MC 2a : Gestion des cyberincidents

Table des matières

Objectifs du module

Bienvenue dans le module de connaissances sur **la gestion des cyberincidents**, dans le cadre du projet GFCE-Afrique.

Les participants à ce module de connaissances vont acquérir des connaissances sur les considérations politiques et techniques pour la gestion des incidents de cybersécurité à travers le partage des meilleures pratiques, les études de cas, les exercices et la réflexion.

À la fin du module, vous serez en mesure de répondre aux questions et de trouver des ressources supplémentaires dans les domaines d'intérêt suivants :

- Types d'équipes de gestion des cyberincidents,
- Création d'une CSIRT (Computer Security Incident Response Team),
- Services offerts par les CSIRT,
- Outils et compétences nécessaires pour gérer une CSIRT.
- Réseaux régionaux et internationaux de CSIRT, dont AfricaCERT, FIRST et OIC-CERT

1. Introduction

L'Afrique compte plus de 500 millions d'utilisateurs d'Internet, ce qui représente 38 % de la population du continent. On s'attend à un accroissement de l'adoption et de la dépendance des technologies de l'information et de la communication dans les secteurs économiques, les institutions publiques et la société. Les pays devront donc mettre en place une capacité nationale de cybersécurité efficace pour protéger et défendre leurs citoyens, leurs informations et leurs infrastructures.

Face aux réalités virtuelles continues accélérées par la pandémie de COVID-19, il est impératif que les pays africains renforcent leurs capacités et leur efficacité en matière de gestion des incidents de cybersécurité.

> *Les cybercriminels développent et renforcent leurs attaques à un rythme alarmant, exploitant la peur et l'incertitude engendrées par la situation sociale et économique instable imputable à la pandémie de COVID-19.*
>
> Jürgen Stock, Secrétaire Général d'INTERPOL
> Source : Rapport d'évaluation des cybermenaces en Afrique, octobre 2021

La cybersécurité a été identifiée comme l'un des principaux projets phares de l'Agenda 2063 en matière de développement de l'énergie et des infrastructures. Le projet de cybersécurité est guidé par la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. Le chapitre 3 de la Convention prévoit la promotion de la cybersécurité par des mesures prises au niveau national. Ces mesures comprennent une politique et une stratégie nationales en matière de cybersécurité, des mesures législatives et réglementaires, ainsi que des structures nationales de surveillance de la cybersécurité par la mise en place d'institutions appropriées telles que la CERT (Computer Emergency Response Team) ou les CSIRT (Computer Security Incident Response Teams).

2. Types d'équipes d'intervention en cas de cyberincidents

Face à l'augmentation significative des incidents de sécurité informatique entraînant des implications sociales, économiques et politiques, la plupart des pays africains envisagent divers mécanismes pour minimiser et atténuer l'impact de ces incidents, notamment la mise en place ou l'amélioration des équipes de coordination en charge du traitement et de la réponse aux incidents.

Études de cas : *Incidents de cybersécurité en Afrique pendant la pandémie de COVID-19*

Le rapport d'Interpol Évaluation des cybermenaces en Afrique, octobre 2021 a identifié les principales menaces dans la région : escroqueries en ligne, extorsion numérique, compromission de la messagerie en entreprise (BEC, Business Email Compromise), ransomware (rançongiciel) et botnets.

Des experts au Kenya ont affirmé que la COVID-19 a déclenché "une épidémie de cybercriminalité", avec une augmentation de 37,3 % des cyberattaques entre avril et juin 2021, par rapport à janvier et mars 2021.
Les cyberattaques, notamment par hameçonnage, diffusion de logiciels malveillants et attaques associées aux vulnérabilités du télétravail ont enregistré une nette augmentation, comme l'indique le rapport sur la cybersécurité en Afrique - Kenya, 2019/2020. Il s'agit notamment de l'accès à distance, des risques associés à une surveillance réduite et de l'exploitation des nouvelles infrastructures de télétravail.

Il existe différents types d'équipes en charge de surveiller, alerter, coordonner les efforts de réponse et de récupération, et faciliter la collaboration entre les entités gouvernementales, les organisations individuelles, les fabricants, les secteurs tertiaires et les services publics, le monde universitaire et la communauté internationale sur les questions de cybersécurité.

Ces équipes sont désignées par des acronymes tels que CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team), SOC (Security Operations Centre), NCSC (National Computer Security Center), ISAC (Information Sharing and Analysis Center) et, plus récemment, CDC (Cyber Defence Centres).

En fonction du mandat et du type de circonscription, les intervenants africains peuvent employer l'un de ces termes pour désigner l'équipe en charge de la gestion des incidents de cybersécurité. Par exemple, le nom des CSIRT nationales repose souvent sur l'abréviation CSIRT/CIRT/CERT : CERT-MU, EG-CERT. Le nom des équipes en charge d'un secteur spécifique se compose d'une forme abrégée du secteur et du code pays de deux lettres : EG-FinCIRT. Le nom de l'entreprise ou de l'organisation, ou une version abrégée de celui-ci, est inclus si l'équipe fournit des services à l'entreprise, par exemple Siemens CSIRT.

Le terme CSIRT désigne normalement une CIRT, une CERT ou une SIRT. Une organisation utilisant ce terme doit fournir un service de traitement des incidents (réponse aux incidents). Un SOC désigne une équipe qui surveille les opérations de sécurité pour

les réseaux et les centres de données. Il est important de noter que le terme CERT est une marque déposée au niveau mondial par le CERT Coordination Center (CERT/CC) qui relève du Software Engineering Institute (SEI) de l'Université Carnegie Mellon (CMU) aux États-Unis. Les organisations qui souhaitent utiliser le terme « CERT » dans le nom de leur équipe doivent contacter le SEI-CMU afin de demander l'autorisation (cette politique peut être modifiée à l'avenir).

Ressources : *Définitions*

Le RFC (Request for Comments) 2350 définit une CSIRT comme une équipe qui coordonne et appuie la réponse aux incidents de sécurité impliquant des sites au sein d'une circonscription définie. Pour être considérée comme une CSIRT, une équipe doit fournir un canal (sécurisé) permettant la réception de rapports sur des incidents présumés.

Le FIRST (Forum for Incident Response Teams) définit une CSIRT (équipe de réponse aux incidents de sécurité informatique) comme une capacité ou une unité organisationnelle (qui peut être virtuelle) fournissant des services et un soutien à une circonscription définie pour prévenir, détecter, traiter et gérer les incidents de sécurité informatique, conformément à sa mission. On appelle « circonscription » un ensemble spécifique de personnes et/ou d'organisations possédant des caractéristiques communes, auquel une CSIRT fournit des services.

La recommandation ITU-T X.1060 de l'Union internationale des télécommunications définit le centre de cyberdéfense (CDC) comme une entité au sein d'une organisation qui propose des services de sécurité dans le but de répondre aux risques liés à la cybersécurité pesant sur ses activités commerciales.

Le SEI-CMU définit une CSIRT (équipe de réponse aux incidents de sécurité informatique) comme une organisation de services en charge d'assurer la réception, l'examen et la réponse aux rapports et à l'activité des incidents de sécurité informatique. Ces services sont proposés à une circonscription définie.

Le FIRST définit un ISAC (centre de partage et d'analyse de l'information) comme une plate-forme de coopération pour les équipes de sécurité qui relèvent du même secteur ou partagent un objectif commun. Elle peut offrir la plupart des services d'une CSIRT, mais elle n'assure pas le traitement des incidents.

Un SOC (centre d'opérations de sécurité) assure la surveillance en temps réel centralisée des réseaux et systèmes d'une organisation, ainsi que la coordination de la réponse et du traitement des incidents.

2.1. CSIRT nationales (Équipe nationale d'intervention en cas d'incident contre la sécurité informatique)

Les pays africains disposent de différents moyens pour renforcer leurs capacités en matière de cybersécurité. Ils peuvent notamment mettre en place des CSIRT (Computer Security Incident Response Teams) nationales, qui constituent un élément clé pour la mise en œuvre des stratégies nationales de cybersécurité. Avec l'opérationnalisation d'une CSIRT nationale, un pays peut améliorer ses capacités en matière de cybersécurité, notamment la surveillance en temps réel, l'émission d'alertes rapides, la réponse aux incidents, la récupération rapide et l'atténuation des conséquences.

Les bonnes pratiques globales du GFCE identifient les caractéristiques et les capacités spécifiques des N-CSIRT ;

- portée nationale et reconnaissance gouvernementale,
- intégration à la structure nationale de gestion de crise,
- coopération et collaboration avec de multiples intervenants dans la lutte contre les cybermenaces et les incidents, aux niveaux national, bilatéral et international, et
- collaboration avec d'autres CSIRT nationales et/ou régionales, des CSIRT gouvernementales, des PSIRT (équipes d'intervention en cas d'incident relatif à la sécurité des produits pour les fabricants/fournisseurs) et des communautés internationales de premier plan pour faire progresser la gouvernance, les cadres juridiques et les capacités des CSIRT

Une N-CSIRT doit au minimum assurer la gestion des incidents de cybersécurité, la sensibilisation et la communication avec sa circonscription et les services de connaissance situationnelle.

Selon l'Union internationale des télécommunications (UIT), on comptait en mars 2019 118 CSIRT nationales, comme le montre la figure 1 ci-dessous.

