CATALOGUE DES SERVICES OFFERTS

Version 1.0

Public

Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire
18 BP 2203, Abidjan 18 – Côte d'Ivoire
Tel : +225 20 34 43 73 / Poste : 51 00

TABLE DES MATIERES

1. SERVICES PROACTIFS

1.1. Analyse des vulnérabilités en ligne

Pôle : Gestion des incidents

Code de référence : SP-VA-01

Public cible : Gouvernement et ses démembrements, Administration publique, Opérateurs d'Infrastructures critiques

Objectif :

Tirer parti des capacités du secteur gouvernemental et privé pour améliorer la posture de sécurité

Description :

Le service d'analyse des vulnérabilités en ligne est fourni aux organisations du secteur gouvernemental et aux PME. L'objectif de ce service est d'aider les organisations concernées à maintenir la durabilité et la résilience de leurs systèmes d'information. En proposant l'analyse des vulnérabilités en tant que service, le CI-CERT vise à aider les organisations du secteur gouvernemental et les PME avec des outils de base pour identifier les faiblesses techniques et améliorer la sécurité technique de leurs systèmes d'information.

Exigences :

Signature d'une convention ou envoi de mail à l'adresse infos@cicert.ci

Livrables :

Analyse des vulnérabilités en ligne dans un environnement de confiance à l'aide l'outils les plus recommandés. Génération de rapports d'analyse des vulnérabilités avec démonstration des risques de gravité et recommandations.

1.2. Tests de pénétration

Pôle : **Gestion des incidents**

Code de référence : **SP-PT-02**

Public cible : **Gouvernement et ses démembrements, Administration publique, Opérateurs d'Infrastructures critiques**

Objectif :

Maintenir la résilience dans les agences gouvernementales et les entreprises privées en évaluant le niveau de sécurité dans les systèmes d'information.

Description :

En tant que partenaire de confiance, le CI-CERT effectuera des tests de pénétration sur la base de convention avec les parties prenantes.
Ce service examinera les systèmes d'information afin de déterminer les problèmes de sécurité, y compris la configuration incorrecte du système, les vulnérabilités logicielles ou matérielles, les faiblesses de sécurité et les faiblesses des applications Web. Cet exercice comprendra des tentatives de compromission du système et d'exploitation des vulnérabilités du point de vue d'un attaquant. Il aidera les organisations à évaluer leur statut de sécurité réel. Le CI-CERT fournira des recommandations et des avis techniques basés sur l'évaluation, et leur application relèverait de la responsabilité de l'organisation.

Exigences :

- Signature d'un accord de non-divulgation (NDA) ;
- L'approbation de la structure concernée est obligatoire pour commencer à exécuter ce service. Elle doit comprendre et accepter les risques et les impacts commerciaux qui pourraient être encourus au cours de cet exercice. Ces informations seront partagées avec l'organisme avant l'exécution de ce service.

Livrables :

- **Rapports d'évaluation de la sécurité** : exécutif (pour les cadres supérieurs) et technique (pour les administrateurs informatiques). Les rapports contiennent des constatations et des recommandations.
- **Activités de suivi** pour aider à mettre en œuvre les recommandations et à atténuer les risques.

1.3. Alertes et avis de sécurité

Pôle : Cyberintelligence

Code de référence : SP-AS-02

Public cible : Tous publics

Objectif :

Diffuser des informations en temps sur les menaces et vulnérabilités.

Description :

Fournissez des alertes avec des informations détaillées sur les menaces, les vulnérabilités et les risques dans les technologies de l'information et les logiciels ou matériels de communication susceptibles d'intéresser le public. Les alertes incluent des informations spécifiques au fournisseur ainsi que des détails provenant d'autres tiers. Les alertes incluent également une résolution détaillée, un correctif ou une solution de contournement pour aider les clients à atténuer le risque.

Exigences :

Inscription à la newsletter.

Livrables :

Alertes et avis par e-mail, avec des informations détaillées sur les menaces et les vulnérabilités.

1.4. Bulletin de sécurité

Pôle : Cyberintelligence

Code de référence : SP-BS-03

Public cible : Tous publics

Objectif :

Diffuser les connaissances sur les problèmes de sécurité essentiels non urgents, y compris les actualités, les vulnérabilités, les menaces et les outils liés à la sécurité de l'information.

