Novembre 2019

Équipe d'intervention en cas d'incident informatique (CSIRT)
Cadre de services

Version 2.1

Avis: Le présent document décrit ce que le Forum des équipes d'intervention et de sécurité en cas d'incident, Inc. (FIRST.Org) considère comme des bonnes pratiques. Son contenu n'est fourni qu'à titre informatif. FIRST.Org réfute toute responsabilité quant aux éventuels préjudices consécutifs ou liés à l'utilisation de ces informations.

Cadre de services de la CSIRT

1 Objectif

Le Cadre de services de la CSIRT est un document de premier plan décrivant de manière structurée les services de cybersécurité et les fonctions associées que sont susceptibles de fournir les Équipes d'intervention en cas d'incident informatique ainsi que les autres équipes dispensant des services en rapport avec la gestion des incidents. Ce cadre a été élaboré par des experts reconnus de la communauté FIRST appuyés par la communauté des Groupes de travail CSIRT (TF-CSIRT) et l'Union internationale des télécommunications (UIT).

Le Cadre de services de la CSIRT a pour mission et pour objectif de faciliter la mise en place et de l'amélioration des opérations des CSIRT, notamment dans le but d'aider les équipes engagées dans le processus de sélection, d'élargissement ou d'amélioration de leur portefeuille de services. Les services décrits sont ceux qu'une CSIRT est potentiellement susceptible de fournir. Aucune CSIRT n'est enjointe à fournir la totalité des services décrits. Chaque équipe devra choisir les services utiles à sa mission et à ses parties prenantes, telles que décrites dans son mandat.

Afin d'aider les équipes, le Cadre identifie et définit les principales catégories de services et leurs composantes. Il fournit l'intitulé et la description de chaque service, sous-service, fonction et éventuellement sous-fonction, selon le cas. Ce document constitue le point de départ d'un cadre de services cohérent proposant une terminologie et des définitions standard à utiliser par l'ensemble de la communauté. À noter que le présent document n'explique pas les modalités de création ou d'amélioration d'une équipe CSIRT ou apparentée. Ce type d'informations figure dans d'autres documents, dont certains sont cités dans les ressources listées à l'Annexe 1.

Le Cadre de services de la CSIRT n'émet ni suggestions, ni recommandations quant aux capacités, à la maturité ou à la qualité d'un type spécifique de CSIRT. Ces sujets importants pour la valeur qu'apportent les CSIRT à leurs parties prenantes ont été volontairement exclus du présent document. Ce cadre n'aborde pas non plus la mise en œuvre et ne propose pas de méthode particulière de mise en œuvre d'un service donné. Il est important de comprendre que ces services peuvent être mis en œuvre de multiples manières, répondant néanmoins aux attentes raisonnables des parties prenantes.

2 Introduction et contexte

Une Équipe d'intervention en cas d'incident informatique est une unité organisationnelle (éventuellement virtuelle) ou une capacité qui fournit des services et un appui à des parties prenantes définies aux fins de prévention, détection, gestion et riposte à des incidents informatiques, conformément à sa mission.

Une CSIRT déployée dans les règles dispose d'un mandat clair, d'un modèle de gouvernance, d'un cadre de services personnalisé, de technologies et de processus visant à fournir, mesurer et améliorer en permanence les services définis.

Au fil des années, diverses entités de la communauté des CSIRT ont élaboré leurs propres listes ou cadres de services. À mesure de l'évolution des technologies, des outils et des processus, la communauté a jugé que les listes existantes omettaient certains sujets et certaines activités. Désireux d'assurer le développement et l'avancement des CSIRT à l'échelle internationale, le FIRST a reconnu qu'il s'agissait d'un élément essentiel de l'élaboration d'un langage commun à toutes les CSIRT et aux autres entités amenées à collaborer avec elles. Compte tenu de la diversité géographique et fonctionnelle des membres du FIRST, il a été estimé que la communauté qu'il constitue serait à même d'inventorier et de répertorier les services fournis par les CSIRT. C'est ainsi qu'a vu le jour une approche communautaire autour de l'élaboration d'un cadre amélioré de services CSIRT, dont la version initiale a été publiée en 2017.

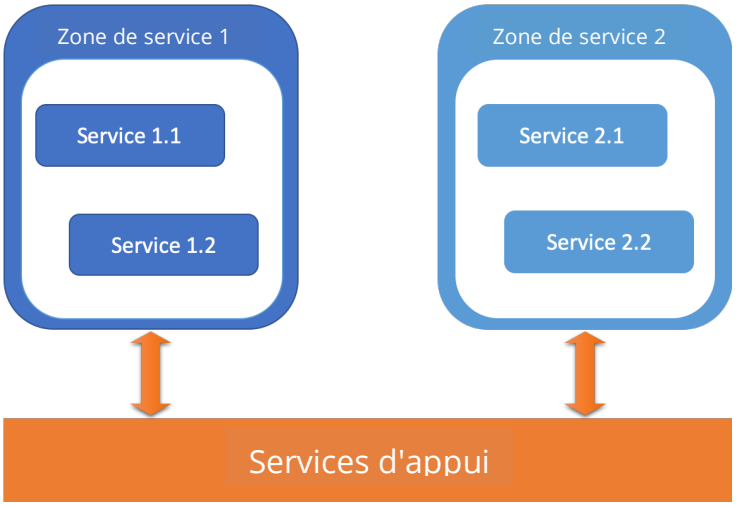
Depuis lors, une approche similaire a débouché sur un Cadre de services des équipes d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT) visant à traiter les nombreux aspects opérationnels nécessitant un ensemble différent de services et d'activités correspondantes. Tous les cadres de services sont accessibles sur le site web du FIRST[1].

Cette version améliorée est la deuxième du Cadre de services de la CSIRT. Sur la base des commentaires émis par plusieurs experts concernant la première version, elle a été restructurée et enrichie lorsque cela s'est avéré nécessaire. Les activités internes ne constituant pas des offres de services aux parties prenantes ont notamment été supprimées. Les activités internes et externes secondant l'ensemble du cycle de vie d'une offre de services, quelle qu'elle soit, peuvent s'organiser en services et en fonctions, tout comme les services destinés aux parties prenantes. Ces services et ces fonctions sont qualifiés la plupart du temps de services d'appui. Les activités administratives telles que la gestion et le recrutement de personnel, le remboursement des frais de déplacement ou l'organisation d'événements de formation en constituent des exemples[2].

À notre connaissance, il existe de multiples manières de fournir ces services d'appui, qui dépendent la plupart du temps de l'organisation hébergeant la CSIRT ou d'offres de services apparentées. Par exemple, le recrutement et la gestion du personnel seront sûrement nécessaires pour appuyer la CSIRT mais sont considérés comme des tâches d'appui organisationnelles type et non spécifiques aux CSIRT.

[1] https://www.first.org/standards/frameworks/csirts/ pour les documents en rapport avec les CSIRT.

[2] Voir [Kossakowski 2001] pour une discussion engageant les services d'assistance interne et leur relation avec d'autres services.



Bien que des services et des fonctions internes constituent la colonne vertébrale permettant à n'importe quelle équipe ou unité organisationnelle de remplir sa mission, ces services d'appui sont considérés hors périmètre et ne sont ni abordés en détail, ni discutés dans les cadres de services du FIRST.

Dans la mesure où les CSIRT seront toujours confrontées à de nouveaux défis pour protéger leurs parties prenantes contre les nouvelles menaces émergentes, les services abordés dans le présent cadre seront examinés, approuvés et étendus ou amendés, selon les cas, dans les versions futures[3].

3 Différence entre CSIRT et PSIRT

L'accent mis sur les parties prenantes et la nature des services proposés constituent les deux principaux facteurs de différenciation entre la CSIRT d'une organisation et ses autres équipes en charge de la sécurité telles que la PSIRT. En général, l'accent sur les produits constitue le principal facteur de différenciation entre la PSIRT et les autres équipes de sécurité d'une organisation, dont la CSIRT, parmi d'autres.

Les CSIRT d'entreprise sont axées sur la sécurité des systèmes informatiques et des réseaux qui constituent l'infrastructure des organisations. S'il existe au sein d'une grande organisation plusieurs équipes de sécurité et CSIRT, l'une d'entre elles pourra jouer le rôle de coordonnateur et de point de contact unique avec les parties externes. Ces équipes sont dénommées CSIRT de coordination.

Les CSIRT de coordination sont également mises en place en tant qu'entités indépendantes au service d'un ensemble spécifique d'individus et/ou d'organisations appelés parties prenantes. Les organisations appartenant à des parties prenantes spécifiques présentent des caractéristiques communes (par exemple, appartenance à un réseau de recherche national ou à

[3] Un Groupe d'intérêt (SIG) du FIRST a été créé pour piloter le "Développement du cadre des CSIRT".

un pays donné). Les CSIRT de coordination jouent le rôle de point de contact unique pour l'ensemble du groupe et sont axées sur les aspects globaux de la sécurité de ces organisations.

Actuellement, des CSIRT nationales ont été mises en place. Ces types spécifiques de CSIRT de coordination facilitent et souvent coordonnent les activités des CSIRT d'un pays donné ou proposent des services limités à l'ensemble des citoyens, à des secteurs spécifiques d'entités infrastructurelles critiques, etc., du pays concerné.

S'il existe des différences substantielles entre les CSIRT et les PSIRT, il importe de ne pas omettre pour autant leurs synergies. Retenons avant tout que les CSIRT et les PSIRT n'opèrent pas indépendamment les unes des autres car de nombreuses CSIRT avertissent leurs parties prenantes des vulnérabilités de sécurité, pour ne prendre qu'un exemple. Ces avertissements reposent presque toujours sur des informations fournies par les PSIRT des fournisseurs.

4 Structure du Cadre de services de la CSIRT

Le Cadre des services de la CSIRT repose sur les relations entre quatre éléments principaux:

ZONES DE SERVICE → SERVICES → FONCTIONS → SOUS-FONCTIONS

Ces éléments sont définis comme suit:

ZONES DE SERVICE

Les zones de service regroupent les services liés à un aspect commun. Ils s'appuient sur des catégories générales pour faciliter l'organisation des services, la compréhension et la communication. La spécification de chaque zone de service inclut un champ "Description" consistant en un texte général de haut niveau décrivant le zone de service et en énumérant les services.

SERVICES

Un service est un ensemble de fonctions reconnaissables et cohérentes visant un résultat spécifique. Ce résultat peut être escompté ou demandé par les parties prenantes ou pour le compte d'une entité ou de ses parties prenantes.

La spécification des services suit le modèle suivant:

- Un champ "Description" décrivant la nature du service.
- Un champ "Objectif" décrivant l'objet du service.
- Un champ "Résultat" décrivant les résultats mesurables du service.

FONCTIONS

Une fonction est une activité ou un ensemble d'activités visant à atteindre l'objectif d'un service donné. Les fonctions peuvent être partagées et utilisées dans le contexte de plusieurs services.

La description des fonctions suit le modèle suivant:

- Un champ "Description" décrivant la fonction.
- Un champ "Objectif" décrivant la finalité de la fonction.
- Un champ "Résultat" décrivant les résultats mesurables de la fonction.
- La liste des sous-fonctions susceptibles d'être assurées dans le cadre de la fonction.

SOUS-FONCTIONS

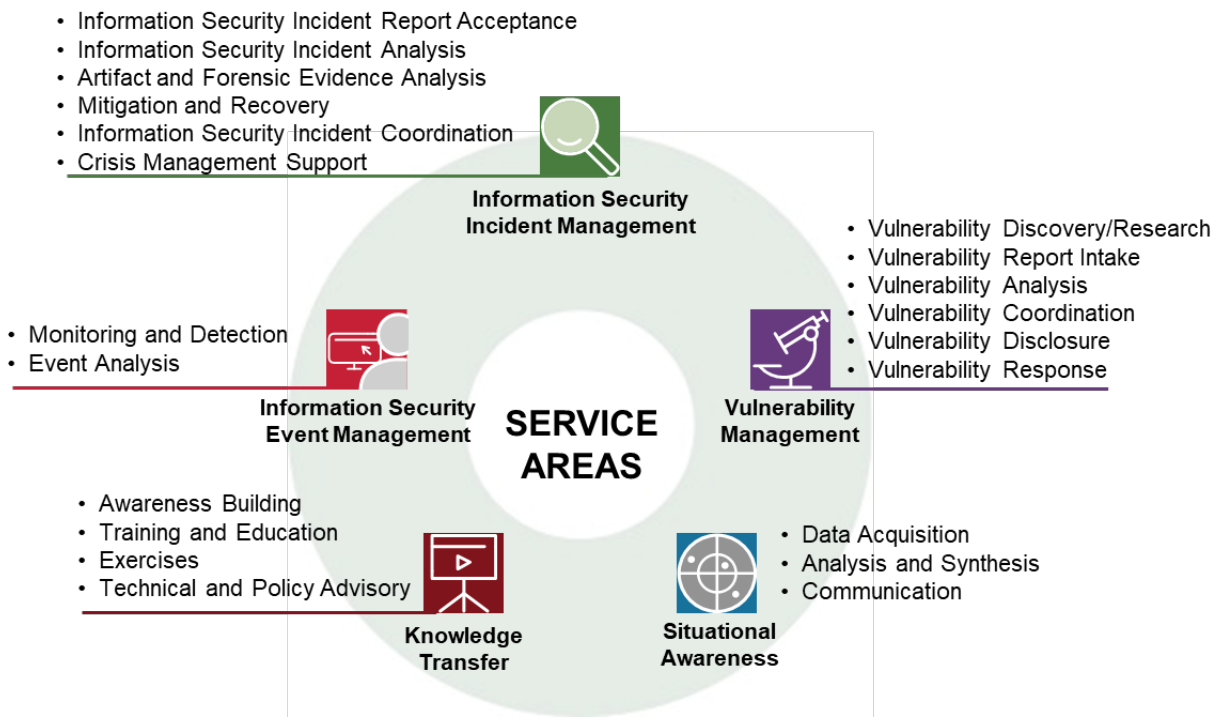
Une sous-fonction est une activité ou un ensemble d'activités visant à atteindre l'objectif d'une fonction donnée. Les sous-fonctions peuvent être partagées et utilisées dans le contexte de plusieurs fonctions et/ou services. Des sous-fonctions peuvent éventuellement être assurées ou requises pour n'importe lesquels de ces fonctions et/ou services.

La description des sous-fonctions suit le modèle suivant:

- Un champ "Description" décrivant la sous-fonction.
- Un champ "Objectif" décrivant la finalité de la sous-fonction.
- Un champ "Résultat" décrivant les résultats mesurables de la sous-fonction.

Le Cadre de services de la CSIRT ne décrit pas en détail les sous-fonctions. Il ne fournit qu'une brève description de leurs caractéristiques.

La figure ci-après représente les zones de service et les services du Cadre de services de la CSIRT. L'Annexe 4 propose un tableau complet des zones de service, des services et des fonctions.



Légende de la figure:

Gestion des incidents relatifs à la sécurité des informations ■ Acceptation des signalements d'incidents relatifs à la sécurité des informations ■ Analyse des incidents relatifs à la sécurité des informations ■ Analyse des artefacts et des preuves judiciaires ■ Atténuation et reprise ■ Coordination des incidents relatifs à la sécurité des informations ■ Appui à la gestion de crise **Gestion des événements relatifs à la sécurité des informations** ■ Surveillance et detection ■ Analyse des événements **Transfert de connaissance** ■ Renforcement des connaissances ■ Formation et apprentissage ■ Exercices ■ Conseil technique et stratégique	**ZONES DE SERVICE**	**Appréciation de la situation** ■ Acquisition de données ■ Analyse et synthèse ■ Communication **Gestion des vulnérabilités** ■ Découverte/recherche de vulnérabilités ■ Recueil des rapports de vulnérabilité ■ Analyse des vulnérabilités ■ Coordination des vulnérabilités ■ Divulgation des vulnérabilités ■ Intervention en cas de vulnérabilité

5 Zone de service: Gestion des événements relatifs à la sécurité des informations

La gestion des événements relatifs à la sécurité des informations vise à identifier les incidents relatifs à la sécurité des informations à partir de la corrélation et de l'analyse des événements de sécurité fournis par diverses sources de données événementielles et contextuelles. Dans les grandes organisations, ce zone de service est parfois assigné, en totalité ou en partie, à un Centre opérationnel de sécurité (COS), chargé éventuellement de la gestion des incidents relatifs à la sécurité des informations de premier ou même de deuxième niveau, tels que la mise en place de mesures d'atténuation ou d'ajustement des contrôles de sécurité. Comme tout service de gestion des incidents relatifs à la sécurité des informations dépend de données caractérisées et exactes sur les événements survenus, l'interface entre le COS et la CSIRT à laquelle elle est assignée est cruciale[4].

Les services suivants sont considérés comme des offres relevant de ce zone de service spécifique:

- Surveillance et détection.
- Analyse des événements.

5.1 Service: Surveillance et détection

Objectif: mettre en œuvre le traitement automatisé et continu de diverses sources d'événements relatifs à la sécurité des informations et de données contextuelles afin d'identifier les incidents potentiels (attaques, intrusions, atteintes aux données ou violations de la politique en matière de sécurité, notamment).

Description: sur la base de journaux, de données NetFlow, d'alertes IDS, de réseaux de capteurs, de sources externes ou d'autres données sur les événements relatifs à la sécurité des informations, application de diverses méthodes allant d'une simple logique ou de règles de concordance de modèle à l'application de modèles statistiques ou d'apprentissage automatique afin d'identifier les incidents potentiels. Ces activités peuvent porter sur un volume considérable de données et requièrent en principe – mais pas nécessairement – des outils de traitement spécialisés tels que la gestion des informations et des événements de sécurité (SIEM) ou des plateformes de mégadonnées. Un objectif important de l'amélioration continue est la réduction du nombre de fausses alertes à analyser dans le cadre du service Analyse.

[4] Bien que le présent cadre de services n'ait pas pour but de définir un cadre de services pour le COS, les services des domaines Incidents relatifs à la sécurité des informations et Gestion des incidents doivent être utiles et directement applicables lors de la définition des services du COS.

Résultat: identification et analyse, dans le cadre du service Analyse, des risques d'incidents relatifs à la sécurité des informations.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Gestion des journaux et des capteurs.
- Gestion des cas d'utilisation de détection.
- Gestion des données contextuelles.

5.1.1 Fonction: Gestion des journaux et des capteurs

Objectif: gérer les sources de journaux et les capteurs.

Description: les capteurs et les sources de journaux nécessitent une gestion opérationnelle pendant tout leur cycle de vie. Les capteurs doivent être déployés, embarqués et supprimés. Les pannes, la qualité/le périmètre des données et les problèmes de configuration doivent être identifiés et résolus. Les capteurs dotés d'une forme ou une autre de configuration, telle que les définitions de modèle, doivent fait l'objet d'une maintenance pour conserver leur efficacité. S'ils constituent la base de cas d'utilisation de détection, les capteurs doivent également inclure des services de détection externes ou des sources OSINT (intelligence à code source ouvert).

Résultat: un flux fiable d'événements pertinents relatifs à la sécurité des informations peut servir de données d'entrée aux cas d'utilisation de détection.

5.1.2 Fonction: Gestion des cas d'utilisation de détection

Objectif: gérer le portefeuille de cas d'utilisation de détection pendant tout leur cycle de vie.

Description: de nouvelles approches sont développées, testées, améliorées et éventuellement incorporées à un cas d'utilisation de détection en production. Il convient d'élaborer des instructions relatives au tri, à la caractérisation et à la corrélation par les analystes, par exemple sous forme de manuels et de procédures opérationnelles normalisées (PON). Les cas d'utilisation non performants, c'est-à-dire ceux dont le rapport bénéfice/effort est défavorable, doivent être améliorés, redéfinis ou abandonnés. Le portefeuille de cas d'utilisation de détection doit élargir la prise en compte des risques et être coordonné avec les contrôles préventifs.

Résultat: élaboration d'un portefeuille de cas d'utilisation de détection efficaces pertinent pour les parties prenantes.

5.1.3 Fonction: Gestion des données contextuelles

Objectif: gérer les sources de données contextuelles pour la détection et l'enrichissement.

Description: il faut gérer pendant tout leur cycle de vie les diverses sources de données contextuelles intervenant dans la détection et l'enrichissement. Il peut s'agir d'interfaces API directes vers d'autres systèmes informatiques ou d'exportations à partir d'autres systèmes

informatiques – base de données de gestion de la configuration (CMDB), gestion des identités et de l'accès (IAM) – ou de systèmes Threat Intel ou bien encore d'ensembles de données totalement distincts devant être gérés manuellement. Dans ce dernier cas, il s'agira de listes d'indicateurs, de listes noires et de listes blanches visant à supprimer les faux positifs.