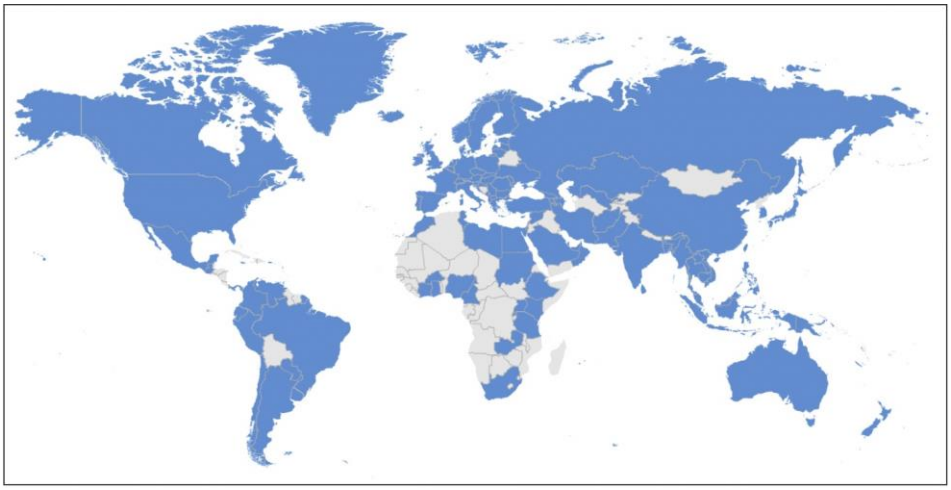


***Illustration 1** : CSIRT nationales dans le monde* Source : UIT

2.2. Équipe d'intervention en cas d'incident contre la sécurité des produits

Alors que les pays africains s'engagent de plus en plus dans la fabrication et l'innovation, il convient de prendre en compte la sécurité dans la conception, la planification, le développement, les tests et la maintenance des produits, solutions et services

Selon le FIRST, une PSIRT (équipe d'intervention en cas d'incident relatif à la sécurité des produits) est « une entité au sein d'une organisation qui, à la base, se concentre sur l'identification, l'évaluation et le traitement des risques associés aux vulnérabilités de sécurité dans les produits, y compris les offres, les solutions, les composants et/ou les services qu'une organisation produit et/ou vend ». Le Cadre de services de l'Équipe d'intervention en cas d'incident relatif à la sécurité des produits (PSIRT) FIRST fournit des conseils sur le profil et les capacités d'une équipe, créée pour gérer les vulnérabilités identifiées dans les produits et les offres.

Parmi les exemples de PSIRT, on peut citer Siemens ProductCERT, qui fait partie du portefeuille de traitement des cyberincidents et des vulnérabilités (IHVH) de Siemens et PST (Product Security Team) de Kaspersky. Le Microsoft Security Development Lifecycle (SDL) consiste en un ensemble de pratiques qui soutiennent la garantie de sécurité et la conformité, y compris l'établissement d'un processus standard de réponse aux incidents.

Ressource : ***Présentation*** : Groupe d'intérêt spécial (SIG) PSIRT (CSIRT produit)

La présentation faite lors du Symposium FIRST et AfricaCERT pour l'Afrique et les régions arabes, qui s'est tenu du 7 au 9 décembre 2021 par les coprésidents du SIG PSIRT Pete Allor (Red Hat) et Josh Dembling (Intel) couvre les domaines suivants :

- Vidéos de formation PSIRT et guide de maturité 2018
- Cadre des services PSIRT V.1.1.2019
- Cadre de services PSIRT V.1.X. (T2 2022)
- Identification de la mission, des objectifs et des résultats attendus

2.3. CSIRT par secteur

Selon le SEI de l'université Carnegie Mellon : Cadre sectoriel CSIRT, « les CSIRT sectorielles sont en charge de promouvoir la réponse aux incidents et leur gestion pour un secteur ou un sous-ensemble particulier d'un pays ou d'une économie (par exemple, le secteur financier, énergétique ou gouvernemental)

Également appelées CSIRT sectorielles, centres de cybersécurité sectoriels, CERT sectorielles ou ISAC (centres d'analyse et de partage de l'information), ces équipes d'intervention en cas d'incident sont spécialisées et spécifiquement adaptées... elles

offrent l'avantage de combler le fossé entre les secteurs public et privé, et elles fournissent un mécanisme ou une plate-forme pour la coopération, le partage de l'information et l'instauration de la confiance ».

Études de cas : CSIRT sectorielles en Afrique

Tunisie : La CERT financière offre des services de sécurité au secteur financier tunisien. Ces services comprennent : la surveillance, la gestion des incidents, les renseignements sur les menaces et la sensibilisation. La CERT financière est membre du FIRST.

Égypte : EG-FinCIRT mise en place par la Banque centrale d'Égypte conformément à la stratégie de la banque pour évoluer vers une économie moins monétaire, soutenir les applications fintech et l'inclusion financière. Le document Central Bank of Egypt, Economic Review Vol. 60 No. 4 2019/2020 indique que l'EG-FinCIRT fournit une réponse aux incidents, une surveillance proactive et une analyse des incidents de sécurité de l'information au secteur financier, avec un important investissement en capital humain consenti pour soutenir ces fonctions.

Ghana : Le NCA-CERT a été créé par la National Communications Authority, qui réglemente l'industrie des communications, pour répondre aux incidents dans le secteur des communications.

La principale circonscription de la NCA-CERT regroupe les opérateurs autorisés dans le secteur des communications et leurs abonnés. Elle fournit une plate-forme pour le partage d'informations et coordonne les incidents dans le secteur des communications.

La CERT travaille avec ses acteurs pour intégrer les meilleures pratiques de cybersécurité dans ses programmes de réglementation et d'octroi de licences, tout en fournissant des services tels que la gestion des incidents, l'analyse, la garantie de l'information, la connaissance situationnelle, les communications et la sensibilisation, le développement des capacités, la recherche et le développement.

2.4. Centre des opérations de sécurité

Il n'existe pas de définition officielle du SOC (centre d'opérations de sécurité). Un SOC ou une CSIRT interne protège et défend les activités commerciales d'une organisation contre les risques de cybersécurité, par la surveillance et la gestion fondamentale de ces risques. Un SOC fournit généralement des services habituels, notamment l'analyse de la détection des incidents, ainsi que la surveillance et la maintenance des systèmes de réponse pour la sécurité. Le centre est géré par un responsable de la sécurité (CSO) ou un responsable de la sécurité des informations (CISO).

Lors de la mise en place d'un SOC, une organisation doit procéder petit à petit, selon une procédure contrôlée, pour créer un SOC à part entière. Au départ, il convient d'acquérir de l'expérience dans la surveillance des données de journalisation de différents composants d'infrastructure ou de middleware, l'enregistrement des incidents à l'aide des outils appropriés, la production de rapports périodiques et l'enregistrement des enseignements tirés. Le personnel doit participer aux réunions pertinentes au sein de l'organisation. Une politique de sécurité de l'information approuvée par la direction est essentielle pour le bon fonctionnement d'un SOC.

La conformité ou la certification à la norme ISO/CEI 27001 démontre la qualité et l'efficacité des politiques, procédures et contrôles de sécurité de l'information au sein de l'organisation. Cette norme peut être utilisée pour appuyer le fonctionnement du SOC.

2.5. CSIRT commerciale

Une CSIRT commerciale offre des services de sécurité gérés à des clients ou organisations payants. Dans la plupart des cas, ces organisations disposent de ressources limitées en termes de financement et de personnel qualifié (expertise) pour fournir la gamme complète des services requis pour une CSIRT ou un SOC.

Pour instaurer la confiance des clients dans les services fournis par une CSIRT commerciale, il est recommandé que ces entités soient réglementées et certifiées sur la base de normes internationales.

Ressource :

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a reconnu qu'elle ne pouvait pas, par elle-même, appuyer les exploitants d'infrastructures critiques. Elle a donc mis en place un processus d'évaluation lui permettant de qualifier les « prestataires de services de confiance » et les produits de cybersécurité privés dans les domaines suivants :

- prestataires d'audit de la sécurité des systèmes d'information (PASSI)
- prestataires de détection d'incidents de sécurité qualifiés (PDIS)
- prestataires de réponse aux incidents de sécurité (PRIS)
- prestataires de services d'intégration/architecture (planifié)

Études de cas *: L'espace pour les CSIRTS commerciales ou les services de sécurité gérés*

La CIRT de Serianu fournit les services suivants aux organisations africaines : intervention et enquête sur les incidents, remédiation et soutien technologique, détection et surveillance gérées des menaces, évaluation et garantie de sécurité, quantification des cyberrisques, formation et sensibilisation. Serianu est présent au Kenya, en Ouganda, en Tanzanie, en Éthiopie, au Nigeria, au Ghana, au Botswana et au Lesotho.

CSIRT.TN

Commented [1]: (French website)

3. Quels critères faut-il prendre en compte lors de la mise en place d'une CSIRT nationale ?

Il existe différents guides et meilleures pratiques auxquels les pays africains pourraient se référer pour la création et l'établissement d'une CSIRT. Ces cadres recommandent l'utilisation d'une approche progressive pour la mise en place d'une CSIRT nationale, notamment le :

- Programme de cybersécurité de l'UIT : Cadre CIRT
- Recommandation X.1060 ITU-T : Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense
- Agence de l'Union européenne pour la cybersécurité (ENISA) : How to set up a CSIRT and SOC (en anglais)
- GFCE Global Good Practice: National Computer Security Incident Response Teams (CSIRTs) (en anglais)
- GFCE Cyber Incident Management in Low-Income Countries - Part 1- A Holistic View on CSIRT Development et Part 2- A Guideline for Development (en anglais)

3.1. Cadre de la CSIRT

L'UIT a utilisé le cadre CIRT pour aider les pays africains, notamment le Botswana, le Burundi, la Gambie, le Ghana, le Kenya, le Malawi, la Tanzanie, l'Ouganda et la Zambie, à mettre en place des équipes nationales. Ce cadre se compose de quatre (4) phases : évaluation, conception, établissement et amélioration.

Phase 1 : Évaluation Cette phase implique d'évaluer la posture de cybersécurité du pays en menant un diagnostic sur site et en impliquant les intervenants dans une série d'ateliers en vue de déterminer la valeur et le fondement justifiant l'établissement d'une CSIRT et d'obtenir un appui pour les mécanismes de ressources et de financement. Le résultat de cette phase est un rapport d'évaluation, préparé par les experts de l'UIT, qui contient les questions clés, les conclusions et les analyses, les recommandations et un plan de mise en œuvre échelonnée pour la mise en place de la CIRT nationale.

Phase 2 : Conception Le résultat de cette phase est un document de conception détaillé, qui comprend un examen de la mission et du positionnement de la CSIRT, la définition du modèle de services conformément au cadre de services FIRST CSIRT, une liste des flux de travail, des politiques et des procédures, une carte des processus, un plan d'engagement des intervenants et une stratégie de communication, la conception des réseaux, une liste des équipements et outils matériels et logiciels, la sélection des locaux et du personnel.

Phase 3 : Mise en place Cette phase comprend le développement des capacités (processus, politiques, procédures, technologie et ressources humaines), le déploiement et le test des capacités, la personnalisation, la mise au point et la formation, les opérations, le transfert et la fermeture. Les résultats de cette phase sont les rapports, la documentation et l'acceptation opérationnelle de la CIRT par le pays bénéficiaire.

Phase 4 : Amélioration Cette phase établit de nouveaux services (connaissance situationnelle et informatique légale) basés sur le cadre de services FIRST CSIRT (voir section 5.2), des services personnalisés et une meilleure automatisation des services existants.