Description :

Fournir des informations périodiques non urgentes et des mises à jour relatives aux menaces de cybersécurité, aux vulnérabilités, aux actualités sur la sécurité de l'information, aux annonces, aux outils, aux normes, aux livres, aux livres blancs, aux conférences, aux techniques de cybercriminalité, à l'analyse technique, etc.

Exigences :

S'abonner à la newsletter

Livrables :

Bulletin d'information par e-mail contenant des informations non urgentes, avec des mises à jour mondiales sur la sécurité des informations.

1.5. Rapports de sécurité

Pôle : Cyberintelligence

Code de référence : SP-RS-03

Public cible : Tous publics

Objectif :

Accroître la sensibilisation du grand public aux dernières tendances en matière de sécurité de l'information, qui concerne la Côte d'Ivoire.

Description :

Fournir un rapport sur l'état des menaces de sécurité au niveau national. Ce rapport présente les résultats que le CI-CERT a obtenu à partir de diverses ressources, y compris ses propres capteurs et des capteurs tiers. Les données collectées sont analysées pour mieux comprendre les menaces actuelles, les tendances et l'atténuation des risques.

Exigences :

Inscrivez-vous sur la liste de diffusion (www.cicert.ci) pour vous abonner aux rapports de sécurité.

Livrables :

Rapport de cybersécurité.

1.6. Sensibilisation à la cybersécurité

Pôle : Cyberintelligence

Code de référence : SP-SC-04

Public cible : Tous publics

Objectif :

Aider les utilisateurs de technologie à comprendre les principes fondamentaux de la sécurité de l'information, les menaces associées à l'utilisation des technologies de l'information ou de la communication et des pratiques sécurisées pour minimiser l'occurrence des incidents.

Description :

Toute personne travaillant dans un environnement axé sur la technologie doit être exposée aux menaces auxquelles ces environnements sont confrontés du point de vue d'une utilisation prévue régulière.

Pour tirer le meilleur parti de la technologie, les utilisateurs doivent être habilités à connaître les pratiques et méthodes sécurisées afin de minimiser les risques associés à leur utilisation.

Exigences :

Aucune

Livrables :

Plaquettes de sensibilisation.

2. SERVICES REACTIFS

2.1. Réponse aux incidents

Pôle : **Gestion des incidents**

Code de référence : **SR-RI-01**

Public cible : **Tous publics**

Objectif :

Minimisez les risques associés aux incidents de sécurité des informations.

Description :

Le service de réponse aux incidents du CI-CERT fournit la capacité de traiter et de répondre aux incidents de sécurité qui peuvent survenir dans un système d'information.
Si un incident de sécurité de l'information se produit en Côte d'Ivoire, n'importe qui peut s'adresser à CI-CERT pour profiter de son expertise dans la gestion de tels incidents et minimiser les dommages pouvant résulter de l'incident.
Le CI-CERT a une approche formelle, ciblée et coordonnée pour répondre aux incidents de sécurité de l'information et peut fournir aux organisations une réponse efficace aux incidents.
Le CI-CERT est facilement accessible et disponible par téléphone au 20 34 43 74 Poste 5100 du lundi au vendredi de 08h à 12h et de 13h à 17h, par e-mail à l'adresse **incidents@cicert.ci** et en ligne sur le site **https://www.cicert.ci** .
Sur demande, le CI-CERT peut vous aider à répondre à un incident de sécurité et guider la restauration grâce à une analyse efficace. Grâce à ses collaborations internationales, le CI-CERT, ainsi que les équipes régionales d'intervention en cas d'urgence informatique, peuvent fournir des réponses plus rapides si l'attaque provient d'une source étrangère.
Avec l'aide du CI-CERT, les entreprises peuvent réagir rapidement et efficacement aux incidents de sécurité de l'information, réduisant ainsi les pertes et la restauration plus précoce des opérations normales.

Exigences :

Suivre les directives de réponse aux incidents.

Livrables :

Rapport d'incident.

2.2. Analyse Forensique

Pôle : Gestion d'incidents

Code de référence : SR-AF-02

Public cible : Gouvernement et ses démembrements, Administration publique, Opérateurs d'Infrastructures critiques

Objectif :

Enquêter dans le cadre d'infractions liées à la cybercriminalité à l'effet de mettre en évidence les preuves numériques de la réalisation de l'infraction.

