Forum des équipes d'intervention et de sécurité en cas d'incident, Inc. (FIRST.Org)

Printemps 2016 | 16

Cadre de services de l'Équipe d'intervention en cas d'incident de sécurité (SIRT)

Version 1.0

Cadre de services de la SIRT

Introduction

La présente liste répertorie les services qu'une SIRT (Équipe d'intervention en cas d'incident de sécurité) peut envisager de mettre en œuvre afin de répondre aux besoins de ses parties prenantes, ainsi que les mesures à prendre pour combler leurs lacunes dans ce domaine. Elle regroupe à la fois les services traditionnels offerts par les SIRT et les services apparus récemment, que les équipes et organisations existantes proposent au fur et à mesure de leur évolution. Le présent document recense donc les services devant être couverts par un cadre de services de la SIRT.

Chaque service listé ci-dessous est ventilé par fonction primaire et sous-fonction, qui permettent à une SIRT de fournir ce service dans l'accomplissement de sa mission plus générale. Veuillez noter que, bien que présentées ici de façon distincte, de nombreuses fonctions et sous-fonctions sont utilisées dans la prestation de plusieurs services et/ou fonctions et peuvent être interdépendantes. Si le présent document reconnaît l'existence de ces relations, il ne cherche pas, à ce stade, à les définir.

Les services seront ultérieurement regroupés comme dans une zone de services. Pour le moment, nous nous limiterons toutefois à trois types d'équipes d'intervention en cas d'incident: les CSIRT nationales, les CSIRT sectorielles (infrastructures essentielles) et les CSIRT d'entreprise (organisationnelle). Une version ultérieure de ce présent Cadre de services prendra en compte deux autres types: les Équipes d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT) et les interventions régionales/multipartites en cas d'incident. Des documents complémentaires ultérieurs fourniront des exemples pour chaque type ainsi que les zones de service/services/fonctions servant traditionnellement à l'élaboration d'un programme de base. Un document supplémentaire, qui exposera pour chaque sous-fonction les tâches, les sous-tâches et les actions correspondantes, sera publié en vue de la conception de modules de formation. Le niveau de maturité est également géré de concert avec plusieurs autres parties afin de veiller à l'obtention, à terme, d'un consensus à l'échelle mondiale.

Objectif

Le Cadre de services de la CSIRT définit un ensemble de services et de fonctions qu'une CSIRT exécute pour satisfaire les besoins de ses parties prenantes. Il a pour objectif, en décrivant les services fournis par une CSIRT au moyen d'une terminologie et d'une approche acceptées par la communauté internationale, de faciliter l'interopérabilité de la CSIRT, les activités de renforcement des capacités mondiales ainsi que l'éducation et la formation.

Historique

La liste de services publiée par le CERT/CC a été utilisée dans de nombreux cas comme un descriptif cohérent des CSIRT et de leurs services, permettant d'effectuer des comparaisons. Au cours d'examens récents des listes existantes, il est apparu que la liste du CERT/CC, quoique largement utilisée et adaptée, n'était plus à jour et qu'il lui manquait des composantes essentielles à la mission des CSIRT d'aujourd'hui. Le FIRST, désireux de faciliter le développement international et la maturation des CSIRT, a reconnu que ce projet jouait un rôle fondamental pour cadrer l'élaboration d'un programme de formation complet destiné aux CSIRT. Étant donné la diversité géographique et fonctionnelle des membres du FIRST, il a été estimé que la communauté qu'il rassemble serait une source appropriée en mesure d'inventorier et de répertorier les services fournis par les CSIRT. Il a également été reconnu qu'une approche similaire était nécessaire pour les services proposés par les PSIRT. Celle-ci figurera donc dans une prochaine version de ce Cadre de services.

Définitions

Nous donnons ci-après une définition de certains termes utilisés dans le présent document. Veuillez noter que les termes «zones de service», «services» et «fonctions» désignent *ce qui est fait* à différents niveaux de détails, tandis que les mots «tâches» et «actions» servent à décrire, à différents niveaux de détails aussi, *comment* ces activités sont réalisées. Les tâches et les actions sont exposées dans un document complémentaire. Elles peuvent être/seront mises à jour plus fréquemment:

- **Zone de service** – Groupe de services liés à un aspect commun. Une zone de service permet d'organiser les services selon une classification de haut niveau et facilite ainsi leur compréhension. (Cette notion sera davantage développée dans la version 2.0.)
- **Service** – Ensemble d'actions identifiables et homogènes visant l'obtention d'un résultat précis en faveur ou pour le compte de la partie prenante d'une équipe d'intervention en cas d'incident. Liste des fonctions utilisées pour mettre en œuvre le service.
- **Fonction** – Outil servant à réaliser l'objectif ou la tâche d'un service en particulier. Liste des tâches qui peuvent être accomplies dans le cadre de la fonction.
- **Tâches** – Liste des actions qui doivent être menées pour accomplir la tâche.

- **Actions** – Description à divers niveaux de détail/maturité du processus suivi pour parvenir à un résultat.

- **Capacité** – Activité mesurable qui relève des rôles et responsabilités d'une organisation. Dans le cadre de services de la SIRT, les capacités peuvent être définies soient en termes de services, soit en termes de fonctions, sous-fonctions, tâches ou actions requises.

- «**Capabilité»** – Nombre d'occurrences simultanées d'une capacité donnée dans un processus qu'une organisation peut exécuter avant d'épuiser d'une façon ou d'une autre ses ressources.

- **Maturité** – Degré d'efficacité avec lequel une organisation concrétise une capacité donnée dans le cadre de sa mission et de ses pouvoirs. C'est un niveau de maîtrise atteint soit dans les actions et les tâches, soit dans un groupe de fonctions ou de services.

Catégories d'équipes d'intervention en cas d'incident:

- CSIRT nationale (équipe d'intervention en cas d'incident informatique) – Entité constituée par une autorité nationale afin de coordonner sur le plan national la gestion des incidents dans le domaine de la cybersécurité. Elle est généralement composée de l'ensemble des ministères et agences du gouvernement, les organismes chargés de l'application des lois et la société civile. Il s'agit aussi habituellement de l'interlocuteur privilégié des CSIRT nationales d'autres pays ainsi que des acteurs régionaux et internationaux.

- CSIRT sectorielle (infrastructures essentielles) – Équipe chargée du suivi et de la gestion et du traitement des incidents dans le domaine de la cybersécurité qui touchent un secteur spécifique (par ex. l'énergie, les télécoms, la finance).

- CSIRT d'entreprise (organisationnelle) – Généralement, équipe chargée du suivi, de la gestion et du traitement des incidents dans le domaine de la cybersécurité qui touchent les infrastructures et les services TIC d'une organisation en particulier.

- CSIRT régionale/multipartite – Équipe dirigée par un ou plusieurs chefs chargée du suivi, de la gestion et du traitement des incidents dans le domaine de la cybersécurité qui touchent une région en particulier ou un certain nombre d'organisations.

- Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT) – Équipe implantée au sein d'une entreprise commerciale (traditionnellement un fournisseur) et chargée de la gestion des informations (réception, enquête, élaboration de rapports internes ou publics) relatives aux failles de sécurité liées aux produits ou aux services commercialisés par cette organisation.

Service 1 Gestion des incidents

Fonction 1.1 **Traitement des incidents:** services relatifs à la gestion des cyberincidents qui consistent notamment à prévenir les parties prenantes et à coordonner les activités de réaction, d'atténuation et de rétablissement. Le traitement des incidents est étroitement lié aux activités d'analyse, qui sont définies dans la partie «Analyses».

Sous-fonction 1.1.1 **Collecte d'informations:** services relatifs au recueil, au classement et au stockage d'informations liées aux événements et incidents, notamment:

- **Collecte de rapports d'incident:** collecte de rapports d'incidents et de rapports sur des événements malveillants ou suspects auprès de parties prenantes et de tierces parties (p. ex. autres équipes de sécurité ou organismes de diffusion de renseignements commerciaux), accessibles en lecture manuelle ou automatique.
- **Collecte de données numériques:** compilation et classement de données numériques qui pourraient, sans garantie toutefois, être utiles pour comprendre les incidents (p. ex. images sur disque, dossiers, flux/registres de réseaux).
- **Autres types de données (non numériques):** compilation et classement de données non numériques (fiches de présence papier, diagramme d'architecture, modèles économiques, données relatives à l'évaluation d'un site, politiques, cadres de gestion des risques dans l'organisation, etc.).
- **Collecte d'artefacts:** processus techniques et opérationnels consistant à recueillir, classer, archiver et rechercher des artefacts soupçonnés être des vestiges d'une activité adverse.
- **Collecte de preuves:** activité consistant à rassembler des informations et des données à des fins d'exécution de la loi, qui consiste souvent à recueillir des métadonnées relatives à la source, à la méthode de collecte et au propriétaire, ainsi qu'aux informations protégées.

Sous-fonction 1.1.2 **Réaction**: services visant à réduire les effets d'un incident et à rétablir les fonctions opérationnelles des parties prenantes.

- **Endiguement:** arrêt immédiat des préjudices et limitation de la portée de l'activité malveillante au moyen de mesures tactiques à court terme (p. ex. blocage ou filtrage du trafic); il peut aussi s'agir de retrouver la maîtrise des systèmes.
- **Atténuation:** prévention d'éventuels préjudices additionnels grâce à des mesures d'éradication et de contournement, ou par la mise en œuvre de stratégies d'endiguement plus approfondies et plus complètes.
- **Dépannage:** modification du domaine, de l'infrastructure ou du réseau affecté en vue de les réparer et d'empêcher ce type d'activités de se reproduire. Il s'agit entre autres de renforcer les défenses de l'organisation et son état de préparation par la modification des politiques et par des formations et des cours supplémentaires.
- **Rétablissement:** restauration de l'intégrité des systèmes touchés et récupération de l'état opérationnel, non dégradé des données, systèmes et réseaux affectés.