3.2. Mise en place d'une CSIRT et d'un SOC

L'ENISA propose des directives concernant la mise en place d'une CSIRT et d'un SOC, qui sont organisées en cinq (5) phases : évaluation de l'état de préparation, conception, mise en œuvre, opérations et amélioration.

Phase 1 : Évaluation de l'état de préparation – Cette phase a pour but de déterminer la mission préliminaire de l'autorité, la structure de gouvernance définissant les responsabilités des intervenants d'une CSIRT nationale et l'identification de l'organisation hôte de la CSIRT. Ces éléments sont généralement exprimés par le biais d'une loi, d'une stratégie de cybersécurité ou d'un plan de cybersécurité.

Bonne pratique : Un positionnement organisationnel bien pensé

La CSIRT nationale doit être positionnée de manière à tirer parti de la structure organisationnelle de la nation, autrement dit établie par la loi, connectée à la structure nationale de gestion de crise et disponible en tant que point de contact international pour les incidents de cybersécurité.

Cette phase comprend l'examen et l'approbation d'une feuille de route et d'un budget de haut niveau, incluant le calendrier prévu pour les phases de mise en place de la CSIRT et les exigences détaillées pour la phase de conception

Bonnes pratiques : Définir la mission adéquate et assurer l'intégration de haut en bas :

Selon la bonne pratique globale du GFCE - CSIRT (Équipes nationales de réponse aux incidents de sécurité informatique), l'efficacité d'une CSIRT est déterminée par un mandat défini dans la stratégie, la réglementation ou la loi nationale en matière de cybersécurité.

La stratégie nationale doit définir le mandat, la mission, l'autorité et les responsabilités de la CSIRT envers sa circonscription, les parties prenantes et le modèle de gouvernance. Il doit impérativement exister une obligation légale de signaler les incidents de cybersécurité.

Afin de garantir une intégration de haut en bas, une CSIRT nationale doit bénéficier d'un soutien politique et gouvernemental, avec des structures de gouvernance et de responsabilité bien établies, ainsi qu'une connexion à la structure nationale de gestion de crise. La connexion de la CSIRT aux CSIRT régionales et internationales soutient les mécanismes de coordination obligatoires entre pays voisins, comme l'exigent les protocoles internationaux, notamment la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles.

Phase 2 : Conception Les recommandations de cette phase sont alignées sur le modèle de maturité de la gestion des incidents de sécurité (SIM3) dans les domaines de l'organisation, des ressources humaines, des outils et des processus référencés dans le modèle. Le résultat de cette phase comprend le mandat détaillé approuvé, ainsi que les plans couvrant les services de la CSIRT, les processus, l'organisation des flux de travail, les compétences et la structure de formation, les installations, les technologies et l'automatisation des processus, la coopération, la gestion de la sécurité informatique et de l'information et les exigences détaillées pour la phase de mise en œuvre. Une bonne pratique consiste à publier la structure de conception résultante au format fourni dans le RFC (Request for Comments) 2350 : Expectations for Computer Security Incident Response.

Phase 3 : Mise en œuvre Les résultats de cette phase comprennent une structure organisationnelle approuvée et mise en œuvre, l'embauche et la formation du personnel, la mise en œuvre du processus et des procédures, la signature d'accords avec la circonscription, les intervenants et les partenaires, ainsi que la communication et les célébrations du lancement de la CSIRT. À la fin de la phase de mise en œuvre, la CSIRT devrait être prête à fournir des services à ses membres et à entamer la phase d'exploitation.

Phase 4 : Exploitation– Dans cette phase, la CSIRT fournit les services conformément à son mandat sur une base quotidienne. Les résultats de cette phase sont les indicateurs clés de performance (KPI) mesurés à des fins de gestion et de gouvernance, le suivi de la qualité, l'examen annuel des performances opérationnelles, l'examen annuel des besoins des intervenants, l'approbation du budget annuel et la collecte des besoins d'amélioration.

Bonne pratique : Atelier ou réunion annuelle des intervenants de la CSIRT

Un atelier ou une réunion annuelle avec les intervenants de la CSIRT, au cours duquel sont présentées la performance de la CSIRT ainsi que les priorités et attentes des intervenants concernant la CSIRT, est identifié comme une bonne pratique.

Phase 5 : Amélioration – Les résultats de cette phase comprennent une liste d'initiatives d'amélioration, les exigences associées et le budget préliminaire. Les initiatives d'amélioration peuvent provenir de la phase opérationnelle, d'une feuille de route de haut niveau, des intervenants ou de la demande de la direction d'améliorer la maturité et la capacité de la CSIRT sur la base de cadres tels que le modèle de maturité de la gestion des incidents de sécurité (SIM3) et le modèle de capacité et de maturité du centre d'opérations de sécurité (SOC-CMM).

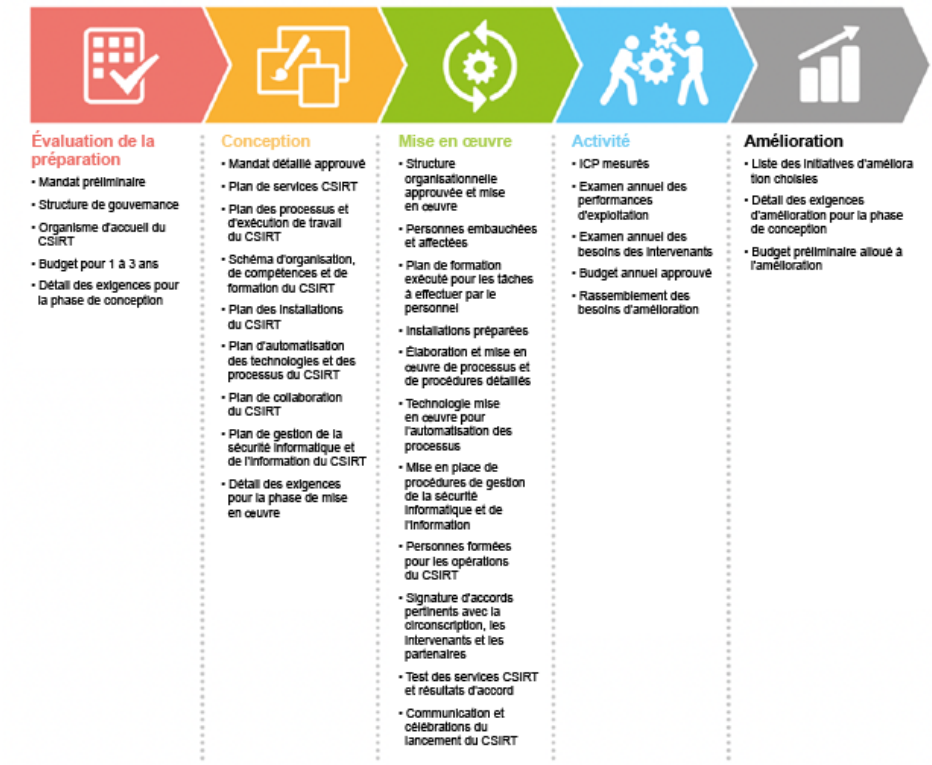


Illustration 2 : *Résumé des résultats de la mise en place de la CSIRT Source :ENISA*

Des formations sont disponibles à l'intention des managers et les chefs de projet qui ont été chargés de mettre en place une CSIRT. Il s'agit notamment des formations CMU-SEI Création d'une équipe de réponse aux incidents de sécurité informatique et Gestion des équipes de réponse aux incidents de sécurité informatique, qui aident les managers à améliorer l'efficacité de l'équipe.

Ressource *: Mise en place des CSIRT*

Mise en place d'une CSIRT : ce manuel décrit le processus et les exigences régissant la mise en place d'une CSIRT, ainsi que des exemples pertinents.

Le Manuel pour les équipes de réponse aux incidents de sécurité informatique (CSIRT) fournit une description de différents modèles organisationnels pour la mise en œuvre de capacités de traitement des incidents.

4. Comment évaluer l'état de préparation aux cyberincidents

Divers outils et modèles de maturité permettent d'identifier les besoins/manques dans divers aspects de la capacité de cybersécurité d'un pays ou d'une équipe.

Il s'agit notamment du modèle de maturité pour la gestion des incidents de sécurité (SIM3), du modèle de capacité et de maturité des centres d'opérations de sécurité (SOC-CMM) et de l'outil d'auto-évaluation de la maturité des CSIRT.

Bonne pratique : Mesurer et améliorer la maturité

À partir du modèle SIM3, les CSIRT effectuent une auto-évaluation basée sur 44 paramètres de maturité dans les domaines de l'organisation, des aspects humains, des outils et des processus. Les CSIRT émergentes et existantes peuvent utiliser le Kit de Maturité pour améliorer leur niveau de maturité. En définissant un chemin de croissance de la maturité basé sur le modèle SIM3, une CSIRT peut améliorer son niveau de maturité, du niveau « basique », au niveau « intermédiaire », puis au niveau « certifiable », à partir d'une combinaison d'auto-évaluations et d'examens par les pairs.

4.1. Modèle de maturité pour la gestion des incidents de sécurité (SIM3)

Le modèle de maturité pour la gestion des incidents de sécurité(SIM3) permet de mesurer la maturité d'une réponse aux incidents ou d'une équipe de sécurité en fonction de quatre domaines : l'organisation, les aspects humains, les outils et les processus. Le modèle SIM3 est disponible gratuitement auprès de la fondation Open CSIRT Foundation (OCF), à but non lucratif. Ce modèle est utilisé pour l'auto-évaluation des équipes. Il appuie le schéma de certification TI dans le cadre du TF-CSIRT et est envisagé pour adhésion par le FIRST.

4.2. Modèle de capacité et de maturité des centres d'opérations de sécurité (SOC-CMM)

Le modèle de capacité et de maturité des centres d'opérations de sécurité (SOC-CMM) se compose de 5 domaines et de 25 aspects. Les domaines comprennent les affaires, les personnes, les processus, la technologie et les services.

4.3. Maturité de la CSIRT - Outil d'auto-évaluation

Le produit Maturité de la CSIRT - Outil d'auto-évaluation aide les CSIRT à auto-évaluer la maturité de leur équipe en fonction de 44 paramètres du modèle SIM3 dans 4 grands domaines : organisation, aspect humain, outils et processus.

Exercice :

Réalisez une auto-évaluation de votre pays ou d'un N-CSIRT en utilisant l'un des outils ou modèles de maturité ci-dessus.

