Pintemps 2020

Cadre de services de l'Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT)

Versión 1.1

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 de bonnes pratiques. Son contenu n'est fourni qu'à titre d'information. FIRST.Org réfute toute responsabilité quant aux éventuels préjudices consécutifs ou liés à l'utilisation de ces informations..

Cadre de services de la PSIRT

Objectif

Les *Cadres de services* sont des documents de haut niveau détaillant les services que peuvent fournir les équipes d'intervention en cas d'incident informatique (CSIRT) et les équipes d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT). Ils sont élaborés par des experts reconnus de la communauté FIRST. Le FIRST s'efforce d'y intégrer les retours d'information de l'ensemble des secteurs, notamment des CSIRT ayant une responsabilité nationale, des CSIRT et PSIRT du secteur privé ainsi que d'autres parties prenantes. Ces documents devaient servir de référence lors de la création de nouveaux supports de formation. Toutefois, leur champ d'application est aujourd'hui nettement plus vaste; ils peuvent par exemple être utilisés lors de l'élaboration d'un catalogue de services initial pour de nouvelles équipes.

Lors de la création du Cadre de services, il est devenu évident que les PSIRT fournissaient différents services et qu'elles intervenaient dans des environnements relativement distincts. Il a donc été décidé de créer un document séparé consacré aux PSIRT. Ces deux documents seront harmonisés, en mettant en évidence leurs nombreuses similitudes. L'élaboration des cadres est dirigée par l'*Education Advisory Board*.

Ces Cadres visent à aider les organisations à renforcer, à maintenir et à élargir les capacités de leurs CSIRT ou PSIRT. Ce sont des guides qui définissent différents modèles, capacités, services et résultats. Les équipes sont ainsi libres de mettre en œuvre leur propre modèle et de renforcer les capacités qui répondent aux besoins uniques de leurs parties prenantes Les Cadres visent à aider les équipes d'intervention en cas d'incident de sécurité (SIRT) en précisant les responsabilités fondamentales, en fournissant des orientations sur les modalités de renforcement des capacités nécessaires pour assumer ces responsabilités, et en offrant des informations sur la façon dont les équipes peuvent ajouter et transmettre de la valeur à leurs organisations.

Introduction

Une Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT) est une entité au sein d'une organisation qui, fondamentalement, met l'accent sur l'identification, l'évaluation et l'élimination des risques associés aux failles de sécurité des produits, y compris les offres, les solutions, les composants et/ou les services produits et/ou vendus par une organisation.

Une PSIRT correctement déployée n'est pas un groupe opérant de façon indépendante, déconnecté de l'élaboration des produits de l'organisation. Au contraire, elle fait partie intégrante de l'initiative d'ingénierie sécurisée élargie de l'organisation. Cette structure veille à ce que les activités de garantie de la sécurité soient intégrées au cycle de développement sécurisé (SDL).

Les interventions en cas d'incident relatif à la sécurité des produits sont souvent associées à la phase de maintenance du SDL, car la majorité des failles de sécurité touchant les produits sont signalées en tant que défauts de qualité une fois que le produit a été lancé sur le marché.

Toutefois, la PSIRT peut avoir une influence sur la définition préalable des besoins concernant les phases d'architecture, de conception, de planification et de modélisation des risques. Les fonctions de la PSIRT peuvent également apporter de la valeur ajoutée en fournissant des orientations et en assurant un contrôle pour le traitement des problèmes de sécurité détectés en interne.

Structure du Cadre de services de la PSIRT

ZONE DE SERVICES – SERVICES – FONCTIONS – SOUS-FONCTIONS

ZONES DE SERVICES

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

SERVICES

Un service est un ensemble d'actions identifiables et homogènes visant l'obtention d'un résultat précis en faveur ou pour le compte de la partie prenante d'une équipe d'intervention en cas d'incident.

La spécification des services suit le modèle suivant:

- Un champ "Description" décrivant la nature du service.
- Un champ "Objectif et Résultat" décrivant l'objet et 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 et Résultat" décrivant l'objet et les résultats mesurables du service.
- La liste des sous-fonctions susceptibles d'être effectuées dans le cadre de la fonction.

SOUS-FONCTION

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.

Différence entre PSIRT et CSIRT

L'accent mis sur la nature des produits proposés constitue le principal facteur de différenciation entre la PSIRT d'une organisation et ses autres équipes d'intervention en cas d'incident telles que la CSIRT. En règle générale, les CSIRT d'entreprise sont axées sur la sécurité des systèmes informatiques et/ou des réseaux qui forment l'infrastructure des organisations.

S'il existe des différences substantielles entre les équipes CSIRT et PSIRT d'entreprise, il importe de ne pas omettre pour autant leurs synergies. Il convient de retenir que la PSIRT n'opère pas indépendamment des autres acteurs d'une organisation. Le présent cadre veillera en permanence à mettre en évidence les domaines de collaboration et de synergie qui doivent être entretenus.

Structure organisationnelle de la PSIRT

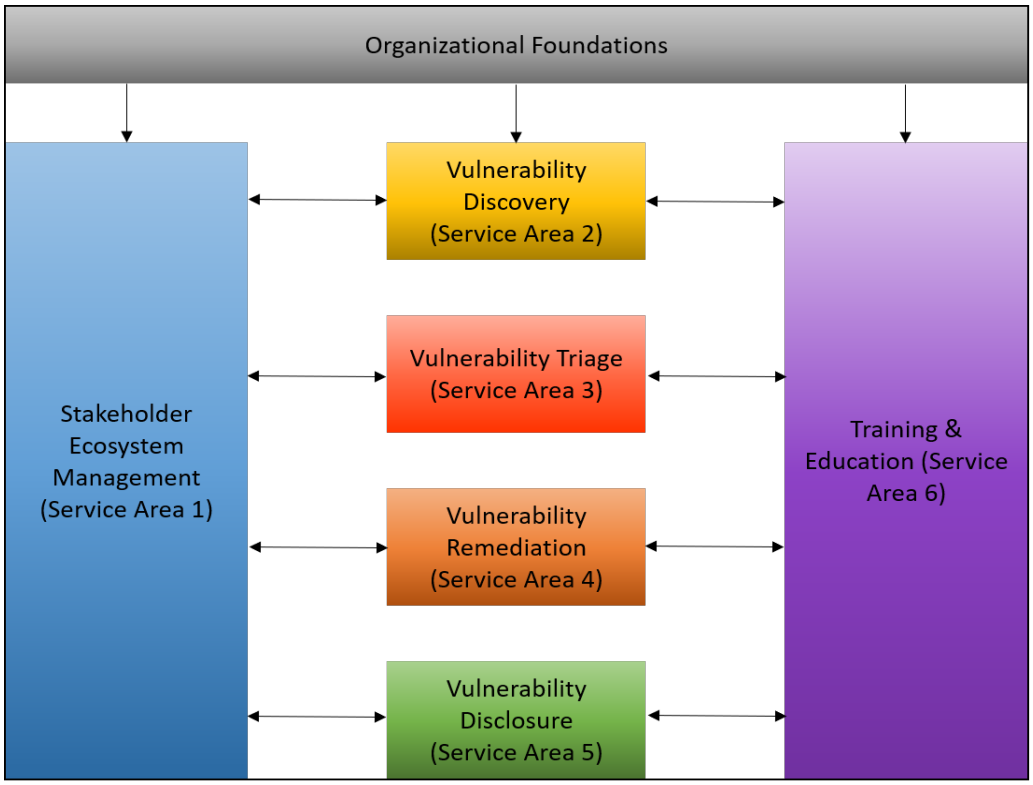


Figure 1: Structure organisationnelle

Légende de la Figure 1:
Fondements opérationnels
Gestion de l'écosystème des parties prenantes (zone de service 1)
Découverte de vulnérabilités (zone de service 2)
Tri et analyse des vulnérabilités (zone de service 3)
Correction des vulnérabilités (zone de service 4)
Divulgation des vulnérabilités (zone de service 5)
Formation et apprentissage (zone de service 6)

Les PSIRT peuvent être aussi uniques et variées que les produits qu'elles aident à protéger. Les caractéristiques opérationnelles, les modèles de fonctionnement, les portefeuilles de produits, les structures organisationnelles et les stratégies de développement des produits varient d'une organisation à l'autre au sein d'un même secteur ou d'une même industrie. C'est pourquoi il n'existe aucune stratégie d'intervention ni aucun modèle d'équipe universel en cas d'incident relatif à la sécurité des produits auxquels toutes les organisations peuvent se référer. Néanmoins, trois modèles de PSIRT sont employés par la majorité des entreprises: les modèles réparti, centralisé et hybride.

Modèle réparti

Le modèle réparti nécessite une petite PSIRT réduite à ses éléments essentiels. Celle-ci doit collaborer avec les représentants des équipes de produit au traitement des failles de sécurité détectées au sein des produits. Dans le cadre de ce modèle, la PSIRT, de taille réduite, assume les responsabilités suivantes:

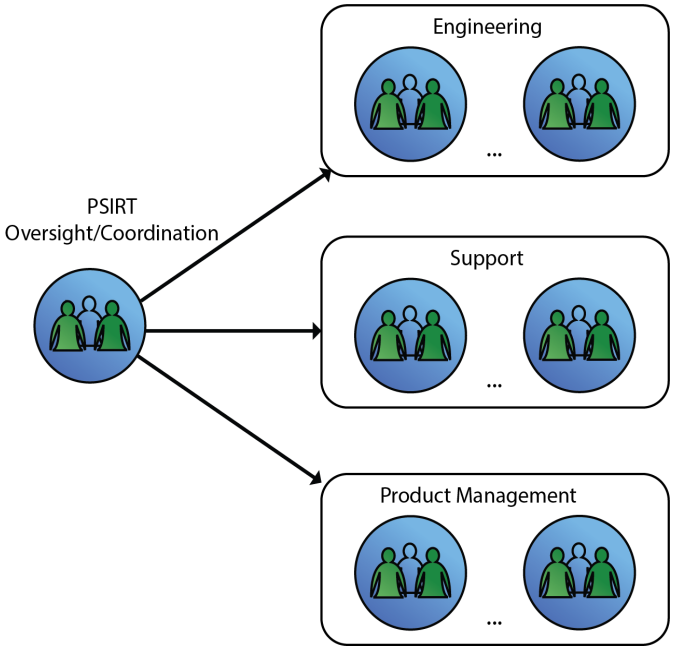


Figure 2: Modèle réparti

Légende de la Figure 2:

Contrôle/coordination de la PSIRT	Ingénierie
	Appui
	Gestion des produits

- Créer des politiques, des processus, des procédures et des directives afin de trier, d'analyser, de corriger et de communiquer les corrections, les mesures d'atténuations ou d'autres informations et conseils visant à traiter les failles de sécurité.

- Établir un registre des représentants des ingénieurs en sécurité des produits (à plusieurs niveaux) dans l'ensemble de l'organisation.
- Guider et orienter les interventions visant à remédier aux failles de sécurité des produits et à gérer les risques susceptibles d'affecter l'entreprise.
- Agir comme point de collecte pour les failles de sécurité entrantes lorsque les économies d'échelle bénéficient d'un point de contrôle central.
- Informer le propriétaire/gestionnaire du produit et l'ingénieur en sécurité de la présence de nouvelles failles de sécurité, aider à l'élaboration de plans de correction, et rédiger/publier des communications sur les corrections ou les mesures d'atténuation, ainsi que sur la gestion des incidents.

Le modèle réparti convient particulièrement à une organisation disposant d'un vaste portefeuille de produits éclectiques, car le coût de la mission de la PSIRT est amorti au sein de l'organisation. Ce modèle permet également d'accroître la portée de la mission de la PSIRT en tirant parti des salariés compétents au sein des équipes d'ingénierie des produits.

Le modèle réparti s'accompagne toutefois d'une difficulté: les personnes en charge du tri et de la mise en œuvre des corrections en cas de failles de sécurité ne sont pas directement sous l'autorité de la PSIRT et ne relèvent pas de cette dernière.

Modèle centralisé

Dans le cas du modèle centralisé, la PSIRT est constituée d'un plus grand nombre de membres, issus de différents départements, et placés sous l'autorité d'un ou plusieurs cadres supérieurs responsables de la sécurité des produits de l'organisation. Ce modèle se structure généralement comme suit :

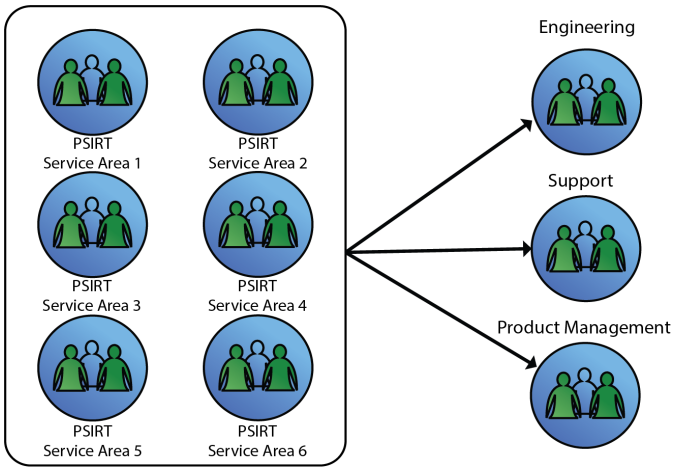


Figure 3: Modèle centralisé

Légende de la Figure 3
Zone de service
Ingénierie
Appui
Gestion des produits

- *Le Département de la gestion du programme de la PSIRT:* crée des politiques, des processus, des procédures et des directives afin de trier, d'analyser, de corriger et de communiquer les corrections visant à traiter les failles de sécurité; gère les opérations de l'ensemble de l'initiative PSIRT ainsi que le système de tickets, et représente la direction de la PSIRT auprès de l'organisation.
- *L'équipe PSIRT en charge des renseignements de sécurité et du tri:* surveille les différentes sources externes afin d'identifier des failles de sécurité; évalue les effets initiaux des failles de sécurité sur le portefeuille de produits de l'organisation.
- *L'équipe PSIRT en charge de la correction et des communications:* fournit directement aux équipes d'ingénierie des produits les corrections du code rectifiant les failles de sécurité.

Ce modèle fonctionne bien au sein d'une organisation de taille plus réduite et/ou d'une organisation disposant d'un portefeuille de produits homogène. Il concentre et cultive un niveau élevé de compétence et d'expertise en matière de sécurité au sein d'un domaine de l'organisation. Ce modèle présente néanmoins une contrainte, à savoir le coût de maintien d'une équipe centrale spécialisée dont, en outre, le déploiement s'avère difficile lorsque le portefeuille de produits s'élargit et/ou se diversifie.

Modèle hybride

- Le modèle hybride est une variante comprenant des caractéristiques des modèles réparti et centralisé. Une organisation peut choisir d'adopter des caractéristiques et des attributs des deux modèles, créant ainsi un modèle hybride qui prend en compte les facteurs suivants:
- la structure et la taille de l'organisation;
- la taille et la diversité du portefeuille de produits;
- la stratégie de développement des produits.

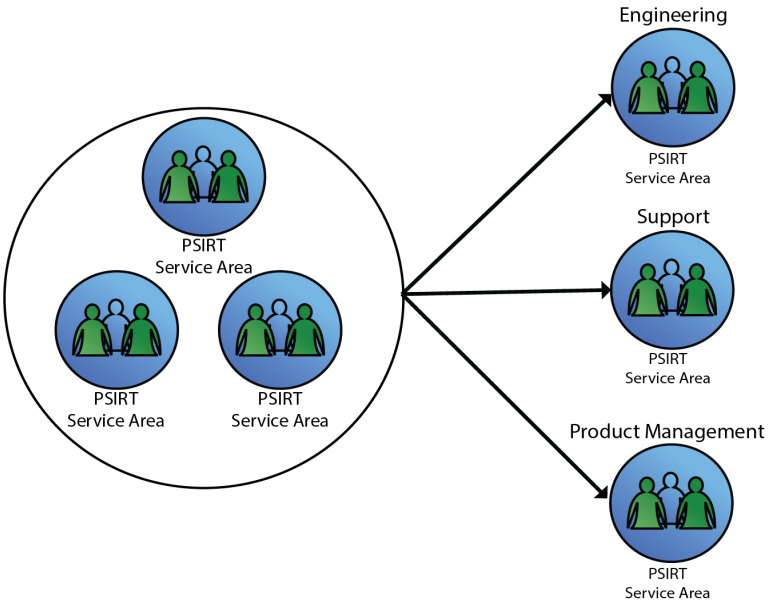


Figure 4: Modèle hybride

Légende de la Figure 4:
Zone de service
Ingénierie
Appui
Gestion des produits

Autres considérations

Il convient d'accorder suffisamment d'autonomie aux PSIRT pour qu'elles puissent rester objectives et indépendantes dans leur approche des failles de sécurité affectant les produits de l'organisation. C'est pourquoi l'organisation, lors de l'élaboration de la stratégie et de la structure de sa PSIRT, doit tenir compte de la meilleure façon d'inclure l'équipe en son sein et de l'intégrer à sa structure de signalement. L'entreprise doit nommer un responsable chargé de la PSIRT, auquel l'équipe est tenue de rendre des comptes.

À mesure qu'une PSIRT gagne en maturité et se déploie, et que sa mission évolue, la composition ou la structure de signalement de l'équipe est amenée à changer. L'évolution et la maturité d'une PSIRT sont guidées par ses principales parties prenantes et, malheureusement, l'impact d'une grave vulnérabilité sur un large spectre de la base de parties prenantes de l'organisation. Les parties prenantes sont souvent définies par le modèle adopté par l'organisation, ainsi que par la taille de cette dernière.

Parties prenantes

La prise en compte des besoins et des exigences des parties prenantes constitue un élément fondamental de la définition de la stratégie et de la structure d'une PSIRT. L'identité des parties prenantes et leur degré d'influence peuvent dépendre du modèle de PSIRT adopté par l'organisation. Le maintien de relations positives est essentiel. La *Zone de service 1: Gestion de l'écosystème des parties prenantes* contient de plus amples informations sur l'écosystème des parties prenantes et leurs modalités de gestion.

Enfin, il convient de prendre en compte les éléments d'influence lors de la constitution de l'équipe d'intervention en cas d'incident relatif aux produits et de l'élaboration de sa stratégie. Ils se distinguent des parties prenantes, ces dernières étant des personnes ou des groupes de personnes discrètement nommés. À l'inverse, les éléments d'influence désignent les normes, la législation, les réglementations et les tendances sectorielles et gouvernementales. Les exigences qu'ils imposent sur la formation, les stratégies, les politiques et les caractéristiques opérationnelles d'une PSIRT peuvent s'avérer plus strictes que celles des parties prenantes.

Quel est le rôle d'une PSIRT?

Selon le modèle choisi, la portée et les activités opérationnelles d'une PSIRT peuvent varier, sans pour autant modifier les mesures nécessaires pour traiter les failles de sécurité des produits d'une organisation. Le modèle précise la portée des capacités, des mesures et des responsabilités directement attribuées à la PSIRT plutôt que celles réparties dans l'ensemble de l'organisation.

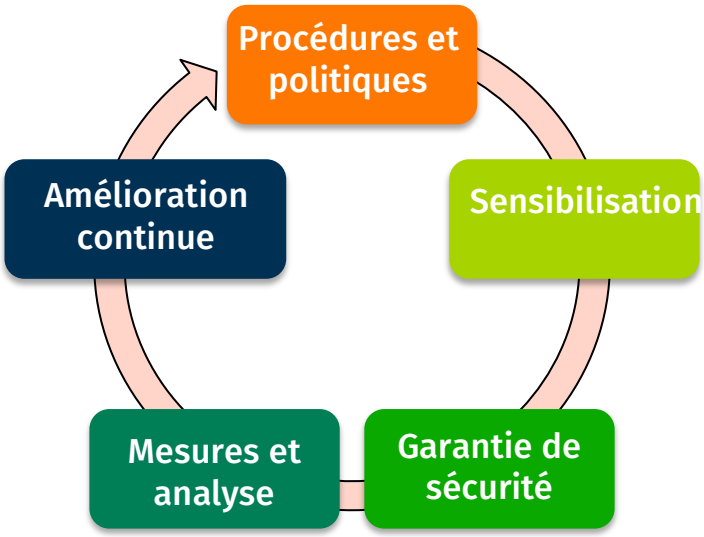


Figure 5: Activités générales de la PSIRT

Procédure continue et élaboration des politiques

Les PSIRT élaborent les politiques de l'organisation relatives à de la sécurité des produits. Les exigences définies par la PSIRT doivent être motivées et dictées par les besoins de l'entreprise, et non l'inverse. La direction de l'organisation doit examiner les politiques élaborées par la PSIRT et leur transmettre son autorité avant de les mettre en œuvre. Les politiques approuvées doivent s'accompagner de procédures claires qui, une fois suivies, garantissent leur respect par l'organisation.

Sensibiliser les parties prenantes

Outre ses politiques et procédures, la PSIRT doit mettre au point des flux de travail et des systèmes de gestion qui simplifient l'exécution et la réalisation des actions requises pour traiter les failles de sécurité des produits. Ces processus permettront à l'organisation d'intégrer plus facilement la sécurité des produits à ses activités économiques quotidiennes ordinaires.

Au moment de lancer la mission et de déployer les politiques et les procédures de la PSIRT, il convient d'éviter l'erreur majeure consistant à les considérer comme des responsabilités ou exigences distinctes. Par conséquent, il est essentiel de sensibiliser l'ensemble des membres de l'organisation aux bases de la sécurité des produits et au rôle qu'ils jouent. L'organisation doit être incluse, habilitée et responsabilisée dans son ensemble afin de répondre aux exigences des politiques de la PSIRT.

L'importance des mesures

Il est essentiel de mesurer la réussite de la mission d'intervention en cas d'incident relatif à la sécurité des produits. Les exigences ne sont pas définies par les mesures effectuées; ces dernières soutiennent le programme, aident à définir les ressources nécessaires, et peuvent contribuer à identifier les domaines dans lesquels les procédures/les outils doivent être améliorés. La création et le suivi des mesures peuvent également aider les PSIRT à gagner en

maturité en mettant en évidence les problèmes ou les obstacles liés au déploiement et à l'adoption d'une PSIRT. Les sections *Service 1.7 Mesures relatives aux parties prenantes* et *Service 5.3 Mesures relatives aux vulnérabilités* approfondissent les types de mesures dont il peut être utile d'effectuer le suivi.

Définitions

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

- **Acceptation des risques**[1] – 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.
- **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.
- **Bulletin de sécurité**[2] – Annonce ou bulletin servant à informer, conseiller et avertir concernant la vulnérabilité d'un produit.
- **Coordonnateur**[3] – Participant facultatif pouvant aider les fournisseurs et les découvreurs à gérer et à divulguer les informations relatives aux vulnérabilités.
- **Correction (ou correctif)**[4] – 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 mesures d'atténuation sont également appelées solutions de repli temporaire ou contremesures.
- **Cycle de développement sécurisé (SDL)** – Processus de développement aidant les développeurs à mettre au point des produits plus sûrs et à traiter les exigences de conformité en matière de sécurité tout en réduisant les coûts de développement.

[1] The Project Management Body of Knowledge (PMBOK) Guide and Standards.
[2] ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation des vulnérabilités – Termes et définition 3.1.
[3] ISO/IEC 30111:2013 Technologies de l'information – Techniques de sécurité – Processus de gestion des vulnérabilités – Termes et définition 3.1.
[4] ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation des vulnérabilités – Termes et définition 3.6.

- **Découvreur**[5] – 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.
- **Échelles de bogues** – Critères définissant les types de bogues pouvant être considérés comme une faille de sécurité. Les bogues qui remplissent ces critères seront traités comme une vulnérabilité par le biais des procédures opérationnelles normalisées de la PSIRT.
- **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.
- **Fournisseur**[6] – Personne ou organisation ayant développé le produit ou le service, ou étant responsable de sa maintenance.
- *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.
- **Partenaires** – Fabricants d'équipement d'origine (OEM), fournisseurs, producteurs de concepts d'origine (ODM).
- **Parties prenantes**[7] – Les parties prenantes de la PSIRT sont les groupes élaborant et modifiant le produit ou les composants du produit, garantissant une stratégie de communication relative au produit appropriée, et les groupes pouvant bénéficier de la sécurité du produit. En bref, les parties prenantes de la PSIRT contribuent à la sécurité du produit et à l'intervention en cas d'incident, ou en bénéficient.
- **Produit**[8] – Système mis en œuvre ou développé à des fins commerciales ou non.
- **Registre des risques**[9] – Document dans lequel sont consignés les résultats de l'analyse des risques et de la planification des interventions en cas de risque.
- **Risque**[10] – "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.
- **Seuil de qualité** – Ensemble de critères devant être remplis avant que le produit passe à la phase de développement ou de lancement suivante.

---

[5] ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation des vulnérabilités – Termes et définition 3.3.

[6] ISO/IEC 30111:2013 Technologies de l'information – Techniques de sécurité – Processus de gestion des vulnérabilités – Termes et définition 3.7.

[7] Architecture Content Framework.

[8] ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation des vulnérabilités – Termes et définition 3.5.

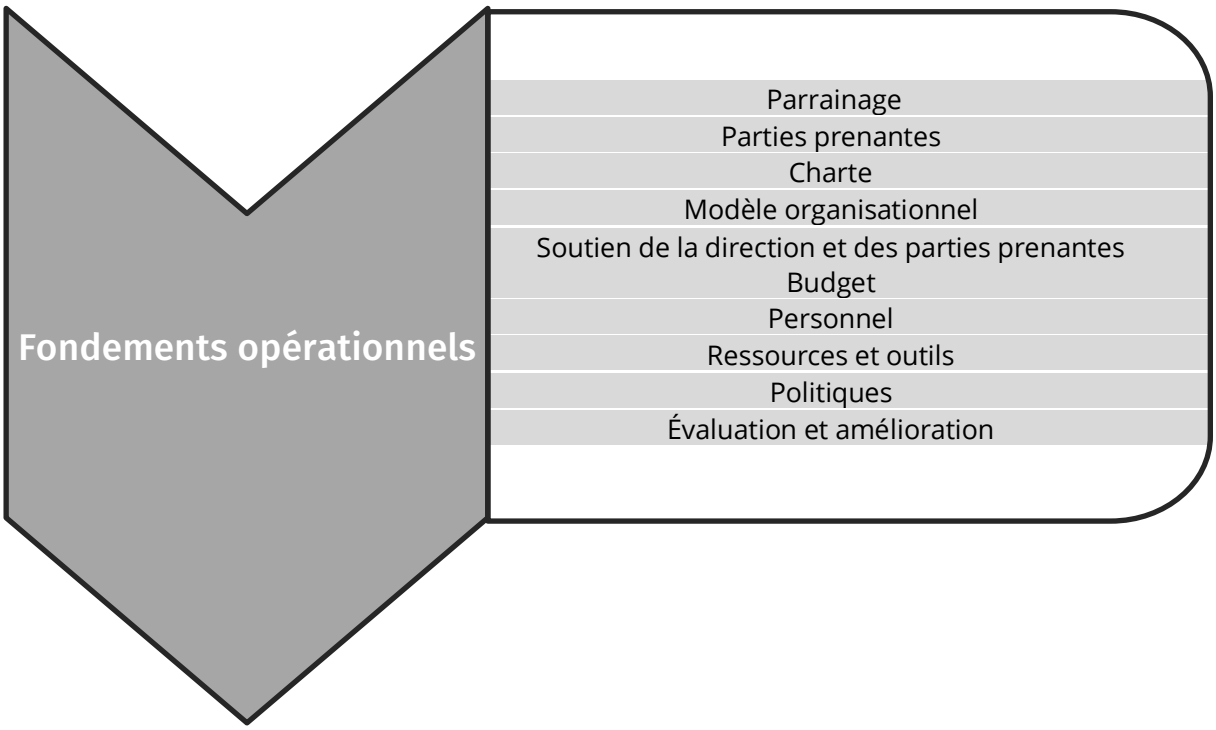
[9] The Project Management Body of Knowledge (PMBOK) Guide and Standards.

[10] ISO 31000:2009/ ISO Guide 73:2002 Gestion des risques — Principes et lignes directrices – Termes/Définitions 2.1.

- **Tiers** – Tout fournisseur ou producteur en amont fournissant des composants intégrés à un produit ou à une solution/un service.
- **Vulnérabilité**[11] – Faille exploitable dans un logiciel, un matériel ou un service en ligne.

[11] ISO/IEC 30111:2013 Technologies de l'information – Techniques de sécurité – Processus de gestion des vulnérabilités – Termes et définition 3.8.

Fondements opérationnels



Cette section définit et décrit les bases ou éléments essentiels dont a besoin une organisation pour planifier, établir et opérer de façon efficace une PSIRT.

Objectif
Donner à une organisation les moyens de planifier et de mettre en œuvre les éléments fondamentaux nécessaires à l'établissement et à au fonctionnement d'une PSIRT.

Résultat
L'identification, la planification et la mise en œuvre des éléments opérationnels fondamentaux de la PSIRT aident les organisations à établir leur équipe. En outre, cela permet de préparer cette dernière à mener sa mission à bien et à soutenir la capacité de l'entreprise à fournir ses produits et services aux parties prenantes prévues.

I. Stratégique

A. Parrainage de la direction

Obtenir un parrainage de la direction de l'organisation et de ses décideurs principaux.

Objectif
Informer et obtenir le soutien (adhésion) de la direction de l'organisation (par exemple, cadres dirigeants, conseil d'administration) ou d'autres décideurs pour permettre à la PSIRT de fonctionner efficacement.

Résultat
Financement et soutien continus fondés sur les mesures liées aux activités souhaitées.

Afin d'obtenir le parrainage de la direction, l'organisation doit informer ou sensibiliser les dirigeants en leur fournissant un plan et d'autres renseignements complémentaires pour les aider à comprendre la finalité, l'importance et les risques potentiels des failles de sécurité ainsi que les avantages de disposer d'une PSIRT. (Voir les sections "Charte de la PSIRT" et "Budget" ci-après.)