Sous-fonction 1.1.3 **Coordination**: activité de partage d'information et de conseil, à l'intérieur comme à l'extérieur de la CSIRT. La coordination est généralement nécessaire lorsque la CSIRT dépend d'une expertise et de ressources qui ne sont pas sous son contrôle direct pour réaliser les actions nécessaires à l'atténuation d'un incident. En offrant des services de coordination bilatérale ou multilatérale, la CSIRT participe à un échange d'informations qui permet aux ressources ayant les capacités d'agir de le faire ou d'aider leurs pairs à détecter les activités des adversaires, à s'en protéger ou à y remédier.

Sous-fonction 1.1.4 **Suivi des incidents**: recensement des informations relatives aux mesures prises en vue de résoudre un incident, y compris les informations essentielles collectées, les analyses réalisées, les mesures de correction et d'atténuation appliquées, l'achèvement et la résolution.

Fonction 1.2 **Vulnérabilité, configuration et gestion des actifs:** services destinés à comprendre et à corriger les vulnérabilités, les questions de configuration et l'inventaire des actifs.

Sous-fonction 1.2.1 **Recherche des vulnérabilités**: identification de nouvelles vulnérabilités grâce à la recherche et à l'expérimentation (p. ex. test à données aléatoires et rétro-ingénierie).

Sous-fonction 1.2.2 **Signalement des vulnérabilités**: processus opérationnels et techniques consistant à rassembler, classer, archiver et suivre les rapports de vulnérabilité.

Sous-fonction 1.2.3 **Coordination des vulnérabilités**: vise à informer les organisations concernées concernant l'existence d'une vulnérabilité en vue d'effectuer les réparations nécessaires et de limiter les répercussions éventuelles.

Sous-fonction 1.2.4 **Correction des causes primaires de vulnérabilité:** mise en œuvre des mesures correctives formelles nécessaires pour remédier à une vulnérabilité identifiée. Traditionnellement effectuée par le fournisseur du produit.

Service 2 Analyse

Fonction 2.1 **Analyse d'incident:** services destinés à identifier et caractériser les informations relatives à des événements ou des incidents telles que la portée, les parties touchées, les systèmes impliqués, la chronologie (découverte, occurrence, établissement d'un rapport), l'état d'avancement (en cours ou achevé).

Remarque: l'analyse d'un incident est approfondie à l'occasion d'examens plus ciblés tels que ceux portant sur les artefacts, les erreurs de configuration, la vulnérabilité, le réseau ou les informations criminalistiques.

Sous-fonction 2.1.1 **Validation d'incident**: vise à vérifier de façon probante qu'un incident signalé a bel et bien eu lieu et qu'il a affecté les systèmes touchés.

Objectif: fournir des preuves techniques attestant qu'un événement est un incident de sécurité ou une panne de réseau ou de matériel, et identifier les effets et les préjudices potentiels en termes de sécurité sur la confidentialité, la disponibilité et/ou l'intégrité du patrimoine informationnel.

***Résultat**: déterminer si un événement signalé est bel et bien un incident qui doit être traité, ou si le rapport peut être enregistré dans les systèmes correspondants et clôturé sans suite. Collecter des renseignements relatifs aux circonstances qui ont conduit la partie prenante à croire à l'existence d'un incident de sécurité et déterminer l'existence d'une intention malveillante ou si l'événement peut s'expliquer par la présence d'autres facteurs (mauvaise configuration ou panne matérielle).*

Sous-fonction 2.1.2 **Analyse d'impact**: permet d'identifier et de caractériser l'impact subi par la fonction opérationnelle que sous-tendent les systèmes touchés.

Objectif: déterminer la taille et l'ampleur de l'incident en répertoriant les éléments affectés liés à l'infrastructure, aux services, aux données, aux départements ou à l'organisation. Une stratégie générale de correction peut être élaborée sur la base de cette analyse.

***Résultat**: évaluer le préjudice (potentiel) qu'un incident a causé ou pourrait causer. Identifier non seulement les aspects techniques, mais aussi les préjudices subis en termes de couverture médiatique, perte de confiance ou de crédibilité, atteinte à la réputation.*

Sous-fonction 2.1.3 **Enseignements tirés**: réflexion menée après l'application des mesures afin d'identifier les améliorations devant être apportées aux processus, politiques, procédures, ressources et outils dans le but de faciliter l'atténuation et de prévenir de futurs dangers.

Objectif: déterminer les défaillances, mettre en place des mesures préventives et partager les enseignements tirés avec les professionnels de la sécurité au moyen de publications et de présentations.

***Résultat**: ensemble de recommandations envisagées comme des modifications éventuelles des systèmes d'information, des processus et des procédures au sein des départements concernés dans l'organisation touchée.*

Fonction 2.2 **Analyse des artefacts:** services destinés à comprendre les capacités des artefacts (p. ex. logiciels malveillants, exploitations des failles de sécurité, spams et fichiers de configuration) et leur but, ainsi que leur introduction, leur détection et leur neutralisation.

***Objectif:** dans le cadre du processus de traitement de l'incident, les artefacts numériques peuvent se trouver dans les systèmes affectés ou sur les sites de distribution de logiciels malveillants. Il peut s'agir parfois des vestiges d'une attaque, comme des scripts, des fichiers, des images, des fichiers de configuration, des outils, les résultats d'un outil, des journaux, etc. L'analyse des artefacts vise à déterminer la manière dont ils ont été utilisés par l'intrus, de façon à s'introduire dans les systèmes et les réseaux de l'organisation, ou s'attache à comprendre les agissements de l'intrus une fois à l'intérieur du système. L'analyse des artefacts s'efforce de comprendre comment ces derniers opèrent, que ce soit de façon isolée ou en conjonction avec d'autres éléments. On y parvient en recourant à différentes techniques, comme l'analyse de surface, la rétro-ingénierie, l'analyse de l'exécution et l'analyse comparative. Chaque technique apporte son lot d'informations sur l'artefact. Les méthodes d'analyse consistent entre autres à identifier le type et les caractéristiques d'un artefact, à le comparer à d'autres artefacts connus, à en observer l'exécution dans un environnement spécifique ainsi qu'à désassembler et interpréter les artefacts binaires. Les analystes procédant à ce type d'examen essaient de reconstruire et d'identifier les agissements de l'intrus, de façon à évaluer les préjudices, à élaborer des solutions permettant d'en atténuer les effets et à fournir des informations aux parties prenantes et aux autres chercheurs.*

***Résultat:** comprendre la nature d'un artefact numérique retrouvé ainsi que ses relations avec d'autres artefacts, attaques et exploitations des failles. Identifier des solutions permettant de circonscrire l'action des artefacts analysés en comprenant les tactiques, techniques et procédures utilisées par les intrus pour mettre en péril les systèmes et les réseaux et poursuivre leurs activités malveillantes.*

Sous-fonction 2.2.1 **Analyse de surface**: consiste à identifier et caractériser les informations de base et les métadonnées relatives aux artefacts (type de fichier, sortie de chaînes, hachage de chiffrement, taille de fichier, nom de fichier) ainsi qu'à examiner toutes les informations, publiques ou privées, ayant trait à la source de ces artefacts.

Objectif: *l'analyse de surface, qui constitue la première étape du processus de recueil des informations de base, compare les informations collectées sur l'artefact à d'autres artefacts publics ou privés et/ou recueils de signatures. Toutes les informations connues (préjudice potentiel, fonctionnalités et atténuation) sont rassemblées et analysées. Des analyses supplémentaires sont parfois nécessaires en fonction de l'objectif de l'analyse en cours.*

Résultat*: identification des caractéristiques et/ou de la signature de l'artefact numérique et de toute autre information déjà connue à son sujet, y compris sa dangerosité, ses effets et les mesures d'atténuation[1]. (Ces informations peuvent servir lors des étapes suivantes.)*

Sous-fonction 2.2.2 **Rétro-ingénierie**: analyse statique approfondie d'un artefact visant à déterminer l'ensemble de ses fonctionnalités, quel que soit l'environnement dans lequel il est exécuté.

Objectif: *réaliser une analyse plus détaillée des artefacts de façon à identifier les effets cachés et les facteurs de déclenchement. La rétro-ingénierie permet à l'analyste de contourner les techniques d'obfuscation et de compilation (artefacts binaires) afin d'identifier le programme, le script ou le code utilisé pour donner corps au logiciel malveillant, en décodant le code source ou en désassemblant le binaire pour le convertir en langage assembleur et l'interpréter. Le décodage de l'ensemble du langage machine dévoile les fonctions et les actions du logiciel malveillant. La rétro-ingénierie est une analyse approfondie qui est réalisée quand les analyses de surface et de l'exécution ne permettent pas d'obtenir les informations requises.*

Résultat*: déterminer l'ensemble des fonctionnalités d'un artefact numérique de façon à comprendre comment il opère, ce qui le déclenche, les failles exploitables du système, l'ensemble de ses effets et les dégâts qu'il peut occasionner, et pouvoir ainsi élaborer des solutions d'atténuation et, si besoin est, créer une nouvelle signature pour effectuer une comparaison avec d'autres échantillons.*

Sous-fonction 2.2.3 **Analyse de l'exécution**: permet de comprendre les capacités d'un artefact en l'observant lors de son exécution dans un environnement réel ou émulé (p. ex. carré, environnement virtuel et émulateurs matériels ou logiciels).

