RÉPUBLIQUE TOGOLAISE

ANCy
Agence Nationale de la Cybersécurité

RAPPORT D'ACTIVITÉS

2024

Agence Nationale de la Cybersécurité (ANCy)

RAPPORT D'ACTIVITÉS DE L'AGENCE NATIONALE DE LA CYBERSECURITÉ

ANNÉE

2024

Sommaire

Liste des sigles et abréviations

ADNEC	Abu Dhabi National Exhibition Centre
ANCy	Agence Nationale de la Cybersécurité
ANID	Agence Nationale d'Identification
ARCOP	Autorité de Régulation de la Commande Publique
ARSE	Autorité de Régulation du Secteur de l'Energie
ASAIGE	Autorité de Sécurité de l'Aéroport International Gnassingbé Eyadema
ATD	Agence Togo Digital
CDA	Cyber Defense Africa
CEDEAO	Communauté Économique des États de l'Afrique de l'Ouest
CERT	Computer Emergency Response Team
CIFAF	Centre International de Formation en Afrique des Avocats Francophones
CNDH	Commission Nationale des Droits de l'Homme
CPES	Cellule Présidentielle d'Exécution et de Suivi des projets prioritaires
CSIRT	Computer Security Incident Response Team
CTF	Capture The Flag
DCPJ	Direction Centrale de la Police Judiciaire
EPL	École Polytechnique de Lomé
EPS	Évènement par Seconde
FAIEJ	Fonds d'Appui aux Initiatives Économiques des Jeunes
FIHA	Festival International d'Histoire d'Aného
FISA	Forum International des Secrétaires et Assistant Administratif
FITD	Forum International sur la Transformation Digitale
FNFI	Fonds National de la Finance Inclusive
INAM	Institut National d'Assurance Maladie
IPDCP	Instance de Protection des Données à Caractère Personnel
IYF	International Youth Fellowship
MENTD	Ministère de l'Économie Numérique et de la Transformation Digitale
PME/PMI	Petites et Moyennes Entreprises / Petites et Moyennes Industries
PR	Président de la République
SIEM	Security Information and Event Management
SNCy	Stratégie Nationale de Cybersécurité
SOC	Security Operation Center

Liste des tableaux

Liste des figures

Liste des graphiques

Mot du Directeur Général

« L'année 2024 a été un tournant majeur pour la cybersécurité au Togo, marquée par des avancées stratégiques et une reconnaissance internationale. »

Grâce à des efforts soutenus et au leadership des autorités nationales, le Togo a intégré le Tier 2 du classement mondial de cybersécurité, se positionnant parmi les leaders mondiaux tels qu'Israël, la Suisse et la Chine, avec un score de 88,8 selon l'Indice mondial de cybersécurité de l'Union Internationale des Télécom (IUT). Cette progression rapide, inédite entre 2018 et 2024, témoigne des actions déterminantes entreprises pour sécuriser l'espace numérique national.

En 2024, plusieurs réalisations clés ont jalonné le parcours de notre pays, notamment la publication de la Stratégie Nationale de Cybersécurité 2024-2028, véritable feuille de route pour l'écosystème numérique, et l'adoption de référentiels d'exigence pour les prestataires de services, la qualification des produits de cybersécurité et l'agrément des centres d'évaluation. De plus, des campagnes de sensibilisation et des efforts de renforcement des capacités ont également permis de développer une culture numérique inclusive et résiliente.

Pour 2025, nous concentrerons nos efforts autour de trois priorités majeures :

- Intensification de la sensibilisation et de la formation, notamment auprès des jeunes et des professionnels, pour développer une véritable culture de cybersécurité ;
- Démarrage effectif de la qualification des prestataires de services de confiance en cybersécurité et des produits de sécurité, pour garantir des standards élevés de sécurité numérique à nos opérateurs de services essentiels (OSE) ;
- Renforcement de la lutte contre la cybercriminalité, en collaboration avec les acteurs publics et privés, pour protéger efficacement les infrastructures numériques et les citoyens.

Comme vous l'aurez constaté, l'année 2025 s'annonce tout aussi déterminante que la précédente. Avec une résolution renouvelée, nous nous engageons à poursuivre nos efforts pour consolider ces acquis et à relever ceux à venir.

Je tiens à remercier les uns et les autres, pour votre soutien indéfectible et votre précieuse collaboration. Ensemble, continuons à bâtir un futur numérique sûr et prospère pour tous.

Je vous remercie.

Commandant Gbota GWALIBA
Directeur Général

Introduction

En 2024, le paysage mondial de la cybersécurité a continué d'évoluer sous l'effet de menaces de plus en plus sophistiquées, exploitant des vulnérabilités inédites. Simultanément, l'intensification des régulations internationales en cybersécurité a incité les États à renforcer leurs mécanismes de protection pour garantir la résilience numérique.

En Afrique, l'intégration croissante à l'économie numérique mondiale a généré de nombreuses opportunités économiques, mais également une exposition accrue aux cybermenaces.

La transformation numérique accélérée, l'essor de l'intelligence artificielle, et l'interconnexion massive des infrastructures critiques ont complexifié ces défis.

Le Togo, acteur clé en matière de digitalisation et de connectivité en Afrique, n'a pas échappé à cette dynamique, renforçant sa position en intégrant la catégorie Tier II «Advancing » du classement de l'Union Internationale des Télécommunications (UIT). Face à ces enjeux, l'Agence Nationale de la Cybersécurité (ANCy) a joué un rôle central en protégeant les infrastructures critiques, en sensibilisant la population sur les comportements sécurisés, et en collaborant avec des partenaires régionaux, internationaux et privés.

Ces efforts ont permis au Togo de progresser significativement dans la protection de son cyberespace, tout en posant les bases d'une cybersécurité durable.

Le présent rapport d'activités est un document clé qui s'inscrit dans la continuité des efforts initiés les années précédentes. Il met en lumière les progrès tangibles réalisés dans la protection du cyberespace togolais en 2024, analyse les leçons apprises, oriente les priorités stratégiques futures et réaffirme l'engagement du Togo à devenir une référence en matière de cybersécurité en Afrique.

CHAPITRE I

Présentation de l'Agence Nationale de la Cybersécurité (ANCy)

1.1 Les attributions et missions de l'ANCy

Créée par la loi **n° 2018-026 du 7 décembre 2018** modifiée par la loi **n° 2022-009 du 24 juin 2022** sur la cybersécurité et la lutte contre la cybercriminalité, l'Agence Nationale de la Cybersécurité (ANCy) est régie par le décret **n° 2019-026/PR du 13 février 2019**, qui définit son organisation, ses attributions et son fonctionnement.

Placée sous l'autorité du Premier Ministre, Président de son comité stratégique, l'ANCy est administrativement et techniquement rattachée au ministère en charge de l'économie numérique et de la transformation digitale, ainsi qu'au ministère de la sécurité et de la protection civile.

En tant qu'autorité nationale en matière de sécurité des infrastructures essentielles et des systèmes d'information, l'ANCy joue un rôle clé dans la définition et l'exécution de la politique nationale de cybersécurité. Elle contribue activement à la défense et à la sécurité de la République Togolaise. A ce titre elle est chargée de :

- Coordonner l'action gouvernementale en matière de sécurité et de défense des systèmes d'information ;
- Répondre aux crises affectant ou menaçant la sécurité informatique des infrastructures essentielles au Togo ;
- Fixer les règles de cybersécurité et veiller à leur application par les divers acteurs ;
- Certifier les dispositifs matériels ou logiciels de cybersécurité en République togolaise ;
- Contrôler le bon fonctionnement du CERT (Computer Emergency Response Team) et du SOC (Security Operation Center) national opérés par CDA ;
- Désigner et auditer les Opérateurs de Services Essentiels (OSE) ;
- Délivrer des agréments aux centres d'évaluation ;
- Qualifier les prestataires de service de confiance en cybersécurité et les produits de sécurité ;
- Participer à la lutte contre la cybercriminalité ;
- Former et sensibiliser le public en cybersécurité.

Pour accomplir convenablement ses missions, l'ANCy est dotée d'un cadre de gouvernance, composé d'un comité stratégique et d'une direction générale.

1.2 Gouvernance de la cybersécurité

1.2.1 Cadre de Gouvernance de l'ANCy

1.2.1.1 Le Comité Stratégique

Placé sous l'autorité du Premier Ministre, le Comité stratégique est l'organe d'administration et de gouvernance de l'ANCy. Sur les orientations du Président de la République, il élabore les propositions relatives à la politique nationale de cybersécurité, procède aux arbitrages et validations et autorise tous les actes et opérations relatifs aux missions de l'Agence.

Le Comité Stratégique est composé des membres suivants :

- Le Premier Ministre, président ;
- Le Ministre chargé de la sécurité, membre ;
- Le Ministre chargé de la défense, membre ;
- Le Ministre chargé de la justice, membre ;
- Le Ministre chargé de l'économie numérique, membre ;
- Deux (2) représentants de la Présidence de la République, membres.

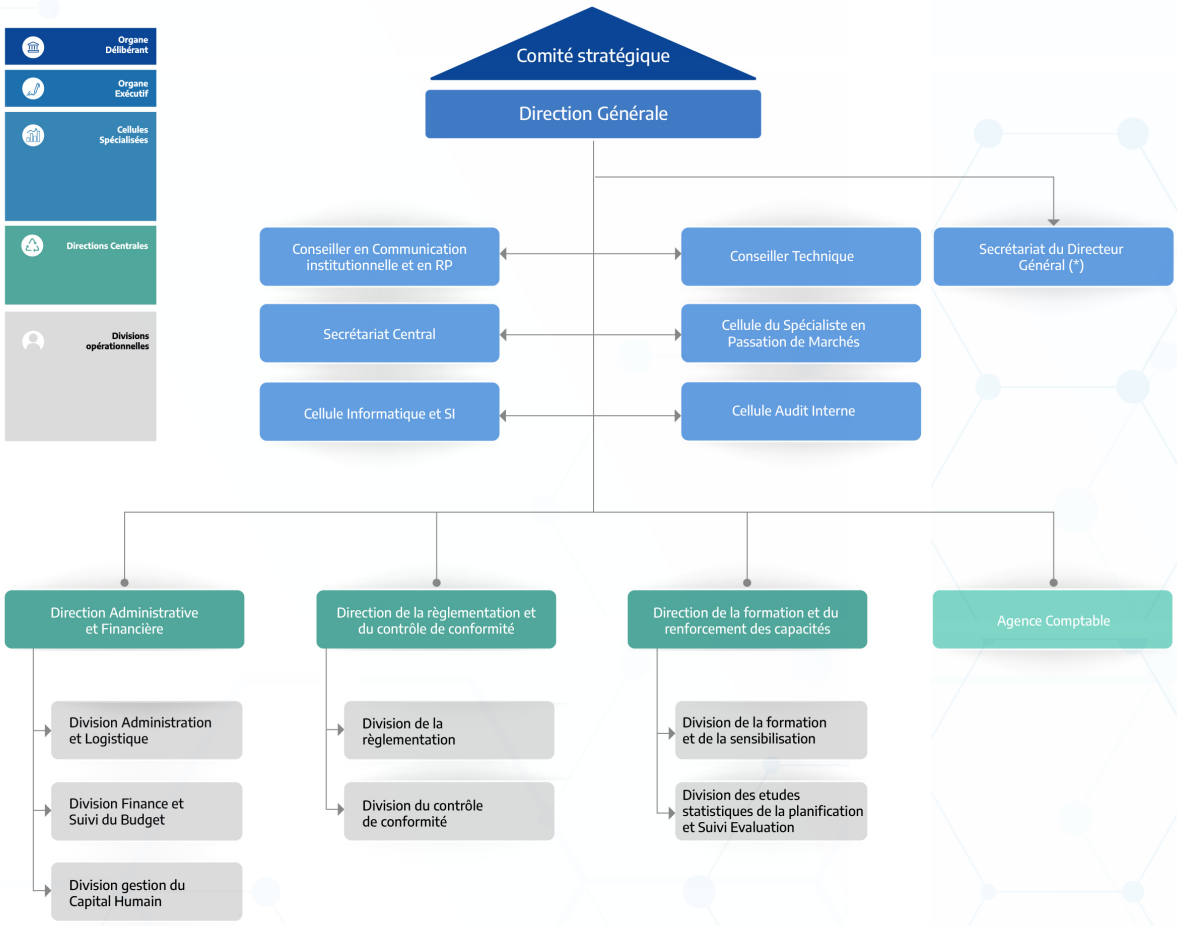


Figure 1 : Organigramme de l'ANCy

1.2.1.3. La Direction Générale

La direction de l'Agence nationale de la cybersécurité (ANCy) est assurée par un Directeur Général, nommé par décret du Président de la République, pour un mandat de trois (3) ans renouvelables une fois. Sous le contrôle du Comité Stratégique, le Directeur Général a plusieurs responsabilités, dont :

- Proposer des réformes juridiques et institutionnelles nécessaires à la mise à niveau de la législation nationale au regard du caractère évolutif des menaces technologiques ;
- Négocier et signer, selon les directives générales du comité stratégique, les accords et conventions nationaux et internationaux dans le cadre des missions de l'ANCy ;
- Établir le plan d'organisation et de fonctionnement des services de l'Agence.

Le Directeur Général est le garant de la sécurité et de l'efficacité opérationnelle de l'ANCy dans son rôle de protection des systèmes d'information au Togo.

La Direction Général comprend :

- La Direction administrative et financière ;
- La direction de la réglementation et du contrôle de conformité ;
- La direction de la formation et du renforcement des capacités.

Toutes les missions susmentionnées s'inscrivent dans un cadre juridique bien précis.

Photo 1 : siège de l'ANCy

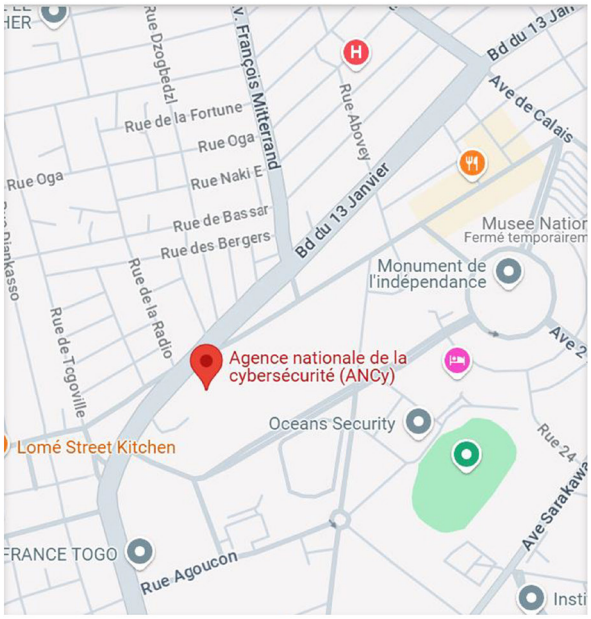


Figure 2 : Localisation géographique de l'ANCy

1.3 Le cadre juridique de la cybersécurité au Togo

La cybercriminalité est aujourd'hui au cœur des préoccupations des États, des Organisations Internationales et des entreprises dans un contexte de dépendance croissante aux technologies numériques. Pour répondre efficacement aux défis posés par la menace cyber, un cadre juridique robuste adossé aux textes internationaux a été mis en place par les autorités togolaises. Les objectifs poursuivis par ce cadre juridique sont de quatre (4) ordres : protéger les infrastructures critiques, garantir la souveraineté numérique, renforcer la coopération internationale et assurer les droits fondamentaux des citoyens face aux risques liés au cyberespace.

1.3.1 Les textes internationaux

Il s'agit notamment de :

- La Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée à Malabo en Guinée Équatoriale le 27 juin 2014 ; et
- La Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

1.3.2 Les textes nationaux

Ils sont composés d'une (1) loi, de trois (3) décrets et d'un (1) arrêté.

- Loi n°2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n°2022- 009 du 24 juin 2022 ;
- Décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'agence nationale de la cybersécurité ;
- Décret n°2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Décret n°2022-090/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- Arrêté n°2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

RÉPUBLIQUE TOGOLAISE

Ministère de l'Economie Numérique et de la Transformation Digitale

CHAPITRE II

La Gestion Administrative

2.1. Mise en place d'un environnement de stage équipé

Il a été mis en place un environnement de travail équipé, pour accueillir les étudiants togolais en fin de parcours dans le domaine de la cybersécurité, et qui ont besoin d'un stage de fin de formation. Cet environnement de travail s'efforce d'être le plus pratique possible en dupliquant l'environnement réel de travail des équipes de l'ANCy et de CDA.

Ce qui permettra aux stagiaires de toucher du doigt les réalités opérationnelles quotidiennes des équipes. Cette initiative s'inscrit dans le cadre du Pilier 1 de la Stratégie Nationale de Cybersécurité (SNCy), qui vise le développement des compétences techniques nationales.

L'objectif est de former une main-d'œuvre qualifiée et opérationnelle pour répondre aux besoins croissants du marché de la cybersécurité au Togo.

