour les messages RID) pourra être remplacé par le protocole SOAP, BEEP ou un protocole défini ultérieurement. Le système RID tient compte d'éléments de sécurité et de confidentialité et permet ainsi de séparer l'échange de messages du transport.

Le Tableau I.6 donne une liste des fonctionnalités qui sont représentatives des types de protocoles d'échange pouvant être utilisés pour échanger des informations.

Appendice I

Techniques d'échange structuré d'informations sur la cybersécurité

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

Tableau I.1 – Techniques utilisées dans la grappe d'échange Failles, vulnérabilités et état

Technique	Description	Références
Vulnérabilités et expositions courantes (CVE)	Les vulnérabilités et expositions courantes (CVE) correspondent à une méthode qui permet d'identifier et d'échanger des informations sur les vulnérabilités et les expositions courantes en matière de sécurité de l'information et fournit des dénominations communes pour les problèmes connus du public. L'objectif des CVE est de faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services) sur la base de cette "liste courante". Les CVE sont conçues pour permettre d'utiliser en association des bases de données sur les vulnérabilités et d'autres ressources, et faciliter la comparaison des outils et services de sécurité. Ainsi, les CVE ne prennent pas en considération les informations telles que des informations sur les risques, les incidences et les solutions, ou des informations techniques détaillées. Elles prennent uniquement en considération le numéro d'identification standard avec un indicateur d'état, une brève description, et des références aux rapports et avis de vulnérabilité associés. Le but des CVE est de pouvoir identifier toutes les vulnérabilités et expositions connues du public. Elles sont conçues pour prendre en considération des informations bien établies, mais l'objectif premier est d'identifier les vulnérabilités et les expositions qui sont détectées par les outils de sécurité, ainsi que tout nouveau problème rendu public, puis de régler les éventuels problèmes de sécurité plus anciens qui nécessitent une validation.	[b-UIT-T X.1520]
Système d'évaluation des vulnérabilités courantes (CVSS)	Le système d'évaluation des vulnérabilités courantes (CVSS) définit un cadre ouvert pour la communication des caractéristiques et des incidences des vulnérabilités en matière de TIC. Le CVSS se compose de trois groupes: base, temporel et environnemental. Chaque groupe produit une note numérique de 0 à 10 et un vecteur, qui est une représentation textuelle comprimée qui reflète les valeurs utilisées pour calculer la note. Le groupe Base représente les qualités intrinsèques d'une vulnérabilité. Le groupe Temporel représente les caractéristiques d'une vulnérabilité qui changent dans le temps. Le groupe Environnemental représente les caractéristiques d'une vulnérabilité qui sont uniques à l'environnement de l'utilisateur. Le CVSS permet aux gestionnaires des TIC, aux fournisseurs de bulletins d'information sur les vulnérabilités, aux fournisseurs de systèmes de sécurité, aux fournisseurs d'applications et aux chercheurs de tirer profit de l'adoption d'un langage commun d'évaluation des vulnérabilités en matière de TIC.	[b-ITU-T X.1521]

Tableau I.1 – Techniques utilisées dans la grappe d'échange Failles, vulnérabilités et état

Technique	Description	Références
Liste des failles courantes (CWE)	La liste des failles courantes (CWE) permet d'identifier et d'échanger des ensembles unifiés et mesurables de failles logicielles. Elle rend possible une discussion, une description, un choix et un emploi plus efficace d'outils et de services de sécurité logicielle qui permettent de repérer les failles dans le code source et dans les systèmes d'exploitation. La CWE permet aussi de mieux comprendre et mieux gérer les failles logicielles liées à l'architecture et à la conception. Les implémentations CWE sont compilées et actualisées par un groupe international d'experts d'horizons très divers (entreprises, universités et organismes publics), garantissant ainsi un contenu très vaste et détaillé. La liste CWE offre une terminologie normalisée, permet aux fournisseurs de services d'informer les utilisateurs des failles potentielles spécifiques et des solutions proposées; elle permet aussi aux acheteurs de logiciels de comparer des produits similaires proposés par plusieurs fournisseurs.	[b-CWE]
Système d'évaluation des failles courantes (CWSS)	Le système d'évaluation des failles courantes (CWSS) offre un cadre ouvert pour communiquer les caractéristiques et les incidences des failles logicielles.	[b-CWSS]
Langage ouvert d'évaluation des vulnérabilités (OVAL)	Le langage ouvert d'évaluation des vulnérabilités (OVAL) est une spécification internationale visant à promouvoir des contenus de sécurité ouverts et publics et à normaliser le transfert de ces informations entre les différents outils et services de sécurité. OVAL comprend un langage utilisé pour coder les détails des systèmes et différents répertoires de contenus tenus à jour par la communauté. Ce langage normalise les trois principales étapes du processus d'évaluation: représenter des informations de configuration des systèmes pour essais; analyser le système pour détecter la présence de l'état spécifié de la machine (vulnérabilité, configuration, état du correctif, etc.) et communiquer les résultats de cette évaluation. Les répertoires sont des collections de contenus ouverts et publics qui utilisent ce langage. Les schémas OVAL écrits en XML ont été mis au point pour servir de cadre et de vocabulaire au langage OVAL. Ces schémas correspondent aux trois étapes du processus d'évaluation: schéma des caractéristiques de système OVAL pour représenter les informations système, schéma de définition OVAL pour exprimer l'état d'une machine spécifique et schéma des résultats OVAL pour communiquer les résultats d'une évaluation.	[b-OVAL]

Tableau I.1 – Techniques utilisées dans la grappe d'échange Failles, vulnérabilités et état

Technique	Description	Références
Format de description extensible de la liste de contrôle de la configuration (XCCDF)	Le format de description extensible de la liste de contrôle de la configuration (XCCDF) est un langage de spécification permettant d'établir des listes de contrôle, des critères de référence et des types de documents associés concernant la sécurité. Un document XCCDF est un ensemble structuré de règles de configuration de sécurité relatives à un ensemble de systèmes cibles. La spécification est conçue pour permettre la prise en charge de l'échange d'informations, de la production de documents, de l'adaptation en fonction de l'organisation et de la situation, des tests automatiques de conformité et de la notation. La spécification définit également un modèle et un format de données pour l'enregistrement des résultats des tests effectués par rapport aux critères de référence. Elle vise à fournir une base uniformisée pour l'établissement des listes des contrôles de sécurité, des critères de référence et d'autres orientations en matière de configuration, et à encourager ainsi une application plus généralisée de bonnes pratiques en matière de sécurité. Les documents XCCDF sont rédigés en langage XML.	[b-XCCDF]
Système commun d'énumération des éléments d'une plate-forme (CPE)	Le système commun d'énumération des éléments d'une plate-forme (CPE) est une méthode normalisée permettant d'identifier et de décrire les systèmes logiciels et le matériel du parc informatique d'une entreprise. Le système CPE comprend une spécification de dénomination qui définit la structure logique des noms CPE ayant une structure correcte et les procédures de rattachement ou de détachement de ces noms grâce à un codage pouvant être déchiffré par des machines; une spécification de correspondance, qui définit les procédures permettant de comparer les noms CPE pour déterminer s'ils correspondent à certains ou à la totalité des produits ou plates-formes et une spécification de dictionnaire qui définit le concept de dictionnaire d'identificateurs et prescrit des règles de haut niveau que les responsables de la tenue à jour du dictionnaire doivent respecter.	[b-CPE]
Liste des configurations courantes (CCE)	La liste des configurations courantes (CCE) donne des identificateurs non ambigus aux problèmes de configuration de systèmes afin de faciliter la corrélation rapide et précise de données de configuration dans de multiples sources et outils informatiques. Par exemple, on peut utiliser les identificateurs CCE pour associer des contrôles effectués dans des outils d'évaluation de la configuration à des déclarations figurant dans des documents sur les bonnes pratiques en matière de configuration.	[b-CCE]

Tableau I.1 – Techniques utilisées dans la grappe d'échange Failles, vulnérabilités et état