Objectif: *comprendre en détail le fonctionnement d'un artefact. Le recours à un environnement simulé permet de répertorier les modifications provoquées par l'exécution sur l'hôte, le trafic du réseau et les résultats. L'objectif principal est d'observer de près l'artefact à l'œuvre, dans une situation aussi proche que possible de la réalité.*

Résultat*: récolter davantage de détails sur le fonctionnement de l'artefact numérique en observant son comportement durant l'exécution, de façon à identifier les modifications apportées au système hôte et d'autres interactions éventuelles avec le système, ainsi que les répercussions sur le trafic du réseau, dans le but de mieux comprendre les altérations et les effets subis par le système, créer de nouvelles signatures pour l'artefact et déterminer des mesures d'atténuation. (Remarque: l'analyse de l'exécution ne laisse pas apparaître toutes les fonctionnalités de l'artefact, car toutes ses sections de code n'ont pas forcément été activées. Elle permet à l'analyste de voir uniquement l'action du logiciel malveillant en situation de test, mais pas tout ce qu'il est capable de faire.)*

Sous-fonction 2.2.4 **Analyse comparative**: destinée à identifier les fonctionnalités et les intentions communes, y compris l'examen par famille d'artefacts recensés.

Objectif: *étudier les relations entre plusieurs artefacts. Cette analyse dévoile parfois des similitudes dans le code (modus operandi), les cibles, l'intention et les auteurs. Ces similitudes peuvent servir à évaluer la portée d'une attaque (la cible est-elle plus importante qu'anticipé? Le même code a-t-il déjà été utilisé?). L'analyse comparative recourt à des techniques telles que les comparaisons de concordance exacte ou de similarité de code. Elle apporte un éclairage sur la façon dont un artefact, ou des versions similaires, a été utilisé et modifié dans le temps, et permet ainsi de mieux comprendre l'évaluation d'un logiciel malveillant ou d'autres types d'artefact.*

Résultat*: recenser les points communs ou les relations avec d'autres artefacts en vue d'identifier des tendances ou des similarités qui permettront de mieux saisir les fonctionnalités et les effets d'un artefact numérique, ainsi que la façon d'en atténuer l'action.*

Fonction 2.3 **Analyse du support physique**: services consistant à analyser des données pertinentes fournies par les systèmes, les réseaux, le stockage numérique et les supports amovibles en vue de mieux comprendre comment empêcher, détecter et/ou atténuer les incidents similaires ou connexes. Ces services peuvent fournir des informations utiles pour des examens juridiques, criminalistiques ou de conformité, ou d'autres bilans historiques.

Objectif: *collecter et analyser des données probantes fournies par les supports physiques tels que disques durs, dispositifs mobiles, supports de stockage amovibles, stockage dans le nuage ou autres formats comme le papier et la vidéo. Si les résultats de l'analyse doivent être produits dans un contexte juridique ou de mise en conformité, les informations devront être collectées dans le respect des normes de procédure judiciaire qui garantissent l'intégrité et le maintien de la continuité des preuves. Les preuves sont variées. Il peut s'agir d'un artefact, tel un logiciel malveillant abandonné, d'une modification de l'état des fichiers, registres ou autres composantes du système, de captures du trafic réseau ou d'autres fichiers journaux ou informations en mémoire. Veuillez noter que l'analyse du support physique a pour but de trouver des preuves de ce qu'il s'est passé et éventuellement d'identifier les responsables; elle diffère de l'analyse d'artefact, qui est destinée à comprendre un artefact donné et ses relations. Cela étant dit, les techniques d'analyse d'artefact peuvent être utilisées dans le cadre de l'analyse des supports techniques. Les services d'analyse de support technique peuvent aussi être sollicités en dehors d'un incident informatique, en rapport avec des questions relatives aux ressources humaines ou avec des enquêtes juridiques ou organisationnelles.*

Résultat: *présenter des résultats qui 1) dressent l'inventaire du patrimoine informationnel (les éléments de propriété intellectuelle ou d'autres informations sensibles trouvées); 2) retracent une chronologie des événements qui puisse mettre en évidence les ajouts, les altérations et les suppressions subis par tous les supports physiques affectés par l'incident et, si possible, en identifier la cause, mais aussi montrer comment l'ensemble des preuves s'articulent pour expliquer l'étendue et les effets de l'incident.*

Fonction 2.4 **Analyse de la vulnérabilité/de l'exploitation des failles:** services fournis en vue de comprendre plus en détail les vulnérabilités qui ont contribué au cyberincident.

Sous-fonction 2.4.1 **Analyse de la vulnérabilité technique (logiciels malveillants)/de l'exploitation des failles**: comprendre la ou les faiblesse(s) exploitée(s) en vue de provoquer l'incident et les techniques adverses utilisées à cette fin.

Objectif: informer les parties prenantes de toutes les vulnérabilités connues (points d'entrée communs des attaquants) de façon à ce que les systèmes soient mis à jour et surveillés en vue d'empêcher toute exploitation des failles de sécurité et de minimiser les préjudices subis.

***Résultat**: acquérir une compréhension parfaite de la vulnérabilité et de la façon dont des agents malveillants pourraient la mettre à profit en vue d'infiltrer/exploiter les systèmes.*

Sous-fonction 2.4.2 **Analyse des causes primaires**: vise à comprendre la défaillance, qu'elle relève de la «conception» ou de la «mise en œuvre», qui a favorisé l'attaque.

Objectif: identifier la cause primaire et le point faible en vue de faciliter la résolution complète du problème.

***Résultat**: appréhender de façon précise les facteurs qui autorisent l'existence d'une faille et les circonstances dans lesquelles un attaquant peut ainsi l'exploiter.*

Sous-fonction 2.4.3 **Analyse correctrice:** vise à comprendre les étapes nécessaires pour corriger la défaillance sous-jacente qui a rendu l'attaque possible, et empêcher ce genre d'attaque à l'avenir.

Objectif: identifier le problème qui a favorisé l'émergence d'un point faible, corriger la faille, modifier une procédure ou une caractéristique, faire examiner la correction par un tiers et repérer toute nouvelle vulnérabilité introduite par les mesures correctrices.

***Résultat**: mettre en place un programme d'amélioration des processus, infrastructures et caractéristiques de façon à annihiler un vecteur spécifique d'attaque et empêcher ainsi ce type d'attaque de se reproduire.*

Sous-fonction 2.4.4 **Analyse d'atténuation**: vise à déterminer les moyens d'atténuer (empêcher) les risques résultant d'une attaque ou d'une vulnérabilité sans nécessairement corriger la défaillance sous-jacente à l'origine du problème.

Service 3 Garantie des informations

Fonction 3.1 **<u>Évaluation des risques/de la conformité</u>:** services relatifs à l'évaluation des risques ou aux activités d'évaluation de la conformité. Il peut s'agir de réaliser l'évaluation elle-même ou de contribuer à l'examen des résultats d'une évaluation. Ces services sont généralement fournis en vue de respecter des normes de conformité (p. ex. ISO 27XXX, COBIT).

Objectif: améliorer l'identification des opportunités et des menaces; améliorer les contrôles; améliorer la prévention des pertes et la gestion des incidents en rapport avec la sécurité des informations et d'autres fonctions pertinentes.

Résultat: **cohérence du processus d'évaluation et de gestion des risques liés à l'information appliqué aux ressources et données essentielles; contribution à l'évaluation des risques; sélection de solutions appropriées pour le traitement des risques contenant des mesures de gestion des incidents et l'intervention de la criminalistique, le cas échéant.**

Sous-fonction 3.1.1 **Inventaire des ressources/données essentielles**: identification des ressources et des données qui jouent un rôle essentiel dans l'accomplissement de la mission de l'organisation. Ces ressources et données ne sont pas forcément la propriété de l'organisation (elles peuvent appartenir p. ex. à un fournisseur de services en nuage ou à un ensemble de données externe). L'inventaire comprend également l'identification de leur localisation, de leur propriétaire, de leur niveau de sensibilité informationnelle, de leur fonction en rapport avec la mission et de leur état/niveau actuel.

Objectif: identifier régulièrement les ressources et les données pouvant nécessiter une gestion des incidents afin de permettre à l'organisation de mener à bien sa mission en conjonction avec les secteurs d'activité impliqués.

Résultat: *un inventaire, une liste ou une base de données régulièrement actualisé(e) qui recense les ressources et données essentielles, dont l'organisation se sert aux fins d'évaluation des risques.*

Sous-fonction 3.1.2 **Détermination des critères d'évaluation**: se doter de la ou des politique(s) de gestion des risques ainsi que des normes listées/identifiées auprès de la direction afin d'évaluer le niveau/l'état de la sécurité. Soumettre aux gestionnaires des risques et au Responsable en chef de la sécurité des données (CISO) des critères d'évaluation ou de comparaison. Citons quelques exemples de normes: Bâle II, COBIT, ITIL, normes de certification et d'accréditation.

Objectif: faciliter le choix d'une méthode approuvée d'évaluation des risques liés à l'information qui sera utilisée au sein de l'organisation, et contribuer à l'évaluation et à la gestion des risques au niveau de l'organisation.

Résultat: *choix d'une méthode d'évaluation des risques liés à l'information qui sera utilisée au sein de l'organisation tout entière; validation du choix et adhésion par la direction; adoption de politiques imposant à l'échelle de l'organisation l'utilisation de la méthode choisie quand cela est approprié; adoption de mesures, modèles et résultats; adoption de processus et procédures d'évaluation des risques liés à l'information; adoption de mécanismes destinés à prendre en compte les résultats de l'évaluation des risques liés à l'information dans la gestion des risques et les prises de décision au niveau de l'organisation.*

Sous-fonction 3.1.3 **Réalisation d'une évaluation**: aide à la réalisation d'examens et à la participation aux évaluations afin de veiller à ce que les exigences en matière de risque et de sécurité soient respectées.

Objectif: réaliser, pour une sélection de ressources et données essentielles, l'évaluation des risques liés à l'information au moyen de la méthode approuvée, le plus minutieusement possible.

Résultat: *une évaluation des risques liés à l'information pour une sélection de ressources et de données essentielles.*

Sous-fonction 3.1.4 **Résultats et recommandations**: obtenir et présenter des résultats, des rapports et/ou des recommandations (p. ex. rédaction de rapports en utilisant les tâches liées à la publication de l'information).