5. Quels sont les services offerts par les CSIRT ?

Les services complets et minimaux qu'une CSIRT devrait offrir à ses membres sont la gestion des incidents liés à la cybersécurité, la communication avec sa circonscription et la sensibilisation aux risques liés à la cybersécurité. Cependant, les entités de la communauté CSIRT ont développé leurs propres listes de services.

Bonne pratique : décider de l'ensemble et de la portée des services de la CSIRT nationale

La Bonne pratique globale du GFCE - Équipes nationales de réponse aux incidents de sécurité informatique (CSIRT) identifie comme une bonne pratique la détermination dès le départ des services et des domaines de service.

5.1.

Le GFCE et l'UIT recommandent tous deux l'utilisation du cadre de services CSIRT, qui comprend la gestion des incidents, l'analyse, l'assurance de l'information, la connaissance situationnelle, la sensibilisation/communication, le développement des capacités, ainsi que la recherche et le développement.

5.2. Cadre de services FIRST CSIRT

Le Cadre de services FIRST CSIRT classe les services CSIRT en cinq domaines de services, chaque domaine comportant plusieurs services. La plupart des CSIRT offrent un service de réponse aux incidents. Les cas CSIRT peuvent être classés en fonction de la catégorie, du niveau de criticité et du niveau de sensibilité. Les cinq domaines de services sont les suivants :

- Gestion des événements de sécurité de l'information (ISEM)
- Gestion des incidents de sécurité de l'information (ISIM)
- Gestion des vulnérabilités (VM)
- Connaissance de la situation (SA)

- Transfert de connaissances (KT)

5.2.1. Gestion des événements de sécurité de l'information (ISEM)

Ce domaine de service identifie les incidents de sécurité de l'information sur la base de la corrélation et de l'analyse des événements de sécurité provenant d'une grande variété de sources d'événements et de données contextuelles. Les offres de services ISEM comprennent la surveillance et la détection, ainsi que l'analyse des événements. À l'aide d'outils de traitement automatique continu, la CSIRT extrait des données de diverses sources d'événements de sécurité de l'information et de données contextuelles, afin d'identifier les incidents potentiels de sécurité de l'information. L'analyse des événements consiste à regrouper et à corréler les événements pour les définir comme des incidents potentiels de sécurité de l'information qui doivent être transmis au service de gestion des incidents de sécurité de l'information, ou comme de fausses alarmes.

Sur la base du cadre de référence pour la cybersécurité de l'initiative NICE (National Initiative for Cybersecurity Education), la CSIRT doit avoir des compétences dans les secteurs de la gestion des données, la conception d'infrastructure, la gestion de réseau et les systèmes d'exploitation afin de fournir le service de surveillance et de détection. Les compétences requises pour fournir le service d'analyse des événements sont la gestion des incidents, l'analyse des données, l'analyse des menaces, l'informatique légale et la surveillance des cybermenaces. La formation et la certification dans ces domaines sont fournies par SANS, Udemy, EC-Council, IBM, AfricaCERT, ENISA, FIRST, CIRCL, CERT-Tools Community, ICANN et CREST.

5.2.2. Gestion des incidents de sécurité de l'information (ISIM)

Il s'agit du principal service qu'une CSIRT fournit aux membres de sa circonscription. L'équipe recueille, évalue et analyse les rapports d'incidents liés à la sécurité de l'information. Les résultats de l'analyse sont utilisés pour formuler des recommandations à l'intention des utilisateurs en vue d'atténuer les incidents et d'y remédier. Ce service exige que la CSIRT effectue des opérations de coordination avec d'autres CSIRT ou des experts en sécurité afin de garantir le traitement de tous les aspects de l'incident et de contribuer à réduire les attaques futures similaires.

Divers cadres et directives proposent des conseils sur les services des CSIRT, notamment le Guide de traitement des incidents de sécurité informatique. Ce guide fournit des directives sur la création d'une politique et d'un plan de réponse aux incidents, l'élaboration de procédures pour le traitement et le signalement des incidents, la définition de directives de communication, la sélection d'une structure d'équipe et d'un modèle de dotation en personnel, l'établissement de relations et de lignes de communication entre

les parties internes et externes, et la détermination des services que l'équipe de réponse aux incidents doit fournir. Parmi les autres figurent le Carnegie Mellon University Engineering Institute (CMU-SEI) et le RFC-2350.

Les compétences de base requises dans le domaine de l'ISIM comprennent : l'informatique légale, l'analyse des données, la gestion des incidents, l'analyse des menaces, l'évaluation des vulnérabilités, la sécurité des systèmes d'information/réseaux, le test, l'évaluation et l'administration des systèmes, le cryptage et les compétences générales, notamment la pensée critique, la communication écrite et orale, la gestion des relations avec les clients, la gestion des conflits et des connaissances. L'équipe requiert des compétences en matière de droit, de réglementation, de politiques et d'éthique.

Les formations identifiées pour ce domaine de service comprennent, sans s'y limiter, celles proposées par SANS - Hacker Tools, Techniques, and Incident Handling, CMU-SEI- CERT Incident Response Process Professional Certificate, EC-Council - Certified Incident Handler Program, Udemy - Cyber Security Incident Handling and Response, Cyber Security Incident Response et Mile2- C)IHE Certified Incident Handling Engineer course.

5.2.3. Gestion des vulnérabilités (VM)

Le domaine de service de gestion des vulnérabilités comprend les services liés à la découverte/recherche, l'analyse et le traitement des vulnérabilités de sécurité nouvelles ou signalées, dont la coordination, la divulgation et la réponse. Dans ce domaine de service, les CSIRT offrent des services qui établissent un processus continu d'identification, d'analyse, de diffusion et de correction des vulnérabilités dans les systèmes d'information.

Les directives régissant la prestation de ce service sont contenues dans les normes ISO/CEI 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité, ISO/CEI 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité, the Cadre des services PSIRT du FIRST et la directive néerlandaise National Cybersecurity Center Coordinated Vulnerability Disclosure: the Guideline.

Pour offrir ce service, une équipe doit posséder des compétences en matière d'évaluation des vulnérabilités, d'analyse des menaces, de langages informatiques, de systèmes d'exploitation, de technologie web, de gestion de réseau, d'administration de système, de test et d'évaluation de logiciels, de confidentialité et de protection des données, de cryptage, d'assurance de l'information, de gestion de l'identité, de gestion des ressources/inventaires, d'administration de bases de données, ainsi que des compétences générales telles que la pensée critique, la gestion des conflits, la

communication orale et écrite, ainsi que la gestion des connaissances et des relations avec les clients.

Les formations et certifications dans ces domaines comprennent notamment SANS, CREST, Offensive Security, EC-Council, CompTIA, MILE2, et Udemy

Étude de cas : Vulnérabilité de Log4shell ou Log4j

Log4shell est une vulnérabilité critique dans l'outil de journalisation Log4j, d'utilisation courante. Le National Cybersecurity Centre du Royaume-Uni a publié des informations sur la « vulnérabilité de Log4j - ce que tout le monde doit savoir », y compris des conseils sur les organisations qui ont été affectées.

Le 13 décembre 2021, le réseau des CSIRT de l'UE est passé en mode « coopération » d'alerte sur le Log4j. Les membres du réseau des CSIRT ont échangé des informations, contribué à la mise à jour de la liste des logiciels vulnérables, publié des avis pertinents à l'intention de leurs circonscriptions et ils se sont réunis pour discuter des résultats de deux enquêtes de signalement et des situations nationales du 10 au 12 décembre 2021.

Le 12 janvier 2022, sur la base des données collectées, des rapports nationaux et de l'absence d'incidents à grande échelle ou transfrontaliers, le réseau des CSIRT de l'UE a décidé de revenir au mode de coopération par défaut, en ce qui concerne la vulnérabilité log4j/log4shell.

5.2.4. Connaissance de la situation (SA)

La connaissance situationnelle comprend la capacité à identifier, traiter, comprendre et communiquer l'état actuel et les changements potentiels anticipés dans la zone de compétence d'une CSIRT. Ce service exige de l'équipe qu'elle recueille, intègre et diffuse des informations à ses membres pour leur permettre de prendre des décisions éclairées. Les informations sont mises à disposition pour la prestation d'autres services, notamment la gestion des événements de sécurité, la gestion des incidents et le transfert de connaissances.

Les services offerts dans ce domaine comprennent l'acquisition, l'analyse, la synthèse et la communication des données. Afin de fournir ce service à ses membres, la CSIRT doit posséder des compétences en matière de gestion des ressources et des stocks, d'architecture d'entreprise, d'intégration de systèmes, d'analyse des menaces, d'évaluation des vulnérabilités, d'analyse et de gestion des données, de modélisation et

de simulation, de protection des données et de la confidentialité, d'assurance de l'information, de gestion de l'identité, de cryptage et de compétences générales en communication orale et écrite, de gestion des connaissances et des relations avec les clients, de sensibilisation à l'organisation et la technologie.

5.2.5. Transfert de connaissances (KT)

Compte tenu de la position unique du service de la CSIRT, l'équipe recueille, analyse et identifie les menaces, les tendances et les risques en matière de sécurité, et elle développe des pratiques opérationnelles pour aider ses organisations à détecter, prévenir et gérer les incidents. Le transfert de ces connaissances par le biais de la sensibilisation, de la formation et de l'éducation, d'exercices, de services de conseil technique et stratégique aux membres de la circonscription, est essentiel pour améliorer la cybersécurité globale.

Les compétences requises pour ce service sont la communication orale et écrite, les compétences interpersonnelles, la gestion des connaissances, la présentation efficace, la gestion des effectifs, la gestion stratégique, l'enseignement, la gestion des relations avec les clients, la continuité des activités, la gestion des conflits et des risques.

