RÉPUBLIQUE TOGOLAISE

Ministère de l'Économie Numérique
et de la Transformation Digitale

ANCy
Agence Nationale
de la Cybersécurité

RAPPORT D'ACTIVITES **2023**

SOMMAIRE

Liste des sigles et abréviations

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 Eyadéma
ATD :	Agence Togo Digital
BOAD :	Banque Ouest Africaine de Développement
BTCI :	Banque Togolaise pour le Commerce et l'Industrie
CDA :	Cyber Defense Africa
CEDEAO :	Communauté Economique des Etats de l'Afrique de l'Ouest
CEET :	Compagnie Energie Electrique du Togo
CENI :	Commission Electorale Nationale Indépendante
CENTIF :	Cellule Nationale de Traitement des Informations Financières
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
CRRH :	Caisse Régionale de Refinancement Hypothécaire
CSIRT :	Computer Security Incident Response TEam
CTF :	Capture The Flag
DGIPE :	Direction Générale de l'Informatique et du Personnel de l'Etat
DGTCP :	Direction Générale du Trésor et de la Comptabilité Publique
EPL :	Ecole Polytechnique de Lomé
EPS :	Evènement par Seconde
FAIEJ :	Fonds d'Appui aux Initiatives Economiques des Jeunes
INAM :	Institut National d'Assurance Maladie
LONATO :	Loterie Nationale Togolaise

Liste des tableaux

Liste des figures

Liste des graphiques

Introduction

L'Afrique fait de plus en plus face à des défis croissants en matière de cybersécurité, alors qu'elle se connecte de plus en plus à l'économie numérique mondiale. L'utilisation accrue des technologies de l'information et de la communication offre des opportunités économiques et sociales importantes, mais elle rend également les pays africains plus vulnérables aux cybermenaces. Le Togo qui, en l'espace d'une décennie, a établi des records en matière de digitalisation de ses services, n'échappe pas à cette réalité.

Face à ces risques, la création de l'Agence nationale de la cybersécurité (ANCy) démontre la volonté des plus hautes autorités nationales d'être à l'avant-garde de la lutte contre ce fléau mondial qui sape les efforts de développement de États.

Les activités exposées dans le présent rapport sont la preuve de l'engagement de l'État togolais à renforcer la résilience des administrations, des entreprises et des individus en matière de cybersécurité.

Cet engagement se matérialise à travers les efforts qui ont été déployés pour élaborer des politiques nationales, renforcer la coopération régionale, sensibiliser et former, ainsi que pour initier le développement d'une main-d'œuvre qualifiée en cybersécurité. De plus, les initiatives visant à renforcer la législation et à améliorer la collaboration avec le secteur privé et les organisations internationales sont également en cours.

Le présent rapport d'activités est conçu pour informer sur l'essentiel des activités déployées tout au long de l'année 2023. Ces actions ont été menées en étroite collaboration avec Cyber Defense Africa (CDA), le bras technique et opérationnel de l'ANCy.

Commandant Gbota GWALIBA
Directeur Général de l'ANCy

MOT DU DIRECTEUR GENERAL

Mesdames et Messieurs,

L'Agence nationale de la cybersécurité (ANCy) est ravie de vous présenter son rapport d'activités pour l'année 2023. Cette période a été marquée par des avancées significatives dans notre engagement envers la protection des infrastructures et des services numériques essentiels, ainsi que la sensibilisation de la population togolaise aux enjeux de la cybersécurité.

Notre vision principale reste la même : **« Participer à la transformation digitale du Togo à travers la sécurisation de son cyberespace ».** Pour y parvenir, nous coordonnons l'action gouvernementale en matière de défense des systèmes d'information, désignons et auditons les Opérateurs de Services Essentiels (OSE), enregistrons et qualifions les prestataires de services de cybersécurité, et étendons notre influence grâce à la sensibilisation à tous les niveaux de la population face aux défis de la cybersécurité.

En 2023, l'ANCy a intensifié ses efforts pour renforcer la résilience des OSE, les organisations tant privées que publiques, et les individus face aux menaces de cybersécurité en constante évolution. À travers des sensibilisations ciblées, des formations spécialisées et des partenariats stratégiques, nous avons collaboré étroitement avec ces acteurs clés pour renforcer leur résilience cybersécurité. En partenariat avec Cyber Defense Africa (CDA), nous avons contribué à éliminer plusieurs menaces, à riposter à plusieurs attaques et à restaurer l'intégrité des systèmes.