Objectif: faciliter la documentation détaillée des résultats d'une évaluation des risques, et énumérer les mesures à prendre et les recommandations à envisager.

Résultat: *un rapport autorisé et approuvé qui présente en détail les ressources ou les données essentielles évaluées, la procédure suivie pour l'évaluation des risques, les données utilisées dans le cadre de cette évaluation, les résultats obtenus, les recommandations, les actions, les programmes et les calendriers de distribution.*

Sous-fonction 3.1.5 **Suivi**: aider le CISO et/ou le gestionnaire des risques à réaliser le suivi de l'état des évaluations et de la mise en œuvre consécutive des recommandations.

Objectif: garantir la mise en œuvre de l'ensemble des programmes, actions et recommandations dans les délais fixés.

Résultat: *mise à jour régulière des programmes et des calendriers; liste des actions menées à terme; révision des calendriers si les actions n'ont pas été achevées à temps; rapport d'avancement au vu des programmes et des calendriers.*

Sous-fonction 3.1.6 **Test**: évaluation active du respect des niveaux de risque, qui comprend notamment des tests d'intrusion, des analyses et évaluations des vulnérabilités, des tests d'application, des audits et vérifications.

Objectif: s'assurer, en procédant à des tests, que les traitements choisis et appliqués conviennent aux objectifs poursuivis, qu'ils sont mis en œuvre correctement et qu'ils permettent d'atténuer les risques dans la mesure escomptée.

Résultat: *un programme de tests détaillé mentionnant les résultats attendus; le détail des tests et des résultats obtenus; une comparaison avec les résultats attendus; des actions, accompagnées d'un calendrier, destinées à corriger les écarts par rapport aux attentes.*

Fonction 3.2 **Gestion des correctifs:** services fournissant aux parties prenantes les capacités nécessaires pour gérer l'identification du stock, les systèmes à corriger, le déploiement et la vérification de la mise en place des correctifs.

Objectif: faciliter l'identification, l'acquisition, l'installation et la vérification des correctifs pour les produits et les systèmes, et fournir une évaluation de l'utilité et de l'impact des correctifs sous l'angle de la gestion des incidents.

Résultat: *prise de conscience et compréhension par l'organisation des correctifs nécessaires; compréhension des correctifs devant être appliqués par les prestataires de services;*

compréhension de l'impact des correctifs sur les risques liés à l'information; compréhension de l'impact sur la gestion des incidents.

Fonction 3.3 **Gestion des politiques d'exploitation**: services destinés à élaborer, actualiser, institutionnaliser et faire respecter les concepts relatifs au fonctionnement de l'organisation et d'autres politiques.

Objectif: jouer le rôle, auprès d'une partie prenante ou d'un secteur d'activité, de conseiller de confiance en matière de continuité des activités et de retour à la normale après une catastrophe, en fournissant des conseils objectifs et factuels, qui tiennent compte de l'opportunité ou du problème à l'étude, du contexte dans lequel ce conseil peut servir et de toutes les contraintes de ressources envisageables.

Résultat: *des décisions managériales qui tiennent compte de la continuité des activités et du retour à la normale après une catastrophe; la gestion des incidents envisagée comme une source de conseils fiables; participation des membres de l'équipe de gestion des incidents aux décisions managériales quand et où cela est approprié.*

Fonction 3.4 **Conseils en matière d'analyse des risques/continuité des activités/retour à la normale après une catastrophe:** services fournis aux parties prenantes et relatifs aux activités de résilience de l'organisation en fonction des risques identifiés. Ils englobent tout un éventail d'activités liées à la gestion des risques, depuis la conduite de l'évaluation elle-même jusqu'à la fourniture d'une assistance (étude et relativisation des résultats d'une évaluation).

Objectif: jouer le rôle, auprès d'une partie prenante ou d'un secteur d'activité, de conseiller de confiance en matière de sécurité des informations et de gestion des incidents, en fournissant des conseils objectifs et factuels qui tiennent compte de l'opportunité ou du problème à l'étude, de l'environnement dans lequel ces conseils peuvent servir et de toutes les contraintes de ressources envisageables.

Résultat: *des décisions managériales qui tiennent compte de la sécurité des informations et de la gestion des incidents; une gestion des incidents considérée comme une source de conseils fiables; participation des membres de l'équipe de gestion des incidents aux décisions managériales quand et où cela est approprié.*

639

640 Fonction 3.5 **Conseils en matière de sécurité**: services fournissant à une partie prenante ou à
641 un secteur d'activité des conseils relatifs à l'exécution et à la mise en œuvre d'opérations ou de
642 fonctions pertinentes en matière de sécurité.
643

Service 4 Appréciation de la situation

Objectif: ce service regroupe un ensemble d'activités qui permet à l'organisation de mieux apprécier son environnement. Il consiste notamment à identifier les éléments critiques pouvant affecter la mission de l'organisation, à surveiller ces éléments et à utiliser cette connaissance à l'appui du processus décisionnel et d'autres actions.

Résultat: *permet d'apprécier à leur juste valeur les événements et les activités, à l'intérieur et à l'extérieur de l'organisation, susceptibles d'affecter sa capacité à mener ses activités dans les délais impartis et en toute sécurité.*

Fonction 4.1 **Activités de détection/mesure:** services axés sur l'élaboration, le déploiement et l'exploitation de systèmes et de méthodes d'analyse destinés à identifier les activités à étudier.

Objectif: créer les infrastructures et les processus de collecte des informations nécessaires pour que l'organisation puisse apprécier sa situation.

Résultat: *une infrastructure de collecte des informations (détecteurs) à l'échelle de l'organisation qui fournit des renseignements pour apprécier la situation.*

Sous-fonction 4.1.1 **Détermination des besoins**: comprendre les besoins des parties prenantes et obtenir les autorisations dans le cadre desquelles la CSIRT peut exercer ses activités.

Objectif: le processus de détermination des besoins identifie les besoins de l'organisation en matière d'appréciation de la situation, puis établit le lien entre ces besoins et la nature des informations requises pour y répondre.

Résultat: *comprendre, d'un point de vue informationnel, le niveau d'appréciation requis pour l'organisation et ses parties prenantes. Veiller en outre à ce que l'organisation possède toutes les autorisations politiques et légales pour collecter les informations.*

Sous-fonction 4.1.2 **Identification des données requises**: déterminer les données requises pour répondre aux besoins.

Objectif: il existe toutes sortes de détecteurs, depuis le système automatisé jusqu'à l'être humain. Ces sources d'information (données) sont utilisées pour dresser un panorama de la perception globale de la situation de l'organisation. Le processus d'«identification des données requises» établit le lien entre les besoins en termes d'appréciation de la situation et les sources potentielles d'information (c'est-à-dire les détecteurs).

Résultat: *identification des données requises pour répondre aux besoins de l'organisation en matière d'appréciation de la situation. Si certaines sources de données existent déjà, il pourra s'avérer nécessaire d'en concevoir ou d'en acquérir d'autres.*

Sous-fonction 4.1.3 **Méthodes d'acquisition des données**: déterminer les méthodes, outils, techniques et technologies mobilisés pour rassembler les données requises.

Objectif: ce processus identifie les méthodes de collecte, de traitement et de stockage des informations (données) collectées.

Résultat: *déterminer dans les moindres détails la façon dont les informations seront collectées, stockées, traitées et assainies.*

Sous-fonction 4.1.4 **Gestion des détecteurs**: entretien et amélioration constante des performances des détecteurs en rapport avec les besoins définis.

Objectif: entretenir et surveiller les détecteurs pour garantir leur bon fonctionnement et leur exactitude.

Résultat: *mise en œuvre d'un programme de gestion et d'entretien des détecteurs tout au long de leur cycle de vie.*

Sous-fonction 4.1.5 **Gestion des résultats**: tri et diffusion des informations et des indicateurs obtenus grâce aux détecteurs. Habituellement réalisé grâce à un tableau de bord, visible par plusieurs niveaux au sein de l'organisation.

Fonction 4.2 **Fusion/Corrélation:** services consistant à réaliser des analyses intégrant des sources de données multiples. Capte tous les flux d'informations, quelle qu'en soit la source, et les intègre à une vision d'ensemble de la situation (appréciation de la situation).

Objectif: identifier de nouvelles relations entre les incidents, les indicateurs et les acteurs, lesquels permettront d'améliorer les mesures d'atténuation ou l'intervention en cas d'incident lié à la sécurité.

Résultat*: adoption dans l'organisation d'un processus cohérent visant à exploiter toute nouvelle information relative à une menace et à l'intégrer aux informations figurant déjà dans le patrimoine de connaissances de l'organisation. Le résultat final de ce processus sera l'obtention d'un ensemble d'informations élargi qui permettra à la CSIRT de prendre des décisions avec davantage d'efficacité et de précision.*

Sous-fonction 4.2.1 **Détermination des algorithmes de fusion**: déterminer les méthodes et les techniques (algorithmes) ou les technologies mobilisées pour analyser (fusionner) les informations.

Objectif: dans le cadre du traitement des incidents, il est important que la CSIRT conserve une bonne vision opérationnelle des informations provenant de sources diverses. La fusion permet une gestion des informations qui autorise la CSIRT à intégrer rapidement de nouvelles données, dès leur réception, et à les contextualiser entièrement de façon à ce qu'elles soient exploitables durant le processus de traitement de l'incident.

***Résultat**: élaborer un processus interne qui permet l'intégration de nouvelles informations, leur évaluation dans le contexte des informations existantes et l'exploitation fructueuse par la CSIRT de ce nouvel ensemble agrégé d'informations, en cas d'incident.*

Sous-fonction 4.2.2 **Analyse de fusion**: analyse (fusion) des sources de données à l'aide des données présentes dans le système de gestion des connaissances afin d'identifier les éléments communs et les liens entre les données.