Résultat: mise à disposition de données contextuelles à jour pour la détection et l'enrichissement.

5.2 Service: Analyse des événements

Objectif: le tri a détecté de potentiels incidents relatifs à la sécurité des informations et les a qualifiés comme tels, devant être soit remontés vers le zone de service Gestion des incidents relatifs à la sécurité des informations, soit considérés comme de fausses alertes.

Description: le flux des incidents relatifs à la sécurité des informations potentiels doit être trié et chacun d'eux caractérisé, à l'aide du manuel et/ou d'une analyse automatique, soit en tant qu'incident relatif à la sécurité des informations (vrai positif), soit en tant que fausse alerte (faux positif). Cette opération peut requérir la collecte manuelle ou automatique d'informations supplémentaires en fonction du cas d'utilisation de détection. Il faut donner la priorité à l'analyse des incidents relatifs à la sécurité des informations potentiellement plus critiques afin de réagir à ce qui est le plus important, au moment opportun. La caractérisation structurée des incidents relatifs à la sécurité des informations potentiels détectés permet une amélioration continue ciblée grâce à l'identification des cas d'utilisation de détection, des sources de données ou des processus présentant des problèmes de qualité.

Résultat: existence d'incidents relatifs à la sécurité des informations caractérisés et corrélés pouvant servir de données d'entrée au zone de service Gestion des incidents relatifs à la sécurité des informations et caractérisation des faux positifs à des fins d'amélioration continue.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Corrélation.
- Caractérisation.

5.2.1 Fonction: Corrélation

Objectif: identifier les événements directement liés à d'autres incidents de sécurité potentiels ou existants.

Description: les incidents relatifs à la sécurité des informations potentiels portant sur les mêmes ressources (par exemple: systèmes, services, clients) ou identités (par exemple: utilisateurs) ou directement liés d'une autre manière à d'autres incidents relatifs à la sécurité des informations potentiels sont regroupés et remontés en tant qu'unique incident relatif à la sécurité des informations afin d'éviter les doubles emplois. Les nouveaux incidents relatifs à la sécurité des informations potentiels directement liés à des incidents existants de même nature sont assignés aux incidents relatifs à la sécurité des informations existants – et ne donnent pas lieu à la création d'un nouvel incident distinct.

Résultat: regroupement des incidents relatifs à la sécurité des informations potentiels apparentés justifiant une caractérisation combinée ou mise à jour d'un incident relatif à la sécurité des informations existant déjà géré par la zone de service Gestion des incidents relatifs à la sécurité des informations.

5.2.2 Fonction: Caractérisation

Objectif: trier et caractériser les incidents relatifs à la sécurité des informations potentiels détectés afin d'identifier, de classifier et de hiérarchiser les vrais positifs.

Description: les incidents relatifs à la sécurité des informations potentiels doivent être triés et chacun d'eux caractérisés soit en tant qu'incident relatif à la sécurité des informations (vrai positif), soit en tant que fausse alerte (faux positif). Comme les analystes disposent d'un nombre limité d'incidents relatifs à la sécurité des informations potentiels qu'ils peuvent analyser – et afin d'éviter une accumulation d'alertes –, l'automatisation est essentielle. Des outils éprouvés améliorent l'efficacité du tri grâce à l'enrichissement à l'aide d'informations contextuelles, à l'affectation de scores de risque basés sur la criticité des ressources et des identités concernées et/ou à l'identification d'événements relatifs à la sécurité des informations apparentés. Les cas récurrents qu'il est possible d'automatiser doivent être identifiés et automatisés. Les incidents relatifs à la sécurité des informations potentiels les plus critiques doivent être analysés avant les moins critiques. Outre la caractérisation en vrais ou faux positifs, une caractérisation affinée constitue un facteur important pour l'amélioration continue des cas d'utilisation de détection ainsi que pour la gestion des sources de journaux, des capteurs et des sources de données contextuelles. Une caractérisation affinée peut également faciliter la définition d'indicateurs clés de performance (KPI) de meilleure qualité pour mesurer le succès de ce zone de service.

Résultat: possibilité de traitement des incidents relatifs à la sécurité des informations potentiels caractérisés comme tels dans le cadre du zone de service Gestion des incidents relatifs à la sécurité des informations.

6 Zone de service: gestion des incidents relatifs à la sécurité des informations

Ce zone de service constitue le cœur des CSIRT. Ses services sont essentiels pour aider les parties prenantes en cas d'attaque ou d'incident. Les CSIRT doivent être prêtes à apporter aide et soutien. Grâce à leur position et à leur expertise uniques, elles sont en mesure non seulement de collecter et d'évaluer les signalements d'incidents relatifs à la sécurité des informations, mais aussi d'analyser les données pertinentes et d'effectuer l'analyse technique détaillée des incidents eux-mêmes et des artefacts utilisés.

Cette analyse permet de recommander des mesures d'atténuation et des étapes de retour à la normale et aidera les parties prenantes à appliquer les recommandations. Elle requiert également une coordination avec des entités externes telles que des CSIRT homologues ou des experts en sécurité, des fournisseurs ou des PSIRT pour traiter tous les aspects et réduire le nombre d'attaques réussies par la suite.

L'expertise spéciale que les CSIRT peuvent apporter est également cruciale pour gérer les crises (liées à la sécurité des informations). Dans la plupart des cas, les CSIRT ne gèrent pas les crises, mais peuvent soutenir ce type d'activité. Par exemple, la mise à disposition de leurs contacts peut grandement améliorer l'application des étapes d'atténuation requises ou les mécanismes de protection.

L'utilisation de leurs connaissances et de l'infrastructure disponible au service de leurs parties prenantes est essentielle pour améliorer la gestion globale des incidents relatifs à la sécurité des informations.

Les services suivants sont considérés comme des offres potentielles de ce zone de service:

- Acceptation des signalements d'incidents relatifs à la sécurité des informations.
- Analyse des incidents relatifs à la sécurité des informations.
- Analyse des artefacts et des preuves judiciaires.
- Atténuation et reprise.
- Coordination des incidents relatifs à la sécurité des informations.
- Appui à la gestion de crise.

6.1 Service: Acceptation des signalements d'incidents relatifs à la sécurité des informations

Objectif: recevoir et traiter les incidents relatifs à la sécurité des informations potentiels signalés par les parties prenantes, les services de la Gestion des événements relatifs à la sécurité des informations ou des tiers.

Description: la tâche la plus importante des CSIRT est l'acceptation des signalements d'événements relatifs à la sécurité des informations confirmés et potentiels affectant les réseaux, les dispositifs, les composants, les utilisateurs, les organisations ou l'infrastructure des parties prenantes, désignés sous le terme "cibles". Les CSIRT doivent prévoir que les incidents relatifs à la sécurité des informations potentiels pourront être signalés par diverses sources dans différents formats, manuels et automatiques.

Afin d'améliorer l'efficacité du signalement par les parties prenantes, les CSIRT doivent fournir un ou plusieurs mécanismes, ainsi que des orientations ou des instructions, quant au contenu et à la méthode de signalement sécurisée des incidents relatifs à la sécurité des informations. Les mécanismes de signalement peuvent prendre différentes formes: courrier électronique, site web, formulaire, portail dédié au signalement des incidents relatifs à la sécurité des informations ou autres méthodes permettant de soumettre les signalements en toute sécurité et sûreté. Si les orientations concernant le signalement des incidents relatifs à la sécurité des informations ne figurent pas dans le formulaire ad hoc, elles doivent être fournies dans des documents séparés ou via une page web et énumérer les informations spécifiques qu'il est souhaitable d'inclure dans le signalement.

En raison du nombre potentiellement important d'incidents relatifs à la sécurité des informations

potentiels remontés automatiquement après détection via un service de la Gestion des événements relatifs à la sécurité des informations, il est impératif de planifier à l'avance l'adoption de ces interfaces ou l'autorisation préalable de leur utilisation par les parties prenantes[5].

Résultat: la réception, la validation initiale et la classification des signalements d'incidents relatifs à la sécurité des informations sont menées avec professionnalisme et de façon cohérente.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Réception des signalements d'incidents relatifs à la sécurité des informations.
- Tri et traitement des incidents relatifs à la sécurité des informations.

6.1.1 Fonction: réception des signalements d'incidents relatifs à la sécurité des informations

Objectif: accepter ou recevoir des informations à propos d'incidents relatifs à la sécurité des informations signalés par des parties prenantes ou des tiers.

Description: l'efficacité du recueil des signalements d'incidents relatifs à la sécurité des informations requiert des mécanismes et des processus de réception des signalements envoyés par les parties prenantes, les intéressés et des tiers (par exemple, découvreurs, chercheurs, centres de partage et analyse des informations [ISAC], autres CSIRT). Les signalements d'incidents relatifs à la sécurité des informations peuvent mentionner les dispositifs/réseaux/utilisateurs/organisations concernés, les situations déjà identifiées telles que l'exploitation de vulnérabilités, l'impact technique et commercial/administratif et les mesures prises pour lancer les étapes de remédiation et/ou d'atténuation ainsi que leur éventuelle résolution. Parfois, les informations sur les incidents relatifs à la sécurité des informations pourront parvenir avec les données d'autres services, principalement la Réception des signalements de vulnérabilité (par exemple, si un incident relatif à la sécurité des informations signalé a été identifié lors de l'analyse d'un rapport de vulnérabilité). La soumission automatique des signalements pourra éventuellement être prise en compte en fonction d'autres choix des interfaces et des protocoles mis en œuvre.

Résultat: gestion appropriée des signalements d'incidents relatifs à la sécurité des informations émanant de parties prenantes ou de tiers, dont lancement de leur documentation ou de leur suivi.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

[5] Comme l'on peut s'y attendre pour tous les services en rapport avec le recueil d'informations et de données, il existe de nombreuses similitudes. Il est donc courant de combiner ce type de services fournis par plusieurs zones de service en un service/une fonction unique. Comme cela n'est pas obligatoire et qu'il n'existe pas de combinaison fixe des zones de service, nous avons choisi de les présenter séparément dans le Cadre de services de la CSIRT, mais chaque équipe est libre de choisir le modèle organisationnel le mieux adapté à sa situation.

- Surveillance régulière des canaux de communication et vérification de la mesure dans laquelle les méthodes de contact de la CSIRT indiquées sont opérationnelles et permettent de soumettre des signalements.
- Envoi de l'accusé de réception initial à l'auteur du signalement d'un incident relatif à la sécurité des informations demandant, le cas échéant, des informations complémentaires, et définition des attentes avec l'auteur du signalement.

6.1.2 Fonction: tri et traitement des incidents relatifs à la sécurité des informations

Objectif: examen, classification, hiérarchisation et traitement initiaux d'un incident relatif à la sécurité des informations signalé.

Description: les signalements d'incidents relatifs à la sécurité des informations sont soumis à un examen et à un tri afin d'en acquérir une compréhension initiale. Il est particulièrement important de savoir si l'incident exerce un impact réel sur la sécurité des informations de la cible et peut nuire (ou a déjà nui) à la confidentialité, la disponibilité, l'intégrité et/ou l'authenticité des informations ou d'autres ressources. En fonction de la quantité de détails et de la qualité des informations fournies dans le signalement initial, il apparaîtra, ou non, de façon évidente si un véritable incident relatif à la sécurité des informations a eu lieu ou s'il s'agit d'un autre problème, par exemple, une mauvaise configuration ou une défaillance matérielle. L'étape suivante dépendra de l'évaluation préliminaire (par exemple, traitement du signalement aux fins d'analyse complémentaire, demande d'informations supplémentaires à l'auteur du signalement ou à d'autres sources, décision de clore l'incident sans autre intervention ou de le traiter comme une fausse alerte).

Il est possible que des attaques émanent des parties prenantes des CSIRT, qu'elles visent ces parties prenantes ou que seuls des dommages collatéraux atteignent lesdites parties. Si les CSIRT ne fournissent pas d'informations sur les cibles identifiées aux services de la Gestion de la sécurité des informations, le signalement devra être confié en toute sécurité à un groupe externe, tel que la ou les organisations touchées ou une ou plusieurs CSIRT.

Sauf en cas de motif de refus d'un signalement relatif à la sécurité des informations ou de son envoi à une autre entité responsable de sa gestion, les signalements doivent être transmis au service Analyse de vulnérabilité pour un complément d'examen, d'analyse et de gestion.

Résultat: il est possible de déterminer si un problème signalé est bien un incident relatif à la sécurité des informations nécessitant d'être traité par la CSIRT ou s'il convient de le transmettre à une entité compétente.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Traitement des signalements et des données soumises, y compris des artefacts ou des contenus isolés, afin de protéger l'intégrité de l'environnement de travail et d'éviter que les attaques menées contre la CSIRT par ce biais soient couronnées de succès.

- Mise à jour des accusés de réception des signalements en fonction de commentaires sur les étapes complémentaires sur la base des résultats de la classification ou de la hiérarchisation disponibles.
- Fusion des nouvelles informations sur les incidents relatifs à la sécurité des informations déjà traités avec les données disponibles afin d'assurer la cohérence de l'analyse et du traitement.

6.2 Service: analyse des incidents relatifs à la sécurité des informations

Objectif: analyser et comprendre les incidents relatifs à la sécurité des informations confirmés.

Description: ce service regroupe des fonctions visant à comprendre l'incident relatif à la sécurité des informations ainsi que son impact réel et potentiel afin d'identifier les problèmes, les vulnérabilités ou les faiblesses sous-jacentes (causes premières) qui ont permis la réussite de l'attaque, de la compromission ou de l'exploit.

Souvent, les analyses détaillées sont complexes et chronophages. L'objectif consiste à identifier et à caractériser l'incident relatif à la sécurité des informations au niveau de détail requis ou justifié par la compréhension existante de son impact. Les incidents relatifs à la sécurité des informations peuvent être caractérisés par périmètre, entités touchées, outils ou attaques déployés, période, etc. Ce service peut être mené parallèlement au service et aux fonctions de coordination des incidents relatifs à la sécurité des informations ou à des mesures d'atténuation/reprise.

Les CSIRT peuvent utiliser d'autres informations et leurs propres analyses (voir quelques options ci-dessous) ou les connaissances fournies par les fournisseurs, des équipes chargées de la sécurité des produits ou des chercheurs en sécurité pour mieux comprendre ce qui s'est passé et les mesures à prendre pour remédier aux pertes ou aux préjudices.

Résultat: meilleure connaissance des détails importants des incidents relatifs à la sécurité des informations (par exemple, description, impact, périmètre, attaques/exploits et remèdes).

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Tri des incidents relatifs à la sécurité des informations (hiérarchisation et classification).
- Collecte des informations.
- Coordination de l'analyse détaillée.
- Analyse des causes premières des incidents relatifs à la sécurité des informations.
- Corrélation des incidents.

6.2.1 Fonction: Tri des incidents relatifs à la sécurité des informations (hiérarchisation et classification)

Objectif: classer, hiérarchiser et créer une évaluation initiale de l'incident relatif à la sécurité des informations.

Description: le service Analyse des incidents relatifs à la sécurité des informations commence par examiner les informations disponibles afin de classer, hiérarchiser et évaluer l'impact de ces incidents sur les systèmes concernés, conformément au mandat de la CSIRT. Certaines d'entre elles pourront avoir été documentées lors de la fonction Tri et traitement des signalements d'incidents relatifs à la sécurité des informations (du service Réception des signalements d'incidents relatifs à la sécurité des informations), si les incidents en question ont été signalés à la CSIRT par une partie prenante ou un tiers.

En l'absence de tri préalable, l'incident relatif à la sécurité des informations pourra être assigné à un expert à même d'apporter la confirmation technique qu'il a des répercussions sur les systèmes concernés et relève du mandat de la CSIRT (c'est-à-dire un impact potentiel sur la sécurité des réseaux ou des systèmes susceptible de nuire à la confidentialité, la disponibilité ou l'intégrité des informations dans un domaine relevant du mandat de la CSIRT).

Résultat: classification, hiérarchisation et mise à jour des informations sur un incident relatif à la sécurité des informations.

6.2.2 Fonction: Collecte des informations

Objectif: recueillir, cataloguer, stocker et suivre les informations sur les incidents relatifs à la sécurité des informations ainsi que sur tous les événements relatifs à la sécurité des informations considérés comme constitutifs.

Description: collecter toutes les informations utiles afin de comprendre au mieux le contexte de manière à évaluer convenablement l'origine et le contenu des informations et à les baliser à des fins de traitement complémentaire.

Lors de la collecte des informations, il est impératif d'accepter et de respecter les politiques de partage convenues et les limites quant à la nature des données à utiliser dans tel ou tel contexte ou pour tel ou tel type de traitement. Les mécanismes et les procédures de collecte doivent quant à eux assurer l'exactitude de l'étiquetage et de l'attribution des sources afin d'en valider ultérieurement les origines, ainsi que la pertinence ou l'authenticité.

Résultat: existence d'informations structurées sur les données ou les mégadonnées numériques et non numériques collectées assorties d'informations de suivi et de points de contrôle de l'intégrité de la manipulation et du stockage. Selon que les résultats serviront à une analyse future (informelle) ou aux missions des forces de l'ordre, les exigences relatives à l'établissement d'une chaîne de responsabilité formelle susceptible d'être défendue devant les tribunaux à un stade ultérieur différeront.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Évaluation et validation des sources de données et d'informations.
- Collecte des signalements relatifs aux événements malveillants ou suspects, aux événements relatifs à la sécurité des informations, aux incidents relatifs à la sécurité des informations potentiels remontés et/ou aux signalements d'incidents relatifs à la sécurité des informations émanant de parties prenantes et de tiers (par exemple, autres équipes de sécurité ou

organismes de diffusion de renseignements commerciaux), via des formulaires accessibles en lecture manuelle ou automatique, ou déchiffrables par des machines.

- Compilation et recensement des données numériques potentiellement – mais pas nécessairement – utiles pour comprendre l'incident (par exemple, images de disques et de la mémoire, fichiers comportant des métadonnées ou des sommes de contrôle, caractéristiques de l'architecture réseau, journaux), y compris, sans limitation, les artefacts considérés comme les vestiges d'une activité malveillante.
- Compilation et recensement de données non numériques (par exemple, feuilles de présence physique, schémas d'architecture, modèles stratégiques, données d'évaluation des sites, politiques, cadres de risque des entreprises).
- Compilation et recensement i) des métadonnées concernant la source, la méthode de collecte, les personnes ayant manipulé les données ou les objets et le propriétaire, et ii) des informations sur les responsabilités, notamment dans la mesure où elles peuvent servir ultérieurement de preuves pour l'analyse judiciaire ou les missions des forces de l'ordre.

6.2.3 Fonction: Coordination de l'analyse détaillée

Objectif: appliquer et suivre les autres analyses techniques éventuelles en rapport avec un incident relatif à la sécurité des informations.

Description: si une analyse technique plus détaillée s'avère nécessaire, elle pourra être effectuée par d'autres experts (internes ou externes à l'organisation hôte ou à la CSIRT) ou par des tiers (tels qu'un fournisseur de services spécialisé dans ce type d'analyse). Il faut mettre en œuvre et suivre ce type d'activités jusqu'à la réalisation de l'analyse souhaitée.

Résultat: existence d'une liste des analyses en attente et externalisées, du point de vue du responsable de la gestion de l'incident coordonnant la réponse à un incident relatif à la sécurité des informations donné.

6.2.4 Fonction: Analyse des causes premières des incidents relatifs à la sécurité des informations

Objectif: identifier la cause première de l'incident relatif à la sécurité des informations, ainsi que les circonstances ayant permis l'existence des vulnérabilités exploitées ou la réussite de leur exploitation (y compris, sans limitation, le comportement des utilisateurs).

Description: cette fonction recouvre le processus et les actions requis pour comprendre l'architecture, l'usage ou les défaillances de mise en œuvre ayant compromis ou mis en danger des systèmes, des réseaux, des utilisateurs, des organisations, etc., face au type d'attaque, d'exploit ou de compromission visant les cibles d'un incident relatif à la sécurité des informations. Elle s'intéresse également aux circonstances dans lesquelles l'attaquant risque de compromettre d'autres systèmes en élargissant son accès initial.

En fonction de la nature de l'incident relatif à la sécurité des informations, la CSIRT pourra avoir du mal à assurer cette fonction de A à Z. Dans de nombreux cas, il est préférable que la cible concernée s'en charge, car, notamment dans le contexte des CSIRT de coordination, il n'existe aucune connaissance technique des systèmes ou des réseaux compromis.