Certaines des initiatives les plus significatives de 2023 ont été notre campagne de sensibilisation à l'échelle nationale, et l'organisation de la grande finale du Hackathon de la CEDEAO. La cybersécurité étant une responsabilité partagée, nous avons déployé d'importants efforts pour informer et éduquer diverses couches de la population, des étudiants aux décideurs, sur les risques liés à l'utilisation des technologies numériques et les meilleures pratiques à adopter pour se protéger en ligne.

Chers lecteurs, ce rapport d'activités offre un aperçu détaillé des réalisations de l'ANCy en 2023 tout en représentant un appel à une action continue.

Nous exprimons nos sincères remerciements à nos partenaires, aux OSE, aux prestataires de services de cybersécurité et à la population togolaise pour leur collaboration et leur engagement continu envers une cybersécurité renforcée.

Commandant Gbota GWALIBA
Directeur Général de l'ANCy

1- PRESENTATION DE L'ANCy

1.1. Les attributions de l'ANCy

L'Agence nationale de la cybersécurité (ANCy) a été créée par la loi n 2018-026 du 07 décembre 2018 sur la cybersécurité et la cybercriminalité. Elle est organisée par le décret n 2019-026/PR du 13 février 2019 portant organisation, attributions et fonctionnement de l'Agence nationale de la cybersécurité. Placée sous l'autorité du Premier Ministre, Président de son comité stratégique, l'ANCy est sous la tutelle technique et administrative du ministère chargé de l'économie numérique et de la transformation digitale, ainsi que du ministère de la sécurité et de la protection civile.

En tant qu'autorité nationale en matière de sécurité des systèmes d'information au Togo, l'ANCy joue un rôle significatif dans la définition et la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité. Elle contribue activement à la défense et à la sécurité de la République Togolaise en assurant la sensibilisation des utilisateurs des équipements, des services et installations informatiques, la prévention des intrusions, ainsi que la sécurisation et la défense de l'ensemble des systèmes d'information.

L'ANCy coordonne également la riposte aux attaques informatiques et instruit les demandes de qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité des systèmes d'information au Togo. En ce qui concerne la coordination et la riposte aux attaques informatiques, l'ANCy s'appuie sur Cyber Defense Africa (CDA), qui agit en tant que bras technique et opérationnel. CDA est chargé de mettre en œuvre le Computer Emergency Response Team (CERT) et le Security Operation Center (SOC) à l'échelle nationale, en tant que services délégués par l'ANCy.

1.2. Les missions de l'ANCy

Les missions assignées à l'Agence nationale de la cybersécurité sont les suivantes :

- 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 ;
- Participer à la lutte contre la cybercriminalité ;
- Former et sensibiliser le public en cybersécurité.

Pour accomplir ses missions, l'ANCy dispose d'un cadre de gouvernance.

1.3. Le cadre de gouvernance de l'ANCy

Le cadre de gouvernance de l'ANCy s'articule autour de deux organes : le Comité Stratégique et la Direction Générale.