Voir la section Service 1.1 Gestion des parties prenantes internes pour obtenir des informations connexes.

B. Partie prenante

Identifier les parties prenantes et la relation qu'entretiendra votre PSIRT avec ces groupes.

Objectif
Comprendre l'identité des personnes qui bénéficieront des services de la PSIRT et avec lesquelles cette dernière interagira.

Résultat
Liste clairement définie des parties concernées.

Elle doit inclure les parties prenantes externes, telles que les clients de l'organisation, les chercheurs en sécurité externes, les CSIRT et d'autres PSIRT, ainsi que les parties prenantes internes, à l'instar des développeurs de logiciels, des ingénieurs, du service clientèle, des équipes juridiques et des équipes des relations publiques, d'affaires et avec les médias.

Voir les sections *Zone de service 1 Gestion de l'écosystème des parties prenantes* (*Service 1.1 Gestion des parties prenantes internes, Service 1.2 Mobilisation de la communauté des découvreurs, Service 1.3 Mobilisation de la communauté et de l'organisation*, et *Service 1.4 Gestion des parties prenantes en aval*) pour obtenir des informations connexes.

C. Charte de la PSIRT

Élaborer une charte ou tout autre document (par exemple, plan stratégique, plan de mise en œuvre, ou document de fond relatif aux opérations).

Objectif
Définir, décrire et documenter les éléments de programme de base qui sous-tendront les activités de la PSIRT.

Résultat
Un document décrivant les raisons pour lesquelles la PSIRT a été créée/financée et les résultats souhaités à son égard.

La charte/le plan relatif à la PSIRT doit présenter les éléments suivants:

- la mission de la PSIRT (doit soutenir la mission de l'organisation et s'aligner sur celle-ci);
- l'objectif, les rôles et les responsabilités;
- les produits et services (par exemple, recevoir des rapports de vulnérabilité, élaborer des mises à jour et des correctifs, diffuser des annonces relatives aux correctifs).

D. Modèle organisationnel

Choisir et documenter la structure et le modèle organisationnels qu'utilisera la PSIRT.

Objectif
Définir, décrire et documenter le modèle organisationnel qui sous-tendra les activités de la PSIRT.

Résultat
Établir une structure d'équipe strictement définie dont les rôles et les responsabilités sont documentés.

Le modèle organisationnel documenté doit décrire la structure de signalement interne des PSIRT et identifier l'autorité dont relève la PSIRT. Voir la section "Structure organisationnelle de la PSIRT", dans laquelle certains modèles organisationnels courants sont décrits (par exemple, modèle réparti, modèle centralisé, modèle hybride). Voir la section *Service 1.5 Coordination des communications relatives aux incidents au sein de l'organisation* pour de plus amples informations sur ce sujet.

E. Soutien de la direction et des parties prenantes

Obtenir le soutien et l'adhésion de la direction et des parties prenantes internes de l'organisation.

Objectif
Informer et obtenir le soutien et l'adhésion d'autres dirigeants et parties prenantes internes pour permettre le fonctionnement efficace de la PSIRT.

Résultat
Les parties prenantes sont informées des mesures clés liées aux activités pour garantir leur soutien continu.

Voir la section *Service 1.1 Gestion des parties prenantes internes* pour obtenir des informations connexes.

II. Tactique

A. Budget

Déterminer les coûts des ressources nécessaires pour faire fonctionner la PSIRT et obtenir les fonds adéquats pour financer ces ressources.

Objectif
Définir, décrire et documenter le modèle organisationnel qui sous-tendra les activités de la PSIRT et son financement.

Résultat
Coûts opérationnels, dépenses et modèle de financement documentés de la PSIRT.

Le budget doit inclure les dépenses relatives au personnel de la PSIRT (salaires, avantages, et autres frais grevés), les frais liés aux équipements et autres charges d'investissement (par

exemple, systèmes/appareils informatiques, logiciels, licences), et budget de formation (y compris les frais de déplacement).

B. Personnel

Déterminer les ressources en personnel nécessaires pour assurer les services de la PSIRT et disposer d'un personnel qualifié.

Objectif
Définir, décrire et documenter le modèle organisationnel sur lequel reposera la dotation en personnel de la PSIRT.

Résultat
Les besoins en matière de ressources en personnel de la PSIRT seront documentés.

Il s'agit notamment d'identifier les différents postes ou rôles et responsabilités du personnel pour chaque membre de la PSIRT, ainsi que les compétences (connaissances, compétences, et aptitudes) et toute autre exigence (par exemple, formation, expérience, certifications) attendue à l'égard de ces rôles. Ces postes ou rôles peuvent être occupés par des salariés à temps plein, des fournisseurs, des prestataires ou plusieurs d'entre eux.

Dans le cadre du plan de recrutement (ou comme indiqué dans un document distinct), les exigences en matière de formation doivent être définies et planifiées, notamment la formation générale destinée à l'ensemble des membres de la PSIRT et les formations individuelles spécifiques à chaque rôle (par exemple, accueil/mentorat; formation continue, apprentissage et sensibilisation; formation spécifique pour le développement professionnel).

Voir la section *Service 6.1 Formation de la PSIRT* pour obtenir des informations connexes.

C. Ressources et outils

Identifier les ressources et outils complémentaires nécessaires et les acquérir.

Objectif
Identifier les ressources, l'équipement, et les outils nécessaires au fonctionnement de la PSIRT et les acquérir.

Résultat
Les besoins en matière d'outils et de ressources pour la PSIRT seront documentés et compris.

Parmi ces ressources et outils figurent:

les infrastructures, telles que les installations (bureaux);

- les outils/la technologie/l'équipement (matériel informatique, logiciels) (consulter, par exemple, la section *Service 3.3 Reproduction des vulnérabilités)*;
- le système/les méthodes de signalement des vulnérabilités (par exemple, site Internet, courriel, téléphone) (consulter la section *Service 2.1 Recueil des rapports de vulnérabilité*);

- une communication sécurisée (par exemple, logiciel de chiffrement PGP/chiffrement) (consulter la section *Fonction 1.5.2 Gestion de la communication sécurisée*);

une base de données/un système de suivi des vulnérabilités (à titre d'exemple, consulter les sections *Fonction 1.5.3 Mises à jour du système de suivi des failles de sécurité* et *Fonction 3.2.1 Base de données des découvreurs*)

III. Opérationnel

A. Politiques et procédures

Documenter les politiques, les processus et les procédures liés au déroulement des opérations de la PSIRT.

> ***Objectif***
> *Définir, décrire et documenter les politiques et les procédures qui sous-tendront les activités de la PSIRT.*
>
> ***Résultat***
> *La PSIRT disposera de politiques formelles décrivant son autorité et la gouvernance exercée/les opérations effectuées. La PSIRT disposera également de procédures/directives formellement documentées décrivant les modalités d'exercice de ses fonctions.*

La documentation des politiques et des procédures garantira une compréhension commune au sein de l'ensemble du personnel de la PSIRT, permettra la cohérence et la reproductibilité des produits et des services fournis par la PSIRT, et servira de support de formation pour les nouveaux membres de l'équipe.

B. Évaluation et amélioration

Définir les mesures nécessaires à l'évaluation de la performance et/ou de l'efficacité afin d'identifier de potentielles améliorations.

> ***Objectif***
> *Évaluer ou examiner le fonctionnement d'une PSIRT et identifier de potentielles améliorations.*
>
> ***Résultat***
> *La PSIRT sera capable d'évaluer ses performances et d'identifier les améliorations nécessaires.*

La PSIRT doit évaluer et examiner de façon continue et/ou régulière ses performances (à savoir la fourniture de ses produits et services) et identifier toute amélioration potentielle.

Les mesures et les méthodes d'évaluation peuvent être informelles (par exemple, collecte des retours d'information des parties prenantes) ou formelles, et peuvent être employées selon les besoins (par exemple, documentation des enseignements tirés [voir la section *Fonction 1.1.3 Procédure de réunion d'enquête après incident*]) ou d'après un calendrier prédéfini.

Les informations fournies dans le présent Cadre de services de la PSIRT peuvent constituer l'une des sources des critères ou capacités utilisés pour évaluer les opérations d'une PSIRT.

Zone de service 1

Légende de la figure:

Gestion de l'écosystème des parties prenantes	Gestion des parties prenantes internes Participation de la communauté des découvreurs Participation de la communauté et de l'organisation Gestion des parties prenantes en aval Coordination des communications relatives aux incidents au sein de l'organisation Reconnaissance et distinction des découvreurs Mesures relatives aux parties prenantes

La présente zone de service décrit les services et les fonctions que peut exercer une PSIRT afin de collaborer de façon appropriée avec les parties prenantes internes et externes. L'exécution des services dans ce cadre est maintenue tout au long du cycle de vie d'un incident ou du cycle de maturité de la PSIRT. Cette zone de service vise à garantir que l'ensemble des parties prenantes de la PSIRT sont correctement informées et engagées dans la procédure d'intervention.

Avant de fournir formellement ces services, la PSIRT doit identifier les parties prenantes spécifiques pertinentes pour ses activités. Parmi elles figurent l'équipe de direction, les équipes de développement internes, les fournisseurs de composants ou développeurs externes, voire même la clientèle de l'organisation. Il peut s'avérer extrêmement utile de compiler un registre des parties prenantes des produits/versions pour rationaliser le processus de communication. Avant de communiquer avec ces parties prenantes, il serait bénéfique de comprendre les points de vue, artefacts ou méthodes au moyen desquels elles souhaitent être sollicitées (portail Web, e-mail personnalisé, chat sur Internet, système de tickets, etc.) Aux fins du présent document, les parties prenantes sont réparties en plusieurs groupes (d'autres peuvent être déterminées en

fonction des circonstances spécifiques de votre activité): les découvreurs, les pairs/partenaires, les équipes internes, et les clients de vos produits.

Objectif
Mettre en évidence les processus et mécanismes de partage d'informations avec les différentes parties prenantes avec lesquelles une PSIRT peut et doit interagir.

Résultat
Un engagement réussi avec l'écosystème des parties prenantes des PSIRT garantira l'élaboration en temps voulu des rapports des vulnérabilités découvertes ainsi que la satisfaction des parties prenantes/partenaires lorsque les parties prenantes de l'organisation doivent être informées de l'existence de failles de sécurité.

Service 1.1 Gestion des parties prenantes internes

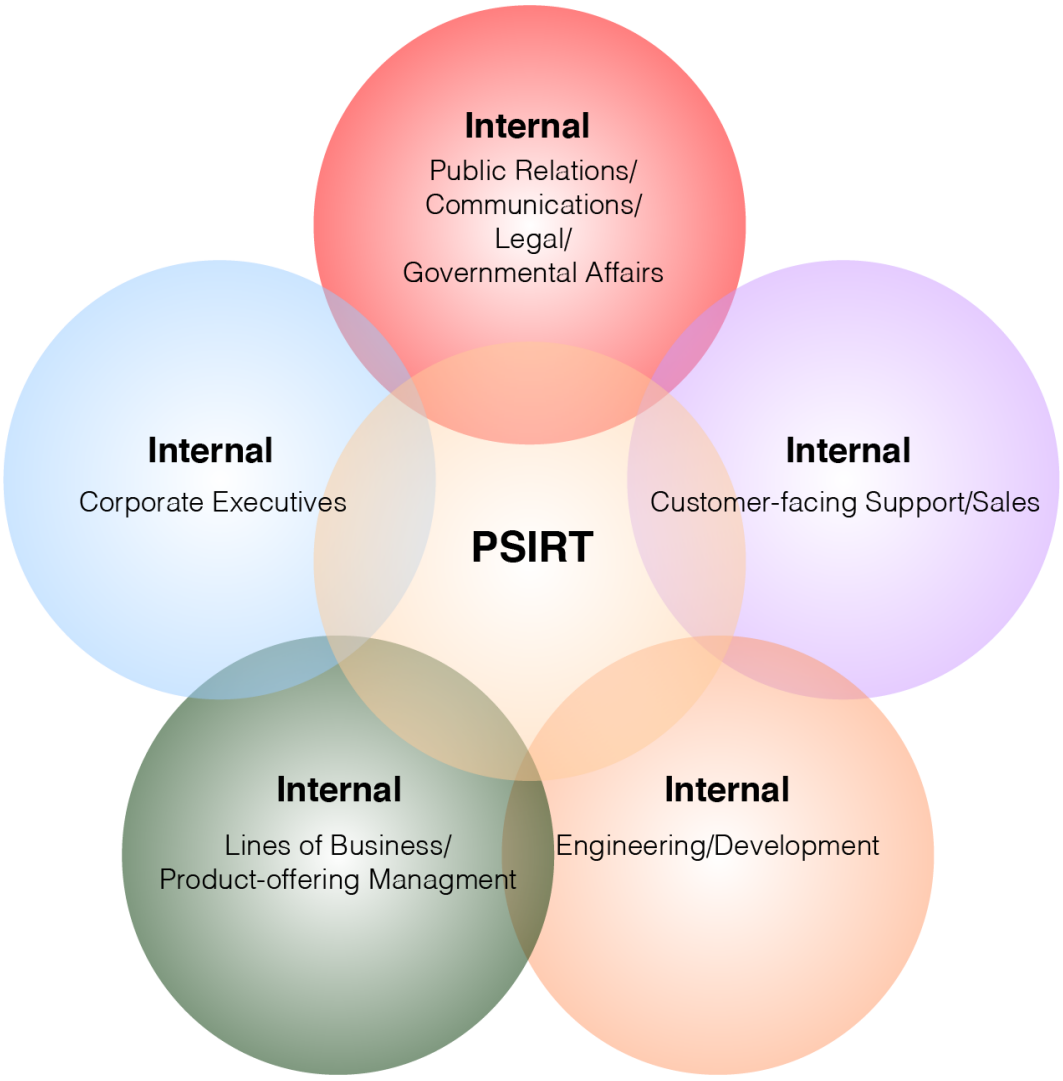


Figure 6: Gestion des parties prenantes internes

Légende de la Figure 6:

Interne
Relations publiques/
Communications/
Affaires juridiques/
gouvernementales

Interne
Cadres de l'organisation

Interne
Vente/Assistance des clients

PSIRT

Interne
Secteurs d'activité/
Gestion des offres de Produits

Interne
Ingénierie/Développement

Définir des processus relatifs à la collaboration avec les parties prenantes internes afin de garantir la transmission d'informations et l'offre d'assistance en cas d'incidents. Une coopération réussie avec les parties prenantes internes permettra d'améliorer les efforts de communication et d'intervention en indiquant clairement le rôle des PSIRT au sein de l'organisation et en établissant des liens internes entre les équipes de produit et les analystes de la sécurité.

Objectif
Établir l'autorité et l'expertise des PSIRT auprès des parties prenantes internes afin de faciliter la bonne coordination de la correction des vulnérabilités et de la sécurité des produits.

Résultat
Avec des parties prenantes internes fortement engagées, aucune difficulté ne devrait entraver les processus et l'obtention de résultats de la PSIRT. Par exemple, les défauts découverts par les salariés soulagent la pression immédiate exercée par les embargos externes ou l'attention des médias, permettant ainsi de traiter les problèmes selon un calendrier qui bénéficie à l'organisation, à ses clients ainsi qu'à la communauté dans son ensemble, et qui minimise le risque de divulgation publique de vulnérabilités non corrigées.

Fonction 1.1.1 Mobiliser les parties prenantes internes

Maintenir un dialogue actif avec les équipes internes prenant part à l'élaboration, à l'évaluation, au conditionnement et à la maintenance des offres de l'organisation. Les parties prenantes ne sont pas seulement des ressources d'ingénierie, elles peuvent également être des équipes d'évaluation/d'assurance qualité, d'ingénierie de version, d'assistance en contact direct avec les parties prenantes, de vente et marketing, ou d'autres experts dans des domaines techniques.

Objectif
Gagner de la visibilité sur les plates-formes de messagerie/d'information pour notifier les associés de l'existence des PSIRT et de leurs processus et fonctions.

Résultat
La PSIRT disposera d'une liste formellement documentée des parties prenantes internes et comprendra leurs rôles et responsabilités.

Sous-fonction 1.1.1.1 Mobiliser la direction et les cadres

Pour être efficace, une PSIRT doit comprendre son environnement organisationnel et être en mesure de réagir à celui-ci. La PSIRT tire profit à différents niveaux de sa coopération avec la direction et les cadres de l'organisation. Ainsi, le travail de la PSIRT au sein de l'organisation gagne en légitimité, notamment grâce au parrainage de la direction. De ce fait, la PSIRT peut transmettre des informations à la direction afin d'étayer la prise de décisions concernant l'entreprise. Enfin, une telle collaboration permet à la direction d'informer la PSIRT des changements de politique et d'orientation de l'organisation susceptibles d'altérer la mission de l'équipe.

Sous-fonction 1.1.1.2 Mobiliser les équipes affectées aux relations publiques et à la communication d'entreprise, ainsi que l'équipe juridique

Collaborer avec les équipes internes des services juridique et de communication permettra à la PSIRT de garantir sa conformité aux normes en vigueur relatives à la valorisation de la marque et à la communication de l'organisation, ainsi qu'à l'environnement réglementaire/légal auquel cette dernière doit se conformer (par exemple, confidentialité, espace fédéral). Chacune de ces parties prenantes internes ouvre des voies spécifiques permettant d'atteindre les parties prenantes essentielles de la PSIRT. En outre, il convient d'anticiper tout événement ou incident critique en installant des lignes de communication visant à coordonner efficacement le travail des différentes parties.

Sous-fonction 1.1.1.3 Mobiliser les secteurs d'activité

Coopérer avec les parties prenantes du domaine du développement permet de garantir la bonne documentation des problèmes, leur hiérarchisation adéquate ainsi que leur traitement approprié. Par exemple, les ingénieurs de la PSIRT ou les délégués autorisés doivent coordonner la correction des vulnérabilités avec les groupes d'ingénieurs de logiciels responsables du code défectueux. En cas d'incident, ces partenariats contribuent également à transmettre rapidement des informations et à résoudre tout problème de manière prompte et efficace. Les parties prenantes évoquées ici comprennent les chefs de programme ou de produit, les groupes de contrôle du SDL, les chefs de projets, les propriétaires de produit, et toute autre personne ayant des responsabilités liées à des activités similaires.

Sous-fonction 1.1.1.4 Mobiliser les équipes affectées au développement/à l'ingénierie

Les ingénieurs de la PSIRT doivent coordonner la correction des vulnérabilités avec les groupes d'ingénieurs de logiciels responsables du code défectueux. Coopérer avec les parties prenantes du domaine du développement permet de garantir la bonne documentation des problèmes, leur hiérarchisation adéquate ainsi que leur traitement approprié. En cas d'incident, ces partenariats contribuent également à transmettre rapidement des informations et à résoudre tout problème de manière prompte et efficace.

Sous-fonction 1.1.1.5 Mobiliser les équipes affectées à la vente et à l'assistance des clients en contact direct avec ces derniers

Les ingénieurs de la PSIRT doivent fournir des explications et des artefacts aux équipes affectées à l'assistance des parties prenantes de manière à pouvoir répondre aux requêtes et aux demandes d'assistance des parties prenantes à mesure que les problèmes évoluent et sont rendus publics. L'"assistance" pourrait comprendre le personnel de première ligne (à savoir le "centre de service"), les ressources d'assistance premium (par exemple, la gestion de comptes techniques, les gestionnaires de réussite des parties prenantes, etc.), les équipes de vente internes/externes, ou les ressources de terrain (conseil, ingénierie de ventes, etc.).

Sous-fonction 1.1.1.6 Participation du groupe de travail interne

Dans les organisations plus matures, les ingénieurs de la PSIRT peuvent nouer des relations avec les parties prenantes internes et les renforcer en participant à différents groupes de travail ou initiatives internes. Cela permet de réaffirmer/d'établir l'expertise technique de la PSIRT et de mettre en place des canaux de réseautage/communication pour les efforts à venir.

Fonction 1.1.2 Cycle de développement sécurisé interne

Le maintien et l'application d'un cycle de développement sécurisé sont le principal facteur contribuant à asseoir la confiance des parties prenantes dans les produits d'une organisation. Les parties prenantes peuvent ne plus accorder leur confiance aux produits de l'organisation si celle-ci n'est pas capable de prouver que les normes de sécurité seront appliquées tout au long du cycle de vie de ses produits. Les parties prenantes peuvent alors soumettre l'organisation à des exigences plus strictes (charge de la preuve, droit d'audit, etc.), ce qui l'expose à des pertes de revenus et entamer davantage la confiance des parties prenantes.

Objectif
Les organisations qui suivent de bonnes pratiques à l'égard du cycle de développement sécurisé mobiliseront moins de ressources afin de corriger les défauts de sécurité de leur produit en détectant ces erreurs plus tôt lors du développement des produits. Toutes les personnes impliquées dans ce cycle seront clairement informées des attentes en matière de fonctions et fonctionnalités de sécurité, ainsi que des exigences liées aux offres. Elles comprendront également leurs rôles et responsabilités au sein de ce cycle.

Résultat
La PSIRT disposera d'informations claires concernant la commercialisation d'un produit et pourra fournir des mesures et des données relatives aux performances de mise en œuvre. La PSIRT d'une organisation bien établie peut fournir des données ayant trait aux vulnérabilités courantes de ses produits emblématiques afin d'éviter de reproduire des erreurs similaires à l'avenir.

Sous-fonction 1.1.2.1 Participer aux activités du SDL

Le SDL est un processus de gouvernance qui aide une organisation à produire des offres stables et reproductibles conformes aux normes communes. La participation de la PSIRT aux processus de création et de maintenance du SDL de l'organisation permet de veiller au respect des pratiques et contrôles adéquats en matière de sécurité.

Sous-fonction 1.1.2.2 Participer à la gouvernance du SDL

Le SDL est un processus de gouvernance qui aide une organisation à produire des offres stables et reproductibles conformes aux normes communes. La participation de la PSIRT à la gouvernance et à l'application du SDL de l'organisation permet de veiller au respect des pratiques et contrôles adéquats en matière de sécurité. En outre, elle permet de garantir la bonne documentation des exceptions et leur examen approprié.

Fonction 1.1.3 Procédure de réunion d'enquête après incident

Suite à la découverte de vulnérabilités au sein de l'offre de l'organisation, la PSIRT exige de mettre en œuvre une procédure d'examen des problèmes, qu'ils soient liés au code, au processus ou au personnel afin d'en informer la hiérarchie et les parties prenantes concernées. Certaines failles de sécurité graves ou caractérisées par une forte exposition au public peuvent nécessiter une analyse plus approfondie de la réaction et de l'intervention de l'entreprise. Une réunion d'enquête après incident mobilise l'ensemble des parties prenantes internes ayant pris part aux efforts de correction et de communication, et vise à documenter les mesures efficaces, les mesures susceptibles d'être améliorées et les modifications nécessaires en vue de futures interventions.

Objectif
Fournir un compte rendu clair et factuel des événements qui surviennent lors d'une intervention en cas de vulnérabilité, mais aussi en cas d'incident relatif à la sécurité, en présentant les points de vue de toutes les parties/équipes impliquées. En cas de problème majeur, la PSIRT peut soutenir ou mener l'intervention de l'organisation visant à résoudre un problème connu du public et ayant de fortes répercussions.

Résultat
La PSIRT fournira des données relatives aux performances de l'organisation concernant son intervention face aux vulnérabilités logicielles. Ces données seront intégrées aux "enseignements tirés" en vue d'améliorations futures au cours des événements.

Sous-fonction 1.1.3.1 Établir un processus d'examen des failles de sécurité des produits

La mise en place d'un processus cohérent pour examiner les problèmes de façon rétrospective vise à garantir que les produits sont continuellement améliorés grâce aux enseignements tirés.

Sous-fonction 1.1.3.2 Examiner le délai des processus et publier des mises à jour

Identifier les forces et les faiblesses.

Sous-fonction 1.1.3.3 Examiner les incidents de premier plan

Coordonner les enseignements tirés, la réaction et l'examen des incidents de premier plan à l'échelle de l'organisation, et fournir des données relatives aux signalements à l'entreprise et à d'autres parties prenantes selon les besoins.

Service 1.2 Participation de la communauté des découvreurs

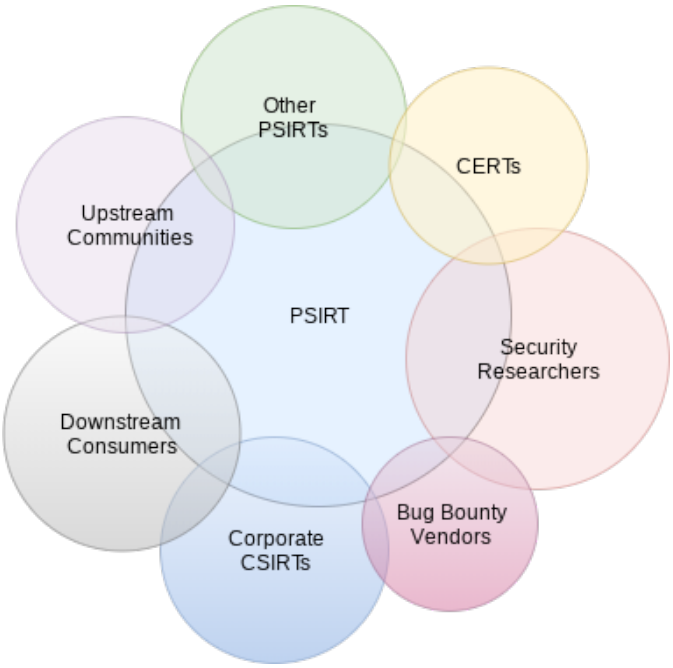


Figure 7: Exemples de parties prenantes externes pour la PSIRT

Légende de la Figure 7:

Autres PSIRT

Communautés en amont — CERT

Clients en aval — PSIRT — Découvreurs en matière de sécurité

CSIRT d'organisation — Fournisseurs de services de bug bounty

Services liés à la participation de la communauté des chercheurs en tant que partie prenante. Les découvreurs peuvent avoir un large éventail de rôles et des perspectives uniques – il peut s'agir d'universitaires, de professionnels du développement, de découvreurs professionnels en matière de sécurité ou d'amateurs. Les découvreurs peuvent effectuer des recherches sur les attaques ou les défauts théoriques dans l'optique d'une publication et d'une réussite universitaire, alors que d'autres peuvent être des découvreurs professionnels en matière de sécurité, motivés par des moyens financiers ou organisationnels. D'autres encore peuvent être des amateurs ou des passionnés prenant part à ces activités sur leur temps libre, peut-être afin d'être respectés et

reconnus au sein de leur communauté. La participation de la communauté de découvreurs est une approche proactive de l'intervention en cas d'incident relatif à la sécurité des produits.

Objectif
Faire de la PSIRT d'une organisation un contributeur actif de la communauté des chercheurs, et améliorer son appréciation des menaces susceptibles d'affecter la sécurité des produits d'une organisation. En cas de relations négatives ou antagonistes avec les découvreurs, l'organisation risque de ne plus disposer d'un accès rapide aux informations découlant des recherches, ce qui pourrait la désavantager dans la riposte aux failles de sécurité, et ainsi influer sur le sentiment des parties prenantes à l'égard de l'organisation.

Résultat
Une coopération efficace avec la communauté renforcera la réputation d'une organisation et sa position sur le marché dans le cadre de la promotion de la sécurité des produits. Par ailleurs, une collaboration positive avec les découvreurs peut garantir un accès rapide aux recherches et/ou aux divulgations de failles de sécurité, ce qui peut aider l'organisation à préparer sa réaction en vue d'une éventuelle communication publique.

Fonction 1.2.1 Mobiliser les découvreurs

Mettre en œuvre des activités visant à maintenir un dialogue actif avec les découvreurs disposant d'une expertise dans la sécurité des produits d'une entreprise et d'un accès à différents canaux. Les PSIRT peuvent conduire de nombreuses activités afin de renforcer leur coopération avec leurs communautés de découvreurs. Ces activités peuvent comprendre l'invitation de découvreurs hautement qualifiés à signer des contrats d'exclusivité, une collaboration lors de conférences et d'autres événements, voire le parrainage de recherches universitaires.

Objectif
Gagner de la visibilité sur les sites de médias sociaux. Surveiller les sites de médias sociaux et les sites courants/forums à la recherche d'indicateurs montrant que des découvreurs ou des parties prenantes ont potentiellement détecté un problème. Envisager une présence régulière aux conférences sur la sécurité permettant l'organisation de réunions en personne.

Résultat
La PSIRT recevra plus fréquemment et plus tôt des rapports de qualité de la part de découvreurs hautement impliqués, en raison des attentes de communication clairement définies.

Fonction 1.2.2 Collaborer avec d'autres PSIRT

Entretenir des relations enrichissantes avec des PSIRT homologues peut faciliter le partage d'informations et se traduire par une assistance mutuelle et/ou une coordination en cas d'incidents. La collaboration avec ces organisations paires peut contribuer à combler des manques de données essentielles pour remédier aux vulnérabilités, et soumet l'organisation à l'expertise des pairs, les deux groupes se consultant au sujet des problèmes. La PSIRT doit établir des canaux de communication (aussi bien normaux que sécurisés) avec des PSIRT homologues clés. La création et l'entretien de relations enrichissantes avec des pairs du secteur sont essentiels pour le partage d'informations et la coordination sur des problèmes affectant les deux organisations.

Objectif

Établir des canaux de communication entre votre organisation et d'autres PSIRT afin de partager des informations sur les vulnérabilités, des renseignements sur les menaces et des bonnes pratiques.

Résultat

Constituer une communauté de PSIRT homologues peut s'avérer utile pour répondre aux vulnérabilités liées à la chaîne d'approvisionnement de logiciels. Il est possible d'en attendre une rapidité d'intervention accrue.