Des formations dans ce domaine sont disponibles auprès de CREST, MITRE, SANS-Security Strategic Planning, Policy, and Leadership, A Practical Introduction to Cyber Security Risk Management, NIST - les liens renvoient à des contenus éducatifs en ligne gratuits ou peu coûteux, ESET, NINJIO - Cybersecurity Awareness Training, KnowBe4 - Security Awareness et CybSafe - security awareness training

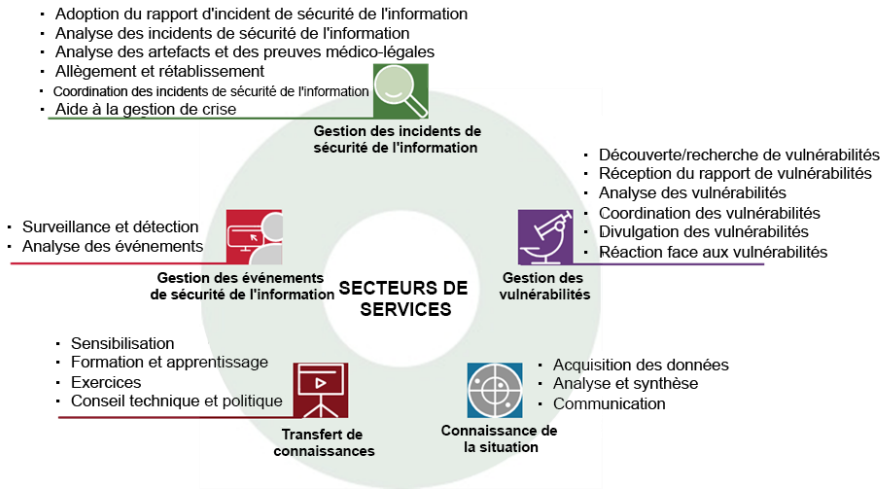


Illustration 3 : *Cadre des services CSIRT, domaines de service et service* Source : FIRST

5.3. Catégories de services de la recommandation UIT-T X.1060

La recommandation X.1060 ITU-T du secteur de la normalisation de l'Union internationale des télécommunications établit un cadre permettant aux organisations de construire et de gérer un centre de cyberdéfense qui peut être une CSIRT ou un SOC. Trois (3) processus (construction, gestion et évaluation) permettent à une CSIRT de déterminer quels services de sécurité doivent être inclus dans son catalogue de services, son profil et son portefeuille.

La recommandation UIT-T X.1060 identifie neuf (9) catégories de services. Sur la base des niveaux de recommandation de base, standard et avancé, un CDC peut extraire un catalogue de services de cette liste de services. En outre, en déterminant l'affectation du service comme étant internalisée, externalisée ou non affectée, le CDC peut développer un profil de service, puis un portefeuille de services en mesurant le score de service actuel (en l'état) ou le score de service cible à moyen-long terme (futur) :

A) gestion stratégique du CDC ;

B) analyse en temps réel ;

C) analyse approfondie ;

D) réponse aux incidents ;

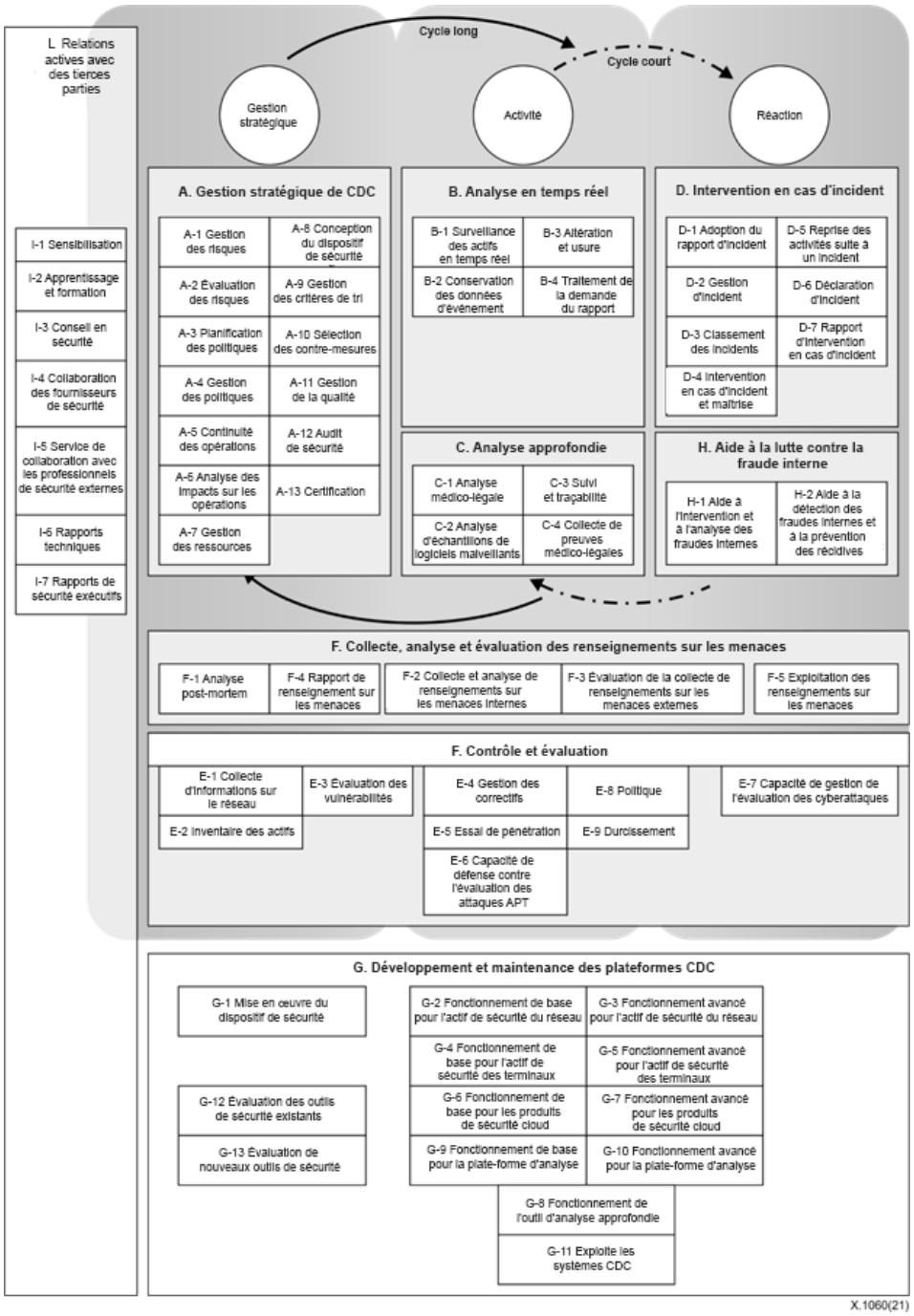
E) contrôle et évaluation ;

F) collecte, analyse et évaluation des renseignements sur les menaces ;

G) développement et maintenance des plateformes CDC ;

H) aide à la lutte contre la fraude interne ;

I) relations actives avec les parties externes.


L. Relations actives avec des tierces parties
Cycle long
Cycle court
Gestion stratégique
Activité
Réaction
A. Gestion stratégique de CDC
A-1 Gestion des risques
A-8 Conception du dispositif de sécurité
A-2 Évaluation des risques
A-9 Gestion des critères de tri
A-3 Planification des politiques
A-10 Sélection des contre-mesures
A-4 Gestion des politiques
A-11 Gestion de la qualité
A-5 Continuité des opérations
A-12 Audit de sécurité
A-6 Analyse des impacts sur les opérations
A-13 Certification
A-7 Gestion des ressources
B. Analyse en temps réel
B-1 Surveillance des actifs en temps réel
B-3 Altération et usure
B-2 Conservation des données d'événement
B-4 Traitement de la demande du rapport
C. Analyse approfondie
C-1 Analyse médico-légale
C-3 Suivi et traçabilité
C-2 Analyse d'échantillons de logiciels malveillants
C-4 Collecte de preuves médico-légales
D. Intervention en cas d'incident
D-1 Adoption du rapport d'incident
D-5 Reprise des activités suite à un incident
D-2 Gestion d'incident
D-6 Déclaration d'incident
D-3 Classement des incidents
D-7 Rapport d'intervention en cas d'incident
D-4 Intervention en cas d'incident et maîtrise
H. Aide à la lutte contre la fraude interne
H-1 Aide à l'intervention et à l'analyse des fraudes internes
H-2 Aide à la détection des fraudes internes et à la prévention des récidives
I-1 Sensibilisation
I-2 Apprentissage et formation
I-3 Conseil en sécurité
I-4 Collaboration des fournisseurs de sécurité
I-5 Service de collaboration avec les professionnels de sécurité externes
I-6 Rapports techniques
I-7 Rapports de sécurité exécutifs
F. Collecte, analyse et évaluation des renseignements sur les menaces
F-1 Analyse post-mortem
F-4 Rapport de renseignement sur les menaces
F-2 Collecte et analyse de renseignements sur les menaces internes
F-3 Évaluation de la collecte de renseignements sur les menaces externes
F-5 Exploitation des renseignements sur les menaces
F. Contrôle et évaluation
E-1 Collecte d'informations sur le réseau
E-3 Évaluation des vulnérabilités
E-2 Inventaire des actifs
E-4 Gestion des correctifs
E-8 Politique
E-5 Essai de pénétration
E-9 Durcissement
E-6 Capacité de défense contre l'évaluation des attaques APT
E-7 Capacité de gestion de l'évaluation des cyberattaques
G. Développement et maintenance des plateformes CDC
G-1 Mise en œuvre du dispositif de sécurité
G-2 Fonctionnement de base pour l'actif de sécurité du réseau
G-3 Fonctionnement avancé pour l'actif de sécurité du réseau
G-4 Fonctionnement de base pour l'actif de sécurité des terminaux
G-5 Fonctionnement avancé pour l'actif de sécurité des terminaux
G-12 Évaluation des outils de sécurité existants
G-6 Fonctionnement de base pour les produits de sécurité cloud
G-7 Fonctionnement avancé pour les produits de sécurité cloud
G-13 Évaluation de nouveaux outils de sécurité
G-9 Fonctionnement de base pour la plate-forme d'analyse
G-10 Fonctionnement avancé pour la plate-forme d'analyse
G-8 Fonctionnement de l'outil d'analyse approfondie
G-11 Exploite les systèmes CDC

X.1060(21)

Illustration 4 *: Services du Centre de cyberdéfense* Source : Recommandation ITU-T X.1060

Exercice :

Établir les services offerts par la CSIRT nationale de votre pays, et identifier et justifier l'inclusion de services supplémentaires dans le portefeuille de l'équipe.

6. À qui s'adresse la CSIRT ?

Une approche multi-intervenants au sein d'un pays et d'une organisation est essentielle pour une gestion efficace des incidents. Le GFCE identifie la création de communautés comme une bonne pratique qui facilite le partage d'informations de confiance, de même que l'échange d'expériences et de connaissances.

Bonne pratique : Créer des communautés

Une CSIRT nationale doit investir du temps et des efforts continus pour instaurer et maintenir la confiance avec les membres de sa circonscription et les autres intervenants, tant au niveau national qu'international. Cela peut se faire par la gestion des relations avec les membres de la circonscription, des ateliers ciblés et des exercices conjoints.