1.3.1. Le Comité Stratégique

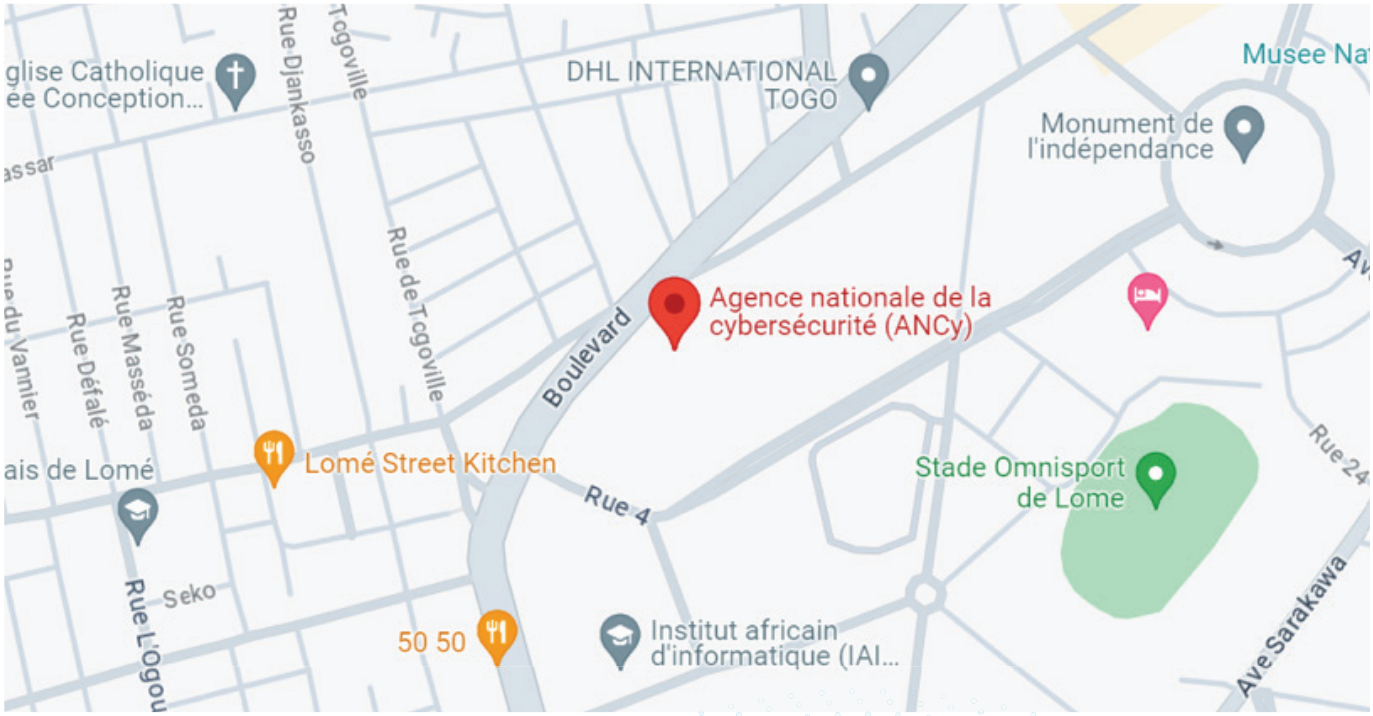
Le comité stratégique est l'organe stratégique de l'ANCy. Il est placé sous l'autorité du Premier Ministre et constitue l'organe d'administration et de gestion de l'ANCy. Sur les orientations du Président de la République, il élabore les propositions relatives à la politique nationale de cybersécurité. Sa principale mission est de définir et d'orienter la politique générale de l'ANCy. Il joue également un rôle essentiel dans l'évaluation de la gestion de l'Agence.

Le comité stratégique de l'ANCy 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.

1.3.2. La Direction Générale

Siège de l'ANCy



Localisation géographique de l'ANCy

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.

2- LE CADRE JURIDIQUE DE LA CYBERSÉCURITÉ AU TOGO

2.1. Les textes internationaux

Il s'agit essentiellement 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 ;

- La directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

2.2. Les textes nationaux

Les textes nationaux sont composés de quatre (4) lois, de six (6) décrets et d'un (1) arrêté.

- Loi n°2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n°2013-003 du 19 février 2013 ;

- Loi n°2017-007 du 22 juin 2017 relative aux transactions électroniques ;

- 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 22 juin 2022 ;

- Loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;

- Décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;

- Décret n°2018-144/PR du 03 octobre 2018 portant modification du décret n°2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques ;

- 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°2020-16/PR du 23 décembre 2020 portant sur le déploiement national de réseaux de communications électroniques en fibre optique ;

- Décret n°2021-072/PR du 24 juin 2021 portant définition des règles d'identification des marchés pertinents et de désignation des opérateurs puissants dans le secteur des communications électroniques ;

- 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 ;

- L'arrêté n°2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

L'ensemble des textes législatifs et réglementaires précités permettent à l'Agence de mener ses activités avec efficacité.