Sous-fonction 1.2.2.1 Identifier et recenser les PSIRT homologues

Collecter les informations de contact et les processus de participation en vue de leur utilisation ultérieure. La PSIRT doit coopérer et interagir avec la communauté élargie des PSIRT afin de partager des bonnes pratiques et des idées relatives aux enseignements tirés. La résolution des vulnérabilités mises en évidence est généralement le résultat de la collaboration de plusieurs groupes. Cela permet à la PSIRT d'étendre ses capacités internes en tirant parti de ses homologues externes, auprès desquels elle obtient des informations et/ou de l'aide.

Sous-fonction 1.2.2.2 Définir un processus de divulgation coordonné

Les PSIRT doivent soigneusement recenser les paramètres et les accords de partage des informations relatives aux vulnérabilités. La PSIRT doit honorer les paramètres d'embargo fixés par le découvreur de la vulnérabilité et/ou l'organisation à l'origine du signalement (tout en espérant que les siens soient également honorés).

Sous-fonction 1.2.2.3 Établir un processus de partage des informations relatives à la sécurité

La PSIRT doit établir des méthodes de partage des informations relatives aux vulnérabilités et d'autres renseignements confidentiels de façon sécurisée avec les parties visées par l'accord de divulgation coordonnée. Ces options peuvent comprendre la communication hors bande ou non électronique, les courriels/portails chiffrés ou les listes de diffusion privées.

Sous-fonction 1.2.2.4 Prendre part à des Groupes d'intérêt (SIG) et à des Groupes de travail du secteur

Coopérer avec les pairs sur des sujets présentant un intérêt pour le secteur permet de renforcer et d'entretenir les liens tout en contribuant à la professionnalisation du secteur grâce à la résolution collaborative des problèmes.

Fonction 1.2.3 Collaborer avec les coordonnateurs (CSIRT et autres organisations de centres de coordination)

La collaboration avec les CSIRT gouvernementales contribue à instaurer un climat de confiance propice au partage d'informations et aide la PSIRT à gagner la confiance et le respect d'importantes équipes homologues. Parmi les autres organisations partageant des

intérêts ou disposant de communautés pertinentes figurent notamment: FIRST, MITRE, Advancing Open Standards for the Information Society (OASIS), Industry Consortium for Advancement of Security on the Internet (ICASI), l'Organisation internationale de normalisation (ISO). Les groupes participants peuvent être considérés en fonction du secteur national, commercial, régional ou industriel.

Objectif
Les organisations sont des cibles fréquentes des auteurs de menaces qui utilisent souvent des vulnérabilités encore inconnues pour pénétrer les réseaux. Nouer des relations avec les CSIRT permet de gagner la confiance et les contacts nécessaires pour potentiellement obtenir des rapports de vulnérabilité aux premiers stades.

Résultat
De bonnes relations avec les CSIRT et d'autres organisations de centre de coordination sont utiles pour être informé très tôt des vulnérabilités. Il est possible d'en attendre une rapidité d'intervention accrue.

Sous-fonction 1.2.3.1 Mobiliser les communautés et les partenaires

La PSIRT doit rechercher dans quels cadres les groupes externes souhaités engagent un dialogue et s'efforcer de participer à ces forums.

Fonction 1.2.4 Collaborer avec les chercheurs du domaine de la sécurité

L'éventail des chercheurs du domaine de la sécurité est vaste: des universitaires, des amateurs, et des professionnels de la sécurité, pour n'en citer que quelques-uns. Ces personnes sont les principaux découvreurs de vulnérabilités au sein du secteur. Les chercheurs essaieront de contacter le propriétaire d'un produit, mais, pour différentes raisons, ils n'atteindront pas toujours la partie appropriée. Les PSIRT recevront de façon passive des rapports de ces individus ou groupes et seront contraintes de travailler dans des délais contrôlés de l'extérieur. Il est dans le meilleur intérêt de la PSIRT d'adopter une approche proactive avec les chercheurs du domaine de la sécurité impliqués dans l'étude des domaines qui affectent les produits de la PSIRT et de collaborer de façon positive avec ces groupes afin disposer d'un meilleur aperçu des problèmes découverts.

Sous-fonction 1.2.4.1 Collaborer avec les fournisseurs de systèmes de sécurité

Les principaux fournisseurs commerciaux de systèmes de sécurité collaborent avec les parties prenantes lors des atteintes à la sécurité et disposent souvent de données judiciaires auxquelles la PSIRT n'a normalement pas accès. Nouer de bonnes relations avec ces fournisseurs permet d'instaurer un climat de confiance et un respect mutuel, et peut idéalement aider la PSIRT à avoir accès aux données essentielles relatives aux menaces auxquelles elle n'aurait pas pu avoir accès autrement.

Sous-fonction 1.2.4.2 Recenser les fournisseurs de systèmes de sécurité pertinents

Le fait de connaître des fournisseurs de systèmes de sécurité et de collaborer adéquatement avec eux peut accélérer les communications et les efforts relatifs au signalement/à la correction des vulnérabilités alors qu'ils rapportent les problèmes à la

PSIRT. Il convient d'identifier les informations auxquelles ces fournisseurs auront accès et les informations qu'ils pourront conserver. Le lien entre l'organisation et le fournisseur de services de bug bounty doit être soigneusement documenté et examiné avant de nouer une relation, de sorte que toutes les parties concernées soient informées du comportement qu'elles doivent adopter, des ressources auxquelles elles peuvent avoir accès, de la façon dont les données sont partagées et des personnes avec lesquelles elles sont partagées.

Sous-fonction 1.2.4.3 Recenser les méthodes de collaboration avec les fournisseurs de systèmes de sécurité

La PSIRT doit rechercher dans quels cadres les groupes externes souhaités engagent un dialogue et s'efforcer de participer à ces forums.

Fonction 1.2.5 Collaborer avec les fournisseurs de services de bug bounty

Nouer une relation avec des fournisseurs de services de bug bounty en vue d'améliorer les efforts de communication et de partage de données en matière de gestion des vulnérabilités.

Objectif
Si votre organisation reçoit fréquemment des rapports de vulnérabilité de la part de fournisseurs/courtiers rémunérant des découvreurs de bogues, envisager de maintenir une relation directe avec ces organisations, qui établissent souvent des accords sur le niveau de service pour le traitement des vulnérabilités.

Résultat
Une relation directe avec des fournisseurs de services de bug bounty peut permettre de nouer un dialogue constructif en vue de communiquer le processus de publication d'un correctif de sécurité d'un produit. Outre la conclusion d'accords sur le niveau de service acceptables, ces relations contribueront à réduire les risques de nouvelles vulnérabilités, dans l'intérêt commun de toutes les parties prenantes.

Sous-fonction 1.2.5.1 Identifier et recenser les programmes de bug bounty pertinents

Identifier et recenser les fournisseurs de services de bug bounty pouvant s'appliquer aux produits de l'organisation.

Sous-fonction 1.2.5.2 Mobiliser les fournisseurs de services de bug bounty

Identifier les canaux de communication permettant d'engager un dialogue actif avec ces fournisseurs de services de bug bounty.

Fonction 1.2.6 Anticiper les besoins des CSIRT

Les CSIRT sont une catégorie spéciale de parties prenantes "en aval" qui s'intéressent essentiellement aux problèmes de sécurité. Bien qu'il soit généralement possible d'interagir avec ces groupes grâce aux pratiques courantes de mobilisation des parties prenantes et de gestion de la clientèle, la PSIRT doit comprendre les exigences et le point de vue uniques de

ces groupes axés sur la sécurité, qui la contacteront et exploiteront ses informations. Cela comprend les formats et délais de divulgation (voir la section *Service 5.3 Divulgation*), ainsi que les canaux de communication pour des demandes spécifiques.

Service 1.3 Participation de la communauté et de l'organisation

Deux groupes de parties prenantes avec lesquelles les PSIRT interagiront méritent une attention particulière. Parfois désignée comme "en amont" ou "en aval", la participation de la communauté est essentielle pour encourager les efforts conjoints de correction ou soutenir une assistance mutuelle avec d'autres acteurs au sein des groupes homologues de l'organisation. L'expression "en amont" est utilisée pour désigner les groupes ou individus fournissant les composants ou les projets nécessaires aux produits d'une organisation. L'expression "en aval" désigne les individus, les groupes ou les organisations qui intègrent les produits mis au point par votre organisation à leur offre. La participation en aval est couverte dans la section *Service 1.4 Gestion des parties prenantes en aval.*

Une communauté dynamique en amont peut contribuer à alimenter les flux de produits en innovations et à alléger le fardeau des mesures correctives complexes liées aux vulnérabilités. En outre, elle peut pallier le manque d'expertise en la matière au sein de l'organisation. De même, le maintien de relations professionnelles avec les individus et les équipes d'autres organisations peut contribuer à étendre les capacités de la PSIRT en permettant un accès à des perspectives, à de l'expertise, et à des connaissances historiques externes. Cet objectif peut être atteint en mobilisant de façon proactive les professionnels de la sécurité en tant que partie prenante, et en nouant des relations avec des partenaires et des PSIRT homologues.

Objectif
La PSIRT doit mettre au point et maintenir un écosystème actif de partenaires et d'homologues. Ces associations de communautés peuvent contribuer à la création d'une approche plurielle pour détecter et résoudre les failles, ainsi que partager les bonnes pratiques entre différents groupes afin d'améliorer l'expérience générale en matière de correction des vulnérabilités.

Résultat
De bonnes relations et un écosystème actif de partenaires et d'homologues faciliteront le partage de bonnes pratiques et d'informations sur les menaces. Une PSIRT bénéficiant d'une bonne réputation parmi les professionnels de la sécurité peut aider à attirer des ressources et des collaborateurs pour le traitement de situations critiques.

Fonction 1.3.1 Identifier et collaborer avec les communautés et partenaires en amont

Les produits comprennent généralement du code ou des composants qui n'ont pas été créés par l'organisation. Les créateurs de ces éléments sont parfois appelés tiers, fournisseurs, fournisseurs en amont, fabricants d'équipement d'origine (OEM) ou simplement partenaires. Il est utile d'identifier ces partenaires au sein de votre écosystème et de déterminer comment l'organisation les contactera et les mobilisera lorsque des vulnérabilités seront découvertes dans le code d'un tiers.

Objectif

Nouer des relations de travail cordiales avec les personnes ou les groupes qui vous fournissent des composants ou avec les groupes auxquels vous fournissez des composants. Connaître les modalités de contact de ces groupes afin de maintenir la PSIRT informée de problèmes imminents, et connaître les points de contact de ces groupes afin de les tenir informés lorsque la PSIRT découvre qu'ils fournissent des composants affectés par un problème.

Résultat

La PSIRT comprendra mieux d'où proviennent les composants et qui les fournit. Cela devrait garantir un accès plus rapide aux informations et aux correctifs lorsque des défauts sont découverts dans ces composants.

Sous-fonction 1.3.1.1 Identifier et recenser les communautés et les partenaires en amont

Les communautés et les partenaires en amont fournissent le code et/ou les connaissances et l'expertise qui sont intégrés à l'offre de l'organisation. Il est essentiel de connaître ces fournisseurs et de collaborer avec eux pour garantir des interactions rapides et efficaces à mesure que des failles de sécurité sont signalées à la PSIRT et sont traitées avec son concours. Idéalement, ces relations sont documentées dans des contrats, et couvertes par des accords de non-divulgation et d'autres protections pour l'organisation.

Sous-fonction 1.3.1.2 Mobiliser les communautés et les partenaires

Chaque communauté ou partenaire en amont peut avoir différents outils ou méthodes qu'il utilise pour développer ses logiciels/son offre et communiquer à leur sujet. La PSIRT doit comprendre comment coopérer avec ces groupes externes et veiller à ce qu'ils disposent des contacts/méthodes appropriés pour collaborer sur les problèmes de sécurité les impliquant.

Sous-fonction 1.3.1.3 Collaborer avec les communautés en amont

Collaborer avec les communautés et les partenaires en amont permet d'instaurer un climat de confiance précieux entre les différents groupes, tout en contribuant au renforcement des capacités de cette équipe externe avec l'expertise dont dispose l'organisation.

Sous-fonction 1.3.1.4 Prendre part à des événements de la communauté et du secteur

Les conférences et les réunions professionnelles de l'organisation sont d'excellents endroits pour permettre aux PSIRT d'interagir avec les parties prenantes et les partenaires. Elles permettent à l'organisation de recevoir des retours directs ainsi que de gagner une bonne réputation au sein de la communauté externe et l'estime de cette dernière, laquelle pourra être mise à profit en vue d'une future coordination/collaboration.

Sous-fonction 1.3.1.5 Mobiliser les équipes de sécurité de la communauté

Il est essentiel que la PSIRT connaisse les modalités de contact et les points de contact des équipes de sécurité des fournisseurs de logiciels/matériel informatique/services en amont (PSIRT, CSIRT, ingénieurs en sécurité). L'établissement de voies de communication et la transmission de rapports entre la PSIRT et ces groupes permettent de garantir des interactions harmonieuses en temps de crise ou lors de la correction de vulnérabilités.

Fonction 1.3.2 Identifier et collaborer avec les communautés et les partenaires en aval

Bien que l'expression "en aval" soit connotée, elle ne signifie pas que la PSIRT doit ignorer ces groupes de parties prenantes essentiels. L'expression "en aval" désigne tout produit, toute organisation, ou tout individu qui bénéficie des produits et de l'offre de l'entreprise dont relève la PSIRT et qui les utilise à ses propres fins. Il s'agit, le plus souvent, des clients ou des consommateurs des biens et des services proposés. Souvent, une autre entreprise peut utiliser les produits de l'organisation dont relève la PSIRT ou acquérir des licences relatives à ces produits, et revendre ces derniers dans le cadre de son offre. Par ailleurs, dans le cas de logiciels à source ouverte, souvent concernés par cette situation, un groupe fournit les logiciels et se charge de leur maintenance, tandis qu'un vaste groupe de parties auxiliaires exploite ces ressources; ces parties se situent en aval.

Sous-fonction 1.3.2.1 Identifier et recenser les communautés, les consommateurs et les partenaires en aval

Les communautés et les partenaires en amont exploitent le code et/ou les connaissances et l'expertise qui sont intégrés à l'offre de l'organisation. Idéalement, ces relations sont documentées dans des contrats, et couvertes par des accords de non-divulgation et d'autres protections pour l'organisation.

Sous-fonction 1.3.2.2 Mobiliser les communautés en aval

Chaque communauté ou partenaire en aval peut avoir différents outils ou méthodes qu'il utilise pour développer ses logiciels/son offre et communiquer à leur sujet. La PSIRT doit comprendre comment coopérer avec ces groupes externes et veiller à ce qu'ils disposent des contacts/méthodes appropriés pour collaborer sur les problèmes de sécurité impliquant ces parties externes.

Service 1.4 Gestion des parties prenantes en aval

Afin de mobiliser votre base de parties prenantes, la PSIRT doit mettre au point des processus et des méthodes d'interaction avec la communauté des parties prenantes concernant les interventions pour la sécurité des produits. Les parties prenantes des produits de l'organisation figurent parmi les acteurs dont il convient impérativement de maintenir la satisfaction, étant donné qu'elles représentent les perspectives de recettes actuelles et futures de l'organisation.

Objectif
La PSIRT doit mettre au point et maintenir des canaux de communication avec la base de parties prenantes de l'organisation afin d'assurer la circulation des informations relatives aux failles de sécurité des produits ou lors des événements d'intervention en cas d'incident.

Résultat
En entretenant de bonnes relations avec vos parties prenantes, vous assurerez (ou dans certains cas, augmenterez) vos recettes, mais vous leur donnerez également la possibilité de s'exprimer sur votre produit, ce qui favorisera un sentiment d'implication et de participation à la solution.

Fonction 1.4.1 Collaborer avec les parties prenantes en aval

Les parties prenantes de vos produits et services doivent disposer de canaux de communication pour qu'elles puissent partager des informations et leurs opinions, et obtenir une assistance quant aux modalités de gestion des failles de sécurité par l'organisation. Collaborer de manière proactive avec les parties prenantes de l'organisation contribue à donner une expérience positive de la marque et à maintenir/renforcer la fidélité des parties prenantes.

Objectif
Fournir des méthodes pour que les parties prenantes en aval de l'organisation puissent communiquer avec la PSIRT et bénéficier d'une assistance sur les questions de sécurité. Ne pas réagir de façon appropriée aux demandes ou requêtes des parties prenantes pourrait affecter négativement la marque en raison des commentaires publics négatifs, de la perte de renouvellements ou de la perte de nouvelles activités.

Résultat
Les parties prenantes en aval doivent recevoir des orientations claires et rapides concernant les failles de sécurité. Cela permettra de renforcer les niveaux de confiance à l'égard du produit et contribuera à accroître la fidélité vis-à-vis de la marque. S'appuyer sur la PSIRT pour créer une expérience positive dans son ensemble et établir l'expérience de cette dernière auprès des parties prenantes. De manière générale, améliorer l'opinion des parties prenantes envers l'ensemble de la marque.

Sous-fonction 1.4.1.1 Fournir des politiques claires concernant le cycle de vie des produits et l'assistance

L'organisation doit indiquer précisément et publiquement quelles doivent être les attentes des parties prenantes à l'égard de la correction des failles de sécurité et de la durée de prise en charge de ses produits. Pour plus d'informations, se reporter à la section *Zone de service 4.*

Sous-fonction 1.4.1.2 Participation des parties prenantes

Les parties prenantes des produits et services de l'organisation auront des questions, auront besoin d'aide, ou nécessiteront la correction de failles de sécurité signalées. La PSIRT doit répondre activement aux demandes des parties prenantes, prodiguer des conseils clairs et précis sur les failles de sécurité et proposer des mesures d'atténuation des risques jusqu'à ce que le correctif soit fourni aux parties prenantes.

Service 1.5 Coordination des communications relatives aux incidents au sein de l'organisation

Les incidents de sécurité affectent de nombreux groupes internes et, potentiellement, les produits de l'organisation. Les PSIRT sont au cœur de la coordination des efforts de correction des vulnérabilités et servent également de centre de partage des informations relatives à un événement avec les parties prenantes internes autorisées.

Objectif
Veiller à ce que toutes les parties au sein d'une entreprise soient informées de l'état d'une intervention visant à remédier à une faille de sécurité afin de pouvoir prendre des décisions éclairées quant aux prochaines mesures à appliquer. La communication peut prendre de nombreuses formes (courriel, courrier traditionnel, flux RSS, médias sociaux, etc.), mais, à terme, tous les canaux fournissent des informations claires, opportunes et précises concernant les failles de sécurité et les incidents intéressant les parties prenantes.

Résultat
Les parties prenantes internes seront tenues au courant de la portée et de l'impact des menaces envers l'offre de l'organisation. Les parties prenantes doivent être tenues informées, de manière à ce qu'elles puissent prendre des mesures pertinentes, à mesure que la faille de sécurité est corrigée et que des mesures d'atténuation sont mises en place.

Fonction 1.5.1 Fournir des canaux/outils de communication externes

Pour collaborer efficacement avec les parties prenantes, la PSIRT doit fournir plusieurs canaux de communication. Les différentes parties prenantes pourront préférer certains outils à d'autres. Les PSIRT doivent élaborer et publier leurs messages à l'intention d'un public ciblé. La PSIRT doit également être équipée de façon à pouvoir recevoir des rapports relatifs à la sécurité, des commentaires et des questions provenant de sources variées.

Objectif
Fournir des méthodes aux parties prenantes pour faciliter la communication avec la PSIRT.

Résultat
Ces canaux (courrier électronique, chat, formulaire web, etc.) permettent aux $parties prenantes internes de communiquer et de partager des informations avec la PSIRT.

Sous-fonction 1.5.1.1 Fournir des canaux de communication clairs

Les parties prenantes doivent disposer de canaux par lesquels soumettre leurs questions, vérifier le statut des failles de sécurité et signaler les problèmes à la PSIRT. Si une partie prenante est affectée par une faille de sécurité ou en découvre une, elle doit pouvoir établir facilement un rapport et l'envoyer à la PSIRT.

Sous-fonction 1.5.1.1.2 Fournir des canaux de communication internes

Pour assurer la participation des parties prenantes internes, les PSIRT doivent mettre à disposition des canaux de communication afin d'informer sur l'état de résolution des vulnérabilités. Les parties prenantes internes doivent pouvoir contacter facilement la PSIRT et savoir ce qu'elles peuvent attendre de leurs demandes.

Sous-fonction 1.5.1.1.3 Fournir des canaux de communication externes

Pour assurer la participation des parties prenantes externes, les PSIRT doivent mettre à disposition des canaux de communication afin d'informer sur l'état de résolution des vulnérabilités. Il s'agirait notamment de vérifier/qualifier les activités de communication externe afin de s'assurer de leur validité et de leur acheminement adéquat vers les associés internes.

Fonction 1.5.2 Gestion de la communication sécurisée

Bien souvent, la PSIRT doit gérer des informations considérées comme confidentielles (à savoir des problèmes placés sous embargo). La PSIRT doit être en mesure de communiquer en toute sécurité et confidentialité avec les découvreurs, d'autres organisations, ou diverses ressources internes. Le respect des accords de divulgation et la communication par le seul biais de méthodes privées permettent de gagner la confiance des découvreurs. La protection des informations confidentielles ayant trait aux vulnérabilités vis-à-vis des parties non autorisées contribue également à garantir un traitement adéquat et efficace du problème, conformément aux conditions de l'embargo. Par ailleurs, les canaux sécurisés peuvent contribuer à protéger l'identité des découvreurs qui souhaitent conserver leur anonymat. Il convient d'établir une politique de conservation des données afin de veiller à ce qu'elles soient correctement supprimées dès lors qu'elles ne sont plus utilisées.

Objectif
Offrir aux parties la possibilité d'échanger en toute confidentialité des informations sur les failles de sécurité. Ces canaux protègent le caractère confidentiel de la faille de sécurité et du découvreur jusqu'à ce qu'ils puissent être rendus publics.

Résultat
Les parties aidant à la résolution des problèmes de sécurité peuvent partager des informations de façon confidentielle avec d'autres personnes qui ont besoin d'être informées d'un problème. Les découvreurs sont plus à même de transmettre de nouveaux rapports à l'organisation s'ils ont le sentiment que leurs préoccupations sont prises en compte par cette dernière.

Sous-fonction 1.5.2.1 Fournir des canaux de communication sécurisés

La PSIRT doit veiller à ce que les découvreurs de vulnérabilités et les partenaires travaillant sur les failles affectant l'offre de l'organisation disposent de méthodes privées et sécurisées de partage des informations.

Fonction 1.5.3 Mises à jour du système de suivi des failles de sécurité

La PSIRT doit avoir accès au(x) système(s) de compilation de tous les défauts des produits et être en mesure de créer et d'utiliser un système de suivi et de partage d'informations ayant trait aux failles de sécurité.

Objectif
Le recensement et le suivi appropriés des failles de sécurité permettent à l'organisation de préciser le moment et l'endroit où les vulnérabilités ont été traitées. Ce système de suivi des failles permet également à la PSIRT, aux découvreurs et aux ingénieurs travaillant activement à la résolution du problème de communiquer ensemble.

Résultat: *En utilisant un système conçu pour le suivi adéquat des failles de sécurité, toutes les parties ayant besoin d'accéder aux informations relatives à une faille peuvent examiner l'historique, les progrès et les commentaires y afférents.*

Sous-fonction 1.5.3.1 Assurer le suivi des failles de sécurité des produits

Les failles de sécurité doivent faire l'objet d'un suivi, et ces systèmes doivent être accessibles (au titre du principe de moindre privilège). Par ailleurs, les parties internes et externes (le cas échéant) doivent être en mesure d'actualiser la procédure et de suivre les progrès effectués. Les découvreurs externes doivent être adéquatement informés du statut des rapports transmis à la PSIRT.

Sous-fonction 1.5.3.2 Créer et publier une procédure de suivi des failles de sécurité

La PSIRT doit veiller à ce que les découvreurs de vulnérabilités et les partenaires travaillant sur les failles affectant l'offre de l'organisation disposent de méthodes privées et sécurisées de partage des informations.

Fonction 1.5.4 Partage et publication d'informations

Une fois qu'un problème a été traité, la PSIRT doit mettre à disposition les informations relatives à la nature de cette faille de sécurité, en utilisant un système d'évaluation des vulnérabilités courantes comme facteur, à sa gravité et à ses impacts, aux risques potentiels susceptibles d'être exploités, et à la façon de résoudre le problème ou de l'atténuer. L'une des manières les plus fréquentes de rendre publiques les informations relatives à une vulnérabilité et de les diffuser à grande échelle consiste à intégrer la vulnérabilité à la liste des vulnérabilités et expositions courantes (CVE). Le référencement du problème est ainsi garanti, un numéro d'identification, une description et au moins une référence publique uniques lui étant attribués.

Objectif
Partager les détails relatifs aux failles de sécurité qui ont été signalées et résolues. Il convient de fournir des mesures de traitement ou d'atténuation alternatives afin de contenir le risque identifié par les parties prenantes jusqu'à ce des correctifs formels puissent être appliqués.

Résultat
Les parties prenantes seront informées des problèmes de sécurité, de leurs conséquences potentielles, et des modalités de leur résolution. Les parties prenantes qui reçoivent des informations et des mises à jour à temps sont plus susceptibles de percevoir l'organisation de façon positive et, soit de poursuivre avec son offre ou de recourir plus largement à l'organisation.

Sous-fonction 1.5.4.1 Fournir de multiples outils de communication

Les différentes parties prenantes privilégieront des méthodes d'interaction/de communication différentes à mesure que les vulnérabilités sont rendues publiques. La PSIRT ne doit pas se limiter aux mises à jour consultatives traditionnelles et veiller à employer d'autres méthodes pour garantir une sensibilisation et un engagement optimaux des parties prenantes à l'égard de la vulnérabilité. Une fois les vulnérabilités corrigées, la PSIRT doit employer différentes méthodes pour communiquer sur le correctif.

Sous-fonction 1.5.4.2 Fournir des retours d'informations aux parties prenantes

Les retours d'informations permettent d'améliorer les nouveaux processus et interventions. Ils peuvent mettre en lumière les domaines dans lesquels la PSIRT excelle et devrait poursuivre ses efforts, et ceux dans lesquels la PSIRT doit évoluer et s'améliorer.

Service 1.6 Reconnaissance et distinction des découvreurs

La reconnaissance des découvreurs aide à asseoir leur crédibilité et celle de leur organisation (le cas échéant) au sein de la communauté, tout en les remerciant de leur collaboration avec la PSIRT.

Objectif
Les efforts déployés par les découvreurs afin de coordonner la divulgation des vulnérabilités affectant un produit sont reconnus. Ils peuvent ainsi bâtir leur réputation à partir de ces distinctions, alimenter leur portefeuille d'expertise et prouver leur valeur à l'organisation.

Résultat
Une collaboration positive avec les découvreurs permettra d'améliorer la sécurité des produits. La reconnaissance des découvreurs aide les salariés internes à bâtir leur réputation et à démontrer leur expertise.

Fonction 1.6.1 Distinguer

La reconnaissance de la ou des personnes responsables de la découverte d'une faille de sécurité est un élément vital au sein du flux de travail relatif aux failles de sécurité. Même une simple expression de gratitude peut contribuer à instaurer un climat de confiance et de respect au sein de la communauté et montre que l'organisation est attentive aux problèmes de sécurité.

Objectif
Les efforts déployés par les découvreurs afin de divulguer de façon responsable la vulnérabilité d'un produit sont reconnus. Ils peuvent ainsi bâtir leur réputation à partir de ces distinctions et alimenter leur portefeuille d'expertise.

Résultat
Une collaboration positive avec les découvreurs permettra d'améliorer la sécurité des produits. La reconnaissance des découvreurs les aide à bâtir leur réputation et les encourage à transmettre de nouveaux rapports de vulnérabilité à la PSIRT.

Sous-fonction 1.6.1.1 Distinguer

La reconnaissance écrite des efforts d'un découvreur et de son implication dans la découverte d'une faille de sécurité est le seul outil à la fois efficace et économique dont dispose la PSIRT pour récompenser ces individus. Il est de coutume d'inclure les remerciements à l'égard du ou des découvreurs dans les bulletins de sécurité, les notes de version des logiciels et le texte de la CVE. La PSIRT doit comprendre les modalités d'attribution interne des vulnérabilités découvertes.

Fonction 1.6.2 Récompenser les découvreurs

Afin de générer des résultats positifs et d'encourager le partage accru des recherches, la PSIRT peut choisir d'élaborer un programme visant à récompenser ou encourager cette collaboration dans l'espoir qu'elle se poursuive et s'étende à l'avenir.

Objectif
Récompenser la ou les personnes qui signalent des failles de sécurité dans les produits et services de l'organisation. Les récompenses peuvent prendre de nombreuses formes: des notes de remerciement au format électronique ou physique, des cadeaux à l'image de l'entreprise, des dons monétaires, ou d'autres biens/incitations. La PSIRT doit garantir la transparence des récompenses octroyées et des règles les entourant.

Résultat
Cette pratique vise à générer de la bonne volonté envers l'organisation dont relève la PSIRT et à encourager la poursuite de la collaboration à l'avenir à l'égard des problèmes liés à la sécurité.

Sous-fonction 1.6.2.1 Créer un programme de récompenses à l'intention des découvreurs

La PSIRT peut soutenir un programme de récompenses visant à encourager les comportements positifs parmi les découvreurs de failles de sécurité. Les récompenses peuvent consister en des dons monétaires, des cadeaux à l'image de l'entreprise ou de nombreux autres éléments qui pourront avoir de la valeur aux yeux du découvreur, au-delà de la reconnaissance de leur rôle dans la découverte du problème.

Sous-fonction 1.6.2.2 Lancer un bug bounty rémunéré

La récompense peut prendre la forme d'une compensation monétaire. Certaines organisations rémunèrent les découvreurs qui leur transmettent des informations sur des vulnérabilités.

Sous-fonction 1.6.2.3 Créer un "Tableau de points"

Le "Tableau de points" est une autre forme de compensation. Elle apporte un aspect ludique aux activités de détection et de signalement des failles de sécurité, et encourage une compétition amicale en promouvant des "leaders" et en établissant des classements dont pourront se prévaloir les découvreurs.