Objectif: dans le cadre du traitement des incidents, la CSIRT devra maintenir en permanence une bonne compréhension de la menace que fait peser un incident spécifique sur l'organisation. Pour y parvenir, il lui faudra se tenir au courant de l'incident lui-même mais aussi de l'évolution des tactiques, techniques et procédures exploitées par l'adversaire. Elle devra constamment rassembler de nouvelles informations et les évaluer au regard des informations existantes. La sous-fonction 4.2.2 utilisera les algorithmes de fusion choisis dans la sous-fonction 4.2.1 pour analyser les informations ayant trait aux menaces et provenant de sources externes.

***Résultat**: comprendre comment les nouvelles informations sur les menaces affectent les incidents existants, et bien préparer l'organisation à toute modification de tiers de confiance par un adversaire ou lui permettre de mettre constamment à jour ses techniques d'atténuation et de réaction afin de mieux traiter les incidents connexes.*

Fonction 4.3 **Développement et conservation des renseignements de sécurité:** services fournis à des parties prenantes internes ou externes en vue de développer et de conserver des sources tierces de renseignements de sécurité. Il s'agit d'informations portant sur les menaces ou la sécurité nécessaires à la conduite des opérations ou à la gestion des menaces. Ces services comprennent, entre autres, l'analyse, le développement, la diffusion et la gestion des renseignements de sécurité, tels qu'indicateurs de menace, logique de détection des menaces (règles et signatures anti-logiciel malveillant) et les tactiques, techniques et procédures des adversaires. Ils dépendent des activités d'échange d'informations, définies dans la partie 5.6 «Sensibilisation/communications».

Objectif: les informations provenant d'entités externes sont essentielles pour apprécier la situation de façon suffisamment précise. Une CSIRT a besoin d'une grande quantité d'informations de haute qualité ayant directement trait à ses activités. Mais le coût et le volume de travail nécessaires pour y parvenir sont tels qu'il faut cibler un ensemble de sources soigneusement choisies.

Résultat: *des informations diverses et de grande qualité couvrant tous les domaines d'activité pertinents de la CSIRT sont ingérées, principalement au moyen de processus entièrement automatisés, par le système de gestion des données (fonction 4.4). Ce service permet également de mettre en place des processus permettant de détecter des anomalies et des changements de tendance dans les flux d'informations provenant de sources externes.*

Sous-fonction 4.3.1 **Identification et recensement des sources**: identification, actualisation et intégration en continu des sources d'information au sein des processus de gestion et d'analyse des connaissances.

Objectif: obtenir auprès de sources externes des informations pertinentes et de grande qualité, en vue d'accroître l'efficacité de l'intervention en cas d'incident et d'améliorer de façon proactive l'appréciation de la situation (et, plus généralement, le dispositif de sécurité de l'organisation). Les sources externes complètent les données collectées en interne: rapports d'incident (fonction 1.1), rapports de vulnérabilité (fonction 1.2) et données fournies par les détecteurs de la CSIRT (fonction 4.1).

Résultat: *acquisition d'informations relatives à la sécurité pertinentes et de grande qualité auprès de sources internes et externes, en accès libre et/ou commerciales. Toutes les informations collectées sont stockées dans le système de gestion des données (fonction 4.4).*

Sous-fonction 4.3.2 **Collecte et classement de sources d'information**: acquisition de sources d'information sur les menaces. Ces sources peuvent être internes, externes, en accès libre et/ou payantes.

Objectif: évaluer la qualité des informations collectées. Observer les changements dans les caractéristiques (y compris la quantité) des données provenant de sources externes afin de déceler des anomalies et/ou des nouvelles tendances.

Résultat: *documentation assortie d'une évaluation de la qualité des sources. Traitement automatisé ou semi-automatisé des principaux changements dans les caractéristiques générales des informations provenant de sources externes.*

Fonction 4.4 **Gestion des données et des connaissances:** services offerts aux parties prenantes pour les aider à recueillir, développer, partager et utiliser efficacement les connaissances de l'organisation afin d'intégrer des balises de données (p. ex., STIX, TAXII, IODEF, TLP), des bases de données sur les indicateurs et des catalogues répertoriant les logiciels malveillants et les vulnérabilités.

Objectif: en matière de cybersécurité, les parties prenantes doivent disposer en temps opportun de données et de connaissances ayant un niveau de qualité adapté à leurs besoins. Les données relatives à la cybersécurité sont des informations destinées à être traitées par les systèmes en vue de faciliter l'automatisation de la sécurité. Les connaissances relatives à la cybersécurité sont des informations destinées aux analystes/opérateurs de cybersécurité humains. Par ailleurs, d'autres services et fonctions de la CSIRT requièrent des données et des connaissances relatives à la cybersécurité. Ces informations étant réutilisées dans plusieurs services et fonctions, le meilleur moyen de les gérer est de créer une base de données générale au sein de la CSIRT.

Résultat*: des données et connaissances relatives à la cybersécurité ayant le niveau de qualité requis sont fournies aux parties prenantes en temps utile. D'autres services et fonctions de la CSIRT peuvent facilement obtenir les données et connaissances dont ils ont besoin auprès d'une source unique au sein de la CSIRT.*

- **Gestion de la représentation des données:** normalisation du format de représentation et d'échange des données (p. ex. STIX, TAXII, IODEF, RID, etc.)
- **Gestion du stockage des données:** conception, mise en place et maintenance de systèmes de gestion du stockage
- **Assimilation des données:** processus et systèmes utilisés pour générer, valider et stocker les informations

- **Extraction des données:** processus, politiques et techniques d'extraction des informations
- **Évaluation des outils:** évaluation et intégration des outils utilisés pour la gestion, l'analyse et le partage des données

Fonction 4.5 **Mesures liées à l'organisation**: services axés sur l'identification, la mise en place, la collecte et l'analyse de la concrétisation des objectifs de performance de l'organisation, ainsi que sur la mesure de son efficacité.

Objectif: une des difficultés majeures que rencontrent les CSIRT et les organismes de gestion des incidents consiste à déterminer dans quelle mesure ils remplissent leur mission. À mesure que les équipes acquièrent de l'expérience dans l'exercice de leurs activités, elles se demandent: «Suis-je vraiment efficace?» Elles sont à la recherche de moyens d'évaluer leurs activités non seulement en vue d'identifier les forces et les faiblesses des processus, des technologies et des méthodes, mais aussi de réaliser une analyse comparative avec d'autres équipes similaires. Elles sont également à la recherche de données quantitatives probantes et de mesures qui révèlent si elles font preuve d'efficacité dans la prévention, la détection, l'analyse et le traitement d'événements et d'incidents informatiques. Cette fonction s'attache, d'une part, à identifier les questions (informations) réclamant une réponse de façon à ce que la direction, les CSIRT et les parties prenantes, entre autres, puissent évaluer leur activité et démontrer leur valeur et, d'autre part, à instaurer des mécanismes de collecte des mesures afin de fournir les données quantitatives nécessaires, puis les collecter et les analyser, et présenter les résultats.

Résultat: *susciter une prise de conscience et fournir les preuves empiriques nécessaires pour démontrer l'efficacité avec laquelle un organisme de gestion des incidents remplit sa mission, tout en cherchant des voies d'amélioration. Utiliser ces informations pour faciliter la prise de décision et améliorer les performances et la responsabilisation.*

Service 5 Sensibilisation/Communications

Fonction 5.1 **Conseils sur les politiques de cybersécurité:** services d'aide à l'élaboration et à l'adoption d'une politique de cybersécurité en vue d'influencer positivement l'environnement de la CSIRT, ses parties prenantes et d'autres acteurs au moyen de conseils d'experts prodigués aux décideurs.

Sous-fonction 5.1.1 En interne

- **Consultation sur les aspects stratégiques et juridiques:** souligner les implications ayant trait aux aspects stratégiques et juridiques qui concernent les pouvoirs et les mandats de l'organisation et des parties prenantes.
- **Conception de politiques**: élaborer une politique qui concerne ou affecte les activités et les pouvoirs de l'organisation et des parties prenantes.

Sous-fonction 5.1.2 En externe

- **Contribution aux politiques:** fournir des conseils concernant les questions liées aux politiques techniques et de sécurité susceptibles d'affecter l'organisation et ses parties prenantes ou d'autres partenaires.
- **Politique d'influence:** fournir des informations faisant autorité ou des conseils d'expert destinés à orienter la révision des politiques, des réglementations ou des lois. Il peut s'agir, entre autres, de témoigner devant des organismes législatifs, scientifiques ou de toute autre nature; de rédiger des prises de position, des livres blancs ou des articles; d'intervenir sur des blogs ou des réseaux sociaux; de se réunir avec des parties prenantes, etc.
- **Élaboration de normes ou de bonnes pratiques**: contribuer aux efforts des organismes définissant les normes et les bonnes pratiques au niveau mondial, régional, national ou sectoriel (IETF, ISO, FIRST) en vue de faciliter la normalisation des processus/bonnes pratiques et ainsi de maximiser la compatibilité, l'interopérabilité, la sûreté, la reproductibilité ou la qualité.

Fonction 5.2 **Gestion des relations**: services axés sur l'instauration et le maintien de relations en faveur de l'organisation.

Sous-fonction 5.2.1 **Gestion des relations entre pairs**: développement et maintien de relations avec des organisations susceptibles de faciliter l'exécution de la mission de la CSIRT. Il peut s'agir de favoriser l'interopérabilité ou de renforcer la collaboration au sein des organisations ou entre elles.

Sous-fonction 5.2.2 **Gestion des relations avec les parties prenantes**: élaboration et mise en œuvre de pratiques, de stratégies et de technologies servant à identifier, distinguer, comprendre, gérer, suivre et évaluer les parties prenantes et autres acteurs concernés.

Sous-fonction 5.2.3 **Gestion de la communication**: gestion des listes utilisées pour les annonces, les alertes, les avertissements, les flux de données et d'autres publications ou partages d'informations.