Grâce à la coopération et à la transparence (relative), la CSIRT doit s'efforcer d'être un partenaire digne de confiance, politiquement neutre, impartial et professionnel/technique dans les communautés nationales et internationales.

Exercice :

En utilisant la carte institutionnelle de cybersécurité interactive de l'ENISA, découvrez comment les acteurs en Europe sont impliqués dans les fonctions au sein d'une communauté.

Les membres d'une circonscription d'une CSIRT sont les destinataires ou les clients des services de la CSIRT. Dans ses chartes, énoncés de mission, documents de concept d'opérations ou documents similaires, l'équipe doit clairement définir sa clientèle. L'équipe doit comprendre sa circonscription afin de déterminer ses besoins, les ressources qu'elle doit protéger, et ses interactions potentielles avec la CSIRT.

Bonne pratique : Établir la composition, l'autorité et la responsabilité de la CSIRT nationale

Les circonscriptions sont les entités et les communautés pour lesquelles la CSIRT fournit un service et un soutien. L'étendue de l'autorité et de la responsabilité de la CSIRT doit être prédéterminée dans son rôle et son mandat.

Il existe différents types de CSIRT en fonction de la circonscription desservie, comme indiqué dans le tableau 1 ci-dessous :

Secteur	**Objectif**	**Membres de circonscription typiques**
CSIRT du secteur académique	Institutions académiques et éducatives, telles que les universités ou les centres de recherche, et les environnements Internet des campus.	Personnel et étudiants des universités.
CSIRT commerciale	Services commerciaux. Il peut s'agir d'une organisation indépendante, d'un FAI ou d'un fournisseur de services gérés.	Clients payants
CSIRT du secteur CIP/CIIP	Protection des informations stratégiques et/ou protection des informations et des infrastructures stratégiques. Cela couvre l'infrastructure informatique de tous les secteurs stratégiques d'un pays.	Secteurs gouvernementaux, stratégiques et citoyens.

CSIRT du secteur gouvernemental	Le gouvernement à proprement parler.	Agences gouvernementales.
CSIRT interne/Centre opérationnel de sécurité (SOC)	L'organisation hôte à proprement parler.	Personnel interne et département informatique.
CSIRT du secteur militaire	Organisations militaires ayant des responsabilités dans l'infrastructure informatique.	Personnel des institutions militaires et des entités étroitement associées telles que le ministère
CSIRT national	Centre national, considéré comme le point de contact central en matière de sécurité.	Pas de membres directs de la circonscription, bien qu'une CERT nationale soit parfois associée à une CERT gouvernementale
CSIRT du secteur des petites et moyennes entreprises (PME)	Il s'agit d'une CSIRT auto-organisée pour fournir des services à sa propre branche d'activité ou à un groupe d'utilisateurs similaire.	Les PME et leur personnel
CSIRT/PSIRT de fournisseur	Produits spécifiques du fournisseur, généralement pour remédier aux vulnérabilités ou offrir des conseils sur des d'attaques spécifiques. Un acronyme courant est PSIRT (Product Security Incident Response Team - Équipe de réponse aux incidents de sécurité des produits).	Propriétaires de produits

***Tableau 1** : Types de CSIRT et membres de circonscriptions* Source : ENISA Une approche étape par étape de la mise en place d'une CSIRT

7. De quels outils une CSIRT a-t-elle besoin ?

Différents outils sont disponibles pour permettre à une CSIRT de remplir ses fonctions, dont beaucoup sont open source et donc gratuits.

Le GFCE a identifié divers outils open source et commerciaux qui permettront aux CSIRT de fournir des services dans les cinq domaines de services donnés dans le cadre des services CSIRT FIRST : gestion des événements de sécurité de l'information (ISEM), gestion des incidents de sécurité de l'information (ISIM), gestion des vulnérabilités (VM), connaissance situationnelle (SA) et transfert de connaissances (KT).

Le FIRST fournit une liste d'outils de sécurité (Annexe C) pour l'interrogation des domaines et des adresses IP, la surveillance des réseaux, l'audit des réseaux, l'évaluation des vulnérabilités, la détection des intrusions, l'analyse des logiciels malveillants et les outils WiFi.

8. Politiques, cadres et directives

Les politiques, cadres et directives sont essentiels pour soutenir les processus et procédures de gestion et de traitement des incidents, et de traitement et d'échange d'informations d'une CSIRT.

En développant ces politiques, cadres et directives pour fournir des services dans les 5 domaines du cadre de services CSIRT FIRST, la directive du GFCE pour le développement de la gestion des cyberincidents dans les pays à faible revenu recommande qu'une équipe fasse référence aux normes internationales telles que l'ISO/CEI 29147:2018, la recommandation ITU-T X.1500, et des cadres tels que le cadre MITRE ATT&CK, le cadre SANS, les documents d'orientation CMU SEI.

9. Ressources et financement d'une CSIRT

La mise en place d'une capacité de réponse aux incidents efficace nécessite une planification et des ressources importantes.

Plusieurs types de modèles de financement peuvent être utilisés lors de la mise en place et de l'exploitation d'une CSIRT :

- un centre de coûts au sein d'une organisation, ou

- des subventions totales ou partielles, en détaillant la subvention, y compris l'émetteur et la source, l'objectif, le montant et la durée de la subvention si elle est déterminée.
- la vente de services en interne ou en externe
- le financement par un consortium d'organisations telles que des universités dans un réseau de recherche.
- ou une combinaison des propositions énumérées ci-dessus

Le financement doit couvrir :

- Les dépenses d'investissement (CAPEX) : pour couvrir les coûts initiaux liés à l'acquisition des composants matériels et logiciels, des équipements et outils, et des locaux.
- Les coûts d'exploitation (OPEX) : pour couvrir les coûts opérationnels récurrents liés à l'engagement avec la circonscription, le personnel, les installations et les licences logicielles, la prestation, la maintenance et l'entretien des services, la technologie, les processus et les capacités organisationnelles.

9.1. À quoi ressemble le budget d'une CSIRT ?

Un budget initial de la CSIRT est établi pendant la phase initiale de l'établissement de la CSIRT. Le guide de l'ENISA sur la mise en place d'une CSIRT et d'un SOC recommande que le budget pour l'année initiale couvre au moins :

- Les salaires du personnel initial,
- Les coûts d'établissement de l'installation,
- Les salaires ou les frais de services de consultance pour la création des résultats de la phase de conception,
- Le recrutement et la formation pour l'acquisition de compétences de la CSIRT, et
- La technologie et les licences préliminaires.

Ressource : Coûts indicatifs de la mise en place d'une CSIRT pour 2020

Poste budgétaire	**Coût moyen par an**
Membre du personnel de la CSIRT (y compris les managers)	40 000 - 60 000 EUROS

Trois membres du personnel minimum En fonction de la taille de la circonscription et du mandat, les CSIRT emploient généralement le personnel suivant : petit - 3-7, moyen - 10-15, grand - 30-60.	120 000 - 180 000 EUROS
12 employés supplémentaires (six équipes de deux membres pour une couverture 24/7, chaque équipe couvrant 8 heures) si nécessaire pour assurer des opérations 24/7, 365 jours par an.	480 000 EUROS
Location de bureaux par membre du personnel et par an	3 000 - 4 000 EUROS
Formation du personnel et participation à des conférences par personne et par an	3 000 - 10 000 EUROS
En fonction de la portée, services de conseil pour la mise en place d'une CSIRT (conception et mise en œuvre)	75 000 - 1 000 000 EUROS (sur une période de 1 à 3 ans)
Matériel, mise en réseau et équipement spécialisé pour l'exécution des opérations spécifiques de la CSIRT (l'utilisation de services cloud réduit les investissements initiaux en matériel)	100 000 - 300 000 EUROS
Logiciels et services logiciels (les solutions open-source peuvent réduire les coûts)	50 000 EUROS

Remarque : Les estimations des coûts sont fournies à titre d'exemple uniquement et ne représentent pas un pays en particulier.

Source : How to set up CSIRT and SOC, ENISA

Point de réflexion

Le guide de l'ENISA : How to set up CSIRT and SOC indique que « *L'écart entre le mandat détaillé et le budget est une raison courante pour laquelle les CSIRT ne remplissent pas leur mandat*. »
D'où la CSIRT nationale tire-t-elle son mandat ?
Quelles sont les sources de financement de la CSIRT nationale dans votre pays ?
Quel modèle de financement est utilisé dans votre pays ?
Quelles sont les considérations relatives au budget initial et au budget de fonctionnement ?

Laissez votre commentaire ci-dessous.

10. Capacités d'une CSIRT

10.1. Formation et certification

Le rôle d'une CSIRT est de gérer la réponse opérationnelle aux incidents, quel que soit le type d'incident, qu'il s'agisse d'incidents hors bande ou d'incidents quotidiens. Pour accomplir ces tâches, une CSIRT doit être efficace et professionnelle, avec des experts qualifiés dans le domaine de la sécurité informatique.

Vidéo : Profil du professionnel de la cybersécurité

La formation d'un professionnel de la cybersécurité : Écoutez comment bikozulu s'entretient avec le gourou de la cybersécurité, le Dr Bright Gameli

La formation aux compétences techniques et non techniques, l'analyse des logiciels malveillants, les systèmes de contrôle industriel/SCADA, la surveillance et l'analyse des cybermenaces, la communication orale/écrite, la gestion des relations aux niveaux international et national, la gestion du stress et la résolution des problèmes, ont été identifiés comme importants pour améliorer la fonctionnalité des CSIRT dans l'enquête du GFCE sur les pays à faible revenu. Les défis associés à l'acquisition de ces compétences, à savoir les budgets limités, le manque de formateurs compétents et les lourdes charges de travail, peuvent être surmontés par une collaboration régionale et internationale en matière de renforcement des capacités.

Bonnes pratiques : Rechercher le soutien des autres pour renforcer les capacités des CSIRT nationales

La référence à la Bonne pratique globale du GFCE - Équipes nationales de réponse aux incidents de sécurité informatique (CSIRT), le partage d'informations ainsi que la recherche de connaissances et d'expertise pour des solutions pratiques et applicables auprès des communautés mondiales et régionales sont essentiels pour la mise en place d'une CSIRT nationale. Renforcement des capacités par le biais de communautés telles que le Forum for Incident Response Teams (FIRST), AfriCERT, OIC-CERT, l'initiative Meridian process buddy.

Pour constituer la masse critique d'experts en cybersécurité nécessaire à la protection du continent, il est proposé que les pays envisagent d'initier dès leur plus jeune âge les enfants à la cybersécurité. Pour tirer parti de l'accès accru au haut débit, cette formation pourrait être dispensée en ligne.