Service 1.7 Mesures relatives aux parties prenantes

Fournir des renseignements concernant les effectifs de la PSIRT, ses performances, ou d'autres mesures est essentiel pour maintenir les parties prenantes informées de l'efficacité de la PSIRT. Les différentes parties prenantes auront des points de vue uniques qui doivent être traités avec des artefacts (ou points de vue) aux formats potentiellement différents. La PSIRT doit comprendre comment chaque groupe de parties prenantes souhaite utiliser ces informations. Ces mesures pourraient constituer des indicateurs clés de performance (KPI) pour la PSIRT. La *Fonction 2.5.1* porte sur les rapports opérationnels et la façon dont la PSIRT doit envisager de les transmettre afin de garantir la bonne exécution des opérations. La *Fonction 2.5.2*, quant à elle, examine les rapports d'activité que la PSIRT peut envisager de fournir aux parties prenantes.

Objectif
Fournir des données relatives aux mesures et performances de la PSIRT. Ainsi, les parties prenantes peuvent comprendre l'efficacité des prestations de la PSIRT dans un domaine ou un service particulier.

Résultat
En examinant les mesures de la PSIRT, les parties prenantes doivent comprendre l'efficacité avec laquelle une PSIRT fournit un service et être capables de transmettre des retours d'informations pour apporter des ajustements à cette prestation de services.

Fonction 1.7.1 Comprendre les exigences des parties prenantes en matière d'artefacts

Pour déterminer efficacement la façon dont une PSIRT fournit des services, il convient en premier lieu de comprendre les points de vue spécifiques à chaque groupe de parties prenantes. Certaines parties prenantes peuvent être préoccupées par les délais de conception des correctifs de sécurité, tandis que d'autres peuvent être sensibles au coût de l'intervention de la PSIRT. Chaque point de vue est pertinent et exige des artefacts différents pour communiquer efficacement les informations souhaitées. Chaque groupe de parties prenantes doit être interrogé afin d'identifier les aspects de la PSIRT à propos desquels ils ont besoin de données, ainsi que la meilleure méthode pour partager ces informations.

Objectif
Comprendre les interrogations des parties prenantes concernant les activités et les services de la PSIRT. Une fois ces exigences réunies et acceptées, la méthode/les modalités de mise en œuvre et la fréquence des mises à jour doivent être choisies.

Résultat
Une liste documentée des exigences des parties prenantes en matière d'artefacts (rapport/opinion/tableau de bord) sera créée à des fins de maintenance.

Sous-fonction 1.7.1.1 Exigences relatives à la collecte de mesures des parties prenantes

Les parties prenantes seront concernées par un ensemble spécifique de données qui pourront ne pas intéresser d'autres parties prenantes. Par exemple, ces mesures pourraient porter sur les coûts, la qualité et les performances de l'équipe en charge de la correction.

Fonction 1.7.2 Collecter des mesures relatives aux parties prenantes

Les processus et mesures exigés pour documenter les mesures requises pour l'ensemble des groupes de parties prenantes. Dans la mesure du possible, les outils utilisés par la PSIRT doivent permettre de collecter et de transmettre des informations relatives aux processus et aux performances de la PSIRT. En principe, les mesures doivent être centralisées (dans une base de données, un tableur, ou tout autre outil) de sorte que les performances historiques puissent être régulièrement examinées et que les avis des différentes parties prenantes puissent être facilement pris en compte, en limitant la charge de travail supplémentaire.

Objectif
Rassembler, générer, regrouper et/ou collecter les points de données nécessaires pour satisfaire les exigences des parties prenantes relatives aux performances de la PSIRT. Ces informations doivent être stockées de façon centralisée en vue d'un examen rétrospectif et de leur réutilisation par les parties prenantes (par exemple, si deux groupes de parties prenantes ou plus souhaitent les mêmes informations).

Résultat
Les mesures souhaitées relatives aux parties prenantes seront collectées en vue de la création d'artefacts (rapports, avis, tableaux de bord, etc.).

Sous-fonction 1.7.2.1 Collecter des mesures relatives aux parties prenantes

La PSIRT doit mettre au point des procédures et des méthodes pour collecter les mesures requises en respectant les intervalles précisés (accords sur le niveau de service/accords sur le niveau opérationnel).

Sous-fonction 1.7.2.2 Conserver les mesures relatives aux parties prenantes

La PSIRT devra effectuer une analyse de l'historique des performances et d'autres tendances, il est donc utile d'élaborer un répertoire pour ces données afin qu'elles puissent être utilisées à l'avenir.

Fonction 1.7.3 Analyser les mesures relatives aux parties prenantes

Sans contexte, les données sont inutiles. Des hypothèses incorrectes peuvent être déduites, et les services peuvent ne pas être ajustés pour répondre aux demandes changeantes des entreprises ou des parties prenantes. Une fois que la PSIRT a collecté les données requises, des efforts doivent être déployés pour examiner ces données et fournir le contexte précisant ce que ces données signifient pour la partie prenante.

Objectif
Comprendre la signification des données collectées et fournir le contexte à la partie prenante concernant l'utilisation de ces données. Idéalement, la partie prenante doit pouvoir comprendre les résultats d'un indicateur clé de performance donné ainsi que les facteurs l'ayant influencée au cours de la période considérée. Elle doit en outre être capable d'identifier les tendances se dessinant au sein de cet indicateur.

Résultat
Les données historiques seront stockées et comparées aux performances actuelles pour identifier les tendances.

Sous-fonction 1.7.3.1 Analyser et examiner les données des mesures

La PSIRT doit consacrer du temps et des efforts à l'examen des données recueillies et détailler le contexte en parallèle des mesures rapportées.

Sous-fonction 1.7.3.2 Analyser les tendances des données et les performances historiques

La collecte de données historiques permet de dégager des tendances uniques ou d'identifier des problèmes chroniques que la PSIRT ou ses partenaires peuvent résoudre.

Sous-fonction 1.7.3.3 Contextualiser les données

Contextualiser les données pour que les parties prenantes puissent correctement comprendre ce qui leur sera transmis et fournir un moyen de traiter les questions ou les problèmes.

Fonction 1.7.4 Fournir des artefacts présentant des mesures relatives aux parties prenantes

Une fois les données collectées et analysées, elles doivent être transmises aux parties prenantes dans un format convenu à l'avance. Il peut s'agir d'un artefact ou d'un avis visant à traiter le point de vue d'une partie prenante. Ces artefacts peuvent prendre la forme d'une page Web, d'un courriel, d'un rapport plus formalisé ou de toute autre méthode.

Objectif
Les données doivent être transmises aux parties prenantes dans un format qui leur est accessible afin de les aider à mieux connaître et comprendre les performances de la PSIRT dans le cadre de la prestation de services. Ces données doivent être compréhensibles et suffisamment contextualisées pour permettre à la partie prenante de prendre des décisions fondées sur ces performances.

Résultat
Les données seront fournies aux parties prenantes dans un format approprié dans les délais convenus.

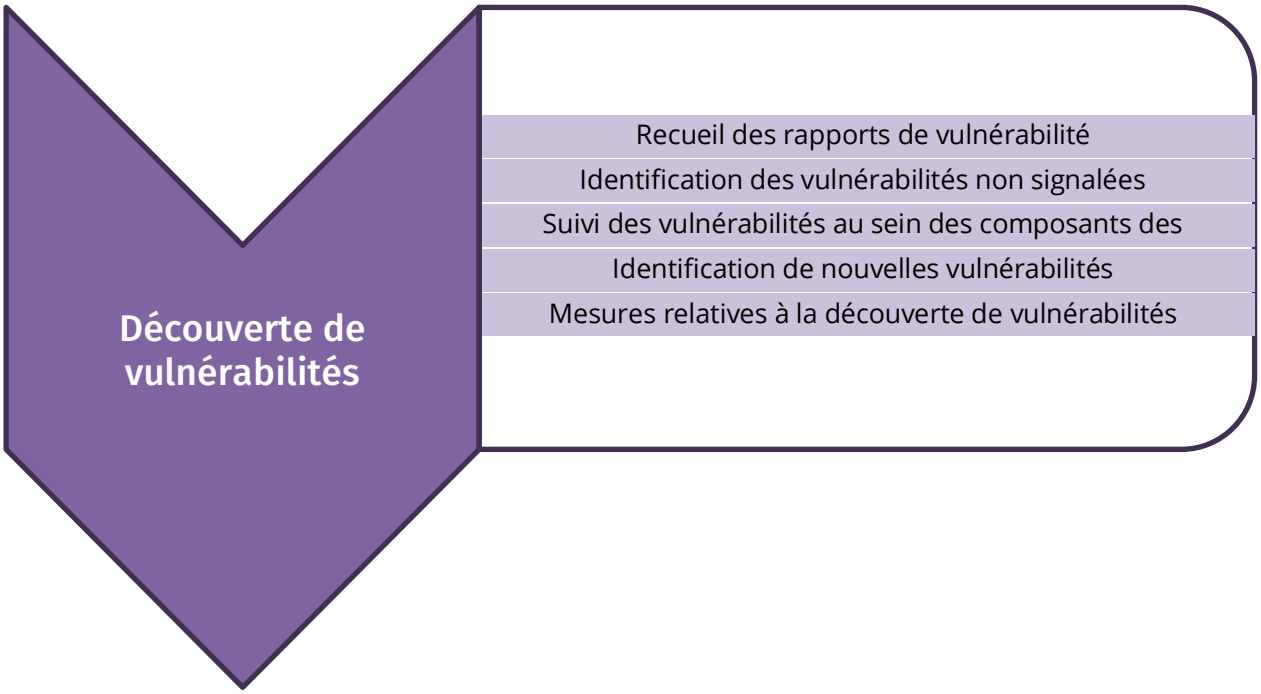
Sous-fonction 1.7.4.1 Fournir des artefacts de mesure aux parties prenantes

Chaque partie prenante représente un point de vue spécifique. Chaque point de vue doit être traité en mettant en avant les données sous la forme d'un artefact de signalement. Il se peut que ces artefacts doivent être ajustés pour correspondre à des points de vue divergents. Les artefacts peuvent être des rapports envoyés par courrier électronique ou publiés sur une page Web, un portail Web dynamique, des notes de synthèse, des tableaux, des graphiques, ou de nombreux autres mécanismes de transmission de données.

Sous-fonction 1.7.4.2 Examiner les mesures et les enseignements tirés

L'un des objectifs les plus importants de la PSIRT doit consister à constamment améliorer le processus de gestion des vulnérabilités. L'examen des mesures de la performance et des retours d'informations des parties prenantes aide la PSIRT à déterminer des domaines méritant une certaine attention ou devant être améliorés.

Zone de service 2 Découverte de vulnérabilités



Cette zone de service décrit les services et les fonctions que doit assumer une PSIRT pour découvrir des vulnérabilités potentielles. Les activités entreprises dans le cadre de cette zone de service donneront lieu au lancement du processus de gestion des vulnérabilités décrit dans d'autres sections du présent document. La maturité d'une PSIRT peut être mesurée à travers la disponibilité et l'efficacité des différents services prévus dans cette zone de service.

Objectif
Établir des processus et des mécanismes de collecte de renseignements relatifs aux vulnérabilités des produits, aux composants tiers vulnérables ou aux faiblesses architecturales de différentes sources.

Résultat
Renforcer l'appréciation de la situation pour les rapports et les vulnérabilités potentielles qui nécessitent une action de la part des parties prenantes.

Service 2.1 Recueil des rapports de vulnérabilité

Le scénario principal s'appliquant à une PSIRT est le recueil de rapports relatifs à des vulnérabilités affectant le produit d'une partie prenante. Afin de recueillir des rapports de vulnérabilité, il convient en premier lieu de mettre en place et d'assurer la maintenance des infrastructures nécessaires, de définir et diffuser les points de contact, ainsi que de déterminer un seuil de préparation à respecter.

Objectif
Établir des processus et des mécanismes qui permettront à une entité de signaler facilement une vulnérabilité affectant le produit d'une partie prenante et de maintenir la PSIRT prête en cas de rapport de vulnérabilité.

Résultat
Préparation de la PSIRT aux rapports de vulnérabilité et recueil professionnel de ces derniers.

Fonction 2.1.1 Garantir la disponibilité

Les PSIRT doivent se faire connaître et se mettre à disposition des parties externes ou des voies de recours hiérarchiques internes. Un canal de communication clair et défini peut aider les découvreurs, les partenaires ou les parties prenantes à signaler une vulnérabilité aux PSIRT.

Objectif
Permettre à une entité souhaitant signaler une vulnérabilité de trouver facilement les informations de contact nécessaires et le mode de soumission préféré.

Résultat
Obtenir un plus grand nombre de rapports et écarter toute demande pour laquelle la PSIRT n'était pas disposée à accepter la soumission d'informations relatives à la vulnérabilité.

Sous-fonction 2.1.1.1 Identifier le type de soumission de rapport privilégié

S'attendre à être informé des vulnérabilités par le biais de différents canaux et d'un niveau de qualité variable. Il est toujours utile de définir la meilleure façon de soumettre un rapport. Cela peut prendre la forme d'un formulaire web, d'un système de tickets public, d'une adresse électronique, d'une assistance téléphonique, ou tout autre moyen de soumission.

Sous-fonction 2.1.1.2 Publier les données de contact

Les informations de contact préférées de la PSIRT doivent figurer dans la documentation du produit, être indiquées sur la page web de l'entreprise, être indexées dans les moteurs de recherche, être inscrites sur les listes principales de CSIRT/PSIRT, et être communiquées aux entités de publication de listes CVE, telles que les autorités de numérotation des CVE (CNA), et être transmises aux communautés de professionnels de la sécurité.

Sous-fonction 2.1.1.3 Enregistrer les points de contact courants

Il est utile de réserver des termes courants liés à la PSIRT tels que "psirt@", "incidents@" ou "sécurité@" dans le nom de domaine de votre entreprise. Cette précaution contribuera à rediriger vers vous les communications pertinentes de la PSIRT.

Sous-fonction 2.1.1.4 Relier la PSIRT à l'entreprise

Vérifier que le service des parties prenantes (pour les demandes ou les rapports de vulnérabilité des parties prenantes), le département de la communication (pour les demandes des médias), ainsi que vos équipes de développement des produits (pour

remonter les découvertes internes majeures) ont connaissance de l'existence de la PSIRT et savent comment la contacter.

Sous-fonction 2.1.1.5 Définir et respecter le seuil de préparation

En fonction du secteur et des exigences établies par les parties prenantes, mettre au point un service de garde ou un service continu ajusté aux fuseaux horaires afin de maintenir le niveau de préparation nécessaire pour répondre aux rapports critiques.

Sous-fonction 2.1.1.6 Se préparer aux soumissions chiffrées

Les rapports de vulnérabilité contiennent souvent des informations sensibles sur l'environnement opérationnel et les produits au sein desquels la vulnérabilité a été détectée. Pour éviter toute fuite ou divulgation accidentelle d'informations, promouvoir des moyens permettant de soumettre des rapports de façon chiffrée, tels que le S/MIME ou les courriels protégés par PGP ou un formulaire Web HTTPS.

Fonction 2.1.2 Traiter les rapports de vulnérabilité

Les rapports de vulnérabilité sont reçus depuis différentes sources et sous différentes formes. Le suivi régulier des canaux de communication entrant et une réaction rapide après réception des rapports sont essentiels. Les délais de réaction à l'égard des découvreurs externes doivent être définis au sein d'un accord sur le niveau de service interne à l'entreprise.

Objectif
Fournir des processus et des mécanismes permettant de recevoir des rapports de vulnérabilité d'autres parties de l'entreprise fournisseuse, des parties prenantes, et de tiers (découvreurs, autres PSIRT, CSIRT, etc.).

Résultat
Gestion professionnelle des rapports de vulnérabilité fournis par des tiers.

Sous-fonction 2.1.2.1 Assurer le suivi les canaux de communication

Vérifier régulièrement les méthodes de contact avec la PSIRT indiquées, ainsi que d'autres canaux disponibles tels que les boîtes mail d'usage général ou les comptes de médias sociaux de l'entreprise.

Sous-fonction 2.1.2.2 Traiter les rapports séparément

Les rapports de vulnérabilité seront étudiés par la PSIRT, qui constitue de ce fait une cible facile pour les soumissions malveillantes. Élaborer des politiques et des procédures techniques pour protéger l'environnement de travail contre de telles tentatives en fournissant des moyens permettant de traiter les rapports de vulnérabilité en toute sécurité.

Sous-fonction 2.1.2.3 Accusé de réception des rapports en temps utile

Si l'analyse détaillée du rapport est généralement complexe et chronophage, un simple accusé de réception peut être rapidement transmis. Une réaction rapide montre que le rapport est pris au sérieux, ce qui contribue sensiblement à instaurer un climat de confiance. La communication ultérieure tout au long du processus de traitement peut s'appuyer sur cette première interaction et montre que la PSIRT s'engage à effectuer une résolution complète du problème.

Service 2.2 Identification des vulnérabilités non signalées

Les vulnérabilités communiquées au fournisseur directement ou par les parties les ayant signalées sont simples à appréhender. Toutefois, il est important de se rendre compte qu'il existe d'autres vulnérabilités pouvant être divulguées par le biais de canaux informels, tels que les médias d'information, les blogs techniques, les bases de données d'experts, les médias sociaux ou les publications techniques et les conférences.

Objectif
Maintenir le niveau d'appréciation de la situation, diminuer le temps de détection des menaces affectant le produit d'une partie prenante et réduire la probabilité de divulgations complètes.

Résultat
Une appréciation de la situation accrue à l'égard des menaces de sécurité pour le portefeuille de produits d'une partie prenante.

Fonction 2.2.1 Assurer le suivi des bases de données d'exploits

Les bases de données d'exploits ou les flux commerciaux disponibles publiquement doivent être surveillés activement afin d'y découvrir de nouvelles vulnérabilités potentielles méritant d'être examinées. Un exploit pleinement fonctionnel peut conduire à la communication proactive d'une entreprise avec ses parties prenantes.

Objectif
Découvrir les vulnérabilités n'ayant jamais été signalées par le biais des canaux appropriés.

Résultat
Une meilleure connaissance de l'existence des exploits fonctionnels sur le marché.

Fonction 2.2.2 Assurer le suivi des programmes de conférence

Des conférences pertinentes portant sur la sécurité doivent faire l'objet d'un suivi pour déterminer des soumissions présentant un intérêt. Outre le référencement direct des produits ou des marques, les soumissions peuvent traiter de thèmes plus larges, comme les défauts des protocoles qui peuvent nécessiter l'intervention d'une PSIRT. Si le résumé du document soulève des questions, il convient de collaborer avec le découvreur au plus tôt pour déterminer si des mesures doivent être prises. Par ailleurs, la présence en conférence et la coopération proactive avec les auteurs peuvent encourager des contacts directs avec la PSIRT en vue de recherches futures.

Objectif
Éviter toute surprise due à une divulgation non coordonnée ou identifier les défaillances susceptibles d'affecter directement ou indirectement les produits des parties prenantes qui n'ont pas encore été examinés par les auteurs.

Résultat
Possibilité d'entrer activement en contact avec les auteurs avant toute publication afin de déterminer si d'éventuels produits des parties prenantes sont affectés ou si un problème est survenu lors de la soumission du rapport.

Fonction 2.2.3 Assurer le suivi des publications de découvreurs renommés

Soyez attentifs aux publications des découvreurs connus pour la pertinence de leurs publications ou leur vaste expertise du secteur ou des produits et services d'une entreprise spécifique. Leurs travaux scientifiques, leurs billets de blogs, ou leur participation à une liste de diffusion peuvent indiquer de possibles vulnérabilités ou faiblesses qui méritent de s'y intéresser.

Objectif
Maintenir l'état des connaissances scientifiques et techniques sur les thèmes relevant de la sécurité qui intéressent les parties prenantes.

Résultat
Expertise dans les menaces et les faiblesses courantes et les possibles contremesures permettant de soutenir les parties prenantes lors de la résolution des problèmes de sécurité.

Fonction 2.2.4 Surveiller les médias de masse

Les médias de masse sont généralement les premiers à détecter des problèmes, en particulier en cas d'incidents catastrophiques touchant les installations ou le personnel des parties prenantes. Surveiller les médias de masse peut aider à détecter des situations dans lesquelles les parties prenantes de la PSIRT peuvent être un fournisseur important ou prédominant.

Objectif
Le rejet de la vulnérabilité d'un produit a contribué à provoquer l'incident.

Résultat
Une meilleure préparation dans l'éventualité où des parties prenantes ou des médias demandent des informations concernant les vulnérabilités affectant un produit qui auraient pu contribuer à provoquer l'incident.

Service 2.3 Suivi des vulnérabilités des composants des produits

Les vulnérabilités se répartissent sommairement en trois catégories: 1) les vulnérabilités dans le code source propre au produit; 2) les vulnérabilités dans les composants du produit maintenus par des sources internes aux fournisseurs; et 3) les vulnérabilités dans les composants fournis par des sources externes aux fournisseurs (tiers). Du point de vue des produits, les vulnérabilités 2) et 3) concernent des composants externes, mais les failles détectées dans ces composants peuvent à terme impacter le produit de remplacement. Bien que le propriétaire d'un produit ne dispose que d'un contrôle indirect sur la résolution du problème sous-jacent, la partie prenante

dispose d'un certain de degré de propriété sur la chaîne d'approvisionnement et la correction de la vulnérabilité en ce qui concerne le produit touché. C'est notamment le cas lorsque le problème affectant le composant vulnérable ne peut pas être résolu indépendamment du produit auquel il est intégré. Les composants intégrés à code source ouvert sont également considérés comme des composants tiers.

Objectif
Détecter, collecter, et surveiller les vulnérabilités dans la chaîne d'approvisionnement des produits d'une partie prenante, et tenir les équipes de produits informées des vulnérabilités affectant leur produit.

Résultat
Une meilleure connaissance de la détection précoce des vulnérabilités héritées de la chaîne d'approvisionnement qui affectent les produits d'une partie prenante.

Fonction 2.3.1 Inventaire des composants des produits

Maintenir une liste des fournisseurs ainsi que des produits et des versions fournis par des parties internes et externes qui sont intégrés aux produits. Cette procédure est essentielle pour rapidement identifier les produits affectés par des vulnérabilités héritées.

Objectif
Déterminer les produits comprenant des composants vulnérables susceptibles de provoquer une défaillance dans le produit.

Résultat
Une nomenclature des matériels pour tous les produits afin de rechercher les composants vulnérables au sein des produits.

Fonction 2.3.2 Assurer le suivi des bulletins des tiers

Obtenir des informations opportunes concernant les vulnérabilités dans les composants tiers en s'abonnant aux bulletins des fournisseurs ou en établissant des canaux de communication spécifiques avec ces derniers. S'abonner à des listes de diffusion traitant de la sécurité pour les projets à code source ouvert. Cela peut être garanti par le recours à des fournisseurs d'informations sur les vulnérabilités.

Objectif
Détecter les vulnérabilités au sein des composants tiers à l'origine d'une vulnérabilité dans le produit d'une partie prenante.

Résultat
Lancer éventuellement une procédure de gestion des vulnérabilités avant l'élaboration d'un rapport externe sur les produits affectés.

Fonction 2.3.3 Assurer le suivi des sources d'informations sur les vulnérabilités

Il peut ne pas toujours être possible de s'abonner aux bulletins des fournisseurs pour les composants tiers. C'est notamment le cas lorsque le fournisseur n'en publie pas, qu'il a cessé ses activités ou que la communauté des logiciels libres liée au composant n'est pas proactive. Les ressources telles que la Base de données nationale des vulnérabilités (NVD) ou les sources d'informations commerciales peuvent aider à détecter des vulnérabilités non signalées.

Objectif
Détecter les vulnérabilités non signalées au sein des composants tiers.

Résultat
Une meilleure visibilité des vulnérabilités qui seraient passées inaperçues.

Fonction 2.3.4 Mettre en place des procédures pour le recueil d'informations sur les vulnérabilités au sein de la chaîne d'approvisionnement interne des fournisseurs

Dans la majorité des cas, les composants des produits de sources internes de fournisseurs ne feront pas l'objet de bulletins publics sur les problèmes de sécurité résolus. Afin d'obtenir des informations relatives aux vulnérabilités dans la chaîne d'approvisionnement interne des fournisseurs, il convient de mettre en place des canaux de communication spécifiques avec ces fournisseurs.

Objectif
Détecter les vulnérabilités au sein de la chaîne d'approvisionnement interne des fournisseurs à l'origine d'une vulnérabilité affectant le produit d'une partie prenante.

Résultat
Une meilleure visibilité des vulnérabilités au sein de la chaîne d'approvisionnement interne des fournisseurs qui seraient passées inaperçues.

Fonction 2.3.5 Notification des équipes de développement internes

Établir des canaux automatisés pour transmettre des notifications sur les vulnérabilités tierces directement aux équipes de développement des produits affectés. Il suffit généralement de suivre les instructions du fournisseur en amont pour corriger le problème touchant le produit en aval. Conformément à la politique de hiérarchisation, définir le moment auquel les vulnérabilités doivent être catégorisées différemment et remontées en vue de leur gestion par la PSIRT. Ce dernier point est particulièrement important si une partie prenante doit intervenir pour obtenir une version corrigée du produit en vue d'en sécuriser l'exploitation.

Objectif
Informer de manière sélective les équipes de développement quant aux dépendances vulnérables et aux correctifs (si disponibles) pour permettre une correction dans la prochaine version du produit.

Résultat
Réduire les efforts que doit déployer la PSIRT dans la gestion manuelle des vulnérabilités étant donné que les informations consultatives fournies par des tiers peuvent être traitées directement dans les processus de développement.

Service 2.4 Identification de nouvelles vulnérabilités

Une PSIRT peut activement prendre part à la découverte interne de nouvelles vulnérabilités, ce qui peut constituer une occasion de traiter des problèmes de sécurité affectant les produits afin de limiter la gestion des relations externes et potentiellement réduire les efforts généraux de coordination. De telles activités doivent venir compléter les activités de vérification de la sécurité qui s'inscrivent dans le SDL. Les activités menées par la PSIRT peuvent comprendre la réalisation d'évaluations de la sécurité des produits avant leur lancement ou pendant la phase de maintenance, ainsi que la fourniture d'une expertise en matière d'outils d'évaluation de la sécurité aux équipes de recherche et développement. Les vulnérabilités découvertes en interne affectant les utilisateurs finaux doivent être traitées de la même façon que celles détectées par des parties externes, tout comme les évaluations et les rapports, qui doivent être coordonnés avec la publication du correctif.

Objectif
Détecter et corriger les vulnérabilités affectant les produits avant leur découverte par des parties externes.

Résultat
Expertise, procédures, et mécanismes pour la découverte de vulnérabilités au sein des produits en interne, et possible réduction des efforts de coordination.

Fonction 2.4.1 Évaluation de la sécurité des produits

L'évaluation de la sécurité des produits désigne la pratique consistant à chercher activement des vulnérabilités actuellement inconnues. Elle peut couvrir un large éventail de techniques et d'outils, tels que le test d'intrusion ou les scanners de vulnérabilités. Ces techniques d'évaluation de la sécurité en boîte noire/boîte grise qui simulent un piratage extérieur à l'entreprise désignent une méthodologie dans laquelle l'attaquant a peu de connaissances voire aucune à l'égard du système ciblé.

Objectif
Détecter des vulnérabilités au moyen de mécanismes proactifs.

Résultat
Une phase d'assurance qualité venant compléter les activités de vérification de la sécurité du SDL.

Sous-fonction 2.4.1.1 Évaluation de la sécurité de vos produits

Les résultats d'analyse d'une évaluation de la sécurité mettant en cause les contrôles de sécurité de votre produit peuvent être d'une grande utilité pour les développeurs qui cherchent à améliorer la position de leur produit avant sa mise sur le marché ou lors de la préparation d'un correctif.

Sous-fonction 2.4.1.2 Évaluation de la sécurité de composants tiers

Pour ce qui est des composants obtenus auprès de tiers, il est recommandé de mener une évaluation de sécurité dédiée renforcée, en plus des procédures générales de gestion des achats. Cette pratique est particulièrement nécessaire pour les composants essentiels afin de garantir une diligence raisonnable de qualité.

Fonction 2.4.2 Maintenir l'expertise nécessaire pour les outils d'évaluation de la sécurité

Les entités commerciales et les communautés mettent constamment au point de nouveaux outils offensifs et d'analyse de la sécurité. La PSIRT doit constamment mettre à jour ses connaissances des outils disponibles. Ces informations sont utiles pour évaluer les produits, valider les résultats des découvreurs externes ou conseiller les équipes de développement dans le choix des outils adaptés à leurs tests internes.

Objectif
Constituer une équipe d'experts bien préparée, disposant des compétences nécessaires pour manipuler des outils complexes et fournir des conseils sur leur utilisation.

Résultat
Tirer parti des meilleurs outils disponibles.

Sous-fonction 2.4.2.1 Formation du personnel de la PSIRT aux outils d'évaluation de la sécurité

La formation du personnel constitue un élément clé dans le maintien de connaissances à jour concernant les outils d'évaluation de la sécurité disponibles. La section *Service 6.3 Validation sécurisée* évoque la formation du personnel de la PSIRT de façon plus détaillée.

Service 2.5 Mesures relatives à la découverte de vulnérabilités

Figure 8: Processus de collecte de mesures relatives à la découverte de

Fournir des renseignements concernant les effectifs de la PSIRT, ses performances, ou d'autres mesures est essentiel pour maintenir les parties prenantes informées de l'efficacité de la PSIRT (voir également les *Fondements opérationnels de la Section III: A. Évaluation et amélioration*). Les différentes parties prenantes auront des points de vue uniques qui doivent être traités avec des

artefacts (ou points de vue) aux formats potentiellement différents. La PSIRT doit comprendre comment chaque groupe de parties prenantes souhaite utiliser ces informations. Ces mesures pourraient être des indicateurs clés de performance pour la PSIRT.

Objectif
Fournir des données relatives aux mesures et performances de la PSIRT. Ainsi, les parties prenantes peuvent comprendre l'efficacité des prestations de la PSIRT dans un domaine ou un service particulier.

Résultat
En examinant les mesures de la PSIRT, les parties prenantes doivent comprendre l'efficacité avec laquelle une PSIRT fournit un service et être capables de transmettre des retours d'informations pour apporter des ajustements à cette prestation de services.

Fonction 2.5.1 Rapports opérationnels

Les rapports opérationnels fournissent des informations sur le volume et le type de vulnérabilités découvertes. Ces rapports peuvent être publiés régulièrement en interne au sein de la PSIRT et à l'intention des parties prenantes internes.

Objectif
Collecter des données régulièrement pour l'élaboration de rapports généraux.

Résultat
Déterminer les domaines nécessitant une analyse, des ressources et des améliorations.

Sous-fonction 2.5.1.1 Total de vulnérabilités découvertes par rapport aux vulnérabilités confirmées Confirmée

Ces données permettent de rendre compte du volume de vulnérabilités gérées par une PSIRT du point de vue des ressources. Ces données peuvent être ventilées par unité opérationnelle, type de produit, ou produits spécifiques.

Sous-fonction 2.5.1.2 Nombre total de vulnérabilités confirmées ventilées par composant tiers

Ces données permettent de rendre compte du risque associé à des composants tiers intégrés spécifiques.

Sous-fonction 2.5.1.3 Nombre total de vulnérabilités confirmées ventilées par liste des failles courantes (CWE)

Ces données peuvent être alimentées en amont du cycle de développement sécurisé et influer sur la formation et l'apprentissage. Ces données peuvent être ventilées par unité opérationnelle, type de produit, ou produits spécifiques.

Sous-fonction 2.5.1.4 Total de vulnérabilités découvertes ventilées par approche de découverte de vulnérabilités

Ces données permettent de déceler des vulnérabilités simples à détecter et peuvent être alimentées en amont du cycle de développement sécurisé. Ces données peuvent être ventilées par unité opérationnelle, type de produit, ou produits spécifiques.

Sous-fonction 2.5.1.5 Total de vulnérabilités découvertes ventilées par source

Ces données permettent de décrire le degré de notoriété de la PSIRT.

Fonction 2.5.2 Rapports d'activité

Les rapports d'activité fournissent des informations sur l'état de la riposte aux vulnérabilités d'une organisation, cette notion renvoyant à la gestion des failles de sécurité et aux interventions en cas de vulnérabilité.

Objectif
Mettre des mesures au point afin de définir les critères de réussite de l'organisation et collecter régulièrement des données en vue de l'établissement de rapports de gestion permettant de détecter les risques.

Résultat
Création d'un tableau de bord mettant en avant les réussites et les possibilités d'amélioration.

Sous-fonction 2.5.2.1 Rapidité d'intervention

Ces données rendent compte du degré de rapidité de la réaction initiale de la PSIRT aux rapports de vulnérabilité, dans les délais fixés par les accords sur le niveau de service.

Sous-fonction 2.5.2.2 Durée d'indisponibilité totale des canaux de communication de la PSIRT

Ces données rendent compte de la disponibilité des canaux de communication de la PSIRT conformément à l'accord sur le niveau de service.

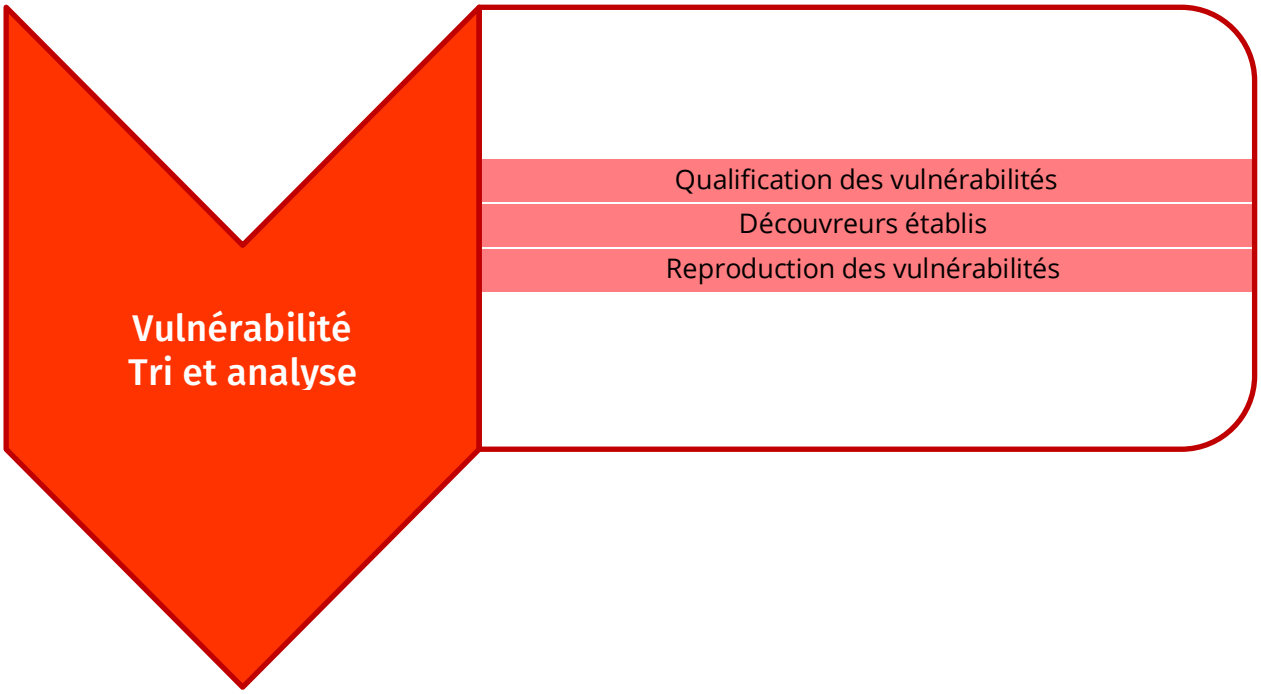
Sous-fonction 2.5.2.3 Taux de la durée de tri

Ce taux mesure le temps écoulé entre le recueil initial des rapports et l'achèvement des activités de tri. Ces données rendent compte de la performance et/ou de la charge de travail du personnel de la PSIRT.

Sous-fonction 2.5.2.4 Nombre de divulgations complètes, de vulnérabilités exploitées en liberté, et de vulnérabilités détectées par le biais des médias

Ces données rendent compte des risques auxquels sont exposés les produits d'une partie prenante.

Zone de service 3 Tri et analyse des vulnérabilités



Le recueil et le tri de vulnérabilités constituent la fonction de gestion des cas d'une PSIRT. Si l'ordre des opérations est très similaire entre les PSIRT, il existe toutefois des divergences, notamment le moment précis où un "cas" est créé ou les différentes fonctions pouvant être exercées par le personnel au sein d'un cas. Lorsque les organisations reçoivent un important volume de rapports de vulnérabilité, ils peuvent envisager de procéder à un tri initial afin de valider les rapports avant que les cas ne soient créés. À l'inverse, au sein des organisations recevant un faible volume de rapports de vulnérabilité, un cas peut être créé avant d'effectuer un tri. La PSIRT a pour objectif final la création d'un processus efficace et défini.

Objectif
Définir la façon dont les rapports de vulnérabilité seront triés.

Résultat
Établir un processus au sein de la PSIRT et des équipes d'ingénieurs connexes.

Service 3.1 Qualification des vulnérabilités

Les organisations définissent des critères de qualification appropriés pour le type et la portée des problèmes qu'ils entendent traiter. Ces critères de qualification permettront d'établir une référence en matière de sécurité et aideront à trier efficacement les rapports de vulnérabilité entrants.

Figure 9: Processus de qualification des vulnérabilités

Fonction 3.1.1 Seuil de qualité et échelles de bogues

Le système d'évaluation des vulnérabilités courantes permet de déterminer les principales caractéristiques d'une vulnérabilité et d'obtenir une note chiffrée rendant compte de sa gravité. La note chiffrée peut être traduite sur le plan qualitatif (degré de gravité faible, moyen, élevé ou très élevé) afin d'aider les entreprises à évaluer correctement leurs processus de gestion des vulnérabilités et à attribuer un degré de priorité à ceux-ci. Ces processus, parfois désignés sous les termes "seuil de qualité" et/ou "échelle de bogues", sont utilisés pour établir des niveaux minimums acceptables de qualité de la sécurité, et des critères de hiérarchisation pour les failles de sécurité. Le fait de définir ces critères avant le lancement des produits garantit la transparence du processus de gestion des vulnérabilités en prédéterminant ce que la PSIRT qualifiera de vulnérabilité d'un produit exigeant une correction. Les vulnérabilités et expositions courantes (CVE) sont une liste d'entrées contenant un numéro d'identification, une description et au moins une référence publique utilisée le plus souvent pour clarifier le problème en cours de traitement.

Objectif
Définir des normes minimales claires et des critères de hiérarchisation pour garantir une certaine transparence aux parties prenantes internes et externes.

Résultat
Présenter clairement les caractéristiques d'une vulnérabilité aux ingénieurs et aux découvreurs. Des critères de hiérarchisation supplémentaires permettront d'atténuer la confusion et les différends liés à la gestion du cycle de vie des vulnérabilités, du tri initial à la communication des correctifs.

Sous-fonction 3.1.1.1 Recenser les failles de sécurité des produits identifiées

Le seuil de qualité ou l'échelle de bogues doivent être documentés, conservés de façon centralisée, et être intégrés à la formation des développeurs/ingénieurs.

Sous-fonction 3.1.1.2 Collaborer avec les équipes de développement des produits

Dans l'éventualité où de nombreux produits et équipes de développement des produits coexistent au sein d'une organisation, il importe de garantir la coopération entre ces équipes afin d'harmoniser la définition d'une faille de sécurité d'un produit.

Fonction 3.1.2 Amélioration continue

Une PSIRT mature doit adopter une approche d'amélioration continue pour réviser ses critères de qualification, le cas échéant, afin de refléter son expérience, les bonnes pratiques du secteur, les changements apportés aux produits et les retours d'informations des parties prenantes. Il est important de communiquer les changements aux parties prenantes internes et externes afin de répondre à leurs attentes.

Objectif
Reconnaître que les critères de qualification sont sujets à révision. Les dynamiques entourant la PSIRT, telles que les attentes des parties prenantes, les tendances du secteur, ou le volume de vulnérabilités entrantes pourront conduire à des ajustements fréquents.

Résultat
La fluidité des critères de qualification des vulnérabilités favorisera l'efficacité de cette pratique.

Sous-fonction 3.1.2.1 Collecter des données

Collecter des données sur le processus de tri, y compris le nombre de rapports entrants, le nombre de rapports considérés comme exposant une vulnérabilité, le nombre de rapports non qualifiés comme tel, et toute divergence rencontrée.

Objectif
Favoriser les améliorations en fonction des données.

Résultat
Les changements apportés aux seuils de qualité et aux échelles de bogues sont motivés par les données.

Service 3.2 Découvreurs établis

Alors que la PSIRT d'une organisation gagne en maturité, il se peut que l'équipe identifie un groupe de découvreurs réguliers responsables du signalement d'un nombre de vulnérabilités supérieur à la normale. Il est recommandé de tenir compte de la réputation du découvreur et de la haute qualité de ses prestations précédentes, de contourner certaines fonctions telles que la qualification et le tri afin de passer directement à l'analyse des causes premières et à l'élaboration de mesures correctives. Cela peut aider à accroître l'efficacité du processus et à favoriser les relations entre découvreurs.

Objectif
Comprendre la communauté des chercheurs et les personnes qui signalent le plus de vulnérabilités affectant vos produits et envisager de remonter immédiatement les rapports des découvreurs de confiance.

Résultat
Réduction du délai de réaction à la suite de la réception des rapports des découvreurs de qualité.

Fonction 3.2.1 Base de données de découvreurs

Élaborer et tenir à jour une base de données des individus et organisations vous ayant signalé des vulnérabilités afin d'assurer le suivi de l'historique, des résultats et de toute autre considération ayant trait à la gestion des cas concernant un découvreur.

Objectif
Accroître l'efficacité du processus de tri et favoriser de meilleures relations avec les découvreurs connus pour la qualité de leurs soumissions.

Résultat
Les rapports des découvreurs qualifiés sont plus rapidement traités au sein du système. Les découvreurs sont satisfaits des résultats et les mesures correctives sont prises avant toute échéance de divulgation publique éventuelle.

Fonction 3.2.2 Gestion accélérée pour les découvreurs établis

Certains découvreurs peuvent être prolifiques ou constants (approuvés/crédibilité) dans la découverte et le signalement de bogues logiciels affectant vos produits ou services. Par exemple, ils peuvent utiliser des outils personnalisés de test à données aléatoires et signaler des incidents sans document rédigé particulier ou sans démonstration de faisabilité. Lorsque vous connaissez bien le découvreur et que vous avez déterminé que la majorité des problèmes qu'il a signalés seront corrigés, il convient d'envisager d'ignorer le processus de qualification/d'approbation et de passer directement à la correction.

Objectif
Accroître l'efficacité du processus de tri et favoriser de meilleures relations avec les découvreurs connus pour la qualité de leurs soumissions.

Résultat
Les rapports des découvreurs qualifiés sont plus rapidement traités au sein du système. Les découvreurs sont satisfaits des résultats et les mesures correctives sont prises avant toute échéance de divulgation publique éventuelle.

Fonction 3.2.3 Profils des découvreurs

Envisager de créer des profils recensant les informations relatives à chaque découvreur afin d'aider les gestionnaires à optimiser leur collaboration avec eux. Ces profils peuvent contenir des éléments tels que l'emplacement géographique, les langues parlées, les conférences dans le cadre desquelles les découvreurs ont effectué des présentations, les méthodologies employées pour découvrir des vulnérabilités, les produits/technologies sur lesquels ils mettent généralement l'accent, s'ils pratiquent des divulgations de vulnérabilités coordonnées, s'ils apprécient présenter leurs découvertes lors de conférences, si vous leur versez des primes ou si vous leur avez proposé d'autres incitations, etc. Consulter les équipes juridiques/de conformité pour déterminer les informations pouvant être collectées et la durée de leur conservation.

Objectif
Apprendre à connaître les personnes qui découvrent des vulnérabilités au sein de vos produits.

Résultat
La gestion d'un événement peut être adaptée à un découvreur spécifique afin d'obtenir les meilleurs résultats possible.

Fonction 3.2.4 Définir la qualité des rapports des découvreurs

Les organisations pourront envisager de définir et de publier des directives relatives aux caractéristiques minimales d'un rapport de vulnérabilité de qualité afin de fournir aux découvreurs des orientations sur le type d'informations dont vous avez besoin pour évaluer leur rapport rapidement. Une référence peut comprendre, entre autres, un document rédigé, des étapes de reproduction, une ou des plates-formes testées, une démonstration de faisabilité.

Objectif
Indiquer aux découvreurs les caractéristiques minimales d'un rapport de vulnérabilité de qualité.

Résultat
Les échanges entre le fournisseur et le découvreur sont limités au strict minimum et le fournisseur peut rapidement se consacrer à un plan de correction.

Service 3.3 Reproduction des vulnérabilités

Au-delà de la qualification, sauf mention contraire, la PSIRT doit s'assurer de la reproductibilité du rapport du découvreur afin de valider et de comprendre les conditions conduisant à cet état de vulnérabilité.

Objectif
Fournir les outils et l'environnement nécessaires à la qualification des rapports de vulnérabilité.

Résultat
Validation efficace, sûre et sécurisée des rapports de vulnérabilité.

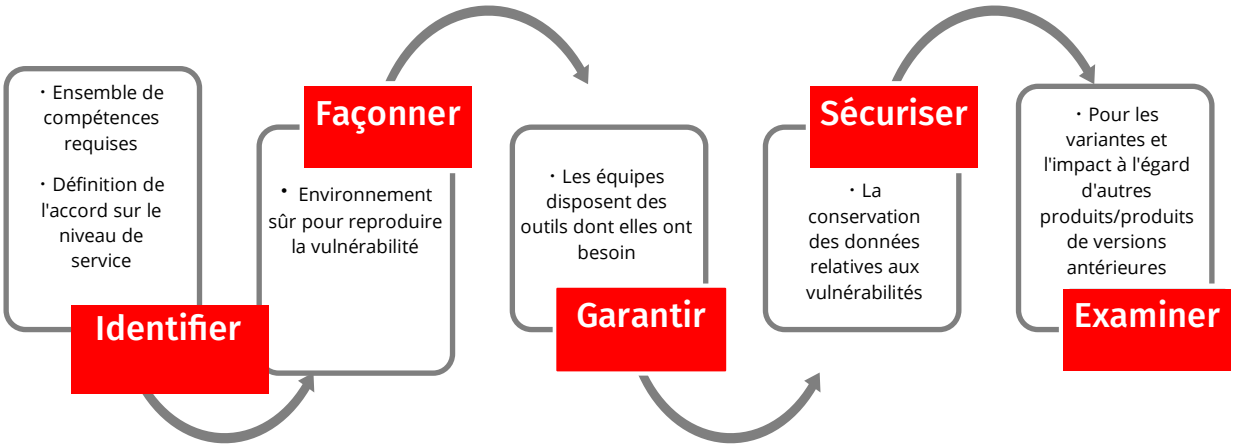


Figure 10: Vérification/reproduction des vulnérabilités

Fonction 3.3.1 Établir un accord sur le niveau de service pour la reproduction des vulnérabilités

Une PSIRT peut ne pas disposer de suffisamment d'expertise technique pour reproduire toutes les vulnérabilités entrantes. Les PSIRT devront peut-être consulter les experts des équipes de développement des produits ou autres, travailler avec eux ou s'appuyer sur eux, il est dont important de disposer d'un accord clairement aligné et défini pour garantir la disponibilité des experts requis. Idéalement, des ressources dédiées travaillant à plein temps ou à temps partiel sont recommandées. Toutefois, si les contraintes budgétaires ne le permettent pas, les experts dans le domaine doivent, au moins, être identifiés au préalable dans le cadre du processus de la PSIRT en vue de pouvoir intervenir rapidement pour des périodes limitées en cas d'incident.

Objectif
Reconnaître qu'une PSIRT peut ne pas disposer d'une expertise technique suffisante pour reproduire toutes les vulnérabilités entrantes.

Résultat
Un alignement interne préalable garantira que des experts sont disponibles rapidement pour aider à la reproduction des vulnérabilités.

Fonction 3.3.2 Environnement du test de reproduction

Un environnement de test dédié doit être mis en place afin de permettre la reproduction de la vulnérabilité par la PSIRT ou l'équipe se consacrant à cette tâche. L'environnement de test doit être clos afin d'éviter les activités malveillantes et de mettre ainsi le rapport du découvreur à l'épreuve. Le cas échéant, un environnement réseau, des simulations, ou de la virtualisation peuvent être utilisés pour créer un environnement sûr.

Objectif
Créer un environnement sûr pour permettre l'inspection et la reproduction des vulnérabilités.

Résultat
Un environnement de test de reproduction bien déployé contribuera au traitement et à la qualification efficaces des vulnérabilités, tout en limitant la vulnérabilité à la portée de l'environnement de test.

Fonction 3.3.3 Outils de reproduction

Les équipes prenant part à la reproduction des vulnérabilités signalées doivent disposer d'outils et de licences de produits à jour pour réaliser ces opérations (par exemple, un débogueur).

Objectif
Veiller à ce que les équipes en charge de la reproduction disposent des outils dont elles ont besoin.

Résultat
Garantir que la reproduction des vulnérabilités signalées est aussi efficace que possible.

Fonction 3.3.4 Stockage des vulnérabilités

Il est recommandé de conserver en toute sécurité les informations sensibles (rapports de vulnérabilité, dossiers de démonstration de faisabilité, etc.) et de limiter leur accès aux seules personnes qui en ont besoin. Il est également conseillé d'assurer la sécurité des informations statiques et en transit. Par exemple, voir la norme ISO 27001.

Objectif
Maintenir la sécurité des informations sensibles et potentiellement préjudiciables relatives aux vulnérabilités.

Résultat
Les informations sensibles sont protégées, leur accès est limité et elles ne sont pas susceptibles de faire l'objet d'une compromission de la part du réseau primaire de l'organisation.

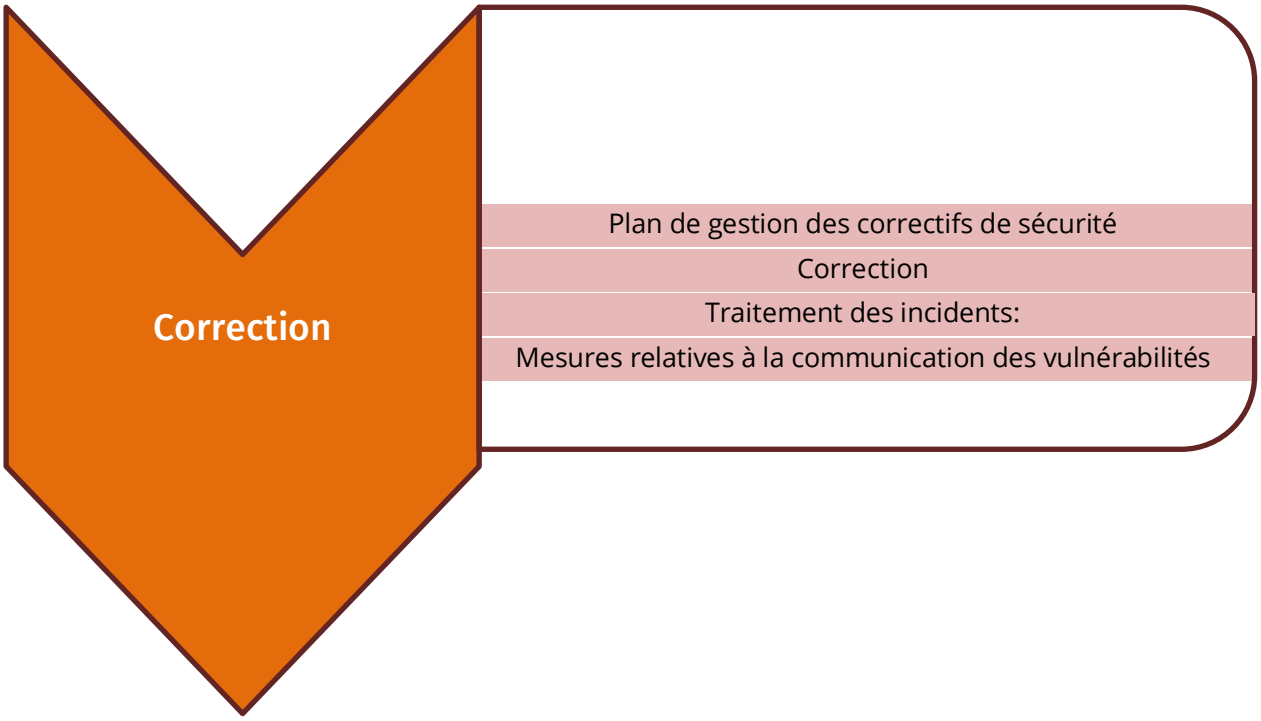
Fonction 3.3.5 Produits affectés

Lors de la reproduction, l'équipe réalisant l'analyse doit s'employer à identifier les produits affectés et à déterminer s'il existe des variantes de cette vulnérabilité. Voir également la section *Fonction 4.1.1 Gestion du cycle de vie des produits.*

Objectif
Obtenir une vue détaillée et comprendre la portée de la vulnérabilité parmi les produits.

Résultat
Les correctifs appliqués pour rectifier la vulnérabilité sont complets parmi les produits pris en charge.

Zone de service 4 Correction



Cette zone de service rend compte des différents services requis pour mettre en œuvre et annoncer un correctif auprès des parties prenantes et des fournisseurs en aval. Le mécanisme de mise en œuvre d'une correction doit être déterminé en fonction de l'impact de la vulnérabilité sur les parties prenantes lorsqu'elle est exploitée. Des procédures doivent être établies pour garantir qu'un correctif est mis en œuvre selon un calendrier prévisible afin que les parties prenantes et les fournisseurs en aval puissent planifier en conséquence le test et le déploiement de ces correctifs.

Objectif
Mettre en évidence les procédures et les mécanismes nécessaires pour communiquer et annoncer un correctif aux parties prenantes et aux fournisseurs en aval.

Résultat
Permettre aux parties prenantes et aux fournisseurs en aval de planifier un correctif en conséquence.

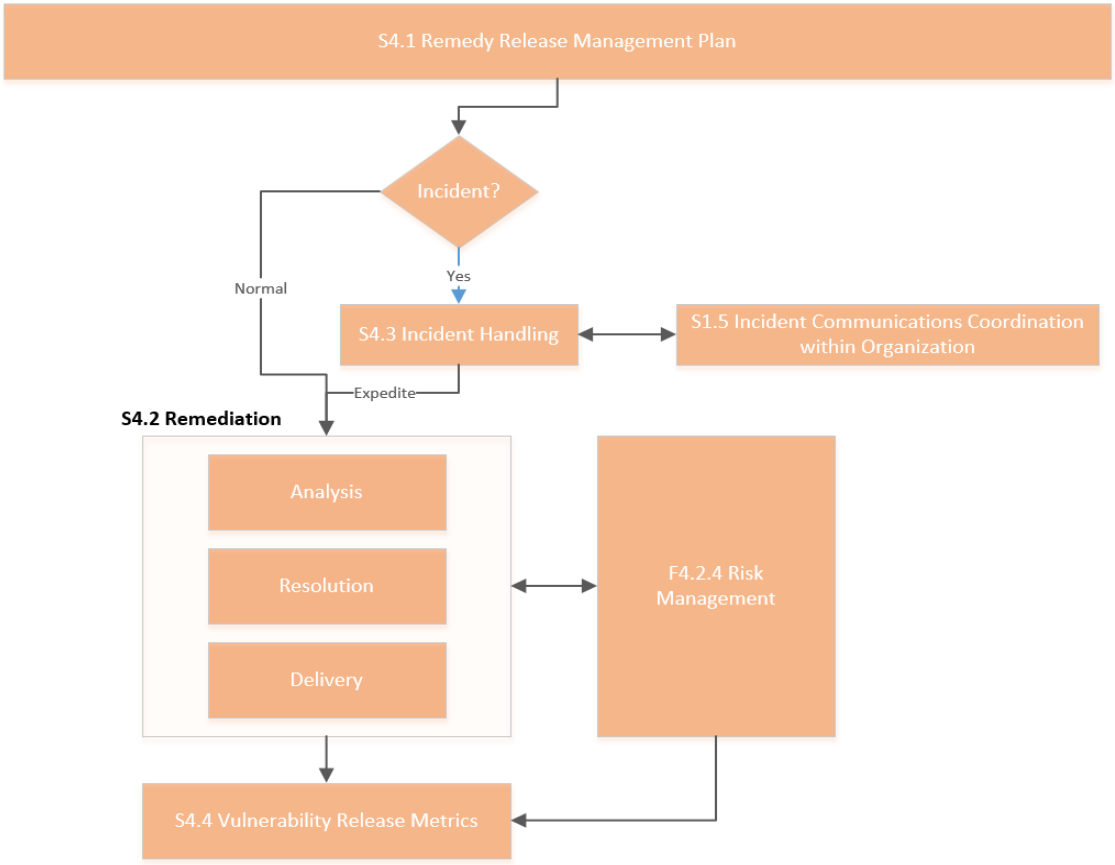


Figure 11: Exemple de processus de publication d'un correctif essentiel

Légende de la Figure 11:

S4.1 Plan de gestion de la publication d'un correctif

Incident

Normal Oui

S4.3 Traitement de l'incident

S1.5 Coordination des communications relatives aux incidents au sein de l'organisation

Accéléré

S4.2 Correction

Analyse

F4.2.4Gestion des risques

Résolution

Mise en œuvre

S4.4 Mesures relatives à la communication des vulnérabilités

Service 4.1 Plan de gestion de la publication d'un correctif

Ce service met l'accent sur la fourniture d'orientations concernant la manière dont le fournisseur prévoit de fixer la fréquence de publication d'un correctif pour les versions d'un produit prises en charge sur le marché. Les parties prenantes, en particulier dans le milieu entrepreneurial, doivent prévoir le déploiement d'un correctif. Certains déploiements, notamment dans le cloud, peuvent disposer de mises à jour automatiques ou d'une politique de gestion des correctifs différente.

Objectif

Informer les parties prenantes sur les produits qui seront pris en charge, les mécanismes de mise en œuvre d'un correctif ainsi que sa fréquence de mise en œuvre.

Résultat

Les parties prenantes seront en mesure de planifier le déploiement des correctifs de sécurité.

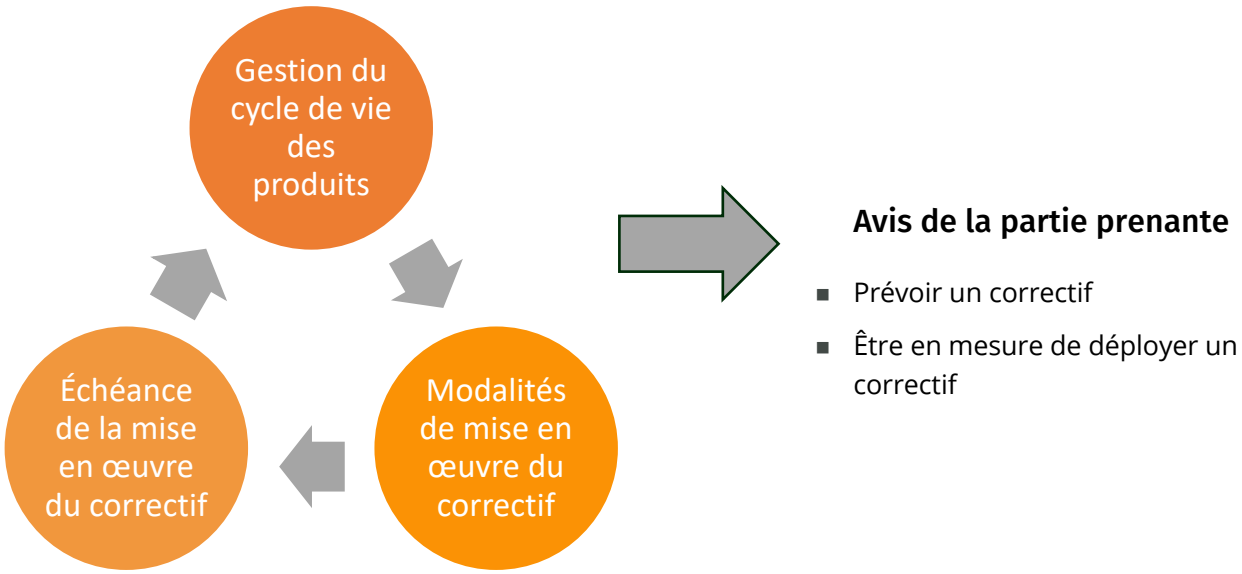


Figure 12: Poser les jalons de la cohérence

Fonction 4.1.1 Gestion du cycle de vie des produits

Les entreprises peuvent avoir des politiques et des accords en matière d'assistance différents avec les parties prenantes. En fonction de ces facteurs, une PSIRT peut coopérer avec des unités opérationnelles/secteurs d'activité et le service d'assistance des parties prenantes pour déterminer comment et s'ils prendront en charge des produits ne rentrant plus dans le champ d'application de l'assistance ou des obligations en la matière. Cela peut dépendre de la gravité de la vulnérabilité et peut inclure des contributions de la part des unités opérationnelles/secteurs d'activité et du service d'assistance des parties prenantes.

Objectif
Fournir une politique claire aux équipes de produits sur la façon dont une organisation prendra en charge les produits affectés par des failles de sécurité.

Résultat
Une politique claire concernant les attentes des unités opérationnelles/secteurs d'activité relatives à la mise en œuvre d'un correctif pour ces types de produits.

Sous-fonction 4.1.1.1 Inventaire des produits

Dresser un inventaire de l'ensemble des produits lancés sur le marché pour garantir que tous les produits applicables pris en charge sont évalués et corrigés.

Sous-fonction 4.1.1.2 Modèles d'assistance

Comprendre les différents types de modèles d'assistance pour les produits, y compris les services payants, les extensions de garantie, les accords de maintenance ou les contrats avec des parties prenantes spécifiques.

Sous-fonction 4.1.1.3 Cycle de vie des produits

Déterminer à quel moment un produit n'est plus pris en charge au sein de son cycle de vie.

Fonction 4.1.2 Méthode de mise en œuvre

Les PSIRT peuvent collaborer avec les équipes de produits et le service d'assistance des parties prenantes pour définir les différentes options de mise en œuvre d'un correctif à destination des parties prenantes. Il convient également de préciser les critères permettant de déterminer le moment propice au déploiement d'un correctif par le biais des moyens identifiés.

Objectif
Maintenir un mécanisme cohérent pour mettre en œuvre les corrections des vulnérabilités selon un ensemble de conditions.

Résultat
Les parties prenantes peuvent planifier et déployer facilement un correctif.

Sous-fonction 4.1.2.1 Formats de conditionnement des produits

Connaître les différents formats de conditionnement pertinents pour la mise en œuvre d'un correctif (par exemple, version exécutable binaire, différences de code source, etc.)

Sous-fonction 4.1.2.2 Mise en œuvre d'un correctif

Comprendre les différents mécanismes de mise en œuvre d'un correctif, tels que les correctifs logiciels, les rustines, les mises à jour de maintenance, les mises à jour de micrologiciels et les modalités de distribution d'un correctif.

Sous-fonction 4.1.2.3 Déploiement d'un correctif

Identifier les modalités de déploiement du correctif pour chaque produit (à savoir: à distance, installation par les clients, mises à jour automatiques ou installation sur place).

Fonction 4.1.3 Fréquence de mise en œuvre

Les parties prenantes et les fournisseurs en aval doivent prévoir un correctif afin de pouvoir maintenir le niveau de sécurité de leur environnement. Fixer une fréquence de mise en œuvre du correctif permettra aux parties prenantes de prévoir et de planifier des ressources pour les mises à jour nécessaires de leurs environnements.

Objectif
Maintenir une fréquence constante de fourniture du correctif aux parties prenantes.

Résultat
Les parties prenantes peuvent planifier et déployer le correctif.

Sous-fonction 4.1.3.1 Fréquence de mise en œuvre du correctif

Collaborer avec les équipes de gestion des produits et de gestion du lancement pour déterminer la fréquence de mise en œuvre d'un correctif. Certains correctifs sont intégrés lors du lancement d'une fonctionnalité et seront donc alignés sur son calendrier de lancement. D'autres produits peuvent nécessiter un correctif d'urgence, ce qui est considéré comme une publication hors bande.

Sous-fonction 4.1.3.2 Recenser les exceptions

Identifier et recenser les exceptions dans le cadre desquelles un correctif n'est pas mis en œuvre selon la fréquence normale.

Service 4.2 Correction

Ce service, qui porte sur la gestion des vulnérabilités signalées par les découvreurs, comprend l'analyse de l'intervention ainsi que des mesures d'atténuation, et définit les versions qui seront corrigées. Il peut également tenir compte de la façon dont le correctif sera mis en œuvre. Par ailleurs, ce service peut prendre compte des solutions de repli pouvant être immédiatement appliquées par la partie prenante avant que le correctif ne soit mis en œuvre.

Objectif
Indiquer à une partie prenante les processus et les bonnes pratiques relatifs à la mise en œuvre d'un correctif en fonction du ou des produits, des versions et des parties prenantes affectées.

Résultat
Un correctif compatible avec les produits affectés et les besoins des parties prenantes.

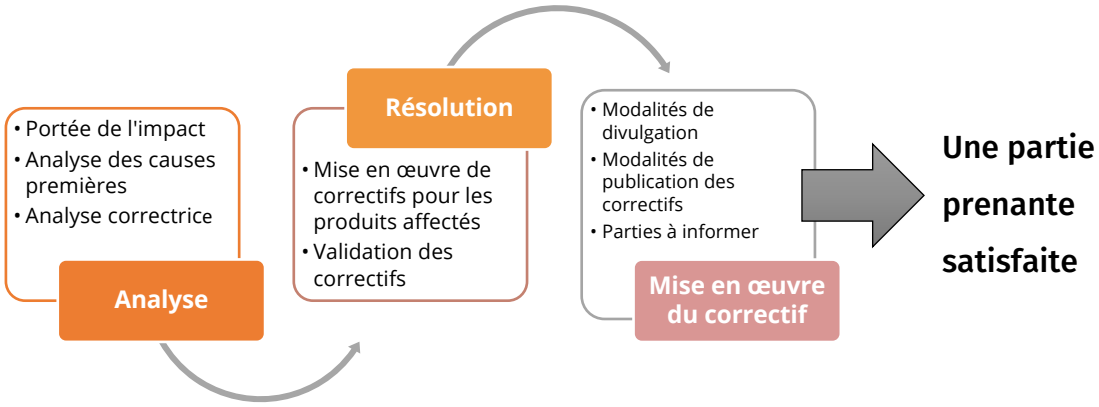


Figure 13: Processus de correction de la vulnérabilité signalée

Fonction 4.2.1 Analyse

Le produit affecté peut comprendre une seule application logicielle, un micrologiciel ou plusieurs programmes disposant de différentes versions du logiciel ou du micrologiciel. Un certain nombre de paramètres doivent être pris en comptes lors de l'élaboration d'un plan de correction pour s'assurer que les besoins de vos parties prenantes sont satisfaits.

Objectif
Identifier les produits, les versions et les parties prenantes affectés.

Résultat
Un correctif compatible avec les produits affectés et les besoins des parties prenantes.

Sous-fonction 4.2.1.1 Valider la vulnérabilité

Valider le rapport de vulnérabilité ou l'incident en fonction au regard du seuil de qualité ou de l'échelle de bogues. Voir la *Fonction 3.1.1 Seuil de qualité et échelles de bogues.*

Sous-fonction 4.2.1.2 Corriger les versions des produits

Déterminer les produits et les versions affectés ainsi que les variantes éventuelles qu'il faudra peut-être corriger en même temps.

Sous-fonction 4.2.1.3 Examiner les accords d'assistance

Examiner les accords d'assistance et les modèles associés aux versions des produits affectés. Se reporter à la *Sous-fonction 4.1.1.2 Modèles d'assistance*.

Sous-fonction 4.2.1.4 Analyse des causes premières

Comprendre la faille de conception ou de mise en œuvre à l'origine de la vulnérabilité.

Sous-fonction 4.2.1.5 Déterminer le mécanisme de rejet d'une vulnérabilité

Par exemple, une vulnérabilité peut être un faux positif ou une faille de conception de sécurité.

Sous-fonction 4.2.1.6 Analyse correctrice

Déterminer les moyens d'atténuer ou de corriger les risques suscités par la vulnérabilité.

Sous-fonction 4.2.1.7 Solutions de repli temporaire

Déterminer si des solutions de repli peuvent être mises en œuvre afin d'atténuer la vulnérabilité pendant l'élaboration d'un correctif.

Sous-fonction 4.2.1.8 Exceptions

Déterminer les éventuelles exceptions au titre desquelles une vulnérabilité ne peut être corrigée. Se reporter à la *Fonction 4.2.4 Processus de gestion des risques.*

Fonction 4.2.2 Résolution au moyen d'un correctif

Avant de publier un correctif pour corriger une vulnérabilité signalée, il convient de le valider par le biais d'un processus d'assurance qualité, par une évaluation de la sécurité, et, le cas échéant, par le découvreur ayant signalé la vulnérabilité. Cette fonction décrit les processus et les mécanismes de validation interne du correctif ainsi que le partenariat avec le découvreur afin de valider et d'approuver un correctif.

Objectif
Mettre en place un processus et un mécanisme de validation interne du correctif ainsi qu'un partenariat avec le découvreur afin d'approuver le correctif, le cas échéant.

Résultat
Approbation par le découvreur interne et/ou externe du correctif qui sera publié.

Sous-fonction 4.2.2.1 Valider les vulnérabilités signalées qui ont été corrigées.

Valider pour veiller à ce que tous les cas de la vulnérabilité signalée aient été corrigés dans l'ensemble des versions des produits affectés.

Sous-fonction 4.2.2.3 Approbation du correctif

Obtenir l'approbation du correctif par l'ingénieur ou l'équipe d'assurance qualité responsable. La validation du correctif doit être intégrée aux pratiques courantes de test/d'assurance qualité.

Sous-fonction 4.2.2.4 Valider le correctif avec les découvreurs

Collaborer avec les parties prenantes ou les découvreurs tiers en vue de la validation du correctif.

Fonction 4.2.3 Mise en œuvre du correctif

Dans le cadre de la publication d'un correctif visant à corriger une vulnérabilité signalée, les délais de divulgation peuvent varier en fonction des exigences opérationnelles de votre organisation. Par exemple, certaines divulgations peuvent coïncider lorsque les correctifs sont disponibles, d'autres peuvent survenir une fois les correctifs publiés, en particulier si ces derniers ont été échelonnés ou, dans certains cas, la priorité peut être donnée aux divulgations en fonction des relations avec les parties prenantes (notamment s'il s'agit de partenaires ou d'entités essentielles). Néanmoins, les principales parties prenantes du secteur doivent être tenues informées des délais.

Objectif
Les divulgations sont planifiées en fonction des correctifs et les parties prenantes sont tenues informées de ces délais.

Résultat
Fournir un correctif parallèlement à la divulgation aux parties prenantes.

Sous-fonction 4.2.3.1 Type de divulgation

Choisir le mécanisme de divulgation de la vulnérabilité le plus adapté. Ce choix peut être fondé sur le type de vulnérabilité ou sa gravité.

Sous-fonction 4.2.3.2 Coordonner la divulgation, le cas échéant

Sous-fonction 4.2.3.3 Inscrire le correctif dans la base de données interne

Collaborer avec le service d'assistance de la partie prenante ou d'autres parties prenantes pour publier le correctif sur le portail web, le site du service d'assistance de la partie prenante ou l'intégrer à l'approbation de version finale (Release to Manufacturing, RTM) par exemple.

Sous-fonction 4.2.3.4 Divulguer le correctif

Collaborer avec le service d'assistance de la partie prenante ou avec les parties prenantes pour divulguer la vulnérabilité signalée.

Fonction 4.2.4 Processus de gestion des risques

Il incombe à la PSIRT de fournir aux parties prenantes suffisamment d'informations afin qu'elles soient en mesure d'évaluer les risques menaçant leurs systèmes en raison de vulnérabilités dans ces derniers et dans les produits pris en charge par l'organisation dont relève la PSIRT. Des évaluations de gestion des risques doivent être réalisées dans l'ensemble de l'organisation lorsqu'une vulnérabilité n'est pas corrigée dans un délai spécifique (conformément aux accords sur le niveau de service ou aux objectifs). Il convient ainsi de disposer d'un mécanisme transparent pour quantifier le risque et de remonter jusqu'aux parties prenantes appropriées figurant dans le registre des risques de l'organisation.

Objectif
Définir un processus d'acceptation formelle des risques à l'égard de toute vulnérabilité non corrigée conformément aux délais exigés dans les accords sur le niveau de service internes.

Résultat
Dans l'ensemble de l'organisation, la transparence à l'égard des risques et l'assurance que ces derniers sont remontés et reconnus de façon appropriée.

Sous-fonction 4.2.4.1 Rôles d'autorité

Déterminer les rôles ayant l'autorité nécessaire pour accepter le risque, par exemple, le responsable de la sécurité des systèmes d'information (CISO)/responsable principal de la sécurité (CSO) ou le gestionnaire des risques, lesquels rôles doivent être informés du risque.

Sous-fonction 4.2.4.2 Définir le processus de gestion des risques

Adopter des pratiques de gestion des risques afin d'assurer le traitement et la maîtrise des risques au sein de l'organisation, et fixer l'ensemble des conditions à réunir pour déclencher le processus.

Sous-fonction 4.2.4.3 Évaluer et quantifier les risques

Évaluer et quantifier les risques en conduisant une évaluation des risques afin de comprendre la menace et les impacts pour l'entreprise.

Sous-fonction 4.2.4.4 Documenter les risques et le registre des risques

Aider le CSO, le gestionnaire des risques ou d'autres parties prenantes dans le suivi de l'état de l'évaluation des risques et, ultérieurement, dans la mise en œuvre des recommandations.

Sous-fonction 4.2.4.5 Recommandations

Mettre à jour le registre des risques en y intégrant les découvertes et les recommandations.

Service 4.3 Traitement des incidents

La PSIRT doit disposer d'un mécanisme pour accélérer les délais de correction afin de traiter les "vulnérabilités critiques" qui peuvent être qualifiées d'exploits actifs en liberté, de vulnérabilités nouvelles et de divulgations publiques non coordonnées. Ce service fournit des orientations relatives à l'incident, tout en alertant les parties prenantes et en coordonnant les activités associées à l'intervention et à l'atténuation d'un incident ainsi qu'au rétablissement, en vue de réduire les délais entre le rapport et la mise en œuvre du correctif.

Objectif
Mettre au point un plan de gestion des vulnérabilités critiques et renforcer les capacités de mobilisation de l'ensemble des ressources requises pour les traiter.

Résultat
Mise en œuvre de correctifs d'urgence en vue de la divulgation imminente ou publique d'une vulnérabilité ou de toute autre situation dans le cadre de laquelle les parties prenantes peuvent être exposées à des risques et une action rapide est requise.

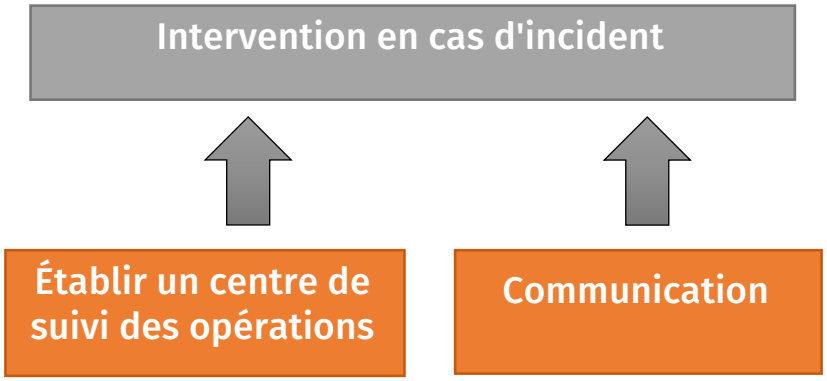


Figure 14: Traitement des incidents:

Fonction 4.3.1 Établir un centre de suivi des opérations

Lorsqu'un incident doit être géré, établir un centre de suivi des opérations englobant la PSIRT, les équipes juridique, de communication, de développement, d'assistance des parties prenantes, le fournisseur et d'autres rôles selon les besoins. Il peut s'agir d'un lieu physique ou virtuel tant que toutes les parties sont disponibles pour intervenir en toute sécurité, selon les besoins. Généralement, des options de rassemblement aussi bien physique qu'à distance sont nécessaires pour garantir la participation des parties prenantes. Les ressources doivent être déterminées à l'avance afin de soutenir de façon appropriée le processus de gestion des incidents.

Objectif
Veiller à ce que les parties prenantes soient disponibles pour répondre aux questions et fournir des orientations. Garantir que les ressources appropriées ont été assignées pour gérer l'incident.

Résultat
Organiser les ressources approuvées.

Sous-fonction 4.3.1.1 Plan de gestion des incidents

Mettre au point un plan de gestion des vulnérabilités critiques et renforcer les capacités de mobilisation de l'ensemble des ressources requises pour les traiter. Il convient de réaliser une session de préparation aux interventions en cas d'incident afin de confirmer l'aptitude de ce plan à gérer les urgences et les événements imprévus.

Sous-fonction 4.3.1.2 Déterminer les ressources requises pour traiter et gérer l'incident

Ces ressources peuvent inclure les salles de réunions, les lignes privées et du personnel supplémentaire. Pour ce qui est de la gestion d'incident de longue durée, la fourniture de nourriture et la mise à disposition d'hébergements doivent être envisagées.

Sous-fonction 4.3.1.3 Intégrer les parties prenantes au plan d'intervention en cas d'incident

Identifier toutes les parties prenantes clés devant participer à la gestion de l'incident dans le cadre de votre plan d'intervention en cas d'incident. Identifier toutes les parties prenantes clés devant participer à la gestion de l'incident dans le cadre de votre plan d'intervention en cas d'incident. Voir les sections *Service 1.1 Gestion des parties prenantes internes* et *Service 1.5 Communications relatives aux incidents*.

Sous-fonction 4.3.1.4 Assigner des rôles et des responsabilités clairs pour gérer l'incident

Les membres du personnel doivent connaître leurs rôles et le déroulement des opérations lorsqu'une intervention doit avoir lieu. Une formation et des exercices théoriques doivent être menés afin de préparer les participants clés de l'intervention.

Fonction 4.3.2 Gestion des incidents

Lorsqu'un incident est déclaré, l'objectif principal de la PSIRT, en partenariat avec ses parties prenantes, est de réduire les effets de l'incident et de travailler à la restauration de la fonction opérationnelle d'un produit et de ses parties prenantes.

Objectif
Créer un programme stratégique et mettre en œuvre un plan pour contenir l'incident.

Résultat
Restaurer les opérations des équipes de produits et des parties prenantes dès que possible.

Sous-fonction 4.3.2.1 Collecte des informations

Recueil, catalogage, et stockage des informations relatives à l'incident.

Sous-fonction 4.3.2.2 Analyse

Le traitement des incidents est étroitement lié aux activités d'analyse, qui sont définies dans la partie "Analyses".

Sous-fonction 4.3.2.3 Intervention

Services visant à réduire les effets d'un incident et à rétablir les fonctions opérationnelles des parties prenantes.

Sous-fonction 4.3.2.4 Suivi de l'incident

Recensement des informations relatives aux mesures prises en vue de résoudre un incident, y compris les informations essentielles collectées, les analyses réalisées, les mesures de correction et d'atténuation appliquées, l'achèvement et la résolution.

Sous-fonction 4.3.2.5 Procédure de réunion d'enquête après incident

Réflexion menée après l'application des mesures afin d'identifier les améliorations devant être apportées aux processus, politiques, procédures, ressources et outils dans le but de faciliter l'atténuation et de prévenir de futurs dangers.

Fonction 4.3.3 Plan de communication

Toutes les parties prenantes et les responsables des actions doivent connaître les plans les plus récents et les progrès accomplis pour rester sur la bonne voie. Mobiliser la direction si nécessaire afin d'éliminer les éventuels obstacles susceptibles d'empêcher une communication collaborative ouverte en cas d'incident.

Objectif
Mettre au point un plan de communication et désigner un point de contact central pour l'incident qui sera chargé de tenir toutes les parties informées de l'évolution de la situation.

Résultat
Organiser une communication étudiée.

Sous-fonction 4.3.3.1 Publication d'informations à destination des parties prenantes internes

Gestion des listes utilisées pour les annonces, les alertes, les flux de données et d'autres publications visant à apprécier la situation.

Sous-fonction 4.3.3.2 Les relations publiques sont bien gérées et coordonnées

Veiller à ce que les informations soient transmises aux médias et aux parties prenantes, mais uniquement par le biais des canaux autorisés de l'organisation. Il peut s'agir notamment de publications sur les médias sociaux.

Sous-fonction 4.3.3.3 Communiquer les activités de rétablissement

Les parties prenantes internes, les cadres et les équipes de gestion doivent connaître les activités de rétablissement.

Sous-fonction 4.3.3.4 Collecter des retours d'informations sur la réunion d'enquête après incident

Les réunions d'enquête après incident sont menées par la PSIRT et des retours d'information sont recueillis afin d'améliorer l'intervention ainsi que les activités du cycle de développement sécurisé (SDL) (par exemple, quelle activité du SDL aurait pu ou aurait dû empêcher le problème en premier lieu?).

Service 4.4 Mesures relatives à la communication des vulnérabilités

Les données requises doivent inclure, entre autres, le nombre de problèmes, la classification, le délai de correction, les produits ou services affectés.

Objectif
Collecter des données régulièrement pour l'élaboration de rapports de gestion.

Résultat
Déterminer les domaines nécessitant une analyse, des ressources et des améliorations.

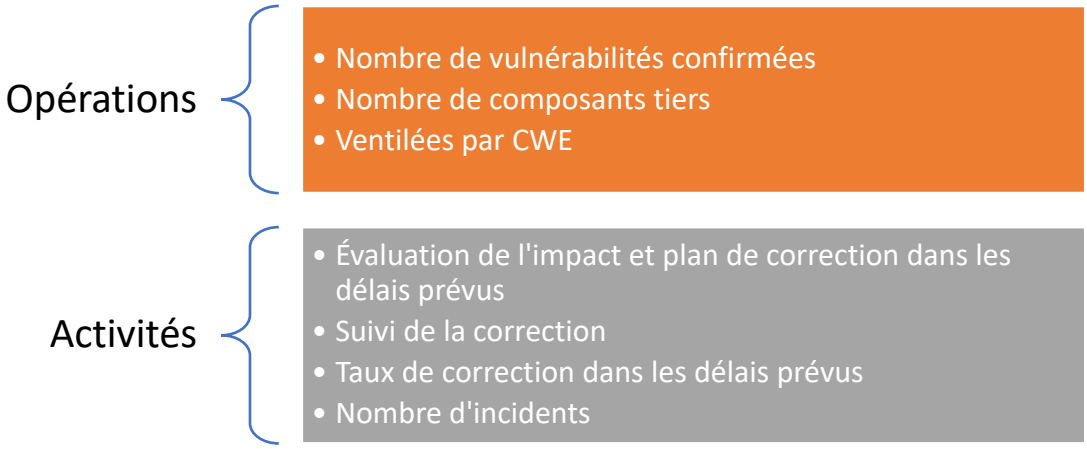


Figure 15: Mesures relatives aux opérations et aux activités

Fonction 4.4.1 Rapports opérationnels

Les rapports opérationnels fournissent des informations sur le volume et le type de vulnérabilités signalées et confirmées au sein des différents produits et versions. Ces rapports doivent être publiés régulièrement en interne au sein de la PSIRT ainsi qu'avec les parties prenantes internes.

Objectif
Collecter des données régulièrement pour l'élaboration de rapports généraux.

Résultat
Déterminer les domaines nécessitant une analyse, des ressources et des améliorations.

Sous-fonction 4.4.1.1 Nombre total de vulnérabilités signalées par rapport aux vulnérabilités confirmées (par produit/unité opérationnelle)

Ces données permettent de rendre compte du volume de vulnérabilités gérées par une PSIRT du point de vue des ressources.

Sous-fonction 4.4.1.2 Nombre total de vulnérabilités confirmées ventilées par composant tiers

Ces données permettent de rendre compte du risque associé à des composants tiers intégrés spécifiques.

Sous-fonction 4.4.1.3 Nombre total de vulnérabilités confirmées ventilées par CWE (par produit/unité opérationnelle)

Ces données peuvent être alimentées en amont du cycle de développement sécurisé et influer sur la formation et l'apprentissage.

Fonction 4.4.2 Rapports d'activité

Les rapports d'activité fournissent des informations sur l'état des capacités de riposte aux vulnérabilités d'une organisation.

Objectif
Établir des mesures du niveau de réussite de l'organisation à l'égard du respect des engagements assortis d'échéances fixées dans les accords sur le niveau de service. Collecter, analyser et communiquer régulièrement les données mesurant le degré d'accomplissement de ces objectifs.

Résultat
Création d'un tableau de bord mettant en avant les réussites et les possibilités d'amélioration.

Sous-fonction 4.4.2.1 Évaluation de l'impact dans les délais prévus

Cet indicateur indique le degré d'efficacité des équipes de produits dans la réalisation d'évaluations de l'impact conformément aux délais fixés au sein du SLA.

Sous-fonction 4.4.2.2 Plan de correction dans les délais prévus

Cet indicateur indique le degré d'efficacité des équipes de produits dans l'élaboration d'un plan de correction conformément aux délais fixés au sein du SLA.

Sous-fonction 4.4.2.3 Suivi de la correction

Cet indicateur indique le degré d'efficacité des équipes de produits dans l'application d'une correction conformément aux délais fixés au sein du SLA.

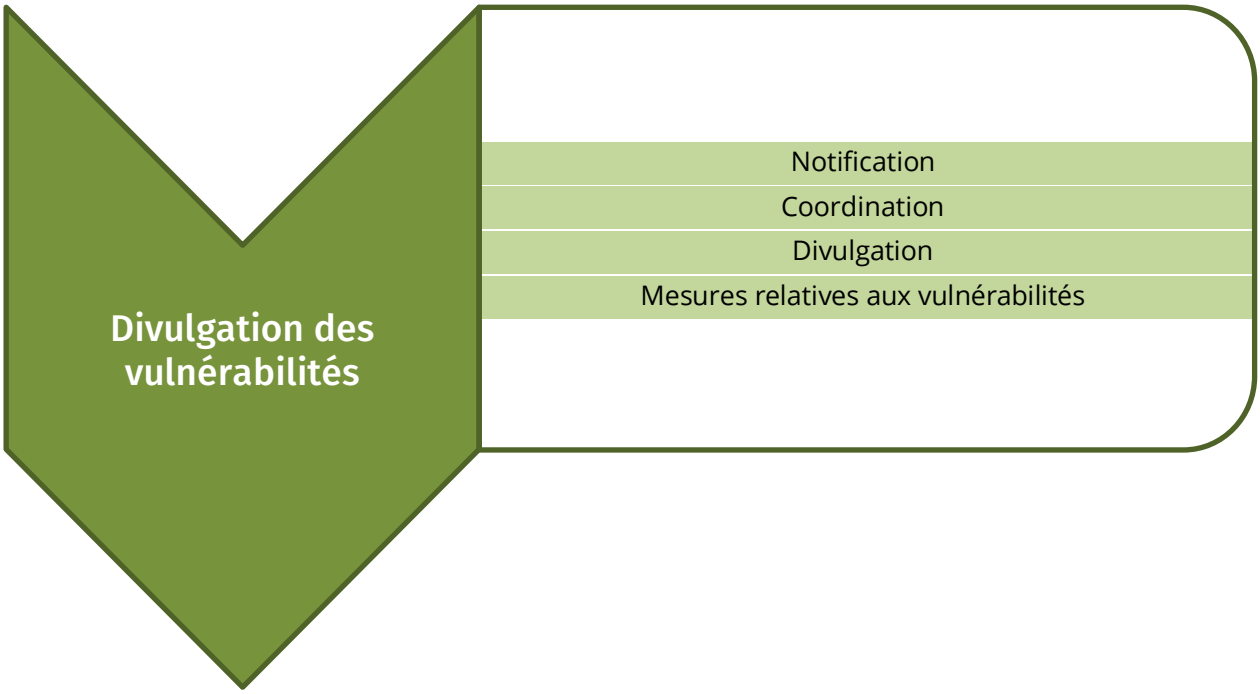
Sous-fonction 4.4.2.4 Taux de correction dans les délais prévus

Cet indicateur indique le degré d'efficacité des équipes de produits dans le respect des objectifs généraux ou des accords pour ce qui est de l'application d'une correction entre le moment de remise du rapport et la mise en œuvre d'un correctif. Ces données peuvent être ventilées par gravité ou par type de vulnérabilité (gamme de produits, type de vulnérabilité).

Sous-fonction 4.4.2.5 Nombre d'incidents

Ces données rendent compte des risques auxquels est exposée l'organisation.

Zone de service 5 Divulgation des vulnérabilités



Il importe de créer un environnement transparent et collaboratif au sein duquel les fournisseurs, les coordonnateurs et les découvreurs peuvent partager des informations avec leurs parties prenantes et entre eux, tout en discutant des plans de divulgation mutuellement acceptables. Une telle collaboration permet de répondre aux besoins principaux, à savoir: la résolution des vulnérabilités, la protection des parties prenantes et la reconnaissance des découvreurs. Le fournisseur doit publier sa politique de divulgation des vulnérabilités afin que les coordonnateurs, d'autres fournisseurs et les découvreurs puissent s'y référer.

Figure 16: Processus de notification des vulnérabilités

Objectif

Faire preuve de transparence vis-à-vis des parties prenantes et des partenaires en collaborant avec les découvreurs, les coordonnateurs et les fournisseurs en aval afin de divulguer de façon responsable les vulnérabilités et les correctifs.

Résultat

Une confiance et une collaboration renforcées, ainsi qu'une divulgation contrôlée.

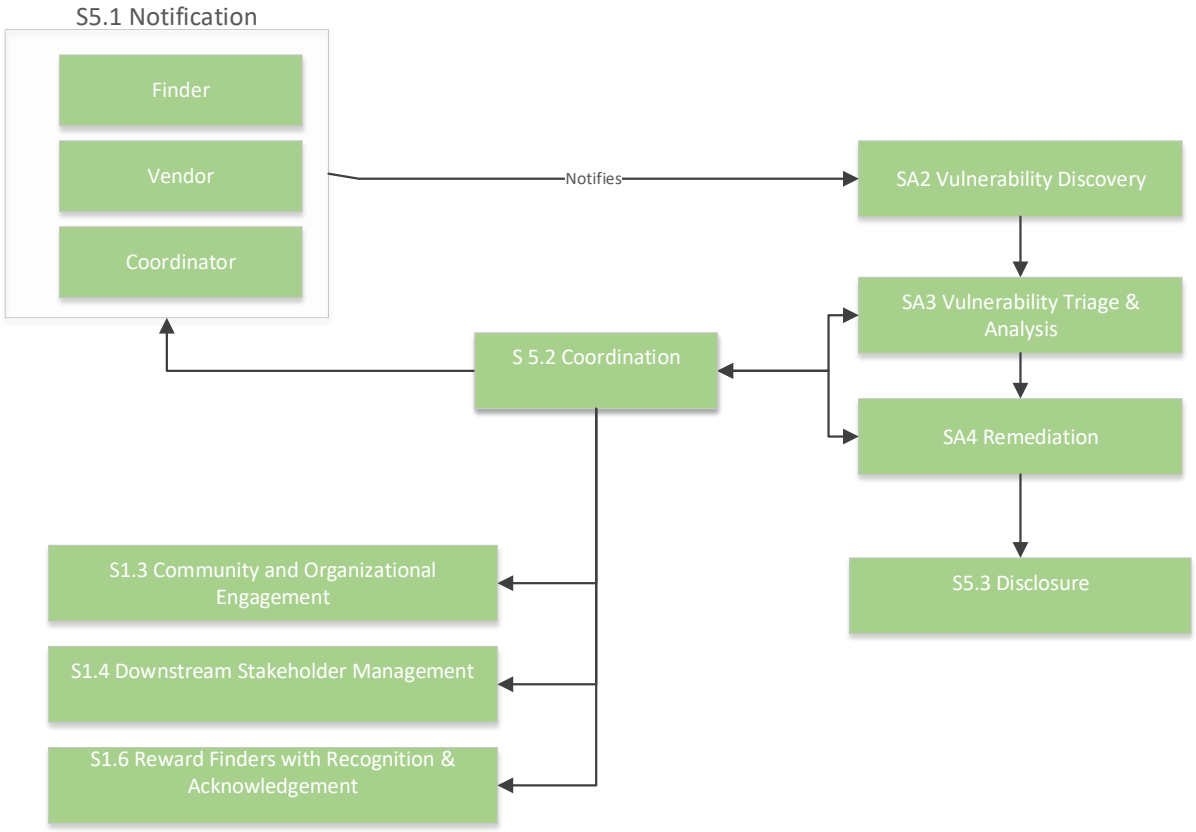


Figure 17: Exemple de haut niveau de coordination des vulnérabilités

Légende de la Figure 17:

S5.1 Notification

Découvreur
Fournisseur
Coordonnateur Notifie SA2 Découverte des vulnérabilités
SA3 Tri et analyse des vulnérabilités S5.2 Coordination
SA4 Correction

S1.3 Participation de la communauté et de l'organisation S5.3 Divulgation
S1.4 Gestion des parties prenantes en aval
S1.6 Reconnaissance et distinction des découvreurs

Service 5.1 Notification

Ce service consiste à déterminer le processus de notification approprié pour fournir en temps opportun des informations relatives à la stratégie d'atténuation, aux correctifs, et aux solutions de repli aux parties prenantes afin que celles-ci soient tenues informées et puissent planifier leurs actions en conséquence. Dans certains cas, des accords contractuels peuvent exister entre les fournisseurs. Par exemple, un fournisseur en amont pourrait être tenu d'informer un fournisseur en aval de vulnérabilités divulguées ou d'incidents connus. Le processus de notification entend garantir que l'ensemble des parties prenantes et des fournisseurs sont en mesure de cerner et gérer les risques inhérents à la vulnérabilité.

Objectif
Faire preuve de transparence vis-à-vis des fournisseurs et des découvreurs à travers la collaboration.

Résultat
Une confiance et une collaboration renforcées avec les découvreurs.

Fonction 5.1.1 Fournisseur intermédiaire (fournisseur en aval)

Un fournisseur intermédiaire, tel qu'un OEM ou un partenaire, peut concevoir et/ou produire une pièce, un sous-système ou un logiciel utilisés dans le produit final d'un autre fournisseur. En de pareils cas, leur équipe PSIRT doit prendre des dispositions pour partager les informations relatives aux vulnérabilités avec les fournisseurs. Les politiques de gestion des vulnérabilités des différents fournisseurs doivent être connues. Parfois, ces attentes sont indiquées dans un accord contractuel. Le délai pour la correction et la divulgation doit être négocié au plus tôt.

Objectif
Créer un environnement de collaboration et définir des attentes claires entre l'OEM et les partenaires et d'autres fournisseurs.

Résultat
Une confiance et une collaboration renforcées, ainsi qu'une divulgation contrôlée entre toutes les parties concernées.

Sous-fonction 5.1.1.1 Signalement par les PSIRT auprès des fournisseurs intermédiaires

Les PSIRT peuvent être mises au courant des vulnérabilités signalées par leurs parties prenantes, et doivent informer la PSIRT du fournisseur intermédiaire desdites vulnérabilités.

Sous-fonction 5.1.1.2 Signalement par le fournisseur intermédiaire

Un fournisseur intermédiaire approvisionnant un fournisseur en composants ou outils peut être mis au courant de vulnérabilités lui étant directement signalées, et doit en informer les PSIRT de ses fournisseurs.

Sous-fonction 5.1.1.3 Accords contractuels

Les PSIRT doivent identifier l'ensemble de leurs fournisseurs intermédiaires et envisager de collaborer avec l'équipe juridique afin de s'assurer de l'ajout de clauses aux accords contractuels pour garantir une intervention opportune face aux vulnérabilités.

Sous-fonction 5.1.1.4 Notification des PSIRT aux parties prenantes

Les PSIRT des fournisseurs peuvent informer leurs parties prenantes, en particulier si le fournisseur intermédiaire n'est pas en mesure de remédier à la vulnérabilité ou s'il met un temps excessif à la corriger. Dans certains cas, la PSIRT d'un fournisseur peut appliquer un processus de notification différencié et informer les parties prenantes qui seraient le plus affectées par la vulnérabilité en question.

Fonction 5.1.2 Coordonnateurs

Une PSIRT peut demander à un coordonnateur de participer en informant les autres fournisseurs ainsi qu'en coordonnant le calendrier d'application du correctif vis-à-vis de leurs bulletins, en particulier si de nombreux fournisseurs sont concernés. Les coordonnateurs tels que le CERT Coordination Center (Centre de coordination des équipes d'intervention en cas d'urgence informatique, CERT/CC)[12]ou des coordinateurs tiers apportent une valeur ajoutée en amenant un large éventail d'organisations à coopérer et collaborer dans le cadre de la prise en charge d'une vulnérabilité.

Objectif
Il peut être demandé aux coordonnateurs d'intervenir et d'aider l'organisation de la PSIRT à communiquer et à collaborer sur la vulnérabilité avec l'ensemble des fournisseurs.

Résultat
Une confiance et une collaboration renforcées, ainsi qu'une divulgation contrôlée entre toutes les parties concernées.

Sous-fonction 5.1.2.1 Identification des coordonnateurs

Référencer et cerner les différents coordonnateurs en fonction de la politique de divulgation des vulnérabilités.

Sous-fonction 5.1.2.2 Mobilisation des coordonnateurs

Collaborer avec un coordonnateur pour s'assurer que l'ensemble des PSIRT des fournisseurs affectés ont été informées.

[12] www.cert.org

Fonction 5.1.3 Découvreurs

Un découvreur, tel qu'un client ou un chercheur tiers, peut informer une PSIRT d'une vulnérabilité par le biais des canaux documentés dans la *zone de service 2 Découverte de vulnérabilités.*

Objectif
Créer un environnement de collaboration et définir des attentes claires avec les découvreurs.

Résultat
Une confiance et une collaboration renforcées, ainsi qu'une divulgation contrôlée avec les découvreurs.

Services 5.2 Coordination

Le cas échéant, la PSIRT d'un fournisseur doit prendre des dispositions pour partager les informations relatives aux vulnérabilités avec les coordonnateurs ou d'autres fournisseurs. La politique de gestion des vulnérabilités du fournisseur doit être connue. Les délais pour la correction et la divulgation doivent être négociés au plus tôt.

Objectif
Documenter les vulnérabilités qui ont été retirées du produit grâce à la correction.

Résultat
Davantage de clarté concernant i) l'avantage que représente la mise en œuvre du correctif et, ii) les moyens de se procurer ledit correctif.

Fonction 5.2.1 Coordination bilatérale

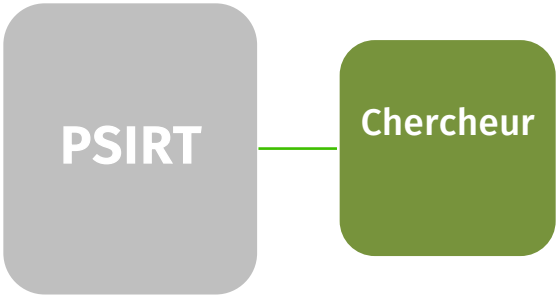


Figure 18: Coordination bilatérale

La PSIRT d'un fournisseur est tenue de maintenir la communication avec les découvreurs qui signalent des vulnérabilités potentielles. Il est important pour les fournisseurs de comprendre les intentions du découvreur et sa position générale à l'égard des vulnérabilités, afin d'encourager et de faciliter une divulgation coordonnée dans les délais convenus. Les PSIRT doivent penser à distinguer les découvreurs qui adhèrent à la divulgation publique.

Objectif
Créer un environnement collaboratif au sein duquel les découvreurs savent qu'ils seront pris au sérieux.

Résultat
Un plan de divulgation négocié qui honore les efforts déployés par le découvreur.

Sous-fonction 5.2.1.1 Réception du rapport

Accuser réception du rapport de vulnérabilité auprès d'un découvreur tiers.

Sous-fonction 5.2.1.2 Mises à jour régulières

Fournir régulièrement au découvreur des mises à jour sur le statut de la vulnérabilité signalée.

Sous-fonction 5.2.1.3 Validation par le découvreur

Fournir le correctif au découvreur afin qu'il puisse le valider également.

Sous-fonction 5.2.1.4 Reconnaissance du découvreur

Distinguer le découvreur ayant signalé la vulnérabilité en reconnaissant ses contributions. Le fournisseur doit vérifier avec le découvreur que la récompense est acceptable.

Fonction 5.2.2 Coordination entre plusieurs fournisseurs

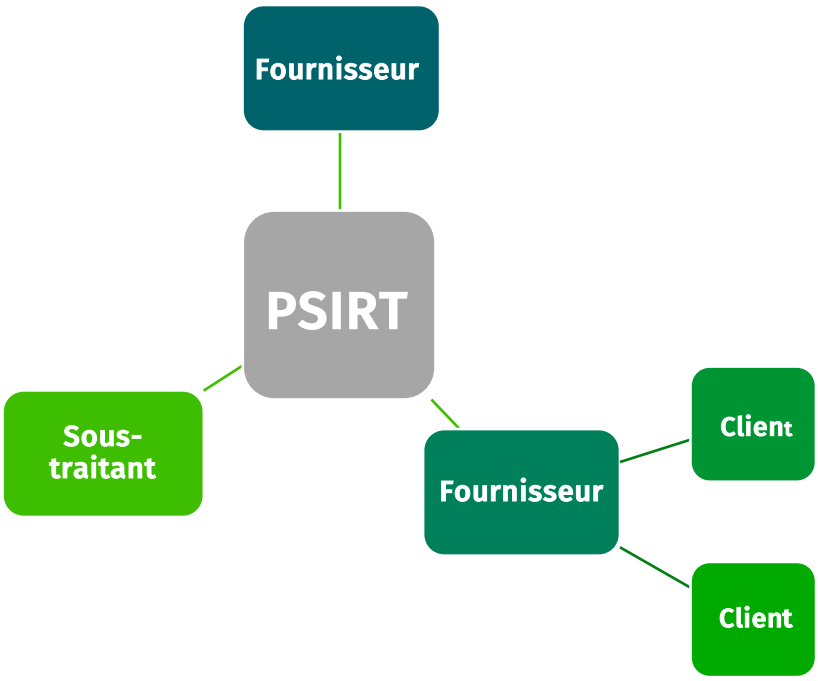


Figure 19: Coordination entre plusieurs fournisseurs

Le cas échéant, la PSIRT d'un fournisseur doit prendre des dispositions pour partager les informations relatives aux vulnérabilités avec les coordonnateurs ou d'autres fournisseurs. La politique de gestion des vulnérabilités du fournisseur doit être connue. Les délais pour la correction et la divulgation doivent être négociés au plus tôt.

Objectif
Faire preuve de transparence vis-à-vis des parties prenantes et des partenaires en collaborant avec l'ensemble des parties afin de divulguer de façon responsable les vulnérabilités et la correction.

Résultat
Une confiance et une collaboration renforcées, ainsi qu'une divulgation contrôlée.

Parties prenantes multiples	Caractéristiques de la relation	Enjeu de la coordination
Fournisseurs en amont	L'OEM fournit la technologie.	Pour fournir un correctif, il est conseillé aux fournisseurs en amont de gérer leurs parties prenantes en aval (voir le *Service 1.4*).
Fournisseurs en aval	Réception des technologies du fournisseur en amont.	Être informé pour appliquer le correctif de sécurité. Il est conseillé aux fournisseurs en aval de déterminer les communautés de fournisseurs en amont et les

Tableau 1: Exemple de coordination multipartite

Sous-fonction 5.2.2.1 Réception du rapport

Le fournisseur de la PSIRT accuse réception du rapport de vulnérabilité transmis par le fournisseur ou le coordonnateur.

Sous-fonction 5.2.2.2 Identification des fournisseurs affectés

Le coordonnateur ou le fournisseur de la PSIRT doivent peut-être identifier les fournisseurs concernés par le rapport de vulnérabilité.

Sous-fonction 5.2.2.3 Partage d'informations relatives aux vulnérabilités

Le coordonnateur ou le fournisseur de la PSIRT partagent les informations relatives aux vulnérabilités avec les différents fournisseurs.

Sous-fonction 5.2.2.4 Planification de la publication du correctif

Le coordonnateur ou le fournisseur de la PSIRT collaborent avec les fournisseurs sur les délais et la disponibilité des corrections, et sur la façon dont les fournisseurs en aval peuvent recevoir le correctif.

Sous-fonction 5.2.2.5 Validation du correctif

Le coordonnateur ou le fournisseur de la PSIRT valident avec les fournisseurs la prise en charge de la vulnérabilité par la correction de sécurité.

Sous-fonction 5.2.2.6 Coordination de la divulgation

Le coordonnateur ou le fournisseur de la PSIRT négocient avec l'ensemble des fournisseurs pour convenir de la manière dont la vulnérabilité sera divulguée et du moment auquel la divulgation sera rendue publique.

Service 5.3 Divulgation

Lorsqu'une correction de sécurité est publiée, des divulgations appropriées doivent être effectuées afin de s'assurer que les parties prenantes et les fournisseurs sont bien informés de la correction. Pour chacune de ces divulgations, le public doit être bien défini (différents types d'annonces peuvent concerner différents types de publics).

Objectif
Documenter les modifications apportées au code et la publication des corrections de sécurité.

Résultat
Davantage de clarté concernant les correctifs appliqués au code et les moyens de se procurer lesdits correctifs.

Fonction 5.3.1 Notes de version

Les notes de version, qui intègrent un fichier Lisez-moi et un historique des modifications, doivent comprendre une ou plusieurs références à la CVE pour le correctif. Les notes de version doivent clairement indiquer la manière dont la vulnérabilité a été prise en charge.

Objectif
Indiquer les correctifs compris dans le code mis à jour.

Résultat
Les parties prenantes peuvent se protéger contre une possible exposition à la vulnérabilité.

Sous-fonction 5.3.1.1 Divulgation des notes de version

Définir les vulnérabilités qui doivent être divulguées dans les notes de version.

Sous-fonction 5.3.1.1 Examen des notes de version

Définir le processus d'examen.

Sous-fonction 5.3.1.2 Approbations des notes de version

Effectuer un examen de la divulgation et approuver cette dernière.

Fonction 5.3.2 Bulletins de sécurité

Les fournisseurs doivent disposer d'un mécanisme leur permettant de publier des bulletins de sécurité à l'intention des parties prenantes sur une page web publique et de divulguer les vulnérabilités qui ont été corrigées.

Objectif
Fournir un répertoire public pour les bulletins de sécurité publiés.

Résultat
Les bulletins de sécurité peuvent être consultés à des fins d'examen et d'intervention par la partie prenante.

Sous-fonction 5.3.2.1 Modèle de bulletin

Définir un modèle de bulletin de sécurité normalisé. Inclure l'intitulé, le résumé, la ou les CVE, l'impact et le statut du produit pris en charge, les reconnaissances, les références et l'historique des révisions.

Sous-fonction 5.3.2.2 Méthode de publication du bulletin

Déterminer le mécanisme de publication du bulletin de sécurité, y compris, entre autres, le document web, le flux RSS, ou l'abonnement.

Sous-fonction 5.3.2.3 Format du bulletin

Afin que les parties prenantes et les intervenants puissent consulter les bulletins à l'aide d'outils automatisés, envisager de publier les bulletins dans un format déchiffrable par les machines, tel que le Common Security Advisory Framework[13] (Cadre commun des annonces de sécurité, CSAF).

Sous-fonction 5.3.2.4 Déclencheurs des bulletins

Définir l'ensemble de conditions à réunir pour déclencher la publication d'un bulletin de sécurité. Par exemple, dans les cas où une mesure doit être prise pour informer les parties prenantes de la correction d'un environnement hébergé (scénario d'atteinte à la sécurité).

Sous-fonction 5.3.2.5 Attribution de la CVE

Déterminer le processus d'attribution d'un identifiant CVE à la vulnérabilité.

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

Sous-fonction 5.3.2.6 Reconnaissance du découvreur

Déterminer si le découvreur souhaite une reconnaissance ou une distinction publique.

Sous-fonction 5.3.2.7 Planification de la divulgation

Définir le processus d'examen (identité des parties prenantes et période d'élaboration de la divulgation).

Sous-fonction 5.3.2.8 Processus d'examen des bulletins

Conduire un processus d'examen avec les parties prenantes définies.

Fonction 5.3.3 Articles fondés sur des connaissances

Le fournisseur doit disposer d'un mécanisme pour publier des articles fondés sur des connaissances qui peuvent accompagner certaines corrections de sécurité pour des vulnérabilités dont la gravité est jugée faible. Ce mécanisme peut autrement être utilisé comme un moyen de détailler les raisons motivant le rejet de vulnérabilités spécifiques signalées comme étant de faux positifs.

Objectif
Fournir un répertoire d'articles fondés sur des connaissances.

Résultat
Les articles fondés sur des connaissances peuvent être consultés à des fins d'examen et d'intervention par la partie prenante.

Sous-fonction 5.3.3.1 Divulgation des articles fondés sur des connaissances

Définir les vulnérabilités qui doivent être divulguées dans un article fondé sur des connaissances.

Sous-fonction 5.3.3.2 Examen des articles fondés sur des connaissances

Définir le processus d'examen.

Sous-fonction 5.3.3.3 Approbation des articles fondés sur des connaissances

Effectuer un examen de la divulgation et approuver cette dernière.

Fonction 5.3.4 Communication avec les parties prenantes internes

Outre les chefs d'entreprise qui doivent être informés des plans de communication relatifs aux vulnérabilités, de nombreux employés travaillent en première ligne avec les parties prenantes, que ce soit en personne ou par téléphone, chaque jour. La communication d'informations confidentielles approfondies et la publication d'une Foire aux questions en prévision des bulletins à venir préparent les personnes susceptibles d'être sollicitées une fois qu'ils auront été publiés.

Objectif
Informer les chefs d'entreprise, les services de communication internationale et les employés en contact direct avec les parties prenantes des annonces "à venir" et des réponses approuvées.

Résultat
Les employés seront en mesure de répondre aux parties prenantes et aux médias qui leur poseront des questions le jour de la publication du bulletin, ce qui leur permettra de contrôler le message.

Sous-fonction 5.3.4.1 Mobilisation des parties prenantes internes

Collaborer avec les parties prenantes internes pour élaborer et/ou examiner le discours que leurs équipes doivent employer lorsque les clients les questionnent à propos de la vulnérabilité.

Service 5.4 Mesures relatives aux vulnérabilités

Les données à collecter doivent comprendre, entre autres, la quantité de problèmes, la classification, le délai de correction, les produits ou services affectés.

Objectif
Collecter des données régulièrement pour l'élaboration de rapports de gestion.

Résultat
Déterminer les domaines nécessitant une analyse, des ressources et des améliorations.

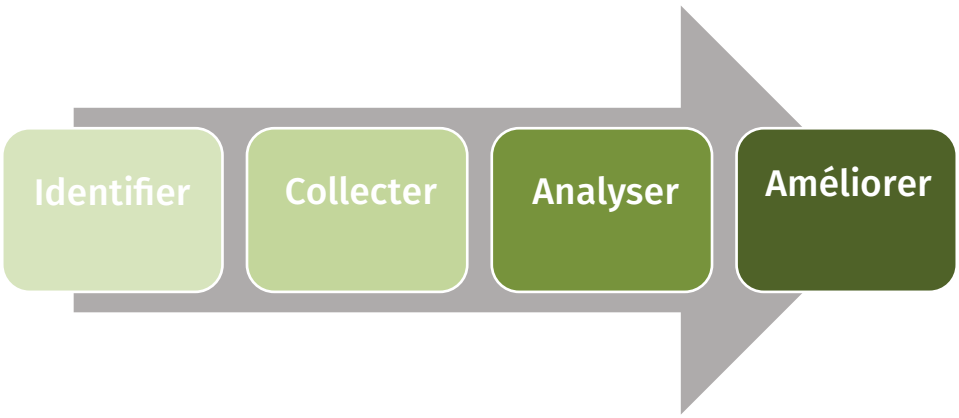


Figure 20: Processus concernant les mesures relatives aux vulnérabilités

Fonction 5.4.1 Rapports opérationnels

Les rapports opérationnels peuvent fournir des informations supplémentaires sur le volume de divulgations publiées ainsi que sur le nombre de consultations des pages concernées. Ces rapports doivent être publiés régulièrement en interne au sein de la PSIRT et à l'intention des parties prenantes internes.

Objectif

Collecter des données régulièrement pour l'élaboration de rapports généraux.

Résultat

Déterminer les domaines nécessitant une analyse, des ressources et des améliorations.

Sous-fonction 5.4.1.1 Nombre de bulletins de sécurité publiés

Le nombre de divulgations différentes peut être rapporté et ventilé par produit. Cela peut contribuer à amener l'équipe à se voir assigner une ressource technique.

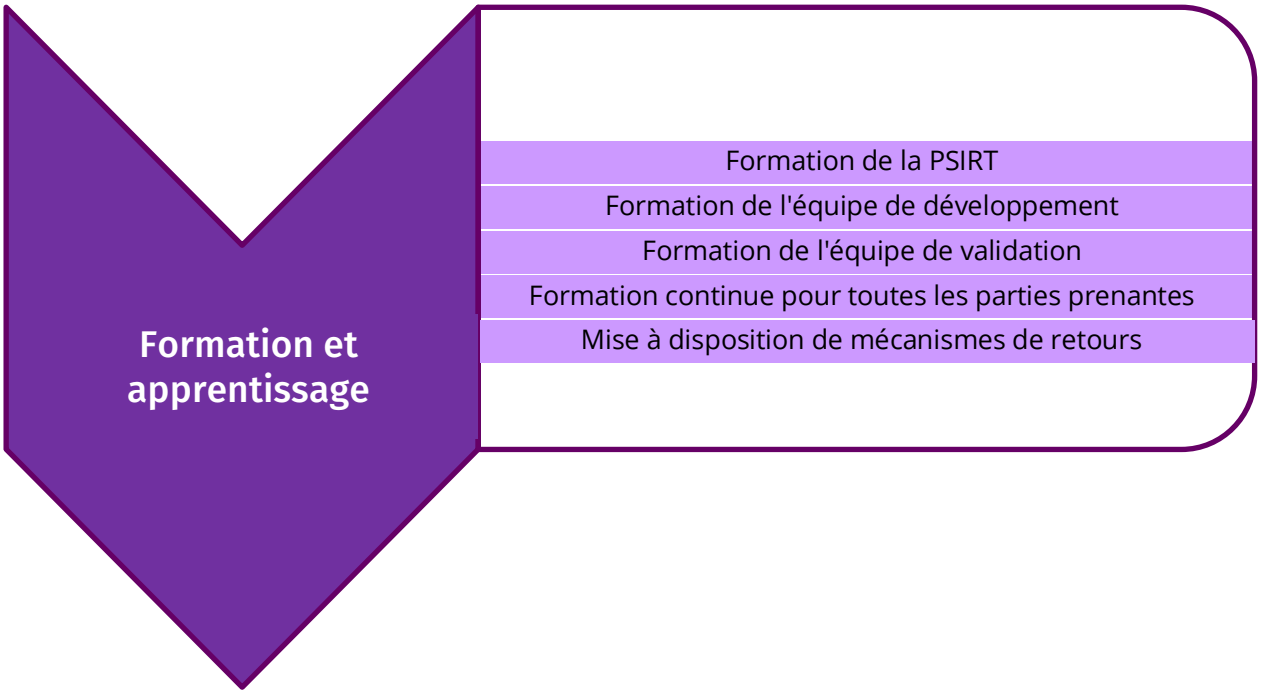
Sous-fonction 5.4.1.2 Nombre de CVE publiées dans la NVD

Le nombre de CVE attribuées peut servir à promouvoir votre statut auprès d'une autorité de numérotation CVE (CNA).

Sous-fonction 5.4.1.3 Nombre de consultations des bulletins de sécurité

Cet indicateur peut encourager une stratégie en faveur d'une notification proactive si le volume de parties prenantes consultant votre bulletin est faible.

Zone de service 6 Formation et apprentissage



Le secteur de la sécurité des produits est en constante évolution, les nouvelles technologies, les services et l'intégration faisant de la formation continue et de l'apprentissage une priorité absolue pour les professionnels de la sécurité. Étant donné que les logiciels imprègnent notre quotidien de mille et une façons, des voitures aux réfrigérateurs, la satisfaction des besoins de sécurisation des produits n'a jamais été aussi importante. Les PSIRT jouent un rôle clé en soutenant un programme éducatif solide pour sensibiliser toutes les parties prenantes aux complexités de l'élaboration, de la validation, et de la fourniture de produits/services conformes aux normes en vigueur dans notre monde connecté.

Les besoins en formation et en apprentissage peuvent varier au sein d'une organisation. Les préoccupations d'un développeur de micrologiciels sont très différentes de celles d'un développeur de services logiciels et exigent souvent des types de formation très spécifiques et uniques. Dans le cadre du présent document, nous répartirons les besoins de formation selon quatre groupes de parties prenantes: les PSIRT, les équipes de développement des produits, les équipes de validation des produits et d'autres parties prenantes participant au processus suivi par la PSIRT.

1. La **formation de la PSIRT** est unique étant donné que ses membres sont affiliés à différents secteurs (service juridique, communication, développement, etc.).
2. **L'équipe de développement des produits** (ingénieurs et développeurs internes): Les développeurs nécessitent une formation dans leurs domaines spécifiques, qui se matérialise par un apprentissage ciblé. L'élaboration de micrologiciels sécurisés, très difficiles à mettre à jour sur le terrain, présente des exigences très différentes de celles s'appliquant à un ingénieur spécialisé dans les applications de bureau.

3. **L'équipe de validation des produits** (ingénieurs et développeurs internes): Les validateurs requièrent une formation continue afin de se familiariser avec les outils et techniques les plus récents pour des activités telles que le test de pénétration, l'analyse de vulnérabilité, et les examens préalables de conception pour déceler des problèmes avant qu'ils ne nécessitent une correction.
4. **Toutes les autres parties prenantes**: ce groupe représente un public moins spécialisé qui nécessite des bases solides en matière de développement, de validation et de fourniture de produits sûrs, ainsi que dans l'intervention en cas de vulnérabilité affectant le produit fourni.

La formation au développement sécurisé, qui n'est pas considérée comme faisant partie du programme de la PSIRT, est traitée en dehors du processus de la PSIRT. Toutefois, il est important que les PSIRT appuient toutes les dimensions de la fourniture de produits sécurisés sur le marché et, à ce titre, collaborent avec différentes équipes de développement pour garantir qu'une formation appropriée est en place. Dans de nombreuses organisations de taille plus réduite, il se peut que la responsabilité consistant à s'assurer que les produits sont élaborés dans une optique de sécurité ne relève pas d'un groupe distinct. Dans ce cas, il peut incomber à la PSIRT de combler ce manque (cette fonction n'entre pas dans le champ du présent document).

Dans chaque section, nous allons identifier différents groupes de parties prenantes et résumer certains domaines cibles qui peuvent aider une PSIRT à participer à des discussions utiles sur la formation et l'apprentissage de ses parties prenantes. Pour former ces dernières, les PSIRT peuvent créer l'ensemble des supports de formation en interne, utiliser des supports externes ou avoir recours à des ressources de formation extérieures.

Service 6.1 Formation de la PSIRT

Le personnel de la PSIRT doit être à l'avant-garde des enjeux liés à la sécurité, entre autres, les tendances, les nouveaux exploits, et les activités du secteur. L'acquisition de connaissances générales commence par des bases solides en lien avec le monde de la sécurité, comme le démontrent les principales certifications en matière de sécurité. Toutefois, les certifications ne fournissent qu'une base qui doit être constamment mise à jour par le biais d'activités, telles que des conférences axées sur la sécurité, la participation à un consortium du secteur, et une connaissance approfondie du secteur dans son ensemble, se traduisant par la lecture assidue de blogs, de la presse du secteur, de publications de consortiums, etc. Les membres de la PSIRT doivent également être au fait de la législation en matière de confidentialité et du monde de la sécurité en constante évolution.

Fonction 6.1.1 Formation technique

Il importe que le personnel de la PSIRT ait une bonne compréhension des concepts de sécurité de base ainsi qu'une connaissance approfondie des produits pris en charge. Les supports de formation doivent être régulièrement révisés afin de s'assurer que, à mesure que le paysage de la sécurité évolue, ils intègrent de nouvelles techniques relatives aux vulnérabilités.

Objectif
Former le personnel de la PSIRT de sorte qu'il comprenne le problème signalé et puisse dument effectuer le tri initial avant de faire remonter ledit problème aux équipes responsables de l'élaboration, de l'évaluation et de la publication des correctifs.

Résultat
Le personnel de la PSIRT se prévaut d'une formation technique suffisante pour exercer ses fonctions.

La formation aux concepts de sécurité varie en fonction du type de produits pris en charge par un fournisseur (par exemple, matériel informatique, micrologiciels, logiciels, mise en réseau, produits dans le nuage, ou l'ensemble de ce qui précède). À un très haut niveau, la formation doit couvrir des thèmes essentiels en matière de sécurité, notamment les attaques courantes, la cryptographie, la confidentialité, l'intégrité, la disponibilité, l'authentification, l'autorisation, les modèles de contrôle d'accès, les utilisateurs multiples, la conformité ou encore les réglementations. Cette formation doit également comprendre toutes les réglementations propres au secteur susceptible d'influer sur les activités de la PSIRT, telles que l'HIPAA (loi américaine sur l'assurance maladie) pour les services de santé et la PCI DSS (norme de sécurité de l'industrie des cartes de paiement) pour les fournisseurs de cartes de paiement et le secteur bancaire. Par ailleurs, un certain niveau de formation liée au produit doit être assuré pour permettre au personnel de la PSIRT de comprendre les problèmes signalés.

Fonction 6.1.2 Formation à la communication

Étant donné que les découvreurs externes signalent les problèmes à la PSIRT, il est important que cette dernière soit formée aux politiques de communication et qu'elle acquière des compétences pratiques relatives à la gestion des communications avec les découvreurs externes et les parties prenantes internes de façon opportune.

Objectif
Veiller à ce que le personnel de la PSIRT suive les politiques de communication de l'organisation tout en interagissant avec des entités externes, ce qui permet d'éliminer les éventuels problèmes d'ordre réglementaire/juridique pouvant découler d'une mauvaise communication.

Résultat
Le personnel de la PSIRT disposera d'une formation suffisante en matière de communication pour exercer les fonctions attribuées en démontrant une précision et une clarté exemplaires.

Fonction 6.1.3 Formation aux processus

Des directives relatives aux processus doivent être établies pour définir la façon dont les problèmes signalés seront suivis, gérés et mesurés. Les rôles des différentes parties prenantes participant au processus de résolution des problèmes signalés doivent être précisés. Le processus doit couvrir la réponse aux découvreurs en temps opportun et l'envoi régulier de mises à jour à ces derniers pour tous les problèmes en cours. Un moyen sécurisé et bien défini doit également être mis en place pour communiquer les informations entre un découvreur externe et le fournisseur.

Objectif
Veiller à un flux d'information régulier dans la gestion des incidents de sécurité relatifs aux produits qui donneront lieu à une résolution des problèmes en temps opportun.

Résultat
Le personnel de la PSIRT sera suffisamment formé sur les processus internes pour exercer ses fonctions.

Fonction 6.1.4 Formation aux outils

Sous-fonction 6.1.4.1 Suivi des bogues et autres outils de gestion à destination de la PSIRT et des ingénieurs

Un outil de suivi des bogues formellement reconnu doit être déterminé pour chaque produit (de préférence le même pour tous les produits) dans une organisation donnée. Tous les bogues doivent être détectés par le biais de cet outil et les bogues de sécurité doivent être uniformément identifiés en tant que tels. Seules les personnes ayant besoin d'être informées doivent être habilitées à consulter les informations relatives aux vulnérabilités de sécurité liées à un produit. En outre, l'outil doit répondre aux exigences programmatiques de mesure en disposant de capacités de signalement manuelles et automatisées.

Objectif
Veiller à ce que les problèmes fassent l'objet d'un suivi efficace et que les informations relatives aux vulnérabilités soient sauvegardées par des outils de suivi certifiés, auxquels seules les personnes à même de justifier leur demande peuvent traiter, suivre et gérer ces problèmes.

Résultat
Le personnel de la PSIRT sera suffisamment formé et informé sur les outils pour exercer ses fonctions.

Sous-fonction 6.1.4.2 Outils de suivi tiers

La majorité des produits comprennent de nombreux composants tiers (dont des composants en accès libre) avec lesquels ils sont fournis. Souvent, les clients ne sont pas au courant des logiciels tiers fournis avec le produit et dépendent ainsi du fournisseur pour l'application de correctifs ou la transmission d'informations sur le correctif. Il est important d'identifier des outils de suivi tiers internes afin de couvrir les dépendances des produits du fournisseur à l'égard des différents composants tiers. La Base de données nationale des failles (NVD), les annonces de sécurité des fournisseurs tiers et d'autres sites externes doivent être surveillés pour suivre les vulnérabilités et les corrections relatives aux composants tiers de sorte que ces correctifs puissent être fournis au client.

Objectif
Identifier des outils pour effectuer un suivi des composants tiers intégrés à des produits afin que les vulnérabilités détectées au sein de ces composants puissent être suivies et publiées.

Résultat
Le personnel de la PSIRT dispose des connaissances et des moyens nécessaires pour assurer le suivi des composants tiers intégrés aux produits fournis.

Fonction 6.1.5 Suivi de l'ensemble des initiatives de formation

Les PSIRT doivent effectuer un suivi de l'ensemble des formations proposées aux parties prenantes. L'équipe doit s'assurer que toutes ces formations sont mises en œuvre à une certaine fréquence, le paysage de la sécurité évoluant très rapidement. En conséquence, les formations et les processus doivent être continuellement ajustés.

Objectif
Veiller à ce que toutes les formations à destination des différentes parties prenantes fassent l'objet d'un suivi.

Résultat
Le personnel de la PSIRT saura que différentes parties prenantes ont été formées quant à leur rôle au sein du processus de la PSIRT.

Service 6.2 Formation de l'équipe de développement

Le développement sécurisé désigne les méthodologies et les mesures adoptées tout au long du processus de développement qui visent particulièrement à réduire le nombre de vulnérabilités et leur gravité s'agissant des produits et services logiciels. Grâce à un programme de formation approprié et à un enseignement centré sur les méthodologies de développement sécurisé, les vulnérabilités peuvent être sensiblement réduites avant la sortie du produit, ce qui s'avère moins coûteux qu'une gestion des manquements a posteriori, une fois que les produits ont été lancés sur le marché.

Le développement sécurisé commence par la prise en compte des exigences et de l'architecture propres aux produits. Par ailleurs, les examens de conception s'intéressant à la sécurité sont essentiels pour détecter de possibles vulnérabilités avant même que le produit n'entre en phase de développement.

De nombreuses activités sont menées dans le cadre d'un programme de développement sécurisé, dont les tenants et les aboutissants dépassent largement le cadre du présent document. Il est fortement recommandé de disposer d'un programme distinct pour moduler les efforts relatifs au cycle de développement sécurisé. Ce programme doit suivre un modèle de programme standard accepté par le secteur[14]. Le modèle de Cycle de développement sécurisé de Microsoft constitue un exemple de cycle de développement sécurisé.

Objectif
Encourager l'organisation à disposer d'un programme de cycle de développement sécurisé (SDL) lui étant propre et dans le cadre duquel les équipes de développement sont formées à l'appui de directives de sécurité étayées, tout en prenant en charge l'architecture et la conception d'un produit.

Résultat
Les équipes de développement seront capables d'élaborer un code sécurisé et de lancer des produits plus sûrs.

[14] https://www.microsoft.com/en-us/sdl/

La formation au développement sécurisé, qui n'est pas toujours considérée comme faisant partie de la PSIRT, peut être traitée en dehors du processus de la PSIRT. Dans tous les cas, il s'agit d'une étape importante qui doit être prise en compte par tout fournisseur soucieux de la sécurité de ses produits.

Fonction 6.2.1 Formation au processus de la PSIRT

Chaque membre du processus de développement doit comprendre les raisons sous-tendant l'existence du processus de la PSIRT, son fonctionnement, et les actions à entreprendre pour développer les produits en vue d'appuyer ledit processus. En règle générale, après le lancement d'un produit, les équipes de développement passent à des projets différents et on observe un relâchement de l'effort. La formation des équipes et la transmission des méthodes appropriées ayant trait à la conservation des informations clés du produit sont essentielles pour que la PSIRT prenne en charge les problèmes de vulnérabilités dans leur intégralité. Il convient de documenter les informations, telles que l'identité de l'architecte de la sécurité, du responsable du développement, et du responsable de l'évaluation afin que la PSIRT puisse revenir vers les personnes indiquées pour évaluer les risques et mettre au point des atténuations. Cette documentation doit également comprendre les thèmes suivants: les composants tiers utilisés, le processus de mise à jour du produit, les journaux existants, les exceptions de sécurité permises ou encore les moyens de notification des parties prenantes. Ces renseignements sont en outre essentiels pour que la PSIRT puisse clôturer un cas de vulnérabilité de sécurité. À mesure que de nouveaux membres arrivent et que d'autres quittent leurs fonctions, des formations de perfectionnement s'avèrent fondamentales.

Objectif
Veiller à ce que toutes les parties prenantes comprennent le processus de la PSIRT et son lien avec leur rôle dans le développement des produits.

Résultat
Une culture de la sécurité parmi les développeurs et une meilleure coopération dans le traitement des vulnérabilités.

Service 6.3 Formation de l'équipe de validation

Les validateurs doivent être constamment tenus à jour des outils et techniques les plus récents concernant les activités suivantes: le test de pénétration, l'analyse des vulnérabilités, le test à données aléatoires, le piratage éthique, etc. La formation des validateurs sur ces sujets relève du SDL et n'entre pas dans le cadre du présent document. Toutefois, la PSIRT doit encourager l'organisation à mettre en place un groupe traitant ces domaines.

Objectif
Encourager l'organisation à disposer d'un programme de SDL lui étant propre et dans le cadre duquel des outils d'évaluation pertinents sont identifiés.

Résultat
Des produits de meilleure qualité et plus sûrs.

Tout comme le développement sécurisé, la formation à la validation sécurisée, qui n'est pas considérée comme faisant partie de la PSIRT, est traitée en dehors du processus de la PSIRT.

Toutefois, il s'agit d'une étape tout aussi importante qui doit être couverte dans le cadre du SDL d'un produit par un fournisseur.

Fonction 6.3.1 Formation au processus de la PSIRT

Certains membres de l'équipe de validation peuvent prendre part à l'évaluation des correctifs requis pour résoudre les vulnérabilités détectées sur un produit. Ils doivent comprendre le processus de la PSIRT, son fonctionnement, les délais escomptés et leur rôle au sein de ce processus. Ils ont besoin de bien comprendre le cycle de vie du produit afin de connaître les versions prises en charge qui doivent être évaluées en vue de la correction des vulnérabilités. Ils doivent également analyser les solutions de repli, le cas échéant. Enfin, il sera important pour eux de tester les régressions.

Objectif
Veiller à ce que toutes les parties prenantes comprennent le processus de la PSIRT et son lien avec leur rôle dans la validation des produits.

Résultat
Une culture de la sécurité parmi les validateurs et une meilleure coopération dans le traitement des vulnérabilités.

Service 6.4 Formation continue pour toutes les parties prenantes

Toutes les parties prenantes nécessitent un certain niveau de formation et de sensibilisation au programme de la PSIRT. De nombreuses parties prenantes participent au processus de la PSIRT de bout en bout. Par conséquent, il est important d'identifier les différents groupes de parties prenantes et d'élaborer des formations répondant à leurs besoins spécifiques.

Objectif
Veiller à ce que toutes les parties prenantes disposent de la formation ou des connaissances de base nécessaires à l'exercice de leur rôle au sein du programme de la PSIRT.

Résultat
Des parties prenantes internes bien informées qui sont au fait i) des modalités de travail futures avec la PSIRT concernant la gestion des problèmes de vulnérabilité émergents, et ii) des services que la PSIRT proposera dans ces situations.

Fonction 6.4.1 Formation de la direction

Ce groupe est généralement impliqué dans l'approbation définitive des politiques de l'entreprise relatives à la communication, à la protection contre les vulnérabilités et autres. L'approbation de la direction peut également être nécessaire pour la création de bulletins de sécurité. Par ailleurs, l'approbation des dirigeants est souvent requise pour les situations critiques qui engendrent des risques élevés, une haute visibilité ou une responsabilité significative. La direction souhaitera peut-être aussi mettre en place des vérifications régulières du statut de sécurité de l'ensemble des produits. C'est pourquoi il est important de l'informer des processus de la PSIRT.

Objectif
Informer les équipes de direction de leur rôle au sein du programme de la PSIRT.

Résultat
Une résolution en temps opportun des approbations nécessitant l'aval de la direction.

Fonction 6.4.2 Formation de l'équipe juridique

L'équipe juridique prend part à l'élaboration des politiques initiales de l'entreprise. Certaines vulnérabilités signalées par des découvreurs peuvent présenter des problèmes touchant à la responsabilité et exiger ainsi l'aide des services juridiques; il importe donc d'identifier les points de contact au préalable.

Objectif
Informer les équipes juridiques de leur rôle au sein du programme de la PSIRT et des délais impartis.

Résultat
Une clôture en temps opportun des problèmes de sécurité exigeant l'approbation de l'équipe juridique.

Fonction 6.4.3 Formation de l'équipe en charge des affaires gouvernementales et de la conformité

Les personnes en charge des affaires gouvernementales sont concernées par les problèmes touchant à la conformité réglementaire. Il importe ainsi d'identifier les points de contact au préalable.

Objectif
Informer l'équipe en charge des affaires gouvernementales de son rôle au sein du programme de la PSIRT.

Résultat
Une résolution en temps opportun des vulnérabilités de sécurité exigeant de se conformer à certaines normes réglementaires.

Fonction 6.4.4 Formation de l'équipe marketing

L'équipe marketing est généralement impliquée lorsqu'il existe un risque pour l'image de marque. Par ailleurs, les bulletins de sécurité peuvent être examinés par cette équipe et des informations marketing connexes peuvent être publiées en parallèle. Les équipes marketing prennent également part au marketing au niveau des enjeux de sécurité des produits.

Objectif
Informer les équipes marketing de leur rôle au sein du programme de la PSIRT et les former sur les éventuelles réclamations relatives à la sécurité des produits.

Résultat
Une coordination adéquate entre la PSIRT et les équipes marketing favorisera un positionnement externe cohérent en matière de sécurité entre les supports marketing et les bulletins de sécurité.

Fonction 6.4.5 Formation de l'équipe des relations publiques

Les équipes des relations publiques peuvent être tenues de répondre aux publications de sécurité ou blogs externes, ou aux demandes de la presse à l'égard des vulnérabilités critiques d'un produit. Les points de contact doivent être identifiés afin que ces équipes puissent être impliquées si des publications externes sont requises.

Objectif
Informer les équipes des relations publiques de leur rôle au sein du programme de la PSIRT.

Résultat
Une coordination adéquate entre la PSIRT et les équipes des relations publiques favorisera un positionnement externe favorable de la part du fournisseur en matière de sécurité.

Fonction 6.4.6 Formation de l'équipe de vente

Les équipes de vente peuvent être formées aux concepts de sécurité de base et aux communications s'agissant des pratiques en matière de sécurité. De même, il est capital que le personnel de vente connaisse les éléments pouvant ou non être partagés avec l'extérieur. Il est recommandé que les employés de vente fassent remonter toute préoccupation formulée à l'égard de la sécurité par les parties prenantes/les clients potentiels au personnel de la PSIRT ou au personnel d'assistance plutôt que de les traiter directement.

Objectif
Informer les équipes de vente concernant i) les éventuelles réclamations pouvant survenir en lien avec la sécurité des produits, et ii) les interlocuteurs à solliciter pour toute question à laquelle elles ne peuvent répondre.

Résultat
Une coordination adéquate entre la PSIRT et les équipes de vente permettra de satisfaire les attentes des clients.

Fonction 6.4.7 Formation de l'équipe d'assistance

Les équipes d'assistance doivent être formées au traitement des signalements de vulnérabilité transmis par les clients. La PSIRT peut être impliquée dans certains cas du fait des missions connexes qui lui incombent. L'équipe d'assistance doit publier des politiques définissant la durée de vie de chaque produit et les versions prises en charge, et précisant si des bulletins de sécurité seront publiés ou non. La majorité des fournisseurs transmettent uniquement des bulletins de sécurité pour les versions couvertes par un service d'assistance. C'est pourquoi ces politiques sont essentielles et doivent être publiées sur le site web du fournisseur, afin de les rendre facilement accessibles aux parties prenantes. Les PSIRT entretiennent généralement une relation étroite avec les équipes d'assistance afin de comprendre le type de problèmes signalés par les clients. Il peut arriver qu'un découvreur soit

également un client, aussi le traitement du problème peut-il alterner entre l'équipe d'assistance et la PSIRT.

Objectif
Informer les équipes d'assistance de leur rôle au sein du processus de la PSIRT.

Résultat
Une coordination adéquate entre les équipes de la PSIRT et d'assistance permettra de satisfaire les attentes des clients et des auteurs du signalement.

Service 6.5 Mise à disposition de mécanismes de retours d'informations

Utiliser les informations collectées lors de l'analyse des causes premières de l'incident afin de former les personnes concernées et d'éviter la résurgence de vulnérabilités similaires.

Objectif
Améliorer continuellement la formation afin de se tenir au fait de l'évolution rapide du paysage de la sécurité.

Résultat
Une formation de meilleure qualité se traduira par une expérience améliorée pour l'ensemble des parties prenantes.

ANNEXE 1: Ressources

- Architecture Content Framework[15].
- ISO 31000:2009 Gestion des risques – Principes et lignes directrices[16]
- ISO/IEC 27000/2018 *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information*
- ISO/IEC 30111:2013 Technologies de l'information – Techniques de sécurité – Processus de traitement de la vulnérabilité[17]
- ISO/IEC 29147:2014 Technologies de l'information – Techniques de sécurité – Divulgation des vulnérabilités[18]
- Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure[19].
- The Project Management Body of Knowledge (PMBOK) Guide and Standards.

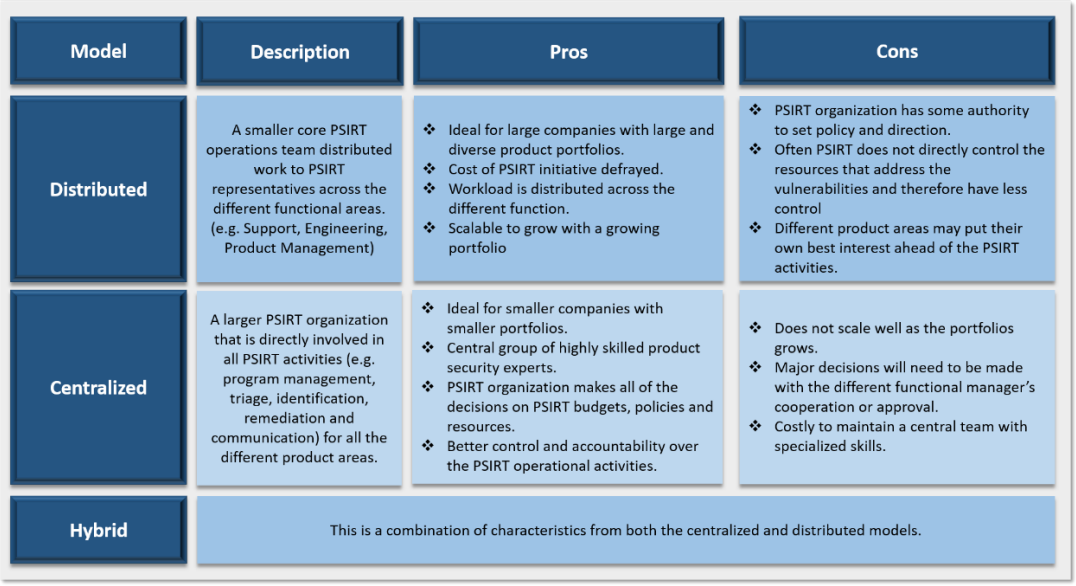
[15] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html
[16] https://www.iso.org/fr/iso-31000-risk-management.html
[17] https://www.iso.org/obp/ui/#iso:std:53231:en
[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en
[19] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

ANNEXE 2: Remerciements

- Barbara Cosgriff, MetLife
- Beverly Finch, Lenovo
- Carl Denis, Siemens
- Chris Robinson, Red Hat
- Jeff Hahn, Honeywell
- Jerry Bryant, Intel
- Josh Dembling, Intel
- Jean-Robert Hountomey, Broadcom
- Kevin Ryan, NetApp
- Langley Rock, Red Hat
- Lisa Bradley, Dell Technologies
- Peter Allor, Red Hat
- Reshma Banerjee, Oracle
- Rupert Wimmer, Siemens
- Shawn Richardson, NVIDIA
- Steve Brukbacher, Johnson Controls
- Tania Ward, Dell Technologies
- Vic Chung, SAP

Annexe 3: Tableaux et illustrations

Annexe 4: Avantages et inconvénients des modèles organisationnels de PSIRT



Model	Description	Pros	Cons
Distributed	A smaller core PSIRT operations team distributed work to PSIRT representatives across the different functional areas. (e.g. Support, Engineering, Product Management)	❖ Ideal for large companies with large and diverse product portfolios. ❖ Cost of PSIRT initiative defrayed. ❖ Workload is distributed across the different function. ❖ Scalable to grow with a growing portfolio	❖ PSIRT organization has some authority to set policy and direction. ❖ Often PSIRT does not directly control the resources that address the vulnerabilities and therefore have less control ❖ Different product areas may put their own best interest ahead of the PSIRT activities.
Centralized	A larger PSIRT organization that is directly involved in all PSIRT activities (e.g. program management, triage, identification, remediation and communication) for all the different product areas.	❖ Ideal for smaller companies with smaller portfolios. ❖ Central group of highly skilled product security experts. ❖ PSIRT organization makes all of the decisions on PSIRT budgets, policies and resources. ❖ Better control and accountability over the PSIRT operational activities.	❖ Does not scale well as the portfolios grows. ❖ Major decisions will need to be made with the different functional manager's cooperation or approval. ❖ Costly to maintain a central team with specialized skills.
Hybrid	This is a combination of characteristics from both the centralized and distributed models.		

Modèle	Description	Avantages	Inconvénients
Réparti	■ Une petite équipe PSIRT réduite à ses éléments essentiels dont les tâches sont réparties entre des représentants de la PSIRT dans les différents domaines fonctionnels (par exemple, appui, ingénierie, gestion des produits)	■ Idéal pour les grandes entreprises ayant un portefeuille de produits vaste et diversifié ■ Amortissement du coût de l'initiative PSIRT ■ Répartition de la charge de travail entre les différentes fonctions ■ Bonne adaptation lorsque le portefeuille s'élargit	■ L'organisation PSIRT a une certaine autorité pour fixer la politique et le cap ■ Souvent, la PSIRT ne contrôle pas directement les ressources pour faire face aux vulnérabilités et a donc moins de contrôle ■ Les différents domaines de produits peuvent faire passer leur propre intérêt avant les activités de la PSIRT
Centralisé	■ Une organisation PSIRT de grande taille qui participe directement à toutes les activités de la PSIRT (par exemple gestion du programme, tri, identification, correction et communication) pour tous les différents domaines de produits.	■ Idéal pour les petites entreprises ayant un petit portefeuille ■ Groupe central d'experts hautement qualifiés en matière de sécurité des produits ■ L'organisation PSIRT prend toutes les décisions concernant les budgets, politiques et ressources de la PSIRT ■ Meilleur contrôle et plus grande responsabilité concernant les activités opérationnelles de la PSIRT	■ Adaptation difficile lorsque le portefeuille s'élargit ■ Les décisions importantes devront être prises avec la coopération ou l'approbation des différents responsables fonctionnels ■ Il est coûteux de maintenir une équipe centrale dotée de compétences spécialisées
Hybride	Il s'agit d'une combinaison des caractéristiques du modèle centralisé et du modèle réparti.		

ANNEXE 5: Catégories d'équipes d'intervention en cas d'incident:

- **CSIRT d'entreprise (organisationnelle)** – Généralement, équipe chargée du suivi, de la gestion et du traitement des incidents dans le domaine de la cybersécurité qui touchent les infrastructures et les services TIC d'une organisation en particulier.
- **CSIRT nationale (équipe d'intervention en cas d'incident informatique)** – entité constituée par une autorité nationale afin de coordonner sur le plan national la gestion des incidents dans le domaine de la cybersécurité. Elle est généralement composée de l'ensemble des ministères et agences du gouvernement, les organismes chargés de l'application des lois et la société civile. Il s'agit aussi habituellement de l'interlocuteur privilégié des CSIRT nationales d'autres pays ainsi que des acteurs régionaux et internationaux.
- **CSIRT régionale/multipartite** – Équipe dirigée par un ou plusieurs chefs chargée du suivi, de la gestion et du traitement des incidents dans le domaine de la cybersécurité qui touchent une région en particulier ou un certain nombre d'organisations.
- **CSIRT sectorielle (infrastructures essentielles)** – Équipe chargée du suivi et de la gestion ainsi que du traitement des incidents dans le domaine de la cybersécurité qui touchent un secteur spécifique (par exemple, l'énergie, les télécoms, la finance).
- **Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT)** – Équipe implantée au sein d'une entreprise commerciale (traditionnellement un fournisseur) et chargée de la gestion des informations (réception, enquête, élaboration de rapports internes ou publics) relatives aux failles de sécurité liées aux produits ou aux services commercialisés par cette organisation.

Glossaire

- **Actions** – Description à divers niveaux de détail/maturité du processus suivi pour parvenir à un résultat.
- **"Capabilité"** – Nombre d'occurrences simultanées d'une capacité donnée dans un processus qu'une organisation peut exécuter avant d'épuiser d'une façon ou d'une autre ses ressources.
- **Capacité** – Activité mesurable qui relève des rôles et responsabilités d'une organisation. Dans le cadre de services de la SIRT, les capacités peuvent être définies soit en termes de services, soit en termes de fonctions, sous-fonctions, tâches ou actions requises.
- **Exposition aux vulnérabilités courantes (CVE)** – Liste d'entrées contenant un numéro d'identification, une description et au moins une référence publique à des vulnérabilités publiquement connues.
- **Health Insurance Portability and Accountability Act (Loi sur la transférabilité et la responsabilité de l'assurance maladie, HIPPA)** [20] –Loi promulguée aux États-Unis destinée à fournir des normes de confidentialité pour protéger la confidentialité des dossiers médicaux des patients et d'autres informations relatives à la santé transmises aux régimes de santé, aux médecins, aux hôpitaux et à d'autres prestataires de santé.
- **Indicateur clé de performance (KPI)**[21] – 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.
- **Liste des failles courantes (CWE)**[22] – liste officielle de types de failles créée aux fins suivantes:
  - décrire une faille de sécurité logicielle dans l'architecture, la conception, ou le code, en utilisant le langage courant;
  - servir d'outil de mesure pour les outils de sécurité des logiciels ciblant ces failles;
  - fournir une norme de référence pour les efforts d'identification, d'atténuation, et de prévention des failles.
- **Maturité** – Degré d'efficacité avec lequel une organisation concrétise une capacité donnée dans le cadre de sa mission et de ses pouvoirs. C'est un niveau de maîtrise atteint soit dans les actions et les tâches, soit dans un groupe de fonctions ou de services.
- **Payment Card Industry Data Security Standard (PCI DSS)**[23] – norme relative à la sécurité des informations améliorant la sécurité des données des détenteurs de carte de paiement dans le monde entier.
- **Système d'évaluation des vulnérabilités courantes (CVSS)**[24] – Score numérique indiquant la gravité d'une vulnérabilité.
- **Tâches** – Liste des actions à mener pour effectuer une fonction donnée.

[20] https://www.medicinenet.com/script/main/art.asp?articlekey=31785
[21] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[22] https://cwe.mitre.org/about/index.html
[23] https://www.pcisecuritystandards.org/pci_security/
[24] https://www.first.org/cvss/