Sous-fonction 5.2.4 **Gestion de la communication sécurisée**: gestion des mécanismes de communication sécurisée utilisés pour le courrier électronique, le Web, la messagerie instantanée ou la téléphonie sans fil.

Sous-fonction 5.2.5 **Conférences/ateliers**: donner l'occasion à la CSIRT et à ses parties prenantes de se réunir pour discuter des menaces et des difficultés qu'ils affrontent, renforcer leurs relations de confiance, échanger des contacts et partager leurs bonnes pratiques ou leurs expériences.

Sous-fonction 5.2.6 **Participation des acteurs concernés et interactions**: cette sous-fonction comprend notamment la coordination avec des organisations sectorielles/verticales et le maintien de relations privilégiées avec les acteurs internes et externes. Mobilisation du personnel de direction en vue de favoriser sa connaissance de la mission de l'organisation et de le sensibiliser à la sécurité.

Fonction 5.3 **Sensibilisation à la sécurité**: services proposés aux parties prenantes en vue d'améliorer la compréhension collective des menaces subies et des actions à prendre pour en réduire les risques.

Fonction 5.4 **Valorisation/promotion**: services consistant à sensibiliser les acteurs et les parties prenantes aux activités de la CSIRT et aux capacités qu'elle est en mesure de fournir, ainsi qu'à la façon de lui faire connaître leurs besoins.

Fonction 5.5 **Partage d'informations et publications**: services axés sur la communication au sens large, notamment les avis transmis par l'organisation à ses parties prenantes à l'appui de ses activités. Par exemple: avis relatifs à des formations, des événements, des politiques et des procédures de l'organisation.

Sous-fonction 5.5.1 **Annonces d'intérêt public**: diffusion d'informations relatives à la sécurité afin de mieux faire connaître, de faciliter l'adoption, et d'appliquer certaines pratiques sectorielles, publiques, de l'organisation ou des parties prenantes en matière de sécurité.

Sous-fonction 5.5.2 Publication d'informations:

- **Définition des besoins:** identifier les informations qui doivent être diffusées, les destinataires, le mode de diffusion et le calendrier (portée). Remarque: il peut s'agir d'une publication visant un public réduit ou d'une publication approfondie destinée à des partenaires.
- **Développement**: définir le format et l'objectif des informations de façon à répondre aux besoins.
- **Réalisation:** compiler avec exactitude les informations de façon à ce qu'elles soient bien comprises par le public visé (p. ex., présenter les résultats des activités de criminalistique et de gestion des incidents, des vulnérabilités et des logiciels malveillants).
- **Examen:** réviser la publication afin d'en vérifier la clarté, l'exactitude, la grammaire, l'orthographe, la sensibilité et l'adhésion aux règles de divulgation des informations de façon à en obtenir l'approbation définitive.
- **Distribution:** distribuer les informations au public visé par l'intermédiaire des canaux requis et appropriés.

Service 6 Renforcement des capacités

Objectif: Pour être solide, la procédure de traitement des incidents et de réaction doit toujours intégrer une composante liée au renforcement des capacités. Les performances générales de l'organisation et son efficacité en dépendent entièrement. Les organisations doivent mener une réflexion plus poussée en vue de discerner les capacités qui affectent réellement leur CSIRT et leurs performances globales, de façon à adapter leurs programmes de formation en conséquence. À l'occasion d'une enquête McKinsey, près de 60% des participants ont déclaré que le renforcement des capacités de l'organisation figurait parmi leurs trois principaux objectifs. Toutefois, à l'heure de répondre aux besoins prioritaires, ils étaient un peu moins de 30% à réellement axer leurs programmes de formation sur le renforcement de la capacité créant le plus de valeur ajoutée et sur les éléments indispensables pour optimiser les performances.

Une capacité peut se définir comme tout type d'activité dans laquelle une organisation excelle et obtient des résultats significatifs. Les organisations doivent acquérir les capacités qui sont les plus essentielles à l'exercice de leurs activités et à la performance de l'équipe, et comprendre les résultats liés aux raisons qui ont orienté leur choix. La culture joue sans conteste un rôle dans le choix des capacités privilégiées et développées par une organisation. Bien que ce soit habituellement la direction qui donne le ton et définisse la vision d'une organisation en la matière, les meilleurs résultats ont été obtenus en adaptant les capacités générales de l'organisation à celles nécessaires au niveau des unités opérationnelles ou des équipes.

***Résultat**: comprendre, documenter et exécuter un programme de renforcement des capacités, et être en mesure d'exploiter et de mesurer les résultats des différentes opportunités mises en œuvre à cette fin, ainsi que les relations entre elles, afin d'améliorer l'état de préparation des membres de l'équipe et de l'organisation en général. Définir et adopter une approche systématique qui fait partie intégrante de la planification des effectifs.*

Fonction 6.1 **Formation et apprentissage:** La «capabilité» est le résultat d'un niveau donné de capacité conjugué à un niveau donné de maturité. Les capacités forment donc les composantes essentielles des services de la CSIRT. Le renforcement des capacités fournit aux parties prenantes (y compris au personnel) d'une CSIRT une formation et des connaissances (exception faite des éléments fonctionnels tels que les formations RH destinées à l'équipe) sur la cybersécurité, la garantie des informations et l'intervention en cas d'incident.

> **Objectif:** un programme de formation et d'apprentissage constitue généralement la première étape de la définition et de la mise en fonctionnement d'une entité de renforcement des capacités. On y parvient grâce à différents types d'activités, comme la formation et l'éducation, la définition détaillée des connaissances, des compétences et des aptitudes requises, la mise à disposition de supports pédagogiques et de formation élaborés, le mentorat, le développement des compétences professionnelles, le recours à des exercices pratiques ou en laboratoire.

Chacune de ces activités, conjuguée aux autres, renforcera les capacités de l'organisation et de l'équipe.

***Résultat**: comprendre le contexte du programme de formation et d'apprentissage ainsi que la façon dont il contribue au renforcement des capacités de la CSIRT. Être en mesure de comprendre et de documenter les différents types de résultats attendus de l'équipe et de l'organisation, ainsi que les indicateurs clés de performance nécessaires à l'appréciation des progrès accomplis.*

Sous-fonction 6.1.1 **Recensement des besoins en termes de connaissances, de compétences et d'aptitudes**: recenser les besoins d'une partie prenante en matière de connaissances, de compétences et d'aptitudes (CCA) en vue de déterminer quelles formations et quels cours lui proposer.

Objectif: évaluer, identifier et documenter correctement les besoins de la CSIRT en termes de CCA en vue d'améliorer l'état de préparation et la force de ses membres.

***Résultat:** identification de la nature des CCA requises, mise en place d'un processus permettant à la CSIRT de répondre aux besoins de l'organisation, et comparaison avec d'autres afin de déterminer les meilleures pratiques. Cela permettra d'évaluer le niveau de performance de l'équipe, d'identifier les éventuelles possibilités d'amélioration et de les situer.*

Sous-fonction 6.1.2 **Élaboration de supports pédagogiques et de formation**: créer ou acquérir des supports pédagogiques et de formation, tels que présentations, cours magistraux, démonstrations, simulations, etc.

Objectif: l'élaboration de supports pédagogiques et de formation permet à la CSIRT d'entretenir la sensibilisation des utilisateurs, de garder l'équipe au fait de l'évolution constante du paysage de la cybersécurité et des menaces y afférentes, et de faciliter la communication entre la CSIRT et ses parties prenantes.

***Résultat**: bonne qualité des supports pédagogiques et de formation de la CSIRT, qui répondent aux besoins de son environnement en évolution constante et font appel à des techniques de présentation et des plates-formes variées et percutantes.*

Sous-fonction 6.1.3 **Transmission du contenu**: transmission des connaissances et des contenus aux «étudiants». Diverses méthodes sont envisageables: formation en ligne/sur support informatique, formations supervisées par un instructeur, formations virtuelles, conférences, présentations, laboratoires, etc.

Objectif: l'adoption d'un processus formalisé de transmission des contenus aidera l'équipe à identifier en toute transparence le meilleur moyen d'administrer une formation aux membres de la CSIRT.

Résultat: *un cadre de transmission des contenus, qui fait appel à toutes les méthodes disponibles (présentation et apprentissage de compétences et processus techniques et non techniques) et à tous les autres procédés (exercices pratiques en laboratoire, enseignement à distance assisté par ordinateur ou cours de formation présentiels, etc.)*

Sous-fonction 6.1.4 **Mentorat**: apprentissage transmis, dans le cadre d'une relation formalisée, par un personnel expérimenté. Il peut s'agir de visites *in situ*, de rotations (échange), de stages d'observation et de débats sur les motifs sous-tendant certaines décisions ou actions spécifiques.

Objectif: un programme de mentorat constitue généralement la première étape de la définition et de la mise en fonctionnement d'une entité de renforcement des capacités. Il facilite la mise en place d'un mécanisme formel et informel par lequel le mentor aide son stagiaire à perfectionner ses savoirs et ses compétences et lui transmet le fruit de sa réflexion ainsi que des expériences personnelles et professionnelles, en dehors de la ligne hiérarchique et de la structure officielles de l'équipe.

Résultat: *renforcement de la capacité de la CSIRT à conserver ses employés, de la fidélité, de la confiance et de l'aptitude générale à prendre des décisions éclairées.*

Sous-fonction 6.1.5 **Développement professionnel**: aider les membres du personnel à planifier l'évolution de leur carrière avec succès et de façon appropriée. Il peut s'agir de participer à des conférences, à des formations pointues, à des activités transversales, etc.

Objectif: la CSIRT utilise le développement professionnel pour favoriser un processus continuel d'acquisition de nouvelles CCA professionnelles liées à la sécurité, d'accession à des responsabilités professionnelles uniques et de préservation de l'environnement général de l'équipe.