Technique	Description	Références
Format des résultats d'évaluation (ARF)	Le format des résultats d'évaluation (ARF) est une spécification ouverte qui fournit un langage structuré permettant aux outils d'évaluation, aux bases de données d'actifs et à d'autres produits qui gèrent des informations sur les actifs d'échanger des résultats d'évaluation par dispositif. Il a vocation à être utilisé par des outils qui recueillent des données détaillées sur la configuration du parc informatique. Le format ARF comprend en outre une spécification de rapport de synthèse pour permettre l'établissement de rapports sur des informations dans de multiples actifs, et un langage de planification des tâches et d'interrogation permettant de demander les résultats d'évaluation. Les spécifications d'automatisation de la sécurité décrivent un processus de bout en bout permettant de fournir des contenus d'évaluation à des mémoires de données, de demander des évaluations sur la base de ce contenu, de rendre compte des résultats de ces évaluations et de faire une synthèse des résultats d'évaluation au niveau de l'entreprise.	[b-ARF]

Tableau I.2 – Techniques utilisées dans la grappe d'échange Événements, incidents et heuristiques

Technique	Description	Références
Expression des événements courants (CEE)	L'expression des événements courants (CEE) normalise la manière de décrire, d'enregistrer et de communiquer les événements informatiques. L'utilisation de ce langage et de cette syntaxe, la gestion des journaux au niveau de l'entreprise, la corrélation, l'agrégation, l'audit et le traitement des incidents peuvent être effectués avec davantage d'efficacité et donner de meilleurs résultats. L'objectif principal en l'espèce est de normaliser la représentation et l'échange de journaux établis par des systèmes électroniques. Le système CCE décompose l'enregistrement et l'échange des journaux en quatre (4) éléments: la taxonomie des événements, la syntaxe des journaux, le transport des journaux et les recommandations pour l'établissement de journaux.	[b-CEE]
Format d'échange de description d'objet incident (IODEF)	Le format d'échange de description d'objet incident (IODEF) définit une représentation de données qui fournit un format type pour l'échange d'informations habituelles entre CIRT sur des incidents de sécurité informatique. Le format IODEF décrit un modèle d'information et propose un modèle de données associé spécifié avec un schéma XML.	[b-IETF RFC 5070]

Tableau I.2 – Techniques utilisées dans la grappe d'échange Événements, incidents et heuristiques

Technique	Description	Références
Format d'échange d'informations sur l'hameçonnage, les fraudes et les utilisations abusives	Ce format d'échange d'informations sur l'hameçonnage, les fraudes et les utilisations abusives élargit le format d'échange de description d'objet incident (IODEF) pour prendre en charge le signalement de l'hameçonnage, de fraudes et d'autres types d'utilisation abusive. Ces extensions offrent en outre un format standard pour l'échange d'informations concernant des incidents de spam courants. Elles sont suffisamment souples pour prendre en charge les informations collectées à partir d'activités tout au long du cycle de fraudes ou de spams électroniques. Ce format permet à la fois l'établissement de rapports simples et de rapports d'analyse complets et de synthèse d'incidents multiples. NOTE – Cette Recommandation ne décrit que des techniques concernant des moyens largement compris et assurés permettant aux entités de cybersécurité d'échanger des informations sur la cybersécurité et ne porte pas sur l'utilisation de ces informations.	[b-IETF RFC 5901]
Liste et classification des schémas d'attaque courants (CAPEC)	La liste et classification des schémas d'attaque courants (CAPEC) est une méthode de spécification pour l'identification, la description et l'énumération de schémas d'attaque. Les schémas d'attaque représentent un mécanisme extrêmement performant pour saisir et communiquer la perspective de l'attaquant. Il s'agit de descriptions de méthodes courantes d'exploitation de logiciels qui reposent sur l'utilisation à des fins de destruction (et non de construction) des schémas de conception et sont le fruit d'une analyse approfondie d'exemples remarquables précis qui se sont produits dans le monde réel. L'objectif de la spécification CAPEC est de fournir un catalogue public des schémas d'attaque ainsi qu'un schéma XML complet et une taxonomie de classification.	[b-CAPEC]
Format de liste et de caractérisation des attributs de logiciels malveillants (MAEC)	Le format de liste et de caractérisation des attributs de logiciels malveillants (MAEC) est un langage formel qui comprend un schéma pour fournir à la fois une syntaxe pour le vocabulaire courant des attributs et comportements énumérés et un format pour échanger des informations structurées sur ces éléments de données. Les listes sont à des niveaux différents d'abstraction: actions au bas niveau, comportements au niveau intermédiaire et mécanismes de haut niveau. Au niveau le plus bas, le format MAEC décrit les attributs liés à la fonctionnalité de base et au fonctionnement de bas niveau des logiciels malveillants. Au niveau intermédiaire, le langage MAEC organise en groupes les actions à faible niveau mentionnées ci-dessus afin de définir les comportements de niveau intermédiaire. Au niveau le plus conceptuel et le plus élevé, le vocabulaire du langage MAEC permet de construire des mécanismes qui abstraient des groupes de comportements malveillants de niveau intermédiaire basés sur la réalisation d'une classification d'ordre supérieur.	[b-MAEC]

Tableau I.3 – Techniques utilisées dans la grappe d'échange de politiques

Technique	Description	Références
Protocole léger de trafic (TLP)	Le protocole TLP a été créé pour encourager un plus grand partage d'informations sensibles. L'initiateur indique dans quelles limites il souhaite que ses informations circulent au-delà du destinataire immédiat. Le protocole TLP offre une méthode simple pour atteindre cet objectif. Il est conçu pour améliorer le flux d'informations entre individus, organisations ou communautés, d'une façon contrôlée et fiable. Il repose sur le concept du marquage de l'information par l'initiateur au moyen d'une des quatre couleurs pour indiquer dans quelle mesure le destinataire peut, éventuellement, élargir la diffusion. Le destinataire doit consulter l'initiateur si une diffusion plus large est requise. Le protocole TLP est accepté comme modèle pour l'échange d'informations de confiance entre communautés de sécurité dans plus de trente pays. Les quatre "niveaux de partage des informations" pour le traitement des informations sensibles sont les suivants: ROUGE – Personnel. Ces informations sont destinées uniquement à des destinataires nommés. Par exemple, dans le contexte d'une réunion, les informations en ROUGE sont limitées aux personnes présentes à la réunion. Dans la plupart des cas, les informations en ROUGE sont transmises oralement ou personnellement. ORANGE – Distribution limitée. Le destinataire peut partager des informations ORANGE avec d'autres personnes de son organisation mais uniquement si ces personnes ont un besoin de savoir. VERT – Au niveau de la communauté. Les informations de cette catégorie peuvent être diffusées largement au sein d'une communauté particulière. Toutefois, elles ne peuvent être ni publiées, ni postées sur l'Internet, ni divulguées à l'extérieur de la communauté. BLANC – Illimitée. Sous réserve du respect des règles standard du droit d'auteur, les informations en BLANC peuvent être diffusées librement, sans restriction.	[b-TLP]

**Tableau I.4 – Techniques utilisées dans la grappe d'identification,
de découverte et d'interrogation**

Technique	Description	Référence
Mécanismes de découverte dans l'échange d'informations sur la cybersécurité	Ces techniques comprennent des méthodes et des mécanismes pouvant être utilisés pour identifier et localiser des sources d'information sur la cybersécurité, des types d'informations sur la cybersécurité, des types spécifiques d'informations sur la cybersécurité, des méthodes disponibles pour accéder à des informations sur la cybersécurité, ainsi que des politiques qui peuvent être appliquées à l'accès aux informations sur la cybersécurité.	
Lignes directrices pour l'administration de l'arc d'identificateur d'objet pour l'échange d'informations sur la cybersécurité	Ces lignes directrices décrivent un espace de noms commun d'identificateurs de cybersécurité et des prescriptions administratives, dans le cadre d'un arc d'identificateur d'objet cohérent, et comprend des identificateurs pour: • les informations sur la cybersécurité; • les organisations de cybersécurité; • la politique en matière de cybersécurité.	
Langage de demande d'informations sur la cybersécurité	Le langage de demande d'informations sur la cybersécurité définit une représentation de données souples qui fournit un cadre pour demander des informations couramment échangées par les équipes d'intervention en cas d'incident informatique (CIRT) à propos d'incidents liés à la sécurité informatique. Cette spécification décrit le modèle d'information pour le langage CYIQL et offre un modèle de données associé spécifié avec un schéma XML.	

