Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1217

(01/2021)

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

Sécurité du cyberespace – Cybersécurité

Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

Recommandation UIT-T X.1217

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1217

Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

Résumé

Du point de vue d'un opérateur de télécommunication, les renseignements sur les menaces constituent un ensemble d'informations organisées, analysées et affinées sur les attaques potentielles et actuelles qui peuvent menacer une organisation. Ces informations peuvent également comprendre les motivations, les intentions, les caractéristiques et les méthodes des auteurs d'attaques, ainsi que leur mode opératoire ou leurs techniques, leurs tactiques et leurs procédures.

En ce qui concerne la sécurité des réseaux et de l'information, la survenue d'incidents de cybersécurité inattendus et à grande échelle a rendu urgente la nécessité de disposer de renseignements sur les menaces. Ces renseignements peuvent aider une organisation à réduire les risques et à améliorer sa sécurité globale. Une taxonomie, une grammaire et une présentation unifiées des renseignements sur les menaces ont été définies afin que différentes organisations puissent échanger ces renseignements.

La Recommandation UIT-T X.1217 contient des lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication après une analyse d'ensemble.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1217	07-01-2021	17	11.1002/1000/14443

Mots clés

Sécurité, renseignements sur les menaces.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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 on 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

Table des matières

Introduction

Du point de vue d'un opérateur de télécommunication, les renseignements sur les menaces constituent un ensemble d'informations organisées, analysées et affinées sur les attaques potentielles et actuelles qui peuvent menacer une organisation. Ces informations peuvent également comprendre les motivations, les intentions, les caractéristiques et les méthodes des auteurs d'attaques, ainsi que leur mode opératoire ou leurs techniques, leurs tactiques et leurs procédures.

En ce qui concerne la sécurité des réseaux et de l'information, la survenue d'incidents de cybersécurité inattendus et à grande échelle a rendu urgente la nécessité de disposer de renseignements sur les menaces. Ces renseignements peuvent aider une organisation à réduire les risques et à améliorer sa sécurité globale en ce qu'ils permettent de comprendre quelles entités sont le plus susceptibles d'être à l'origine d'une attaque, quels sont leur cible, leurs objectifs et leurs motivations et de quelle manière elles comptent s'y prendre.

La norme [OASIS STIXv2] définit un langage et un format de sérialisation à utiliser pour l'échange de renseignements sur les cybermenaces. La norme [OASIS TAXIIv2] définit pour sa part un protocole à utiliser pour l'échange de renseignements sur les cybermenaces grâce au protocole de transfert hypertexte sécurisé (HTTPS). Quant à la Recommandation [UIT-T X.1215], elle indique de quelle façon le langage STIX (expression structurée d'informations sur les menaces) peut être utilisé pour favoriser les échanges de renseignements et d'informations sur les cybermenaces.

Une taxonomie, une grammaire et une présentation unifiées des renseignements sur les menaces ont été définies afin que différentes organisations puissent échanger ces renseignements. Il faut maintenant réfléchir à comment utiliser ces renseignements pour résoudre les problèmes liés à la sécurité des réseaux.

La norme [OASIS OpenC2-L] définit un langage de commande et de contrôle (C2) à utiliser pour le contrôle des fonctions de cybersécurité. La norme [OASIS OpenC2-H] définit quant à elle une interface de programmation d'applications (API) fondée sur le protocole HTTPS pour le transfert de commandes de type OpenC2 aux dispositifs de cybersécurité. La norme [OASIS OpenC2-P] définit pour sa part l'utilisation du langage OpenC2 à des fins de contrôle des pare-feu sans état. L'organisation OASIS s'emploie actuellement à élaborer des profils pour d'autres fonctions de cybersécurité.

La présente Recommandation contient des lignes directrices relatives à l'utilisation de renseignements sur les menaces après une analyse d'ensemble.

Recommandation UIT-T X.1217

Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

1 Domaine d'application

La présente Recommandation propose des lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication après une analyse d'ensemble.

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 de Recommandation.

[UIT-T X.1215] Recommandation UIT-T X.1215 (2019), *Cas d'utilisation pour l'expression structurée d'informations sur les menaces*.

[OASIS OpenC2-H] Spécification OASIS pour le transfert de messages OpenC2 via le protocole HTTPS, version 1.0.
<https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html

[OASIS OpenC2-L] Spécification OASIS sur le langage Open Command and Control (OpenC2), version 1.0.
<https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] Profil Open Command and Control (OpenC2) d'OASIS pour le filtrage des paquets sans état, version 1.0.
<https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

[OASIS STIXv2] Spécifications OASIS STIX 2.1.
<https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

[OASIS TAXIIv2] Spécifications OASIS TAXII 2.1.
<https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html>

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 botnet [b-UIT-T X.1231]: robots logiciels malveillants (bots) commandés à distance, qui sont exécutés de manière autonome ou automatique sur des ordinateurs contaminés, en association avec un serveur de commande et de contrôle appartenant à des botmasters.