***Résultat**: tirer parti du développement professionnel afin que l'équipe gagne en confiance, mais possède également les CCA requises qu'elle met directement en pratique et se tienne informée en fonction de ses responsabilités et besoins.*

Sous-fonction 6.1.6 **Perfectionnement des compétences**: fournir au personnel une formation sur les outils, les processus et les procédures relatifs aux fonctions d'exploitation quotidiennes.

Objectif: une fois les compétences appropriées identifiées, la CSIRT doit entreprendre une série d'actions visant à déterminer son état de préparation.

***Résultat:** un personnel formé et spécialisé, possédant la compréhension requise des compétences et processus techniques et non techniques. Les membres de la CSIRT sont prêts à relever les défis qu'ils rencontrent dans leurs activités quotidiennes et soutiennent à la fois l'équipe et les clients.*

Sous-fonction 6.1.7 **Réalisation d'exercices**: tester l'état de préparation des «étudiants» issus des parties prenantes de façon à vérifier leur capacité à mettre en pratique la formation et à assumer des fonctions liées à un travail ou à une tâche. Il peut s'agir d'environnements virtuels, de simulations, de tests sur le terrain ou en miniature, d'une reconstitution ou d'une combinaison de ces techniques.

Objectif: en réalisant des entraînements/exercices, un CSIRT renforcera la crédibilité de son programme d'intervention en cas d'incident de sécurité et sa capacité à le mettre en œuvre.

***Résultat**: une équipe aussi préparée que possible, veillant à la bonne exécution des principaux processus liés aux CCA et de l'ensemble des travaux. Cela permettra par ailleurs d'évaluer le niveau de performance de l'équipe, de savoir s'il existe des possibilités d'amélioration et de les situer.*

Fonction 6.2 **Organisation d'exercices:** services proposés par l'organisation aux parties prenantes consistant à concevoir, exécuter et évaluer des exercices de cybersécurité destinés à former et/ou évaluer les capacités des parties prenantes prises séparément et dans leur ensemble. Ce genre d'exercices peuvent servir à:

- **tester les politiques et procédures:** l'équipe évalue s'il existe suffisamment de politiques et de procédures en vigueur pour faire face à l'événement. Il s'agit généralement d'un exercice sur papier ou d'une simulation.
- **tester l'état de préparation opérationnel:** l'équipe évalue si les bonnes personnes sont mobilisées pour répondre à l'événement et si les procédures sont exécutées correctement. La plupart du temps, on recourt à des exercices pratiques.

Objectif: les exercices sont réalisés dans le but d'améliorer l'efficacité et l'efficience des services et fonctions de cybersécurité. Cette fonction et les sous-fonctions qui lui sont rattachées répondent à la fois aux besoins de l'organisation et à ceux de ses parties prenantes. Plus spécifiquement, les exercices ayant recours à la simulation d'événements/incidents de cybersécurité peuvent servir un ou plusieurs objectifs:

- Démontrer: décrire les services et fonctions de cybersécurité, ainsi que les vulnérabilités, les menaces et les risques en vue d'une meilleure sensibilisation.
- Former: former le personnel aux nouveaux outils et aux nouvelles techniques et procédures.
- Entraîner: donner l'occasion au personnel d'utiliser les outils, les techniques et les procédures sur lesquels ils ont été formés. L'entraînement est indispensable dans le cas de compétences qui se perdent facilement, et il permet d'améliorer et de prolonger l'efficacité des bénéficiaires.
- Évaluer: analyser et comprendre le niveau d'efficacité et d'efficience des services et fonctions de cybersécurité.
- Certifier: déterminer si un niveau donné d'efficacité et/ou d'efficience peut être atteint dans les services et fonctions de cybersécurité.

***Résultat**: l'efficacité et l'efficience des services et fonctions de cybersécurité s'en trouveront directement améliorées et des enseignements seront tirés en vue d'améliorations futures. Selon l'objectif ou les objectifs spécifique(s) recherchés, il est aussi envisageable d'organiser une démonstration de cybersécurité à l'intention des autres acteurs concernés, de former le personnel et d'évaluer et/ou certifier l'efficacité et l'efficience des services et fonctions. Il est également possible d'identifier les enseignements tirés en vue d'améliorer les exercices futurs.*

Sous-fonction 6.2.1 **Besoins**: comprendre le but de l'exercice mais aussi plus particulièrement les objectifs de toutes les parties prenantes, de façon à tenir compte de leurs souhaits.

Objectif: la participation aux exercices a pour vocation d'améliorer l'efficacité et l'efficience des services et fonctions de cybersécurité. Il existe plusieurs façons de participer:

- Observateur: le personnel observe le déroulement d'un exercice mais ne fait pas partie du public visé. Il n'est donc pas impliqué dans les événements simulés et ses performances ne sont pas évaluées. Observer sans participer directement permet d'améliorer dans une certaine mesure l'efficacité et l'efficience des services et fonctions de la CSIRT. Cela facilite aussi l'organisation de futurs exercices.
- Public visé: le personnel participe à l'exercice en tant que public cible. Il est impliqué dans les événements simulés et parfois évalué.

En fonction des modalités prévues, le personnel pourra être amené à se rendre sur le site où se déroule l'exercice ou à participer à distance, depuis son lieu de travail habituel ou un autre lieu. Il se peut aussi que l'exercice regroupe les participants dans un cadre spécifique, ou bien que chacun participe depuis son propre environnement ou son environnement de travail habituel.

***Résultat**: l'efficacité et l'efficience des services et fonctions de cybersécurité s'en trouveront directement améliorées et des enseignements seront tirés en vue d'améliorations futures. Selon l'objectif ou les objectifs spécifique(s) recherchés, il est aussi envisageable d'organiser une démonstration de cybersécurité à l'intention des autres acteurs concernés, de former le personnel et d'évaluer et/ou certifier l'efficacité et l'efficience des services et fonctions. Il est également possible d'identifier les enseignements tirés en vue d'améliorer les exercices futurs.*

Sous-fonction 6.2.2 **Élaboration d'un scénario et développement d'un environnement**: élaboration de scénarios d'exercices correspondant aux objectifs des parties prenantes.

Objectif: L'organisation d'exercices a pour objectif de donner la possibilité au public visé d'améliorer l'efficacité et l'efficience de leurs services et fonctions en leur donnant l'occasion de traiter des événements/incidents de cybersécurité simulés.

***Résultat**: le public visé a amélioré l'efficacité et l'efficience de ses services et fonctions et a tiré des enseignements en vue d'améliorations futures. Des moyens d'améliorer les exercices futurs ont également été identifiés.*

Sous-fonction 6.2.3 **Participation à un exercice**: en fonction de son niveau de maturité, une organisation peut participer à un exercice de différentes façons.

- **Évaluation:** évaluer les résultats d'un exercice, recueillir les impressions et tirer des enseignements sur la base de ce qui a été observé.
- **Observation:** observer un exercice impliquant un tiers.
- **Coordination:** coordonner un exercice.
- **Participation:** participer à un exercice de cybersécurité. Les participants choisissent le niveau de participation et profitent des résultats de l'exercice (p. ex., un tiers évalue leur participation).

Sous-fonction 6.2.4 **Identification des enseignements tirés**: rédiger à la suite de l'exercice un rapport indiquant les enseignements tirés ou les résultats/bonnes pratiques identifiés.

Fonction 6.3 **<u>Systèmes et outils d'assistance aux parties prenantes</u>:** services axés sur la recommandation, l'élaboration, la mise à disposition et l'acquisition d'outils et de services liés à la cybersécurité en faveur des parties prenantes. L'ensemble de ces systèmes et outils a trait à la CSIRT/sécurité, non pas aux technologies de l'information en général. Il peut s'agir de portails de messagerie/d'alerte.

***Résultat**: la CSIRT dispose de processus et de systèmes destinés à identifier les besoins et les capacités des parties prenantes, et acquiert, met à disposition ou élabore des plates-formes pour répondre à ces besoins.*

Fonction 6.4 **<u>Assistance aux services en faveur des acteurs concernés</u>:** services axés sur les capacités techniques proposés par la CSIRT pour contribuer au renforcement des capacités, de la «capabilité» et de la maturité de ses services en faveur des acteurs concernés. Il s'agit d'une amélioration des niveaux de service.

Objectif: dans le cadre du processus de renforcement et d'amélioration des capacités des parties prenantes de la CSIRT, un effort particulier est fourni pour assister la conception, l'acquisition, la gestion, l'exploitation et la maintenance de leurs infrastructures.

***Résultat:** élaborer une stratégie systématique en ce qui concerne l'évaluation des besoins en infrastructure, la définition des exigences, les schémas de configuration, l'acquisition, la vérification de conformité, la maintenance et l'actualisation, la formation opérationnelle, les audits internes et externes.*

Sous-fonction 6.4.1 **Conception et ingénierie de l'infrastructure**: assister la conception et l'ingénierie de l'infrastructure afin de répondre aux besoins des parties prenantes.

Objectif: faciliter la compréhension générale de la méthodologie de conception, transmettre des connaissances relatives aux normes en vigueur et mettre en évidence les bonnes pratiques en matière de conception et d'ingénierie de l'infrastructure, sur la base d'une évaluation et d'une analyse approfondies des besoins des parties prenantes.

Résultat: *acquisition d'une expérience pratique dans l'élaboration et la comparaison de stratégies et de solutions de conception des infrastructures, fondée sur les bonnes pratiques internationales et tenant compte des normes applicables.*

Sous-fonction 6.4.2 **Acquisition d'infrastructures**: contribuer à l'acquisition des infrastructures, que ce soit en soutenant l'amélioration du niveau de maturité du cadre de gestion des risques ou l'identification des exigences et normes minimales de sécurité pour le libellé des contrats (p. ex. exigence de conformité à une norme donnée, telle que la certification d'un produit).