Résultat: compréhension de l'incident relatif à la sécurité des informations et de la manière dont les acteurs malveillants ont obtenu l'accès initial et l'ont utilisé par la suite permettant de déterminer les méthodes de remédiation ou d'atténuation afin de réduire le risque futur d'exposition ou d'exploitation grâce à l'élimination des causes premières.

6.2.5 Fonction: Corrélation des incidents

Objectif: utiliser toutes les informations disponibles pour comprendre au mieux le contexte et détecter les interrelations qui, à défaut, n'auraient pas été reconnues ou traitées.

Description: cette fonction porte sur la corrélation entre les informations disponibles à propos de multiples incidents relatifs à la sécurité des informations afin de déterminer les interrelations, les tendances ou les atténuations applicables à partir d'incidents relatifs à la sécurité des informations déjà clos pour améliorer la réponse aux incidents de même nature en cours de traitement.

Résultat: compréhension de la situation globale grâce à une connaissance détaillée des similitudes et des interrelations confirmées ou soupçonnées entre des incidents relatifs à la sécurité des informations indépendants par ailleurs.

6.3 Service: analyse des artefacts et des preuves judiciaires

Objectif: analyser et comprendre les artefacts en rapport avec un incident relatif à la sécurité des informations confirmé en tenant compte de la nécessité de protéger les preuves judiciaires.

Description: services liés à la compréhension des capacités et des intentions des artefacts (par exemple, logiciels malveillants, exploits, images de mémoire volatile ou copies de disques, codes d'applications, journaux, documents), leurs mécanismes de diffusion, leur propagation, leur détection, leur atténuation et leur désamorçage ou leur neutralisation. Ils s'appliquent à tous les formats et toutes les sources: matériels, micrologiciels, mémoire, logiciels, etc. Tous les artefacts et toutes les preuves doivent être préservés et collectés sans modification et conservés séparément. Comme certains artefacts et données risquent de devenir des preuves dans le cadre des missions des forces de l'ordre, des règlements ou des exigences spécifiques peuvent s'appliquer.

Même sans chaîne de responsabilités, ce service implique en général des tâches chronophages complexes et requiert de l'expertise, la mise en place d'environnements d'analyse dédiés et surveillés, avec ou sans accès externe à partir de réseaux filaires ou sans fil standard (tels que l'exécution des activités judiciaires dans une salle scellée ou de Faraday), la consignation des activités et le respect des procédures.

Dans le cadre de la gestion des incidents relatifs à la sécurité des informations, 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 intrusion, comme des scripts, des fichiers, des images, des fichiers de configuration, des outils, les résultats d'un outil, des journaux, de morceaux de code actifs ou en sommeil, etc.

L'analyse a pour but de trouver tout ou partie des informations énumérées dans la liste non

exhaustive ci-dessous:

- Contexte permettant à l'artefact de s'exécuter et d'effectuer les tâches qui lui sont dévolues, malveillantes ou non.
- Mode d'utilisation des artefacts pour l'attaque: téléversement, téléchargement, copie, exécution ou création au sein des environnements ou des composantes de l'organisation.
- Systèmes locaux et distants ayant permis la diffusion et les actions.
- Nature des actions de l'auteur de l'intrusion après avoir accédé au système, au réseau, à l'organisation ou à l'infrastructure: recueil passif de données, numérisation et transmission actives de données aux fins d'exfiltration, collecte de requêtes de nouvelles actions, auto-actualisation ou déplacement latéral au sein d'un réseau (local) compromis.
- Nature des actions d'un utilisateur, d'un processus utilisateur ou d'un système utilisateur une fois le compte ou le dispositif utilisateur compromis.
- Comportement caractéristique des artefacts ou des systèmes compromis soit de façon autonome conjointement à des artefacts ou des composants à partir d'une connexion à un réseau local ou à Internet, soit en association.
- Mode d'établissement de la connectivité entre les artefacts ou les systèmes compromis et la cible (par exemple, chemin de l'intrusion, cible initiale ou techniques d'évasion de la détection).
- Type d'architecture de communication utilisé (homologue à homologue et/ou commande-contrôle).
- Nature des actions des auteurs de la menace, type d'empreinte réseau et systèmes.
- Méthode d'évitement de la détection des auteurs de l'intrusion ou des artefacts (même sur de longues durées pouvant inclure un redémarrage ou une réinitialisation).

L'analyse peut faire appel à divers types d'activités tels que:

- analyse des supports physiques ou des surfaces;
- rétro-ingénierie;
- analyse de l'exécution ou analyse dynamique;
- analyse comparative.

Chaque activité fournit des informations supplémentaires sur les artefacts. 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 d'exécution ou d'exploitation 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 détecter la vulnérabilité exploitée, 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: analyse de la nature des artefacts numériques récupérés, des preuves judiciaires analysées, de la relation à d'autres artefacts, objets ou composants internes ou externes; bonne

compréhension des attaques d'infrastructures, des outils et des vulnérabilités exploitées. Hypothèses de travail ou preuve de ce qu'a fait l'auteur de la menace et du mode de fonctionnement des artefacts. Ces connaissances sont cruciales pour évaluer les pertes, les préjudices, les impacts sur l'entreprise, etc., ainsi que pour élaborer des stratégies d'endiguement et d'atténuation ou de retour à la normale. Compréhension des tactiques, des techniques et des procédures utilisées par les auteurs des attaques ou des intrusions visant à compromettre les systèmes, les utilisateurs, les réseaux, les organisations et/ou les infrastructures. Les tactiques, techniques et procédures en question sont celles ayant servi à propager, exfiltrer, actualiser, modifier ou imiter des comportements, des données, des traces d'autosuppression d'activités ou l'exécution d'autres activités malveillantes.

Liste des fonctions considérées comme faisant partie de la mise en œuvre de ce service:

- Analyse des supports physiques ou des surfaces.
- Rétro-ingénierie.
- Analyse de l'exécution et/ou analyse dynamique.
- Analyse comparative.

6.3.1 Fonction: Analyse des supports physiques ou des surfaces

Objectif: comparer les informations recueillies sur l'artefact à d'autres artefacts publics et privés et/ou à des bases de données de signatures

Description: cette fonction recouvre l'identification et la caractérisation des informations de base et des métadonnées relatives aux artefacts, y compris, sans limitation, les types de fichiers, les sorties de chaînes, le hachage de chiffrement, les certificats, les tailles de fichiers, les noms de fichiers/répertoires. Comme toutes les informations disponibles sont collectées et analysées, elles peuvent éventuellement servir à examiner les bases de données d'informations publiques/ouvertes ou privées/fermées pour approfondir les connaissances sur l'artefact ou son comportement, puisque ces informations peuvent servir à décider des étapes suivantes.

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.

6.3.2 Fonction: Rétro-ingénierie

Objectif: exécuter l'analyse statique approfondie d'un artefact dans le but de déterminer l'ensemble de ses fonctionnalités, quel que soit son environnement d'exécution.

Description: 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. L'analyste décode l'ensemble du langage machine et dévoile les fonctions et les actions du logiciel malveillant. La rétro-ingénierie est une analyse approfondie réalisée quand les analyses

de surface et de l'exécution ne permettent pas d'obtenir les informations requises.

Résultat: Détermination de 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 ses préjudices potentiels afin d'élaborer des solutions d'atténuation et, si nécessaire, de créer une nouvelle signature aux fins de comparaison avec d'autres échantillons.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Analyse statique.
- Rétro-ingénierie du code.
- Analyse et description du comportement potentiel.
- Conception potentielle de la signature.

6.3.3 Fonction: analyse de l'exécution ou analyse dynamique

Objectif: donner un aperçu du fonctionnement de l'artefact

Description: cette fonction permet de comprendre les capacités d'un artefact en en observant l'exécution dans un environnement réel ou émulé (par exemple, carré, environnement virtuel et émulateurs matériels ou logiciels).

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: Recueil de détails supplémentaires sur le fonctionnement de l'artefact numérique grâce à l'observation de 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, de créer de nouvelles signatures pour l'artefact et de déterminer des mesures d'atténuation.

Note: l'analyse de l'exécution ne révèle pas l'intégralité des 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.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Préparation d'un environnement d'analyse (en exploitation/restreinte/fermée, émulée/simulée).
- Préparation des dispositifs de collecte, des capteurs et/ou des sondes.

- Collecte des données et des métadonnées initiales relatives au comportement.
- Sondage de l'artefact à plusieurs moments dans des contextes différents.
- Exécution d'une analyse de comportement des systèmes et/ou du réseau, à court et long termes
- Émission de conclusions à partir de l'évaluation de l'ensemble des résultats et des données collectés en comparant les divers résultats et en recherchant dans les bases de connaissances existantes des résultats techniques correspondant aux éléments découverts.

6.3.4 Fonction: Analyse comparative

Objectif: exécuter une analyse visant à identifier les fonctionnalités et les intentions communes, y compris l'examen par famille d'artefacts recensés.

Description: cette fonction consiste à explorer la relation d'un artefact avec d'autres. Elle révèle parfois des similitudes en termes de code ou de mode opératoire, de cibles, d'intention et d'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: recensement des points communs ou des relations avec d'autres artefacts en vue d'identifier des tendances ou des similitudes qui permettront de mieux saisir les fonctionnalités et les effets d'un artefact numérique, ainsi que la façon d'en atténuer l'action.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Définition de caractéristiques et de comportements de référence observés.
- Recherche de caractéristiques identiques ou similaires dans les bases de données/connaissances existantes.
- Mise à jour des bases de données/connaissances existantes avec les symptômes, comportements et/ou signatures nouveaux ou inconnus auparavant pouvant servir à affiner la classification de l'artefact objet de la recherche.

6.4 Service: Atténuation et reprise

Objectif: maîtriser au maximum les incidents relatifs à la sécurité des informations afin de limiter le nombre de victimes, de réduire les pertes, de se remettre des préjudices et d'éviter d'autres attaques et d'autres pertes en supprimant les vulnérabilités ou les failles exploitées; améliorer la cybersécurité globale.

Description: la confirmation par l'analyse d'un incident potentiel relatif à la sécurité des informations et l'élaboration d'une stratégie de riposte doivent être transformées en plan de riposte. Avant même la finalisation de ce plan, des mesures ad hoc pourront être prises. Ce

service comprend également le lancement et le suivi de toutes les activités exécutées jusqu'à ce que l'on puisse considérer l'incident relatif à la sécurité des informations comme clos ou jusqu'à ce qu'apparaissent de nouvelles informations nécessitant une analyse approfondie, ce qui peut également modifier la stratégie et le plan de riposte.

Résultat: atténuation de l'incident relatif à la sécurité des informations et amélioration de la cybersécurité. Les systèmes touchés par l'attaque sous-jacente ou les activités de son auteur sont restaurés. Le réseau et les systèmes compromis redeviennent disponibles. Les données éventuellement perdues sont restaurées, dans la mesure du possible.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Établissement d'un plan de riposte.
- Mesures ad hoc et endiguement.
- Restauration des systèmes.
- Appui à d'autres entités en charge de la sécurité des informations.

Les CSIRT de coordination ne disposent pas de toutes les fonctions. Bien que "soutenir les autres entités chargées de la sécurité des informations" fasse partie de leurs activités, elles aident également parfois à "établir un plan de riposte".

6.4.1 Fonction: Établissement d'un plan de riposte

Objectif: définir et appliquer un plan visant à restaurer l'intégrité des systèmes touchés et à repasser les données, les systèmes et les réseaux concernés à un état opérationnel non dégradé grâce à la reprise de toutes les fonctionnalités des services touchés sans recréer le contexte ayant permis l'existence initiale de la faille de sécurité exploitée.

Description: il ne sera pas possible de riposter de façon efficace si l'impact sur l'entreprise et les exigences de l'atténuation et du retour à la normale ne sont pas pleinement compris. Du fait de l'existence d'un conflit d'intérêts (suivre l'attaque pour obtenir le maximum de renseignements ou maîtriser l'attaque pour éviter d'aggraver les pertes), il faut tenir compte de tous les intérêts et formuler un plan de riposte plausible compte tenu des faits connus et apte à parvenir au résultat souhaité dans les délais requis.

Comme pour tous les plans, il faut impérativement tenir compte du fait que les résultats des nouvelles analyses requièrent l'examen des nouveaux éléments découverts. De fait, il conviendra habituellement de modifier le plan de riposte pour fournir des instructions et des orientations en continu. À défaut – sauf à ce que la riposte soit gérée par un petit groupe opérationnel n'ayant que des besoins limités d'interfaces externes ou d'autres entités – il ne sera pas possible d'effectuer les activités avec efficacité ou efficience en raison de l'absence de coordination.

Résultat: exécution d'un plan de riposte convenu répondant aux exigences de l'entreprise à condition qu'il soit assisté par des ressources disponibles et bénéficie d'un appui. Dans le cadre des CSIRT, le service Coordination assurera le suivi et la coordination.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Détermination de l'impact commercial des incidents relatifs à la sécurité des informations.
- Détermination des besoins de l'organisation et planning d'une reprise réussie.
- Définition des processus et des critères décisionnels (si non définis par des politiques existantes).
- Identification des objets à réactiver: environnements, systèmes, applications, fonctions transversales, etc.
  - Identification de l'appui et des actions requis de la part d'entités internes et externes.
  - Élaboration d'un plan de riposte permettant une intervention efficace dans le cadre des exigences et du calendrier requis par l'organisation sur la base des ressources disponibles et du périmètre technique des actions nécessaires.

6.4.2 Fonction: Mesures ad hoc et endiguement

Objectif: mettre en œuvre des mesures garantissant la non-propagation de l'incident relatif à la sécurité des informations, c'est-à-dire son confinement au système, aux utilisateurs et/ou aux domaines touchés afin d'éviter des pertes supplémentaires (y compris fuite de documents, modifications des bases de données ou des données, etc.).

Description: le défi immédiat en cas d'incident relatif à la sécurité des informations est d'en arrêter la propagation. Tant que des systèmes sont compromis ou que des logiciels malveillants sont actifs sur les systèmes des utilisateurs finaux, les pertes de données et les cibles compromises risquent de se multiplier. L'objectif principal des attaques est principalement de toucher des données et des systèmes spécifiques, y compris les attaques (dont, entre autres, les mouvements latéraux) en direction d'autres entités intérieures ou extérieures à l'organisation victime de l'incident relatif à la sécurité des informations. L'arrêt ou, au minimum, la limitation de la portée des activités malveillantes ou des pertes, requiert des mesures à court terme telles que le blocage ou le filtrage du trafic et de l'accès à des services ou des systèmes spécifiques et peut également entraîner la déconnexion de systèmes cruciaux.

Le refus d'accès à des données constituant potentiellement des preuves critiques en permettra l'analyse exhaustive. Le refus d'accès à d'autres systèmes et réseaux limitera également la redevabilité liée aux préjudices subis par d'autres organisations.

L'arrêt immédiat des préjudices et la limitation de la portée de l'activité malveillante au moyen de mesures tactiques à court terme (par exemple blocage ou filtrage du trafic) peuvent également impliquer de reprendre le contrôle des systèmes. Tant que les auteurs des attaques ou les logiciels malveillants peuvent facilement accéder à d'autres systèmes ou réseaux, aucun retour à un fonctionnement normal ne sera possible.

Résultat: récupération du contrôle sur les systèmes et les réseaux concernés. L'accès aux données, aux systèmes et aux réseaux est refusé aux auteurs des attaques ou aux logiciels malveillants afin d'éviter d'autres attaques et/ou dommages affectant les systèmes et les données.

Les sous-fonctions suivantes pourraient faire partie de la mise en œuvre de cette fonction:

- Blocage temporaire de l'accès par les utilisateurs/systèmes/services/réseaux.
- Déconnexion temporaire des réseaux ou des dorsales des systèmes ou des réseaux.
- Désactivation temporaire des services.
- Obligation pour les utilisateurs de modifier leurs mots de passe ou leurs identifiants chiffrés.
- Surveillance de signes d'intrusion et indicateurs de compromission.
- Vérification que tous les utilisateurs/systèmes/services/réseaux ne sont pas touchés.

6.4.3 Fonction: restauration des systèmes

Objectif: mettre en œuvre les modifications requises dans le domaine, l'infrastructure ou le réseau touchés pour remédier au problème et empêcher la récidive de ce type d'activité.

Description: restaurer l'intégrité des systèmes touchés et repasser les données, systèmes et réseaux touchés à un état opérationnel non dégradé, restaurer toutes les fonctionnalités des services touchés. Alors qu'il est généralement impératif pour les organisations que les systèmes recommencent à fonctionner normalement le plus vite possible, le risque demeure que tous les moyens d'accès non autorisés n'aient pas été supprimés. Par conséquent, sauf si les résultats de l'analyse sont déjà disponibles, même les systèmes réactivés doivent être surveillés et gérés avec soin. Notamment lorsque les vulnérabilités et les failles identifiées ne peuvent pas (encore) être éliminées, il faut appliquer des mécanismes de protection et de détection pour éviter des incidents relatifs à la sécurité des informations identiques ou similaires.

Résultat: application de mesures visant à restaurer les systèmes et les services à leur pleine fonctionnalité/capacité. Des mesures sont appliquées pour mettre un terme aux vulnérabilités ou aux failles détectées ayant contribué à l'incident relatif à la sécurité des informations originel. Les mesures de détection et de réaction sont améliorées conformément aux recommandations de l'analyse et du plan de riposte.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Restauration des données utilisateurs/systèmes à partir de supports physiques de sauvegarde de confiance.
- Restauration des configurations à partir de supports physiques de sauvegarde de confiance ou recréation des contenus.
- Réactivation des services désactivés et rétablissement de l'accès pour les utilisateurs/systèmes/réseaux.
- Exécution d'essais fonctionnels pour valider la capacité des systèmes/services/réseaux au niveau de l'infrastructure et des applications.

6.4.4 Fonction: Appui à d'autres entités en charge de la sécurité des informations

Objectif: permettre aux parties prenantes d'effectuer les activités de gestion et techniques requises pour atténuer un incident relatif à la sécurité des informations et assurer la reprise.

Description: les CSIRT peuvent apporter une assistance directe (sur site) pour aider les parties prenantes à se relever des pertes et à éliminer les vulnérabilités. Il pourra s'agir d'une extension directe de l'offre de services d'analyse sur site (voir ci-dessus). D'un autre côté, les CSIRT pourront choisir de soutenir le personnel des parties prenantes chargé de la riposte à l'incident relatif à la sécurité des informations avec des explications détaillées, des recommandations, etc.

Résultat: amélioration de la riposte des parties prenantes et accélération de la reprise. L'ajout au corpus existant de connaissances peut renforcer l'efficacité et l'efficience futures des activités connexes. De plus, il aide à soutenir les entités des parties prenantes qui manquent de connaissances techniques détaillées pour effectuer l'action de riposte nécessaire.

6.5 Service: coordination des incidents relatifs à la sécurité des informations

Objectif: assurer en temps utile les notifications et la distribution d'informations exactes; maintenir le flux des informations et suivre l'état des activités des entités chargées, de par leur mission ou sur demande, de participer à la réaction à l'incident relatif à la sécurité des informations; s'assurer que le plan d'intervention est mené à bien et que les déviations entraînées par les retards ou de nouvelles informations sont gérées comme il convient.

Description: il est crucial pour toutes les acteurs et les organisations concernés d'être notifiées et tenues au courant des détails et des activités en cours concernant un incident relatif à la sécurité des informations. Dans la mesure où certaines activités requises pour la réussite de l'atténuation et du rétablissement sont susceptibles de nécessiter l'approbation de la direction, il faut établir des fonctions adaptées de remontée et de signalement pour pouvoir gérer avec efficacité et efficience l'incident relatif à la sécurité des informations. Dans la mesure où les équipes CSIRT analysent toutes les informations à mesure qu'elles apparaissent, la coordination garantit que les notifications et les informations parviennent aux bons points de contact, suit leurs réactions et veille à ce que toutes les parties menant les activités rendent compte afin de fournir une appréciation exacte de la situation jusqu'à ce que l'incident relatif à la sécurité des informations soit considéré comme clos et que la coordination ne soit plus nécessaire.

Les acteurs doivent disposer de canaux par lesquels soumettre leurs questions, vérifier le statut des incidents relatifs à la sécurité des informations et signaler les problèmes aux équipes CSIRT. Pour assurer la participation des acteurs internes, les équipes CSIRT doivent mettre à disposition des canaux de communication afin d'informer sur l'état de résolution des incidents relatifs à la sécurité des informations. Afin d'assurer la participation des acteurs externes, les équipes CSIRT doivent maintenir des canaux de communication avec les autres équipes CSIRT et communautés d'équipes CSIRT susceptibles d'émettre des recommandations ou d'apporter une assistance technique.