3- LA GESTION ADMINISTRATIVE

3.1. Le recrutement du personnel

A ce titre, l'ANCy a renforcé son équipe avec le recrutement de cinq (5) profils dont un directeur de la formation et du renforcement des capacités, un chargé de la communication institutionnelle et des relations publiques, un juriste, une secrétaire et un assistant comptable.

3.2. La poursuite des travaux de réhabilitation du siège de l'ANCy

De nouveaux bureaux ont été construits et des bureaux existants ont été réhabilités.

3.3. La réunion du Comité Stratégique de l'ANCy

Tenue le vendredi 22 décembre 2023 à la Primature, la réunion du Comité Stratégique de l'ANCy a permis de faire le bilan des activités de l'Agence durant l'année 2023 et à adopter plusieurs documents importants pour le fonctionnement régulier et optimal de l'Agence. Il s'agit notamment de la Stratégie nationale de cybersécurité 2024-2028, du manuel de procédures, de gestion administrative, ressources humaines, comptables, financières et de passation des marchés et du budget de fonctionnement de l'ANCy, exercice 2024.

4- LA MISE EN ŒUVRE DES MISSIONS

4.1. Les missions opérées par l'ANCy

4.1.1. Les activités relatives aux opérateurs de services essentiels (OSE)

4.1.1.1. La désignation des Opérateurs de services essentiels (OSE)

L'article 5 du décret n 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes reconnaît à l'ANCy la prérogative de désigner les OSE, suivant des critères et une procédure bien précise. En application de cette disposition, de nouveaux OSE ont été désignés en plus de ceux désignés en 2021.

Pour rappel, les OSE sont des entités publiques ou privées qui fournissent un service essentiel et qui sont tributaires des réseaux informatiques ou des systèmes d'information et dont l'arrêt aurait un impact significatif sur le fonctionnement de l'économie ou la société.

4.1.1.2. Le démarrage des audits de conformité

Selon l'article 6 de la loi N 2018-026 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, l'ANCy est chargée de faire les audits de conformité aux OSE. C'est dans ce cadre qu'elle a commissionné CDA, de faire les audits des OSE désignés en 2021.

Ces audits visent à évaluer le niveau de conformité des OSE aux règles nationales de cybersécurité, à détecter leurs vulnérabilités et à leur proposer des correctifs.

4.1.2. Les activités de communication

Les actions de communication de l'ANCy pour le compte de 2023 se sont accentuées par rapport à l'année précédente. Elles sont réparties en deux grandes catégories : les activités de communication média et les activités de communication hors média.

4.1.2.1. Les activités de communication média

L'ANCy, utilise divers moyens de communication pour informer le public, les partenaires et les parties prenantes sur ses projets et ses activités.

Ces activités ont été menées via les canaux des médias traditionnels tels que la télévision, la radio, les journaux, l'internet, etc. Le but de ces activités est de promouvoir un cyber espace sûr et sécurisé, grâce à la contribution des médias, qui relayent les informations sur l'ANCy et la cybersécurité pour atteindre un public large et diversifié.

Les plateformes de **médias sociaux** de l'ANCy ont été utilisées pour partager les actualités, les vidéos, les infographies et interagir avec le public. Ces plateformes sont Facebook, LinkedIn, YouTube et X. Des **vidéos institutionnelles** et de reportage ont été

créées pour transmettre visuellement les missions et messages de l'ANCy.

Le **site web officiel** de l'ANCy, **www.ancy.gouv.tg** a été alimenté avec des mises à jour régulières, des textes et des ressources en ligne pour que le public puisse accéder à des informations pertinentes et actualisées sur la cybersécurité au Togo et les activités de l'ANCy.

L'organisation des **conférences de presse** a permis à l'ANCy de présenter des annonces majeures aux médias, de répondre aux questions des journalistes et surtout de générer une couverture médiatique pour les informations pertinentes.

La participation à plusieurs **émissions radiophoniques** sur Radio Lomé, Taxi FM, Nana FM, Kanal FM, Victoire FM, Pyramide FM et Zéphyr FM ainsi que des émissions télévisées sur les antennes de la TVT, et New World TV ont donné une plus grande envergure aux messages d'information et de sensibilisation portés par l'ANCy.