Ressource :

Un objectif de la Stratégie de transformation numérique pour l'Afrique (2020-2030) est d'*offrir un programme massif de développement des e-compétences en ligne pour fournir des connaissances et des compétences de base en matière de sécurité et de confidentialité dans l'environnement numérique à 100 millions d'Africains par an d'ici 2021 et à 300 millions par an d'ici 2025.*

Sur la base de la classification des services dans le cadre des services CSIRT FIRST (*voir section 5.2*), le GFCE a développé une feuille de route des services N-CSIRT qui propose les exigences en termes de ressources, les connaissances, les aptitudes, les compétences, les politiques, les directives, les cadres, les outils et les formations nécessaires pour gérer chaque service.

Des formations adaptées aux équipes CSIRT sont proposées par Udemy, SANS National Initiative for Cybersecurity Education (NICE), EC Council, ISACA, IBM, ENISA, ISC2, eLearningSecurity, Cyber4Dev, CREST et des collaborations CSIRT mondiales dont AfricaCERT, ENISA, CIRCL, CERT-Tools Community, ICANN. Faites référence à la Section 4.

Exercice :

Une auto-évaluation de la capacité du N-CSIRT à partir des outils et du modèle de maturité ci-dessus peut aider à identifier les ressources et la formation nécessaires pour améliorer les services que l'équipe fournit aux membres de sa circonscription.

Sur la base des services existants et prévus de votre N-CSIRT, de quelle formation l'équipe a-t-elle besoin ?

Identifiez les prestataires de formation.

Étude de cas : L'expérience d'EG-CERT en matière de renforcement des capacités

L'Équipe nationale égyptienne de préparation aux urgences informatiques (EG-CERT), affiliée à l'Autorité nationale égyptienne de régulation des télécommunications (NTRA), a été lancée en avril 2009. EG-CERT offre des services réactifs et proactifs aux membres de sa circonscription qui travaillent dans les secteurs des TIC, de la finance et du gouvernement.

EG-CERT emploie plus de 60 professionnels (dont plus de 45 sont des professionnels de la cybersécurité à plein temps). Consciente de la nécessité d'habiliter les responsables CIIP dans les secteurs stratégiques et d'améliorer les compétences, la NTRA a organisé et parrainé un programme national pilote de formation à la cybersécurité entre 2009-2010. Le programme a formé 220 professionnels dans 38 organisations du secteur gouvernemental/public, du secteur bancaire, du secteur de l'éducation, ainsi que des entreprises du secteur privé des TIC. Les résultats du programme comprennent 179 certificats internationaux de SANS et une sensibilisation, une meilleure préparation et l'instauration d'un réseau de confiance et d'un meilleur esprit de coopération entre les entités et les professionnels participants.

Le parrainage financier de la NTRA a traduit l'engagement, le partenariat et le soutien du secteur public. Il a en outre inspiré d'autres programmes et obtenu la reconnaissance de l'Union internationale des télécommunications (UIT) dans l'indice mondial de cybersécurité, publié en 2015 et les années suivantes.

EG-CERT participe aux questions de cybersécurité nationale, notamment à l'élaboration et à la mise en œuvre de la Stratégie nationale égyptienne de cybersécurité, publiée pour la première fois en 2017, et au Conseil suprême égyptien de la cybersécurité (ESCC) créé en 2014. Au niveau régional et international, EG-CERT participe à des événements de collaboration, notamment les exercices internationaux de cybersécurité, menés sur une base annuelle avec la région Asie-Pacifique - exercice annuel de cybersécurité APCERT, exercices annuels de cybersécurité de l'Organisation des pays islamiques - OIC-CERT et exercice de cybersécurité de l'UIT pour les pays arabes. EG-CERT est membre du FIRST, et membre fondateur du CERT de l'Organisation des pays islamiques (OIC-CERT) et d'AfricaCERT.

Source :
Cyber Incident Management in Low-Income Countries - 1: PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT

10.2. Audit

Les audits de cybersécurité sont un élément essentiel de la stratégie et de la législation en matière de cybersécurité. Cependant, les compétences et les fonds nécessaires à la réalisation de ces audits sont limités.

L'analyse des incidents de cybersécurité contribuerait au renforcement des capacités et à la recherche et au développement (R&D), tandis que l'exploration d'un système de signalement et d'analyse des incidents de cybersécurité pour le continent africain serait utile.

10.3. Exercices de cybersécurité

Les capacités d'une CSIRT sont considérablement améliorées par des cyberentraînements faisant appel à des scénarios pour tester le niveau de préparation, la communication et les capacités de réponse.

Ressource : Améliorer les capacités grâce aux cyberentraînements

AfricaCERT
AfricaCERT a organisé son premier cyberexercice : Testing the Waters, en 2021. L'exercice visait à tester la capacité d'intervention des équipes participantes dans les scénarios suivants : hameçonnage, dégradation, REM, enquête sur les ransomwares. Ces exercices ont été conçus pour mettre les participants dans des conditions réelles et ont permis de tester leurs capacités techniques et de communication. 32 CSIRT de 24 pays, dont les équipes d'APCERT et d'OIC-CERT, ont participé à l'exercice.

APCERT
APCERT organise un cyber exercice pour la région APCERT et ses partenaires. Le thème de l'exercice 2021 d'APCERT était « Attaque de la chaîne d'approvisionnement par hameçonnage - Attention au travail à domicile ». L'exercice reflétait des incidents réels tout en soulignant la collaboration entre les économies pour atténuer les

cybermenaces. Il a validé les protocoles de communication améliorés, les capacités techniques et la qualité des réponses aux incidents qu'APCERT encourage pour garantir la sécurité et la sûreté de l'Internet. Vingt-cinq CSIRT représentant dix-neuf économies de l'APCERT et deux de l'OIC-CERT et de l'AfricaCERT ont participé à cet exercice.

UIT
L'UIT organise des cyberexercices annuels conçus dans un double objectif : servir de plate-forme pour la coopération, le partage d'informations et les discussions sur les questions actuelles de cybersécurité, et fournir des exercices pratiques aux CIRT / CSIRT nationales.

OEA
L'OEA (Organisation des États américains) et l'INCIBE (Institut national espagnol de cybersécurité) organisent chaque année l'International CyberEx qui vise à renforcer la capacité de réponse aux cyberincidents et à améliorer la collaboration et la coopération. L'International CyberEx 2020 comptait 80 équipes et 320 membres d'équipe représentant 39 pays.

OIC-CERT
L'OIC-CERT (Organisation de la coopération islamique - Équipes d'intervention en cas d'urgence informatique) organise chaque année un cyberexercice ciblant les objectifs suivants :
• Tester les capacités de communication des points de contact des membres.
• Vérifier les processus et procédures de gestion des événements imprévus.
• Tester les compétences techniques des équipes participantes.
• Simuler la coopération transfrontalière dans l'atténuation des incidents de sécurité de l'information.

Capture-The-Flag (CTF)
Il s'agit d'une compétition de sécurité informatique dans laquelle les participants s'affrontent dans des défis axés sur le thème de la sécurité afin d'obtenir le meilleur score.

Source :
Cyber Incident Management in Low-Income Countries - 1: PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT

11. Coordination et coopération régionales et mondiales

Le cyberespace étant transfrontalier, il est essentiel de coopérer en toute confiance avec les alliances et réseaux mondiaux de CSIRT, tels que le FIRST (Forum for Incident Response and Security Teams), le Forum africain des équipes d'intervention en cas d'incident informatique (AfricaCERT), le programme d'assistance aux CSIRT de Team

Cymru, le TF-CSIRT, le forum Ops-T (Operations Security Trust), l'OIC-CERT (Organisation de la coopération islamique - Équipes d'intervention en cas d'urgence informatique).

Ces réseaux offrent un forum pour la coopération, l'échange d'informations et l'instauration de la confiance, et ils renforcent les capacités des membres à gérer les incidents transfrontaliers et les réponses coordonnées aux incidents. L'adhésion à ces réseaux exige des équipes qu'elles remplissent un minimum d'exigences, notamment le paiement de cotisations annuelles. La reconnaissance du niveau de maturité de la CSIRT détermine le statut des membres.

Ressources : Trusted Introducer

La confiance est un élément essentiel de la coordination et de la coopération en matière de cybersécurité. Le service Trusted Introducer (TI) propose de solides critères d'adhésion et inclut des niveaux de maturité démontrés et vérifiés pour l'évaluation. Le service TI a établi un centre d'échange de confiance pour sa communauté CSIRT. Le service Trusted Introducer (TI) définit quatre catégories :

- les équipes sont
  - listées, ce qui fournit des informations de base sur l'équipe elle-même ainsi que sur l'approbation de l'équipe par la communauté TI. Les équipes maCERT pour le Maroc, MoRENet CSIRT pour le Mozambique, SA NREN CSIRT pour l'Afrique du Sud, CERT.tg pour le Togo sont listées ;
  - accréditées, ce qui garantit un niveau défini de bonnes pratiques et l'acceptation des politiques TI établies pour ces équipes. L'équipe SA NREN CSIRT pour l'Afrique du Sud est accréditée ;
  - certifiées, si elles ont été accréditées auparavant et si elles peuvent démontrer un niveau confirmé de maturité tel que défini par le cadre SIM de TI.
- les experts en sécurité peuvent participer en tant qu' Associés TI.

Les raisons pour lesquelles les CSIRT en Afrique devraient envisager de devenir une équipe listée Trusted Introducer (TI) sont les suivantes :

- exprimer un intérêt pour la cybersécurité sur une scène internationale
- fournir aux intervenants la preuve d'un engagement à suivre les défis contemporains en matière de sécurité et à respecter les meilleures pratiques et normes approuvées par la communauté
- offrir la possibilité de participer à différents projets de sécurité, dans lesquels le succès repose en grande partie sur les contributions des CSIRT de différents secteurs et de différentes circonscriptions
- apprendre des succès et des échecs des autres équipes lors de réunions personnelles en face à face et de présentations ou de briefings sur le sujet
- rencontrer d'autres équipes de sécurité trois fois par an dans différents sites européens, sur invitation d'équipes volontaires ou de communautés nationales

désireuses de soutenir les objectifs de la TF-CSIRT
- devenir membre d'un environnement très ouvert, amical et non compétitif qui entretient une discussion raisonnable et la recherche d'un consensus en dehors des pressions habituelles de l'activité quotidienne
- Après vous être familiarisé avec la communauté et les pratiques adoptées, vous pouvez entreprendre les démarches appropriées en vue de l'accréditation et de la certification

11.1. FIRST (Forum of Incident Response and Security Teams)

Le FIRST (Forum of Incident Response and Security Teams) offre un modèle d'adhésion aux CSIRT reposant sur la conformité aux critères d'évaluation et la visite du site (désormais virtuelle, à partir d'avril 2020 en raison des restrictions liées à la pandémie de COVID-19).