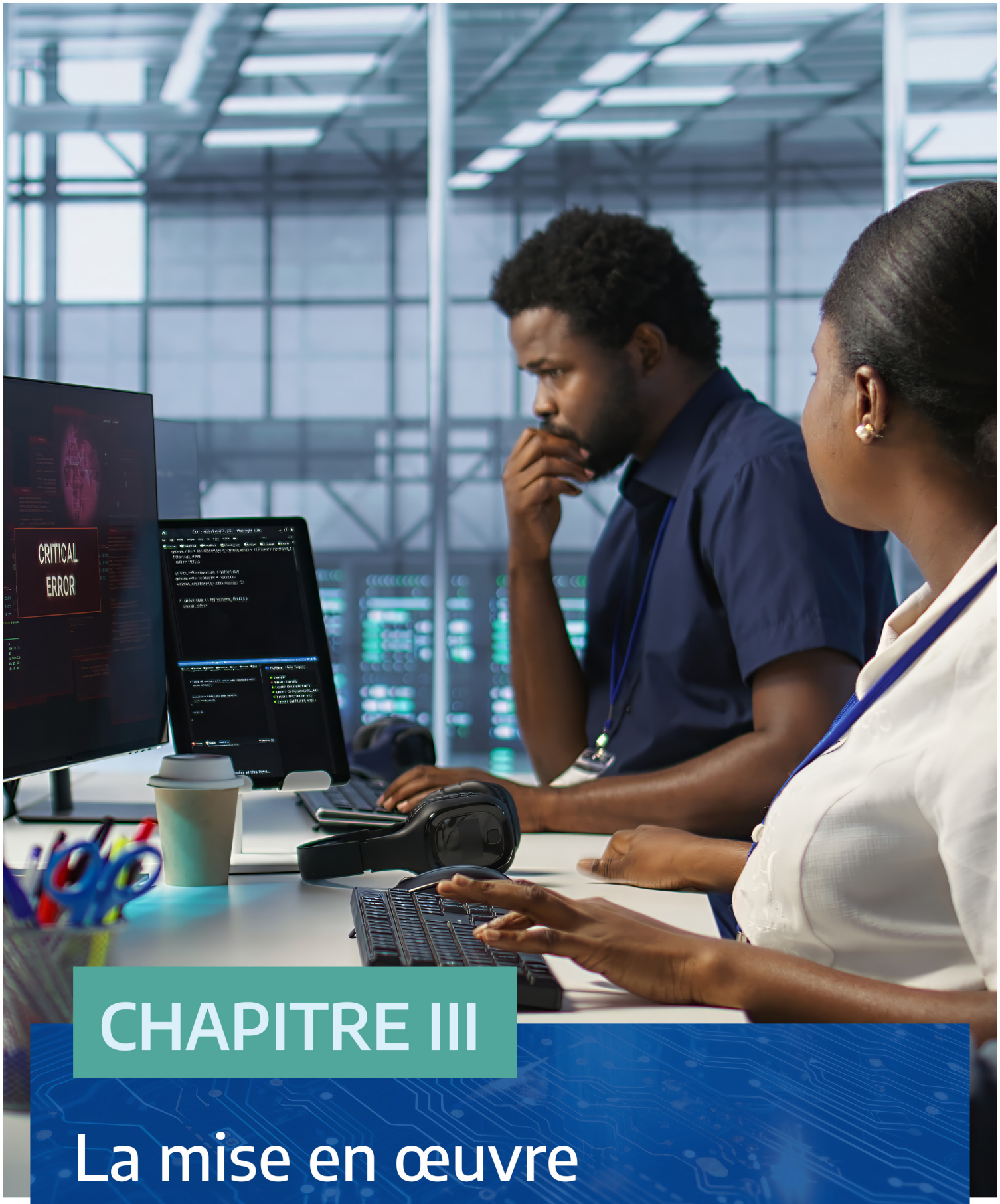
Avec l'expansion rapide du secteur, les prestataires de services seront d'ailleurs contraints de recruter des profils disposant de qualifications spécifiques. En offrant un environnement de stage équipé pour compléter les formations et les aligner véritablement sur les réalités du marché, l'ANCy contribue directement à l'amélioration des compétences locales et à l'augmentation des opportunités d'emploi dans le domaine de la cybersécurité.

2.2. La réunion du Comité Stratégique de l'ANCy

L'ANCy a également procédé à l'adoption de nouveaux outils de gestion. En effet, la réunion du Comité Stratégique de l'ANCy, qui s'est tenue le mardi 3 décembre 2024 à la Primature, a permis de faire le point sur les activités de l'Agence pour l'année 2024.

Elle a également conduit à l'adoption de plusieurs documents essentiels pour son fonctionnement, notamment les référentiels d'exigence pour les prestataires de services de confiance, ainsi que les modèles de qualification des produits de sécurité et d'agrément des centres d'évaluation en cybersécurité.


CYBER
SECURITY



CHAPITRE III

La mise en œuvre des missions

3.1. Les missions opérées par l'ANCy

3.1.1. Le renforcement des capacités internes de l'ANCy

Dans le but d'évaluer l'effectivité et l'efficacité du projet de Plan national de réponse aux incidents informatiques avant soumission au Comité stratégique, l'ANCy a organisé deux exercices respectivement le 23 mars et le 24 août 2024. Ces exercices sont des simulations d'attaques réelles destinées à tester la capacité de l'ANCy à répondre à un incident de cybersécurité dans des conditions proches de la réalité. Ils permettent de s'entraîner à répondre à des incidents, avec des cyberattaques hypothétiques lancées. Ces exercices ont surtout permis de tester la fluidité du Plan national de réponse en cas d'incidents informatiques.

L'ensemble du personnel de l'ANCy a également été formé sur la protection des données à caractère personnel. En effet, dans le cadre de la mise en conformité avec les exigences légales nationales et internationales, notamment la loi n°2019-014 relative à la protection des données à caractère personnel au Togo, cette formation a permis aux agents d'acquérir une maîtrise approfondie des principes fondamentaux tels que la confidentialité, le consentement, la minimisation des données et la sécurité des informations. Par ailleurs, cette formation a renforcé les capacités des équipes à identifier, analyser et gérer efficacement les risques liés aux violations de données et aux cyberincidents.

De plus, une collaboration avec l'Instance de Protection des Données à Caractère Personnel (IPDCP) peut être envisagée pour organiser des ateliers pratiques et des sessions conjointes, facilitant ainsi le partage d'expériences sur les contrôles, audits et sanctions en matière de protection des données. Cette démarche s'inscrit donc, non seulement dans un souci de gouvernance interne efficace, mais aussi dans une perspective d'alignement stratégique avec l'évolution rapide des enjeux de cybersécurité, garantissant ainsi une meilleure protection des infrastructures nationales et une confiance accrue des citoyens et partenaires internationaux.

En outre, deux agents de l'ANCy ont suivi des formations de renforcement de leurs capacités afin de mieux exécuter leurs missions.

3.1.2. Les activités avec les Opérateurs de Services Essentiels (OSE)

3.1.2.1. Les restitutions des rapports des audits de conformité réalisés

L'Agence Nationale de la Cybersécurité (ANCy) a mandaté Cyber Defense Africa (CDA) pour effectuer des audits de conformité auprès de 14 Opérateurs de Services Essentiels (OSE), en application du décret n°2019-095/PR. Les audits visent à évaluer la mise en œuvre des règles nationales de cybersécurité pour renforcer la résilience des infrastructures critiques.

Des rencontres ont donc été organisées pour faire la restitution de ces rapports aux OSE concernés. Au total, 12 restitutions ont été faites sur les 14 audits réalisés. Les restitutions des audits de CAFE INFORMATIQUE et CEET n'ont pas été effectuées. Les scores obtenus par les OSE montrent une disparité marquée dans le respect des exigences de cybersécurité.

On observe des performances élevées chez certains qui se distinguent, allant jusqu'à 87,11% ; et des performances faibles dont la plus petite est de 11,41%.

3.1.2.2. La visite des OSE de l'intérieur

Au cours du mois de juin 2024, l'ANCy a effectué une mission qui consistait à rencontrer les trois (03) OSE de l'intérieur du pays. Ces rencontres ont permis de mieux exposer les missions et le rôle de l'ANCy en tant que partenaire privilégié et régulateur des OSE en matière de cybersécurité et de clarifier aux OSE, en quoi consiste leur statut et son implication dans la protection de la souveraineté numérique du Togo. En retour, les OSE de l'intérieur ont exposé leur situation à la délégation de l'ANCy conduite par son Directeur Général, ce qui a permis l'élaboration de plusieurs approches de solution.

3.1.2.3. La sensibilisation des équipes dirigeantes des OSE

À chaque rencontre avec les OSE, l'ANCy a profité pour faire des sensibilisations aux dirigeants. Outre le rappel des règles générales de cybersécurité obligatoires pour les OSE, des contenus adaptés aux besoins et exigences spécifiques de chaque secteur ont été élaborés. Au total 146 personnes clés des OSE ont vu leurs capacités se renforcer. De telles séances ont permis de responsabiliser les équipes des OSE et de s'assurer qu'elles jouent un rôle actif dans la sécurisation de ces services essentiels.

3.1.3. Les activités de communication

3.1.3.1. Elaboration de la charte graphique de l'ANCy

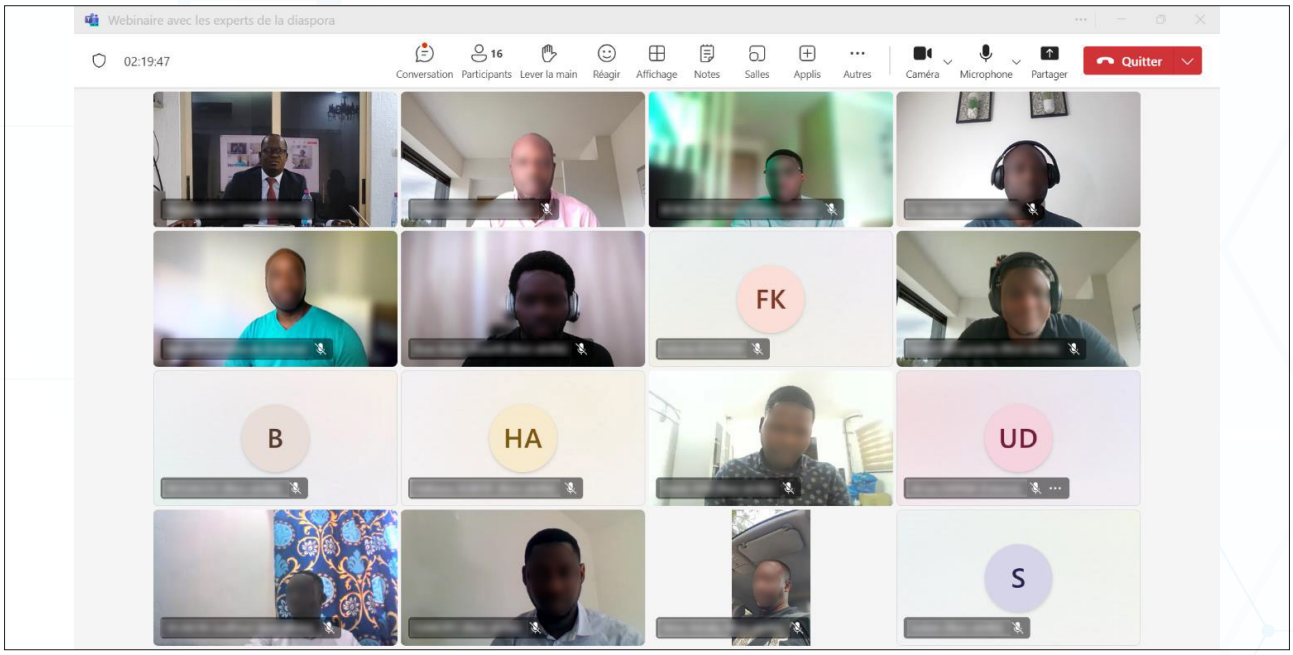
L'ANCy a élaboré sa charte graphique qui décline son identité visuelle officielle. Cette charte inclut les règles et déclinaisons graphiques applicables aux différents éléments en termes d';ergonomie et de graphisme, afin de permettre une harmonisation du code visuel.

La charte graphique de l'ANCy est un instrument essentiel pour renforcer l'image institutionnelle de l'ANCy, démontrer son expertise en cybersécurité et renforcer la confiance du public dans ses missions de protection et de sensibilisation.

Cette charte graphique est accompagnée d'une charte digitale. Il s'agit d'un document formel qui définit les règles, principes, et bonnes pratiques à respecter dans l'utilisation des outils numériques, des plateformes en ligne et des technologies liées au digital au sein de l'ANCy.
Elle vise à encadrer l'usage des ressources numériques, à promouvoir des comportements responsables, et à garantir la sécurité, la conformité et le respect des droits.

3.1.3.2. Webinaire avec les togolais de la Diapora Experts en Cybersécurité

Deux webinaires ont été organisés au cours de l'année 2024. Le premier s'est tenu le 23 janvier 2024 sur le thème « Contribuer à la sécurisation du cyberespace national en tant qu'expert togolais en cybersécurité au sein de la diaspora ». Le deuxième webinaire qui s'est tenu le 18 juillet 2024, a porté sur le « renforcement des capacités nationales en cybersécurité ».



3.1.3.3. Présentation de la Stratégie Nationale de Cybersécurité 2024-2028

Après sa publication le 22 mai 2024, l'ANCy a organisé le 4 octobre 2024 à Lomé, un atelier de présentation de la Stratégie Nationale de Cybersécurité pour la période 2024-2028.

Présidé par le Ministre de la Sécurité et de la Protection Civile, **Ambassadeur Calixte Batossie MADJOULBA**, cet événement a rassemblé près de 300 acteurs de l'écosystème du numérique au Togo pour échanger autour des axes prioritaires de cette nouvelle stratégie. La Stratégie Nationale de Cybersécurité 2024-2028, présentée lors de cet atelier, s'articule autour de 4 axes majeurs. Elle vise principalement à :

1. Promouvoir une culture de la cybersécurité des populations et développer les compétences techniques nationales ;
2. Promouvoir la sécurité des systèmes d'information de l'administration, des opérateurs de services essentiels et de l'économie numérique ;

3. Renforcer le système de réponse aux incidents de cybersécurité;
4. Renforcer les mécanismes de poursuite efficace des crimes et délits de cybersécurité.

Photo 2 : Table d'honneur de l'atelier (Au centre, le Ministre de la Sécurité et de la Protection Civile Calixte B. MADJOULBA, à sa droite le Commandant Gbota GWALIBA, DG de l'ANCy, et sa à gauche monsieur Palakiyem ASSIH, Directeur Technique de CDA

Photo 3 : Photo de famille des participants

Photo 4 : Vue partielle des participants

3.1.3.4. Diffusion de vidéos de sensibilisation pour le grand public

Conformément aux objectifs du pilier 1 de la stratégie nationale de cybersécurité qui vise à promouvoir « une culture de la cybersécurité des populations », l'ANCy a entrepris la diffusion de plusieurs messages de sensibilisation dans les ménages, sur la Télévision Togolaise depuis le mois de juillet 2024.

Ces vidéos, faites sous le format des dessins animés, sensibilisent sur les risques liés à l'utilisation non vigilante de l'internet, les techniques de détection des attaques à l'hameçonnage et l'utilisation de mots de passe robustes.

Grâce à cette campagne, le nombre de requêtes vers le CERT.tg a considérablement augmenté. De même, les témoignages et partages d'expériences sur le terrain permettent de confirmer l'impact positif de ces vidéos de sensibilisation.

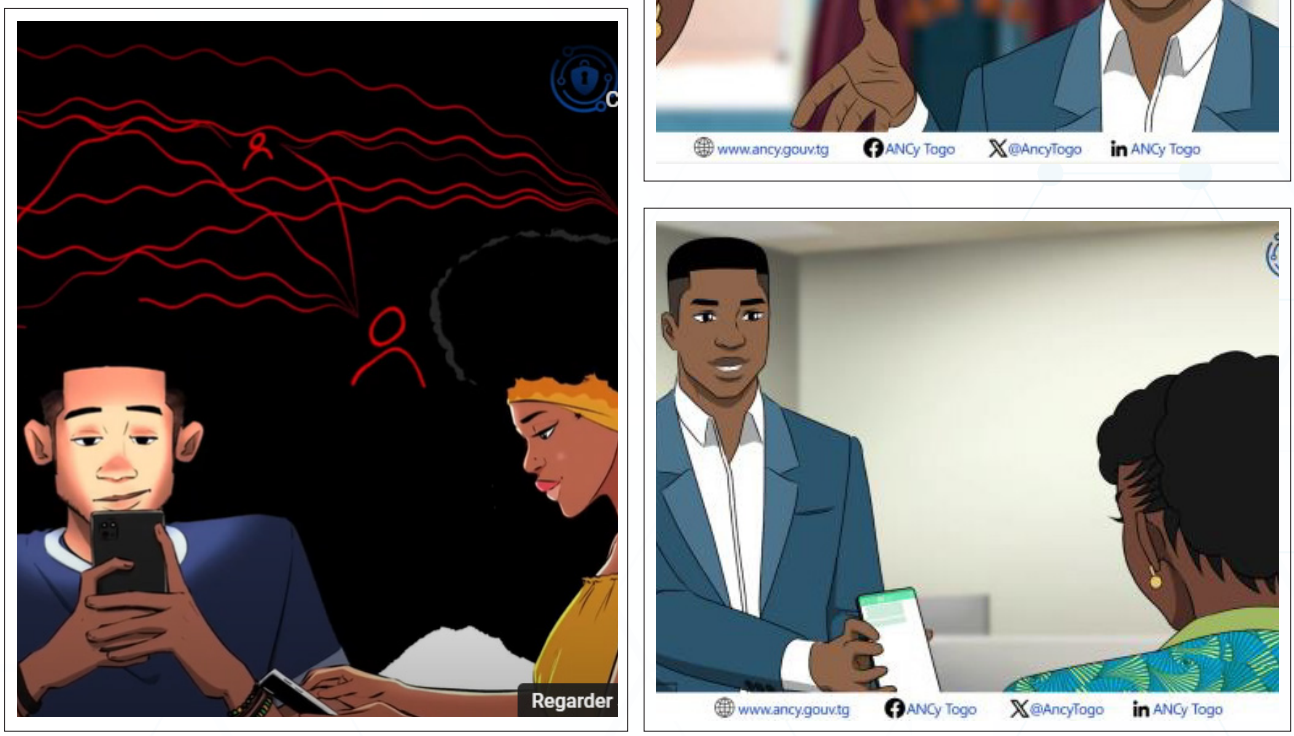


Image 2 : Captures de quelques scènes des vidéos de sensibilisation

3.1.3.5. Participation aux émissions sur les médias et interviews accordés

L'année 2024 a été intense en matière d'interventions médiatiques. Outre les reportages des différentes activités sur le terrain, les membres de l'ANCy sont constamment intervenus sur différents médias pour porter le message de la cybersécurité. À titre d'exemple, le Directeur Général et le Directeur de la Formation et du Renforcement des Capacités ont à plusieurs reprises été les invités d'émissions spéciales ou thématiques sur les chaînes de télévision nationales, les chaîne de radiodiffusion et dans les colonnes de différents journaux et médias en ligne. Leurs interventions se sont déroulées sur les médias à Lomé et dans plusieurs villes de l'intérieur du pays.