Tableau I.5 – Techniques utilisées dans la grappe d'assurance d'identité

Technique	Description	Références
Plates-formes de confiance	Les produits informatiques et de communication dotés d'un module de plate-forme de confiance (TPM) permettant aux entreprises, aux institutions, aux organismes publics et aux consommateurs d'être mieux à même d'effectuer des échanges d'informations de confiance; les modules TPM sont donc pertinents pour la plupart des implémentations CYBEX. Ces modules sont des circuits intégrés spécifiques montés sur différentes plates-formes pour permettre une authentification forte de l'utilisateur et une attestation des machines, qui sont essentielles pour empêcher l'accès inapproprié à des informations confidentielles et sensibles et se protéger contre des réseaux compromis. La technologie de module de plate-forme de confiance repose sur des normes ouvertes pour assurer l'interopérabilité de produits différents dans des environnements multifabricants. La norme TPM la plus courante comprend un ensemble de spécifications élaborées et tenues à jour par le TCG (<i>Trusted Computing Group</i>) et un profil de protection pour l'évaluation de la sécurité à partir de critères communs. Les principes de conception donnent les concepts fondamentaux du module TPM et des informations génériques concernant leur fonctionnalité. Un concepteur de module TPM doit examiner et utiliser les informations contenues dans les spécifications principales TPM (Parties 1-3) et examiner les documents se rapportant au type de plate-forme concerné. Le document propre à un type de plate-forme contient des déclarations normatives qui affectent la conception et la mise en oeuvre d'un module TPM. Un concepteur de module TPM doit examiner les exigences définies par le groupe de travail sur la conformité du TCG et s'y conformer, y compris en matière de tests et d'évaluation. Les modules TPM doivent être conformes aux exigences et passer toutes les évaluations établies par le groupe de travail sur la conformité. Les modules TPM peuvent être soumis à d'autres tests et évaluations plus stricts.	[b-TPM]

Tableau I.5 – Techniques utilisées dans la grappe d'assurance d'identité

Technique	Description	Références
Connexion avec un réseau de confiance	Les opérations de sécurité TIC visent souvent à découvrir l'état du niveau du système d'exploitation ainsi que du logiciel d'application utilisé par le réseau de prise en charge. Par exemple, faute de correctifs de sécurité OS ou de signatures antivirus pour le système, une notification fiable est essentielle pour limiter les dégâts associés à des attaques réseau. Pour faire cette évaluation, il faut des informations fiables confirmant qu'un système connecté se trouve dans un état donné. Pour empêcher des systèmes, par exemple, des systèmes piratés, de falsifier des informations, une bonne évaluation suppose qu'une base matérielle soit installée sur le système à évaluer. Les plates-formes de confiance sont intégrées dans le matériel pour enregistrer certains faits concernant le processus de démarrage et les transmettre sous une forme comportant une signature numérique. De plus, les grands fabricants de puces complètent aujourd'hui les plates-formes de confiance avec une capacité de "démarrage tardif" qui prévoit l'exécution d'un code de confiance plus tard dans la séquence de démarrage, ce qui permet d'enregistrer des événements de manière fiable après le processus de démarrage propre au matériel. Dans la pratique, la gestion de la configuration du réseau est une attestation de déploiement de système: les agents logiciels sur les machines d'une entreprise envoient régulièrement des rapports de configuration à un répertoire central, qui évalue et signale les systèmes non conformes. Les données de ces agents logiciels, tout en étant précieuses, peuvent être facilement modifiées par un attaquant. La généralisation de l'utilisation de plates-formes de confiance pour permettre une évaluation plus fiable de l'état d'un système augmenterait nettement la confiance d'une entreprise dans ses données de gestion des configurations. L'architecture TNC est une architecture ouverte de contrôle d'accès au réseau. Son objectif est de permettre aux opérateurs de réseaux d'assurer l'intégrité des points de terminaison pour toutes les connexions de réseaux, permettant ainsi l'interopérabilité entre points de terminaison de réseaux dans un environnement de fabricants multiples.	[b-TNC]
Assurance de l'authentification d'entité	Cette norme est un cadre applicable au cycle de vie des authentifications et permet de gérer l'assurance de l'identité d'une entité et les informations d'identité associées dans un contexte donné. Plus précisément, elle définit des méthodes pour: 1) mesurer sur le plan qualitatif et attribuer des niveaux d'assurance relatifs à l'authentification des identités d'une entité et des informations d'identité associées; et 2) communiquer des niveaux d'assurance relative d'authentification.	[b-NIST EAA]

Tableau I.5 – Techniques utilisées dans la grappe d'assurance d'identité

Technique	Description	Références
Cadre applicable aux certificats de validation étendue	Le cadre applicable aux certificats de validation étendue est une combinaison intégrée de prescriptions minimales en matière de technologies, de protocoles, de vérification d'identité, de gestion du cycle de vie et de méthodes d'audit qui doivent être satisfaites pour que les certificats de validation étendue (certificats EV) concernant une organisation donnée puissent être délivrés et gérés. Ce cadre est conforme à de nombreuses prescriptions en matière de sécurité, de localisation et de notification.	[b-EVCERT]
Exigences de politique pour les autorités de certification délivrant des certificats de clé publique	Ce document établit les exigences de politique relatives aux autorités de certification (CA) qui délivrent des certificats de clé publique, y compris des certificats de validation étendue (EVC). Il définit des exigences de politique relatives aux pratiques en matière d'exploitation et de gestion des autorités de certification délivrant et gérant des certificats grâce auxquelles les abonnés, les objets certifiés par l'autorité et les parties utilisatrices pourront avoir confiance dans l'applicabilité du certificat appuyant les mécanismes cryptographiques.	[b-ETSI TS 102 042]

Tableau I.6 – Techniques utilisées dans la grappe des protocoles d'échange

Technique	Description	Références
Défense en temps réel interréseaux (RID)	Le système de défense interréseaux en temps réel (RID) offre un cadre permettant d'échanger des informations sur les incidents. La norme RID définit l'ensemble des messages de coordination en cas d'incident nécessaires à la communication sécurisée de documents IODEF entre entités. La RID permet d'envelopper les documents IODEF, éventuellement étendu. Les messages et les formats d'échange types comprennent des éléments/options concernant les politiques, la confidentialité et la sécurité qui sont nécessaires dans un schéma global de coordination en cas d'incident. Le système RID est la couche de sécurité entre les documents IODEF et le protocole de transport. Le choix du transport incombe aux entités qui communiquent les informations d'incident. Le transport peut être le protocole de transport de messages RID défini (HTTP/TLS), le protocole BEEP, le protocole SOAP ou un protocole défini ultérieurement.	[b-IETF RFC 6045]
Transport de messages RID (défense interréseaux en temps réel)	Ce mécanisme définit le transport des messages de défense interréseaux en temps réel (RID) dans les messages de demande de réponse HTTP transportés sur TLS.	[b-IETF RFC 6046]
Profil de protocole d'échange extensible de blocs (BEEP) pour CYBEX	Un profil BEEP pour les techniques d'échange d'informations sur la cybersécurité spécifie le profil BEEP à utiliser dans les techniques CYBEX. Le protocole BEEP est un protocole d'application générique d'interactions orientées "connexion" asynchrones décrites dans [b-IETF RFC 3080]. Il repose sur un mécanisme de mise en trame qui permet des échanges simultanés et indépendants de messages entre homologues. Tous les échanges se font dans le contexte d'un canal (lien vers un aspect bien défini de l'application comme la sécurité du transport, l'authentification de l'utilisateur ou l'échange de données). Chaque canal a un profil associé qui définit la syntaxe et la sémantique des messages échangés.	[b-IETF RFC 3080]
Protocole simple d'accès aux objets (SOAP)	Le protocole SOAP est un protocole simple d'échange d'informations dans un environnement décentralisé et réparti. Ce protocole basé sur le langage XML se compose de trois parties: une enveloppe qui définit un cadre pour la description de ce que contient un message et de la façon de le traiter; un ensemble de règles de codage pour exprimer des exemples de types de données définis par application et une convention pour représenter des appels et des réponses de procédures distantes. Le protocole SOAP peut être utilisé en association avec d'autres protocoles; toutefois, les seuls liens définis dans ce document décrivent comment utiliser le protocole SOAP en association avec le protocole HTTP et son cadre d'extension.	[b-W3C SOAP]

Appendice II

Ontologie d'échange d'informations de cybersécurité

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

L'Appendice II fournit une ontologie de l'échange d'informations sur la cybersécurité, qui illustre un contexte opérationnel pour les techniques CYBEX et permet de créer un écosystème de cybersécurité efficace où des connaissances tirées de rapports, de tests et de l'expérience sont utilisées pour créer et faire évoluer des informations sur les points faibles et les vulnérabilités qui, à leur tour, peuvent être utilisées avec les informations sur l'état du système pour mesurer et améliorer la sécurité.

