Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1060

(06/2021)

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

Sécurité de l'information et des réseaux – Gestion de la sécurité

Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense

Recommandation UIT-T X.1060

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.1429
Sécurité de la technologie des registres distribués	X.1430–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
IMT-T SÉCURITÉ des télécommunications mobiles internationales)	X.1800–X.1819

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

Recommandation UIT-T X.1060

Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense

Résumé

La Recommandation UIT-T X.1060 définit le centre de cyberdéfense (CDC) comme une entité jouant un rôle central dans le traitement des risques de cybersécurité au sein d'une organisation. Un centre de cyberdéfense s'articule autour de trois processus – mise en place, gestion et évaluation – qu'il doit mettre en œuvre concrètement et qui en forment le cadre. La présente Recommandation définit également les services qui sont nécessaires à la mise en œuvre de mesures de cybersécurité plus précises.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1060	29-06-2021	17	11.1002/1000/14721

Mots clés

Centre de cyberdéfense, CIRT, centre des opérations de sécurité (SOC).

* 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

Au sein d'une organisation, les risques liés à la cybersécurité ont une incidence non négligeable sur les activités globales de l'organisation. Les risques auxquels les organisations font face sont les changements environnementaux, tant du point de vue social que commercial, et les pressions externes exercées par les réglementations et les menaces accrues. Les hauts dirigeants, comme les directeurs (CxO), sont par conséquent responsables de la gestion des contrôles pour l'ensemble de l'organisation afin de répondre à ces risques et changements. Leur leadership est attendu au niveau du développement et du contrôle de l'alignement des politiques de sécurité avec les objectifs de l'entreprise, en ce qu'il forme un élément important de la mise en œuvre des contrôles dans le domaine de la cybersécurité; il est souvent assuré par le responsable principal de la sécurité (CSO) ou le responsable de la sécurité des systèmes d'information (CISO). En vue d'assurer la mise en œuvre pratique des mesures de sécurité, il est absolument indispensable de disposer d'une entité prenant en charge les activités du CSO ou du CISO par le biais d'une gestion stratégique au niveau de l'organisation. Cette entité est appelée centre de cyberdéfense (CDC) dans la présente Recommandation.

La présente Recommandation offre un cadre pour la mise en place et la gestion d'un centre de cyberdéfense et l'évaluation de son efficacité. Ce cadre indique comment un centre de cyberdéfense doit définir et mettre en œuvre les services de sécurité afin de favoriser la sécurité d'une organisation. Il aide une organisation à répondre aux risques de cybersécurité.

Recommandation UIT-T X.1060

Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense

1 Champ d'application

La présente Recommandation fixe un cadre destiné aux organisations cherchant à mettre en place et à gérer un centre de cyberdéfense (CDC), ainsi qu'à en évaluer l'efficacité. Ce cadre indique comment un centre de cyberdéfense doit définir et mettre en œuvre les services de sécurité afin de favoriser la sécurité d'une organisation.

La présente Recommandation s'adresse aux responsables de la sécurité au niveau des hauts dirigeants d'une organisation, tels que le responsable principal de la sécurité (CSO) ou le responsable de la sécurité des systèmes d'information (CISO), ainsi que les superviseurs des services de sécurité qui les assistent.

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

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 externalisation [b-ITU-T X.1053]: on parle d'externalisation lorsqu'une entreprise sous-traite à une société extérieure un ou plusieurs de ses processus et/ou fonctions internes. L'entreprise transfère des ressources à cette société tout en conservant la capacité de gérer la relation avec les processus externalisés.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 centre de cyberdéfense (CDC): entité au sein d'une organisation qui propose des services de sécurité dans le but de répondre aux risques liés à la cybersécurité pesant sur ses activités commerciales.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

APT menace persistante avancée (*advanced persistent threat*)

CDC centre de cyberdéfense (*cyber defence centre*)

CISO responsable de la sécurité des systèmes d'information (*chief information security officer*)

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

CSO responsable principal de la sécurité (*chief security officer*)

CxO directeurs ou membres du conseil d'administration (*C-suite*)

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

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

IT informatique (*information technology*)

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

SLA accord de niveau de service (*service level agreement*)

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

5 Conventions

Aucune.

6 Structure de la présente Recommandation

La présente Recommandation explique le concept de centre de cyberdéfense au paragraphe 7. Le paragraphe 8 donne un aperçu général du cadre de mise en place et de gestion d'un centre de cyberdéfense. Le cadre est décrit plus précisément aux paragraphes suivants: processus de mise en place d'un centre de cyberdéfense (paragraphe 9); processus de gestion d'un centre de cyberdéfense (paragraphe 10) et processus d'évaluation d'un centre de cyberdéfense (paragraphe 11). Au paragraphe 12, une description générale des services de sécurité fournis par un centre de cyberdéfense fait office de bonne pratique et chaque service est décrit de manière plus détaillée à l'Annexe A.

7 Aperçu général d'un centre de cyberdéfense

Les organisations œuvrent pour la réussite de leurs entreprises. Dans la perspective de gérer les risques pesant sur les activités commerciales, le responsable de la sécurité des systèmes d'information élabore des politiques en matière de sécurité, et notamment du point de vue de la cybersécurité. Un centre de cyberdéfense est une entité qui met en œuvre des politiques de sécurité, sous la forme plus précise de services CDC, regroupant des activités de sécurité réalisées par les équipes en charge de la sécurité. Les services d'un centre de cyberdéfense (CDC) peuvent définir des fonctions de sécurité comme les capacités d'un système à procéder au traitement d'aspects liés à la sécurité. La Figure 1 présente les parties prenantes et leur rôle dans le fonctionnement d'un centre de cyberdéfense.

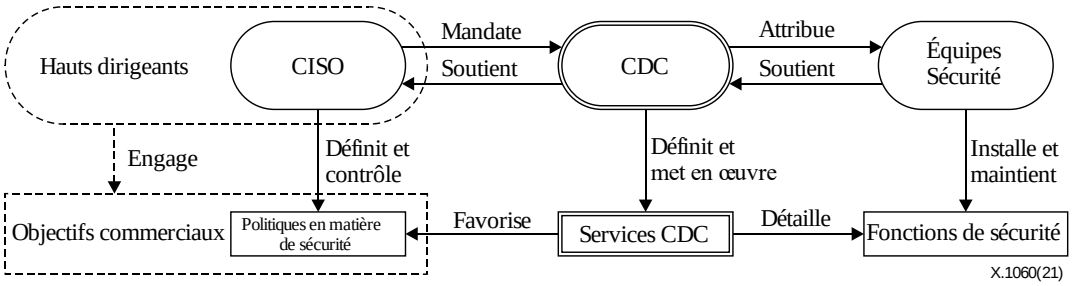

Figure 1 – Les parties prenantes et leur rôle dans le fonctionnement d'un centre de cyberdéfense

Selon la taille et la nature de l'organisation, un centre de cyberdéfense peut se présenter comme une unité indépendante, un comité, ou une petite équipe. Indépendamment du format, il doit exister en tant qu'entité au sein d'une organisation, et disposer de l'autorité et des ressources pour mettre en œuvre les services de sécurité garantissant la sécurisation d'une organisation. De tels services de sécurité doivent être conformes aux politiques de sécurité et garantir la qualité des activités de sécurité; le niveau de chaque service doit être explicitement consigné dans un document d'accord, tel qu'un accord de niveau de service (SLA). La qualité générale du service de sécurité d'un centre de cyberdéfense est évaluée par des mesures précisées au paragraphe 9.4.