Description :

Le CI-CERT offre des services d'analyse forensique basés sur ses capacités d'enquête. La portée des services comprend les enquêtes sur les incidents en direct, les enquêtes et analyses post-incident, les crimes liés à l'infrastructure de l'information.

Le CI-CERT peut aider également contribuer à enquêter sur les réseaux, les crimes mobiles, la reconstruction de sessions et la récupération des mots de passe.

Exigences :

Lettre d'autorisation écrite de la direction générale et du service juridique représentant les intérêts de l'organisation.

Réquisition signée par le Procureur de la République.

Livrables :

Un rapport d'enquête complet soutenu par des preuves numériques traitées à partir d'une analyse médico-légale.

2.3. Analyse de logiciels et fichiers malveillants

Pôle : Gestion de vulnérabilités

Code de référence : SR-MA-03

Public cible : Tous publics

Objectif :

Collecte et analyse des cybermenaces en Côte d'Ivoire pour déterminer l'effet de ces menaces sur le cyberespace national.

Description :

Le CI-CERT peut fournir une analyse des fichiers binaires ou autres codes malicieux pour identifier les menaces potentielles ou les preuves de contenu malveillant.

Ces fichiers binaires peuvent être collectés comme preuves et soumis pour analyse. Ceux-ci peuvent être récupérés à partir d'exploits impliquant des cyberattaques, ou la compromission de l'infrastructure d'information.

Exigences :

Aucune

Livrables :

Un rapport complet montrant l'effet du fichier binaire sur les actifs et les ressources d'information infectés.

3. SERVICES DE MANAGEMENT DE LA QUALITE DE LA SECURITE DE L'INFORMATION

3.1. Conseils en sécurité informatique

Pôle : **Gestion des incidents**

Code de référence : **SMSI-CS-01**

Public cible : **Gouvernement et ses démembrements, Administration publique, Opérateurs d'Infrastructures critiques**

Objectif :

Faire des recommandations relatives à l'utilisation, l'intégration de technologies et de systèmes. Des directives spécifiques peuvent également être publiées.

Description :

Le CI-CERT peut fournir des services de conseil en sécurité spécialisés spécifiques au secteur, tels que des conseils de sécurité de l'information sur la sécurité des appareils embarqués, la sécurité des appareils mobiles, les services basés sur le cloud, etc.

Exigences :

Les services sont fournis sur demande auprès des organisations de tous les secteurs. Les services sont également proposés sur la base d'exigences claires pour des conseils sur des systèmes critiques très spécifiques et sophistiqués.

Livrables :

Le CI-CERT fournira des conseils de sécurité spécialisés, élaborera des normes spécifiques et des meilleures pratiques aux constituants éligibles dans des secteurs critiques spécifiques.

3.2. Formation et développement des capacités en cybersécurité

Pôle : **Cyberintelligence**

Code de référence : **SMSI-CB-02**

Public cible : **Gouvernement et ses démembrements, Administration publique, Entreprises et les organisations privées, Universités et centres de recherche.**

Objectif :

Développer la capacité de main-d'œuvre au sein des organisations constituantes pour sécuriser l'infrastructure technologique de la nation. Donner au personnel technique des organisations constituantes les connaissances nécessaires pour soutenir la mise en œuvre des politiques standard de l'industrie et des contrôles pertinents.

Description :

Une des missions essentielles du CI-CERT est de fournir aux parties prenantes des programmes de formation reconnus internationalement. Les participants peuvent obtenir au terme des formations, des certifications reconnues internationalement en remplissant les conditions du programme. Les programmes de formation sont annoncés aux parties prenantes par plusieurs moyens (par exemple par courrier électronique) et également par courrier adressé à leur direction.

Exigences :

Expérience en informatique ou en génie : les stagiaires doivent démontrer leur engagement à acquérir de nouvelles connaissances et compétences, souscrire aux exigences du programme et s'efforcer de satisfaire aux exigences de certification.

Livrables :

Connaissances et compétences techniques spécifiques à la sécurité de l'information. Un certificat internationalement reconnu peut-être obtenu en réussissant l'examen et en répondant aux exigences du programme.