3.1.2 fraude [b-UIT-T Y.140.1]: fait d'obtenir un avantage financier par le biais d'une fausse représentation ou d'une action non autorisée.

3.1.3 logiciel malveillant [b-UIT-T X.1211]: logiciel conçu expressément pour endommager ou perturber un système, et nuire à la confidentialité, à l'intégrité et/ou à la disponibilité.

3.1.4 hameçonnage, phishing [b-UIT-T X.1244]: tentative d'obtention illicite et frauduleuse d'informations sensibles (nom d'utilisateur, mot de passe, données de compte bancaire, etc.) en se faisant passer pour une entité digne de confiance dans une communication électronique.

3.1.5 vulnérabilité [b-UIT-T X.1524]: toute faille dans le logiciel qui peut être exploitée pour violer un système ou les informations qu'il contient.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 nettoyage des données: processus consistant à supprimer les données sans intérêt et les données faisant double emploi dans le jeu de données initial, afin de lisser les données bruitées et de traiter les valeurs manquantes et les valeurs aberrantes.

3.2.2 élagage de données: processus consistant à élaguer les données inutiles ou anormales.

3.2.3 élimination des données faisant double emploi: processus consistant à éliminer les données faisant double emploi dans le jeu de données initial.

3.2.4 désensibilisation des données: processus consistant à dissimuler les données sensibles.

3.2.5 filtrage des données: processus consistant à supprimer les données sans intérêt et à filtrer les données n'ayant pas leur place dans le jeu de données initial.

3.2.6 mise en correspondance des données: processus consistant à mettre en correspondance les éléments de données du système de données source avec ceux du système de données de destination.

3.2.7 fusion des données: processus consistant à fusionner les données similaires en une seule entrée.

3.2.8 exploration des données: processus informatique consistant à déceler les caractéristiques de grands jeux de données grâce à des méthodes telles que l'intelligence artificielle, l'apprentissage automatique, les statistiques et les systèmes de bases de données.

3.2.9 réduction du bruit dans les données: processus consistant à lisser les données bruitées.

3.2.10 échantillonnage des données: technique statistique utilisée pour traiter les valeurs manquantes et les valeurs aberrantes.

3.2.11 segmentation des données: processus consistant à segmenter des données de différents niveaux.

3.2.12 tri des données: processus consistant à trier des données dans un certain ordre ou par catégorie.

3.2.13 transformation des données: processus consistant à exprimer des données dans un certain format et à transposer les données à une échelle donnée.

3.2.14 collecte d'informations relatives aux incidents: processus consistant à collecter des données sur les incidents liés à la sécurité.

3.2.15 appréciation de la situation: processus consistant à présenter la situation globale et à prévoir les éventuelles menaces et attaques.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'applications (*application programming interface*)

C&C commande et contrôle (*command and control*)

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

DDoS déni de service réparti (*distributed denial of service*)

DNS système de noms de domaine (*domain name system*)

FW pare-feu (*firewall*)

GW passerelle (*gateway*)

HTTPS protocole de transfert hypertexte sécurisé (*hypertext transfer protocol secure*)

ID identité (*identity*)

IDS système de détection des intrusions (*intrusion detection system*)

IP protocole Internet (*internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

MD5 algorithme 5 de condensé de message (*message digest algorithm 5*)

O&M exploitation et maintenance (*operations and maintenance*)

SDN réseau piloté par logiciel (*software defined network*)

SIEM gestion des informations et des événements de sécurité (*security information and event management*)

SoC centre des opérations de sécurité (*security operation centre*)

STIX expression structurée d'informations sur les menaces (*structured threat information expression*)

TAXII échange sécurisé et automatisé de renseignements (*trusted automated exchange of intelligence information*)

URL localisateur uniforme de ressources (*uniform resource locator*)

WAF application web de pare-feu (*web application firewall*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

6 Aperçu général des renseignements sur les menaces

Du point de vue d'un opérateur de télécommunication, les renseignements sur les menaces constituent un ensemble d'informations organisées, analysées et affinées sur les attaques potentielles et actuelles qui peuvent menacer une organisation. Ces informations peuvent également comprendre les motivations, les intentions, les caractéristiques et les méthodes des auteurs d'attaques, ainsi que leur mode opératoire ou leurs techniques, leurs tactiques et leurs procédures.