Outre les médias traditionnels, l'ANCy a également fait grand usage de ses canaux digitaux. Les alertes et divers contenus de sensibilisation ont régulièrement été publiés sur la page Facebook (@AncyTG), le compte X (@AncyTogo), la page LinkedIn (@Agence Nationale de la Cybersécurité, Togo) et bien évidemment sur le site web de l'ANCy(www.ancy.gouv.tg). Toutes les activités disposant d'éléments vidéo ont également été publiés sur la chaîne YouTube de l'ANCy.

L'ANCy a mis un accent particulier sur l'usage des médias pour sensibiliser car les interventions médiatiques régulières augmentent la compréhension des enjeux de la cybersécurité par le public tout en renforçant considérablement sa visibilité et sa crédibilité en tant qu'acteur clé de la cybersécurité.

Elles permettent de sensibiliser efficacement un large public aux bonnes pratiques numériques, contribuant ainsi à prévenir les cybers incidents et à promouvoir un usage sûr des technologies. De plus, la diversité des canaux (télévision, radio, presse écrite, numérique), est le meilleur gage pour toucher le maximum différents groupes sociaux et professionnels, dans leur diversité.

3.1.4. Les activités de formation, sensibilisation et d'éducation

3.1.4.1. Sensibilisation au personnel du Fonds National de Finance Inclusive

Dans le cadre de son engagement à renforcer la résilience numérique des institutions togolaises, l'Agence Nationale de la Cybersécurité (ANCy), en collaboration avec Cyber Defense Africa, a animé une session de sensibilisation dédiée aux membres du Fonds National de la Finance Inclusive (FNFI). Cet atelier du 14 janvier 2024 a offert aux participants des outils concrets pour faire face aux cybermenaces et protéger leurs données sensibles.

Au programme :

- → Les bonnes pratiques pour sécuriser les informations confidentielles.
- → La protection des infrastructures financières face aux risques numériques croissants.
- → Les stratégies de défense pour prévenir et détecter les cyberattaques.

Photo 5 : Sensibilisation du personnel du FNFI

3.1.4.2. Atelier de formation des webmasters sur la gestion sécurisée des sites web d'information

Photo 6 : Vue partielle des participants

Le 26 mars 2024 à Lomé, l'ANCy, conjointement avec CDA, a formé une cinquantaine de webmasters sur la ''gestion sécurisée des sites web d'information'', afin de les aider à renforcer la sécurité de leurs sites et limiter les impacts potentiels d'une cyberattaque.

3.1.4.3. Atelier de formation des startups dans la sécurisation de leurs solutions

Un atelier de travail a réuni le 4 juillet 2024, une quarantaine de Startups évoluant dans le domaine du numérique. L'objectif de cette séance de travail est de comprendre leurs défis afin de mieux les accompagner à renforcer leur posture de sécurité.

Pour atteindre cet objectif, l'importance de la prévention des cyberattaques et la mise en œuvre de bonnes pratiques de cybersécurité, telles que la correction des vulnérabilités, les sauvegardes régulières, la mise en place des politiques de sécurité claires et compréhensibles, la surveillance des systèmes, et les audits de sécurité, a été mise en avant. Cet atelier a permis aux startups renforcer leurs capacités en matière de cybersécurité et d'initier un partenariat durable avec l'ANCy pour sécuriser l'écosystème numérique togolais.

Photo 7 : Vue partielle des participants

3.1.4.4. Atelier de formation des informaticiens de l'administration publique togolaise

Le mardi 13 août 2024 à Lomé, près de 200 informaticiens de l'administration publique Togolaise, ont bénéficié d'une formation en cybersécurité organisée par l'ANCy en collaboration avec Cyber Defense Africa.

La protection des infrastructures critiques et des informations confidentielles du pays revêt dès lors une importance capitale pour garantir la sécurité nationale, économique et sociale.

Pour répondre efficacement à ces défis, il était impératif d'outiller les personnes en charge de la gestion des systèmes d'information de l'administration publique.

Photo 8 : Vue partielle des participants

3.1.4.5. Atelier de sensibilisation des PME/PMI togolaises

Les PME/PMI, présentent une certaine vulnérabilité en raison de leurs ressources limitées pour se défendre efficacement contre les cybermenaces, ce qui en fait des cibles privilégiées pour les cybercriminels.

Pour répondre à ce défi croissant, l'ANCy a jugé utile, au mois d'octobre dédié à la cybersécurité, d'intensifier ses efforts de sensibilisation en organisant le vendredi 11 octobre 2024 à Lomé, une session de formation destinée à cette catégorie d'entreprises.

Photo 9 : Vue partielle des participants

3.1.4.6. Sensibilisation de masse au Festival International d'Histoire d'Aného (FIHA)

Du 14 au 16 novembre 2024, l'ANCy était dans la commune des Lacs I, dans le cadre du Festival International d'Histoire d'Aného (FIHA).

L'objectif était de sensibiliser les populations locales et les participants au festival aux bonnes pratiques de cybersécurité. Plus de cinq cents (500) personnes ont été touchées par la sensibilisation.

Image 3 : Logo du FIHA

3.1.4.7. Atelier de renforcement des capacités des médias sur la sécurité numérique en période de fin d'année

Photo 10 : Le DG de l'ANCy (au centre), entouré des formateurs de l'ANCy (à droite) et de CDA (à gauche)

Le 20 décembre 2024, l'ANCy a animé un atelier de sensibilisation à l'intention de soixante-dix (70) professionnels des médias. L'objectif était de les informer des pratiques malveillantes en ligne, notamment en période de fin d'année, de les outiller pour mieux protéger leurs systèmes d'information et d'appeler à une collaboration proactive dans le relai des communiqués et alertes publiées par l'ANCy.

Cette session a permis d'aborder les risques spécifiques auxquels sont confrontés les journalistes notamment les tentatives d'hameçonnage ciblées, la compromission de sources confidentielles, la manipulation de l'information, et les attaques visant l'intégrité des plateformes médiatiques.

Cette formation a également couvert les méthodes de vérification de l'authenticité des informations, un enjeu important à l'ère de la désinformation. Un réseau de «Journalistes Cyber-Ambassadeurs» a également été mis en place, formant un groupe de professionnels des médias spécialement formés qui servent désormais de points focaux au sein de leurs rédactions respectives.
Cette initiative permet d'assurer une vigilance continue et une diffusion efficace des alertes émises par le CERT.tg

Photo 11 : Un formateur devant des journalistes participants

3.1.4.8. Autres activités de sensibilisation

Les équipes de l'ANCy ont également mené plusieurs autres activités de sensibilisation au profit d'autres structures telles que l'Agence Togo Digital (ATD), l'International Youth Fellowship (IYF), le Google Dev Fest, etc.

3.1.5. Deuxième édition de la compétition nationale de cybersécurité

L'organisation de ce Capture The Flag (CTF) s'inscrit dans le cadre des activités du pilier 1 de la Stratégie Nationale de Cybersécurité (SNCy) consacré à la promotion d'une culture de la cybersécurité des populations et surtout au développement des compétences techniques nationales. La compétition s'est déroulée en deux étapes.

Photo 12 : Vue partielle des participants

D'abord, la présélection en ligne qui s'est déroulée du 8 au 9 novembre 2024 a vu la participation de 198 concurrents. Ensuite, la finale en présentiel a réuni 40 participants, organisés en équipes de quatre (4), du 22 au 23 novembre 2024 à Lomé. Organisée en collaboration avec CDA, cette deuxième édition du CTF national a mis en lumière les talents locaux, renforçant ainsi la cyber-résilience du Togo. À l'issue de la compétition, les trois (03) premières équipes ont été récompensées.

Photo 13 : Une équipe en pleine compétition

Image 4 : Classement final du CTF 2024

3.1.6. La participation aux évènements internationaux sur la cybersécurité

3.1.6.1. La conférence sur la cybersécurité à l'ère quantique

Image 5 : Logo du CyberQ

Organisée par le Conseil de la cybersécurité des Émirats Arabes Unis, avec le soutien de l'Institut de l'innovation technologique (Technology Innovation Institute), la conférence sur la cybersécurité à l'ère quantique s'est tenue du 12 au 13 Novembre 2024 au centre ADNEC à Abou Dhabi et avait pour objectif d'explorer les implications profondes de l'ère quantique émergente sur la sécurité de l'information.

En effet, alors que le monde traverse une période de transformation numérique profonde, il est plus que jamais urgent de comprendre et de traiter les menaces posées par les avancées quantiques.

3.1.6.2. Le GITEX AFRICA

Image 6 : Affiche publicitaire du GITEX Africa Morocco

L'édition de 2024 qui s'est tenue du 29 au 31 mai 2024, a connu la participation de l'ANCy. Il s'agit d'un salon de technologie et de startups en Afrique dont l'objectif est de donner à l'Afrique les moyens de s'intégrer à l'économie mondiale de l'Intelligence artificielle. Le GITEX AFRICA offre une vitrine mondiale de technologie, d'innovation et de networking ainsi qu'une plateforme unique d'accélération pour les startups, PME Innovantes et grands-comptes à l'échelle internationale.

3.1.6.3. Le Forum International des Secrétaires et Assistants Administratifs (FISA)

Photo 14 : M. Malik GERALDO, Directeur de la Formation de l'ANCy lors de la sensibilisation au FISA 2024

La deuxième édition du Forum International des Secrétaires et Assistant(e)s FISA 2024 s'est tenue du 14 au 20 Octobre 2024 à Lomé.

Ce fut une occasion pour l'ANCy de sensibiliser les professionnelles venues de plusieurs pays d'Afrique dont le Togo sur la cybersécurité et la lutte contre la cybercriminalité.

3.1.6.4. Le Forum International sur la Transformation Digitale (FITD) Africa 2024

Image 7 : Affiche officielle du FITD AFRICA 2024

Le FITD est un événement dédié à l'économie numérique en Afrique. Il s'est tenu à Lomé les 27 et 28 juin 2024 sous le thème « Le digital, un facteur de développement pour l'Afrique ». L'objectif principal était de sensibiliser les entreprises et les acteurs de l'écosystème numérique aux opportunités et facteurs clés de succès pour la transformation digitale en Afrique. L'évènement a réuni quinze (15) pays.

3.2. Lutte contre la cybercriminalité

Les données consolidées de la Police Nationale, de la Gendarmerie Nationale et du Centre national de réponse aux incidents informatiques (CERT.tg) pour l'année 2024, confirment une persistance alarmante de la cybercriminalité, marquée par une diversification des modes opératoires et une dimension transnationale croissante. Si les cyber escroqueries dominent le paysage criminel, d'autres formes de délits, telles que la sextorsion, les intrusions informatiques, le vol de données ou de fonds, ainsi que le cyberharcèlement, connaissent une progression notable.

Les cas de cybercriminalité recensés sont les suivants :

- Cyber-escroquerie : 276 ;
- Cyber-vol : 181 ;
- Cyber-arnaque : 131 ;
- Cyberharcèlement, menaces et chantage : 61 ;
- Intrusion dans un système informatique et vol de données : 42 ;
- Hameçonnage (phishing) : 35.
- Sextorsion : 12 ;

Les victimes sont majoritairement togolaises, qu'il s'agisse de particuliers, d'entreprises ou d'institutions publiques. Toutefois, quelques ressortissants européens et américains figurent également parmi les personnes affectées.

Du côté des auteurs, la cybercriminalité au Togo est caractérisée par une dimension transnationale notable, impliquant des ressortissants béninois, nigérians, ivoiriens, asiatiques, ainsi que des individus originaires d'Europe de l'Est. La participation minoritaire de citoyens togolais confirme toutefois une menace hybride, mêlant réseaux locaux et internationaux.

L'évaluation financière des préjudices s'établit à plus de 277 millions de francs CFA pour la période considérée. Certaines opérations particulièrement préjudiciables ont engendré des pertes unitaires substantielles, atteignant jusqu'à 200 millions de FCFA dans un cas documenté d'intrusion informatique sophistiquée.

Au-delà de l'impact économique, les préjudices psychologiques et moraux, particulièrement dans les affaires de sextorsion, pèsent lourdement sur les victimes, notamment les jeunes, avec des répercussions durables sur leur bien-être et leur intégration sociale.

Face à ces menaces croissantes, les autorités togolaises ont déployé un dispositif de riposte multidimensionnel, dans lequel l'Agence Nationale de la Cybersécurité (ANCy) coordonne des initiatives de sensibilisation destinées à l'ensemble des segments de la population, avec une intensification programmée pour réduire les vulnérabilités comportementales.

Toutefois, plusieurs défis subsistent. En effet, il demeure complexe d'évaluer avec précision les préjudices financiers pour certains types d'attaques. De même, la traque des cybercriminels opérant au-delà des frontières nationales reste difficile, tout comme la mobilisation rapide de ressources techniques pour certaines réponses d'urgence.

D'où l'impérieuse et urgente nécessité d'investir davantage dans la formation des acteurs clés (forces de l'ordre, experts en cybersécurité), de mettre en place une synergie opérationnelle entre institutions nationales (police, gendarmerie, ANCy, opérateurs télécoms et financiers) et un dialogue renforcé avec les partenaires internationaux pour traiter efficacement la dimension transnationale de cette criminalité. Parallèlement, l'éducation numérique des citoyens, via des campagnes ciblées, reste un levier essentiel pour réduire les risques liés aux comportements humains.

Malgré un contexte actuel préoccupant, le Togo dispose des bases nécessaires pour construire un écosystème cyber résilient. L'approche intégrée combinant formation, technologie, communication et coopération constitue le socle d'un modèle de cybersécurité adapté aux réalités nationales. Le succès de cette approche dépendra de notre capacité collective à anticiper les menaces, à innover dans les réponses, et à ancrer durablement la cybersécurité dans la culture nationale.

3.3. Les missions de l'ANCy opérées par CDA

CDA, en tant que bras opérationnel de l'Agence Nationale de la Cybersécurité (ANCy), a cette année encore assumé la lourde charge de :

- Opérer le CERT national (CERT.tg) 24h/24 et 7j/7 ;
- Opérer le SOC (System Operating Center) national 24h/24 et 7j/7 ;
- Sensibiliser les usagers des équipements, des services et installations informatiques, ainsi que de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information ;
- Coordonner la riposte aux attaques informatiques ;
- Fournir un support technique pour le compte de l'ANCy.

Cependant, les missions principales de CDA ont ainsi été d'opérer le CERT et le SOC national.

Le CERT national est responsable de la fonction générale de surveillance des risques au Togo associés au cyberespace, de la protection de la société civile contre les utilisations malveillantes des outils ou services Internet, ainsi que des réponses à apporter aux attaques qui peuvent se produire.

L'équipe CERT fournit ces services gratuitement 24 heures sur 24 et 7 jours sur 7 au gouvernement togolais, au grand public et à toute organisation au Togo :

- Analyse des données sur la menace dans le cyberespace togolais selon les informations recueillies auprès de la population togolaise, des entreprises, administrations et autres organisations togolaises ainsi que de la communauté mondiale des CERT et CSIRT ;
- Traitement, réponse et coordination des incidents de cybersécurité nationaux ;
- Notification des menaces détectées et communiquées par les citoyens togolais au centre d'appel, par courrier électronique et sur le site web ;
- Annonce des intrusions, des vulnérabilités et des bulletins de sécurité ;
- Analyse avancée des logiciels malveillants au niveau national et/ou international ;
- Rapports sur les tendances des cyberattaques et leur impact potentiel sur le pays ;
- Formation générale à la cybersécurité et campagnes de sensibilisation proposées au grand public, aux écoles, aux universités, etc. ;
- Réalisation d'audits de sécurité et délivrance de certificats de conformité sous la supervision de l'ANCy ;
- Participation et contribution à des études techniques spécifiques ou à des projets de recherches et développements sur la cybersécurité ;
- Participation à l'élaboration de normes de cybersécurité dans tout le pays.

L'équipe SOC fournit des services payants 24 heures sur 24 et 7 jours sur 7 aux opérateurs de services essentiels et à toutes organisations souhaitant bénéficier de services de protection proactive en cybersécurité.