8 Cadre pour la mise en place et l'exploitation d'un centre de cyberdéfense

La Figure 2 présente un cadre de mise en place et d'exploitation d'un centre de cyberdéfense. Ce cadre comprend trois processus: la mise en place, la gestion et l'évaluation. Pour garantir la sécurité d'une organisation, un centre de cyberdéfense doit être mis en place et géré comme il se doit. Il doit également faire l'objet d'une évaluation régulière et en temps utile, ainsi que d'une amélioration continue. Le présent cadre permet à l'organisation de mettre à jour ses activités liées à la sécurité.

Au cours du processus de mise en place, il convient de prendre en compte les activités liées à la sécurité au sein de l'organisation. Les bonnes pratiques en matière de services de sécurité d'un centre de cyberdéfense sont listées à l'Annexe A. Une organisation peut établir son propre catalogue de services en sélectionnant les services depuis cette liste et en ajoutant des services propres à l'organisation. Chaque service du catalogue doit également définir un profil comprenant: le(s) propriétaire(s), les rôles et responsabilités, ainsi que le type d'affectation de service (interne, externe ou une combinaison des deux). Une fois que le profil du service est défini, il convient de déterminer le résultat actuel de départ et le résultat ciblé pour chaque service proposé par un centre de cyberdéfense en vue du processus d'évaluation.

Le processus de gestion comprend trois phases et deux cycles. La phase de gestion stratégique se concentre sur la gestion des activités générales d'un centre de cyberdéfense, la phase d'exploitation gère les opérations de routine de surveillance et d'analyse, enfin la phase d'intervention gère les interventions d'urgence. Ces phases s'inscrivent dans des cycles à la fois courts et longs; l'exploitation et l'intervention nécessitent des résolutions en temps utiles au sein de cycles courts. Tandis que la gestion stratégique doit prendre en compte une amélioration à long terme, associée aux résultats issus de cycles courts s'inscrivant dans un cycle long. L'amélioration à long terme requiert généralement des décisions portant sur de nouveaux investissements et des modifications importantes des architectures système.

Le processus d'évaluation examine le catalogue, le profil et le portefeuille des services du centre de cyberdéfense (voir Figure 4), qui doivent faire l'objet d'une évaluation objective au bon moment pour chacun.

Les résultats de l'évaluation doivent être examinés et se refléter au niveau des trois processus d'un centre de cyberdéfense. Un cycle récurrent des processus de mise en place, de gestion et

d'évaluation visant à améliorer les activités de sécurité doit être défini et maintenu au sein de l'organisation.

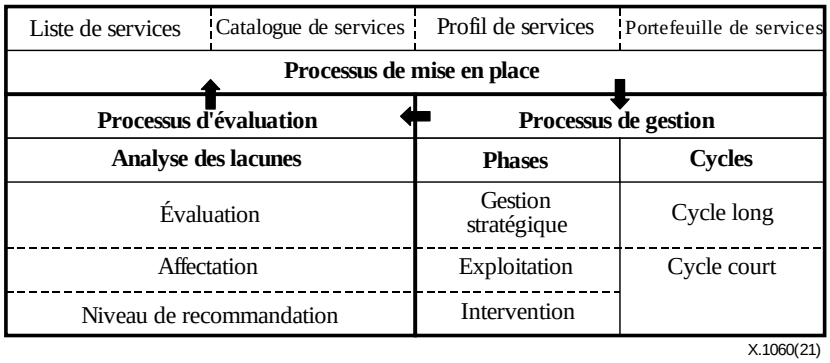

Figure 2 – Cadre pour la mise en place et l'exploitation d'un centre de cyberdéfense

9 Processus de mise en place

9.1 Aperçu général

Le centre de cyberdéfense dispose d'un processus de mise en place afin de déterminer quels services de sécurité doivent être mis en œuvre dans l'organisation. Les services candidats à la mise en œuvre sont sélectionnés à partir de la liste de services du centre de cyberdéfense, fondée sur les bonnes pratiques de l'organisation. Pour consulter la liste de services CDC, voir le paragraphe 12.

La Figure 3 montre les trois phases de la mise en place d'un centre de cyberdéfense.

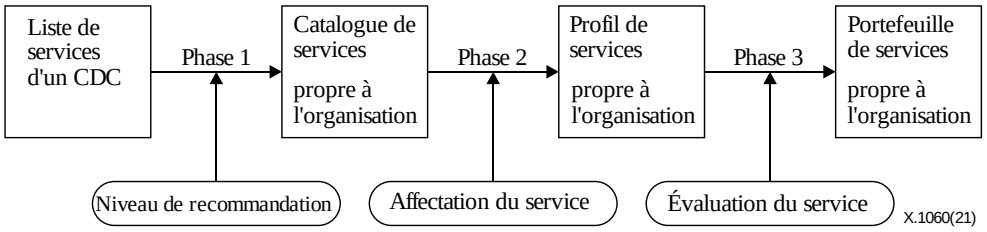

Figure 3 – Phases de mise en place d'un centre de cyberdéfense

1) Phase 1: Création d'un catalogue des services proposés par le centre de cyberdéfense

L'organisation doit commencer par créer un catalogue des services du centre de cyberdéfense.

Au cours de cette phase, les services candidats à la mise en œuvre sont extraits de la liste générale de services. Les détails de la liste générale figurent au paragraphe 12. S'il manque des services, de nouveaux services doivent être définis et ajoutés au catalogue des services du centre de cyberdéfense.

2) Phase 2: Création d'un profil des services du centre de cyberdéfense

Pour les services listés dans le catalogue des services du centre de cyberdéfense, l'organisation doit déterminer les rôles et responsabilités des équipes qui fournissent ces services. Au cours de cette phase, il convient de considérer l'affectation des services du centre de cyberdéfense figurant au paragraphe 9.3.

L'organisation doit ainsi produire le profil des services du centre de cyberdéfense.

3) Phase 3: Création d'un portefeuille des services du centre de cyberdéfense

Après avoir décidé du profil des services du centre de cyberdéfense, l'organisation doit mesurer le résultat des services actuels (valeur de départ) de chaque service et définir un résultat de service objectif à moyen ou long terme (valeur cible).

Une fois que les niveaux départ et cible ont été définis, l'organisation doit produire le portefeuille de service d'un centre de cyberdéfense.

La Figure 4 présente une grille de services d'un centre de cyberdéfense. La grille sera complétée après les phases 1 à 3.