L'ontologie CYBEX définit les termes suivants:

- 1) **Opérations de cybersécurité:** Méthodes et processus utilisés pour contrôler et gérer la sécurité dans des limites opérationnelles définies, incluant:
 - la collecte et l'analyse d'informations pouvant avoir un effet sur la sécurité;
 - la détection de comportements ou d'événements nuisant à la sécurité ou permettant de déterminer le risque de futur effet négatif;
 - les mesures prises en réponse à un comportement ou à un événement nuisible pour limiter, atténuer et/ou empêcher de futurs incidents;
 - les communications liées à la sécurité concernant l'état et la condition des systèmes.
- 2) **Entité de cybersécurité:** Toute entité qui fait partie d'un échange d'informations sur la cybersécurité, y compris l'objet proprement dit des informations.
- 3) **Informations opérationnelles de cybersécurité:** Toute information nécessaire aux entités de cybersécurité pour conduire des opérations de cybersécurité.

Les techniques de cybersécurité décrites dans les spécifications CYBEX sont décrites de façon plus détaillées dans la présente ontologie CYBEX. Il s'agit en fait d'un modèle à utiliser pour décrire le monde abstrait des opérations de cybersécurité. L'ontologie se compose d'un ensemble de types, de propriétés et de relations (voir la Figure II.1). Les lignes pleines indiquent le lien entre les types d'informations, tandis que les flèches indiquent des entrées d'informations provenant d'une entité fonctionnelle et destinées à une base de connaissances/base de données. Les entités fonctionnelles figurant à droite sont génériques et les entités comme les équipes CIRT peuvent englober une ou plusieurs de ces fonctions.

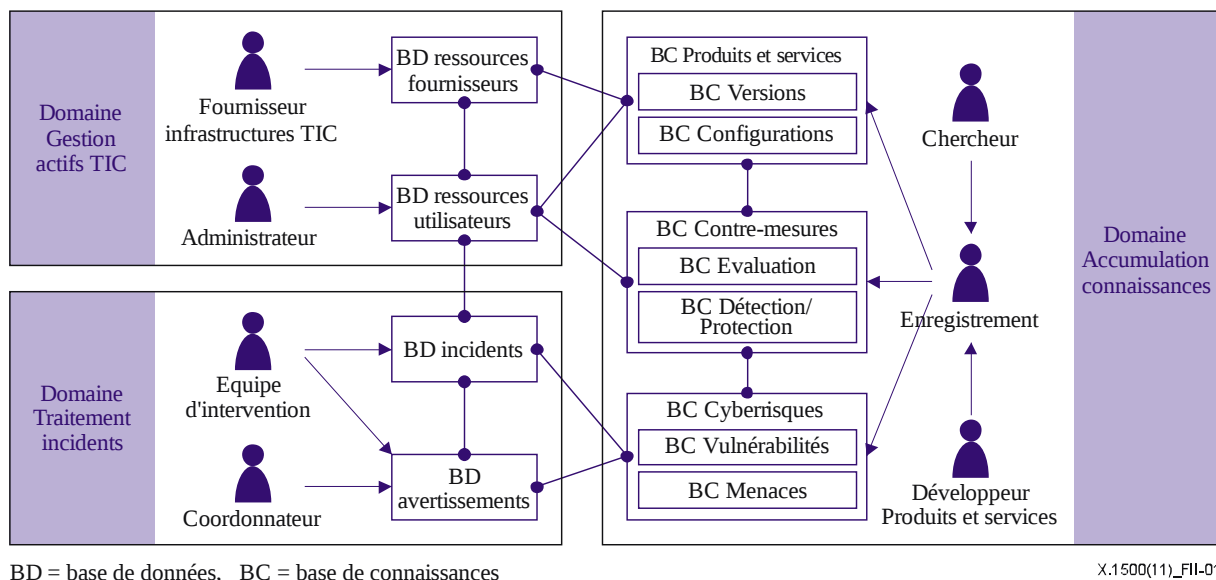


Figure II.1 – Modèle d'ontologie CYBEX

Dans cette ontologie, on utilise un modèle pour définir des domaines d'opérations de cybersécurité, qui est ensuite utilisé pour identifier les entités de cybersécurité requises pour prendre en charge des opérations dans chaque domaine. Dans les paragraphes qui suivent, l'ontologie est décrite en détail, et illustre comment les techniques CYBEX peuvent être utilisées pour prendre en charge cette ontologie.

II.1 Domaines opérationnels

Les opérations de cybersécurité se divisent pour l'essentiel en trois domaines: traitement des incidents, gestion des actifs TIC et accumulation de connaissances.

Le domaine du traitement des incidents s'occupe de détecter et de traiter les incidents de cybersécurité en surveillant les incidents, les événements informatiques qui constituent les incidents et les comportements d'attaque identifiés dans ces incidents. Par exemple, il s'agit de détecter les anomalies grâce à des alarmes émises par des détecteurs, puis de regrouper les détails en collectant différents journaux. Parfois, ce domaine permet de fournir des alertes et des avertissements, par exemple, des avertissements préalables contre des menaces potentielles pour les organisations d'utilisateurs.

Le domaine de la gestion des actifs TIC comprend les opérations de cybersécurité effectuées dans chaque organisation d'utilisateurs comme l'installation, la configuration et la gestion des actifs TIC de l'organisation. Il s'agit à la fois des opérations de prévention des incidents et des opérations de contrôle des dégâts dans chaque organisation.

Le domaine de l'accumulation des connaissances comprend les informations liées à la cybersécurité. Il produit et accumule des connaissances que d'autres organisations peuvent réutiliser.

II.2 Entités de cybersécurité

En se basant sur les domaines opérationnels décrits ci-dessus, on peut identifier les entités fonctionnelles de cybersécurité qui sont nécessaires à la conduite des opérations de cybersécurité dans chaque domaine.

Deux entités sont nécessaires au fonctionnement du domaine du traitement des incidents: l'équipe d'intervention et le coordonnateur. L'équipe d'intervention est une entité qui contrôle et analyse différents types d'incidents, par exemple, un accès non autorisé, l'hameçonnage et des attaques DDoS et il accumule des informations sur les incidents. Sur la base de ces informations, l'équipe

peut mettre en oeuvre des contre-mesures, par exemple inscrire l'adresse des sites d'hameçonnage sur des listes noires. Le coordonnateur est une entité qui assure la coordination avec d'autres entités et étudie des menaces potentielles en s'appuyant sur des informations d'incidents connus.

Le domaine de la gestion des actifs TIC comprend deux entités opérationnelles: l'administrateur et le fournisseur d'infrastructure TIC. L'administrateur assure l'administration du système de son organisation et possède des informations sur ses propres actifs TIC. On trouve en règle générale un administrateur TIC dans chaque organisation. Le fournisseur d'infrastructure TIC fournit à chaque organisation des infrastructures TIC, qui incluent la connectivité au réseau, les services d'informatique en nuage comme les logiciels en tant que services (SaaS), les plates-formes en tant que services (PaaS) et l'infrastructure en tant que service (IaaS) ainsi que des services d'identité. Les fournisseurs de services Internet et les fournisseurs de services d'application (ASP) sont des exemples types.