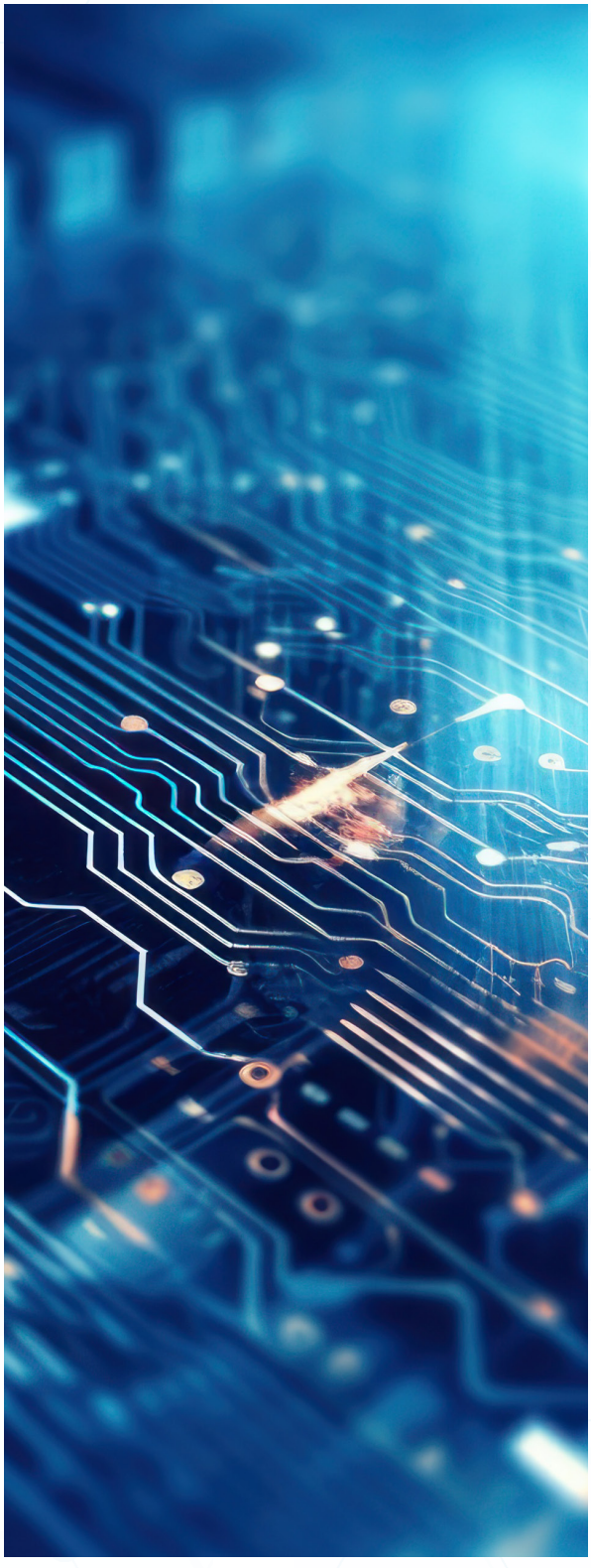
Elle se consacre à la sécurité des entreprises qu'elle protège et utilise le soutien et les services de l'équipe CERT lorsque cela est nécessaire.
Les services délivrés par l'équipe SOC sont des prestations de type services managés

dits « SOC as a Service » (ou SOCaaS) :

- Administration et maintenance de l'infrastructure SIEM (Security Information & Event Management) national et/ou sur le site de chaque organisme bénéficiant des services SOC ;
- Surveillance sur mesure des événements de sécurité 24 heures sur 24 et 7 jours sur 7 ;
- Détection et identification des menaces et des attaques ciblées ;
- Réponse aux menaces et mesures correctives (en collaboration au besoin avec l'équipe CERT) ;
- Assistance dans le processus de correction et de rétablissement du système d'information (en collaboration avec l'équipe CERT) ;
- Analyse ciblée des logiciels malveillants (en collaboration avec l'équipe CERT) ;
- Analyse et gestion des vulnérabilités inhérentes à l'organisme protégé ;
- Rapports périodiques ;

CDA délivre également d'autres prestations nécessaires à la sécurisation des systèmes d'information des organismes protégés :

- Conseil en cybersécurité (rédaction de politiques de sécurité des systèmes d'informations, réalisation de cartographies des infrastructures essentielles, autres...) ;
- Formations avancées en cybersécurité ;
- Intégration de solutions de cybersécurité ;
- Audits et tests d'intrusions.



3.3.1. Les chiffres clés de 2024

Sur l'année 2024, CDA a surveillé, via son service SOC, plusieurs équipements réseau, serveurs et applications. Au total, **les systèmes ont analysé 92 téraoctets de données** provenant des équipements protégés.

Ces données analysées ont évolué au fil des intégrations clients pendant toute l'année 2024.

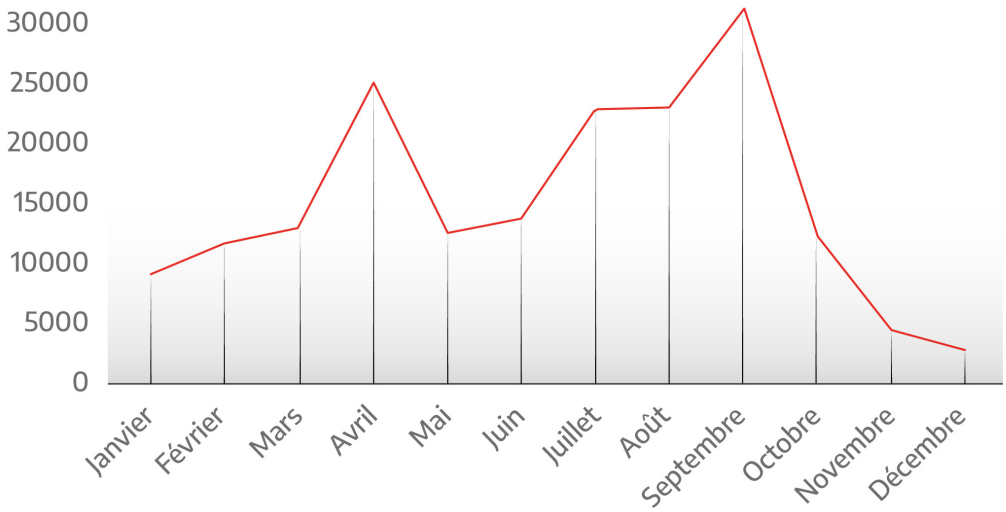
Ces logs sont corrélés et analysés dans le but de rechercher des anomalies dues à une cyberattaque. Les analystes SOC de CDA ont ainsi traité 181 088 incidents de cybersécurité (ou anomalies) au cours de l'année 2024.

Figure 3 : Nombre total d'incidents traités

3.3.1.1. Évolution des incidents traités au cours de l'année 2024

Les incidents de cybersécurité sont le résultat des règles de corrélations définis dans l'outil SIEM par les équipes CDA. Dans le cadre de l'amélioration continue du Service SOC, CDA affine régulièrement (fine tune) non seulement les règles de corrélation mais aussi la sévérité des incidents.

Ainsi, les incidents traités de janvier à décembre 2024 présente des variations plus importantes. Le nombre d'incidents traités a augmenté de manière significative en avril et a atteint un pic en août. Il y a eu une baisse progressive après ce pic jusqu'en décembre.(ou anomalies) au cours de l'année 2024.

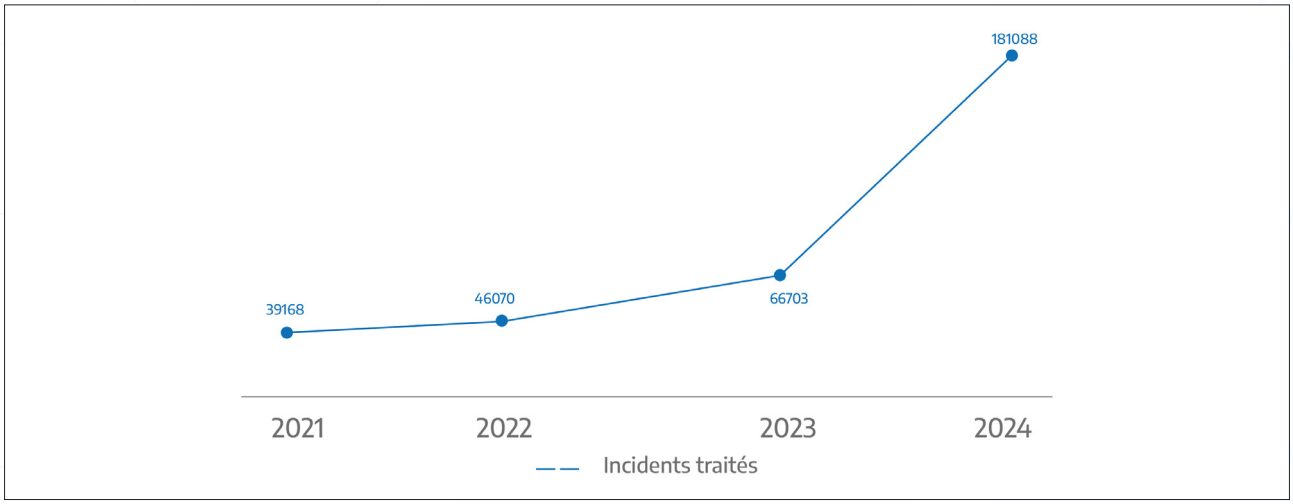


Graphique 1 : Nombre total d'incidents traités

3.3.2. L'évolution des données clés depuis le démarrage du SOC

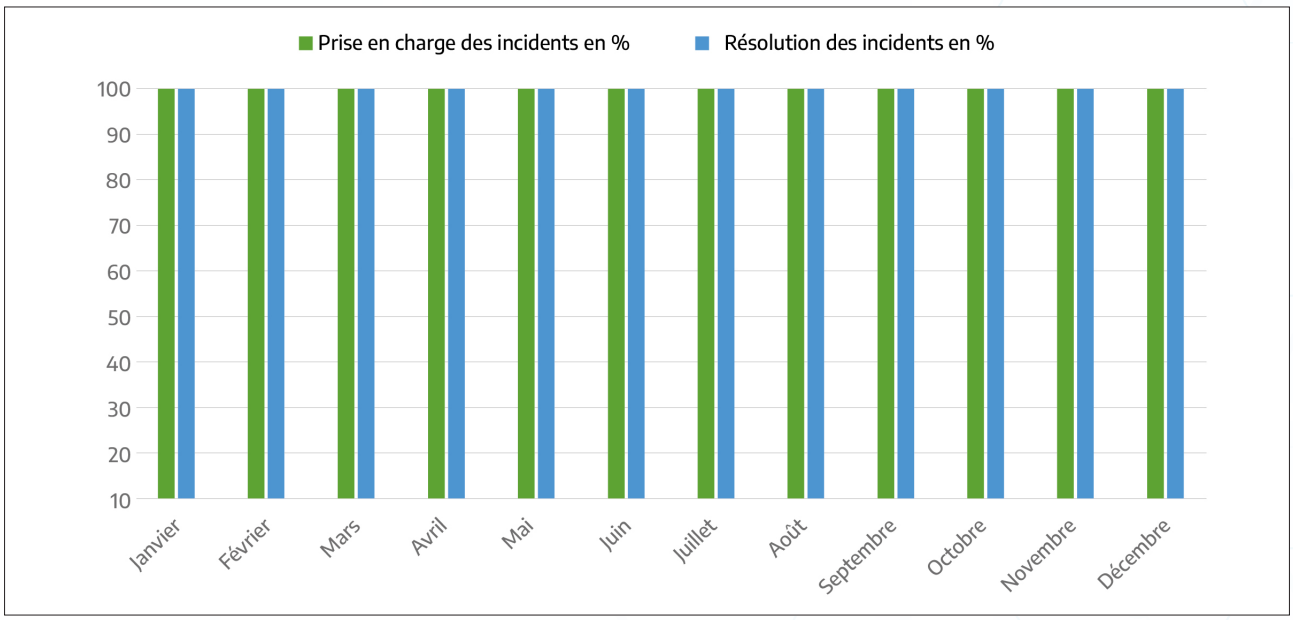
3.3.2.1. Incidents traités

Le nombre d'incidents détectés augmente année après année du fait également du nombre croissant de clients SOC intégrés et a atteint un pic en août. Il y a eu une baisse progressive après ce pic jusqu'en décembre. (ou anomalies) au cours de l'année 2024.



Graphique 2 : Evolution des données clés en 2024

3.3.2.2. Respect des SLAs

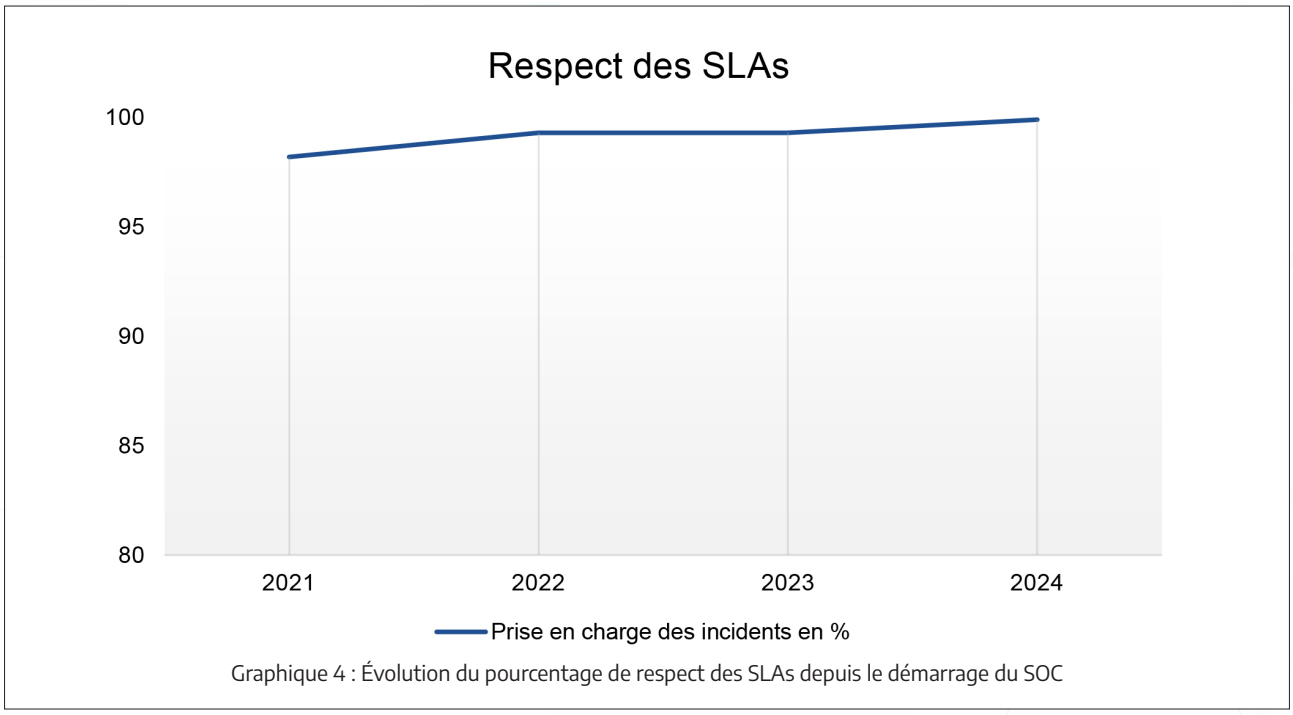


Graphique 3 : Respect des SLAs

CDA est tenu au respect des SLAs convenus avec l'ANCy dans le cadre du contrat de délégation de services, à savoir 30 minutes maximum pour la prise en compte d'un incident et 15 jours maximum pour la résolution. Le temps de résolution des incidents est indépendant et n'est pas totalement sous le contrôle de CDA.

Les temps de prise en charge des incidents par CDA en respect des SLAs sont compris entre 99,4 et 100%. La moyenne de respect des SLA sur toute l'année 2024 pour la prise en charge des incidents est de 99.9% et de 99,9% pour la résolution des incidents.

C'est donc un excellent niveau de qualité de service qui a été maintenu depuis 2022 grâce à la mise en place de nouveaux mécanismes de détection et de signalement d'incidents et au recrutement continu de nouveaux analystes.



Graphique 4 : Évolution du pourcentage de respect des SLAs depuis le démarrage du SOC

3.3.3. Activités SOC de 2024

3.3.3.1. Les clients SOC de CDA en 2024

Le SOC de CDA a participé à protéger les infrastructures informatiques des acteurs économiques et le gouvernement togolais.

CDA bénéficie d'un réseau étendu et solide, constitué de clients répartis sur 8 pays en Afrique. Ce réseau témoigne de sa capacité à fournir des solutions sur mesure et à grande échelle pour répondre aux défis complexes de cybersécurité.

CDA travaille en étroite collaboration avec des partenaires locaux et internationaux, ce qui lui permet de rester à la pointe des évolutions technologiques et des menaces en cybersécurité. Grâce à cette approche, CDA a pu développer une expertise unique adaptée aux besoins spécifiques de l'Afrique tout en garantissant la sécurité et la conformité des systèmes de ses clients.

3.3.3.2. Audit de conformité des OSE

Dans le cadre de l'application des dispositions pertinentes à l'endroit des Opérateurs de Services Essentiels (OSE), tels que stipulés dans l'article 15 alinéa 1 du décret N° 2019-095/PR relatifs aux opérateurs de service essentiels, aux infrastructures essentielles et aux obligations y afférentes, CDA, en tant que prestataire qualifié mandaté par l'ANCy, pour l'exécution des audits de conformité aux règles nationales de cybersécurité, a poursuivi cette année les missions d'audit qui avaient été reprogrammés sur 2024.

Aussi, CDA a assisté l'ANCy cette année dans la restitution des audits de conformité des OSE réalisés en 2023.

3.3.3.3. Partenariats SOC

Après les partenariats avec EC-COUNCIL et PECB les années précédentes, CDA a encore cette année 2024 noué des partenariats avec des acteurs clés de la formation en cybersécurité comme CompTIA (Security+ et CySA+).

CompTIA (Computing Technology Industry Association) est une organisation professionnelle à but non lucratif fondée en 1982, qui se consacre à l'avancement de l'industrie mondiale des technologies de l'information (TI).

Elle propose des certifications indépendantes des fournisseurs, permettant de valider des compétences en informatique dans divers domaines tels que le support technique, les réseaux, la cybersécurité et le Cloud.