Il existe deux types d'adhésion :

- Les **membres titulaires** représentent des équipes de réponse aux incidents de sécurité qui aident une communauté des technologies de l'information ou une autre circonscription définie à prévenir et à traiter les incidents liés à la sécurité. Une fois l'adhésion confirmée, l'équipe doit s'acquitter d'un droit d'inscription initial unique de 800 USD pour devenir membre titulaire et d'une cotisation annuelle de 2 000 USD ;
- **Les membres de liaison** sont des individus ou des représentants d'organisations autres que les équipes de réponse aux incidents ou les équipes de sécurité qui ont un intérêt légitime et une valeur pour le FIRST. Le droit d'inscription initial ne s'applique pas aux membres de liaison, qui versent une cotisation annuelle de 100 USD.

Les avantages de l'adhésion au forum FIRST comprennent l'accès à un forum pour des interactions de confiance, le partage d'informations lors des conférences annuelles et des colloques techniques, des outils techniques et

11.2. AfricaCERT

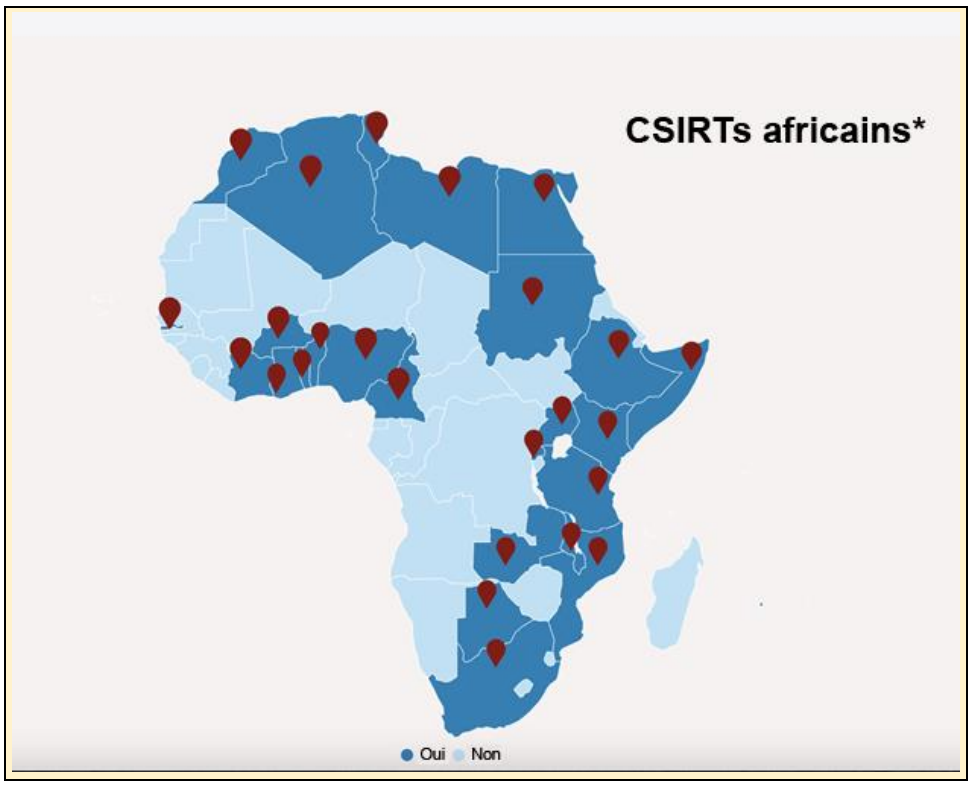
Les objectifs du Forum africain des équipes de réponse aux incidents informatiques (AfricaCERT) consistent à favoriser :
- la coordination et la coopération régionales et mondiales
- l'aide à la mise en place de CSIRT
- les programmes d'éducation et de sensibilisation
- les informations, les bonnes pratiques et le partage d'expériences
- l'amélioration de l'état de préparation et de la résilience à la cybercriminalité

- la recherche collaborative, le développement et l'innovation

L'adhésion à AfricaCERT se fait par le biais d'une demande appuyée par un sponsor. Le formulaire de candidature soumis par email est examiné et évalué par les membres du conseil d'administration d'AfricaCERT. Il existe 3 catégories de membres :

- Membre opérationnel : doit être situé en Afrique et doit être un participant actif aux affaires d'AfricaCERT.
- Membre de soutien : une entité de n'importe quelle région dont les activités sont liées à la cybersécurité, y compris les ONG et les universités.
- Membre individuel : les personnes intéressées peuvent demander une adhésion à titre individuel, parrainée par deux membres opérationnels d'AfricaCERT. Les membres individuels paient une cotisation de 25 USD.

Ressources : *Carte interactive des membres d'AfricaCERT* Source : DiploFoundation



11.3. Organisation de la Coopération Islamique - Équipe d'intervention en cas d'urgence informatique (OIC-CERT)

L'OIC-CERT (Organisation de la coopération islamique - Équipes d'intervention en cas d'urgence informatique) vise à soutenir la collaboration et la coopération des CERT dans les pays membres de l'OCI. L'OIC-CERT vise à :

- renforcer les relations entre les CERT des pays membres de l'OCI et les intervenants
- encourager le partage d'expériences et d'informations
- prévenir et réduire la cybercriminalité, harmoniser les politiques, les lois et les réglementations en matière de cybersécurité
- renforcer les capacités et la sensibilisation en matière de cybersécurité
- promouvoir la collaboration en matière de recherche, de développement et d'innovation dans le domaine de la cybersécurité

- promouvoir la coopération internationale
- contribuer à l'établissement et au développement des CERT nationales.

L'OIC-CERT compte 6 catégories de membres :

- Membre titulaire
- Membre général
- Membre professionnel
- Membre affilié
- Membre commercial
- Membre associé
- Membre honoraire

***Illustration 5** : Membres de l'OIC-CERT* Source : OIC-CERT

11.4. Initiative Meridian Process Buddy

Les pays peuvent établir une collaboration bilatérale et multilatérale. L'« initiative Buddy » du GFCE-Meridian est mentionnée comme une bonne pratique, en plus d'autres bonnes pratiques de mise en réseau et de partage d'informations.

Bonne pratique : Le système de jumelage

Une nation amie (ou une nation guide) peut partager, de manière formelle ou informelle,

dans un environnement
confidentiel, des approches et des enseignements précieux en matière d'organisation ou de processus avec une nation dont les politiques sont moins développées, les ressources et les connaissances limitées.

Les dispositifs d'élaboration de stratégies de cybersécurité au sein de l'Union africaine (UA) peuvent servir de système de jumelage.

12. Les femmes dans la cybersécurité

À l'échelle mondiale, les femmes sont sous-représentées dans le secteur de la cybersécurité et sont moins bien rémunérées que leurs homologues masculins. Diverses institutions cherchent à former, recruter et retenir les femmes dans le domaine de la cybersécurité, ainsi qu'à les aider à occuper des postes de direction et de gestion.

Le projet Gender and Cybersecurity: creating a more inclusive digital world (Genre et cybersécurité : créer un monde numérique plus inclusif) du GFCE vise à explorer les raisons possibles et les solutions pour remédier à cet écart entre les sexes dans le domaine de la cybersécurité. Peu de femmes en Afrique, et 10 % à l'échelle du globe, sont représentées dans la profession de la cybersécurité, car les étudiantes ne sont pas conscientes que ce domaine est une option de carrière. En outre, il est nécessaire de renforcer la confiance des femmes pour qu'elles puissent occuper des postes de direction et des postes stratégiques, et de leur offrir un mentorat. Le réseau de renforcement des cybercapacités des femmes du GFCE vise à améliorer la coopération et le partage des connaissances, à identifier les besoins en matière de cybercapacités au niveau régional et à soutenir la croissance d'une communauté de cyberexperts de confiance.

Ressource : *Podcast Combler l'écart entre les sexes en matière de cybersécurité avec Louise Marie Hurel et Angela Matlapeng*

Les femmes sont sous-représentées dans le domaine de la cybersécurité.

Le programme de mentorat Women in Cyber de l'UIT, organisé conjointement par le Partenariat mondial EQUALS et le FIRST (Forum for Incident Response Teams), vise à combler cette lacune. Le programme est le résultat du webinaire CyberDrill 2020 Empowering Women in Cybersecurity (Webinaire CyberDrill 2020 sur l'autonomisation des femmes dans le domaine de la cybersécurité), au cours duquel le besoin de modèles et de mentorat a été identifié comme essentiel pour augmenter le nombre de femmes leaders dans le domaine de la cybersécurité.

Dans cet épisode de UNconnected, Doreen Bogdan-Martin, directrice du Bureau de développement des télécommunications de l'UIT, s'entretient avec Louise Marie Hurel

et Angela Matlapeng qui ont participé au programme en tant que mentor et mentorée, respectivement. Elles présentent les défis et les opportunités pour les femmes dans le domaine de la cybersécurité, ainsi que la voie à suivre pour que les femmes puissent co-créer et mener des solutions dans ce domaine.

13. Conclusion

Félicitations, vous avez atteint la fin du module. Dans la partie finale, nous réfléchirons aux principaux points à retenir de ce module, en vous laissant un espace supplémentaire pour noter les points qui vous semblent importants et qui ne sont pas inclus ci-dessus.

À l'aide de ressources, d'exemples, de réflexions et d'exercices, nous avons examiné l'importance de la gestion des cyberincidents et du renforcement des capacités en matière de cybersécurité par la mise en place d'une CSIRT. Nous nous sommes familiarisés avec les services offerts par les CSIRT et nous avons identifié les outils et les compétences nécessaires à la gestion d'une CSIRT. Enfin, nous avons abordé l'importance de la coopération régionale et internationale et identifié les conditions d'adhésion aux réseaux régionaux et internationaux de CSIRT tels qu'AfricaCERT, FIRST et OIC-CERT.

Réflexion : les points importants

Notez 5 points importants que vous avez recueillis en suivant ce module.

Étapes suivantes

Passez à FIRST : La réponse aux incidents pour les décideurs politiques