Pour ce qui est de l'exploitation des réseaux de télécommunication, les renseignements sur les menaces fournissent des connaissances utilisées pour prévenir les cyberattaques ou atténuer leurs effets et comprennent notamment les motivations, les intentions, les caractéristiques, les méthodes, les modes opératoires, les techniques, les tactiques et les procédures des auteurs d'attaques. Ces renseignements n'ont aucun lien avec les informations d'identification personnelle.

En ce qui concerne la sécurité des réseaux et de l'information, la survenue d'incidents de cybersécurité inattendus et à grande échelle a rendu urgente la nécessité de disposer de renseignements sur les menaces. Ces renseignements peuvent aider une organisation à réduire les risques et à améliorer sa sécurité globale en ce qu'ils permettent de comprendre quelles entités sont le plus susceptibles d'être à l'origine d'une attaque, quels sont leur cible, leurs objectifs et leurs motivations et de quelle manière elles comptent s'y prendre.

La norme [OASIS STIXv2] définit un langage et un format de sérialisation à utiliser pour l'échange de renseignements sur les cybermenaces. La norme [OASIS TAXIIv2] définit pour sa part un protocole à utiliser pour l'échange de renseignements sur les cybermenaces grâce au protocole de transfert hypertexte sécurisé (HTTPS). Quant à la Recommandation [UIT-T X.1215], elle indique de quelle façon le langage STIX (expression structurée d'informations sur les menaces) peut être utilisé pour favoriser les échanges de renseignements et d'informations sur les cybermenaces.

Une taxonomie, une grammaire et une présentation unifiées des renseignements sur les menaces ont été définies afin que différentes organisations puissent échanger ces renseignements. Il faut maintenant réfléchir à comment utiliser ces renseignements pour résoudre les problèmes liés à la sécurité des réseaux.

La norme [OASIS OpenC2-L] définit un langage de commande et de contrôle (C2) à utiliser pour le contrôle des fonctions de cybersécurité. La norme [OASIS OpenC2-H] définit quant à elle une interface de programmation d'applications (API) fondée sur le protocole HTTPS pour le transfert de commandes de type OpenC2 aux dispositifs de cybersécurité. La norme [OASIS OpenC2-P] définit pour sa part l'utilisation du langage OpenC2 à des fins de contrôle des pare-feu sans état. L'organisation OASIS s'emploie actuellement à élaborer des profils pour d'autres fonctions de cybersécurité.

7 Aperçu général de l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

La Figure 7-1 montre comment des renseignements sur les menaces sont utilisés dans le cadre de l'exploitation des réseaux de télécommunication.