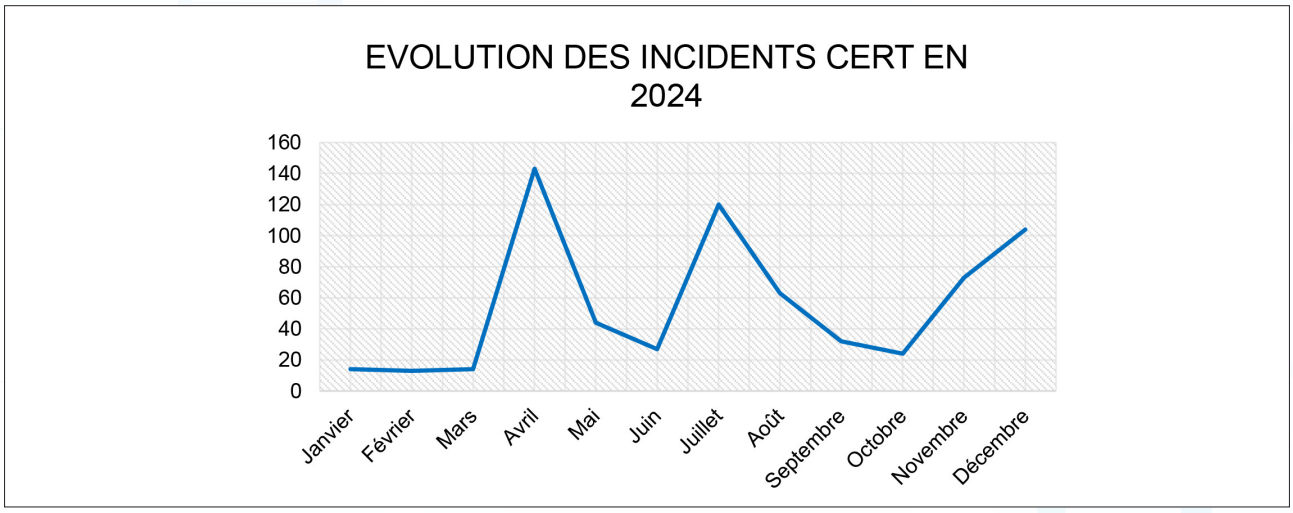
3.3.4. Activités CERT.tg en 2024

3.3.4.1. Traitement des Incidents CERT

a. Tableau des incidents traités

CDA a traité mille trois cent quatorze (1 314) incidents CERT au cours de l'année 2024 dont six cent soixante-onze (671) vrais positifs (voir annexe).

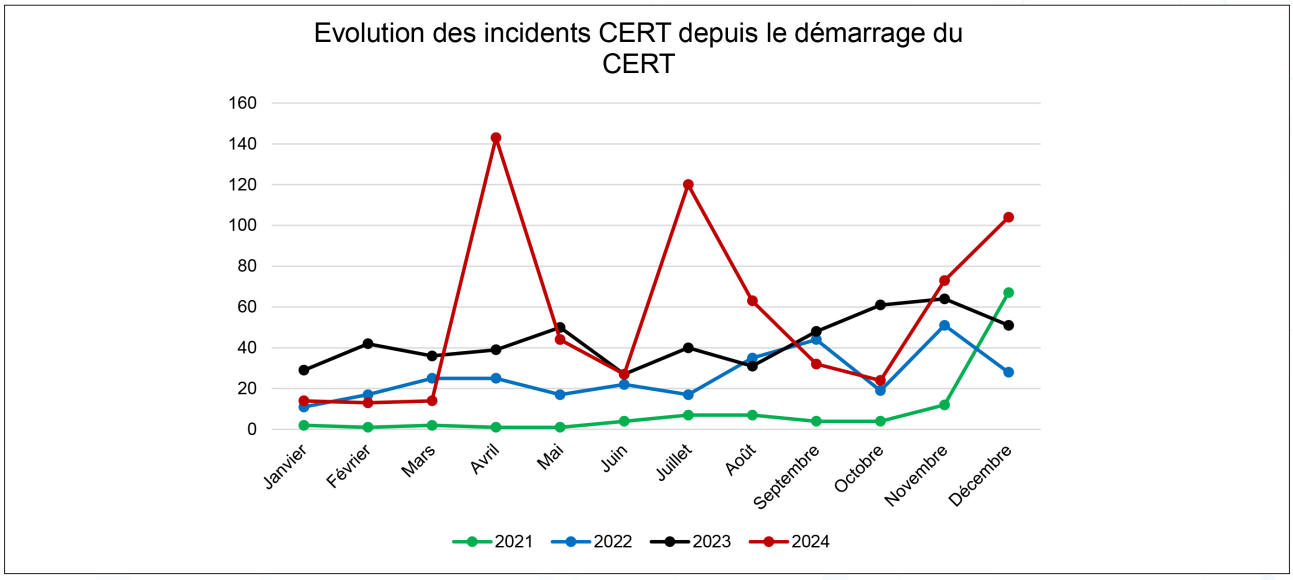
b. Évolution des incidents traités



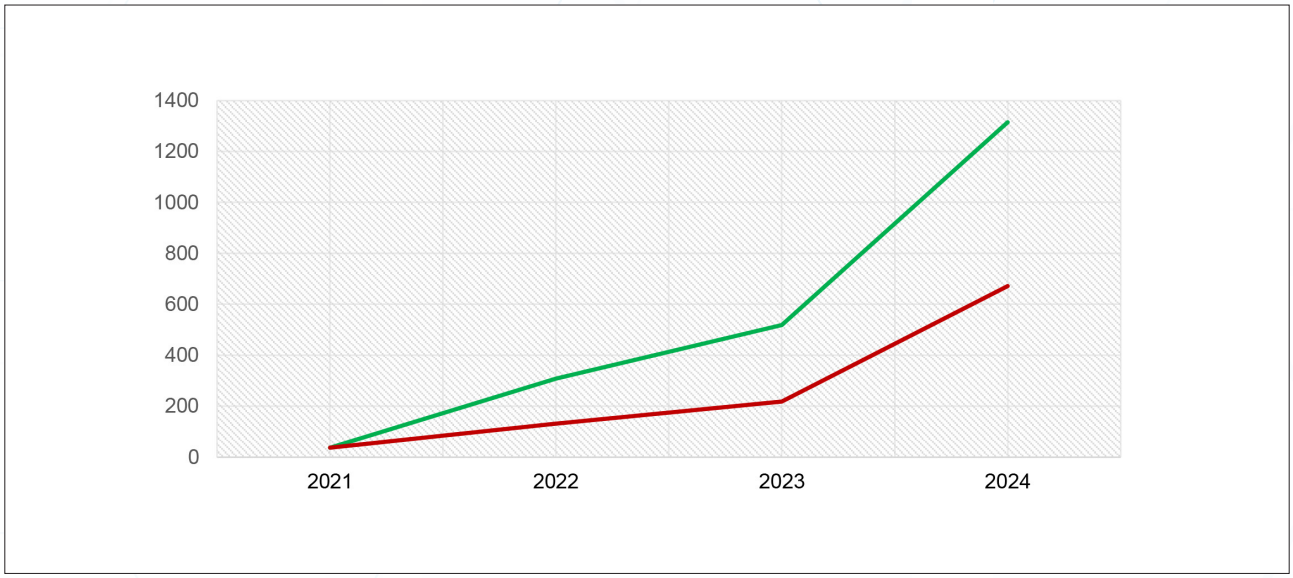
Graphique 5 : Évolution du pourcentage de respect des SLAs depuis le démarrage du SOC

Les services CERT sont principalement destinés aux citoyens. Nous constatons une évolution des incidents au fur et à mesure que la communication autour de l'ANCy, de CDA et du CERT évolue.

Il est constaté également une tendance qui se répète chaque année avec une forte croissance du nombre d'incidents déclarés par les citoyens togolais en fin d'année.



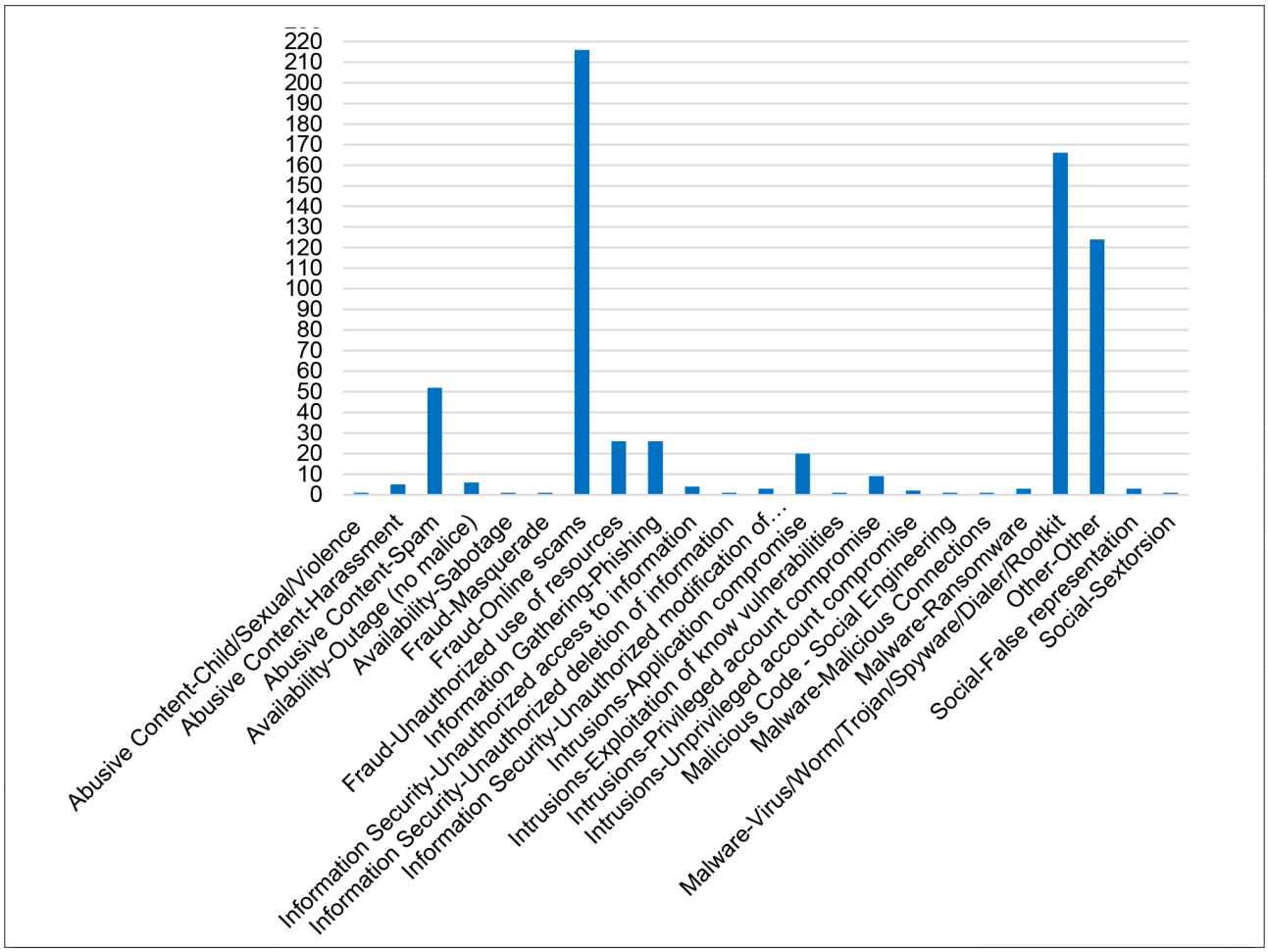
Graphique 6 : Évolution des incidents CERT par mois



Graphique 7 : Évolution des incidents CERT par année

La forte croissance du nombre d'incidents déclarés démontre que les citoyens togolais sollicitent de plus en plus le CERT National lorsqu'ils ont des incidents de cybersécurité.

c. Répartition des incidents CERT traités en 2024



Graphique 8 : Répartition des incidents CERT traités

Les incidents les plus fréquemment traités par le CERT.tg sont les campagnes de phishing, les fraudes en ligne et les spams comme au cours des 3 dernières années. Bien qu'une hausse significative du nombre total d'incidents en 2024 soit constatée, la tendance reste presque similaire à celle de 2023, à l'exception des malwares, dont le nombre a considérablement augmenté cette année.

3.3.4.2. Audit de sécurité pour les entités gouvernementales

En 2024, CDA a réalisé 13 audits d'applications web portées par le Gouvernement, des audits de salles de serveurs et des audits complets de sécurité des entités gouvernementales

3.3.4.3. Alertes sur les vols d'identifiants (Stealers)

CDA effectue une analyse quotidienne des sites web, blogs, groupes, et autres plateformes afin d'identifier des informations susceptibles de compromettre la sécurité du système d'information du gouvernement togolais ou des OSE. Ainsi, CDA a trouvé huit cent quatre-vingt-huit (884) identifiants provenant de Stealers.

Les Stealers sont des malwares qui visent à voler des informations telles que les identifiants et les cookies enregistrés dans un navigateur ainsi que d'autres données sensibles. Souvent véhiculés par des logiciels piratés ou usurpés, ils affectent majoritairement des appareils personnels mais touchent couramment les entreprises.

CDA a trouvé et envoyé aux entités concernés les identifiants (nom d'utilisateurs et mots de passes) d'utilisateurs des plateformes listés ci-dessous.

CDA effectue une analyse quotidienne

3.3.4.4. Surveillance des sites web

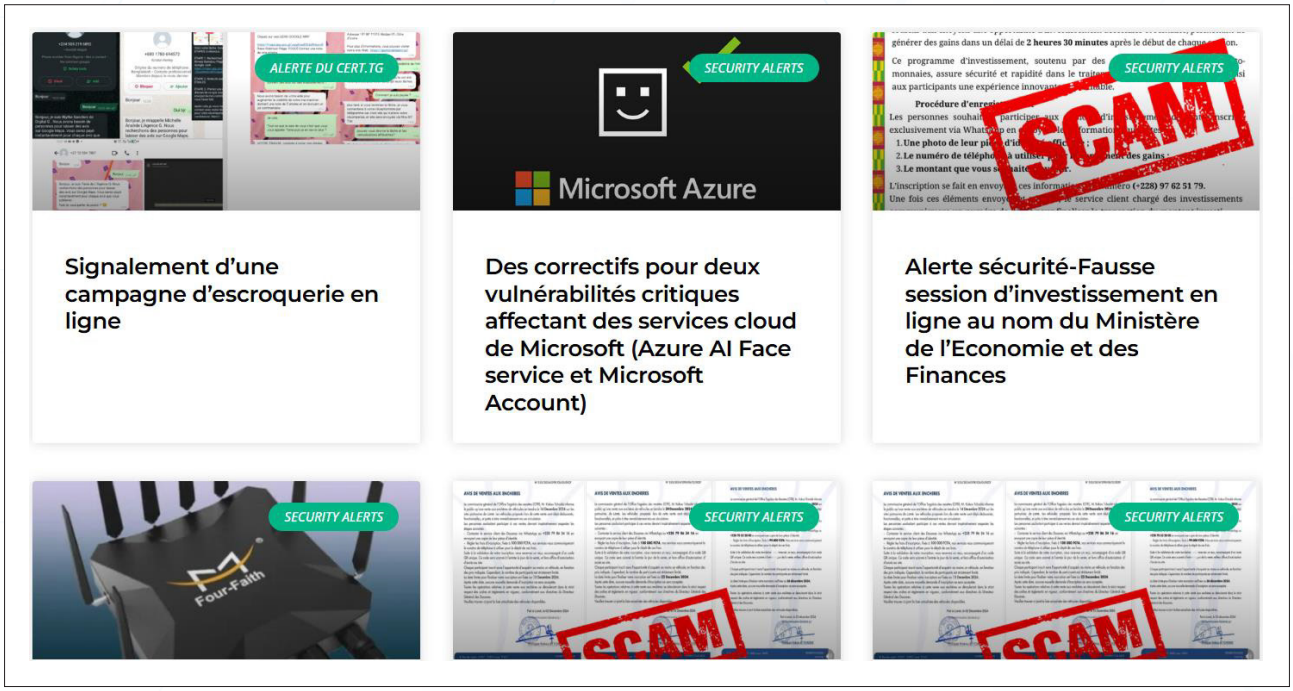
des sites web, blogs, groupes, et autres plateformes Comme en 2023, CDA a continué dans le cadre des activités CERT la surveillance des sites web gouvernementaux et autres sites web d'importance au Togo.

Cette surveillance se décline en deux fonctionnalités clés : (i) visualisation sur un écran dans le SOC des sites web sélectionnés ; (ii) alertes reçus par les analystes SOC de niveau 1 lorsqu'un changement substantiel est détecté sur un site surveillé.

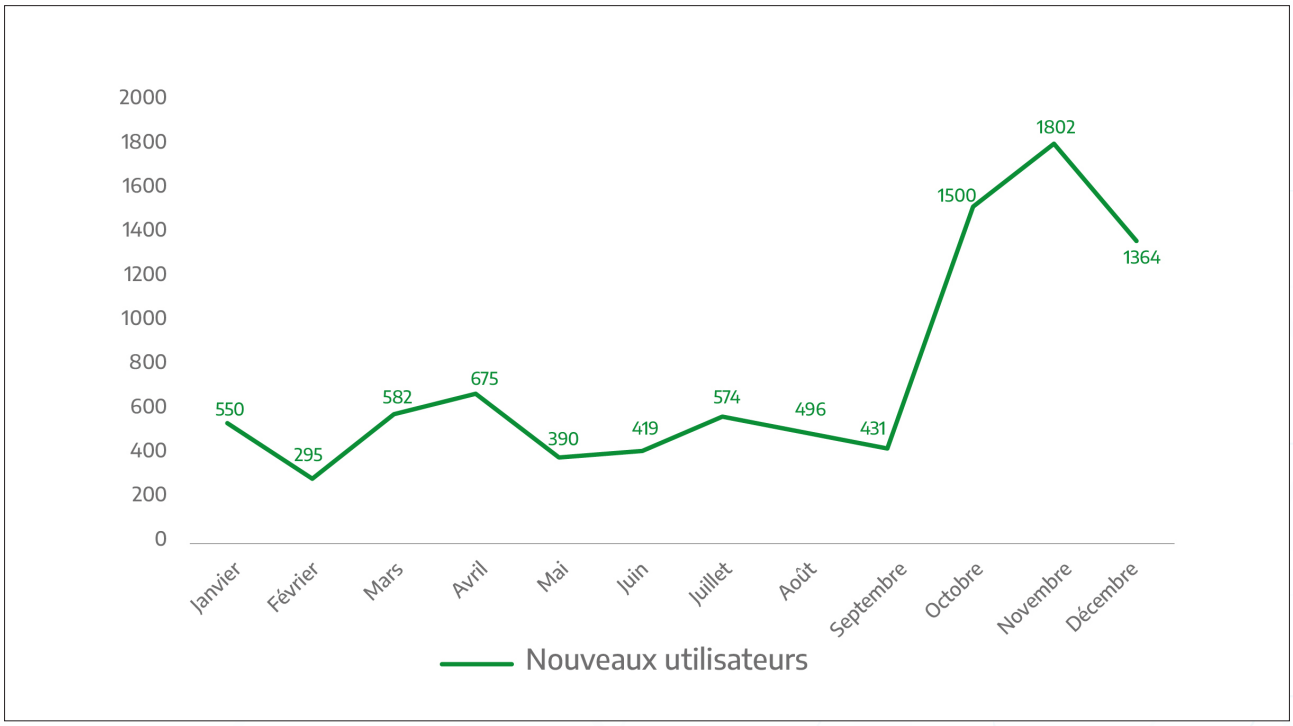
3.3.5. Site web CERT.tg

3.3.5.1. Site Internet CERT.tg en bref

Cette année encore, le site CERT.tg disponible en Français et en Anglais s'est enrichi pour répondre aux besoins des particuliers et des entreprises. Ces évolutions se manifestent par l'ajout de contenus, notamment la publication des vulnérabilités découvertes et de plus de bulletins de sécurité, ainsi que par la mise à jour du RFC 2350.

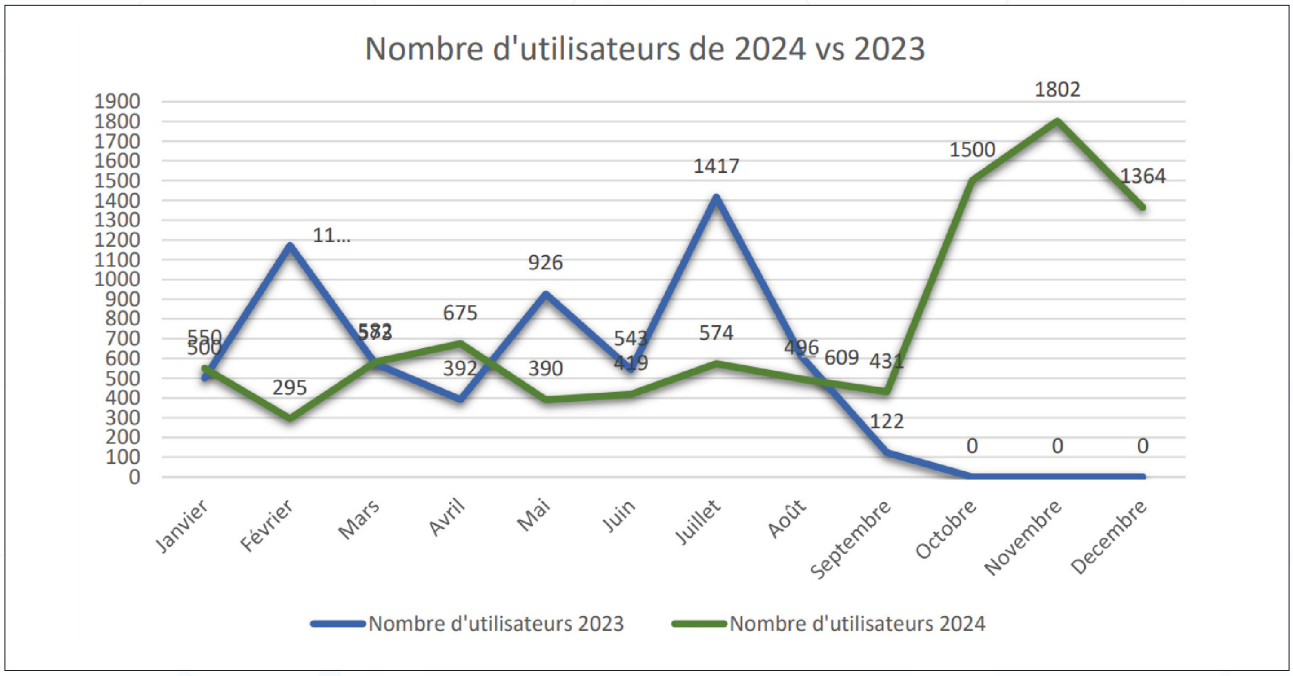


a. Statistiques du site Internet CERT.tg en 2023



Graphique 9 : Statistiques du site Internet CERT.tg

Les données collectées montrent une fluctuation du nombre de nouveaux visiteurs au cours de l'année, avec une augmentation au dernier trimestre de l'année.



Graphique 10 : Nombre d'utilisateurs entre 2023 et 2024

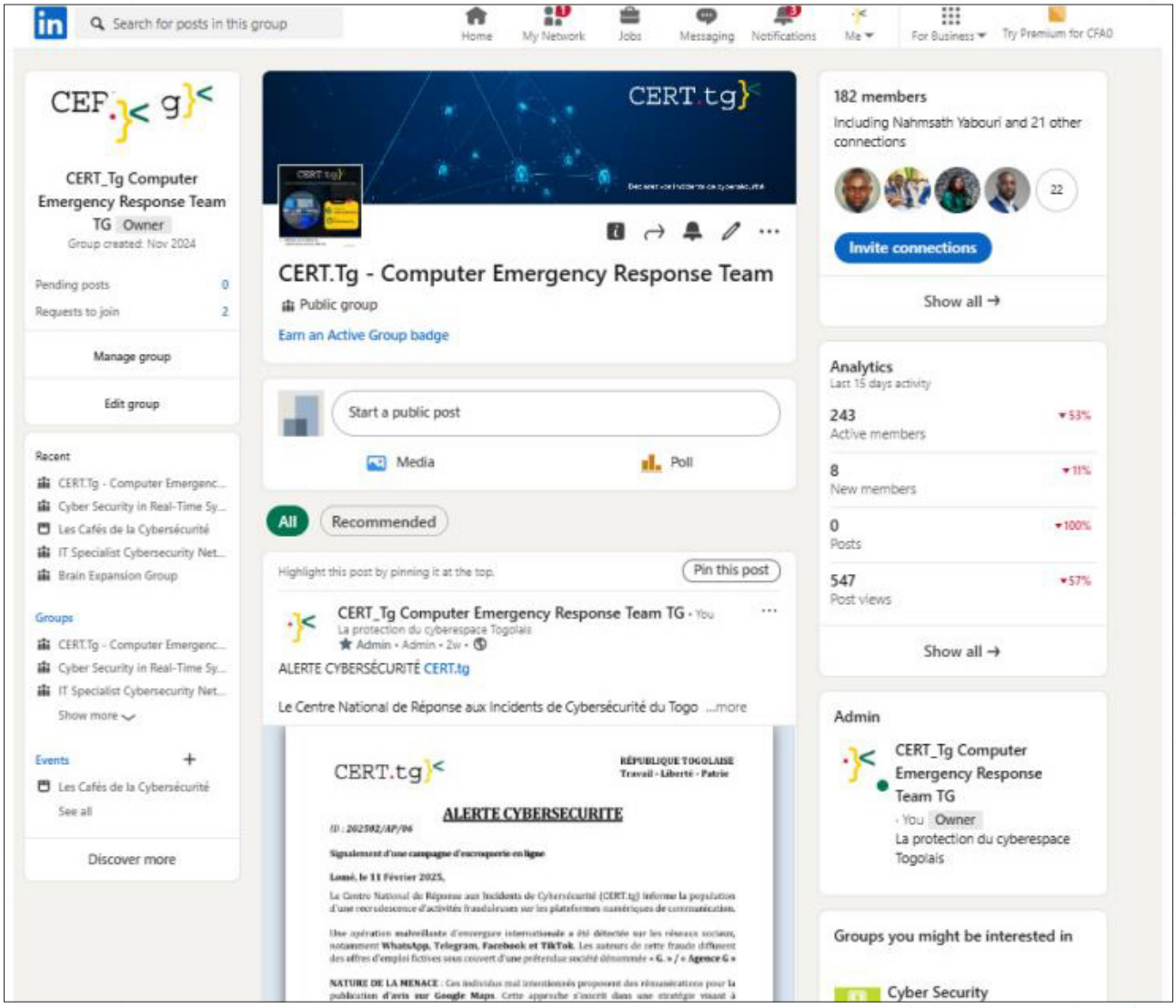


Image 8 : Exemple de publication d'alerte sur CERT.tg

3.3.6. Formations et sensibilisations à la cybersécurité

3.3.6.1. Sensibilisations en présentiel

L'humain étant le maillon faible de la chaine de sécurité, il est important de renforcer la protection des administrations pour réduire les risques. Il est crucial de sensibiliser et d'équiper les fonctionnaires, acteurs majeurs de l'administration togolaise, afin qu'ils puissent faire face aux défis grandissants de la cybersécurité.

Le CERT.tg organise donc des campagnes de sensibilisation en fonction des incidents de sécurité observés sur le réseau E-Gouv en priorisant les entités générant le plus d'incidents. Ainsi, des sessions de sensibilisations ont été organisées pour un total de trois-cent soixante-six (366) participants en 2024. Ce qui augmente le nombre total de ministères et administrations sensibilisés à cinquante-quatre (54) pour un total de sept mille sept-cent quatre-trois (7 743) participants à ce jour.

3.3.6.2. Sensibilisation sur les médias

CDA, soucieux de sensibiliser le plus grand nombre de la population à la cybersécurité à travers ses activités CERT, utilise le site web www.cert.tg, des réseaux sociaux tels que LinkedIn, Facebook, Twitter et TikTok ainsi qu'un canal de relais par les journalistes afin d'appuyer l'action de sensibilisation.

Au cours de l'année 2024, 20 alertes et communiqués de cybersécurité ont été publiés sur ces différents canaux du CERT.tg. Ces alertes ont été relayés par plusieurs autres pages de réseaux sociaux et repris dans plusieurs médias.

TOGOREGARD	https://togoregard.tg/phishing-le-cert-tg-met-en-garde-contre-une-nouvelle-arnaque/
UNIVERS	https://univers.tg/index.php/2025/01/23/attention-aux-cyberattaques-le-cert-tg-alerte-sur-une-vague-de-phishing/
NOUVELANGLE	https://nouvelangle.tg/nouvelle-tentative-darnaque-alerte-du-cert/
LEDEFENSEURINFO	https://ledefenseurinfo.tg/fr/togo-vers-un-denouement-heureux-pour-le-recensement-biometrique/
TDN	https://tdn.tg/togo-arnaque-investissement-ministere-finances/
AUXNOUVELLES	https://auxnouvelles.tg/2025/01/21/arnaque-en-cours-au-nom-du-ministere-de-leconomie-et-des-finances-les-precisions-du-cert-tg/
LEMISSAIRE	https://lemissaire.tg/les-medias-togolais-partenaires-cles-dans-la-lutte-contre-la-cybercriminalite/

Tableau 1 : Quelques pages ayant relayé les alertes du CERT.tg

3.3.6.3. Sensibilisation sur les réseaux sociaux

Les différentes actions de sensibilisations et les messages réguliers postés sur les réseaux sociaux de l'ANCy, du CERT et de CDA ont fait augmenter significativement le nombre d'abonnés aux différentes pages de l'ANCy, du CERT et de CDA. Ce qui signifie que de plus en plus de personnes reçoivent les informations de sensibilisation à la cybersécurité publiées par de l'ANCy, le CERT national et par CDA.

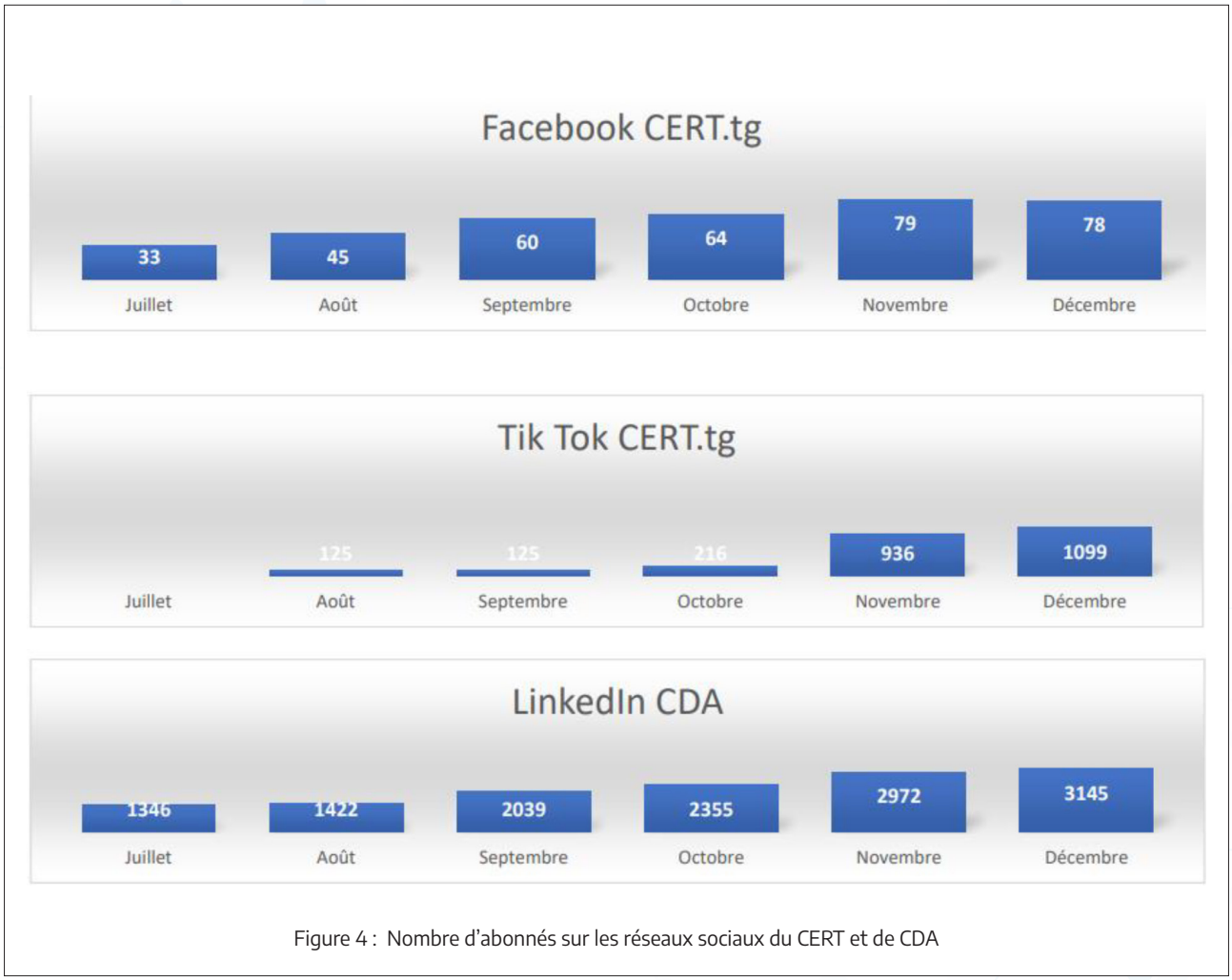


Figure 4 : Nombre d'abonnés sur les réseaux sociaux du CERT et de CDA

3.3.6.4. Université de Lomé

Dans le cadre du CyberMois, CDA a animé, le 17 octobre 2024, une session de sensibilisation à la Faculté de Droit de l'Université de Lomé. Destinée aux étudiants du Master en Droit de la Propriété Intellectuelle et du Numérique, cette session visait à renforcer leur compréhension des enjeux de cybersécurité au Togo, un pays confronté à une augmentation des menaces cybernétiques.

Photo 15 : Photo de famille à la fin de la sensibilisation

Les échanges ont permis d'explorer les incidents les plus fréquents, de participer à des cas pratiques et d'aborder les opportunités professionnelles en cybersécurité. Un accent particulier a été mis sur le rôle du droit dans la lutte contre les cybermenaces, soulignant l'importance d'une approche juridique pour un espace numérique plus sécurisé.

3.3.6.5. Sensibilisation au Lycée Français Louis Pasteur à Lagos

En collaboration avec les équipes d'Axendit Limited, (Ex Asseco Nigeria), CDA a animé une session éducative auprès des élèves et du personnel du Lycée Français Louis Pasteur au Nigeria.

L'objectif de cette initiative était de sensibiliser les jeunes aux cybermenaces, d'encourager des pratiques numériques responsables et de les outiller contre le cyberharcèlement.

Photo 16 : Sensibilisation au lycée français de Lagos

3.3.6.6. Sensibilisation des développeurs avec l'ATD

Dans un contexte où les menaces évoluent constamment, CDA a lancé une série d'initiatives pour sensibiliser les entreprises aux risques majeurs tels que les attaques par ransomware, les fuites de données, et les failles dans les API et applications web.

Des webinaires interactifs ont été animés pour les professionnels de la cybersécurité afin de partager des solutions pratiques et des bonnes pratiques pour sécuriser les infrastructures numériques. L'une d'entre elle a été faite en collaboration avec l'Agence Togo Digital.

3.3.6.7. Carrière en cybersécurité

CDA a participé à plusieurs webinaires en mettant des ressources à disposition pour des initiatives visant à mettre en lumière les carrières en cybersécurité.

3.3.6.8. Promotion de la cybersécurité auprès des entreprises africaines

CDA a également mené des actions pour promouvoir la cyber-sensibilisation auprès des entreprises africaines. En réponse à la forte demande d'une meilleure sécurisation des infrastructures locales, l'entreprise a organisé plusieurs sessions de formation et d'audit de cybersécurité à l'intention des PME africaines. Ces formations se sont concentrées sur des enjeux concrets, tels que la protection des données sensibles, la gestion des identités numériques, et la mise en œuvre de stratégies de défense contre les attaques persistantes avancées.

Ce travail a permis de développer une culture de cybersécurité au sein des entreprises africaines, qui est essentielle pour lutter contre l'augmentation des cyberattaques ciblant les entreprises locales.

3.3.6.9. Cyber Monday : Une chronique sur les enjeux de cybersécurité

CDA a introduit la chronique du Cyber Monday, un rendez-vous hebdomadaire qui attire une forte communauté de professionnels, d'experts et de passionnés de cybersécurité. Cette chronique aborde les dernières tendances, les menaces émergentes, ainsi que les meilleures pratiques à adopter pour se protéger contre les attaques numériques. À travers des analyses approfondies, des retours d'expérience, et des études de cas, le Cyber Monday permet à CDA d'entretenir une relation continue avec sa communauté, en partageant des conseils pratiques et des informations pertinentes sur les cybermenaces actuelles.

3.3.6.10. Cybermois et campagne de sensibilisation à la cyberhygiène

Dans le cadre de la campagne du Cybermois, CDA a intensifié ses efforts de sensibilisation à la cyberhygiène, en mettant l'accent sur des pratiques simples mais efficaces pour se protéger des cybermenaces. Une série d'articles et de publications a abordé des sujets pratiques comme la gestion des mots de passe, la détection de phishing, et la mise à jour régulière des systèmes de sécurité. Ces actions ont permis à CDA de toucher un large public, en particulier les utilisateurs finaux, sur des enjeux de sécurité quotidiens.

3.3.6.11. Formation continue et certifications en cybersécurité

Des programmes de formation de haut niveau pour répondre aux besoins croissants de professionnels certifiés en cybersécurité.

Des formations telles que le Lead Cybersecurity Manager et l'ISO 27001 Lead Auditor ont été organisées, attirant un public varié d'experts et de décideurs.

Ces formations ont été complétées par des sessions pratiques, permettant aux participants de mettre en œuvre des stratégies de défense sur des infrastructures réelles.

Ces actions ont permis de développer un réseau de professionnels certifiés capables de relever les défis croissants en matière de cybersécurité en Afrique et au-delà.

3.3.6.12. Participation à des événements et ateliers

a. Forum autour de l'IA

Photo 18 : M. ASSIH Palakiyem, Directeur Technique de CDA

CDA a animé un panel dédié aux défis et opportunités de l'Intelligence Artificielle en cybersécurité lors du grand atelier du Digital intitulé « Autour de l'IA » du 13 au 15 novembre 2024. C'est un forum organisé par le Ministère de l'Économie Numérique et de la Transformation Digitale à travers l'Agence Togo Digital (ATD) et soutenu par le projet ProDigiT (GIZ), l'Union Européenne (CoTIA TOGO) et d'autres partenaires.

Cet échange a renforcé une conviction : l'IA doit être encadrée et utilisée de manière responsable pour constituer un levier de croissance plutôt qu'une menace et s'est porté sur les sujets suivants :

- → Les risques cyber liés à une utilisation non éthique de l'IA.
- → Les dangers liés au partage d'informations sensibles avec les IA. Les biais cognitifs de l'IA et leur impact sur la prise de décision.
- → Une simulation d'attaque via ChatGPT a également été réalisée lors du dernier café de la cybersécurité a également été partager pour illustrer ces enjeux.

b. ISOC Togo : Internet sécurisé et gouvernance numérique

Photo 19 : L'assistance lors de la présentation

Photo 20 : Intervention de CDA au 10e forum de l'ISOC Togo

Lors du 10è Forum National sur la Gouvernance de l'Internet, organisé par ISOC Togo, CDA a animé l'atelier d'ouverture dédié à la cybersécurité. À travers une session interactive, les participants ont été sensibilisés aux cybermenaces et aux bonnes pratiques de protection.

Sous le thème **« Innovation de Rupture & IA : Avancées, Opportunités et Enjeux pour le Togo »**, cet événement, qui s'est déroulé à la maison des jeunes de Lomé le 24 octobre 2024, a été l'occasion d'échanger sur les défis et solutions liés à la gouvernance numérique.

CDA a partagé des perspectives concrètes pour renforcer la sécurité du paysage digital togolais et promouvoir un Internet plus sûr.

c. CSIRT régionaux

Du 13 au 15 novembre 2024, les experts techniques et stratégiques des CSIRT nationaux des États membres de la CEDEAO se sont réunis à Praia, au Cap-Vert, pour poser les bases de la création d'un centre de partage et d'analyse de l'information – ISAC (Information Sharing and Analysis Center) de la CEDEAO.

En tant qu'opérateur technique du Centre National de Réponse aux incidents de Cybersécurité du Togo (CERT.tg), CDA a activement contribué aux échanges et aux réflexions sur ce projet stratégique.
Au cœur des discussions, plusieurs enjeux majeurs ont été abordés :

→ La mise en place de mécanismes efficaces pour un échange structuré d'informations sur les incidents et menaces ;
→ Le partage d'expertises, d'analyses et de bonnes pratiques en matière de cybersécurité. La nécessité d'une plateforme régionale pour renforcer la collaboration et la résilience collective face aux cybermenaces.

Avec la mise en place de l'ISAC, une feuille de route stratégique est en cours d'élaboration afin d'assurer son opérationnalisation et sa pérennité.

Le renforcement de la coopération régionale et internationale reste une priorité pour bâtir un cyberespace plus sûr et résilient en Afrique de l'Ouest.

Photo 21 : M. DOH Kossi, représentant le CERT.tg

d. Allemagne : Her CyberTracks

Les collaboratrices de Cyber Defense Africa ont participé au programme Her CyberTracks en Allemagne. Cette initiative, portée par l'International Telecommunication Union et la Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ), vise à renforcer la présence des femmes dans le domaine de la cybersécurité, encore largement sous-représenté. Le programme offre aux participantes des outils et ressources nécessaires pour exceller à travers des ateliers pratiques et des échanges avec des leaders du secteur.

En 2023, seulement 23% des professionnels en cybersécurité étaient des femmes. Ce manque de diversité affaiblit les efforts en cybersécurité, car une protection robuste nécessite des équipes et des politiques reflétant la diversité des utilisateurs en ligne. Les femmes continuent d'être disproportionnellement ciblées par des menaces comme le cyberharcèlement et le doxxing. Malgré certains progrès, beaucoup reste à faire pour atteindre une véritable inclusion

3.3.6.13. Cafés de la cybersécurité

Les Cafés de la Cybersécurité sont des rencontres trimestrielles exclusives initiées par Cyber Defense Africa pour rassembler les acteurs et professionnels de la cybersécurité autour des enjeux stratégiques du secteur.

Edition	Liens
1ère Edition	https://fr.linkedin.com/posts/cyber-defense-africa_caf%C3%A9s-cybers%C3%A9curit%C3%A9-cybers%C3%A9curit%C3%A9-networking-activity-7184243840407457792-nrwY?utm_source=li_share&utm_content=feedcontent&utm_medium=g_dt_web&utm_campaign=copy
2ème Edition	https://fr.linkedin.com/posts/cyber-defense-africa_cybers%C3%A9curit%C3%A9-caf%C3%A9sdelacybers%C3%A9curit%C3%A9-cda-activity-7229033975908880384-E-qY?utm_source=li_share&utm_content=feedcontent&utm_medium=g_dt_web&utm_campaign=copy
3ème Edition	https://fr.linkedin.com/posts/cyber-defense-africa_lescaf%C3%A9sdelacybersecurit%C3%A9-cyberdrills-activity-7241810312822165504-t918?utm_source=li_share&utm_content=feedcontent&utm_medium=g_dt_web&utm_campaign=copy
4ème Edition	https://cybersecuritymag.africa/cda-convie-les-acteurs-une-simulation-sur-le-role-des-soc-togo

Tableau 2 : Liens des éditions passées des cafés de la cybersécurité

a. 1ère Edition : Cartographie des menaces

Elle a été marquée par une cartographie des cybermenaces en Afrique et au Togo plus particulièrement. Cette édition a également vu le lancement du CISO Club pour partager des expériences, d'anticiper les risques, de renforcer l'expertise et de favoriser la collaboration entre pairs. Ces clubs jouent aussi un rôle clé dans la veille technologique, la sensibilisation et l'influence des politiques de cybersécurité.

b. 2ème Edition : Simulation d'une attaque via ChatGpt

Tenue le 13 juin 2024, cette édition a mis l'accent sur la gestion des incidents de sécurité. Une démonstration en direct par le partenaire NetWitness a illustré comment générer une attaque via ChatGPT et comment la détecter et y répondre en temps réel grâce à une solution XDR (Extended Detection and Response). Les participants ont exploré les meilleures pratiques pour réagir efficacement en cas d'attaque.

c. 3ème Edition : les Cyberdrills

Le 12 septembre 2024, la troisième édition a plongé les participants dans des Cyberdrills. Simulation d'incidents de sécurité basée sur des attaques réelles et des exercices pratiques pour tester les capacités des professionnels à identifier des menaces, qualifier des événements et élaborer un plan d'action pour contrer, prévenir et renforcer la résilience des SI.

d. 4ème Edition: Red Team vs Blue Team

Cette édition s'est axée sur le rôle des SOC dans la protection des entreprises contre les cybermenaces. Une simulation immersive a opposé la Red Team (attaquants) à la Blue Team (défenseurs), mettant en lumière les stratégies offensives et défensives. Les discussions ont également porté sur les avantages de l'externalisation des SOC et les solutions proposées par CDA.

Photo 22 : Participants lors de la 4ème édition

Les actions de communication de Cyber Defense Africa ont non seulement renforcé sa visibilité et son autorité dans le domaine de la cybersécurité, mais elles ont aussi contribué à créer un environnement sécurisé pour les entreprises africaines. Par des actions concrètes, telles que des partenariats stratégiques, et une sensibilisation continue à travers des initiatives comme le Cyber Monday, CDA a réussi à mobiliser une communauté de professionnels, à encourager l'inclusion dans le secteur et à promouvoir une cyber-résilience collective. Ces actions témoignent d'un engagement constant pour améliorer la sécurité numérique à l'échelle locale et internationale.

3.3.6.14. Création du CISO Club Togo

Le CISO Club Togo est un réseau professionnel dédié aux Responsables de la Sécurité des Systèmes d'Information au Togo. Il offre un cadre d'échange, de formation, et de collaboration sur les défis de cybersécurité, abordant des thèmes comme la gestion des risques, la sécurisation des infrastructures critiques, et la réponse aux incidents.

Le club soutient aussi la progression de ses membres avec des groupes de travail pour les certifications clés et favorise une culture de sécurité renforcée au sein des entreprises et institutions togolaises. Le CISO Club c'est une chaine publique sur WhatsApp qui permet la diffusion large des alertes, un groupe privé sur WhatsApp ainsi que sur Telegram.

3.3.7. Références

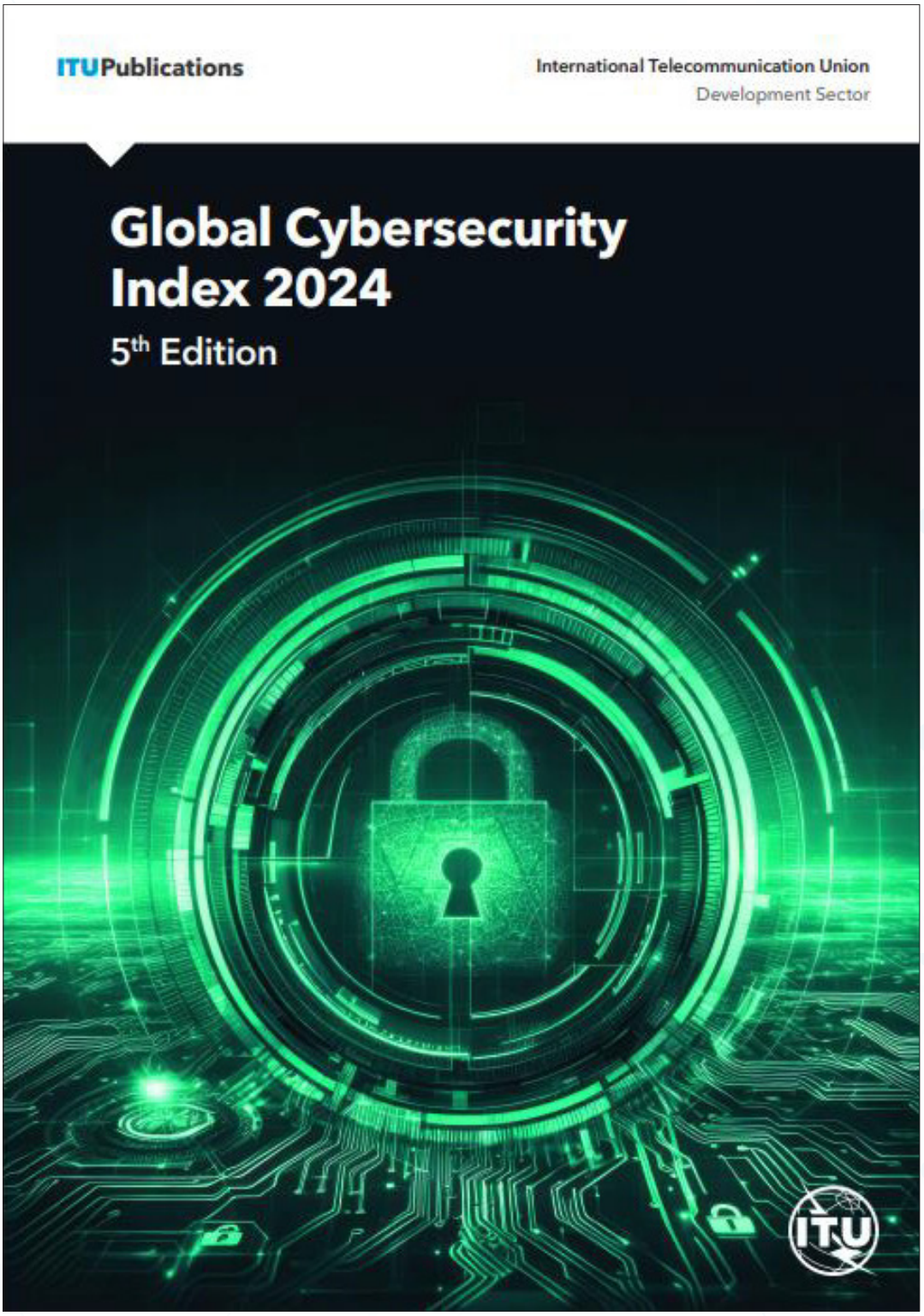
Référence	URL
Site Web ANCy	https://ancy.gouv.tg
Site Web CDA	https://cda.tg
Site Web CERT.tg	https://cert.tg
ITU Global Cyber Index	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
FIRST & FIRSTCON2022	https://www.first.org/conference/2022/
Africa CERT	https://www.africacert.org/about-us/
ANCy-CDA : Présentation des règles de cybersécurité au Togo	https://ancy.gouv.tg/les-regles-de-cybersecurite-ont-ete-presentees-ce-22-septembre-2022-aux-differents-acteurs-du-cyberespace-togolais-par-lancy-et-cyber-defense-africa-cda/
CEDEAO/OCWAR-C : Semaine du CSIRT	https://www.ocwarc.eu/ecowas-csirt-week-guinea-bissau/
ANCy-CDA : Validation de la stratégie nationale de la cybersécurité	https://ancy.gouv.tg/du-mercredi-23-au-vendredi-25-novembre-2022-setait-tenu-latelier-de-validation-de-la-strategie-nationale-de-la-cybersecurite-avec-la-participation-des-institutions-nationales/

Tableau 3 : Liste des références de CDA

CHAPITRE IV

Le Global Cybersecurity Index (GCI)

Depuis son lancement en 2015, le GCI est une référence de confiance, mesurant les engagements des pays à la cybersécurité et la sensibilisation à l'importance et aux différentes dimensions de la question. Comme la cybersécurité est une question vaste et complexe, transversale aux industries et aux secteurs, le développement ou l'engagement est évalué selon cinq piliers : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération – puis agrégées en une note globale.



Les méthodes et techniques d'évaluation font souvent objet d'amélioration. Ainsi CDA depuis octobre 2022, fait partie du groupe de travail des experts de cette 5ème édition du GCI (v5) qui a pour objectifs de :

- Donner son avis sur les qualités clés à privilégier dans tout modèle de niveaux du GCI ;
- Proposer des modèles pour les niveaux, avec une méthodologie et un raisonnement ;
- Participer de manière productive aux discussions ;
- Exprimer des préférences sur le modèle par paliers préféré.

En 2024, le Togo se classe désormais 8e en Afrique et 67e dans le monde. Des bonds de 25 et de 143 places respectivement au classement africain et mondial, de 2018 à 2024.

Le Togo est devenu le pays à réaliser la progression la plus rapide en matière de cybersécurité dans le monde depuis 2018. Avec un score éloquent de 88,8, le Togo est désormais classé dans la catégorie Tiers 2 « Advancing », aux côtés de nations comme la Chine, Israël, la Suisse, la Pologne et la Russie notamment.

Tier Performance: Africa

T5 *Building*	T4 *Evolving*	T3 *Establishing*	T2 *Advancing*	T1 *Role-modelling*
Burundi	Angola	Botswana	Benin	Ghana
Central African Rep.	Cabo Verde	Burkina Faso	South Africa	Kenya
Eritrea	Chad	Cameroon	Togo	Mauritius
Guinea-Bissau	Congo (Rep. of the)	Côte d'Ivoire	Zambia	Rwanda
	Equatorial Guinea	Dem. Rep. of the Congo		Tanzania
	Gabon	Eswatini		
	Lesotho	Ethiopia		
	Liberia	Gambia		
	Madagascar	Guinea		
	Mali	Malawi		
	Namibia	Mozambique		
	Niger	Nigeria		
	Sao Tome and Principe	Senegal		
	Seychelles	Sierra Leone		
	South Sudan	Uganda		
	Zimbabwe			

Image 11 : Performances des pays africains au GCI 2024

Ce classement met en évidence les avancées du Togo dans l'alignement sur des normes et pratiques rigoureuses dans le domaine de la cybersécurité. Cette nette progression démontre l'engagement du pays à renforcer ses infrastructures de cybersécurité et à se positionner comme un acteur clé sur les scènes régionale et mondiale. Pour preuve, le gouvernement togolais a mis en place des mesures légales robustes, développé des capacités techniques avancées, sensibilisé les diverses couches de la population et favorisé une coopération étroite avec des partenaires internationaux et régionaux.

Ces actions sont notamment portées par le Ministère de l'Économie Numérique et de la Transformation Digitale (MENTD) à travers ses structures spécialisées.

Une illustration forte des innovations du Togo en matière de cybersécurité est ce modèle unique de partenariat public-privé (PPP) établi entre la République Togolaise et le Groupe Asseco, un leader mondial dans le domaine, pour la mise en place de Cyber Defense Africa (CDA). Bras opérationnel de l'Agence Nationale de Cybersécurité (ANCy), visant à atteindre une qualité de service élevée et un accès à une expertise de pointe, CDA fournit des services de cybersécurité aux administrations publics et aux entreprises privées, en particulier celles des secteurs sensibles comme le secteur financier, l'énergie ou les télécommunications.

CDA contribue également à renforcer les capacités locales en cybersécurité et soutient le développement continu des infrastructures de pointe et des compétences au Togo.

RÉPUBLIQUE TOGOLAISE
Ministère de l'Economie Numérique et de la Transformation Digitale

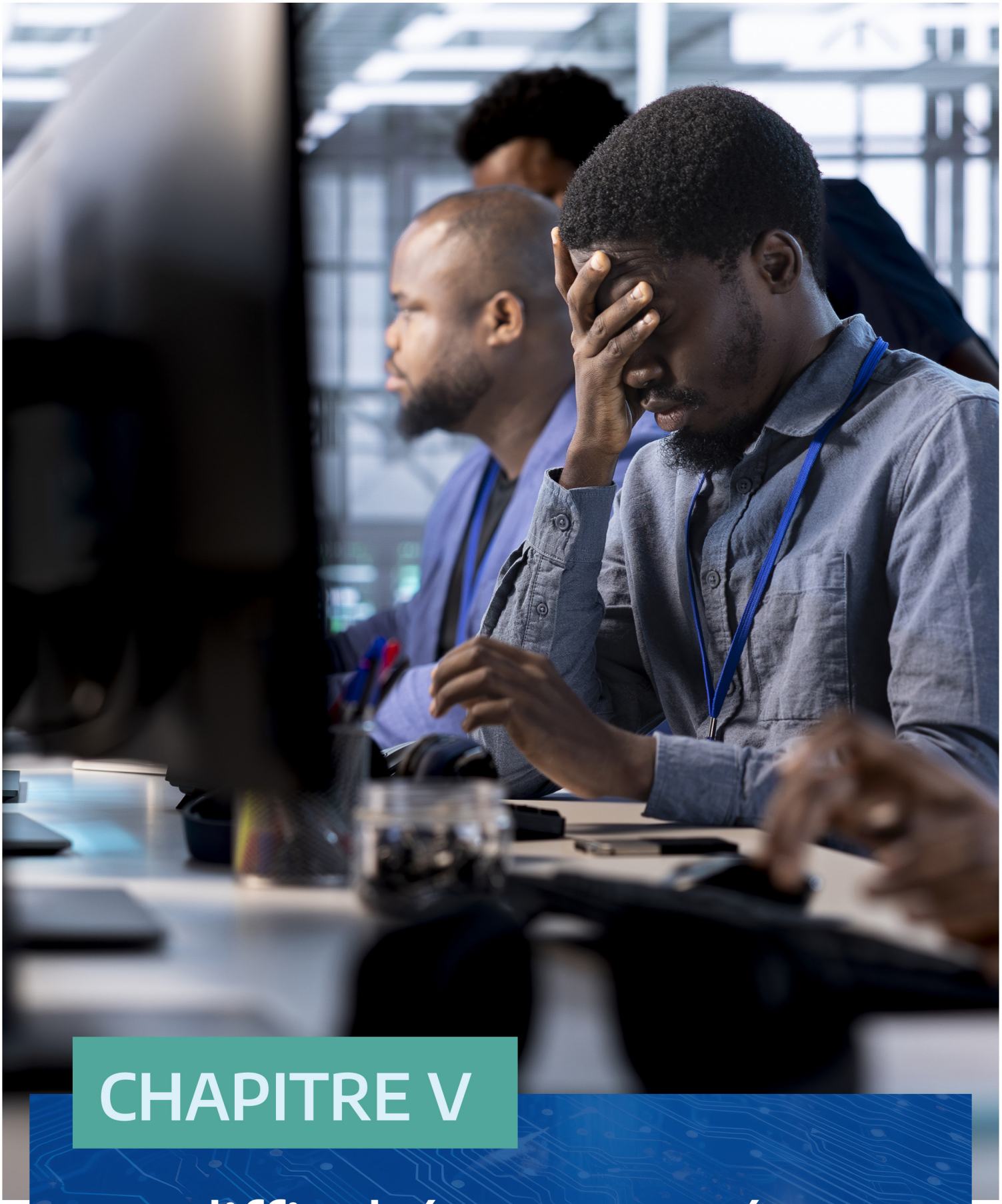
RÉPUBLIQUE TOGOLAISE
Ministère de la Sécurité et de la Protection Civile

ANCy Agence Nationale de la Cybersécurité

CDA

CERT.tg


74627 66 12839 130 11000
21213 61 7183 917330



CHAPITRE V

Les difficultés rencontrées

Les principales difficultés rencontrées par l'ANCy en 2024, qui sont en réalité des défis, sont d'ordre opérationnel et technique. Les défis opérationnels sont essentiellement liés à l'interaction avec les OSE.

5.1. Défis opérationnels

5.1.1. Le manque de certaines ressources humaines qualifiées

De nombreux Opérateurs de Services Essentiels (OSE) rencontrent des défis majeurs dans leur mise en conformité aux exigences de cybersécurité. Le manque de personnel qualifié, particulièrement dans les structures de petite taille ou les secteurs moins lucratifs, constitue un frein important à l'adoption de bonnes pratiques. Par ailleurs, le manque d'implication des dirigeants, souvent due à une sous-estimation des enjeux, retarde les initiatives et affaiblit la résilience des organisations.

Dans certains secteurs traditionnels, la cybersécurité est reléguée au second plan face aux priorités opérationnelles. De plus, certains OSE, n'ayant pas encore été confrontés à des incidents majeurs, minimisent les risques et négligent leur obligation de mise en conformité avec les règles nationales de cybersécurité.

La réticence à adhérer aux audits de conformité, perçus comme coûteux, s'ajoute aux obstacles freinant l'adoption de mesures adéquates. L'utilisation de logiciels obsolètes, en raison du manque de mises à jour des systèmes d'information, accroît leur vulnérabilité face aux cybermenaces.

Malgré les efforts de l'ANCy pour les accompagner, certains OSE restent isolés et peu engagés, limitant ainsi leur progression en matière de cybersécurité.

À cela s'ajoutent des défis structurels tels que la non-opérationnalisation complète des services de qualification des prestataires de services de confiance en cybersécurité, ainsi que le choix de ne pas encore appliquer les sanctions pécuniaires et les astreintes prévues par la réglementation, en raison de la nécessité d'accorder un moratoire aux OSE, pour pouvoir réellement implémenter les exigences des règles de cybersécurité. Tous ces facteurs combinés freinent l'amélioration globale du niveau de cybersécurité des OSE et nécessitent une mobilisation de toutes les parties prenantes.

En outre, l'absence d'experts en audit de la sécurité des systèmes d'information, en particulier dans le cadre du processus de qualification des prestataires de services de confiance en cybersécurité lancé cette année, est un défi majeur pour l'ANCy. Ces audits requièrent des compétences pointues en évaluation des infrastructures, analyse des risques, cryptographie et conformité réglementaire. Or, l'ANCy ne dispose pas actuellement de ressources internes ayant l'expertise nécessaire pour mener à bien ces missions. Faute de spécialistes qualifiés en interne, l'ANCy pourrait être amenée, lors d'un processus de qualification, à faire appel à des consultants spécialisés, entraînant ainsi une dépendance externe.

5.1.2. La sensibilisation et l'adoption des bonnes pratiques

Malgré les nombreuses campagnes menées par l'agence, la sensibilisation et l'adoption des bonnes pratiques en cybersécurité restent des défis majeurs. L'adhésion aux recommandations demeure insuffisante, notamment en raison d'un manque de conscience des risques : le public ne mesure pas pleinement l'ampleur des menaces, considérant les cyberattaques comme des événements éloignés.

Avec la multiplication des services en ligne, le

nombre de personnes à sensibiliser ne cesse d'augmenter. Il existe également des défis liés à la barrière de langue et à l'accessibilité limitée dans certaines zones reculées.

5.2. Défis techniques

Le principal défi technique est l'augmentation des cybermenaces, qui deviennent de plus en plus sophistiquées, notamment avec l'intégration de technologies avancées telles que l'intelligence artificielle (IA) et l'apprentissage automatique. Ces nouvelles menaces utilisent des techniques plus complexes, capables de contourner les mécanismes de défense traditionnels.

Face à l'évolution constante des techniques utilisées par les cybercriminels, il est essentiel de faire une veille continue afin d'adapter régulièrement les programmes de sensibilisation à ces nouvelles menaces.

5.3. Approches de solutions pour surmonter ces difficultés

5.3.1. Renforcement de la posture de sécurité des OSE

Pour renforcer la posture de sécurité des OSE les moins performants, une approche ciblée et adaptée à leurs besoins spécifiques est essentielle.

D'abord, la sensibilisation des dirigeants constitue une priorité, avec l'organisation de séminaires dédiés aux décideurs afin de leur faire prendre conscience des enjeux stratégiques de la cybersécurité et de leur rôle clé dans la mise en conformité. Ces rencontres seront l'occasion d'insister sur les risques liés aux cyberattaques et l'importance d'investir dans des mesures de protection adaptées.

Ensuite, un suivi renforcé sera mis en place, notamment par un mécanisme de suivi trimestriel permettant d'évaluer la progression des OSE en difficulté dans l'exécution de leur feuille de route et de leur plan d'action. Enfin, un plaidoyer auprès des organes de gouvernance est également envisagé en faveur d'un allègement des coûts des audits de conformité, souvent perçus comme un frein à l'engagement des OSE.

Ces actions combinées permettront de réduire les écarts de performance entre les OSE et de renforcer la résilience globale des infrastructures critiques face aux cybermenaces.

5.3.2. Renforcement des capacités du personnel de l'ANCy

En ce qui concerne les audits des prestataires de service de confiance en cybersécurité et les audits de conformité, le recrutement d'auditeurs est en cours afin de renforcer les compétences internes et réduire la dépendance à des ressources externes.

5.3.3. Multiplication des campagnes de sensibilisation ciblée

Un programme national de sensibilisation et de formation continue en cybersécurité est prévu, intégrant des modules adaptés aux réalités de chaque secteur. Cette initiative va s'appuyer sur des collaborations avec des institutions académiques et des partenaires internationaux afin d'assurer la qualité et la pertinence des formations.

CHAPITRE VI

Les perspectives pour 2025

L'année 2025 marque une étape clé dans le renforcement de la mise en œuvre de la Stratégie Nationale de Cybersécurité, avec les actions majeures suivantes :

6.1. Poursuite de l'opérationnalisation de la Stratégie Nationale de Cybersécurité

- Élaboration des manuels d'enseignement de la cybersécurité dans le primaire et le secondaire et intensification des campagnes de sensibilisation ciblées (établissements scolaires, entreprises, communautés locales).
- Organisation d'un CTF à l'intérieur du pays, pour identifier et former de nouveaux talents, et d'un bootcamps pour préparer les talents nationaux aux compétitions internationales.
- Qualification des prestataires de services de confiance en cybersécurité et des produits de sécurité, délivrance des agréments aux centres d'évaluation par l'ANCy.
- Meilleure participation de l'ANCy aux événements internationaux.

6.2. Sensibilisation et formation en cybersécurité

- Formation dans l'enseignement supérieur par un accompagnement dans le déploiement de cursus complets en cybersécurité dans les universités et grandes écoles.
- Réalisation d'un sondage sur les perceptions de la cybersécurité et de la cybercriminalité au Togo, avec des recommandations stratégiques pour chaque segment.
- Poursuite des tournées nationales de sensibilisation, avec une approche sectorielle (éducation, santé, finance, etc.).

6.3. Renforcement des capacités

- Renforcement des compétences du personnel de l'ANCy par des formations certifiantes et des ateliers pratiques.
- Formation avancée pour les personnels stratégiques des administrations et des OSE, avec un focus sur la réponse aux incidents.

6.4. Gestion et opérationnalisation

- → Mise en œuvre d'un tableau de bord pour le suivi des indicateurs de performance de la Stratégie nationale de cybersécurité.
- → Poursuite des audits de conformité des OSE pour couvrir un éventail plus large de secteurs critiques.

6.5. Collaboration et coordination

- → Renforcement des actions pour attirer les Togolais de la diaspora, experts en cybersécurité, via des partenariats avec des universités et entreprises internationales.
- → Organisation d'exercices nationaux élargis d'alerte et de gestion des incidents de cybersécurité pour inclure des simulations multi-sectorielles.
- → Renforcement des échanges entre l'ANCy, les forces de sécurité et la justice, avec des formations conjointes sur les techniques d'investigation numérique.
- → Poursuite de la structuration des rencontres trimestrielles avec les OSE autour de thématiques spécifiques.

6.6. Stratégie et analyse

- → Poursuite de la mise en place des activités Open Source Intelligence (OSINT) avec inclusion de nouvelles technologies de veille et d'analyse des risques.

Conclusion

Le présent rapport d'activités met en lumière les actions menées par l'Agence Nationale de la Cybersécurité (ANCy) pour renforcer la protection et la résilience du cyberespace togolais, dans un contexte mondial marqué par des menaces de plus en plus complexes et évolutives.

Les initiatives déployées ont contribué à des avancées significatives dans la sécurisation des infrastructures critiques du pays, tout en renforçant la sensibilisation et les compétences des acteurs publics et privés aux enjeux de cybersécurité. Ces efforts s'inscrivent dans une démarche d'adaptation continue aux défis émergents, tels que l'intelligence artificielle, l'interconnexion des systèmes critiques et les exigences des régulations internationales et ont permis de renforcer la résilience des institutions et des citoyens face aux cybermenaces.

Pour le compte des années à venir, l'ANCy s'attachera à poursuivre ses efforts pour anticiper les menaces émergentes, innover dans ses approches et garantir un cyberespace sûr et inclusif pour tous les Togolais. Cette vision s'appuie sur une volonté constante de protéger les intérêts nationaux et de contribuer au développement numérique durable du pays.

AncyTG | ancytg | AncyTogo | ANCyTG | https://www.ancy.gouv.tg

Remerciements

Nos remerciements vont aux institutions et organisations suivantes :

Présidence du Conseil ;

Gouvernement ;

Ministère des Armées ;

Ministère de la Sécurité et de la Protection Civile ;

Ministère de l'Économie Numérique et de la Transformation Digitale ;

Ministère de la Justice et de la Législation ;

Ministère de l'Enseignement Supérieur et de la Recherche ;

Ministère des Enseignements Primaire et Secondaire ;

Police nationale ;

Gendarmerie nationale ;

Cyber Defense Africa (CDA) SAS ;

Agence Togo Digital (ATD) ;

Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) ;

Union Internationale des Télécommunications (UIT) ;

Universités de Lomé ;

Université de Kara ;

Chambre de Commerce et d'Industrie du Togo (CCIT) ;

Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO) ;

Organisme de Mise en Œuvre du Millenium Challenge Account (OMCA) ;

Moov Africa Togo ;

Yas Togo ;

GVA CanalBox ;

Teolis.

TABLE DES MATIÈRES


ANCy


RÉPUBLIQUE TOGOLAISE
MSPC
DT CDA


Did you KNOW?


DG ANCy

Rapport Annuel d'Activités 2024

Adresse et contacts

63 Bd du 13 Janvier,
Nyékonakpoe, Lomé-TOGO
07 BP 7878
Email : secretariat.ancy@ancy.gouv.tg
Tel 1 : +228 97 52 58 58
Tel 2 : +228 70 60 60 83

ANCy
Agence Nationale de la Cybersécurité