Résultat: bonne coordination de la réaction sur la base d'entités bien informées qui contribuent à réagir à un incident relatif à la sécurité des informations.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Communication.
- Distribution des notifications.
- Distribution des informations pertinentes.
- Coordination des activités.
- Signalements.
- Communication médiatique.

6.5.1 Fonction: Communication

Objectif: faire participer efficacement les acteurs et établir plusieurs canaux de communication garantissant la confidentialité requise.

Description: Toute équipe CSIRT doit élaborer et publier leurs messages à l'intention d'un public ciblé. Elle doit également être à même de recevoir les retours d'informations, les rapports, les commentaires et les questions en provenance de diverses sources sur la base de sa propre communication.

La politique de sécurité et celle relative au partage des informations peuvent imposer une gestion des règles strictes. Les équipes CSIRT doivent pouvoir informer les acteurs externes et internes de manière fiable, sécurisée et privée.

Il convient de mettre en place des accords de non-divulgation aussi tôt que possible ainsi que des ressources de communication adaptées. Il est également possible d'aller jusqu'au concept "d'embargo sur les informations". De ce fait, il faut instaurer une politique de rétention qui garantisse que les données servant à créer les informations et les informations elles-mêmes soient convenablement gérées, partagées et conservées sur la base de contraintes – notamment de temps – jusqu'à ce que ces contraintes n'aient plus lieu d'être ou à ce que les informations soient rendues publiques.

Les canaux de communication peuvent prendre de multiples formes en fonction des besoins des acteurs et parties prenantes. Toutes les informations communiquées doivent être balisées conformément à la politique de partage des informations. Il est possible d'utiliser un protocole du type feux de circulation.

Résultat: tous les canaux de communication sont disponibles en fonction des exigences de sécurité de toutes les parties émettrices et réceptrices.

Les sous-fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de cette fonction:

- Fourniture de canaux de communication internes.
- Fourniture de canaux de communication externes.

6.5.2 Fonction: Distribution des notifications

Objectif: alerter les entités concernées par l'incident relatif à la sécurité des informations ou celles susceptibles de participer à la réaction et leur fournir les informations requises pour comprendre leur rôle ainsi que les éventuelles attentes quant à leur coopération et à leur appui.

Description: les incidents de sécurité touchent de nombreuses entités internes et potentiellement externes ainsi que, le cas échéant, des systèmes et des réseaux. Étant donné que les équipes CSIRT constituent un point central de réception des rapports d'incidents relatifs à la sécurité des informations potentiels, elles servent aussi de centre de notification des points de contact autorisés. D'ordinaire, les notifications fournissent non seulement les détails techniques nécessaires, mais aussi des informations sur la réaction attendue et un point de contact pour le suivi.

Résultat: mise à disposition des entités devant participer à la réaction ou en être informées d'informations sur les incidents relatifs à la sécurité des informations.

6.5.3 Fonction: Distribution des informations pertinentes

Objectif: maintenir la communication avec les entités identifiées et assurer un flux d'informations disponibles adapté pour permettre à ces entités de profiter des idées existantes et des enseignements tirés afin d'appliquer de meilleures réactions ou de prendre de nouvelles mesures ad hoc.

Description: à mesure que la réaction à un incident relatif à la sécurité des informations progresse, des résultats d'analyse et des rapports supplémentaires émanant potentiellement d'autres experts en matière de sécurité, d'équipes CSIRT ou de victimes apparaissent.

Il peut être utile de transmettre certaines des informations et certains des enseignements tirés à la zone de service Transfert des connaissances (s'il existe) afin d'améliorer la formation et les documents techniques ainsi que de contribuer à sensibiliser à ces problèmes, notamment en cas d'identification de nouvelles attaques ou tendances d'incidents.

Résultat: distribution des informations disponibles aux parties prenantes de la réaction ou aux personnes devant être informées de l'avancement et du statut de la gestion de l'incident.

6.5.4 Fonction: Coordination des activités

Objectif: suivre le statut de toutes les communications et activités.

Description: Étant donné que de nombreuses entités participent potentiellement à la réaction à un incident relatif à la sécurité des informations, le statut de l'ensemble des communications et activités doit faire l'objet d'un suivi. Cela comprend les actions requises par une équipe CSIRT ou les demandes de partage d'autres informations ainsi que les demandes d'analyse technique des artefacts ou le partage d'indicateurs de compromission, d'informations sur les autres victimes, etc. La coordination des activités est principalement de mise lorsque l'équipe CSIRT dépend d'une expertise et de ressources échappant à son contrôle direct, afin de mener les actions nécessaires à l'atténuation d'un incident. Mais cela vaut également au sein de grandes

organisations où une équipe CSIRT interne coordonne les activités d'atténuation et de rétablissement.

En offrant des services de coordination bilatérale ou multilatérale, l'équipe CSIRT participe à un échange d'informations qui permet de donner aux ressources les capacités d'agir ou d'aider leurs pairs à détecter les activités des auteurs des attaques, à s'en protéger ou à les corriger et à clore l'incident relatif à la sécurité des informations.

Résultat: connaissance du statut de toutes les activités et de celui des parties prenantes de la réaction.

6.5.5 Fonction: Signalements

Objectif: faire en sorte que toutes les entités concernées d'une entreprise soient informées du statut des activités en cours afin de décider des étapes suivantes sur la base de la meilleure connaissance possible de la situation.

Description: fournir des informations concises et factuelles sur le statut des activités requises ou effectuées en réaction à un incident relatif à la sécurité des informations. Au lieu d'attendre une demande de ce type d'information dans le cadre d'une action coordonnée en cours requise pour le succès de la réaction, la fourniture de rapports au moment opportun joue un rôle crucial dans l'efficacité de la coordination.

Résultat: information des acteurs internes de la portée des activités en cours, des actions terminées et de celles en attente. En outre, la communication de l'impact des retards évalué, des recommandations et des actions demandées permet de comprendre l'impact global sur la stratégie d'intervention adoptée et le plan élaboré.

6.5.6 Fonction: Communication médiatique

Objectif: collaborer avec les médias (publics) pour fournir des informations factuelles, exactes et faciles à comprendre sur les événements en cours afin d'éviter la propagation de rumeurs et d'informations trompeuses.

Description: la communication avec les médias n'est pas possible dans de nombreux cas. Bien que les équipes CSIRT s'efforcent généralement d'éviter ce type de contact, il est important de comprendre que les médias peuvent aider à atténuer des types spécifiques d'attaques en cours et à grande échelle à l'origine d'incidents relatifs à la sécurité des informations. Pour ce faire, il faut expliquer la cause des incidents relatifs à la sécurité des informations ainsi que leur impact sur les utilisateurs et/ou les organisations. Dans certains cas, une équipe CSIRT peut choisir dès le début de fournir ces informations d'une manière adaptée à leur communication au grand public; mais il ne fait aucun doute que cette approche des compétences internes spécifiques que ne détiennent pas la plupart des équipes CSIRT. Dans tous les cas, toute équipe CSIRT qui communique avec les médias doit veiller avec la plus grande diligence à simplifier autant que possible les aspects techniques et à ne divulguer aucune information confidentielle.

Résultat: constitution d'informations factuelles résumant clairement l'incident relatif à la sécurité des informations en cours, y compris les mesures à prendre par les victimes potentielles ou les grandes lignes de la stratégie d'intervention choisie pour assurer le retour à la normale.

6.6 Service: appui à la gestion de crise

Objectif: fournir une expertise et des contacts à d'autres experts en matière de sécurité, équipes CSIRT et communautés de CSIRT afin d'aider à atténuer la crise.

Description: bien qu'actuellement les incidents relatifs à la sécurité des informations constituent rarement une crise organisationnelle ou nationale, ils en ont le potentiel. Mais la réaction à une crise est généralement associée à une urgence qui menace le bien-être des individus et des sociétés ou au moins l'existence d'une organisation. Comme il est établi dans la gestion de crise, un rôle de haut rang endossera la responsabilité de la crise et modifiera de ce fait la chaîne de responsabilité habituelle pendant la durée de la situation d'urgence.

Dans la mesure où les systèmes et les réseaux risquent de contribuer aux situations d'urgence ou doivent être disponibles pour y réagir, les équipes CSIRT constitueront généralement une ressource cruciale pour la gestion de ces situations et apporteront à la fois une expérience précieuse, des services rodés et des réseaux de points de contact.

Résultat: possibilité d'utilisation par l'équipe de gestion de crise des ressources des équipes CSIRT pour traiter les aspects de la crise relatifs à la cybersécurité. Dans le même temps, les ressources de communication des équipes CSIRT peuvent servir à contacter les acteurs internes et externes pour leur demander de l'aide ou de mener des actions de soutien spécifiques. Elles peuvent également servir à communiquer de façon fiable avec les parties prenantes à l'aide de moyens de communication rodés et de réseaux de confiance.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Distribution des informations aux parties prenantes.
- Signalements relatifs à l'état de la sécurité des informations.
- Communication des décisions stratégiques.

6.6.1 Fonction: Distribution des informations aux parties prenantes

Objectif: fournir des ressources de communication rodées pour aider à réagir à la crise.

Description: à mesure que la réaction à la crise progresse, il faut impérativement distribuer les informations. Dans la mesure où les équipes CSIRT ont mis en place ce type de ressources dans leur propre intérêt, l'équipe de gestion de crise peut juger opportun ou nécessaire de les utiliser.

Résultat: distribution des informations disponibles aux parties prenantes grâce à des relations de confiance établies qui rassurent les destinataires sur l'exactitude des informations diffusées.

6.6.2 Fonction: Signalements relatifs à l'état de la sécurité des informations

Objectif: garantir que l'équipe de gestion de crise a une vue d'ensemble exhaustive des incidents relatifs à la sécurité des informations en cours et des vulnérabilités connues afin d'en tenir compte dans ses priorités et stratégies globales.

Description: la fonction consiste à fournir des informations concises et factuelles sur l'état actuel de la cybersécurité au sein des parties prenantes. Étant donné qu'une crise risque de servir de point de départ à d'autres attaques ou que des attaques sont susceptibles de faire partie des activités globales à l'origine de la crise, il est impératif que l'équipe de gestion de crise connaisse l'ensemble de la situation.

Les équipes CSIRT peuvent informer leurs services et leurs parties prenantes de leur connaissance de la situation. Les politiques standards peuvent l'exiger ou l'attendre en période de crise. Dans tous les cas, la réussite de la gestion de crise dépend du flux des informations en place. Dans la mesure où elle requiert des ressources coordonnées pour traiter les aspects primordiaux de la crise, les signalements doivent être précis, exacts et fournis en temps utile.

Étant donné que des ressources seront nécessaires à la gestion des incidents relatifs à la sécurité des informations en cours, il faut prendre une décision quant à la suspension de la réaction pour toute la durée de l'incident (ce qui permettrait d'allouer les ressources débloquées à d'autres domaines) ou sa poursuite. Des décisions raisonnables ne peuvent être prises que sur la base de la meilleure connaissance possible de la situation.

Résultat: information de l'équipe de gestion de crise de la portée des activités en cours, des actions terminées et de celles en attente. En outre, la communication de l'impact des retards évalué, des recommandations et des actions demandées permet de comprendre l'impact global sur la stratégie choisie pour faire face à la crise en cours.

6.6.3 Fonction: Communication des décisions stratégiques

Objectif: informer les autres entités au moment opportun de l'impact de la crise sur des incidents relatifs à la sécurité des informations en cours.

Description: informer les autres entités au moment opportun de l'impact de la crise sur des incidents relatifs à la sécurité des informations en cours permet de bien comprendre le type de soutien que les équipes CSIRT peuvent également apporter pendant la crise et assure que les entités savent à quoi s'attendre. Cela garantit également que les autres parties cessent de soutenir ou d'interagir avec les équipes CSIRT lorsqu'elles estiment que la crise prend le dessus.

Tandis que l'équipe de gestion de crise risque de décider de repousser la réaction à un incident relatif à la sécurité des informations en raison d'une crise, ces décisions doivent être communiquées à l'ensemble des entités alors informées et impliquées. Cela vise à éviter les malentendus et d'autres problèmes susceptibles de faire perdre confiance dans les équipes CSIRT et/ou l'organisation hôte.

Résultat: distribution des informations sur l'impact de la crise sur le fonctionnement des équipes CSIRT aux parties internes et aux autres entités impliquées dans la réaction à des incidents relatifs à la sécurité des informations en cours. Les attentes des équipes CSIRT à l'égard de ces entités sont clairement énoncées et garantissent que les besoins en informations des équipes CSIRT sont clairement communiqués.

7 Zone de service: Gestion des vulnérabilités

La zone de service Gestion des vulnérabilités regroupe les services liés à la découverte, l'analyse et la gestion des vulnérabilités des systèmes d'information nouvelles ou signalées. Elle inclut également des services liés à la détection de vulnérabilités connues et à la réaction le cas échéant afin d'en prévenir l'exploitation. Par conséquent, cette zone de service englobe des services liés à des vulnérabilités nouvelles et connues.

Bien que la collocation "gestion des vulnérabilités" désigne parfois le simple processus de prévention de l'exploitation de vulnérabilités connues (par exemple, "recensement et correction"), dans le présent Cadre des services des équipes CSIRT, ces activités sont considérées comme des fonctions et des sous-fonctions d'un service appelé Intervention en cas de vulnérabilité, qui est l'un des services que sont susceptibles de fournir les équipes CSIRT. Pour de nombreuses équipes CSIRT, ces fonctions d'interventions en cas de vulnérabilité relèvent d'autres rôles chargés de recenser et de corriger les vulnérabilités.

Les services suivants sont considérés comme relevant des offres de cette zone de service :

- Découverte/recherche de vulnérabilités.
- Recueil des rapports de vulnérabilité.
- Analyse des vulnérabilités.
- Coordination des vulnérabilités.
- Divulgation des vulnérabilités.
- Intervention en cas de vulnérabilité.

Peu d'équipes CSIRT proposeront l'ensemble de ces services. En revanche, elles fourniront ceux relevant de leur domaine de responsabilité. À titre d'exemple, une équipe CSIRT peut limiter ses services à la prise de connaissance d'une nouvelle vulnérabilité à partir de sources publiques (Découverte/recherche de vulnérabilités) ou tierces (Recueil des rapports de vulnérabilité), puis à l'émission d'une alerte de sécurité au profit de ses parties prenantes (Divulgation des vulnérabilités) le cas échéant, sans nécessairement participer à des efforts de coordination avec les fournisseurs de produits ou autres qui développent une solution (Coordination des vulnérabilités), ni participer au déploiement direct d'une réparation (Intervention en cas de vulnérabilité).

7.1 Service: Découverte/recherche de vulnérabilités

Objectif: identifier, rechercher des vulnérabilités nouvelles (ou précédemment inconnues) ou en être informé. Les vulnérabilités peuvent être découvertes par des membres de la zone de service Gestion des vulnérabilités ou au moyen d'autres activités apparentées des équipes CSIRT.

Description: la découverte d'une nouvelle vulnérabilité est la première étape nécessaire du cycle de vie global de gestion des vulnérabilités. Ce service comprend les fonctions et les activités que les équipes CSIRT sont susceptibles d'être amenées à assumer ou mener activement dans le cadre de leurs propres recherches ou d'autres services pour découvrir une nouvelle vulnérabilité. Les fonctions et les activités liées à la réception passive d'informations sur une nouvelle

vulnérabilité de la part d'un tiers sont décrites plus loin dans le cadre du service Recueil des rapports de vulnérabilité. Il peut arriver qu'une équipe CSIRT découvre une nouvelle vulnérabilité lors d'autres activités, telles que l'analyse ou l'étude d'un rapport d'incident. Une autre façon de prendre connaissance d'une nouvelle vulnérabilité est la lecture de sources publiques (par exemple, sites Web, listes de diffusion[6]), d'autres sources externes (par exemple, services premium, abonnements) ou en recherchant activement et délibérément les vulnérabilités (par exemple, tests à données aléatoires, rétro-ingénierie). Les découvertes doivent être documentées et incorporées aux processus de gestion de vulnérabilité de l'organisation, quelle que soit la manière dont l'équipe CSIRT a identifié ou pris connaissance de la vulnérabilité.

Résultat: découverte d'un nombre accru de vulnérabilités potentielles non signalées directement à l'équipe CSIRT.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Découverte de vulnérabilités lors de l'intervention en cas d'incident.
- Découverte de vulnérabilités à partir de sources publiques.
- Recherche de vulnérabilités.

Ces fonctions peuvent être des services (ou des fonctions) exécutés par d'autres acteurs (par exemple des chercheurs, fournisseurs, équipes PSIRT ou spécialistes tiers) que l'équipe CSIRT.

7.1.1 Fonction: Découverte de vulnérabilités lors de l'intervention en cas d'incident

Objectif: identifier une vulnérabilité exploitée dans le cadre d'un incident de sécurité.

Description: l'analyse d'un incident de sécurité peut révéler des informations indiquant qu'une vulnérabilité a été exploitée par l'auteur de l'attaque. L'incident peut découler de l'exploitation d'une vulnérabilité connue non corrigée ou non atténuée par le passé ou d'une nouvelle vulnérabilité (jour zéro).

Certaines de ces informations peuvent être le produit de l'un des services de la zone de service Gestion des incidents relatifs à la sécurité des informations si une vulnérabilité a été exploitée dans le cadre d'un incident. Elles peuvent alors être transmises à la fonction Tri des vulnérabilités ou au service Analyse des vulnérabilités, selon le cas.

Résultat: transmission des informations relatives à une vulnérabilité soupçonnée d'avoir été exploitée dans le cadre d'un incident de sécurité à la zone de service Gestion des vulnérabilités.

[6] La réception d'informations reçues sur une nouvelle vulnérabilité par courrier électronique peut être considérée comme étant une activité du service Découverte des vulnérabilités, de la fonction Découverte de vulnérabilités à partir de sources publiques, du service Recueil des rapports de vulnérabilité ou de la fonction Réception des rapports de vulnérabilité en fonction des processus internes de l'équipe CSIRT ou de la portée de la distribution de ces informations.

7.1.2 Fonction: Découverte de vulnérabilités à partir de sources publiques

Objectif: Prendre connaissance d'une nouvelle vulnérabilité en lisant des sources publiques ou d'autres sources tierces.

Description: Une équipe CSIRT peut initialement prendre connaissance d'une nouvelle vulnérabilité à partir de diverses sources publiques en divulguant l'existence. Ces sources peuvent être des annonces de fournisseurs, des sites Web consacrés à la sécurité, des listes de diffusion, des bases de données sur les vulnérabilités, des conférences sur la sécurité, les réseaux sociaux, etc. Cette fonction est également susceptible de prendre connaissance de nouvelles vulnérabilités au moyen d'autres sources tierces à accès restreint, telles que des abonnements payants ou des services premium au titre desquels les informations ne sont partagées qu'au sein d'un groupe limité. Des membres du personnel pourront être chargés de l'exécution de cette fonction, de la collecte des informations et de leur organisation à des fins d'examen et de partage. Des informations similaires sur les vulnérabilités peuvent également émaner de la zone de service Appréciation de la situation.

Résultat: identification de nouvelles vulnérabilités révélées par des sources publiques ou externes.

7.1.3 Fonction: Recherche de vulnérabilités

Objectif: découvrir ou rechercher de nouvelles vulnérabilités grâce à des activités ou des recherches délibérées.

Description: cette fonction comprend la découverte de nouvelles vulnérabilités du fait d'activités spécifiques des équipes CSIRT telles que le test de systèmes ou de logiciels à l'aide de tests à données aléatoires ou la rétro-ingénierie de logiciels malveillants.

Elle peut également recevoir des informations de la part du ou des service(s) de la ou des zone(s) de service Gestion des incidents relatifs à la sécurité des informations ou Appréciation de la situation qui auraient activé cette fonction pour rechercher des vulnérabilités soupçonnées.

La découverte d'une nouvelle vulnérabilité à l'issue de cette fonction de recherche peut alimenter le service Intervention en cas d'incident, la fonction Détection des vulnérabilités (voir la sous-fonction Recensement des vulnérabilités et Tests d'intrusion des vulnérabilités).

Résultat: la recherche identifie de nouvelles vulnérabilités.

7.2 Service: Recueil des rapports de vulnérabilité

Objectif: recevoir et traiter les informations sur les vulnérabilités signalées par des parties prenantes ou des tiers.