3.3. Base de connaissance nationale pour la gestion de la sécurité de l'information

Pôle : Sécurité de l'information

Code de référence : SMSI-BC-03

Public cible : Tous publics

Objectif :

Amélioration des connaissances en matière de sécurité de l'information.

Description :

Le CI-CERT maintiendra une bibliothèque de documents liés aux meilleures pratiques et normes de sécurité de l'information, y compris les politiques de gestion des identités et des accès (GIA) et les outils connexes, ainsi que les références liées à la résilience et à l'évaluation des risques. Ceux-ci seront disponibles comme point de référence unique pour les agences gouvernementales et les autres mandants intéressés.

Exigences :

Aucune exigence.

Livrables :

Politiques de gestion des identités et des accès GIA et outils et documents connexes Documents relatifs aux politiques et aux normes internationales Documents relatifs à l'évaluation des risques et à la résilience, y compris l'évaluation de la sécurité et les références aux tests de pénétration. Tous les efforts seront faits pour s'assurer que les documents sont à jour et à jour.

3.4. Conseil en management de la sécurité de l'information

Pôle : Sécurité de l'information

Code de référence : SMSI-MS-04

Public cible : Gouvernement et ses démembrements, Administration publique, Infrastructures critiques

Objectif :

Aider à améliorer la posture de sécurité.

Description :

À la demande des mandants concernés, le CI-CERT examinera la maturité de la sécurité de l'information au sein de l'organisation en termes de gestion et d'exigences techniques. Le CI-CERT aidera à l'élaboration de leurs politiques, procédures et normes, et les conseillera sur leurs efficacité, exhaustivité et conformité aux normes acceptées.

Exigences :

La responsabilité de l'application et du respect de ces politiques et normes incombe au constituant.

Livrables :

Rapports, avis et recommandations.

3.5. Conseils en continuité des activités et reprise après sinistre

Pôle : Sécurité de l'Information

Code de référence : SMSI-CA-05

Public cible : Gouvernement et ses démembrements, Administration publique, Infrastructures critiques

Objectif :

Améliorer la résilience et l'état de préparation actuels de l'infrastructure nationale d'information critique.

Description :

Participer à la conception, à l'examen et à la validation des plans de continuité des activités et de reprise après sinistre en offrant des conseils d'experts en la matière, basés sur les meilleures pratiques internationales dans le domaine, comme le préconisent des organisations et normes de référence.

Exigences :

À la demande des mandants éligibles, le CI-CERT examinera, validera et proposera des recommandations concernant l'efficacité et l'état de préparation des mesures de contrôle existantes ou prévues dans les plans de continuité et de reprise d'activités. Les prérequis incluent l'évaluation des risques et l'analyse de l'impact commercial.

Livrables :

Services de conseil spécifiques au domaine (y compris la conception de stratégies, de politiques et de tests de continuité des activités et de reprise après sinistre basés sur les meilleures pratiques internationales). Les recommandations émises par le CI-CERT ne constituent ni ne remplacent la certification ou la conformité aux normes internationales. Fonctions associées : visites sur place, entretiens, revue de la documentation, analyse technique et ateliers.

3.6. Appui à la mise en conformité des infrastructures critiques nationales

Département : Sécurité de l'Information

Code de référence : SMSI-CI-06

Public cible : infrastructures critiques nationales

Objectif :

Aider les opérateurs d'infrastructures critiques à améliorer les pratiques de sécurité et à se conformer aux normes et règlements applicables.

Description :

Le CI-CERT a une approche proactive envers les OIC en les aidant à définir leur stratégie de sécurité de l'information, en sélectionnant les normes de sécurité de l'information appropriées et applicables, et en fournissant des conseils objectifs en vue de la conformité.

En plus d'agir en tant que conseillers sur l'efficacité des politiques, l'exhaustivité et la conformité aux normes acceptées, le CI-CERT aidera à examiner, développer des politiques, des procédures et des normes.

Exigences :

Soutien de la direction des OIC et pré-consentement à l'effort. Ressources dédiées et compétentes de l'OSC.

Livrables :

- Service de conseil et d'orientation de bout en bout.
- Lignes directrices conformes aux meilleures pratiques internationales et futurs cadres nationaux Ivoiriens.