Service	Niveau de recommandation	Affectation du service	Résultat du service	
			Valeur de départ	Valeur cible
Service ex.1	Basique	Interne (dépt. AB)	3	5
Service ex.2	Standard	Externe (Z-MSSP)	2	4
Service ex.3	Avancé	Non attribué	1	2

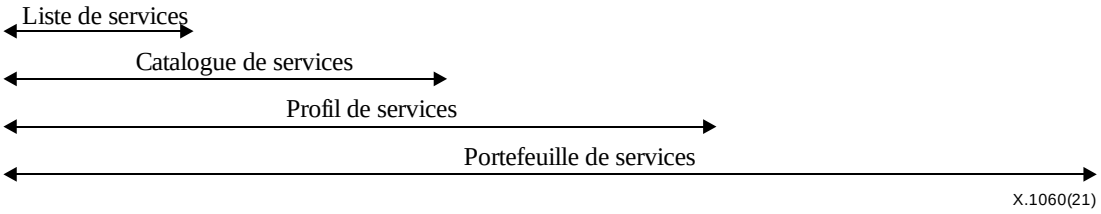

Figure 4 – Grille de services pour un centre de cyberdéfense

9.2 Niveau de recommandation des services du centre de cyberdéfense

Pour pouvoir mettre en œuvre les services CDC les plus pertinents pour elle, l'organisation doit envisager dans quelle mesure un service est nécessaire selon les cinq niveaux définis au Tableau 1. La priorité de mise en œuvre d'un service peut être clarifiée en mesurant les différents niveaux.

Tableau 1 – Niveau de recommandation des services d'un centre de cyberdéfense

Poids	Description
Non nécessaire	Services jugés inutiles
Basique	Services minimaux à mettre en œuvre
Standard	Services dont la mise en œuvre est généralement recommandée
Avancé	Services requis pour accomplir un cycle CDC de haut niveau
Facultatif	Services sélectionnés à titre facultatif selon la forme attendue du centre de cyberdéfense

9.3 Affectation des services d'un centre de cyberdéfense

L'organisation doit préciser en détail quelle équipe doit mettre en œuvre le service du centre de cyberdéfense. Selon ses capacités à mettre en œuvre les services, l'organisation doit définir l'affectation des services du centre de cyberdéfense, incluant les services externalisés. Voir le Tableau 2.

Tableau 2 – Affectation des services du centre de cyberdéfense

Type	Description
Internalisation	Les services sont fournis par une équipe interne à l'organisation. L'organisation doit mentionner l'équipe responsable.
Externalisation	Les services sont fournis par une équipe externe à l'organisation. L'organisation doit spécifier le sous-traitant.
Combinaison des deux	L'organisation fait appel à la fois aux ressources internes et externes. Une équipe responsable et un sous-traitant doivent être désignés par l'organisation.
Non affecté	Bien que l'organisation reconnaisse la pertinence du service, ce dernier n'a pas été affecté au sein de l'organisation.

En cas de recours à la sous-traitance (externalisation), les points A) et B) doivent être précisés.

A) Nature de l'information traitée

L'organisation doit classer l'information traitée, en précisant les définitions ou en distinguant ce qui est "interne" et "externe" à l'organisation. Par exemple, dans le cas d'incidents, l'information sur les dommages ou l'impact d'une attaque doit être considérée comme interne, tandis que l'information concernant l'attaque en elle-même doit être considérée comme externe.

B) Besoin de compétences spécialisées en matière de sécurité

L'organisation doit indiquer si des compétences spécialisées dans le domaine de la sécurité sont nécessaires pour fournir le service.

Les services du centre de cyberdéfense doivent être classés en quadrants I) à IV) sur la base des deux points d'indicateurs suivants. Voir la Figure 5.

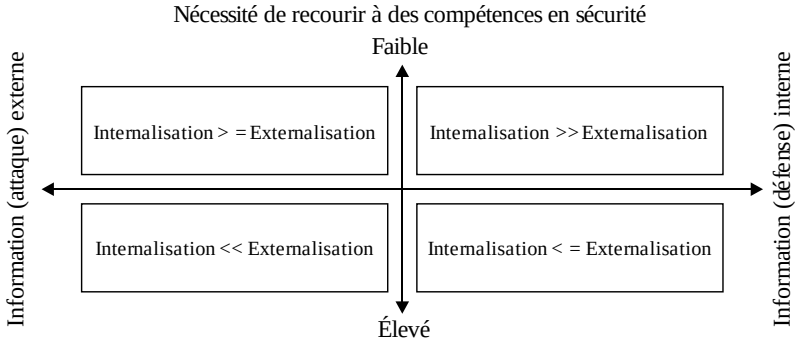

Figure 5 – Quadrants des ressources

I) Internalisation >> Externalisation

Si l'expertise en matière de sécurité n'est pas requise pour traiter des informations confidentielles au sein de l'organisation, le recours à des ressources internes est optimal, et l'externalisation n'est pas souhaitable.

II) Internalisation >= Externalisation

Si l'expertise requise en matière de sécurité n'est pas très pointue, bien que l'information soit externe à l'organisation, l'activité et la gestion doivent être traitées principalement au sein de l'organisation avec l'appui de sous-traitants.

III) Internalisation << Externalisation

Afin de traiter des informations externes à l'organisation, portant principalement sur des attaques, le service doit être mis en œuvre par une organisation disposant de compétences spécifiques (sous-traitants par exemple). À moins que des experts disposant des compétences spécifiques soient

disponibles en interne, il est difficile pour une organisation de mettre en œuvre le service par elle-même.

IV) Internalisation <= Externalisation

Si des compétences spécialisées sont requises pour gérer des informations internes au sein de l'entreprise, cette activité peut être réalisée principalement par une organisation spécialisée (en sous-traitance, par exemple) que l'organisation devra orienter et prendre en charge.

9.4 Évaluation des services du centre de cyberdéfense

Lorsque le portefeuille de services du centre de cyberdéfense est créé, le statut de mise en œuvre, de départ et cible, doit être évalué à l'aide des points de service listés dans le Tableau 3. Il convient de noter que les différents types de service (par exemple interne et externe) seront évalués sur la base du critère affecté aux points de service.

Tableau 3 – Points de service pour le centre de cyberdéfense

Pour les services internes	
L'activité dûment étayée est autorisée par le responsable de la sécurité des systèmes d'information ou un autre directeur de l'organisation en charge de cette responsabilité	+5 points
L'activité est documentée et d'autres acteurs peuvent jouer le rôle d'un opérateur existant	+4 points
L'activité n'est pas documentée, et d'autres acteurs peuvent temporairement jouer le rôle partiel d'un opérateur existant	+3 points
L'activité n'est pas documentée, et l'opérateur existant peut jouer son rôle	+2 points
L'activité n'est pas opérationnelle	+1 point
Décision de ne pas mettre en œuvre en interne	N/A

Pour les services externes	
Le contenu du service et le résultat attendus sont compris et les résultats sont conformes aux attentes	+5 points
Le contenu du service et le résultat attendus sont compris, mais les résultats ne sont pas conformes aux attentes	+4 points
Le contenu du service ou le résultat attendu n'a pas été compris	+3 points
Ni le contenu du service ni le résultat attendu n'ont été compris	+2 points
Ni le résultat ni le rapport n'ont fait l'objet d'un examen	+1 point
Décision de ne pas mettre en œuvre en externe	N/A

10 Processus de gestion

Le centre de cyberdéfense favorise les activités de sécurité au sein de l'organisation à travers la mise en œuvre du processus de gestion du centre de cyberdéfense, comprenant les trois phases et les deux cycles présentés à la Figure 6.