Description: les rapports ou les questions envoyés par des parties prenantes d'une CSIRT ou des tiers peuvent constituer l'une des principales sources d'information sur les vulnérabilités. Les CSIRT doivent anticiper le fait que les vulnérabilités peuvent être signalées par ces diverses sources et mettre à disposition un mécanisme, un processus et des conseils pour leur signalement. Les infrastructures de signalement peuvent inclure un courrier électronique ou un formulaire accessible en ligne. Les parties prenantes ou les tiers ne signalent pas directement

toutes les vulnérabilités par les canaux établis. Les éléments d'aide doivent comprendre des consignes de signalement, les informations de contact et les éventuelles politiques en matière de divulgation.

Pour permettre aux parties prenantes d'effectuer un signalement de manière plus efficace, les CSIRT doivent mettre à disposition un ou plusieurs mécanismes ainsi que des conseils ou des instructions concernant le contenu et la méthode de signalement sécurisés des vulnérabilités. Les mécanismes de signalement peuvent inclure un courrier électronique, un site Web, un formulaire ou un portail dédié au signalement des vulnérabilités ou d'autres méthodes permettant la soumission des rapports en toute sécurité et sûreté. S'ils ne figurent pas dans un formulaire de signalement des vulnérabilités, les conseils de signalement doivent apparaître dans un document séparé ou sur une page Web et lister les informations spécifiques qu'il est souhaitable d'inclure dans le signalement.

Résultat: réception des rapports de vulnérabilité avec le même professionnalisme et la même cohérence que les autres rapports, suivie de leur validation et de leur classification.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Réception des rapports de vulnérabilité.
- Tri et traitement des rapports de vulnérabilité.

7.2.1 Fonction: Réception des rapports de vulnérabilité

Objectif: accepter ou recevoir des informations à propos d'une vulnérabilité signalée par des parties prenantes ou des tiers.

Description: pour être efficace, le recueil des rapports de vulnérabilité requiert des mécanismes et des processus adaptés à la réception de rapports envoyés par des acteurs et des tiers (par exemple, découvreurs, chercheurs, fournisseurs, PSIRT, autres CSIRT ou coordonnateur des vulnérabilités, etc.). Les informations peuvent porter sur les appareils touchés, les conditions nécessaires à l'exploitation de la vulnérabilité, son impact (par exemple, escalade au niveau des privilèges, accès aux données, etc.) ainsi que les mesures prises pour résoudre la vulnérabilité, les étapes de la correction et/ou de l'atténuation ainsi que la résolution. Il arrive que les informations sur la vulnérabilité parviennent avec les données d'autres services, principalement le Recueil des rapports d'incidents relatifs à la sécurité des informations (par exemple, si un rapport d'incident rapporte l'exploitation d'une vulnérabilité).

Résultat: bonne gestion des rapports de vulnérabilité émanant de parties prenantes ou de tiers, y compris la mise en route de leur documentation ou de leur suivi.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

- Surveillance régulière des canaux de communication et vérification de la mesure dans laquelle les moyens de communication avec la CSIRT indiqués sont opérationnels et permettent de soumettre des rapports.

- Envoi de l'accusé de réception initial à l'auteur du rapport de vulnérabilité demandant des informations supplémentaires si nécessaire et définition des attentes avec l'auteur du rapport.

7.2.2 Fonction: Tri et traitement des rapports de vulnérabilité

Objectif: examen, classification, hiérarchisation et traitement initiaux des rapports de vulnérabilité.

Description: les rapports de vulnérabilité sont examinés et triés afin d'acquérir une compréhension initiale de la vulnérabilité concernée et de déterminer les étapes suivantes (par exemple, approfondir l'analyse de la vulnérabilité, demander des informations supplémentaires à l'auteur du rapport ou à d'autres sources, décider de ne rien faire). En fonction de la quantité de détails et de la qualité des informations fournies dans le rapport de vulnérabilité, l'apparition d'une vulnérabilité sera évidente ou pas.

Sauf en cas de motif de rejet du rapport de vulnérabilité, ce dernier doit être transmis au service Analyse des vulnérabilités à des fins d'examen, d'analyse et de traitement. Si la CSIRT ne fournit pas de service Analyse des vulnérabilités, le rapport devra être transmis en toute sécurité à un groupe externe tel que le(s) fournisseur(s) concerné(s), une ou plusieurs PSIRT ou encore un coordonnateur des vulnérabilités.

Résultat: identification des informations permettant de décider de la suite à donner.

Les sous-fonctions suivantes sont considérées faire partie de la mise en œuvre de ce service:

- Traitement des rapports et des données soumises, y compris des artefacts ou des matériels isolés, afin de protéger l'intégrité de l'environnement de travail et d'éviter que les attaques visant la CSIRT par ce biais soient couronnées de succès.
- Mise à jour des accusés de réception des rapports avec des commentaires sur les étapes suivantes fondés sur les résultats de la classification ou de la hiérarchisation.
- Fusion des nouvelles informations sur une vulnérabilité déjà traitée et des données disponibles afin d'assurer la cohérence de l'analyse et du traitement.

7.3 Service: Analyse des vulnérabilités

Objectif: analyser et comprendre une vulnérabilité confirmée.

Description: le service Analyse des vulnérabilités regroupe des fonctions visant à comprendre la vulnérabilité et son impact potentiel, à identifier le problème ou la défaillance sous-jacents (cause première) permettant l'exploitation de la vulnérabilité et à élaborer une ou plusieurs stratégies de correction ou d'atténuation dans le but de prévenir ou de limiter l'exploitation de la vulnérabilité.

Le service Analyse des vulnérabilités et ses fonctions peuvent continuer à être assurés en parallèle tandis que le service Coordination des vulnérabilités de l'exécution ses fonctions opèrent avec d'autres participants dans le cadre d'un processus coordonné de divulgation des

vulnérabilités (CVD)[7].

Résultat: meilleure connaissance des détails clés relatifs à une vulnérabilité (par exemple, description, impact, résolution).

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Tri des vulnérabilités (validation et classification).
- Analyse des causes premières des vulnérabilités.
- Élaboration de la correction des vulnérabilités.

7.3.1 Fonction: Tri des vulnérabilités (validation et classification)

Objectif: classifier, hiérarchiser et effectuer l'évaluation initiale d'une vulnérabilité.

Description: le service Analyse des vulnérabilités commence par l'examen des informations disponibles afin d'en classifier, hiérarchiser et évaluer l'impact sur les systèmes concernés conformément au mandat de la CSIRT. Certaines d'entre elles pourront avoir été documentées lors de la fonction Tri et traitement des vulnérabilités (du service Recueil des rapports de vulnérabilité), si la vulnérabilité en question a été signalée à la CSIRT par une partie prenante ou un tiers.

Si le tri préalable n'a pas déjà été fait, la vulnérabilité pourra être assignée à un expert à même d'apporter la confirmation technique qu'elle a un impact sur les systèmes concernés et relève du mandat de la CSIRT (c'est-à-dire l'impact potentiel sur la sécurité des réseaux ou des systèmes susceptible de nuire à la confidentialité, à la disponibilité ou à l'intégrité des informations dans un domaine relevant du mandat de la CSIRT).

Résultat: classification, hiérarchisation et mise à jour des informations relatives à une vulnérabilité.

7.3.2 Fonction: Analyse des causes premières des vulnérabilités

Objectif: comprendre la défaillance de conception ou de mise en œuvre à l'origine de la vulnérabilité ou de sa découverte.

Description: Cette analyse a pour but d'identifier la cause première de la vulnérabilité, d'appréhender de façon précise les facteurs qui en permettent l'existence ainsi que les circonstances en rendant possible l'exploitation. Elle peut également s'efforcer de comprendre la ou les faiblesse(s) exploitée(s) en vue de provoquer l'incident et les techniques d'attaque utilisées à cette fin. Selon la nature de la vulnérabilité, la CSIRT pourra avoir plus ou moins de mal à effectuer cette fonction de façon approfondie. Dans certains cas, le découvreur ou l'auteur du rapport de vulnérabilité s'en est déjà chargé. Il est très souvent préférable que cette fonction soit prise en charge par le fournisseur du produit ou le développeur du logiciel ou du système

[7] Voir les zones de service Coordination de la vulnérabilité et Divulgation des vulnérabilités pour obtenir des informations sur la divulgation coordonnée des vulnérabilités (CVD).

concerné ou bien encore par leur PSIRT respective. Il est également possible qu'une vulnérabilité soit présente dans plusieurs produits. Dans ce cas, il faudra peut-être réaliser plusieurs analyses du logiciel ou des systèmes concernés requérant une coordination avec plusieurs fournisseurs, PSIRT ou acteurs.

Résultat: la compréhension de la vulnérabilité et de la façon dont des acteurs malveillants pourront l'utiliser sert à déterminer des méthodes de correction ou d'atténuation visant à limiter le risque de découverte ou d'exploitation.

7.3.3 Fonction: Élaboration de la correction des vulnérabilités

Objectif: définir les mesures à prendre pour corriger (remédier) la vulnérabilité sous-jacente ou atténuer (réduire) les effets de son exploitation.

Description: dans l'idéal, cette fonction identifiera une correction ou une réparation de la vulnérabilité. Si le fournisseur ne dispose pas d'un correctif ou d'une réparation au moment opportun, une solution de repli temporaire baptisée atténuation peut être recommandée, telle que désactiver le logiciel concerné ou en modifier la configuration, afin de limiter les effets négatifs potentiels de la vulnérabilité. À noter que l'application ou le déploiement d'une correction (correctif) ou d'une atténuation (solution de repli temporaire) relève d'une fonction d'un autre service appelé Intervention en cas de vulnérabilité dans le présent document.

Dans le cadre des services Analyse des vulnérabilités et Élaboration d'une correction, cette fonction peut éventuellement comprendre des sous-fonctions ou activités, telles que la validation de la modification d'une procédure ou d'une conception, l'examen de la correction par un tiers ou l'identification de nouvelles vulnérabilités introduites lors d'étapes de la correction. Les vulnérabilités n'ayant pas fait l'objet d'une correction ou d'une atténuation doivent être recensées comme des risques acceptables.

Cette fonction recevra souvent des informations ou des données de la part du ou des fournisseurs du produit concerné, parfois dans le cadre du rapport ou de l'annonce initial(e) géré(e) par d'autres services ou fonctions.

Résultat: établissement d'un plan visant à modifier (corriger) le code logiciel, mettre en œuvre une solution de repli temporaire ou améliorer les processus, les infrastructures et/ou les conceptions afin de fermer le vecteur d'attaque concerné et d'empêcher l'exploitation de la vulnérabilité.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

- Élaboration de corrections/correctifs des vulnérabilités.
- Élaboration d'atténuations des vulnérabilités.

Cette fonction est typiquement effectuée par d'autres entités (par exemple, fournisseurs des produits, PSIRT).

7.4 Service: Coordination des vulnérabilités

Objectif: échanger des informations et coordonner les activités avec les participants à un processus coordonné de divulgation des vulnérabilités (CVD).

Description: la gestion de la plupart des vulnérabilités requiert de notifier, collaborer et coordonner l'échange des informations pertinentes avec de multiples parties dont les découvreurs/auteurs de rapports de vulnérabilité, les fournisseurs concernés, les développeurs, les PSRIT ou d'autres experts de confiance (par exemple, chercheurs, CSIRT, coordonnateurs des vulnérabilités) qui peuvent collaborer afin d'analyser et de corriger la vulnérabilité.

Résultat: le partage des informations avec les participants à un processus CVD qui peuvent aider à fournir des informations permettant de corriger/atténuer la vulnérabilité survient de manière efficace et opportune.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Notification/signalement des vulnérabilités.
- Coordination des acteurs concernés par les vulnérabilités.

7.4.1 Fonction: Notification/signalement des vulnérabilités

Objectif: partage ou signalement initial d'informations sur une nouvelle vulnérabilité avec les participants au processus CVD.

Description: la gestion de la plupart des vulnérabilités requiert de notifier, collaborer et coordonner l'échange des informations pertinentes avec de multiples acteurs dont les fournisseurs concernés, les développeurs, les PSRIT ou d'autres experts de confiance (par exemple, les chercheurs, CSIRT, coordonnateurs des vulnérabilités) aptes à collaborer à l'analyse et à la correction de la vulnérabilité.

Résultat: les fournisseurs (ou autres participants au processus CVD) sont informés de l'existence d'une vulnérabilité et peuvent travailler à l'élaboration d'une correction ou d'une atténuation.

7.4.2 Fonction: Coordination des acteurs concernés par les vulnérabilités

Objectif: effectuer une coordination de suivi et partager les informations entre les divers acteurs et les participants aux efforts de divulgation coordonnée des vulnérabilités (CVD).

Description: coordonner l'échange d'informations entre les découvreurs/chercheurs, les fournisseurs, les PSIRT et tout autre participant aux efforts de divulgation coordonnée des vulnérabilités (CVD) afin d'analyser et de corriger la vulnérabilité et d'en préparer la divulgation. Cette coordination doit également comprendre le consensus des participants quant au moment et à la synchronisation de la divulgation.

Résultat: les informations sur les vulnérabilités sont partagées de façon plus efficace, en temps opportun et de manière responsable entre les participants qui peuvent développer ou annoncer une correction/solution d'atténuation.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

- Élaboration de la publication de la vulnérabilité.

7.5 Service: Divulgation des vulnérabilités

Objectif: diffuser des informations sur les vulnérabilités connues aux parties prenantes afin qu'elles puissent prévenir, détecter et corriger/atténuer les vulnérabilités connues.

Description: informer les parties prenantes des vulnérabilités connues (points d'entrée potentiels pour les auteurs des attaques) afin qu'elles puissent tenir leurs systèmes à jour et prévenir l'intrusion d'exploits. Les méthodes de divulgation peuvent inclure la publication d'informations par de multiples canaux de communication (par exemple, site Web, courrier électronique, réseaux sociaux), une base de données sur les vulnérabilités ou d'autres supports. Ce service fait souvent suite à la Coordination des vulnérabilités.

Résultat: capacité des parties prenantes informées à éviter l'exploitation potentielle des vulnérabilités connues avant qu'elle ne se produise ainsi qu'à détecter et atténuer les vulnérabilités existantes.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Politique de divulgation des vulnérabilités et maintenance de l'infrastructure.
- Annonces/communication/diffusion des vulnérabilités.
- Retours d'information postérieurs à la divulgation des vulnérabilités.

7.5.1 Fonction: Politique de divulgation des vulnérabilités et maintenance de l'infrastructure

Objectif: élaborer et tenir à jour une politique prescrivant un cadre et des attentes concernant les méthodes de gestion et de divulgation des vulnérabilités par les CSIRT ainsi que le ou les mécanismes de divulgation.

Description: les CSIRT qui gèrent les rapports de vulnérabilité doivent définir leur politique de divulgation des vulnérabilités et la mettre à disposition de leurs parties prenantes, acteurs et des participants à un processus CVD, de préférence en la publiant sur leur site Internet. Cette politique apportera de la transparence aux acteurs et les aidera à promouvoir des politiques de divulgation adaptées. Les politiques peuvent aller de la non-divulgation (aucune information sur les vulnérabilités n'est divulguée) à la divulgation intégrale (toutes les informations sont divulguées) en passant par une divulgation limitée (certaines informations sont divulguées), ce qui peut inclure des codes types de validation. La politique de divulgation doit inclure des facteurs tels que sa portée, des références à des mécanismes et des consignes de signalement ainsi que les délais attendus et des mécanismes de divulgation.

Résultat: augmentation de la confiance, de la collaboration ainsi que du contrôle de la divulgation et amélioration des relations ainsi que de la coordination avec les participants à un processus CVD.

7.5.2 Fonction: Annonces/communication/diffusion des vulnérabilités

Objectif: fournir des informations aux parties prenantes (et au grand public) concernant une nouvelle vulnérabilité afin qu'elles puissent la détecter, la corriger ou l'atténuer et en empêcher

l'exploitation future.

Description: divulguer des informations sur la vulnérabilité à des parties prenantes définies. La divulgation peut s'effectuer à l'aide de tout ou partie des mécanismes identifiés dans la politique de divulgation des vulnérabilités. Les mécanismes de diffusion peuvent varier en fonction des besoins ou des attentes du public cible. La communication peut prendre la forme d'une annonce ou d'une alerte de sécurité diffusée par courrier électronique ou SMS, d'une publication affichée sur un site Web ou un réseau social ou d'autres formes et canaux de communication adaptés. Le contenu à inclure dans la divulgation doit suivre un format défini, pouvant en général comprendre des informations telles qu'une vue globale ou une description, un identifiant de vulnérabilité unique, l'impact, la gravité ou le système d'évaluation des vulnérabilités courantes (CVSS), la résolution (correction ou atténuation) et des références ou des documents justificatifs.

Résultat: empêchement, détection et correction/atténuation de la vulnérabilité grâce à la fourniture en temps opportun d'informations efficaces et de qualité aux parties prenantes (ou au grand public).

7.5.3 Fonction: Retours d'information postérieurs à la divulgation des vulnérabilités

Objectif: recueillir les questions ou les rapports des parties prenantes concernant la divulgation ou un document relatif à une vulnérabilité et y répondre.

Description: suite à la divulgation d'une nouvelle vulnérabilité, les CSIRT peuvent s'attendre à recevoir des questions de certaines parties prenantes à propos d'un document relatif à la vulnérabilité en question. Il peut s'agir d'une demande d'éclaircissements, de révision ou de modification du mécanisme de divulgation de la vulnérabilité, si nécessaire. Les parties prenantes peuvent simplement accuser réception du document relatif à la vulnérabilité ou signaler un problème ou encore une difficulté en rapport avec le déploiement de la correction/l'atténuation suggérée. S'il s'est avéré que la vulnérabilité a déjà été exploitée, les parties prenantes peuvent signaler de nouveaux incidents imputables à sa divulgation. Ces rapports doivent être transmis aux fonctions du service Signalement des incidents de la CSIRT.

Résultat: fourniture de réponses aux questions et aux demandes d'assistance dans un délai raisonnable suite à la divulgation d'une vulnérabilité.

7.6 Service: Intervention en cas de vulnérabilité[8]

Objectif: recueillir activement des informations sur les vulnérabilités et prendre des mesures de prévention, de détection et de correction/d'atténuation de ces vulnérabilités en conséquence.

Description: Les fonctions relevant de ce service ont pour but de déterminer de l'existence d'une vulnérabilité divulguée sur les systèmes d'une partie prenante ou de son absence, souvent en en recherchant intentionnellement la présence. Le service comprend également des actions

[8] Bien que les fonctions et sous-fonctions relatives à la détection des vulnérabilités soient parfois désignées par le terme "gestion des vulnérabilités", le présent Cadre de services de la CSIRT considère qu'elles font partie du présent service Intervention en cas de vulnérabilité, qui appartient à la zone de service plus large appelée Gestion des vulnérabilités dans le présent document.

ultérieures de correction ou d'atténuation de la vulnérabilité grâce au déploiement de correctifs ou de stratégies de solutions de repli temporaires.

Résultat: les informations ont amené à détecter la présence d'une vulnérabilité, à corriger/atténuer la vulnérabilité découverte et à en empêcher l'exploitation.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Détection/recensement des vulnérabilités.
- Correction des vulnérabilités.

Habituellement, le service Intervention en cas de vulnérabilité et ses fonctions relèvent d'autres groupes spécialisés d'une organisation et non de la CSIRT. Il est également improbable qu'il soit dispensé par une CSIRT de coordination.

7.6.1 Fonction: Détection/recensement des vulnérabilités

Objectif: rechercher activement la présence de vulnérabilités connues dans des systèmes déployés.

Description: cette fonction a pour but de détecter des vulnérabilités non corrigées ou non atténuées avant qu'elles soient exploitées ou impactent le réseau ou encore les dispositifs. Elle peut être lancée suite à l'annonce d'une nouvelle vulnérabilité ou menée dans le cadre de la recherche périodique programmée de vulnérabilités connues. La détection des vulnérabilités est d'autant plus efficace qu'il existe un inventaire des systèmes. L'existence d'un inventaire de ce type dans lequel il est possible de rechercher des informations sur les versions des logiciels peut permettre aux organisations d'évaluer rapidement la prévalence probable dans leur infrastructure d'une vulnérabilité nouvellement signalée.

Cette fonction peut recevoir des données ou être déclenchée par d'autres services et fonctions.

Résultat: détection des vulnérabilités à l'aide de processus formels ou d'outils d'identification.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

- Recensement/recherche des vulnérabilités.
- Évaluations de la sécurité/tests d'intrusion des vulnérabilités.

En général, cette fonction est confiée à d'autres entités (par exemple, service informatique, service sécurité production, spécialistes tiers, propriétaires des systèmes).

7.6.2 Fonction: Correction des vulnérabilités

Objectif: corriger ou atténuer les vulnérabilités afin d'en prévenir l'exploitation, en général grâce à l'application en temps utile de correctifs fournis par le fournisseur ou d'autres solutions.

Description: la correction des vulnérabilités vise à les résoudre ou à les éliminer. En général, la correction des vulnérabilités logicielles survient grâce au déploiement et à l'installation de solutions provenant du fournisseur sous la forme de mises à jour logicielles ou de correctifs. En

l'absence de correctifs approuvés ou en cas d'impossibilité de les déployer, une atténuation ou une solution de repli temporaire peut être appliquée à titre de contre-mesure pour empêcher l'exploitation de la vulnérabilité. Cette fonction suit souvent l'identification positive d'une vulnérabilité résultant de la fonction Détection/Recensement/Recherche des vulnérabilités.

Résultat: évitement ou réduction de l'exposition au risque d'exploitation des vulnérabilités.

Les sous-fonctions suivantes sont considérées comme relevant de cette fonction:

- Correction des vulnérabilités (gestion des correctifs).
- Atténuation des vulnérabilités.

En général, cette fonction ne relève pas de la CSIRT, mais, par exemple, du service informatique, du service sécurité production ou encore des propriétaires des systèmes.

8 Zone de service: Appréciation de la situation

L'appréciation de la situation est l'aptitude à identifier, traiter, comprendre et communiquer les éléments cruciaux des événements survenant dans le domaine de responsabilité de la CSIRT et autour de celui-ci susceptibles d'influer sur le fonctionnement ou la mission de ses parties prenantes. Elle consiste à connaître l'état présent et à en identifier ou en anticiper les changements potentiels. Cette zone de service comprend la détermination des modes de recueil des informations pertinentes auprès de différents domaines ainsi que les modalités d'intégration de ces informations et de leur diffusion au moment opportun dans le but d'aider les parties prenantes à prendre des décisions plus éclairées. Certaines organisations peuvent créer une équipe distincte pour l'Appréciation de la situation tandis que d'autres préfèrent confier cette fonction à l'équipe CSIRT sur la base de sa visibilité, de sa compréhension du contexte, de ses capacités techniques, de son accès aux ressources, de ses connexions externes et de sa mission de prévention des incidents. L'appréciation de la situation n'est pas uniquement axée sur l'intervention en cas d'incident. Elle fait en sorte que les données, les analyses et les actions soient à la disposition d'autres services tels que Gestion des événements de sécurité, Gestion des incidents et Transfert de connaissances. Elle veille également à la bonne intégration des informations en provenance d'autres zones de services et à leur renvoi aux parties prenantes appropriées au moment opportun.

Les services suivants relèvent de zone de service:

- Acquisition de données.
- Analyse et synthèse.
- Communication.

8.1 Service: Acquisition de données

Objectif: collecter les données qui permettront de déterminer plus clairement les activités internes et externes susceptibles d'influer sur la sécurité de parties prenantes.

Description: solliciter, collecter, déterminer et satisfaire les besoins en informations des parties prenantes afin de déterminer les activités internes et externes pertinentes importantes. Ce service comprend la logistique de la collecte des informations pertinentes, notamment mise au courant des événements en cours, programmation d'événements futurs, rapports et flux d'informations , filtrage des informations collectées, organisation des informations à utiliser dans l'analyse d'incidents, la prévention, la détection ou d'autres activités (telles que planification ou tendances), stockage pour une utilisation ultérieure, amélioration de la facilité de recherche, etc. Les données collectées serviront à déterminer les mesures préventives requises et aideront à prendre des décisions éclairées concernant la gestion des incidents et les activités de garantie des informations. Sans perception de base des éléments environnementaux importants, le risque que d'autres services acquièrent une image incorrecte augmente. Les CSIRT devront établir des politiques et des procédures et pourront employer des technologies de collecte et de vérification des informations.

Résultat:

Ce service produit les artefacts suivants:

- Exigences en matière de collecte d'un ensemble de données identifiant les besoins relatifs à l'appréciation de la situation puis établissant le lien entre ces exigences et la nature des informations à collecter pour y répondre.
- Informations sur le statut présent et futur attendu des ressources et des activités des parties prenantes.
- Informations sur les événements ou les tendances externes donnant une idée de l'entourage et de l'environnement actuel des parties prenantes, y compris nouvelles technologies, méthodes, pratiques, risques et menaces.
- Informations convenablement formatées prêtes pour les activités d'analyse et de détection.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Regroupement, diffusion et consignes relatifs aux politiques.
- Recensement des ressources attribuées aux fonctions, aux rôles, aux actions et aux risques principaux.
- Collecte.
- Traitement et préparation des données.

8.1.1 Fonction: Regroupement, diffusion et consignes relatifs aux politiques

Objectif: définir le contexte auquel la partie prenante et ses ressources devraient être conformes afin de savoir ce qui devrait se passer dans l'infrastructure.

Description: la collecte, le regroupement et la diffusion des politiques constituent la base d'une activité normale acceptable. Le résultat final est un contexte établissant la manière dont la partie prenante et son infrastructure sont supposées fonctionner dans des conditions acceptables. Dans le cas des CSIRT organisationnelles, le contexte inclut la compréhension des politiques

acceptables, des plans, des conditions normales d'exploitation, des risques acceptés et des arbitrages de l'organisation. La compréhension et le contexte constituent la base d'évaluation des observations.

Résultat: compréhension des observations acceptables qui se produisent au niveau de la partie prenante. Cette compréhension est axée sur les changements ou les impacts subis par l'infrastructure et les ressources.

8.1.2 Fonction: recensement des ressources attribuées aux fonctions, aux rôles, aux actions et aux risques principaux

Objectif: connaître les ressources existantes, leurs propriétaires, les données de base et l'activité attendue soutient les fonctions d'analyse qui identifient les observations de situations anormales.

Description: les équipes CSIRT doivent comprendre l'état présent de la cybersécurité d'une partie prenante, ainsi que la nature d'une sécurité acceptable. Elles peuvent avoir besoin de connaître:

- les utilisateurs légitimes des systèmes et des dispositifs internes et en interaction avec le public;
- les dispositifs autorisés et leur usage;
- les processus et les applications approuvés, leurs utilisateurs autorisés et la manière dont ils servent la partie prenante.

Ces informations aident à déterminer l'ordre de priorité des ressources potentiellement à risque, susceptible de fournir le contexte des activités de gestion des incidents. Plus les informations à la disposition de l'équipe CSIRT sont précises, plus il est facile d'induire les problèmes de sécurité et d'y remédier. Pour obtenir des informations précises, la CSIRT est susceptible d'avoir accès aux politiques de sécurité en vigueur, aux contrôles d'accès en cours, à des inventaires matériels et logiciels à jour et à des schémas de réseau détaillés.

Résultat:

Cette fonction livre les listes suivantes:

- Liste des fonctions clés et des ressources qui les soutiennent, étant attendu que certaines ressources peuvent soutenir plusieurs fonctions.
- Liste des rôles chargés de chaque fonction et de leur rôle numérique équivalent sur la ressource.
- Liste des actions généralement autorisées par rôle.
- Liste des principaux risques auxquels sont confrontées les ressources et les fonctions.

Ces listes évolueront en fonction des changements de la situation.

8.1.3 Fonction: Collecte

Objectif: collecter les informations à l'appui du service Analyse et interprétation et/ou d'autres services de la CSIRT.

Description: les activités de collecte d'informations et de données dépassent les flux d'informations automatiques. La collecte recouvre l'identification de sources utiles telles que des activités externes pertinentes pour les informations, notamment des nouvelles d'autres parties prenantes, sources médiatiques et autres CSIRT ou organisations de sécurité, activités internes (par exemple, changements organisationnels), développements technologiques, événements externes, événements politiques, tendances des attaques, tendances défensives, conférences, formations disponibles, etc.

La fonction de collecte des données soutient d'autres services tels que Gestion des événements de sécurité, Gestion des incidents et Transfert de connaissances. Elle soutient également des fonctions et des activités de ces services tels que l'analyse, la prédiction, l'atténuation des risques et la réaction à ces derniers. Les informations récemment collectées pourront révéler qu'une attaque sur une partie prenante est plus probable qu'auparavant. Les événements externes pourront exposer des informations qui identifient de nouveaux risques pour les ressources pendant une période ou requièrent de renforcer les activités de détection. Globalement, les données contribuent à fournir des informations exploitables aptes à faciliter la prise de décision et la gestion des incidents.

Résultat: collecte et production de données ainsi que d'ensembles de données fournissant un contexte opérationnel ou environnemental utilisable par d'autres services et fonctions, notamment l'analyse, permettant de créer un aperçu de la situation pour la partie prenante, d'identifier les alertes ou de planifier en vue de l'atténuation de domaines de risques accrus pour les ressources et les infrastructures qui les soutiennent.

8.1.4 Fonction: Traitement et préparation des données

Objectif: établir un ensemble de données fiable, cohérent et à jour apte à soutenir les activités des CSIRT et à répondre aux exigences du service d'analyse.

Description: le traitement et la préparation des données incluent la transformation, le traitement, la normalisation et la validation d'un ensemble de données. L'exactitude des sources de données de cybersécurité doit régulièrement être vérifiée en raison du nombre élevé de faux positifs. En général, les données pertinentes sont fournies dans différents formats et il faut combiner les nouvelles données aux données historiques avant de procéder à une analyse complète. Certains types de données (tels que les articles de journaux) devront peut-être être analysés ou traités dans le cadre du processus de préparation. L'extraction dans un article d'informations pertinentes sur la sécurité (par exemple, noms, dates, lieux, informations techniques, faiblesses, noms des systèmes) et leur comparaison à des données internes pour en évaluer les impacts potentiels en constituent un exemple.

Certaines méthodes d'analyse doivent être stockées dans le même format ou compter le même nombre d'enregistrements s'il s'agit de fichiers. La préparation des données peut donner lieu à de multiples étapes de traitement. L'augmentation des données (également appelée enrichissement) consiste à inclure d'autres informations disponibles en rapport avec une donnée spécifique provenant de sources internes et externes. À titre d'exemple, les équipes pourront collecter des informations sur les adresses IP telles que les identifiants de systèmes autonomes, codes de pays ou données de géolocalisation. Concernant les informations relatives aux ressources internes, les équipes pourront enrichir les données de l'inventaire des ressources à

l'aide du nom de leur propriétaire, son rôle, les autorisations relatives à d'autres ressources, son lieu de travail physique au fil du temps, etc.

Résultat: existence de données prêtes à l'utilisation par d'autres services ou fonctions.

8.2 Service: Analyse et synthèse

Objectif: évaluer si la situation ne répond pas aux attentes (par exemple, lorsque des ressources spécifiques sont sous la menace d'un événement nocif imminent).

Description: processus d'utilisation des données existantes, de l'historique et des techniques d'analyse visant à déterminer l'événement susceptible d'influer sur les ressources et la sécurité des parties prenantes, consistant souvent à répondre à une question ou à vérifier une intuition. L'analyse pourra révéler si les événements ne correspondent pas au comportement type attendu ou fournir des informations sur les circonstances, la nature ou l'origine des événements ou des comportements. L'analyse pourra faire apparaître des implications pour les situations présentes et futures. Par exemple, un système consigne qu'un identifiant utilisateur s'est connecté au système, mais n'indique pas s'il s'agissait d'un utilisateur légitime. Il conviendra d'intégrer à l'analyse de nouvelles sources (telles que des entretiens avec l'utilisateur) pour donner à l'équipe une image plus exacte permettant de déterminer la légitimité de l'événement. Diverses techniques d'analyse et d'interprétation des données collectées et de leur effet sur les parties prenantes peuvent être utilisées.

Résultat: production d'un ensemble de conclusions à propos d'événements probables passés, présents et/ou futurs au sein d'une partie prenante. Il peut également inclure des recommandations à propos de certaines décisions que la partie prenante doit prendre. L'analyse doit reposer sur des faits probants tels que les données d'observation collectées par des capteurs et d'autres sources et l'interprétation de ces faits par des analystes à l'aide de diverses méthodes. L'analyse pourra également inclure des parties prenantes à informer des résultats et la nature des informations à leur communiquer.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Projection et inférence.
- Détection des événements (au moyen d'alertes et/ou de recherche).
- Impact sur la situation.

8.2.1 Fonction: Projection et inférence

Objectif: analyser les informations collectées pendant l'acquisition des données dans le but d'avoir un aperçu de la situation actuelle ou de prédire la situation future.

Description: processus d'inférence de l'état présent d'une situation et réalisation de prédictions d'aperçus probables à court terme sur la base du statut et de la dynamique des données collectées. Parfois les données peuvent rapidement faire apparaître un problème de sécurité.

Résultat: mise à jour de l'aperçu de la situation et des connaissances lorsqu'elle changera et changements possibles.

8.2.2 Fonction: Détection des événements (au moyen d'alertes et/ou de recherche)

Objectif: déterminer et confirmer les détails de l'aperçu actuel de la situation pour la partie prenante.

Description: recherche systématique et souvent orientée d'activités anormales à l'intérieur et à l'extérieur des limites du réseau sur la base d'informations et de tendances externes et internes. Aider la partie prenante à analyser ses données provenant de capteurs et d'autres sources pour tirer des conclusions sur son environnement et sa situation. Par exemple, si un capteur antivirus envoie une alerte de fichier douteux, l'équipe pourra analyser la configuration du système, la configuration du capteur, le fichier objet de l'alerte, l'activité des utilisateurs à ce moment-là, etc., pour déterminer la gravité de l'observation. Cette fonction peut recevoir des données importantes de la zone de services Gestion des événements de sécurité. Les observations des capteurs utilisés pour détecter les événements peuvent être communiquées à de multiples services.

Les équipes CSIRT doivent également obtenir un aperçu de la situation actuelle sur la base d'informations spécifiques sur les menaces. Cette activité est parfois appelée "recherche des menaces". En général, la recherche des menaces consiste soit à préparer l'environnement à la détection d'une activité malveillante spécifique, soit à rechercher une activité malveillante spécifique susceptible d'être présente.

Résultat: mise à jour de l'aperçu de la situation sur la base de la détection d'événements au sein de la partie prenante.

8.2.3 Fonction: aide à la décision dans la gestion des incidents relatifs à la sécurité des informations

Objectif: pendant les incidents, identifier de nouvelles idées susceptibles d'aider à limiter les préjudices, à atténuer le risque futur ou à identifier une nouvelle faille.

Description: l'analyse d'évènements spécifiques aide à identifier des idées aptes à faciliter la résolution des incidents. Parfois, les CSIRT pourront axer leur analyse de la situation sur le soutien à un résultat souhaité spécifique tel que la résolution d'un incident. Certaines réactions à un incident peuvent affecter différemment l'aperçu de la situation et les responsables de la réaction peuvent demander une analyse des choix (par exemple, impact, coût, risque d'échec). Les besoins en matière de prise de décision de la partie prenante peuvent changer à mesure de l'évolution de l'image de la situation et l'équipe CSIRT pourra être amenée à lancer de nouveaux processus d'analyse pour l'aider. Cette activité est en rapport avec la zone de service Gestion des incidents. Les fonctions de Gestion des incidents sont soutenues par la zone de service Appréciation de la situation et l'aperçu de la situation peut évoluer en fonction des activités de la zone de service Gestion des incidents.

Résultat: renforcement de la zone de service Appréciation de la situation pour les fonctions de gestion des incidents sur la base de nouvelles observations. Actualisation de l'aperçu de la situation sur la base des activités de gestion des incidents.

8.2.4 Fonction: Impact sur la situation

Objectif: déterminer l'impact potentiel attendu d'une observation donnée ou de l'observation possible d'un aperçu de la situation.

Description: cette fonction identifie l'impact possible d'une projection ou d'une inférence sur une situation présente ou à court terme. L'impact peut comprendre l'augmentation ou la réduction de certains risques tels que perte des données, période de mise hors service du système ou effets sur la confidentialité/disponibilité/intégrité des données.

Résultat: production d'une analyse de l'impact probable d'une inférence ou d'une projection sur une situation.

8.3 Service: Communication

Objectif: informer les parties prenantes ou autres de la communauté de la sécurité de l'évolution des risques pour l'aperçu de la situation.

Description: il faut impérativement communiquer à la partie prenante les connaissances tirées de l'appréciation de la situation. Cela lui permettra de réagir aux observations et de prendre des mesures qui amélioreront les situations défensives, par exemple, réduire les risques liés à des tiers en améliorant l'environnement de sécurité chez certains fournisseurs à haut risque.

Résultat: communication à la partie prenante d'informations exactes, exploitables et fournies en temps opportun afin qu'elle comprenne mieux sa situation passée et améliore l'aperçu de sa situation présente et future.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Communication interne et externe.
- Rapports et recommandations.
- Mise en œuvre.
- Diffusion/intégration/partage des informations.
- Gestion du partage des informations.

8.3.1 Fonction: Communication interne et externe

Objectif: Donner aux parties prenantes (et autres) un aperçu de la situation présente et de sa possible évolution.

Description: après obtention des résultats du service Analyse et interprétation, les parties prenantes peuvent se servir de ces informations pour améliorer la prise de décision via des

processus de communication interne et externe. Des informations spécifiques sont diffusées aux personnes qui ont besoin de les connaître. La communication comprend la méthode de fourniture et le contenu fourni. Une équipe CSIRT pourra communiquer de nouvelles informations et leur influence sur l'évolution de l'aperçu de la situation. La notification d'un changement que risque d'encourir un membre de la partie prenante du fait d'une nouvelle technique malveillante observée par l'équipe pendant un incident en constitue un exemple. La communication peut également concerner des informations sur les tendances telles que les sources les plus utiles de données d'enrichissement et les mesures que peuvent prendre les parties prenantes pour améliorer leur propre appréciation de la situation.

Résultat: meilleure information des parties prenantes et préparation à la prise de mesures ou de décisions qui amélioreront leur sécurité ou leur situation.

8.3.2 Fonction: Rapports et recommandations

Objectif: créer des résultats, des artefacts ou des conclusions communiquant les informations cruciales découvertes ou issues de l'analyse à l'intention de différents publics d'une façon et dans un format adaptés.

Description: les rapports et les recommandations doivent clairement indiquer les choix et les actions à la disposition des parties prenantes et inclure l'analyse des conséquences à en attendre. La communication des résultats doit comprendre une liste de faits probants à l'appui de l'analyse et de la recommandation (si une recommandation est émise). Les méthodes de création des résultats devront être clairement expliquées au public afin qu'il puisse également juger des allégations présentées. Afin de répondre au besoin de ses parties prenantes d'avoir un aperçu de la situation, l'équipe CSIRT pourra créer des rapports sur un seul événement, une série d'événements, des tendances, des schémas, des événements possibles ou autres.

Résultat: amélioration de la capacité à fournir des rapports exacts et complets en temps opportun sur l'aperçu de la situation, des preuves à l'appui des conclusions et/ou des recommandations de marches à suivre possibles et de leurs conséquences potentielles sur la partie prenante.

8.3.3 Fonction: Mise en œuvre

Objectif: adapter l'environnement des parties prenantes en fonction des éléments communiqués afin qu'elles soient mieux préparées aux changements de l'aperçu de la situation ou à y réagir.

Description: dans certains cas, une équipe CSIRT pourra également appliquer les ajustements recommandés à une partie de l'infrastructure de sécurité, par exemple changer les règles du pare-feu pour un leurre spécifique sur la base de l'analyse de la situation.

Résultat: conduite d'une marche à suivre ou mise en œuvre d'un changement à l'infrastructure par les parties prenantes sur la base des communications reçues contenant une analyse, des projections et/ou des recommandations.

8.3.4 Fonction: diffusion/intégration/partage des informations

Objectif: assembler, normaliser et préparer des informations, puis les communiquer à des parties prenantes et autres extérieures.

Description:

Cette fonction pourra inclure les sous-fonctions suivantes:

- Utilisation des résultats du service d'analyse dans les processus internes et externes de planification et de prise de décision.
- Identification des bons destinataires des informations.
- Mise à disposition des résultats de l'analyse.
- Assurance de livraison.
- Suivi et rapports sur le partage des informations.
- Envoi des informations pertinentes au service Transfert de connaissances à des fins d'utilisation et de diffusion.

Résultat: les résultats de l'analyse d'appréciation de la situation servent de données d'entrée (à la fois en interne et chez les parties prenantes) aux processus décisionnels clés tels que la recherche de menaces, l'analyse des incidents et la résolution. Les résultats sont diffusés dans le cadre de la gestion ou de la détection des incidents. Les informations et les données issues de la zone de service Appréciation de la situation peuvent également devenir des bonnes pratiques, des rapports et des documents de formation et de sensibilisation au moyen de la zone de service Transfert des connaissances.

8.3.5 Fonction: Gestion du partage des informations

Objectif: assurer la réussite du transfert d'informations utilisables.

Description: cette fonction pourra inclure les sous-fonctions suivantes:

- Fourniture d'informations à d'autres groupes.
- Formatage des informations à des fins de transfert.
- Suivi du processus de transfert et de son résultat.

Résultat: assurance que les bonnes informations sont partagées et qu'une fois partagées elles sont reçues par les partenaires, les parties prenantes et d'autres membres de la communauté. L'activité de partage donne lieu à des rapports.

8.3.6 Fonction: retour d'informations

Objectif: améliorer la qualité, l'opportunité, l'exactitude et la pertinence des données reçues de sources internes et externes.

Description: cette fonction consiste à fournir et à recevoir un retour sur les informations fournies, reçues et utilisées par les parties prenantes, d'autres fournisseurs de services ou

d'autres acteurs. Les informations reçues étaient-elles exactes, applicables, opportunes, stratégiques, nouvelles/inédites, etc.? Ont-elles facilité la résolution d'une enquête? Ont-elles généré une nouvelle idée? Cette fonction pourra impliquer de fournir également des informations à d'autres CSIRT (en tant que source externe) sur l'utilité ou le changement des signatures, les résultats concernant les leurres, les classes d'objets d'information (IOC), les avertissements, les informations sur les menaces, les atténuations, etc. Elle pourra également être confiée à la zone de service Transfert de connaissances. Dans ce cas, les résultats devront être communiqués à la zone de service Appréciation de la situation.

Résultat: fourniture des observations et du retour d'information à des sources internes et externes afin d'améliorer l'exactitude, l'opportunité, la qualité et l'utilité des informations reçues.

9 Zone de service: transfert de connaissances

De par la nature de leurs services, les CSIRT sont particulièrement bien placées pour collecter des données pertinentes, procéder à des analyses détaillées et identifier les menaces, les tendances et les risques, ainsi que pour élaborer les bonnes pratiques opérationnelles afin d'aider les organisations à détecter, prévenir et réagir aux incidents de sécurité. Le transfert de ces connaissances à leurs parties prenantes est essentiel pour améliorer la cybersécurité globale.

Les services suivants sont considérés comme des offres relevant de cette zone de service spécifique:

- Renforcement des connaissances.
- Formation et apprentissage.
- Exercices.
- Conseil technique et stratégique.

9.1 Service: Renforcement des connaissances

Objectif: renforcer la sécurité globale de la partie prenante et aider ses membres à détecter, prévenir et rétablir leur activité après des incidents; améliorer la préparation et la formation des parties prenantes.

Description: ce service consiste à collaborer avec la partie prenante, des experts et des partenaires de confiance afin qu'ils connaissent mieux les menaces et les mesures à prendre pour prévenir et atténuer les risques qu'elles posent.

Résultat: la partie prenante acquiert la connaissance requise de ce qui suit:

- Événements, activités et tendances susceptibles de l'empêcher de fonctionner de manière opportune et sécurisée.
- Mesures à prendre pour détecter, prévenir et atténuer les menaces et les activités malveillantes.
- Bonnes pratiques en matière de sécurité et d'exploitation.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Recherche et regroupement des informations.
- Rapports et élaboration de documents de sensibilisation.
- Diffusion des informations
- Sensibilisation.

9.1.1 Fonction: Recherche et regroupement des informations

Objectif: regrouper, collationner et hiérarchiser les informations qu'il est possible de communiquer à la partie prenante à des fins d'amélioration de la sécurité ainsi que de prévention et d'atténuation des risques.

Description: cette fonction consiste à chercher et regrouper les informations pertinentes pour l'élaboration de rapports et de documents de sensibilisation, y compris provenant des résultats d'autres services/fonctions, notamment des zones de service Gestion des événements de sécurité, Gestion des incidents et Appréciation de la situation.

Résultat: les informations relatives aux tendances pertinentes, aux incidents en cours et aux bonnes pratiques sont regroupées et peuvent servir à élaborer des rapports et des documents de sensibilisation destinés à différents publics.

9.1.2 Fonction: rapports et élaboration de documents de sensibilisation

Objectif: utiliser les informations regroupées et trouvées pertinentes pour produire des documents sous diverses formes dans le but d'atteindre différents publics ou de fournir un contenu spécifique de la meilleure façon possible.

Description: cette fonction consiste à élaborer des documents destinés à divers publics (personnel technique, encadrement, utilisateurs finaux, etc.) dans divers formats tels que présentations, courtes vidéos, dessins animés, livrets, analyse technique, rapports sur les tendances et rapports annuels.

Résultat: élaboration par la CSIRT de rapports et de documents de sensibilisation de qualité adéquate répondant aux besoins de la partie prenante et utilisant des techniques et des plateformes de diffusion diversifiées et efficaces.

9.1.3 Fonction: Diffusion des informations

Objectif: diffuser les informations en rapport avec la sécurité afin de sensibiliser aux pratiques de sécurité et d'en améliorer la mise en œuvre.

Description: cette fonction consiste à mettre en œuvre un processus de diffusion des informations qui aide la CSIRT à fournir au mieux à sa partie prenante ses rapports et ses documents de sensibilisation sur la base des caractéristiques de différents publics et contenus.

Résultat: la mise en œuvre du cadre de diffusion des informations permet à la partie prenante de la CSIRT d'accéder à des informations pertinentes au moment opportun par différentes méthodes telles que des podcasts, articles de blogs, articles et vidéos sur les réseaux sociaux, communiqués de presse, publicités, campagnes, rapports publics, etc.

9.1.4 Fonction: sensibilisation

Objectif: élaborer et entretenir des relations avec des experts ou des organisations susceptibles d'aider ou de participer à l'exécution de la mission de la CSIRT.

Description: cette fonction consiste à nouer des partenariats, à promouvoir la coopération et à impliquer les principaux acteurs, internes ou externes, de la partie prenante, dans le but de favoriser la sensibilisation et les bonnes pratiques, d'aider la partie prenante et les acteurs externes à comprendre les services et les avantages de la CSIRT, d'aider la CSIRT à mieux comprendre les besoins des parties prenantes et de permettre à la CSIRT d'accomplir sa mission. Il peut s'agir de favoriser l'interopérabilité ou de renforcer la collaboration au sein des organisations ou entre elles.

Résultat: exécution d'activités de communication actives et cohérentes pouvant inclure des rencontres avec les principaux acteurs, la participation à des réunions sectorielles, des interventions lors de conférences et l'organisation de conférences.

9.2 Service: Formation et apprentissage

Objectif: assurer la formation et l'éducation d'une partie prenante d'une CSIRT (qui peut éventuellement comprendre le personnel de l'organisation et de la CSIRT) sur des sujets en rapport avec la cybersécurité, l'assurance des informations et la gestion des incidents.

Description: un programme de formation et d'éducation pourra aider la CSIRT à nouer des relations et à améliorer la cybersécurité globale de sa partie prenante, y compris l'aptitude à prévenir l'occurrence de futurs incidents. Ce type de programme peut:

- contribuer à entretenir la sensibilisation des utilisateurs;
- aider la partie prenante à comprendre un environnement et des menaces en constante évolution;
- faciliter l'échange d'informations entre la CSIRT et sa partie prenante;
- former la partie prenante aux outils, processus et procédures en rapport avec la sécurité et la gestion des incidents.

Cela peut passer par divers types d'activités telles que la documentation des connaissances, des compétences et des aptitudes (CCA) requises, l'élaboration de documents d'éducation et de formation, la fourniture de contenus, le mentorat, le développement professionnel et des compétences. Conjuguée aux autres, chacune de ces activités renforcera les capacités de la partie prenante et de l'équipe.

Résultat: mise à disposition d'un programme de formation et d'éducation cohérent permettant aux parties prenantes des CSIRT d'acquérir convenablement:

- des méthodes de détection, prévention ou réaction aux menaces;
- des outils et des pratiques de protection des ressources cruciales;
- la compréhension des processus de gestion des incidents et des procédures de demande d'assistance.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- définition des besoins en matière de connaissances, de compétences et d'aptitudes;
- élaboration de documents d'éducation et de formation;
- fourniture de contenus;
- mentorat;
- développement professionnel du personnel de la CSIRT.

9.2.1 Fonction: Définition des besoins en matière de connaissances, de compétences et d'aptitudes

Objectif: évaluer, identifier et documenter convenablement les besoins de la partie prenante en matière de CCA nécessaires afin d'élaborer des documents de formation et d'éducation adaptés et d'améliorer le niveau de compétences.

Description: cette fonction consiste à recueillir les besoins en matière de CCA d'une partie prenante afin de déterminer le type de formation et d'éducation à dispenser.

Résultat: caractérisation et documentation des besoins de la partie prenante en matière de CCA qui serviront de base à l'élaboration de documents d'éducation et de formation pertinents.

9.2.2 Fonction: Élaboration de documents d'éducation et de formation

Objectif: à partir des besoins en matière de CCA de la partie prenante, élaborer des documents d'éducation, d'instruction et de formation adaptés aux méthodes de fourniture identifiées comme les meilleures pour atteindre différents publics ou fournir des contenus spécifiques.

Description: cette fonction consiste à élaborer ou acquérir le contenu de documents d'éducation et de formation tels que présentations, cours magistraux, démonstrations, simulations, vidéos, livres, livrets, etc.

Résultat: élaboration par la CSIRT de documents de formation et d'éducation de qualité convenable et répondant aux besoins de la partie prenante à l'aide de diverses techniques et plateformes de présentation efficaces.

9.2.3 Fonction: Fourniture de contenus

Objectif: élaborer un processus formel de fourniture de contenus pouvant aider la CSIRT à fournir au mieux des contenus à sa partie prenante sur la base des caractéristiques de différents publics et contenus.

Description: cette fonction consiste à transmettre les connaissances et les contenus aux "apprenants". Elle peut faire appel à diverses méthodes, telles que la formation sur ordinateur/en ligne, la formation avec formateur, la formation virtuelle, des conférences, des présentations, des laboratoires, des concours Capture the flag, des livres, des vidéos en ligne, etc.

Résultat: conception d'un cadre de fourniture de contenus visant à aider la partie prenante à acquérir des compétences ainsi que des processus techniques et intellectuels en utilisant toutes les approches possibles, notamment des livres, livrets, vidéos en ligne, présentations, laboratoires pratiques, concours Capture the flag, formations sur ordinateur/en ligne, formations en face à face, etc. Grâce à ces activités, les membres de la partie prenante comprennent les contenus fournis.

9.2.4 Fonction: Mentorat

Objectif: élaborer, à l'intention du personnel de la CSIRT, de membres de la partie prenante ou de partenaires de confiance externes, un programme d'enseignement par du personnel expérimenté au moyen d'une relation de confiance.

Description: le programme de mentorat peut aider à mettre en place un mécanisme formel et informel par lequel le mentor aide son protégé à perfectionner ses savoirs ainsi que ses compétences et lui transmet le fruit de sa réflexion ainsi que ses expériences personnelles et professionnelles, en dehors de la relation hiérarchique et de la structure officielles de l'équipe. Il peut comprendre des visites de sites, la rotation (échange) des postes, l'apprentissage par l'observation et la remise en question du bien-fondé de décisions et d'actions spécifiques.

Résultat: renforcement, au sein de l'équipe CSIRT, de la rétention du personnel, de la loyauté, de la confiance et de l'aptitude générale à prendre des décisions éclairées. Amélioration des niveaux de compétence des parties prenantes et de la relation avec leur CSIRT. Amélioration des capacités de la partie prenante et des membres de la CSIRT, y compris établissement de relations de confiance.

9.2.5 Fonction: Développement professionnel du personnel de la CSIRT

Objectif: aider les membres du personnel de la CSIRT à planifier l'évolution de leur carrière avec succès et de façon adaptée.

Description: après identification des compétences adaptées, la CSIRT utilise le développement professionnel pour favoriser un processus continu d'acquisition de nouvelles CCA professionnelles et d'aptitudes en rapport avec le métier de la sécurité, l'accès à des responsabilités professionnelles uniques et la préservation de l'environnement global de l'équipe. Il pourra notamment s'agir de la participation à des conférences, d'une formation avancée et d'activités de formation croisée.

Résultat: existence d'un personnel développé et formé possédant les compétences techniques et intellectuelles requises et comprenant les processus, au courant des derniers développements propres à leurs fonctions et leurs besoins. 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.

9.3 Service: Exercices

Objectif: effectuer des exercices dans le but d'améliorer l'efficacité et l'efficience des services et des fonctions de cybersécurité.

Description: l'organisation propose aux parties prenantes des services à l'appui de la conception, de l'exécution et de l'évaluation des exercices de cybersécurité destinés à former et/ou évaluer les capacités des parties prenantes prises individuellement et de la communauté d'acteurs globale, y compris en communication. Ces exercices peuvent servir à

- tester les politiques et les procédures: évaluer si les politiques et les procédures en place suffisent à détecter, atténuer les incidents et à y réagir de manière efficace. Il s'agit généralement d'exercices sur papier ou de simulations;
- tester l'état de préparation opérationnel: évaluer si l'organisation possède une fonction de gestion des incidents capable de détecter, d'atténuer les incidents et d'y réagir au moment opportun et avec succès ainsi que s'assurer que les bonnes personnes soient en place, que les répertoires soient à jour et que les procédures soient exécutées correctement.

Ce service répond 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'améliorer la sensibilisation.
- Former: former le personnel aux nouveaux outils ainsi qu'aux nouvelles techniques et procédures.
    - Expérimenter: donner l'occasion au personnel d'utiliser les outils, les techniques et les procédures qu'il est supposé connaître. 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, ainsi que le niveau de préparation du personnel.
    - Vérifier: déterminer si un niveau donné d'efficacité et/ou d'efficience peut être atteint dans les services et les fonctions de cybersécurité.

Résultat: amélioration de l'efficacité et de l'efficience des services et fonctions de cybersécurité ainsi qu'identification d'opportunités d'amélioration futures.

Selon l'objectif ou les objectifs spécifique(s) recherché(s), il est aussi envisageable d'organiser une démonstration de cybersécurité à l'intention des acteurs internes ou externes, de former le personnel et d'évaluer et/ou s'assurer de l'efficacité et de l'efficience des outils, des services et des fonctions. Les enseignements qui serviront à améliorer les exercices futurs pourront également être identifiés et un rapport sera transmis à l'encadrement ou à d'autres acteurs clés.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Analyse des besoins.
- Élaboration du format et de l'environnement.
- Élaboration de scénarios.
- Exécution des exercices.
- Examen des résultats des exercices.

9.3.1 Fonction: Analyse des besoins

Objectif: assurer le résultat effectif de l'exercice en se concentrant sur des questions spécifiques pour la portée et la cible données de l'exercice.

Description: déterminer les objectifs d'apprentissage et la portée de l'exercice. Définir les services, capacités et sujets spécifiques à aborder par l'exercice. S'assurer que l'exercice comprend des activités et des sujets en rapport avec les compétences requises ou désirées par les participants ainsi que les processus à tester.

Résultat: description du but de l'exercice et grandes lignes des objectifs d'apprentissage à atteindre.

9.3.2 Fonction: Élaboration du format et de l'environnement

Objectif: spécifier et déterminer les ressources internes et externes et l'infrastructure requises pour effectuer l'exercice.

Description: définir le format et la plateforme requis pour atteindre les objectifs et obtenir les résultats escomptés de l'exercice.

Résultat: identification du type d'exercice (sur table, pratique, simulation, etc.) ainsi que des ressources internes et externes requises pour l'effectuer.

9.3.3 Fonction: Élaboration de scénarios

Objectif: donner l'occasion au public cible d'améliorer l'efficience et l'efficacité de ses services et fonctions, de ses compétences ainsi que de ses capacités grâce à la gestion d'événements/incidents de cybersécurité simulés, y compris les aspects communication.

Description: élaboration de scénarios d'exercices appuyant les objectifs des acteurs. Les produits comprennent également des instructions et des orientations à l'intention des participants et des responsables des exercices. Ces instructions comprennent les actions recommandées aux participants détaillant tout ou partie des étapes des scénarios.

Résultat: Élaboration d'un scénario principal et de ses variantes ainsi que de divers types d'ajouts formalisés, avec attribution de tâches et de rôles à l'équipe de gestion de l'exercice.

9.3.4 Fonction: Exécution des exercices

Objectif: réaliser des entraînements/exercices permettant à la CSIRT de renforcer la confiance dans son programme d'intervention en cas d'incident de sécurité et sa capacité à le mettre en œuvre.

Description: la fonction consiste à tester l'état de préparation des apprenants issus des parties prenantes de façon à vérifier leur capacité à mettre en pratique la formation et à assumer les fonctions d'un poste ou d'une tâche. Il peut s'agir d'environnements réels ou virtuels, de simulations, de tests sur le terrain ou en miniature, d'une reconstitution ou d'une combinaison de ces techniques, les ajouts étant fournis de manière structurée. 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 localiser.

Résultat: la CSIRT a évalué son niveau de préparation, a vérifié si les CCA, les processus clés et l'exécution fonctionnent bien ensemble ou doivent être adaptés/améliorés.

9.3.5 Fonction: Examen des résultats des exercices

Objectif: effectuer une analyse formelle et objective de l'exercice sur la base d'observations factuelles.

Description: élaborer un rapport après action comprenant les enseignements ou les résultats/bonnes pratiques tirés de l'exercice et fournir une évaluation aux acteurs/à l'encadrement.

Résultat: création de produits mettant en lumière le succès de l'exercice, les domaines à améliorer, les résultats généraux et les mesures recommandées à prendre pour améliorer les capacités de l'organisation en matière de gestion des incidents, processus de travail d'équipe de la CSIRT et capacités de chaque partie prenante ainsi que de la communauté globale des acteurs, y compris les capacités et procédures de communication.

9.4 Service: Conseil technique et stratégique

Objectif: s'assurer que les politiques et les procédures de la partie prenante comprennent des considérations adaptées sur la gestion des incidents et lui permettent en fin de compte de mieux gérer les risques et les menaces, ainsi que renforcer l'efficacité de la CSIRT.

Description: soutenir la partie prenante et les acteurs clés de la CSIRT, internes ou externes à la partie prenante, dans des activités en rapport avec la gestion du risque et la continuité d'activité, en fournissant des conseils techniques si nécessaire et en contribuant à la création et à la mise en œuvre des politiques de la partie prenante, ainsi qu'en l'incitant à améliorer l'efficacité de la CSIRT. Les politiques sont également importantes pour légitimer les services de la CSIRT.

Résultat: capacité de la partie prenante à prendre des décisions organisationnelles basées sur les bonnes pratiques en matière de sécurité opérationnelle incorporant la continuité d'activité et les bonnes pratiques de retour à la normale après un sinistre, tout en comprenant la nécessité d'inclure les équipes de gestion des incidents, en leur qualité de conseillers de confiance, dans les décisions stratégiques le cas échéant.

Les fonctions suivantes sont considérées comme faisant partie de la mise en œuvre de ce service:

- Appui à la gestion des risques.
- Appui à la continuité d'activité et à la planification du rétablissement suite à un sinistre.
- Appui aux politiques.
- Conseil technique.

9.4.1 Fonction: Appui à la gestion des risques

Objectif: améliorer l'identification des opportunités et menaces, les contrôles, la prévention des pertes et la gestion des incidents conjointement à la sécurité des informations et autres fonctions pertinentes.

Description: appui aux activités en rapport avec l'évaluation des risques ou de la conformité. Cela pourra comprendre la conduite d'une évaluation réelle ou un appui à l'évaluation des résultats d'une évaluation.

Résultat: capacité de la partie prenante à identifier les risques et les menaces ainsi qu'à sélectionner des options pertinentes de gestion des risques, y compris des stratégies de gestion des incidents, des contrôles de sécurité ou des atténuations des menaces adaptés et efficaces.

9.4.2 Fonction: Appui à la continuité d'activité et à la planification du rétablissement suite à un sinistre

Objectif: jouer le rôle de conseiller de confiance en matière de continuité des activités et de rétablissement suite à un sinistre en fournissant des conseils objectifs et factuels, qui tiennent compte du contexte dans lequel ces conseils peuvent servir et de toutes les contraintes de ressources envisageables.

Description: appuyer les activités de la partie prenante en rapport avec la résilience organisationnelle, sur la base des risques identifiés.

Résultat: la partie prenante est en mesure de mettre en œuvre convenablement la continuité d'activité et des plans de rétablissement suite à un sinistre comprenant les stratégies de gestion des incidents et alignés sur es dernières.

9.4.3 Fonction: Appui aux politiques

Objectif: jouer le rôle de conseiller de confiance en matière d'élaboration et de mise en œuvre de politiques, en fournissant des conseils objectifs et factuels, qui tiennent compte du contexte dans lequel ces conseils peuvent servir et de toutes les contraintes de ressources envisageables.

Description: cette fonction aide la partie prenante à élaborer, entretenir, normaliser et appliquer les politiques tout en veillant à ce qu'elles rendent possible et appuient les activités de gestion des incidents. Pour les CSIRT internes, elle comprend en général l'appui aux politiques de sécurité des informations et autres politiques opérationnelles. Pour les CSIRT de coordination et nationales, elle pourra comprendre l'appui aux politiques publiques et aux nouvelles législations.

Résultat: la partie prenante est en mesure d'élaborer des politiques efficaces, d'institutionnaliser les politiques et de mettre en place des stratégies efficaces de gestion des incidents.

9.4.4 Fonction: Conseil technique

Objectif: fournir des conseils techniques qui aident la partie prenante à mieux gérer les risques et les menaces et à mettre en œuvre les bonnes pratiques opérationnelles et de sécurité présentes, tout en créant un environnement favorable à des activités efficaces de gestion des incidents.

Description: cette fonction fournit un appui à la partie prenante et émet des recommandations concernant l'amélioration des infrastructures, des outils et des services en rapport avec la cybersécurité dans le but d'améliorer la sécurité et la gestion des incidents dans son ensemble.

Elle pourra fournir des conseils dans les domaines suivants:

- Considérations de sécurité relatives à l'acquisition, la conformité, la vérification, la maintenance et les mises à niveau.
- Audits internes et externes des infrastructures et des outils en rapport avec la cybersécurité.
- Exigences en matière de développement logiciel sécurisé et codage sécurisé.

Résultat: appui à la conception, l'acquisition, la gestion, l'exploitation et la maintenance de l'infrastructure, des systèmes et des outils de la partie prenante, ainsi qu'aide au renforcement des capacités et de la maturité des activités de gestion des incidents.

ANNEXE 1: Remerciements

Les membres de la communauté des CSIRT volontaires suivants ont apporté une contribution significative à la présente version du Cadre des services de la CSIRT. Ils sont cités par ordre alphabétique de nom de famille, sans indication de leur titre, mais avec mention de leur affiliation, de leur rôle et de leur pays:

- Vilius Benetis, NRD CIRT (LT)
- Olivier Caleff (Service Area Coordinator), openCSIRT Foundation (FR)
- Cristine Hoepers (Service Area Coordinator), CERT.br (BR)
- Angela Horneman, CERT/CC, SEI, CMU (US)
- Allen Householder, CERT/CC, SEI, CMU (US)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Art Manion, CERT/CC, SEI, CMU (US)
- Amanda Mullens (Co-Service Area Coordinator), CISCO (US)
- Samuel Perl (Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Daniel Roethlisberger (Service Area Coordinator), Swisscom (CH)
- Sigitas Rokas, NRD CIRT (LT)

- Mary Rossell, Intel (US)
- Robin M. Ruefle (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)
- Mark Zajicek (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)

ANNEXE 2: Termes et définitions

La présente section fournit la définition de certains des termes utilisés dans le Cadre de services de la CSIRT.

- **Action** – Description à divers niveaux de détail de la manière dont quelque chose est fait.
- **Bulletin de sécurité**[9] – Annonce ou bulletin servant à informer, conseiller et avertir concernant la vulnérabilité d'un produit.
- **Capacité** – Activité mesurable qui relève des rôles et responsabilités d'une organisation. Dans le Cadre de services de la FIRST, les capacités peuvent être définies soit en termes de services, soit en termes de fonctions 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.
- **Exposition aux vulnérabilités courantes (CVE)**[10] – Liste d'entrées contenant un numéro d'identification, une description et au moins une référence publique à des vulnérabilités publiquement connues. Elle sert de norme d'identification des vulnérabilités de référence.
- **Système d'évaluation des vulnérabilités courantes (CVSS)**[11] – Score numérique indiquant la gravité d'une vulnérabilité.
- **Liste des failles courantes (CWE)**[12] – Liste officielle des types de failles de sécurité logicielle servant de langage commun de description des failles de sécurité logicielles dans l'architecture, la conception ou le code. Elle sert d'outil de mesure pour les outils de sécurité des logiciels ciblant ces failles et fournit une norme de référence pour les efforts d'identification, d'atténuation, et de prévention des failles.
- **Partie prenante –** Groupe de personnes et/ou d'organisations ayant accès à un ensemble spécifique de services offerts par la CSIRT.
- **Source de données contextuelles** – Source de données fournissant le contexte des points de données, par exemple pour identifier une identité, une ressource ou un événement de sécurité relatif aux informations. Les bases de données utilisateur, les inventaires de

[9] ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation de vulnérabilité – Termes et définition 3.1.
[10] https://cve.mitre.org/.
[11] https://www.first.org/cvss/.
[12] https://cwe.mitre.org/about/index.html.

ressources, les services de répudiation IP ou les données relatives à la surveillance des menaces en constituent des exemples.

- **Divulgation coordonnée des vulnérabilités** – Terme relatif à un processus de divulgation incluant une coordination. Source: ISO/IEC 29147:2018, Termes et définitions.
- **Coordonnateur**[13] – Participant facultatif pouvant aider les fournisseurs et les découvreurs à gérer et à divulguer les informations relatives aux vulnérabilités.
- **Cas d'utilisation de détection** – Condition spécifique que doit détecter la zone de service Gestion des événements relatifs à la sécurité des informations. Ce terme provient de l'ingénierie logicielle, mais est désormais largement utilisé dans l'ingénierie de détection.
- **Embargo** – Délai de publication des détails relatifs à la vulnérabilité jusqu'à ce que les fournisseurs concernés puissent publier des mises à jour de sécurité ou des mesures d'atténuation et des solutions de repli temporaire pour protéger les clients.
- **Découvreur**[14] – Individu ou organisation identifiant une vulnérabilité potentielle dans un produit ou un service en ligne. À noter que les découvreurs peuvent être des chercheurs, des auteurs de rapports, des sociétés de sécurité, des pirates informatiques, des utilisateurs, des gouvernements ou des coordonnateurs.
- **Fonction** – Activité ou ensemble d'activités visant à atteindre l'objectif d'un service donné. Autres définitions: ensemble d'opérations concourant au même résultat[15] et exécutées par un organe ou un ensemble d'organes; rôle joué par un élément dans un ensemble[16].
- **Événement relatif à la sécurité des informations** – Événement observable dans un environnement informatique et pertinent pour la sécurité, tel que l'identifiant de connexion d'un utilisateur ou une alerte IDS. Les événements relatifs à la sécurité des informations produisent généralement des preuves, telles qu'un enregistrement d'audit ou une entrée de journal qu'il est possible de recueillir et d'analyser dans le cadre de la zone de service Gestion des évènements relatifs à la sécurité des informations.
- **Incident relatif à la sécurité des informations**[17] – Tout événement relatif à la sécurité des informations (ou ensemble de tels événements) dommageable indiquant qu'un aspect quelconque de la sécurité des utilisateurs, des systèmes, de l'organisation et/ou des informations du réseau a été compromis. La définition des incidents relatifs à la sécurité des informations peut varier selon les organisations, mais au minimum les catégories suivantes s'appliquent de façon générale:
  - Perte de confidentialité des informations.
  - Compromission de l'intégrité des informations.
  - Refus de service.
  - Mauvais usage des services, des systèmes ou des informations.

---

[13] ISO/IEC 30111:2013 Technologies de l'information – Techniques de sécurité – Processus de gestion des vulnérabilités – Termes et définition 3.1.

[14] ISO/IEC 29147:2014 Technologies de l'information - Techniques de sécurité - Divulgation de vulnérabilité - Termes et définition 3.3.

[15] Source: https://www.larousse.fr/dictionnaires/francais/fonction/34452?q=fonction#34399.

[16] Source: https://www.dictionary.com/browse/function.

[17] Basé sur RFC2350 en remplaçant "sécurité informatique" par "sécurité des informations", https://tools.ietf.org/html/rfc2350.

- Dommages aux systèmes.

Même si elles ont échoué grâce à une protection adéquate, les attaques peuvent être considérées comme des incidents relatifs à la sécurité des informations.

- **Indicateur clé de performance (KPI)**[18] - Valeur mesurable indiquant dans quelle mesure une entreprise atteint efficacement des objectifs stratégiques clés. Les organisations recourent aux KPI à plusieurs niveaux pour évaluer la mesure dans laquelle elles atteignent leurs objectifs.
- **Maturité** – Degré d'efficacité avec lequel une organisation concrétise une capacité donnée dans le cadre de sa mission et de ses pouvoirs. Ce niveau de maîtrise est atteint soit dans l'exécution de fonctions spécifiques, soit dans un groupe de fonctions ou de services. L'aptitude d'une organisation est fonction de la portée et de la qualité des politiques et de la documentation en place ainsi que de sa capacité à exécuter un processus défini.
- **Open Source (code source ouvert)** – Travaux dont la licence permet la liberté de rediffusion et de modification. Le code source est à la disposition du public et distribué gratuitement. Il ne discrimine aucune personne, aucun groupe ou aucun domaine d'activité et est technologiquement neutre. Les logiciels à source ouverte sont souvent gérés par une communauté d'individus et d'entités qui les créent et les mettent à jour de façon collaborative.
- **Produit**[19] - Système mis en œuvre ou développé à des fins commerciales ou non.
- **Correction (ou correctif)**[20] - Changement apporté à un produit ou un service en ligne afin de supprimer ou d'atténuer une vulnérabilité. En général, les corrections consistent à remplacer un fichier binaire, modifier une configuration ou appliquer un correctif au code source et à le recompiler. Autres termes utilisés pour "correction": correctif, réparation, mise à jour, correctif logiciel et mise à niveau. Les atténuations sont également appelées solution de repli temporaire ou contremesures.
- **Divulgation responsable** - Terme faisant référence à un processus ou à un modèle dans lequel une vulnérabilité n'est divulguée qu'au bout d'un délai permettant la mise à disposition d'une correction (correctif ou réparation). Ce terme n'est pas nécessairement synonyme de "divulgation coordonnée des vulnérabilités".
- **Risque**[21] - "Effet de l'incertitude sur les objectifs." Dans cette définition, l'incertitude comprend les événements (susceptibles de se produire ou non) et les incertitudes dues à l'ambiguïté ou au manque d'informations.
- **Acceptation des risques** –[22] Stratégie d'intervention en cas de risque selon laquelle l'équipe de projet décide de prendre acte des risques et de ne pas agir tant qu'ils ne se concrétisent pas.

---

18 https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator.
19 ISO/IEC 29147:2014 Technologies de l'information - Techniques de sécurité - Divulgation de vulnérabilité - Termes et définition 3.5.
20 ISO/IEC 29147:2014 Technologies de l'information - Techniques de sécurité - Divulgation de vulnérabilité - Termes et définition 3.6.
21 ISO 31000:2009/ ISO Guide 73:2002 Gestion des risques — Principes et lignes directrices – Termes/Définitions 2.1.
22 The Project Management Body of Knowledge (PMBOK) Guide and Standards.

- **Registre des risques**[23] – Document dans lequel sont consignés les résultats de l'analyse des risques et de la planification des interventions en cas de risque.
- **Service** – Ensemble de fonctions reconnaissables et cohérentes visant un résultat spécifique. Ce résultat peut être escompté ou demandé par les parties prenantes ou pour le compte d'une entité ou encore de ses acteurs.
- **Accord de niveau de service (SLA)** – Contrat conclu entre un fournisseur de services (interne ou externe) et l'utilisateur final définissant le niveau de service attendu du fournisseur de services.
- **Acteurs**[24] – Individus ou groupes définissant et modifiant les zones de service ou les services et assurant une stratégie de communication des services adaptée ainsi que des groupes pouvant bénéficier des services offerts.
- **Tâches** – Liste des actions à mener pour effectuer une fonction donnée.
- **Fournisseur**[25] – Personne ou organisation ayant développé le produit ou le service ou responsable de sa maintenance.
- **Vulnérabilité**[26] – Faille exploitable dans un logiciel, un matériel ou un service en ligne.

ANNEXE 3: Ressources

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001. https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1 https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976. http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005. https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed]. https://www.cnss.gov/cnss/

[23] The Project Management Body of Knowledge (PMBOK) Guide and Standards.
[24] Architecture Content Framework.
[25] ISO/IEC 30111:2013 Technologies de l'information - Techniques de sécurité - Processus de gestion des vulnérabilités - Termes et définition 3.7.
[26] ISO/IEC 30111:2013 Technologies de l'information - Techniques de sécurité - Processus de gestion des vulnérabilités - Termes et définition 3.8.

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.
https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018
https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013
https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019.
https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

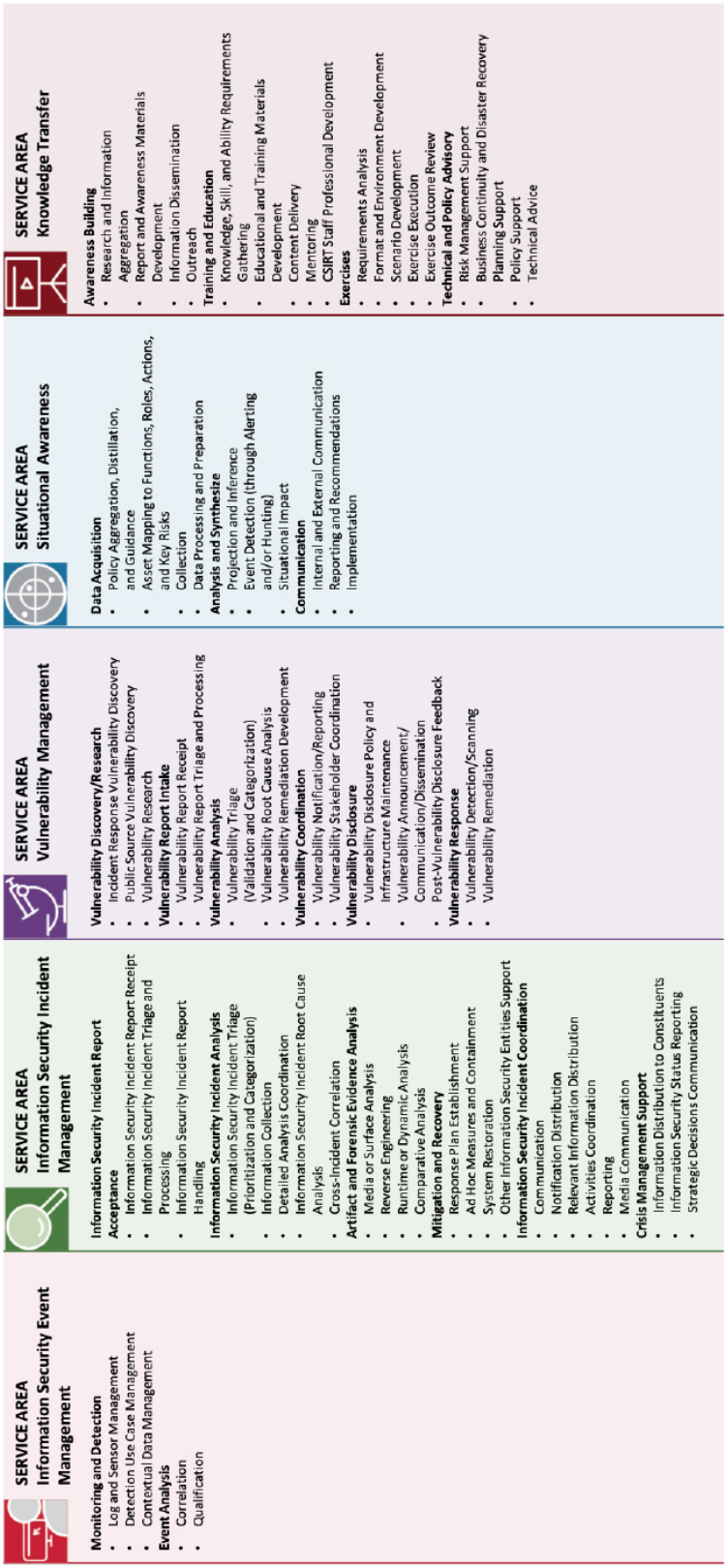
Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.
https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations*. The MITRE Corporation Website*. January 2016
https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

ANNEXE 4: Vue d'ensemble de tous les services des équipes CSIRT et de leurs fonctions



SERVICE AREA
Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA
Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing
- Information Security Incident Report Handling

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesize
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
Knowledge Transfer

Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

Légende de la figure:

ZONE DE SERVICE Gestion des événements relatifs à la sécurité des informations	ZONE DE SERVICE Gestion des incidents relatifs à la sécurité des informations	ZONE DE SERVICE Gestion des vulnérabilités	ZONE DE SERVICE Appréciation de la situation	ZONE DE SERVICE Transfert de connaissances
Surveillance et détection ■ Gestion des journaux et des capteurs ■ Gestion des cas d'utilisation de détection ■ Gestion des données contextuelles **Analyse des événements** ■ Corrélation ■ Caractérisation	**Acceptation des signalements d'incidents relatifs à la sécurité des informations** ■ Réception des signalements d'incidents relatifs à la sécurité des informations ■ Tri et traitement des incidents relatifs à la sécurité des informations ■ Traitement des signalements d'incidents relatifs à la sécurité des informations **Analyse des incidents relatifs à la sécurité des informations** ■ Tri des incidents relatifs à la sécurité des informations (hiérarchisation et classification) ■ Collecte des informations ■ Coordination de l'analyse détaillée ■ Analyse des causes premières des incidents relatifs à la sécurité des informations ■ Corrélation des incidents **Analyse des artefacts et des preuves judiciaires** ■ Analyse des supports physiques ou des surfaces ■ Rétro-ingénierie ■ Analyse de l'exécution ou analyse dynamique ■ Analyse comparative **Atténuation et reprise** ■ Établissement d'un plan de riposte ■ Mesures ad hoc et endiguement	**Découverte/recherche de vulnérabilités** ■ Découverte de vulnérabilités lors de l'intervention en cas d'incident ■ Découverte de vulnérabilités à partir de sources publiques ■ Recherche de vulnérabilités **Recueil des rapports de vulnérabilité** ■ Réception des rapports de vulnérabilité ■ Tri et traitement des rapports de vulnérabilité **Analyse des vulnérabilités** ■ Tri des vulnérabilités (validation et classification) ■ Analyse des causes premières des vulnérabilités ■ Élaboration de la correction des vulnérabilités **Coordination des vulnérabilités** ■ Notification/signalement des vulnérabilités ■ Coordination des acteurs concernés par les vulnérabilités **Divulgation des vulnérabilités** ■ Politique de divulgation des vulnérabilités et maintenance de l'infrastructure ■ Annonces/communication/diffusion des vulnérabilités ■ Retours d'information postérieurs à la divulgation des vulnérabilités	**Acquisition de données** ■ Regroupement, diffusion et consignes relatifs aux politiques ■ Recensement des ressources attribuées aux fonctions, aux rôles, aux actions et aux risques principaux ■ Collecte ■ Traitement et préparation des données **Analyse et synthèse** ■ Projection et inférence ■ Détection des événements (au moyen d'alertes et/ou de recherche) ■ Impact sur la situation **Communication** ■ Communication interne et externe ■ Rapports et recommandations ■ Mise en œuvre	**Renforcement des connaissances** ■ Recherche et regroupement des informations ■ Rapports et élaboration de documents de sensibilisation ■ Diffusion des informations ■ Sensibilisation **Formation et apprentissage** ■ Définition des besoins en matière de connaissances, de compétences et d'aptitudes ■ Élaboration de documents d'éducation et de formation ■ Fourniture de contenus ■ Mentorat ■ Développement professionnel du personnel de la CSIRT **Exercices** ■ Analyse des besoins ■ Élaboration du format et de l'environnement ■ Élaboration de scénarios ■ Exécution des exercices ■ Examen des résultats des exercices **Conseil technique et stratégique** ■ Appui à la gestion des risques ■ Appui à la continuité d'activité et à la planification du rétablissement suite à un sinistre

	■ Restauration des systèmes ■ Appui à d'autres entités en charge de la sécurité des informations **Coordination des incidents relatifs à la sécurité des informations** ■ Communication ■ Distribution des notifications ■ Distribution des informations pertinentes ■ Coordination des activités ■ Signalements ■ Communication médiatique **Appui à la gestion de crise** ■ Distribution des informations aux parties prenantes ■ Signalements relatifs à l'état de la sécurité des informations ■ Communication des décisions stratégiques	**Intervention en cas de vulnérabilité** ■ Détection/recensement des vulnérabilités ■ Correction des vulnérabilités		■ Appui aux politiques ■ Conseil technique