Le domaine de l'accumulation des connaissances comprend trois entités opérationnelles: le chercheur, le développeur de produit ou de service et l'entité d'enregistrement. Le chercheur cherche des informations sur la cybersécurité, en dépouillant et en rassemblant des connaissances. Le développeur de produit ou de service détient des informations sur les produits et les services comme leur dénomination, les versions, leurs vulnérabilités, leurs correctifs et des informations de configuration. Les éditeurs de logiciels, les ASP et les programmeurs de logiciels sont des exemples types. L'entité d'enregistrement est une entité qui classe et organise les connaissances sur la cybersécurité fournies par les chercheurs, les développeurs et les éditeurs, afin que d'autres organisations puissent les utiliser.

II.3 Informations opérationnelles sur la cybersécurité

Sur la base des domaines opérationnels et des entités, cette partie traite des informations opérationnelles sur la cybersécurité fournies par les entités fonctionnelles de chaque domaine opérationnel.

II.3.1 Domaine du traitement des incidents

Le domaine du traitement des incidents comprend une base de données "incidents" et une base de données "avertissements". La base de données "incidents" contient des informations sur les incidents, fournies par une équipe d'intervention. Elle inclut trois types d'enregistrements: événements, incidents et attaques. Un enregistrement d'événement inclut des événements informatiques comme la connexion d'utilisateurs privilégiés à un système. Il contient également des informations sur des paquets, des fichiers et des transactions liés à des incidents. Généralement, la plupart des enregistrements sont fournis automatiquement par des ordinateurs. Un enregistrement d'incident inclut des événements qui sont des incidents potentiels. Cet enregistrement est en règle générale le fruit de plusieurs enregistrements d'événements et de leurs conjectures, qui sont créées automatiquement et/ou manuellement. Un enregistrement d'attaque repose sur l'analyse d'incidents et comporte la date et l'heure précises des attaques ainsi que leur déroulement.

La base de données "avertissements" contient des informations sur les avertissements de cybersécurité fournis par les équipes d'intervention et les coordonnateurs. Les avertissements reposent sur la base de données "incidents" et sur la base de connaissances des cyberrisques.

II.3.2 Domaine de gestion des actifs TIC

Le domaine de gestion des actifs TIC comporte deux bases de données: une base de données des ressources des utilisateurs et une base de données des ressources des fournisseurs.

La base de données des ressources des utilisateurs regroupe les informations relatives aux actifs d'une organisation donnée et contient des informations comme la liste des logiciels, du matériel, leurs configurations, l'état de l'utilisation des ressources, des politiques de sécurité y compris les politiques de contrôle d'accès, les résultats de l'évaluation du niveau de sécurité et la topologie intranet. Ces informations sont fournies par l'administrateur.

La base de données des ressources des fournisseurs regroupe des informations sur les actifs à l'extérieur de l'organisation en question. Elle contient essentiellement des informations sur les ressources extérieures et des informations sur les réseaux extérieurs. Les informations sur les ressources extérieures sont composées d'informations sur les ressources que chaque organisation utilise à l'extérieur de son organisation comme la liste et l'état des services extérieurs d'informatique en nuage (par exemple, centre de données et SaaS). Les informations concernant les réseaux extérieurs sont composées d'informations sur les réseaux qui relient les organisations entre elles, comme leur topologie, les informations d'acheminement, la politique de contrôle d'accès, l'état du trafic et le niveau de sécurité. Ces informations sont fournies par le fournisseur d'infrastructure TIC.

II.3.3 Domaine de l'accumulation des connaissances

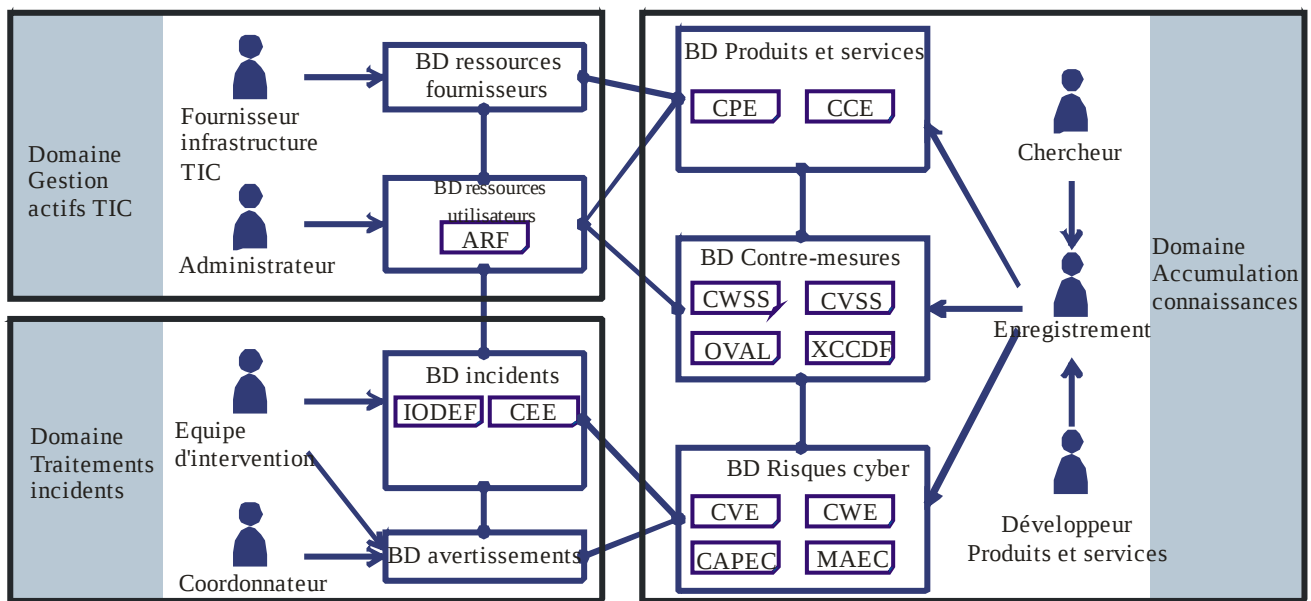
Trois bases de connaissances existent dans le domaine de l'accumulation des connaissances: risques cybernétiques, contre-mesures, produits et services. Elles regroupent des connaissances sur la cybersécurité fournies par les chercheurs et les développeurs de produits ou services, qui sont ensuite organisées et classées par l'entité d'enregistrement.

La base de connaissances sur les risques cybernétiques regroupe des informations sur les risques en matière de cybersécurité et inclut des connaissances sur les vulnérabilités et les menaces. La base de connaissances sur les vulnérabilités regroupe des informations sur les vulnérabilités connues, y compris la dénomination, la taxonomie et la liste des vulnérabilités connues. Elle inclut aussi les vulnérabilités humaines encourues par les utilisateurs humains des TIC. La base de connaissances sur les menaces regroupe des informations sur les menaces connues qui incluent des connaissances sur les attaques et sur les utilisations abusives. Les connaissances sur les attaques incluent des informations sur les schémas d'attaques, les outils d'attaques (par exemple, logiciels malveillants) et leurs tendances, comme les informations sur les tendances des attaques passées en termes de géographie et de cibles. Elle inclut aussi des informations statistiques sur les attaques passées. Les connaissances sur les utilisations abusives incluent des informations sur les utilisations abusives des TIC par des utilisateurs humains sans aucune intention malveillante. Les informations sur les fautes de frappe, les pièges de l'hameçonnage et les violations de conformité sont incluses.

La base de connaissances sur les contre-mesures regroupe des informations sur les contre-mesures visant les risques de cybersécurité et contient deux bases de connaissances: évaluation et détection/protection. La base de connaissances sur les évaluations regroupe les règles connues et les critères d'évaluation du niveau de sécurité des actifs TIC ainsi que la liste de contrôle de la configuration. La base des connaissances concernant la détection/protection rassemble les règles connues et les critères à appliquer pour détecter des menaces pour la sécurité et s'en protéger, par exemple les signatures IDS/IPS et les règles de détection/protection associées.

La base de connaissances sur les produits et services rassemble des informations sur les produits et services. Elle comprend deux bases de connaissances: connaissances des versions et connaissances des configurations. La base de connaissances des versions regroupe des informations sur les versions des produits et des services, y compris leur dénomination et la liste des versions. En ce qui concerne les versions des produits, les rectificatifs de sécurité sont également inclus dans cette base de connaissances. La base de connaissances des configurations rassemble des informations sur la configuration des produits et des services. En ce qui concerne les configurations des produits, elle inclut leur dénomination, la taxonomie et la liste des configurations connues.

Toutes les bases de données et les bases de connaissances mentionnées ci-dessus peuvent utiliser diverses techniques de description de l'information (voir la Figure II.2).



BD = base de données, BC = base de connaissances

X.1500(11)_FI-02

Figure II.2 – Vue détaillée du modèle d'ontologie CYBEX avec illustration des techniques

Pour un complément d'information sur l'ontologie CYBEX, voir la référence [b-Takahashi].

Appendice III

Exemples CYBEX de schémas d'automatisation de la sécurité

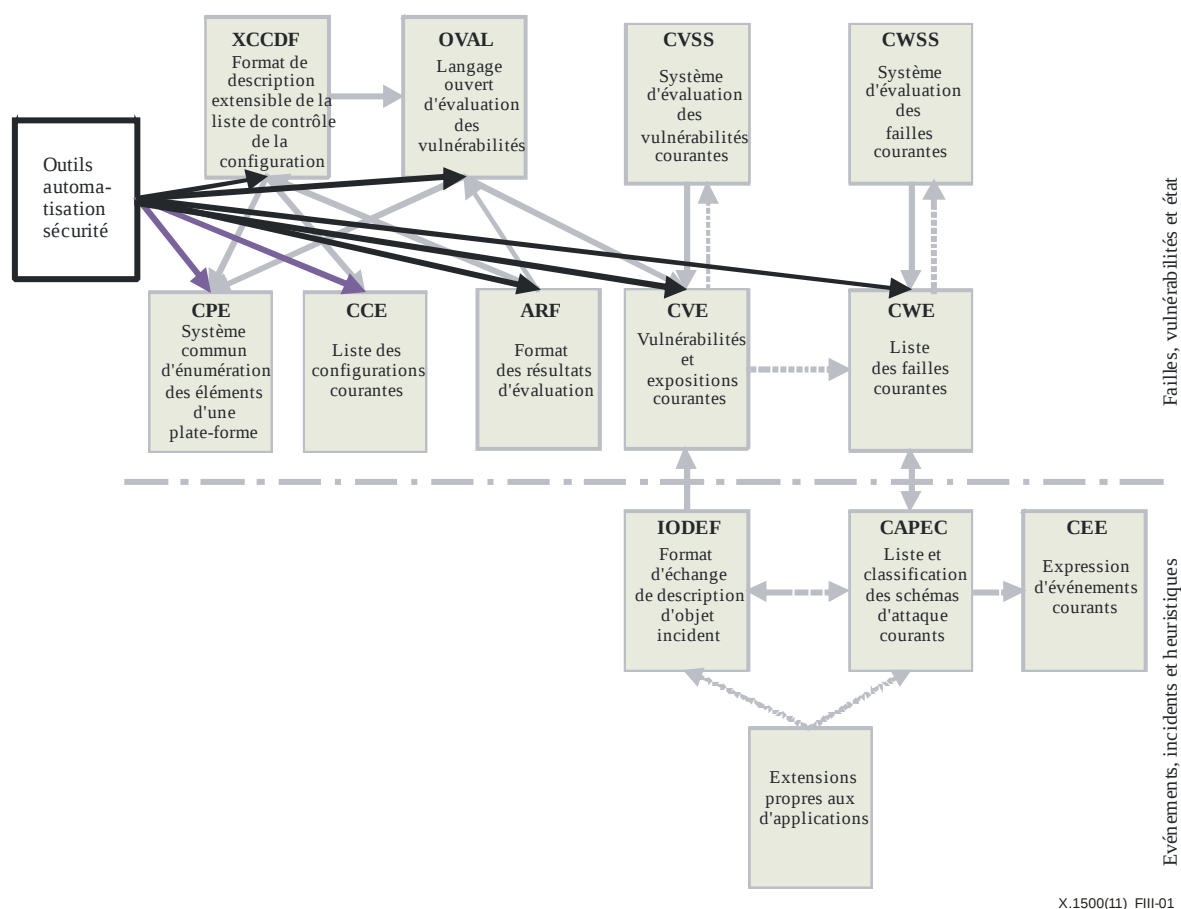
(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

L'Appendice III fournit deux exemples de schémas d'automatisation de sécurité. Ces capacités peuvent être utilisées pour créer des instanciations CYBEX spécifiques incluant l'automatisation d'états sécurisés connus et d'états de confiance, de services et de systèmes, la détection de logiciels malveillants, la capture d'informations sur des incidents et des heuristiques.

Il est vraisemblable qu'un grand nombre de mises en oeuvre verra le jour, en particulier un schéma d'automatisation de la sécurité permettant de veiller à ce que les systèmes TIC soient correctement configurés et corrigés. Les deux premiers grands exemples sont les suivants:

- 1) le protocole d'automatisation des contenus de sécurité (SCAP) mis au point par l'Institut national américain de la normalisation et de la technologie (NIST), pour mettre en oeuvre la configuration de base des postes de travail (FDCC) remplacé ensuite par la référence de configuration de l'Administration des Etats-Unis (USGCB); et
- 2) le cadre d'automatisation des contenus de sécurité JVN au Japon.

Ces deux exemples sont brièvement décrits dans le présent appendice. D'une manière générale, ces mises en oeuvre d'outils d'automatisation de la sécurité prennent la forme décrite dans la Figure III.1, et comprennent des nombres variables de plates-formes d'échange d'informations CYBEX représentées par les pointeurs qui parcourent le diagramme.



X.1500(11)_FIII-01

Figure III.1 – Automatisation de l'assurance et de l'intégrité de la cybersécurité

III.1 Exemple: Configuration de base des postes de travail au niveau fédéral aux Etats-Unis/base de référence de configuration de l'Administration américaine

La FDCC (configuration de base des postes de travail) à laquelle s'est substituée l'USGCB (base de référence de configuration de l'Administration américaine), utilisant le protocole SCAP (protocole d'automatisation des contenus de sécurité du NIST) comprend des spécifications pour l'organisation et l'expression d'informations liées à la sécurité de manière normalisée, ainsi que des données de référence associées comme des identificateurs non ambigus pour les vulnérabilités. Ces deux initiatives visent à créer des bases de référence de configurations de sécurité pour les produits TIC très utilisés par les agences fédérales. La base de référence USGCB est une évolution de la configuration de base des postes de travail. L'USGCB est une initiative menée à l'échelle de l'administration fédérale qui propose des directives aux agences sur ce qui devrait être fait pour améliorer et maintenir des paramètres de configuration effectifs axés pour l'essentiel sur la sécurité.

La spécification technique USGCB décrit les exigences et conventions à appliquer pour assurer des échanges cohérents et précis de contenus SCAP et permettre l'utilisation fiable du contenu sur des outils validés SCAP. La première version comprend six spécifications: XCCDF, OVAL, CPE, CCE, CVE et CVSS. Ces spécifications sont regroupées en trois catégories: langages, listes et système de mesure et de notation des vulnérabilités.

Le protocole SCAP met en oeuvre: 1) un format spécifié et une nomenclature permettant à des produits logiciels de sécurité de communiquer sans défaillance logicielle et de transmettre des informations sur des configurations de sécurité; et 2) des données de référence standard de configuration de sécurité et de défaillances de logiciel spécifiques connues sous l'appellation de contenu SCAP. Ce protocole vise à normaliser la gestion de la sécurité des systèmes, favoriser l'interopérabilité des produits de sécurité et encourager l'utilisation d'expressions standard de contenus de sécurité. Etant donné que de nombreux contenus SCAP différents devraient faire leur apparition pour différents systèmes et niveaux de sécurité, l'étiquetage structuré, la découverte et la vérification de l'assurance de schémas actuels sont des exigences importantes. L'initiative USGCB crée des contenus et des directives basés sur les spécifications SCAP.

III.2 Exemple: Portail japonais d'informations sur la vulnérabilité, JVN

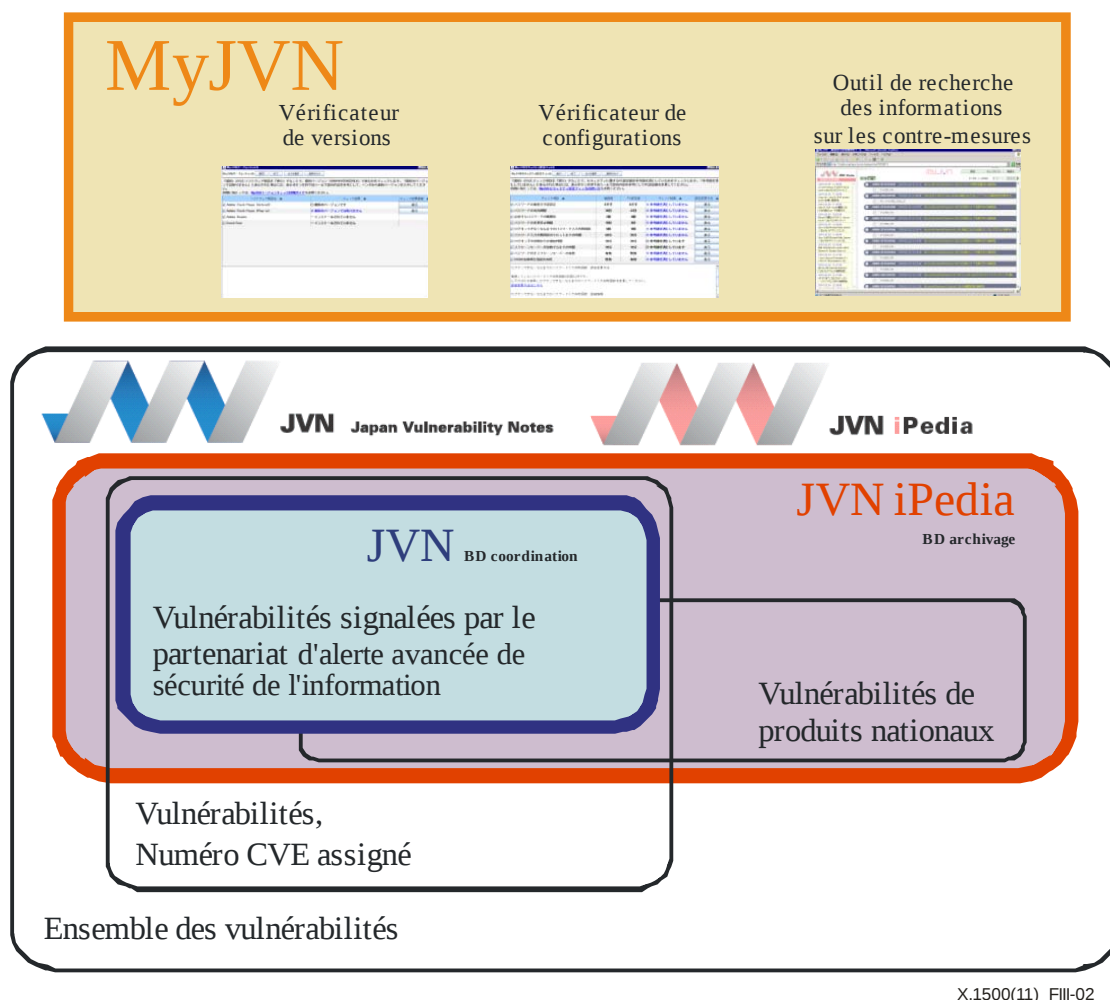
JVN est l'acronyme de "Japan Vulnerability Notes"; ce site donne des informations sur les vulnérabilités et les questions connexes concernant les logiciels utilisés au Japon; son rôle est de contribuer aux contre-mesures de lutte contre les cybermenaces. Pour permettre aux développeurs d'applications d'utiliser des données grâce à une interface ouverte, JVN a adopté le protocole SCAP et contient des informations locales (nationales) et internationales qui constituent le JVN Security Content Automation Framework (cadre d'automatisation de contenus de sécurité JVN). Tout comme la base de données nationale sur les vulnérabilités (NVD), toutes les informations sur les vulnérabilités sont associées à un numéro CVE, à une note CVSS et à un numéro CWS. De plus, le nom CPE du produit affecté est également fourni.

Ce cadre comprend les trois éléments suivants: MyJVN, JVN, et JVN iPedia (voir Figure III.2), qui sont décrit ci-après:

La base MyJVN fournit des informations sur les contre-mesures de vulnérabilité appliquées grâce à une interface API MyJVN, interface lisible par les ordinateurs incluant les interfaces API Web et les outils MyJVN comme le contrôleur de version. Il permet d'utiliser plus efficacement les informations sur les contre-mesures de vulnérabilité stockées dans les bases JVN et JVN iPedia en permettant aux utilisateurs de collecter plus facilement et efficacement les informations qui les intéressent grâce à des services comme le filtrage personnalisé, l'autorecherche et la création de listes de contrôle. Par ailleurs, la base "MyJVN Version Checker", qui est un outil fondé sur le protocole SCAP, permet aux utilisateurs de vérifier facilement si la version du logiciel installée sur leur ordinateur est la plus récente.

La base JVN fournit des informations sur les contre-mesures de vulnérabilités et sur la situation des éditeurs japonais quant aux vulnérabilités signalées par le "Information Security Early Warning Partnership", qui est un partenariat public-privé établi pour promouvoir la sécurité des produits logiciels et des sites web et empêcher que les dommages se propagent sur un grand nombre d'ordinateurs du fait de virus informatiques ou d'accès non autorisés. Lorsque les informations sur les vulnérabilités sont signalées à l'IPA (Information-technology Promotion Agency, Japon) qui est l'organisme hôte de ce partenariat, ces informations sont transmises au JPCERT/CC qui est l'organisme de coordination. Le JPCERT/CC précise les produits logiciels affectés et assure la coordination avec les développeurs. Lorsque des solutions aux vulnérabilités (correctifs ou mises à jour de logiciels) sont mises à la disposition des utilisateurs, des informations détaillées concernant les vulnérabilités avec les déclarations des développeurs sont publiées sur le site de JVN.

La base JVN iPedia donne des informations sur les contre-mesures de vulnérabilités rassemblées sur des produits logiciels, comme des systèmes d'exploitation, des applications, des bibliothèques et des systèmes intégrés, utilisés au Japon. Elle vise à donner des informations sur les vulnérabilités et les contre-mesures au public le plus rapidement possible. Un organisme de coordination travaille en collaboration avec les fabricants pour savoir quand divulguer les nouvelles vulnérabilités signalées. La mission JVN iPedia, quant à elle, a pour objectif de collecter des informations additionnelles sur les vulnérabilités et les contre-mesures trouvées quotidiennement sur des produits logiciels japonais qui ne sont pas publiées sur le site JVN.



X.1500(11)_FIII-02

Figure III.2 – Concept du cadre d'automatisation du contenu de sécurité JVN

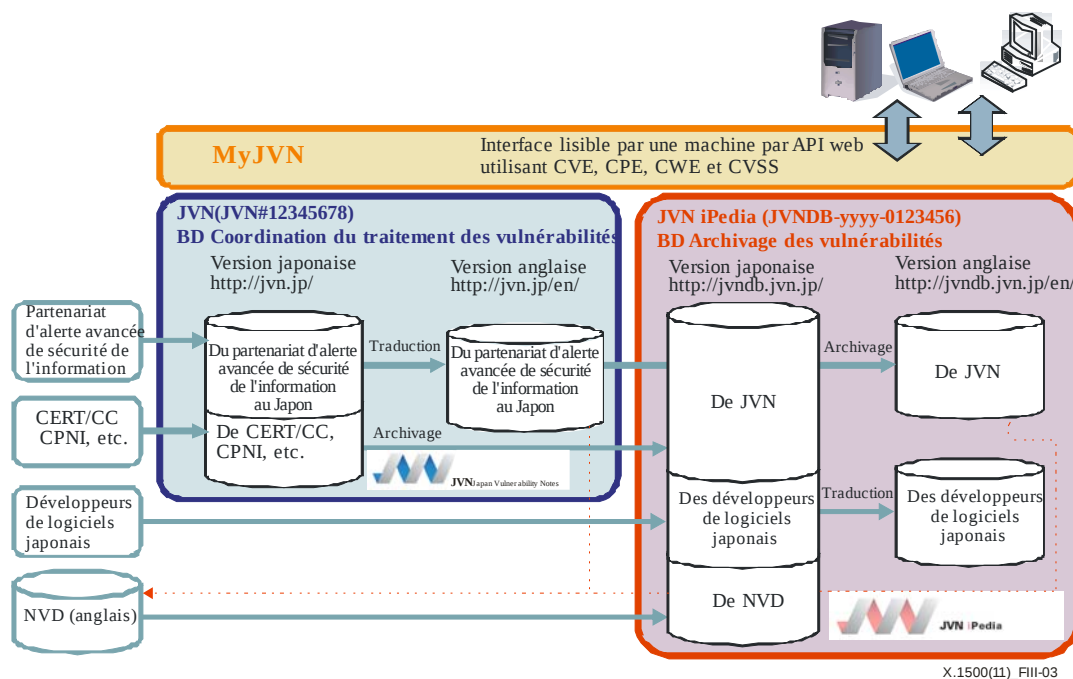


Figure III.3 – Base de données avec informations internationales et locales

Les utilisateurs adoptant des formats standard comme RSS peuvent bénéficier d'une base de données qui contient des informations internationales et locales (voir Figure III.3). Parmi les trois éléments, MyJVN fonctionne comme une interface utilisateur, qui peut être utilisée avec les outils et les API suivants.

Outils MyJVN et API

Les outils MyJVN sont des outils de sécurité basés sur le protocole SCAP, qui améliorent l'utilisation des contre-mesures de vulnérabilité et l'environnement d'échange d'informations pour les utilisateurs. Les principaux outils proposés actuellement sont les suivants:

- **Le Filtered Vulnerability Countermeasure Information Tool:** Cet outil améliore l'utilisation des informations sur les contre-mesures de vulnérabilités stockées dans les bases JVN et dans JVN iPedia en permettant aux utilisateurs de collecter plus facilement et avec davantage d'efficacité les informations visées grâce à des services comme le filtrage personnalisé par CPE.
- **Version Checker:** Version checker est un scanner en ligne basé sur OVAL qui permet aux utilisateurs de vérifier facilement si le logiciel installé sur leur ordinateur est la version la plus récente. Il suffit d'un clic de souris pour vérifier les versions de plusieurs modules logiciels. Les résultats sont faciles à comprendre: une case cochée signifie que la version la plus récente est présente tandis qu'une croix signifie la présence d'une version obsolète. Si la version du logiciel n'est pas la plus récente, les utilisateurs peuvent facilement accéder au site Internet de téléchargement de l'éditeur en quelques clics. MyJVN Version Checker est compatible avec des produits logiciels liés à Internet qui ont été sélectionnés lors de la recherche de coopération avec les éditeurs de logiciels.
- **MyJVN Security Configuration Checker:** Cet outil est un scanner en ligne basé sur XCCDF et OVAL. Il s'agit d'un outil gratuit et facile à utiliser permettant d'évaluer la configuration de sécurité de Windows, y compris les politiques de comptes comme la longueur minimale des mots de passe, leur date d'expiration, l'activation automatique de l'économiseur d'écran, la caractéristique d'autoexécution USB, etc.
- **MyJVN API:** Il s'agit d'une interface logicielle permettant d'accéder à des informations de contre-mesures de vulnérabilités stockées dans les bases JVN et JVN iPedia et de les

utiliser. Pour permettre aux développeurs d'applications d'utiliser des données via une interface ouverte, JVN iPedia a adopté le protocole SCAP qui est un ensemble de normes utilisées pour décrire les informations de contre-mesures de vulnérabilités. Grâce à l'utilisation de l'interface API MyJVN, toute application personnalisée peut accéder aux données contenues dans la base JVN iPedia et divers services de gestion des vulnérabilités peuvent maintenant utiliser avec efficacité les informations de contre-mesures de vulnérabilités.

L'interface API MyJVN offre les fonctions de base suivantes: interface API de service de filtrage d'information et interface API de service de collaboration SCAP. La première interface API prend en charge les fonctions "Get list of products", "Get list of vulnerability overviews", etc., qui sont utilisées par l'outil de filtrage de l'information sur les contre-mesures, tandis que la deuxième prend en charge les fonctions "Get list of OVAL definitions", "Get data of OVAL definition", etc., qui sont utilisées par MyJVN Version Checker et par MyJVN Security Configuration Checker.

Pour tout complément d'information sur JVN, se référer à l'Article [b-Terada].

Bibliographie

- [b-ITU-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication.*
- [b-ITU-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*
- [b-ITU-T X.1205] Recommandation UIT-T X.1205 (2008), *Aperçu général de la cybersécurité.*
- [b-ITU-T X.1520] Recommandation UIT-T X.1520 (2011), *Vulnérabilités et expositions courantes (CVE).*
- [b-ITU-T X.1521] Recommandation UIT-T X.1521 (2011), *Système d'évaluation des vulnérabilités courantes (CVSS).*
- [b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.*
- [b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core.* <http://datatracker.ietf.org/doc/rfc3080/>
- [b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format.* <http://datatracker.ietf.org/doc/rfc5070/>
- [b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing.* <http://datatracker.ietf.org/doc/rfc5901/>
- [b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID).* <http://datatracker.ietf.org/doc/rfc6045/>
- [b-IETF RFC 6046] IETF RFC 6046 (2010), *Transport of Real-time Inter-network Defense (RID) Messages.* <http://datatracker.ietf.org/doc/rfc6046/>
- [b-ARF] Assessment Results Format. <https://measurablesecurity.mitre.org/incubator/arf/>
- [b-CAPEC] Common Attack Pattern Enumeration and Classification. <https://capec.mitre.org/>
- [b-CCE] Common Configuration Enumeration. <https://cce.mitre.org/>
- [b-CEE] Common Event Expression. <https://cee.mitre.org/>
- [b-CPE] Common Platform Enumeration. <https://cpe.mitre.org/>
- [b-CWE] Common Weakness Enumeration. <https://cwe.mitre.org/>
- [b-CWSS] Common Weakness Scoring System. <https://cwe.mitre.org/cwss/>
- [b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3
- [b-MAEC] Malware Attribute Enumeration and Characterization. <https://maec.mitre.org/>
- [b-NIST EAA] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006
- [b-OVAL] Open Vulnerability and Assessment Language. <https://oval.mitre.org/>

- [b-Takahashi] Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.
- [b-Terada] Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June.
http://jvnrss.ise.chuo-u.ac.jp/itg/doc/21thFirstConference_paper.pdf
- [b-TLP] *CPNI Traffic Light Protocol* (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.
- [b-TNC] Trusted Computing Group, *Trusted Network Connect*.
 Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)
 Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)
 Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010)
 Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008)
 Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007)
 Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010)
 Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006)
 Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009)
- [b-TPM] Trusted Computing Group, *Trusted Platform Modules*.
 Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2)
 TPM Structures – TCG Version (TPM Main, Part 2, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3)
 Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4)
 The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1)
- [b-W3C SOAP] W3C Recommendation Simple Object Access Protocol (SOAP), 2007.
SOAP Version 1.2 Part 1: Messaging Framework.
SOAP Version 1.2 Part 2: Adjuncts.
- [b-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