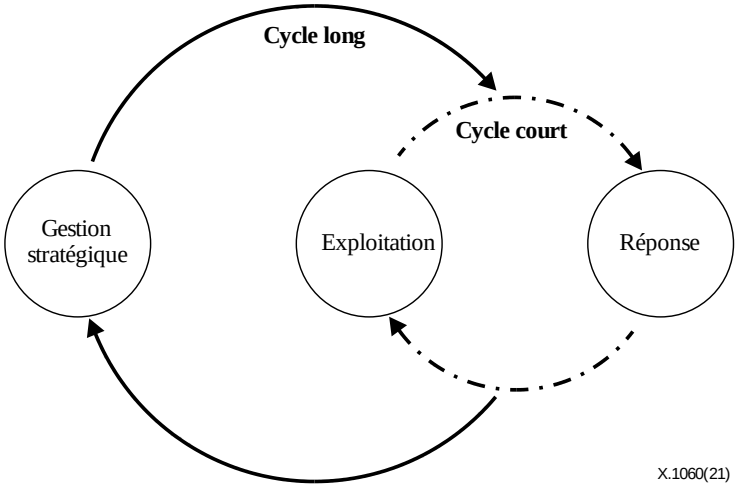

Figure 6 – Processus de gestion du centre de cyberdéfense

(1) Phase de gestion stratégique

La gestion stratégique est responsable et redevable de tous les services stratégiques pertinents en termes de définition, de conception, de planification, de gestion, de certification, etc. qui garantissent le développement du centre de cyberdéfense sur le long terme.

(2) Phase d'exploitation

La maintenance du cadre mis en place doit être réalisée durant la phase d'exploitation. Il s'agit du fonctionnement en temps ordinaire ou habituel comprenant généralement les activités de routine, telles que l'analyse de la détection d'incidents, la surveillance et la maintenance des systèmes de réponse de la sécurité. L'équipe en charge de telles opérations est souvent appelée le centre des opérations de sécurité (SOC).

(3) Phase de réponse

Une réponse aux incidents doit être apportée lorsqu'un événement est détecté par l'analyse durant la phase d'exploitation. Cette phase est toujours une urgence. Les personnes appelées à intervenir en cas d'incidents sont souvent désignées comme l'équipe d'intervention en cas d'incident informatique (CSIRT).

Le travail durant la phase de réponse ne se limite pas à ce qui ressort de la phase d'exploitation, mais l'équipe doit aussi apporter des réponses aux rapports ou aux notifications des parties tierces.

A) Cycle court

L'exploitation et l'intervention sont des activités quotidiennes. Au cours de ces processus, il apparaît toujours des problèmes dans le processus d'activité et des difficultés dans le système de réponse de la sécurité. Une amélioration continue visant à résoudre ces difficultés est par conséquent nécessaire, par exemple l'automatisation de tâches simples, l'amélioration des outils permettant d'analyser la cohérence et l'examen des éléments des rapports, dans le respect des ressources allouées pour un cycle court (personnes, budget, système).

B) Cycle long

Un examen qui nécessite l'affectation de nouvelles ressources doit être pratiqué lors des cycles longs.

Si des problèmes ne pouvant être résolus par le système actuel sont décelés lors du cycle court, la réponse doit alors s'inscrire dans une perspective et un plan de long terme, c'est-à-dire le lancement d'un nouveau produit de sécurité, un examen approfondi des politiques de sécurité et un changement de configuration à grande échelle dans les systèmes de sécurité.

11 Processus d'évaluation

11.1 Aperçu général

Le catalogue, le profil et le portefeuille de services du centre de cyberdéfense formulés dans le processus de mise en place doivent faire l'objet d'une évaluation régulière et en temps utile. La Figure 7 décrit un processus d'évaluation des services du centre de cyberdéfense.

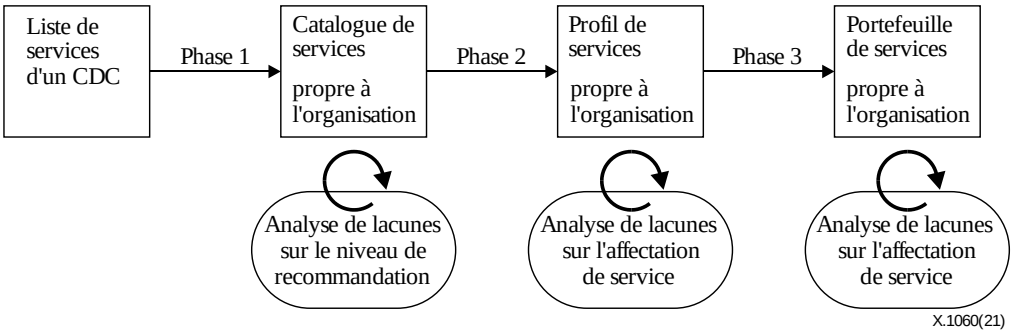

Figure 7 – Processus d'évaluation du centre de cyberdéfense

11.2 Évaluation du catalogue de services du centre de cyberdéfense

Une analyse des lacunes doit être réalisée sur le niveau de recommandation de service du centre de cyberdéfense. Un examen est requis en raison de l'évolution de l'environnement et des menaces, les services "inutiles" doivent notamment être réexaminés et revus pour garantir l'absence d'omissions. Le catalogue de services du centre de cyberdéfense doit être évalué lorsque l'entreprise introduit des changements, tels que le démarrage de nouvelles activités commerciales et la réponse à de nouveaux risques et menaces.

11.3 Évaluation du profil de services du centre de cyberdéfense

Une analyse des lacunes doit être réalisée sur les affectations de service du centre de cyberdéfense. Lors de l'affectation des services, le critère "non attribuable" peut être éliminé et l'organisation peut espérer améliorer le niveau de maturité à travers un examen. Le profil de service du centre de cyberdéfense doit être évalué dès lors qu'un changement organisationnel intervient, tel que des changements d'organisation internes pour les services assurés en interne et des changements au niveau des sous-traitants pour les services assurés par des sous-traitants.

11.4 Évaluation du portefeuille de services du centre de cyberdéfense

Une analyse des lacunes doit être réalisée sur les résultats des différents services du centre de cyberdéfense. La différence entre le résultat cible et le résultat de départ doit être précisée de manière à ce que l'organisation puisse se concentrer sur ce qui doit être amélioré, reconfirmer le résultat de service du centre de cyberdéfense et en extraire des problématiques. Le portefeuille de services d'un centre de cyberdéfense doit faire l'objet d'une évaluation régulière.

12 Catégories de services du centre de cyberdéfense et liste de services

Les catégories et la liste de services du centre de cyberdéfense sont nécessaires au cours des processus de mise en place et de gestion (voir paragraphes 9 et 10).

Le service CDC comprend neuf catégories de services:

A) Gestion stratégique du centre de cyberdéfense

B) Analyse en temps réel

C) Analyse approfondie

D) Réponse en cas d'incident

E) Contrôle et évaluation

F) Collecte, analyse et évaluation de l'information relative à la menace

G) Développement et maintenance de plates-formes du centre de cyberdéfense

H) Prise en charge de l'intervention en cas de fraude interne

I) Relation active avec les parties externes.

A) Gestion stratégique du centre de cyberdéfense

Cette catégorie inclut la planification des politiques et des ressources relatives à toutes les activités mentionnées dans les catégories A) à I) au sein de l'organisation y compris un centre de cyberdéfense en vue de garantir la stabilité de son exploitation.

B) Analyse en temps réel

Cette catégorie surveille et analyse en continu les journaux et les données de différents systèmes, tels que les dispositifs, les serveurs et les produits de sécurité en réseau. L'objectif est de déceler les menaces en temps réel afin d'entraîner une réponse rapide et adaptée à l'incident.

C) Analyse approfondie

Il s'agit d'une catégorie en lien avec l'incident, telle que l'investigation des systèmes touchés, l'examen des données compromises, l'analyse des outils et des méthodes utilisés lors de l'attaque.

L'objectif étant d'élucider l'intégralité du périmètre de l'incident et d'identifier les impacts.

D) Réponse en cas d'incident

Cette catégorie prend des mesures précises basées sur les résultats des analyses en temps réel et l'information concernant la menace pour déjouer et éliminer les menaces.

Son objectif est de minimiser l'impact sur le système et l'activité, et inclut la coordination et le reporting aux parties prenantes.

E) Contrôle et évaluation

Cette catégorie est destinée à l'évaluation de la vulnérabilité des systèmes à protéger, ainsi qu'à former à la réponse en cas d'incident et à l'évaluer. L'objectif de cette catégorie est d'améliorer le niveau de sécurité.

F) Collecte, analyse et évaluation de l'information relative à la menace

Cette catégorie collecte l'information relative à la menace portant sur les vulnérabilités et les attaques (intelligence externe) disponible sur l'Internet et traite l'information portant sur l'analyse en temps réel et la réponse aux incidents (intelligence interne).

L'objectif est d'améliorer la précision de l'analyse en temps réel et de la réponse aux incidents, ainsi que d'améliorer les ressources de sécurité.

G) Développement et maintenance des plates-formes du centre de cyberdéfense

Cette catégorie gère, améliore et développe de nouveaux systèmes (tels que des produits de sécurité, des bases de données contenant des collectes de journaux et des systèmes opérationnels) qui sont nécessaires aux interventions dans le domaine de la sécurité.

L'objectif est d'obtenir des activités de sécurité fluides et durables dans d'autres catégories.

H) Prise en charge de l'intervention en cas de fraude interne

Cette catégorie collecte des données d'audit pour prendre en charge les interventions en cas de fraude interne.

L'objectif de cette catégorie est d'appuyer les interventions en cas de fraude interne et la résolution de la fraude interne en fournissant des journaux et des analyses.

I) Relation active avec les parties externes

Cette catégorie comprend la coordination et la collaboration avec les parties prenantes internes et les organisations externes.

L'objectif est d'améliorer le niveau de sécurité de l'organisation, d'augmenter la valeur de la sécurité au sein de l'organisation, induisant ainsi une poursuite du développement et du renforcement de l'organisation.

La Figure 8 montre une cartographie des catégories de services avec les processus de gestion et le Tableau 4 présente la liste des services.

Les descriptions détaillées de chaque service de la liste de services fournis par un centre de cyberdéfense sont fournies à l'Annexe A.

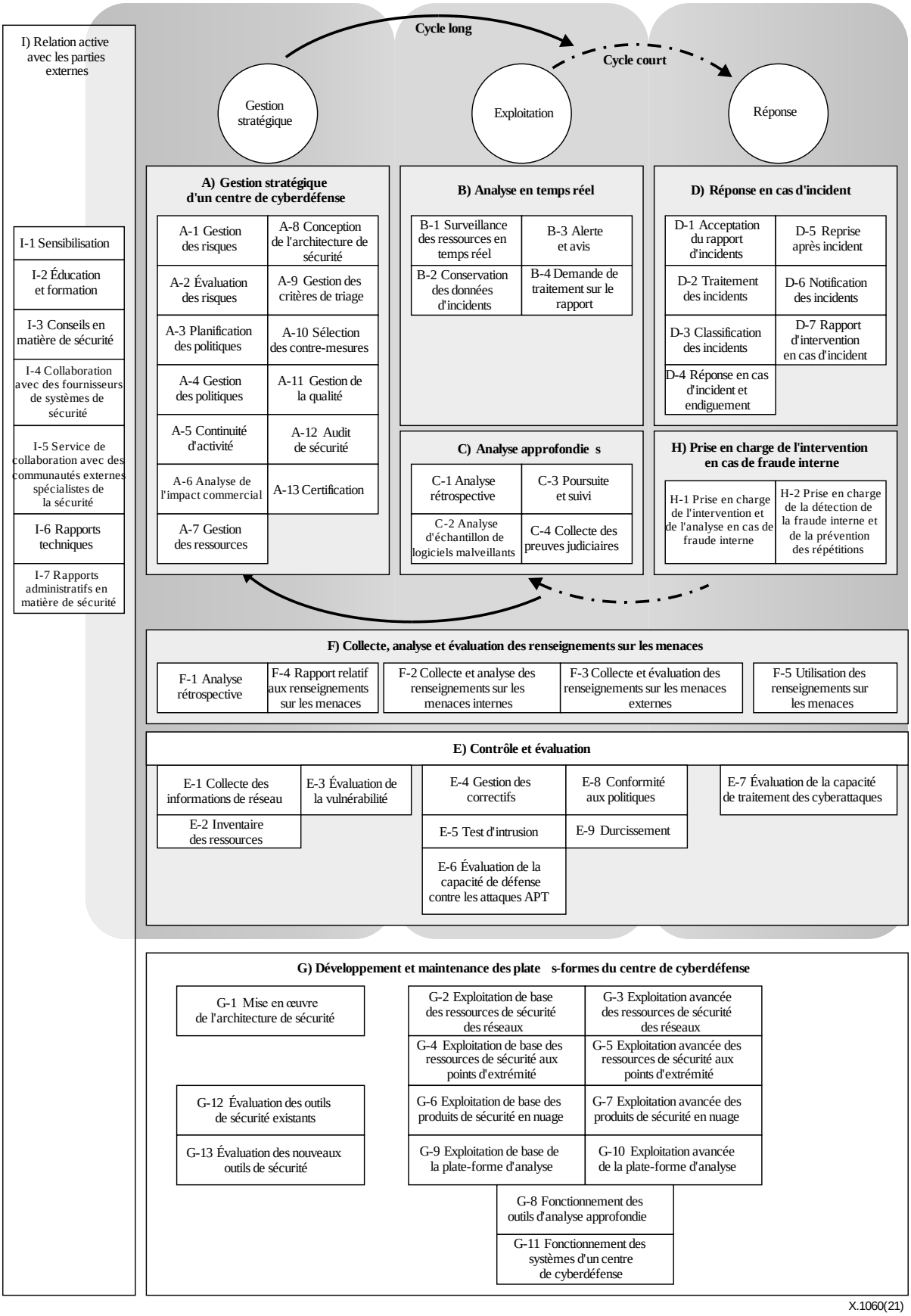

Figure 8 – Les catégories de service d'un centre de cyberdéfense

Tableau 4 – Liste de services d'un centre de cyberdéfense

A	**Gestion stratégique d'un centre de cyberdéfense**
A-1	Gestion des risques
A-2	Évaluation des risques
A-3	Planification des politiques
A-4	Gestion des politiques
A-5	Continuité d'activité
A-6	Analyse de l'impact commercial
A-7	Gestion des ressources
A-8	Conception de l'architecture de sécurité
A-9	Gestion des critères de triage
A-10	Sélection des contre-mesures
A-11	Gestion de la qualité
A-12	Audit de sécurité
A-13	Certification
B	**Analyse en temps réel**
B-1	Surveillance des ressources en temps réel
B-2	Conservation des données d'incidents
B-3	Alerte et avis
B-4	Demande de traitement sur le rapport
C	**Analyse approfondie**
C-1	Analyse rétrospective
C-2	Analyse d'échantillon de logiciels malveillants
C-3	Poursuite et suivi
C-4	Collecte des preuves judiciaires
D	**Réponse en cas d'incident**
D	Acceptation du rapport d'incidents
D-2	Traitement des incidents
D-3	Classification des incidents
D-4	Réponse en cas d'incident et endiguement
D-5	Reprise après incident
D-6	Notification des incidents
D-7	Rapport d'intervention en cas d'incident
E	**Contrôle et évaluation**
E-1	Collecte des informations de réseau
E-2	Inventaire des ressources
E-3	Évaluation de la vulnérabilité
E-4	Gestion des correctifs
E-5	Test d'intrusion
E-6	Évaluation de la capacité de défense contre les attaques APT
E-7	Évaluation de la capacité de traitement des cyberattaques
E-8	Conformité aux politiques
E-9	Durcissement

F	**Collecte, analyse et évaluation des renseignements sur les menaces**
F-1	Analyse rétrospective
F-2	Collecte et analyse des renseignements sur les menaces internes
F-3	Collecte et évaluation des renseignements sur les menaces externes
F-4	Rapport relatif aux renseignements sur les menaces
F-5	Utilisation des renseignements sur les menaces
G	**Développement et maintenance des plates-formes du centre de cyberdéfense**
G-1	Mise en œuvre de l'architecture de sécurité
G-2	Exploitation de base des ressources de sécurité des réseaux
G-3	Exploitation avancée des ressources de sécurité des réseaux
G-4	Exploitation de base des ressources de sécurité aux points d'extrémité
G-5	Exploitation avancée des ressources de sécurité aux points d'extrémité
G-6	Exploitation de base des produits de sécurité en nuage
G-7	Exploitation avancée des produits de sécurité en nuage
G-8	Fonctionnement des outils d'analyse approfondie
G-9	Exploitation de base de la plate-forme d'analyse
G-10	Exploitation avancée de la plate-forme d'analyse
G-11	Fonctionnement des systèmes d'un centre de cyberdéfense
G-12	Évaluation des outils de sécurité existants
G-13	Évaluation des nouveaux outils de sécurité
H	**Prise en charge de l'intervention en cas de fraude interne**
H-1	Prise en charge de l'intervention et de l'analyse en cas de fraude interne
H-2	Prise en charge de la détection de la fraude interne et de la prévention des répétitions
I	**Relation active avec les parties externes**
I-1	Sensibilisation
I-2	Éducation et formation
I-3	Conseils en matière de sécurité
I-4	Collaboration avec des fournisseurs de systèmes de sécurité
I-5	Service de collaboration avec des communautés externes spécialistes de la sécurité
I-6	Rapports techniques
I-7	Rapports administratifs en matière de sécurité

Annexe A

Liste assortie de descriptions des services d'un centre de cyberdéfense

(Cette Annexe fait partie intégrante de la présente Recommandation.)

A.1 Catégorie A: Gestion stratégique d'un centre de cyberdéfense

A.1.1 A-1 Gestion des risques

Le service de gestion des risques vise à coordonner les activités énoncées de A-2 à A-13 dans le but d'orienter et de contrôler une organisation en tenant compte des risques.

A.1.2 A-2 Évaluation des risques

Le service d'évaluation des risques fournit un aperçu du niveau de risque au sein d'une organisation en termes de ressources, de menaces et de mesures de sécurité.

A.1.3 A-3 Planification des politiques

Le service de planification des politiques prend en charge toutes les activités liées à la définition de politiques spécifiques en matière de sécurité et à la compilation des lignes directrices.

A.1.4 A-4 Gestion des politiques

Le service de gestion des politiques vise à mener des examens périodiques dans le but d'évaluer les politiques et règlements d'une organisation et de se conformer aux exigences nouvelles ou externes (par ex. réglementations, directives).

A.1.5 A-5 Continuité d'activité

Le service de continuité d'activité prend en charge les fonctions opérationnelles nécessaires pour garantir la bonne mise en œuvre et exécution du plan de continuité d'une organisation.

A.1.6 A-6 Analyse de l'impact commercial

Le service chargé de l'analyse de l'impact commercial vise à évaluer systématiquement les impacts potentiels résultant d'incidents ou de scénarios divers. Ce service contribue à aider les organisations à comprendre l'ampleur des pertes qui pourraient survenir. Ces pertes incluent non seulement les pertes financières directes, mais aussi d'autres répercussions telles que la perte de la confiance des parties prenantes et les atteintes à la réputation.

A.1.7 A-7 Gestion des ressources

Le service de gestion des ressources planifie les ressources (personnel, budget, systèmes, etc.) pour prendre en charge les activités en matière de sécurité et les allouer de manière adaptée à chaque service.

A.1.8 A-8 Conception de l'architecture de sécurité

La conception de l'architecture de sécurité vise à mettre en place une architecture pour sécuriser l'entreprise. Le développement et la maintenance des plates-formes du centre de cyberdéfense (catégorie G) passent par la compilation de différentes mesures de sécurité qui prennent en compte la conception des systèmes et les contraintes des processus commerciaux (chaîne d'approvisionnement, par exemple).

A.1.9 A-9 Gestion des critères de tri

Le service de gestion des critères de tri définit des critères de tri précis (priorité d'intervention) pour les événements (par exemple, incidents, détection de vulnérabilité, découverte d'un renseignement sur une menace) dans le cadre du périmètre convenu dans la politique générale.

A.1.10 A-10 Sélection des contre-mesures

Le service en charge de la sélection des contre-mesures prend en charge toutes les activités de sélection des contre-mesures correspondant aux critères de tri (A-9) et des meilleures technologies dans le respect de toutes les dispositions en matière de sécurité.

A.1.11 A-11 Gestion de la qualité

Le service de gestion de la qualité vise à examiner les problèmes sous l'angle de la qualité des activités de sécurité et à déterminer s'ils ont ou non un impact négatif sur l'activité (par exemple, facilité d'utilisation, productivité) sur une période donnée (une semaine ou un mois par exemple).

A.1.12 A-12 Audit de sécurité

Le service chargé de l'audit de sécurité vérifie de manière systématique et mesurable la façon dont une organisation met en place et contrôle les politiques de sécurité sur un site ou une période donné(e). Le personnel d'un centre de cyberdéfense est indirectement impliqué dans les activités d'audit afin de fournir les informations et les preuves nécessaires relatives à la mise en œuvre des états de contrôle.

A.1.13 A-13 Certification

Le service de certification prend en charge les activités nécessaires à l'organisation en vue de se conformer aux différentes normes et systèmes de certification.

A.2 Catégorie B: Analyse en temps réel

A.2.1 B-1 Surveillance des ressources en temps réel

Le service chargé de la surveillance des ressources en temps réel a pour but de superviser et d'analyser le statut des systèmes ou des activités suspectes émanant de flux de réseaux et journaux, et de prendre en charge le tri en incident ou événement afin de collecter l'information nécessaire.

A.2.2 B-2 Conservation des données d'incidents

Le service de conservation des données d'incidents collecte et stocke de façon centralisée les incidents obtenus au cours du processus de surveillance et d'analyse de la sécurité.

A.2.3 B-3 Alerte et avis

Le service d'alerte et avis notifie la fonction interne concernée de l'événement qui met en lumière les risques potentiels encourus par les ressources d'information (par exemple, l'alerte des dispositifs de sécurité, bulletins de sécurité, vulnérabilités et menaces diffuses).

A.2.4 B-4 Demande de traitement sur le rapport

Le service chargé de la demande de traitement sur le rapport intervient pour enquêter sur les données et les rapports relatifs aux analyses.

A.3 Catégorie C: Analyse approfondie

A.3.1 C-1 Analyse rétrospective

Le service d'analyse rétrospective analyse les preuves numériques obtenues à partir des ressources de sécurité et fait le lien avec un événement en vue de contribuer à déterminer ce qui s'est produit.

A.3.2 C-2 Analyse d'échantillon de logiciels malveillants

Le service chargé de l'analyse d'échantillon de logiciels malveillants analyse les logiciels malveillants, les programmes et les scripts déployés par les attaquants, retrouvés au cours de chaque processus d'analyse rétrospective.

A.3.3 C-3 Poursuite et suivi

Ce service renvoie à la capacité d'une organisation à poursuivre et suivre la source de toute attaque sur ses infrastructures, ce qui est un facteur déterminant de la réussite dans la réduction des nouvelles attaques et la prévention des incidents de sécurité. Une aptitude reconnue à poursuivre et suivre les auteurs d'attaques aussi bien internes qu'externes (par exemple cyber identification) peut prévenir de futures attaques.

A.3.4 C-4 Collecte des preuves judiciaires

Le service de collecte des preuves judiciaires collecte et conserve les preuves électroniques numériques liées à un incident évalué, il élabore et maintient la validité des preuves ("chaîne de conservation des preuves").

A.4 Catégorie D: Réponse en cas d'incident

A.4.1 D-1 Acceptation du rapport d'incidents

Le service d'acceptation du rapport d'incident reçoit les rapports analytiques des opérations. Toutefois, il peut recevoir des rapports provenant d'une autre organisation au sein de l'entreprise ou d'une organisation extérieure.

A.4.2 D-2 Traitement des incidents

Le service de traitement des incidents est chargé de traiter les incidents acceptés et de coordonner les activités, y compris les activités D-3 à D-7.

A.4.3 D-3 Classification des incidents

Le service de classification des incidents est chargé de classer un incident en vue de contribuer à la compréhension commune des différents types d'incidents qui se produisent et de leurs causes.

A.4.4 D-4 Intervention en cas d'incident et endiguement

Le service en charge de l'intervention en cas d'incident et de l'endiguement vise à contenir un incident avant qu'il ne se diffuse à travers toutes les ressources et n'augmente les dommages sur ces ressources ou n'ait d'incidence sur elles.

A.4.5 D-5 Reprise après incident

Le service de reprise après incident prend en charge le rétablissement de la fonctionnalité d'une cible à son mode d'opération normal.

A.4.6 D-6 Notification des incidents

Le service de notification des incidents se charge de communiquer l'occurrence d'un incident aux équipes d'intervention et aux autres groupes concernés.

A.4.7 D-7 Rapport d'intervention en cas d'incident

Le service chargé de l'intervention en cas d'incident établit et distribue le rapport d'intervention d'un incident clos (si des efforts de contre-mesure ont été déployés, le rapport est remis à la gestion stratégique du centre de cyberdéfense (catégorie A)). Si le personnel du centre de cyberdéfense a besoin d'un rapport au cours du traitement d'un incident, ce service distribue un rapport provisoire.

A.5 Catégorie E: Contrôle et évaluation

A.5.1 E-1 Collecte des informations de réseau

Le service de collecte des informations de réseau reçoit un aperçu de la configuration du réseau à protéger.

A.5.2 E-2 Inventaire des ressources

Le service d'inventaire des ressources réalise la gestion de l'information relative au recensement des systèmes, des ressources et des applications formant l'infrastructure générale de l'activité inclue dans le périmètre de prise en charge du centre de cyberdéfense.

A.5.3 E-3 Évaluation de la vulnérabilité

Le service chargé de l'évaluation de la vulnérabilité étudie les réseaux, les systèmes et les applications afin d'identifier les vulnérabilités, de déterminer comment elles peuvent être exploitées et recommande comment atténuer les risques.

A.5.4 E-4 Gestion des correctifs

Le service assurant la gestion des correctifs prend en charge l'installation de tous les correctifs de sécurité nécessaires, pendant toute la durée où la disponibilité des systèmes informatiques (IT) est maintenue.

A.5.5 E-5 Test d'intrusion

Le service de test d'intrusion révèle les vulnérabilités en termes de sécurité qui pourraient être exploitées par des attaquants et met en lumière les méthodes utilisées (test d'intrusion TLPT, par exemple).

A.5.6 E-6 Évaluation de la capacité de défense contre les attaques APT

Le service d'évaluation de la capacité de défense contre les attaques APT mesure la résistance d'une organisation à des attaques ciblées tout en menant des formations ciblées sur le courriel et des tests relatifs à l'ingénierie sociale.

A.5.7 E-7 Évaluation de la capacité de traitement des cyberattaques

Le service d'évaluation de la capacité de traitement des cyberattaques confirme si les activités concrètes d'intervention en matière de sécurité basées sur un scénario supposant la survenue d'une attaque peuvent être activées et si l'incident peut être stoppé sans tarder (exercice appelé exercice de réponse à une cyberattaque).

A.5.8 E-8 Conformité aux politiques

Le service de conformité aux politiques prend en charge la vérification de la conformité et le respect de politiques de sécurité prédéfinies.

A.5.9 E-9 Durcissement

Le service de durcissement vise à optimiser la configuration des composants informatiques en vue d'identifier, d'évaluer et d'appliquer des configurations de systèmes de sécurité et d'atténuer voire d'éliminer les risques d'attaques.

A.6 Catégorie F: Collecte, analyse et évaluation des renseignements sur les menaces

A.6.1 F-1 Analyse rétrospective

Le service d'analyse rétrospective décrit la résolution d'un incident pour garantir l'examen et l'amélioration des processus et des outils destinés au personnel du centre de cyberdéfense.

A.6.2 F-2 Collecte et analyse des renseignements sur les menaces internes

Le service chargé de la collecte et analyse des renseignements sur les menaces internes vise à collecter des informations (renseignements internes) portant sur l'analyse en temps réel et l'intervention en cas d'incident.

A.6.3 F-3 Collecte et évaluation des renseignements sur les menaces externes

Le service chargé de la collecte et de l'évaluation des renseignements sur les menaces externes vise à collecter des informations (renseignements externes) telles que les nouvelles vulnérabilités, les tendances en matière d'attaques, le comportement des logiciels malveillants et les adresses IP ou les informations du domaine préjudiciables.

A.6.4 F-4 Rapport relatif aux renseignements sur les menaces

Le service de rapport relatif aux renseignements sur les menaces compile les renseignements sur les menaces internes et externes et les consigne en incluant tous les détails.

A.6.5 F-5 Utilisation des renseignements sur les menaces

Le service d'utilisation des renseignements sur les menaces vise à compiler et diffuser les informations relatives aux menaces pour toutes les catégories d'intervention en matière de sécurité.

A.7 Catégorie G: Développement et maintenance des plates-formes du centre de cyberdéfense

A.7.1 G-1 Mise en œuvre de l'architecture de sécurité

Le service de mise en œuvre de l'architecture de sécurité vise à mettre en œuvre l'architecture de sécurité conçue par la gestion stratégique du centre de cyberdéfense (catégorie A) en utilisant les ressources.

A.7.2 G-2 Exploitation basique des ressources de sécurité des réseaux

Le service d'exploitation basique des ressources de sécurité des réseaux vise à exploiter des dispositifs de réseaux, tels que des pare-feu, des systèmes de détection des intrusions/ systèmes de prévention des intrusions, (IDS/IPS), des applications web de pare-feu (WAF) et des variables de substitution.

A.7.3 G-3 Exploitation avancée des ressources de sécurité des réseaux

Le service d'exploitation avancée des ressources de sécurité des réseaux vise à créer des signatures personnalisées d'une organisation destinées à des produits dotés de capacités de détection des attaques, telles que des systèmes de détection des intrusions ou des systèmes de prévention des intrusions et des applications web de pare-feu, et les applique si la signature fournie par le fournisseur est insuffisante.

A.7.4 G-4 Exploitation basique des ressources de sécurité aux points d'extrémité

Le service d'exploitation basique des ressources de sécurité aux points d'extrémité vise à exploiter des produits de contre-mesure, tels que des logiciels antivirus, aux points d'extrémité.

A.7.5 G-5 Exploitation avancée des ressources de sécurité aux points d'extrémité

Le service d'exploitation avancée des ressources de sécurité aux points d'extrémité vise à détecter l'activité suspecte de programmes aux points d'extrémité au moyen de ses produits de protection, il collecte et analyse le statut des registres, l'exécution des processus, etc. Si nécessaire, le service met en place des indicateurs personnalisés pour faciliter la détection de problèmes aux points d'extrémité.

A.7.6 G-6 Exploitation basique des produits de sécurité en nuage

Le service d'exploitation basique des produits de sécurité en nuage est chargé d'exploiter les services de sécurité en nuage.

A.7.7 G-7 Exploitation avancée des produits de sécurité en nuage

Le service d'exploitation avancée des produits de sécurité en nuage est chargé de créer des signatures personnalisées d'une organisation, destinées à des services de sécurité en nuage capables de détecter des attaques. Si la signature fournie par un fournisseur de système de sécurité s'avère insuffisante, le service utilise les signatures personnalisées.

A.7.8 G-8 Exploitation des outils d'analyse approfondie

Le service d'exploitation des outils d'analyse approfondie consiste à exploiter des outils utilisés lors des analyses approfondies tels que l'expertise légale numérique et l'analyse de logiciels malveillants.

A.7.9 G-9 Exploitation basique de la plate-forme d'analyse

Le service d'exploitation basique de la plate-forme d'analyse vise à exploiter l'infrastructure d'analyse qui stocke les données des journaux et permet l'exécution d'analyses régulières, principalement des analyses en temps réel, telles que la gestion des informations et des événements de sécurité (SIEM).

A.7.10 G-10 Exploitation avancée de la plate-forme d'analyse

Le service d'exploitation avancée de la plate-forme d'analyse vise à réaliser des analyses plus détaillées et plus précises à l'aide des systèmes appartenant à l'organisation en vue de conserver des journaux système et des données provenant de captures de paquets que la gestion commerciale des informations et des événements de sécurité ne peut pas capturer, et développe des algorithmes et des logiques d'analyse personnalisés pour ces données ainsi que le système les supportant.

A.7.11 G-11 Exploitation des systèmes du centre de cyberdéfense

Le service d'exploitation des systèmes du centre de cyberdéfense vise à exploiter les systèmes qui exécutent les tâches requises pour les opérations d'intervention en matière de sécurité, telles que les différents outils de réponse de sécurité décrits précédemment, les réponses aux demandes, et le système de gestion de la vulnérabilité.

A.7.12 G-12 Évaluation des outils de sécurité existants

Le service d'évaluation des outils de sécurité existants vise à vérifier l'impact des autres systèmes et activités, principalement en termes de disponibilité, au moment de la mise à jour ou de la modification des paramètres des outils disposant d'une sécurité activée.

A.7.13 G-13 Évaluation des nouveaux outils de sécurité

Le service d'évaluation des nouveaux outils de sécurité cherche à concevoir et installer de nouvelles ressources de sécurité, si de nouvelles mesures sont nécessaires au niveau des activités de sécurité.

A.8 Catégorie H: Prise en charge de l'intervention en cas de fraude interne

A.8.1 H-1 Prise en charge de l'intervention et de l'analyse en cas de fraude interne

Le service de prise en charge de l'intervention et de l'analyse en cas de fraude interne prend en charge l'organisation qui intervient en cas de fraude interne lorsque celle-ci est découverte, en organisant ses activités à partir des fichiers journaux collectés par les activités de sécurité.

A.8.2 H-2 Prise en charge de la détection de la fraude interne et de la prévention des répétitions

Le service de prise en charge de la détection de la fraude interne et de la prévention des répétitions consiste à analyser les détails des activités de fraude interne qui ont été découvertes, et à déterminer s'il est possible de les déceler à partir des journaux voire, le cas échéant, de mettre en œuvre la logique de détection.

A.9 Catégorie I: Relation active avec les parties externes

A.9.1 I-1 Sensibilisation

Le service de sensibilisation, qui consiste à créer une sensibilisation du personnel compétent à travers et en lien avec le centre de cyberdéfense, encourage l'utilisation des bonnes pratiques, des bons outils, politiques et ressources dans le but d'assurer la protection des ressources de l'entreprise.

A.9.2 I-2 Éducation et formation

Le service d'éducation et formation consiste à prendre en charge les activités de formation spécialisées dans les domaines de la sécurité à destination du personnel des organisations que le centre de cyberdéfense soutient.

A.9.3 I-3 Conseils en matière de sécurité

Le service de conseils en matière de sécurité fournit des prestations de conseil à différentes fonctions d'entreprise dans le domaine de la sécurité.

A.9.4 I-4 Collaboration avec des fournisseurs de systèmes de sécurité

Le service de collaboration avec des fournisseurs de systèmes de sécurité consiste à établir une ligne directe de communication avec le fournisseur d'un produit de sécurité ou d'un service acheté, demande une réponse à toute déficience identifiée dans l'intervention de sécurité et échange les commentaires positifs dans les domaines à améliorer.

A.9.5 I-5 Service de collaboration avec des communautés externes spécialistes de la sécurité

Le service de collaboration avec des communautés externes spécialistes de la sécurité vise à échanger des informations de manière proactive via la participation à des communautés externes. De telles informations peuvent regrouper des réflexions sur les activités liées à la sécurité.

A.9.6 I-6 Rapports techniques

Le service de rapports techniques fournit des rapports de résultat sur les activités de surveillance et de gestion. Les activités contribuent à montrer le niveau de sécurité des systèmes et des infrastructures informatiques.

A.9.7 I-7 Rapports administratifs en matière de sécurité

Le service de rapports administratifs en matière de sécurité produit des rapports périodiques et des analyses statistiques à destination des hauts dirigeants en vue de mettre en lumière le niveau de sécurité et les indicateurs de performance opérationnelle au sein d'une organisation.

Bibliographie

[b-UIT-T X.1053] Recommandation UIT-T X.1053 (2017), *Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la Recommandation UIT-T X.1051 pour les petites et moyennes organisations 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	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, 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, 2021