4.1.2.2. Les activités de communication hors média

L'organisation de ces activités de communication n'implique pas l'utilisation directe de médias traditionnels tels que la télévision, la radio, les journaux, etc. Elles ont été organisées en collaboration avec CDA.

Il s'agit des actions directes sur le terrain en vue de montrer l'engagement de l'ANCy envers l'appropriation de la cybersécurité pour tous. Elles avaient pour but de créer des interactions directes avec le public cible, construire une image positive de l'ANCy, sensibiliser le public et renforcer l'engagement envers les missions de l'ANCy. Les activités de communication non-média qui ont été menées sont les suivantes :

- Quinze (15) ateliers et sessions d'information, de formation et de sensibilisation organisés à l'endroit de cibles diversifiées pour les informer des missions de l'ANCy et les éduquer sur la cybersécurité ;
- Deux (02) évènements forains de hackathon organisés, l'un international et l'autre national ;
- La participation à six (06) évènements internationaux majeurs réunissant des acteurs clés gouvernementaux de cybersécurité.

Les activités de communication ont été importantes pour atteindre un large public, favoriser une compréhension générale des missions de l'ANCy, forger une présence médiatique positive et éduquer sur les enjeux de la cybersécurité pour toutes les parties prenantes.

4.1.3. L'organisation de compétitions en cybersécurité

4.1.3.1. Organisation du concours ''Cyber Security Challenge''

En février 2023, Cyber Defense Africa (CDA), l'Agence Nationale de la Cybersécurité (ANCy) et CanalBox Togo (GVA Togo) ont organisé le « Cyber Security Challenge ». Le jeu s'est déroulé sur le réseau social TikTok, offrant ainsi une approche novatrice pour sensibiliser la population aux enjeux de la cybercriminalité au Togo et comment se protéger sur internet. Ce concours a exploité le format de courtes vidéos pour transmettre un message percutant sous le thème «Les dangers de la cybercriminalité au Togo : « Protégez-vous des arnaques en ligne et renforcez vos mots de passe ! ».

L'initiative a connu un succès significatif, générant plusieurs centaines de milliers de vues. Cette viralité a joué un rôle important dans la sensibilisation des populations togolaises aux risques liés à la cybercriminalité. Les vidéos créatives et informatives ont captivé l'attention du public, mettant en lumière les différents stratagèmes utilisés par les cybercriminels et prodiguant des conseils pratiques pour se prémunir contre ces menaces.

Le message central du concours était axé sur l'importance de renforcer la sécurité des mots de passe, un élément crucial dans la protection contre les attaques en ligne.

En incitant les participants et les spectateurs à adopter des pratiques de sécurité numérique plus robustes, le Cyber Security Challenge a contribué à changer les comportements et à encourager une attitude plus prudente dans l'utilisation d'Internet.

En plus de sensibiliser la population, cette initiative a également permis à l'Agence nationale de la cybersécurité (ANCy) d'accroître sa visibilité. En associant son nom à un événement novateur sur une plateforme populaire comme TikTok, l'ANCy a renforcé sa présence et sa crédibilité dans

le domaine de la cybersécurité au Togo. Cette visibilité accrue pourrait également conduire à une augmentation de la confiance du public envers l'ANCy en tant qu'organisme engagé dans la protection des citoyens contre les menaces numériques.

En résumé, le Cyber Security Challenge sur TikTok a réussi à marier efficacement l'innovation technologique et la sensibilisation publique, contribuant ainsi à renforcer la sécurité en ligne et à positionner l'ANCy en tant qu'acteur clé dans la promotion d'une cybersécurité consciente au Togo.

4.1.3.2. Première édition du Capture The Flag national

L'Agence Nationale de la Cybersécurité et Cyber Defense Africa ont conjointement organisé la 1ère édition du concours national de cybersécurité en ligne dénommé CTF national. Il s'est déroulé du 22 au 23 juillet 2023 sur une plateforme en ligne exclusivement dédiée à cette compétition. L'objectif est de renforcer la résilience numérique du pays et mettre un accent particulier sur l'importance de la collaboration entre les acteurs clés de la cybersécurité dont les jeunes hackers.