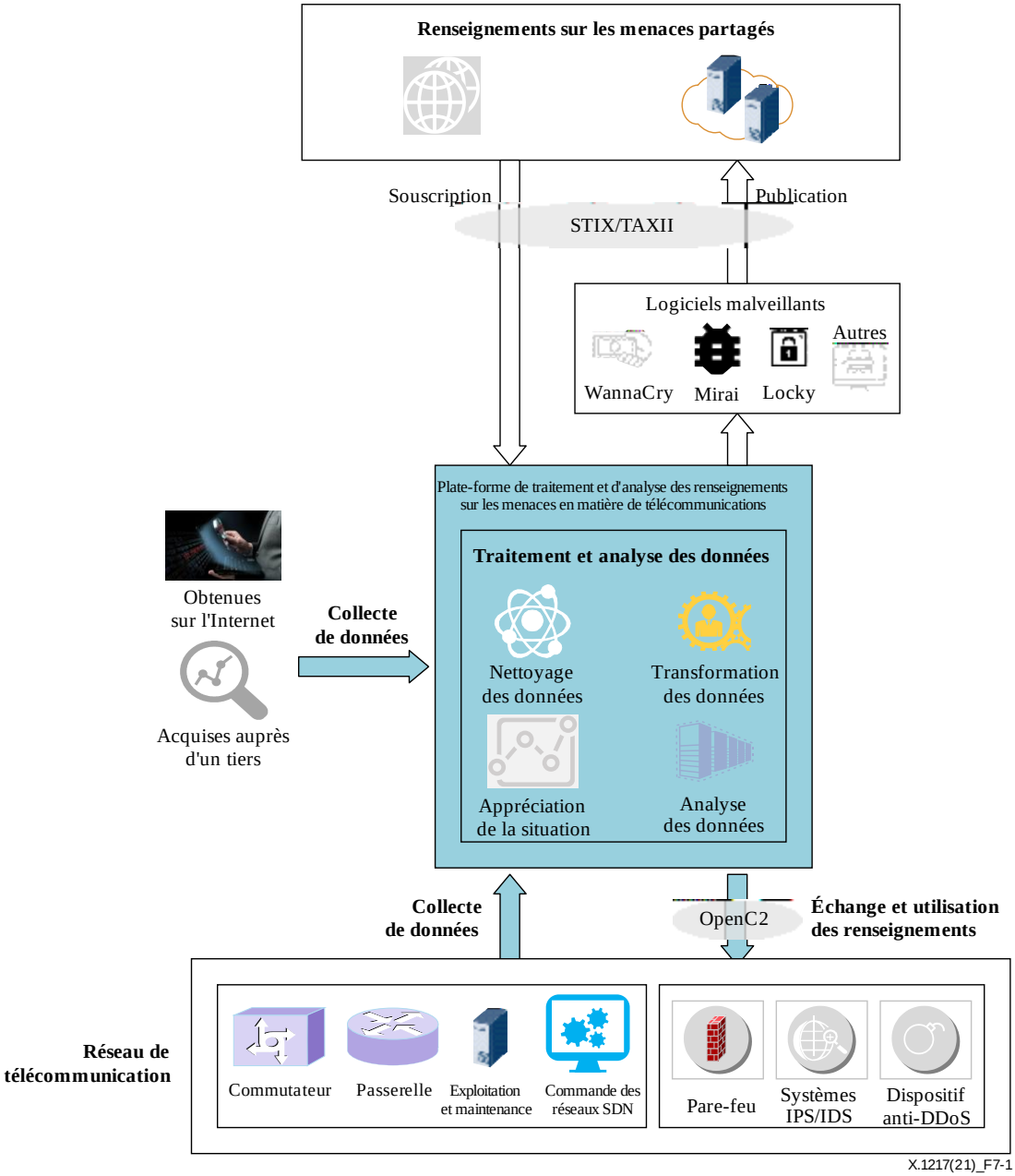

Figure 7-1 – Utilisation des renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

Selon la Figure 7-1, l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication repose sur trois grands processus: la collecte de données, le traitement et l'analyse de données et l'échange et l'utilisation des renseignements.

7.1 Collecte des données

En matière de renseignements sur les menaces, on distingue deux sortes de sources de données:

– les données provenant d'éléments de réseau et de dispositifs de sécurité internes;

– les données provenant de sources externes.

Les données provenant d'éléments de réseau et de dispositifs de sécurité internes comprennent essentiellement les différents journaux, les alertes et les politiques de sécurité, comme les journaux d'incidents, les journaux des systèmes de noms de domaine (DNS), les journaux des pare-feu, etc.

Il est possible de collecter des données auprès de certaines sources externes, par exemple en effectuant des recherches sur l'Internet, en les acquérant auprès de tiers via STIX/TAXII, etc. Les données partagées concernent principalement des adresses IP, des domaines, des URL, des incidents, des vulnérabilités, etc.

Il est obligatoire de procéder à une désensibilisation des données préalablement à la collecte.

7.2 Traitement et analyse des données

Le traitement et l'analyse des données s'articulent autour de quatre composantes fonctionnelles: le nettoyage des données, la transformation des données, l'analyse des données et l'appréciation de la situation.

La Figure 7-2 illustre les composantes fonctionnelles du traitement et de l'analyse des données.

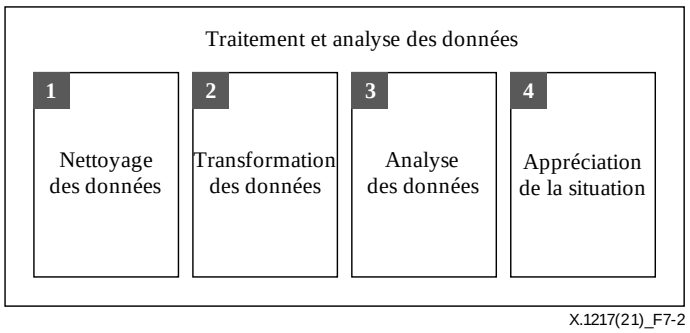

Figure 7-2 – Composantes fonctionnelles du traitement et de l'analyse des données

– Le nettoyage des données consiste à supprimer les données sans intérêt et les données faisant double emploi dans le jeu de données initial, à lisser les données bruitées et à traiter les valeurs manquantes et les valeurs aberrantes.

– La transformation des données comprend l'intégration des données et la normalisation des données:

  • L'intégration des données consiste à utiliser un format donné pour stocker toutes les données provenant de sources multiples.

  • La normalisation des données consiste à supprimer l'influence exercée par l'étendue et l'amplitude des valeurs de tel ou tel indicateur et à transposer les données à une échelle donnée, notamment pour ce qui est de la transformation des fonctions et de la construction d'attributs, etc.

– L'analyse des données utilise divers algorithmes pour analyser les données, en extraire des mots clés et des règles précises, établir des corrélations afin d'obtenir des renseignements sur les menaces et analyser les contre-mesures qu'il convient de prendre.

– L'appréciation de la situation comprend la visualisation et l'alerte prévisionnelle:

  • La visualisation désigne la présentation visuelle de la situation globale grâce aux données analysées, notamment au moyen d'une catégorisation, d'un tri, etc.

  • L'alerte prévisionnelle fait référence au fait de prévoir la diversité des menaces et des parcours et méthodes d'attaque, etc. qui peuvent être utilisés grâce à l'analyse des données et à la situation globale et de diffuser des alertes précoces pour proposer des stratégies de sécurité et se défendre contre d'éventuelles attaques.

7.3 Échange et utilisation des renseignements

L'échange et l'utilisation des renseignements comprennent deux volets:

- En fonction des renseignements sur les menaces, les administrateurs de l'exploitation et de la maintenance peuvent appliquer des politiques de sécurité aux éléments de réseau et aux dispositifs de sécurité.
- Les renseignements sur les menaces peuvent être échangés avec des tiers.

Les renseignements sur les menaces susceptibles d'être échangés et utilisés dans le cadre de l'exploitation des réseaux de télécommunication comprennent des informations sur ces menaces, des informations d'alerte prévisionnelle, des contre-mesures relatives à la sécurité des réseaux, etc.

Les objets de l'échange et de l'utilisation des renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication comprennent les éléments de réseau et les dispositifs de sécurité comme les systèmes de détection des intrusions (IDS) et de prévention des intrusions (IPS), les pare-feu et les dispositifs anti-DDoS. Pour ce qui est de l'application des fonctions de commande et de contrôle liées à la sécurité aux dispositifs de sécurité, il est recommandé d'utiliser les spécifications OpenC2 d'OASIS.

L'échange et l'utilisation des renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication vise à prévenir et limiter les incidents liés à la sécurité tout en intervenant rapidement et efficacement chaque fois qu'un incident lié à la sécurité survient dans un réseau de télécommunication.

8 Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication

Le paragraphe 7 comporte une description des trois grands processus permettant d'utiliser des renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication, à savoir la collecte de données, le traitement et l'analyse de données ainsi que l'échange et l'utilisation des renseignements. Les paragraphes 8.1 à 8.3 énoncent des lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication.

8.1 Collecte des données

La collecte des données est une condition préalable à l'utilisation de renseignements sur les menaces et consiste à collecter toutes les informations et données susceptibles de donner des renseignements sur les menaces. Il est recommandé de faire figurer dans ces données notamment des données tirées d'éléments de réseau et de dispositifs de sécurité internes, par exemple les journaux, alertes et politiques de sécurité, ainsi que des données tirées de sources externes, par exemple des données obtenues dans le cadre de recherches sur l'Internet, des données acquises auprès de tiers, etc. Les données échangées concernent principalement des adresses IP, des domaines, des URL, des incidents, des vulnérabilités, etc.

Il est recommandé de collecter activement des données notamment en ce qui concerne les journaux des systèmes DNS et des pare-feu, etc. Il est recommandé de collecter des données sur les incidents liés à la sécurité. Il est recommandé de collecter des renseignements essentiels, notamment en ce qui concerne les adresses IP, les domaines, les URL, les incidents, les vulnérabilités, etc.

Si les données sont tirées d'éléments de réseau et de dispositifs de sécurité internes, il est possible de les collecter en fonction de leur type (informations sur les incidents ou activité des botnets, par exemple).

Les informations sur les incidents peuvent être tirées d'un dispositif IDS, d'un dispositif IPS, d'une application web de pare-feu (WAF), d'un dispositif anti-DDoS, d'une plate-forme SIEM (gestion des informations et des événements de sécurité) ou d'une plate-forme SoC (centre des opérations de sécurité). Il est recommandé de faire figurer dans les informations ainsi collectées le nom, une description et la catégorie de l'incident ainsi que les ressources concernées. Il est en outre recommandé de mentionner l'heure de l'incident. Des informations sur l'activité des botnets peuvent

être tirées de dispositifs DNS et IDS, de pare-feu WAF, de dispositifs anti-DDoS, etc. Il est recommandé de faire figurer dans les informations ainsi collectées le nom, une description et la catégorie d'activité du botnet ainsi que les ressources concernées. Il est également recommandé de mentionner l'heure de l'activité du botnet.

Si les données sont tirées de l'Internet, il est possible de les collecter en fonction de leur type (informations sur les vulnérabilités, domaines malveillants, URL malveillants, adresses IP malveillantes, informations sur les incidents, etc.).

Les informations sur les vulnérabilités peuvent être tirées de sites web traitant des vulnérabilités, comme les sites web consacrés aux vulnérabilités et expositions courantes (CVE). Il est recommandé de faire figurer dans les informations ainsi collectées l'identité de la vulnérabilité, son nom, une description et son type, ainsi que les versions, les vendeurs et les produits concernés par la vulnérabilité, etc.

Les informations sur les domaines et URL malveillants peuvent être classées en différentes catégories de menaces (commande et contrôle, botnet, logiciel malveillant, code correspondant à un cheval de Troie, hameçonnage, fraude, etc.). Ces informations peuvent être tirées de sites web, de rapports de vendeurs, de rapports de sécurité élaborés par des tiers, etc. Il est recommandé de faire figurer dans les informations ainsi collectées le serveur de noms de domaine, le type de système DNS, le type de menace, le niveau de crédibilité, etc.

Les informations sur les adresses IP malveillantes peuvent être obtenues auprès de divers sites web, vendeurs et entreprises de sécurité, etc. Ces informations peuvent être classées en différentes catégories de menaces (déni DDoS, exploitations, source de spam, attaque web, botnet, logiciel malveillant, commande et contrôle, etc.). Il est recommandé de faire figurer dans les informations ainsi collectées l'adresse IP, le type de menace, le niveau de crédibilité, etc.

Les informations sur les incidents peuvent être tirées d'actualités en matière de sécurité et de rapports de vendeurs. Il est recommandé de faire figurer dans ces informations le nom, la description et la catégorie de l'incident ainsi que les ressources concernées.

Les données acquises auprès de tiers portent essentiellement sur les adresses IP, les noms de domaine, les URL, les incidents, les vulnérabilités, etc. Pour chacune de ces catégories, les informations sont identiques à celles décrites ci-dessus.

Il est recommandé d'utiliser des outils automatiques ou des scripts pour tirer des données d'éléments de réseau et de dispositifs de sécurité internes. Il est recommandé d'utiliser des scripts ou des mécanismes d'échange et de partage de données pour tirer des données de sources externes. Ensuite, pour le traitement des données ainsi collectées, il est recommandé d'adopter le format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2]. Pour ce qui est de l'échange de renseignements sur les menaces, il est recommandé, pour la collecte des données, d'adopter le format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2].

Il est recommandé de désensibiliser les données, c'est-à-dire de dissimuler les données initiales sensibles à l'aide de caractères ou de données afin de les protéger, préalablement à la collecte.

8.2 Traitement et analyse des données

8.2.1 Nettoyage des données

Le nettoyage des données est une étape essentielle dans l'utilisation des renseignements sur les menaces et vise à nettoyer les données collectées pour les uniformiser, les rendre utilisables et les préparer aux étapes de la transformation et de l'analyse.

– Il est recommandé de procéder à un filtrage des données, à la réduction du bruit dans les données et à l'élimination des données faisant double emploi.

– Il est recommandé de procéder à un filtrage des données, c'est-à-dire de supprimer les données sans intérêt et de filtrer les données n'ayant pas leur place dans le jeu de données initial.
– Il est recommandé de procéder à une réduction du bruit dans les données et à l'élimination des données faisant double emploi pour lisser les données bruitées et supprimer les doublons dans le jeu de données initial.

Étant donné que différents types de données sont collectées (adresses IP, domaines, URL, incidents, vulnérabilités, etc.), le nettoyage des données peut prendre différentes formes en fonction du type de données collectées.

L'élimination des données faisant double emploi consiste principalement à supprimer les doublons pour économiser de l'espace de stockage. Les critères retenus diffèrent selon le type de données. Pour ce qui est des informations sur les adresses IP, s'il y a identité de l'adresse IP et d'autres éléments de l'entrée comme le type de menace ou le niveau de crédibilité, alors ces données font double emploi et les doublons doivent être éliminés; dans le cas contraire, les données doivent être fusionnées. Pour ce qui est des informations sur le domaine, s'il y a identité de toutes les entrées concernant le serveur de noms de domaine, le type de système DNS, le type de menace et le niveau de crédibilité, alors ces données font double emploi et les doublons doivent être éliminés; dans le cas contraire, les données doivent être fusionnées. Pour ce qui est des informations sur la vulnérabilité, si l'identité de la vulnérabilité est la même, alors ces données font double emploi et les doublons doivent être éliminés. Pour les autres types de données, il est recommandé de calculer le taux de similarité. Si celui-ci est supérieur au seuil fixé, alors les doublons doivent être éliminés.

Il est recommandé de fusionner les informations similaires en une seule entrée. Pour ce qui est des informations sur les adresses IP, le domaine, l'URL et les informations sur les incidents, s'il y a identité des adresses IP, du serveur de noms de domaine, de l'URL et de la description de l'incident, alors ces données peuvent être fusionnées. Pour les autres types de données, le taux de similarité peut être calculé. Si celui-ci est supérieur au seuil fixé, alors les informations doivent être fusionnées.

– Il est recommandé de procéder à l'échantillonnage, à la fusion et au tri des données, afin de traiter les valeurs manquantes et les valeurs aberrantes et d'accroître l'utilité des données en vue de leur tri.
– Il est recommandé d'utiliser des outils automatiques pour filtrer les données et éliminer celles faisant double emploi.

8.2.2 Transformation des données

La transformation des données vise à supprimer l'influence exercée par l'étendue et l'amplitude des valeurs de tel ou tel indicateur et à transposer les données à une échelle donnée, notamment pour ce qui est de la transformation des fonctions et de la construction d'attributs, etc., et à exprimer les données nettoyées dans un format unifié en vue de leur analyse.

Pour procéder à la transformation des données, il est recommandé de les mettre en correspondance, de les élaguer et de les segmenter afin d'obtenir des données ayant une valeur utile. Lorsque la graphie diffère, il est recommandé de la modifier pour obtenir une graphie unifiée. Il est recommandé d'uniformiser le format des données tirées de sources multiples pour les exprimer dans un même format. Il est recommandé de faire converger les données provenant de sources multiples pour les stocker de manière uniforme.

Les procédures de transformation sont similaires pour tous les types de données (adresses IP, domaine, URL et vulnérabilité face aux incidents). Il est recommandé de suivre des règles de mise en correspondance pour tous les types de données, lesquelles peuvent varier selon le type de données. Par exemple, la règle applicable aux informations sur les incidents consiste à utiliser un format standard pour les champs du nom, de la description, de la catégorie et des ressources concernées. Il

est recommandé de transposer dans le format défini les informations sur les pare-feu telles que l'horodate de la carte, l'URL de requête, le nom de l'hôte, le type d'attaque et le contenu de l'attaque.

Pour ce qui est de l'élagage et de la segmentation des données, il est recommandé de transformer les données à l'aide d'outils automatiques. Concernant la modification de la graphie, il est recommandé de transformer les données à l'aide d'outils automatiques. Pour ce qui est de l'uniformisation du format, il est recommandé, pour la transformation des données, d'adopter le format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2].

8.2.3 Analyse des données

L'analyse des données est l'étape décisive dans l'utilisation de renseignements sur les menaces et consiste à utiliser divers algorithmes pour analyser les données transformées, en extraire des mots clés et des règles précises, établir des corrélations, etc., afin d'obtenir des renseignements sur les menaces et analyser les contre-mesures qu'il convient de prendre.

Pour analyser les données, il est recommandé de procéder à la récupération et à l'exploration des données pour obtenir des renseignements essentiels sur les menaces et ainsi créer des alertes ou déterminer les contre-mesures qu'il convient de prendre. Il est recommandé de conduire une analyse du comportement et une analyse de la corrélation des incidents afin d'identifier les renseignements sur les menaces qui ont une utilité, comme les adresses IP, les noms de domaine, le condensé de hachage, les informations sur l'auteur de l'attaque, les mesures à prendre, etc. Il est recommandé de recouper les informations et de rechercher activement les menaces pour obtenir des renseignements sous-jacents sur les menaces, prendre des contre-mesures et intervenir.

Par exemple, l'algorithme d'apprentissage automatique utilisé pour les journaux des systèmes DNS peut être utilisé pour déceler les fonctions de commande et de contrôle des botnets. Il est recommandé d'utiliser conjointement les journaux de pare-feu ainsi que la source et le type de la menace et l'heure de l'attaque, entre autres informations, pour calculer le niveau de menace. Les informations sur l'URL et les adresses IP peuvent être utilisées pour calculer le niveau de réputation.

Il est recommandé d'utiliser systématiquement des algorithmes d'analyse des données. Il est recommandé d'exprimer les résultats de l'analyse des données au format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2].

8.2.4 Appréciation de la situation

L'appréciation de la situation consiste à utiliser les données issues de l'analyse pour prévoir les tendances et envoyer des alertes tout en ayant une vision d'ensemble de la situation.

Pour apprécier la situation, il est recommandé de la visualiser dans sa globalité à l'aide des données issues de l'analyse. Il est recommandé de prévoir et de signaler les tendances pour envisager toutes les possibilités en matière de menaces, de parcours et de méthodes d'attaque, etc. à partir de l'analyse des données et de la situation globale, et d'envoyer des alertes précoces pour proposer des stratégies de sécurité afin de se défendre contre d'éventuelles attaques. La méthode d'appréciation de la situation repose sur des algorithmes qui font notamment appel à l'apprentissage automatique, à des analyses linéaires, aux probabilités, et à l'intelligence artificielle.

Il est recommandé de systématiquement prévoir et signaler les tendances. Il est recommandé que les résultats de ces activités soient présentés selon le format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2]. Pour ce qui est de la visualisation et de la présentation de la situation, il est recommandé de présenter la situation globale en matière de données à l'aide d'outils de visualisation.

8.3 Échange et utilisation des renseignements

L'échange et l'utilisation des renseignements sur les menaces vise à prévenir et limiter les incidents liés à la sécurité et à intervenir rapidement et efficacement chaque fois qu'un incident lié à la sécurité survient dans un réseau de télécommunication.

Les différents départements et communautés d'opérateurs de télécommunication peuvent s'échanger les renseignements issus des étapes de traitement et d'analyse des données, notamment les informations sur les menaces, les alertes prévisionnelles, les contre-mesures liées à la sécurité des réseaux, les politiques de sécurité, etc. Cet échange peut prendre différentes formes. Les renseignements peuvent par exemple être présentés sous forme de rapports ou d'avis, ou encore d'indicateurs de détection.

Il est recommandé d'obtenir des renseignements à partir d'éléments de réseau, de dispositifs de sécurité et de centres d'alerte, etc. Les administrateurs de l'exploitation et de la maintenance pourront élaborer des politiques de sécurité fondées sur les renseignements ainsi obtenus et les appliquer aux éléments de réseau et dispositifs de sécurité. Ils pourront en outre mettre à jour les versions des logiciels et modifier la configuration des éléments de réseau et des dispositifs de sécurité, selon que de besoin.

Il est recommandé d'utiliser les renseignements sur les URL pour les passerelles, lesquelles pourront mettre à jour leur politique de sécurité en filtrant les URL malveillants à mettre à l'index. Il est également recommandé d'utiliser ces renseignements pour les systèmes IDS ou IPS en mettant à jour les règles de protection à l'aide des URL correspondants.

Il est recommandé d'utiliser les renseignements sur les domaines malveillants pour les serveurs DNS, lesquels pourront mettre à jour leur configuration en définissant les domaines malveillants à mettre à l'index.

Il est recommandé d'utiliser les renseignements sur les adresses IP malveillantes pour les pare-feu, lesquels pourront mettre à jour leur politique de sécurité en filtrant les adresses IP malveillantes. Ces renseignements peuvent aussi être utilisés pour les systèmes IDS ou IPS en mettant à jour les règles de protection à l'aide des adresses IP correspondantes.

Il est recommandé d'utiliser les renseignements sur les vulnérabilités pour les éléments de réseau, lesquels pourront corriger leurs vulnérabilités grâce à une mise à jour logicielle ou matérielle. En outre, ces renseignements peuvent, à titre d'option, servir à fabriquer des modules de détection puis à mettre à jour le scanner de détection. Ils peuvent également, à titre d'option, être utilisés dans un système d'intervention d'urgence pour identifier les incidents et contribuer à prendre des mesures pour prévenir les attaques.

Il est recommandé de présenter les renseignements selon le format standard défini dans les normes [OASIS STIXv2] et [OASIS TAXIIv2]. Il est recommandé d'utiliser les spécifications OpenC2 d'OASIS pour les fonctions de commande et de contrôle liées à la sécurité.

Bibliographie

[b-UIT-T X.1211] Recommandation UIT-T X.1211 (2014), *Techniques pour prévenir les attaques sur le web*.

[b-UIT-T X.1231] Recommandation UIT-T X.1231 (2008), *Stratégies techniques de lutte contre le spam*.

[b-UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Liste des failles courantes*.

[b-UIT-T Y.140.1] Recommandation UIT-T Y.140.1 (2004), *Guide pour les attributs et spécifications d'interconnexion entre opérateurs de réseaux publics de télécommunication et fournisseurs de services de télécommunication*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020