Objectif: acquérir une compréhension affinée de l'élaboration d'un cahier des charges relatif à l'acquisition d'infrastructures, dans le respect des exigences institutionnelles, techniques et opérationnelles.

Résultat: *bonne compréhension du processus d'acquisition d'infrastructures, conformément aux normes applicables et dans le respect des diverses mesures techniques et procédures contractuelles qui doivent être suivies.*

Sous-fonction 6.4.3 **Évaluation d'outils infrastructurels**: évaluation d'outils pour le compte des parties prenantes.

Objectif: assister l'évaluation de la fonctionnalité et de la conformité de divers outils, que ce soit le matériel informatique, les logiciels ou les applications personnalisées.

Résultat: *analyse de la performance des outils ainsi que de leur conformité aux normes et au cahier des charges préétabli.*

Sous-fonction 6.4.4 **Identification des fournisseurs d'infrastructures**: aider à recruter les fournisseurs d'infrastructures requis (vendeurs de matériel informatique, prestataires de services, etc.).

Objectif: mettre en évidence les facteurs essentiels à la réussite de l'identification des fournisseurs et développer des mécanismes permettant de nouer des relations durables et efficaces avec des fournisseurs de solutions sur la base d'une définition claire des responsabilités.

Résultat: *mise en place d'indicateurs clés de performance applicables aux fournisseurs d'infrastructure, assortis de contrats de niveau de service appropriés, garantissant l'efficacité et l'efficience du processus.*

Service 7 Recherche et développement

Fonction 7.1 **Élaboration de méthodes de détection/étude/correction des vulnérabilités et d'analyse de leurs causes principales**: services destinés à définir et identifier les nouvelles capacités, et à améliorer les méthodes dans le but de fournir des services relatifs aux vulnérabilités ou de coordonner d'autres organisations ou pratiques commerciales exerçant ces mêmes activités.

Objectif: certaines organisations se contentent des informations obtenues auprès de sources externes pour identifier leurs vulnérabilités, mais d'autres souhaiteront ou auront besoin d'être en possession des capacités organiques pour les déceler et les analyser en interne. Cette fonction est destinée à mettre en évidence la façon dont une organisation peut configurer l'architecture de ces fonctions de recherche de vulnérabilités.

Résultat: *déterminer, si besoin, les méthodes auxquelles peut avoir recours une organisation pour mieux comprendre ses vulnérabilités.*

Fonction 7.2 **Élaboration de processus de compilation/fusion/corrélation de renseignements de sécurité:** services consistant à définir et identifier les nouvelles capacités, et à améliorer les méthodes d'analyse des informations et de partage des services connexes, dès lors qu'il s'agit de renseignements sur les activités ou les menaces.

Objectif: pour être efficace, la fonction de renseignements de sécurité doit être en mesure de collecter des informations et d'en communiquer les éléments utiles avec des tiers. Cette collecte dépend souvent des relations humaines liant les parties en place: le niveau de confiance est-il suffisant pour autoriser le partage d'informations sensibles? Un analyste doit être capable de nouer ce genre de relations, d'identifier les informations appropriées devant être partagées, de déterminer les protocoles les plus adaptés aux échanges automatisés, à la gestion des relations et aux enquêtes conjointes, et d'évaluer l'efficacité d'une source d'informations.

Résultat*: l'organisation dispose de processus et de procédures de collecte, d'analyse, de synthèse et d'évaluation de la pertinence des informations provenant de sources externes qui décrivent les menaces pesant sur le patrimoine informationnel. L'organisation possède l'aptitude organique de choisir de nouvelles sources et de nouveaux partenaires d'échange.*

Fonction 7.3 **Élaboration d'outils**: services destinés à élaborer et identifier de nouvelles capacités, à partager de nouveaux outils et à automatiser l'exécution de processus relatifs à la CSIRT.

> ***Résultat**: les outils élaborés par les CSIRT pour faciliter l'automatisation de leurs tâches sont évolutifs et fiables, produisent des résultats infaillibles et ne détériorent pas le dispositif de sécurité de la CSIRT qui les utilise. Libère les analystes en vue de la réalisation de tâches ponctuelles.*

Ressources

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/CEI 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

Glossaire

Bâle II – Deuxième accord de Bâle, comportant des recommandations émises par le Comité de Bâle sur le contrôle bancaire et relatives aux normes et réglementations bancaires.

«Capabilité» – Nombre d'occurrences simultanées d'une capacité donnée dans un processus qu'une organisation peut exécuter avant d'épuiser d'une façon ou d'une autre ses ressources.

Capacité – Activité mesurable qui relève des rôles et responsabilités d'une organisation. Dans le Cadre de services de la SIRT, les capacités peuvent être définies soient en termes de services, soit en termes de fonctions, sous-fonctions ou tâches requises.

Carré – Dispositif de sécurité permettant de cloisonner des programmes en cours d'exécution.

CEI – Commission électrotechnique internationale.

CERT/CC – Computer Emergency Response Team Coordination Center (Centre de coordination des équipes d'intervention en cas d'urgence informatique).

CISO – Responsable de la sécurité des systèmes d'information.

COBIT – Objectifs de contrôle dans les domaines de l'information et des technologies connexes.

CSIRT – Équipe d'intervention en cas d'incident informatique.

Émulateur matériel/logiciel – Matériel informatique ou logiciel qui permet à un système informatique (l'«hôte») de se comporter comme un autre système informatique (l'«invité»). Généralement utilisé pour permettre au système hôte d'exécuter un logiciel ou d'utiliser des dispositifs périphériques conçus pour le système invité.

Ensemble de données externe – Base de données détenue par un tiers.

Environnement virtuel – Émulation d'un système informatique donné.

FIRST – Forum des équipes d'intervention et de sécurité en cas d'incident.

Fonction – Outil servant à réaliser l'objectif ou la tâche d'un service en particulier.

Hachage de chiffrement – Fonction de hachage qu'il est pratiquement impossible d'inverser, c'est-à-dire d'en recréer les données d'entrée uniquement à partir des valeurs de hachage.

IETF – Groupe d'étude sur l'ingénierie Internet.

IODEF – Format d'échange de descriptions d'objet concernant les incidents, un format de représentation des données fournissant un cadre pour le partage d'informations relatives aux incidents relatifs à la

sécurité informatique habituellement échangées par les équipes d'intervention en cas d'incident informatique (CSIRT).

ISO – Organisation internationale de normalisation.

ITIL – Bibliothèque de données sur l'infrastructure des technologies de l'information, qui consiste en un ensemble de pratiques pour la gestion des services informatiques axée sur l'adaptation des services informatiques aux besoins de l'organisation.

Maturité – Degré d'efficacité avec lequel une organisation concrétise une capacité donnée dans le cadre de sa mission et de ses pouvoirs.

Nuage – Environnement informatique partagé qui permet à des applications logicielles d'être utilisées à partir de dispositifs connectés.

Open Source (code source ouvert) – Modèle de développement qui privilégie l'accès universel, par l'intermédiaire d'une licence d'exploitation gratuite, au «code source» d'un produit ainsi que sa redistribution universelle, autorisant ainsi tout un chacun à y apporter des améliorations.

Recensement et évaluation des vulnérabilités – Technique de sécurité utilisée pour identifier les failles de sécurité dans un système informatique.

Rétro-ingénierie – Processus consistant à extraire des connaissances ou des informations relatives au fonctionnement de n'importe quel produit de l'activité humaine afin d'en faire une copie ou de reproduire quelque chose à partir des informations extraites.

RID – Défense interréseaux en temps réel, une méthode de communication interréseaux proactive visant à faciliter le partage d'informations relatives à la prise en charge des incidents, tout en intégrant des mécanismes de détection, d'identification de la source et d'atténuation, afin de disposer d'une solution de prise en charge des incidents complète.

Service – Action (assistance ou réalisation de travaux) en faveur ou pour le compte des parties prenantes.

Sortie de chaînes – Résultat sous la forme d'une séquence de caractères, que ce soit une constante littérale ou un certain type de variable.

STIX – *Structured Threat Information eXpression.* Effort collaboratif et communautaire visant à définir et élaborer un langage normalisé pour décrire les informations sur les menaces informatiques de façon structurée.

Suite ISO/CEI 27000 (ISO27k) – Normes de sécurité de l'information qui fournissent des recommandations issues des bonnes pratiques sur la gestion, les risques et le contrôle de la sécurité des informations, dans le cadre d'un système général de gestion de la sécurité des informations, et qui présente une structure identique aux systèmes de gestion pour l'assurance qualité (la suite ISO 9000) et pour la protection de l'environnement (la suite ISO 14000).

TAXII – *Trusted Automated Exchange of Indicator Information.* Ensemble de services et d'échanges de messages qui, une fois mis en œuvre, permet le partage d'informations concrètes sur les cybermenaces par-delà les frontières des organisations et des secteurs de produits/services.

Test à données aléatoires – Technique de test de logiciels, souvent automatisée ou semi-automatisée, qui consiste à alimenter un programme informatique avec des données invalides, inattendues ou aléatoires.

Test d'application – Enquête réalisée dans le but de fournir aux parties prenantes des informations relatives à la qualité du produit ou du service testé.

Test d'intrusion – Attaque perpétrée contre un système informatique dans l'optique de déceler des failles de sécurité et de pouvoir accéder à ce système, à ses fonctionnalités et à ses données.

TLP – *Traffic Light Protocol* (ou Protocole par feux de signalisation). Utilisé pour veiller à ce que les informations sensibles soient partagées avec les bons destinataires.

Annexe – Structure d'un service

Comme nous l'avons signalé précédemment, la structure d'un service adoptée dans le présent cadre distingue trois premières couches (zones de service, service et fonctions) qui correspondent à ce qui est fait, et deux autres (tâches et actions) qui décrivent comment ces activités sont réalisées.
Pour simplifier, la structure générale s'organise comme suit: