# Modèle logique du Fonds Common Good Cyber :

| Produits (Outputs) | Résultats (Outcomes) | Objectif |
|---|---|---|
| **Produit 1.1 :** Fourniture accrue de services de sécurité Internet assurant directement le maintien et la protection des infrastructures critiques.<br>**Produit 1.2 :** Surveillance régulière de la sécurité assurée par les bénéficiaires.<br>**Produit 1.3 :** Partage de renseignements sur les menaces et de bonnes pratiques entre les acteurs de l'écosystème de la cybersécurité. | Résultat 1: Des infrastructures critiques plus sécurisées, maintenues par un écosystème diversifié d'opérateurs de confiance. | Écosystème de cybersécurité renforcé d'organisations à but non lucratif fournissant un soutien plus efficace en matière de cybersécurité, favorisant des conditions propices et répondant aux menaces, y compris la répression transnationale numérique (RTN) |
| **Produit 2.1 :** Soutien en matière de cybersécurité fourni aux utilisateurs à haut risque.<br>**Produit 2.2 :** Conseils pratiques et outils adaptés aux besoins de groupes spécifiques d'utilisateurs à haut risque pour prévenir les attaques, y répondre et rétablir leurs activités après un incident. | Résultat 2 : Protection et résilience accrues des utilisateurs exposés à des menaces ciblées, notamment la répression transnationale numérique (RTN) et les violences basées sur le genre facilitées par la technologie. | Changement de plus haut niveau auquel le Fonds peut contribuer de manière significative. |
| **Produit 3.1 :** Renforcement du partage des connaissances et de la coordination entre les bénéficiaires et les partenaires de l'écosystème.<br>**Produit 3.2 :** Élaboration de ressources, de politiques et de recommandations à l'échelle de l'écosystème visant à renforcer les conditions propices à un Internet plus sûr pour tous. | Résultat 3 : Réseaux de collaboration et partenariats mondiaux renforcés pour promouvoir un Internet plus sûr pour tous, y compris les groupes vulnérables et les communautés à haut risque. | **But (Impact)** |
| **Produit 4.1 :** Attribution de subventions pluriannuelles et flexibles à des organisations de la société civile œuvrant dans le domaine de la cybersécurité.<br>**Produit 4.2** : Ateliers ou rencontres de renforcement des capacités des bénéficiaires portant sur la stratégie, la gestion financière, la collecte de données, les bonnes pratiques techniques et d'autres sujets liés au développement organisationnel. | Résultat 4 : Capacités organisationnelles et stabilité financière renforcées des bénéficiaires. | Renforcement de la sécurité en ligne pour tous et meilleure protection des utilisateurs d'Internet à haut risque. |
| | | Changement global et systémique que nous espérons voir se concrétiser à long terme et auquel le Fonds contribue, à son échelle |
| Produits et services directement générés par les activités soutenues par le Fonds. | Changements qui échappent au contrôle direct du Fonds, mais auxquels il cherche à contribuer. | |

# Théorie du changement :

**SI** la Fondation Internet Society, en collaboration avec la Global Cyber Alliance, met en œuvre un programme de subventions doté de ressources suffisantes sur une période de cinq ans, offrant un financement pluriannuel et flexible à des organisations à but non lucratif œuvrant dans le domaine de la cybersécurité — en particulier dans la Majorité mondiale — et complète ce financement par un renforcement des capacités techniques et organisationnelles, un soutien spécialisé en matière de plaidoyer ainsi que des possibilités d'apprentissage entre pairs et de partage des connaissances,

**ALORS** ces organisations à but non lucratif (bénéficiaires des subventions de la Fondation Internet Society) maintiendront des infrastructures critiques plus sécurisées, fourniront un meilleur soutien aux utilisateurs à haut risque confrontés à des menaces de cybersécurité et renforceront les réseaux de collaboration ainsi que les partenariats mondiaux œuvrant à promouvoir des initiatives en faveur de la sûreté et de la sécurité, contribuant ainsi, à terme, à un écosystème de cybersécurité plus solide favorisant un Internet plus sûr pour tous.

# Guide de renseignement des indicateurs du Fonds Common Good Cyber (CGCF)

Le présent guide fournit les lignes directrices pour le renseignement des indicateurs du Fonds Common Good Cyber (CGCF). Il vise à assurer une compréhension commune des indicateurs ainsi qu'une communication cohérente, fiable et comparable des résultats par l'ensemble des bénéficiaires.

Lors du renseignement des indicateurs, tenez compte de l'ensemble des programmes et initiatives financés ou soutenus par le CGCF. Les données communiquées doivent refléter les résultats obtenus dans le cadre de ces programmes et initiatives.

Le CGCF pouvant soutenir des programmes directement ou indirectement, il vous appartient de déterminer, avec discernement, quelles données sont pertinentes à inclure dans votre rapport.

Seuls les résultats obtenus au cours de la période de référence doivent être communiqués. Les résultats obtenus en dehors de cette période ne doivent pas être inclus.

En cas de doute sur les données à communiquer, veuillez contacter votre point de contact au sein du CGCF.

## *Indicateurs de capacité organisationnelle et de durabilité (applicables à tous les bénéficiaires)*

Les indicateurs de capacité organisationnelle et de durabilité s'appliquent à tous les bénéficiaires du CGCF, quel que soit leur domaine d'intervention. Ils visent à mesurer l'évolution de la capacité organisationnelle, de durabilité et d'efficacité opérationnelle des bénéficiaires au cours de la période de subvention.

| ***Indicateurs de capacité organisationnelle et de durabilité (applicables à tous les bénéficiaires)*** | |
|---|---|
| **Indicateur** | Instructions pour le renseignement |
| Nombre de bénéficiaires indiquant avoir davantage de sources de financement actives à la fin de la période de subvention qu'au début | Nombre de bénéficiaires déclarant disposer d'un plus grand nombre total de sources de financement actives à la fin de la période de subvention (ou au moment de la présentation du rapport, pour les rapports intermédiaires) qu'au début. Les « sources de financement » peuvent inclure des subventions, des contrats, des dons, les parrainages, des revenus générés, etc.<br><br>Cet indicateur n'a pas pour objectif de démontrer de manière définitive que le Fonds est à lui seul responsable de l'amélioration de la situation financière d'un bénéficiaire ; il vise plutôt à rendre compte de l'évolution de sa situation financière, à laquelle s le CGCF a pu contribuer, grâce à un financement direct ou à un soutien au renforcement des capacités organisationnelles. |
| Nombre d'améliorations opérationnelles spécifiques ou d'actions de renforcement organisationnel mises en œuvre | Les bénéficiaires indiquent eux-mêmes s'ils ont apporté des améliorations concrètes sur les plans financier, administratif, opérationnel ou organisationnel après avoir reçu un financement du CGCF et/ou participé à des activités de |

| | |
|---|---|
| par les bénéficiaires pendant la période de subvention | renforcement des capacités organisées par la Fondation Internet Society à l'intention des bénéficiaires du CGCF.<br><br>Les bénéficiaires doivent être en mesure de citer des exemples précis d'améliorations auxquelles le financement du CGCF ou les activités de renforcement des capacités ont, selon eux, contribué, telles que la mise en place ou la mise à jour de protocoles/politiques, de systèmes financiers, de stratégies ou de processus de gouvernance ; des changements au niveau des effectifs ; de nouvelles stratégies de communication ; ou encore l'utilisation/l'adoption de nouveaux outils par l'organisation. |
| Nombre de bénéficiaires indiquant une confiance accrue dans leur capacité à gérer des fonds destinés au soutien en cybersécurité au cours de la période de subvention | Les bénéficiaires indiquent s'ils se sentent plus à l'aise pour gérer les ressources financières liées aux activités de cybersécurité après avoir reçu un financement du CGCF et/ou participé à des activités de renforcement des capacités organisées par la Fondation Internet Society à l'intention des bénéficiaires du CGCF. |

### *Indicateurs par domaine d'intervention*

| **Pour les subventions visant à maintenir des infrastructures critiques de cybersécurité (renseigner uniquement les indicateurs applicables)** | |
|---|---|
| **Indicateur** | Instructions pour le renseignement |
| Nombre estimé d'utilisateurs finaux bénéficiant de services d'infrastructure de | Nombre total de personnes bénéficiant directement ou indirectement de services d'infrastructure soutenus par la subvention et fournis par les bénéficiaires au cours de la période de référence. Cet indicateur comprend les utilisateurs de réseaux, de plateformes ou de systèmes |

| | |
|---|---|
| cybersécurité améliorés ou maintenus par les bénéficiaires | dont la sécurité a été renforcée grâce aux activités menées par les bénéficiaires.<br><br>Il s'agit d'une estimation raisonnée destinée à illustrer l'ampleur des retombées résultant de la protection ou du soutien des services d'infrastructure de cybersécurité assurés par les bénéficiaires. Cette estimation peut être imprécise, car ces services fonctionnent souvent à des niveaux mutualisés, en amont ou à l'échelle d'Internet, ce qui peut entraîner des bénéfices indirects pour un grand nombre d'utilisateurs.<br><br>Les « services d'infrastructure » comprennent des services opérationnels mutualisés qui contribuent à sécuriser, pérenniser et renforcer la disponibilité, l'intégrité et la fiabilité des systèmes Internet essentiels, notamment en identifiant les menaces, en permettant la mise en œuvre de mesures correctives, en soutenant la réponse aux incidents et en fournissant des fonctions favorisant la confiance, telles qu'une infrastructure de certificats sécurisée. |
| Nombre de vulnérabilités liées aux infrastructures identifiées par les bénéficiaires avant qu'elles ne soient exploitées | Cet indicateur mesure le nombre de vulnérabilités de sécurité distinctes et significatives affectant les infrastructures concernées, identifiées par les bénéficiaires au cours de la période de référence avant toute exploitation malveillante confirmée.<br><br>Les « vulnérabilités » désignent des faiblesses importantes en matière de sécurité, notamment des failles de sécurité, des erreurs de configuration, des paramètres par défaut non sécurisés, des contrôles d'accès insuffisants ou d'autres conditions susceptibles de permettre un accès non autorisé, une compromission, une perturbation ou un usage abusif.<br><br>Les bénéficiaires doivent s'appuyer sur leur expertise technique et leurs critères internes pour déterminer si une vulnérabilité identifiée constitue une faiblesse de sécurité significative devant être prise en compte dans cet indicateur, notamment lorsqu'elle pourrait entraîner des dommages si elle n'est pas corrigée. |

| | |
|---|---|
| Pourcentage de vulnérabilités identifiées ayant été correctement atténuées par les bénéficiaires ou officiellement reconnues en vue d'une remédiation par l'opérateur d'infrastructure responsable, avant d'avoir un impact sur les utilisateurs (ventilé entre numérateur et dénominateur) | Cet indicateur mesure la part des vulnérabilités identifiées par les bénéficiaires qu'ils parviennent à atténuer avant qu'elles n'aient un impact sur les utilisateurs.<br><br>Les « vulnérabilités » désignent des faiblesses importantes en matière de sécurité, notamment des failles de sécurité, des erreurs de configuration, des paramètres par défaut non sécurisés, des contrôles d'accès insuffisants ou d'autres conditions susceptibles de permettre un accès non autorisé, une compromission, une perturbation ou un usage abusif.<br><br>Une vulnérabilité est considérée comme « correctement atténuée » si des mesures ont été prises pour la traiter ou réduire son impact avant qu'elle n'entraîne des dommages pour les utilisateurs ou les systèmes. Une vulnérabilité est considérée comme officiellement reconnue en vue d'une remédiation si l'opérateur d'infrastructure responsable indique qu'il en a connaissance et qu'il prévoit de la traiter dans le cadre d'une procédure de divulgation coordonnée.<br><br>Pour le dénominateur, les bénéficiaires doivent indiquer le nombre total de vulnérabilités identifiées conformément à l'indicateur ci-dessus. Pour le numérateur, les bénéficiaires doivent indiquer le nombre total de vulnérabilités (parmi celles identifiées) qui ont été correctement atténuées. Le système de reporting Fluxx utilisera ces deux valeurs pour calculer automatiquement le pourcentage |
| Nombre d'organisations (p. ex. CSIRT nationaux ou sectoriels, opérateurs d'infrastructure, fournisseurs de | Cet indicateur mesure le nombre d'organisations ayant pris des mesures pendant la période de référence après avoir reçu des informations sur des menaces de cybersécurité, des rapports, des alertes ou des renseignements partagés grâce à des activités soutenues par la subvention. |

| | |
|---|---|
| services et organisations de la société civile) répondant aux menaces de cybersécurité ou y remédiant grâce aux rapports ou renseignements partagés avec le soutien de la subvention | La « réponse » aux menaces comprend la prise de mesures visant à gérer ou à contenir une menace ou un incident détecté, notamment le blocage du trafic malveillant, le retrait d'une infrastructure malveillante, l'alerte des utilisateurs ou membres concernés, l'escalade vers une équipe de réponse aux incidents, la diffusion d'avis, la mise en œuvre de mesures de confinement ou le partage ultérieur des informations afin de permettre une action opérationnelle.<br><br>La « remédiation » des menaces comprend les mesures prises pour corriger, réduire ou éliminer le risque ou la vulnérabilité sous-jacente, notamment l'application de correctifs sur les systèmes vulnérables, la correction des erreurs de configuration, la désactivation des services exposés, la rotation des identifiants, la mise à jour des règles ou des contrôles, ou encore la suppression de la condition ayant permis l'apparition de la menace.<br><br>Il s'agit d'un indicateur de contribution, et non d'un indicateur d'attribution. Les bénéficiaires ne sont pas tenus de démontrer que la réponse apportée résulte uniquement de leurs actions. Les bénéficiaires doivent plutôt démontrer qu'il existe un lien plausible entre les informations partagées et les mesures prises par l'organisation.<br><br>Les sources de données potentielles pour cet indicateur peuvent inclure des courriels, appels ou réunions de suivi avec les personnes ayant reçu les rapports ou renseignements, afin d'échanger sur les mesures prises ou de les confirmer, via des canaux de communication nouveaux ou existants. |
| Nombre de bénéficiaires proposant de nouveaux services de sécurité Internet ou | Les bénéficiaires indiquent (Oui/Non) s'ils proposent de nouveaux services de cybersécurité ou renforcent des services existants dans le cadre de leur subvention. Si la réponse est Oui, les bénéficiaires sont ensuite invités à fournir une description plus détaillée du ou des services proposés. Parmi les exemples de services figurent la surveillance, la |

| | |
|---|---|
| renforçant les services existants pour les utilisateurs, fournisseurs ou autorités | réponse aux incidents, l'accompagnement consultatif, ainsi que de nouveaux protocoles ou protocoles améliorés de signalement et de partage de données.<br><br>Les services « renforcés » désignent les modifications apportées aux services existants des bénéficiaires qui permettent d'élargir leur couverture ou d'en améliorer la qualité. Les ajustements mineurs apportés aux activités courantes ne doivent pas être comptabilisés automatiquement comme un renforcement des services, sauf s'ils entraînent une évolution significative de leur portée. |
| Nombre d'activités distinctes de surveillance des menaces régulièrement menées par les bénéficiaires | Les « activités distinctes de surveillance des menaces » désignent des types spécifiques d'activités de surveillance, comprenant notamment, sans s'y limiter, l'analyse des indicateurs de compromission (IoC) (artefacts techniques ou éléments observables pouvant révéler une activité malveillante, tels que des adresses IP, des domaines, des hachages de fichiers, des clés de registre, des noms de processus, des certificats suspects ou d'autres signes avant-coureurs pouvant indiquer une compromission ou une tentative de compromission), l'identification de campagnes adverses distinctes, l'analyse de nouvelles tactiques, techniques et procédures (TTP), et/ou la documentation de groupes de vulnérabilités critiques.<br><br>Cet indicateur inclut uniquement les activités de surveillance soutenues par la subvention et menées au cours de la période de référence. Compte tenu de la nature de cette activité technique, un nombre plus élevé d'activités de surveillance des menaces ne constitue pas nécessairement un indicateur de meilleure performance, certaines activités étant plus complexes que d'autres. Le cas échéant, les bénéficiaires doivent inclure dans leur rapport narratif une brève description de leurs activités de surveillance des menaces afin de contextualiser le nombre déclaré. |

| | |
|---|---|
| Nombre de rapports d'intérêt public présentant des conclusions jugées hautement fiables, élaborés et partagés par les bénéficiaires | Cet indicateur comptabilise les rapports produits par les bénéficiaires au cours de la période de référence qui présentent des conclusions solides, fondées sur des éléments probants, concernant des menaces, des risques, des incidents ou des pratiques de sécurité, et qui sont partagés publiquement ou avec des partenaires concernés.<br><br>Les « conclusions jugées hautement fiables » désignent des informations étayées par des éléments probants solides et suffisamment fiables pour guider l'action ou la prise de décision.<br><br>« Partagé publiquement » signifie que le rapport est accessible à des acteurs externes à l'organisation, par exemple par sa publication sur un site Web, son partage avec des partenaires, des décideurs ou des parties prenantes concernées, ou sa diffusion lors d'événements ou au sein de réseaux. |
| Nombre d'outils opérationnels, de plateformes ou de mécanismes de coordination axés sur les infrastructures, développés ou renforcés avec le soutien du Fonds et activement utilisés par plusieurs acteurs de l'écosystème | Cet indicateur comptabilise les outils, plateformes ou mécanismes de coordination soutenus par le Fonds au cours de la période de référence et permettant aux organisations de collaborer pour surveiller, partager des informations ou répondre aux menaces de cybersécurité affectant les infrastructures.<br><br>« Activement utilisé » signifie que l'outil, la plateforme ou le mécanisme continue d'être utilisé après sa création ou son amélioration, notamment pour le partage régulier de données, la coordination ou des contributions conjointes. Pour être pris en compte, les bénéficiaires doivent pouvoir démontrer, éléments à l'appui, que l'outil, la plateforme ou le mécanisme est utilisé par plusieurs organisations ou acteurs de l'écosystème de la cybersécurité, tels que des OSC, des CSIRT, des plateformes, des réseaux ou d'autres acteurs. |

| **Pour les subventions visant à fournir un soutien à grande échelle pour protéger les utilisateurs d'Internet contre les préjudices numériques, notamment les activités cybernétiques dirigées par des États et la répression transnationale numérique (renseigner uniquement les indicateurs applicables)** | |
|---|---|
| **Indicateur** | Instructions pour le renseignement |
| Pourcentage d'utilisateurs à haut risque déclarant avoir adopté de nouvelles pratiques ou de nouveaux outils après avoir bénéficié d'un soutien en cybersécurité (ventilé entre numérateur et dénominateur) | Cet indicateur est mesuré auprès des utilisateurs à haut risque qui, à l'issue de l'accompagnement, acceptent de fournir au bénéficiaire un retour d'information sécurisé et anonyme. Les nouvelles pratiques ou les nouveaux outils comprennent notamment les outils de communication sécurisée, l'authentification à deux facteurs, des pratiques plus sûres en matière de mots de passe, ainsi que des pratiques de détection des menaces ou de signalement. « Avec succès » signifie que l'utilisateur met correctement en œuvre une pratique ou utilise un outil dans ses activités quotidiennes pour renforcer sa sécurité.<br><br>Pour le dénominateur, les bénéficiaires doivent déclarer le nombre total de personnes ayant bénéficié d'un soutien en cybersécurité financé par la subvention et avec lesquelles ils ont assuré un suivi.<br><br>Pour le numérateur, les bénéficiaires doivent déclarer le nombre total de personnes ayant indiqué lors du suivi avoir mis en œuvre un nouvel outil ou une nouvelle pratique dans leurs activités quotidiennes pour renforcer leur sécurité. Le système de reporting Fluxx utilisera ces deux valeurs pour calculer automatiquement le pourcentage Bien que les bénéficiaires soient encouragés à assurer un suivi auprès d'autant d'utilisateurs que possible, un taux de réponse de 100 % est peu probable et le suivi peut être effectué sur la base d'un échantillon. Les sources de données potentielles pour cet indicateur comprennent les enquêtes de suivi menées par les bénéficiaires, ainsi que les appels ou |

| | |
|---|---|
| | entretiens réalisés avec les utilisateurs qu'ils accompagnent. Toutefois, les bénéficiaires ne sont pas tenus de communiquer des informations détaillées sur des pratiques des utilisateurs à haut risque qui pourraient compromettre leur sécurité. |
| Pourcentage d'utilisateurs d'Internet déclarant se sentir mieux protégés contre les préjudices numériques après avoir bénéficié d'un soutien en cybersécurité fourni par les bénéficiaires (ventilé entre numérateur et dénominateur) | Pourcentage d'utilisateurs à haut risque déclarant se sentir plus en sécurité en ligne après avoir reçu un soutien de la part des bénéficiaires. Cet indicateur mesure la perception des utilisateurs quant à leur sécurité en ligne et ne constitue pas une mesure directe de leur niveau réel de sécurité. Le fait de se sentir plus en sécurité en ligne comprend une plus grande confiance dans sa capacité à se protéger, à reconnaître les risques (p. ex. les arnaques, la surveillance ou le harcèlement) et à réagir aux menaces lorsqu'elles surviennent.<br><br>Pour le dénominateur, les bénéficiaires doivent déclarer le nombre total de personnes ayant bénéficié d'un soutien en cybersécurité financé par la subvention et avec lesquelles ils ont assuré un suivi. Pour le numérateur, les bénéficiaires indiqueront le nombre total de personnes qui, lors du suivi, ont déclaré se sentir plus en sécurité en ligne après avoir reçu un soutien. Le système de reporting Fluxx utilisera ces deux valeurs pour calculer automatiquement le pourcentage.<br><br>Bien que les bénéficiaires soient encouragés à assurer un suivi auprès d'autant d'utilisateurs que possible, un taux de réponse de 100 % est peu probable et le suivi peut être effectué sur la base d'un échantillon. Les sources de données potentielles pour cet indicateur comprennent les enquêtes de suivi menées par les bénéficiaires, ainsi que les appels ou entretiens réalisés avec les utilisateurs qu'ils accompagnent. |
| Nombre de prestataires de soutien | Les prestataires de soutien en cybersécurité s'entendent comme des bénéficiaires de subventions qui proposent des formations, des |

| | |
|---|---|
| en cybersécurité signalant des évolutions positives des tendances en matière d'incidents parmi les utilisateurs à haut risque qu'ils accompagnent | services ou d'autres formes d'accompagnement aux utilisateurs à haut risque afin de renforcer leur sûreté et leur sécurité. Les bénéficiaires indiquent s'ils ont constaté eux-mêmes, ou par le biais de signalements, des changements dans la manière dont les utilisateurs à haut risque qu'ils accompagnent vivent les incidents de cybersécurité ou y réagissent.<br><br>Les évolutions positives des tendances en matière d'incidents peuvent correspondre à des changements observés par les bénéficiaires qui témoignent d'une amélioration de la sûreté et de la sécurité des utilisateurs qu'ils accompagnent, tels qu'une diminution de la fréquence des demandes de soutien ou une évolution du profil des personnes sollicitant ce soutien. Ces changements peuvent également se traduire par des retours reçus par les bénéficiaires de la part des utilisateurs qu'ils accompagnent, indiquant une réaction plus rapide, un impact moindre, une réduction des temps d'interruption, moins de pertes de communications ou de fichiers, une récupération plus rapide de l'accès ou des fonctionnalités, ou une perturbation moindre de leurs activités professionnelles habituelles.<br><br>Les bénéficiaires doivent définir clairement en interne ce que signifie un « changement positif » dans leur contexte et organiser la collecte et l'analyse des données en conséquence. |
| Indicateur qualitatif : exemples de personnes ou d'organisations réagissant plus efficacement aux violences basées sur le genre facilitées par la technologie après | Cet indicateur présente des exemples concrets montrant comment des personnes ou des organisations sont mieux à même de prévenir, de gérer ou de surmonter les violences basées sur le genre en ligne après avoir reçu un soutien de la part des bénéficiaires. Comme pour toutes les données collectées, les bénéficiaires doivent respecter les principes de confidentialité, de consentement éclairé et de « ne pas nuire » lors de la collecte d'exemples pour cet indicateur. |

| | |
|---|---|
| avoir reçu un soutien en matière de cybersécurité de la part des bénéficiaires | |
| Nombre d'utilisateurs à haut risque ayant bénéficié d'un soutien en matière de cybersécurité, ventilé par<br><br>Genre (homme, femme, autre, inconnu, total)<br><br>Type de soutien (formation, accompagnement en réponse aux incidents, autre)<br><br>Profil des utilisateurs (journalistes, défenseurs des droits humains, organisations de la société civile, autre) | Cet indicateur comptabilise le nombre de personnes exposées à un risque accru d'incidents de cybersécurité (p. ex. des journalistes, des militants, des femmes dirigeantes, des acteurs de la société civile et d'autres personnes, y compris celles ciblées par la répression transnationale numérique) ayant reçu un soutien direct en matière de cybersécurité de la part des bénéficiaires. Le soutien comprend des formations (définies comme des sessions formelles avec un objectif d'apprentissage clair, axées sur l'acquisition de compétences ou de capacités), un accompagnement en réponse aux incidents (par exemple, la gestion d'une ligne d'assistance), ou toute autre intervention pertinente.<br><br>Les bénéficiaires sont encouragés à comptabiliser, lorsque cela est possible, le nombre de personnes uniques ayant reçu un soutien au cours de la période de référence ; si une même personne reçoit un soutien à plusieurs reprises, elle devrait idéalement n'être comptabilisée qu'une seule fois.<br><br>Les sources potentielles de données comprennent les dossiers des bénéficiaires, les bases de données ou les listes de présence aux formations. |
| Nombre de sessions de soutien en matière de cybersécurité | Cet indicateur comptabilise le volume des activités de soutien en matière de cybersécurité menées par les bénéficiaires au cours de la période de référence. Les « sessions » s'entendent dans le contexte des |

| | |
|---|---|
| organisées par les bénéficiaires, ventilé par :<br>Type de soutien [formation, accompagnement en réponse aux incidents, autre]<br>Pays des utilisateurs (auto-identifié) [y compris « non précisé »] | activités de chaque bénéficiaire et peuvent inclure des sessions de formation, des appels/échanges par chat/tickets liés aux incidents, etc.<br>Les sources potentielles de données comprennent les dossiers des bénéficiaires, les bases de données ou les listes de présence aux formations. |
| Nombre de supports d'orientation, d'outils ou de ressources en matière de cybersécurité fournis aux utilisateurs à haut risque avec le soutien du Fonds | Cet indicateur comptabilise les supports ou outils fournis par les bénéficiaires au cours de la période de référence pour aider les utilisateurs à prévenir les cybermenaces ou les incidents, à y répondre ou à rétablir leurs activités après un incident. Parmi les exemples figurent des guides, des boîtes à outils, des listes de contrôle, des outils numériques et des outils de communication sécurisés. Chaque support ou outil est comptabilisé une seule fois, quel que soit le nombre d'utilisateurs qui le reçoivent. |

| **Pour les subventions axées sur la promotion d'un Internet plus sûr pour les groupes vulnérables et les communautés à haut risque, notamment la société civile et les journalistes (renseigner uniquement les indicateurs applicables)** | |
|---|---|
| **Indicateur** | Instructions pour le renseignement |
| Nombre de discussions sur les politiques publiques liées à la cybersécurité ou de déclarations officielles du gouvernement intégrant des recommandations ou des éléments probants provenant des bénéficiaires ou des communautés qu'ils accompagnent | Nombre de discussions sur les politiques publiques ou de déclarations au cours de la période de référence qui utilisent, examinent ou prennent en compte des données, des analyses/résultats de recherche, des lignes directrices ou des recommandations produites par les bénéficiaires (ou par les communautés avec lesquelles ils travaillent) dans le cadre de cette subvention.<br><br>Les « discussions sur les politiques publiques » désignent les consultations, ateliers, tables rondes, séances parlementaires ou autres échanges auxquels participent les décideurs politiques.<br><br>Les « déclarations officielles du gouvernement » désignent les déclarations publiques orales ou les politiques, stratégies, communiqués de presse ou autres documents écrits liés aux politiques de cybersécurité.<br><br>Les sources potentielles de données pour cet indicateur comprennent des appels de suivi ou des entretiens avec les parties prenantes, ainsi que l'examen de sites Web gouvernementaux, de documents de politique publique et de sources médiatiques fiables à la suite de la diffusion des éléments probants ou des recommandations. |
| Nombre de changements à l'échelle de l'écosystème dans les | Les changements à l'échelle de l'écosystème sont des changements systémiques plutôt que des changements mis en œuvre par une seule organisation, entreprise ou personne. |

| | |
|---|---|
| pratiques ou les normes des plateformes résultant des efforts coordonnés des acteurs de l'écosystème en matière de sûreté et de sécurité | Les changements dans les « pratiques ou normes des plateformes » comprennent l'adoption de nouvelles pratiques ou protocoles renforcés en matière de sûreté et de sécurité, de politiques de plateforme ou de normes techniques, qui reflètent une réponse plus large de l'écosystème aux problématiques identifiées, étayées par des éléments probants ou mises en avant grâce à des efforts coordonnés incluant les bénéficiaires. Les « acteurs de l'écosystème » comprennent les bénéficiaires et d'autres parties prenantes pertinentes, telles que les organisations de la société civile, les acteurs de la communauté technique, les plateformes, les décideurs politiques, les prestataires de services et les acteurs du secteur privé.<br><br>Il s'agit d'un indicateur de contribution, et non d'un indicateur d'attribution. Les bénéficiaires ne sont pas tenus de démontrer qu'ils sont les seuls à l'origine du changement. Les bénéficiaires doivent plutôt démontrer qu'il existe un lien plausible entre leurs efforts et les changements intervenus dans l'écosystème de la cybersécurité au cours de la période de référence. |
| Nombre de pratiques coordonnées, nouvelles ou améliorées, et d'efforts de collaboration régulièrement mis en œuvre par plusieurs acteurs de l'écosystème dans le cadre d'initiatives en | Les bénéficiaires indiquent le nombre de pratiques coordonnées ou d'efforts de collaboration qui commencent à être mis en œuvre ***après*** la réalisation de leurs activités en matière de sûreté/sécurité soutenues par le Fonds. Cet indicateur vise à rendre compte de tout renforcement des réseaux de collaboration ou des partenariats mondiaux auquel les bénéficiaires estiment raisonnablement que leurs activités ont contribué.<br><br>Les « pratiques coordonnées ou efforts de collaboration » comprennent des dispositifs interorganisationnels tels que le partage d'informations sur les menaces, des procédures coordonnées d'alerte ou de notification, des processus conjoints de qualification ou d'escalade des incidents, des processus coordonnés de divulgation des vulnérabilités, |

| | |
|---|---|
| matière de sûreté et de sécurité | des mécanismes d'orientation vers des services de soutien, des guides opérationnels ou procédures communes, ainsi que d'autres mécanismes récurrents permettant à plusieurs acteurs d'agir de manière plus coordonnée et plus rapide.<br>« Nouvelles ou améliorées » signifie que les pratiques ont été créées ou renforcées au cours du projet grâce aux activités des bénéficiaires. |
| Nombre d'activités organisées par les bénéficiaires réunissant des acteurs de l'écosystème afin de favoriser le partage des connaissances et la coordination liés à la promotion d'un Internet plus sûr pour tout le monde | Les bénéficiaires indiquent le nombre d'activités qu'ils ont organisées au cours de la période de référence avec le soutien du Fonds, réunissant différents acteurs de l'écosystème de la cybersécurité (p. ex. des organisations de la société civile, des CSIRT, des plateformes ou des réseaux) afin de partager des connaissances, de discuter des défis et de coordonner les actions.<br>Les activités comprennent des ateliers, des séminaires, des rencontres et des sessions conjointes de planification. |
| Indicateur qualitatif : exemples d'activités en faveur d'un Internet plus sûr organisées par les bénéficiaires, qui abordent les violences basées sur le genre facilitées par la technologie comme thème central et/ou intègrent les | Les bénéficiaires indiquent et décrivent brièvement toute activité qu'ils ont soutenue au cours de la période de référence visant à répondre aux risques liés au genre (p. ex. le harcèlement ou les abus en ligne) ou intégrant les perspectives d'organisations dirigées par des femmes.<br>Les sources potentielles de données pour cet indicateur comprennent les ordres du jour, les notes ou tout autre document pertinent issu de l'activité organisée par les bénéficiaires. |

| | |
|---|---|
| perspectives d'organisations dirigées par des femmes | |
| Nombre de documents écrits présentant des recommandations et des lignes directrices pour les politiques ou normes de cybersécurité, élaborés et diffusés publiquement par les bénéficiaires | Cet indicateur comptabilise les rapports, lignes directrices ou documents de politique publique élaborés par les bénéficiaires au cours de la période de référence, visant à améliorer les politiques, normes ou pratiques en matière de cybersécurité, et diffusés publiquement ou partagés avec les parties prenantes concernées.<br><br>« Diffusé publiquement » signifie que le document est partagé au-delà de l'organisation (p. ex. via un site Web, auprès de décideurs politiques ou de parties prenantes, ou par l'intermédiaire d'événements ou de réseaux). Une publication sur les réseaux sociaux uniquement ne constitue pas une diffusion, sauf si elle est accompagnée d'une autre forme de diffusion.<br><br>Un nombre plus élevé de documents produits n'est pas nécessairement préférable ; la pertinence et la qualité des documents sont tout aussi importantes. |
| Indicateur qualitatif : exemples de recommandations et de lignes directrices tenant compte des enjeux de genre incluses dans les documents de politique de | Cet indicateur rend compte d'exemples concrets de la manière dont les bénéficiaires intègrent les considérations liées au genre (p. ex. les risques auxquels les femmes sont confrontées, la conception inclusive ou les mesures de protection) dans leurs recommandations ou lignes directrices en matière de politiques au cours de la période de référence.<br><br>Les sources potentielles de données pour cet indicateur comprennent des extraits de rapports ou de documents produits par les bénéficiaires présentant des recommandations intégrant les considérations liées au genre. |

| | |
|---|---|
| cybersécurité élaborés par les bénéficiaires | |