Les gagnants du Cyber Security Challenge

La présentation a été faite lors d'une rencontre stratégique qui a rassemblé les étudiants des universités publiques et privées du Togo, dont l'IPNet Institute, l'Université Catholique de l'Afrique de l'Ouest (UCAO), la Faculté des Sciences de l'Université de

Kara, entre autres. Cette rencontre, tenue le 22 juin 2023 à Lomé, a marqué le lancement officiel du concours national de cyber hacking, une initiative d'une importance capitale pour inciter les talents à contribuer au renforcement de la résilience numérique du Togo.

avant le rôle que chacun doit jouer pour renforcer la posture de sécurité numérique du Togo.

Le lancement du concours a été planifié de manière à inspirer l'engagement des étudiants envers la cybersécurité et à stimuler leur intérêt pour les domaines liés au hacking éthique, en présentant le concours comme une opportunité d'appliquer leurs compétences de manière constructive.

Vue partielle des participants au lancement de la 1ère édition du CTF national

Cette rencontre a permis de mettre en avant l'importance du concours national de cyber hacking en tant que levier essentiel pour améliorer la cybersécurité au Togo. La présentation a mis en évidence la nécessité de sensibiliser les étudiants et les futurs professionnels de l'informatique aux

enjeux de la sécurité numérique. Elle a également souligné l'importance de la collaboration entre les principaux acteurs de la cybersécurité, mettant en

La compétition elle-même s'est déroulée du 22 au 23 juillet 2023, sur une plateforme dédiée, pour que les étudiants mettent en pratique leurs connaissances en matière de cybersécurité

Il faut dire que des événements pareils contribuent à former la prochaine génération d'experts en sécurité informatique et à renforcer les capacités du pays dans la lutte contre les cybermenaces.

Les 3 lauréats du CTF national présentant leurs récompenses

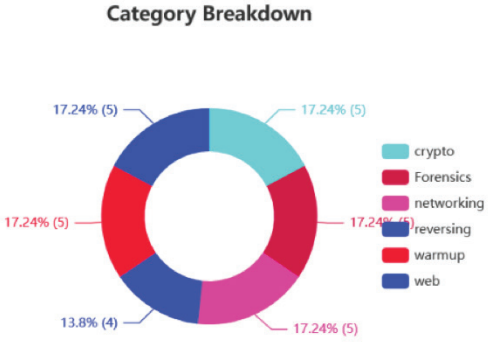
A l'issue de la compétition, trois (3) lauréats ont été récompensés lors d'une cérémonie tenue le 12 décembre 2023 au siège de l'ANCy à Lomé. Pour cette première édition, ils étaient 115 jeunes hackers éthiques à affronter les défis. Les trois (3) premiers ont été récompensés avec des prix composés de matériels informatiques mais aussi de certification et d'inscription à des compétitions de hacking en ligne.

4.1.3.3. Organisation de la 2ème édition du Hackathon de la CEDEAO 2023

L'ANCy et CDA ont conjointement organisée en collaboration avec la commission de la CEDEAO, OCWAR-C et Expertise France, la deuxième édition de la compétition régionale de cybersécurité dénommée ECOWAS HACKATON 2023 a rassemblé des équipes venues de onze (11) pays de la sous-région du 16 au 18 octobre 2023 à Lomé.

Place	User	Score
1	0x1	2750
2	K4n3ki	2750
3	Kurosu	2750
4	Alr3ady_D3ad	2750
5	44r0n_M3TA	2650

Score des 5 premiers



Répartition des compétiteurs par catégorie

Cette année, la Mauritanie a remporté la première, suivie de près par le Bénin, qui s'est classé deuxième, et le Nigeria, à la troisième place. Le Togo, pour sa part, occupe une honorable cinquième place malgré son handicap numéraire, puisqu'au lieu de quatre candidats, seuls trois candidats étaient effectivement présents.

Le Hackathon a émergé comme un acteur clé dans le façonnement des compétences et la promotion d'un environnement numérique sécurisé au sein de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO). L'organisation de la grande finale au Togo souligne l'engagement des plus hautes autorités du pays à soutenir les initiatives visant à renforcer la cybersécurité dans la région.

Cette compétition régionale, orchestrée en collaboration avec la commission de la CEDEAO, OCWAR-C (Centre ouest-africain de lutte contre la cybercriminalité) et Expertise France, a réuni des équipes provenant de onze pays de la sous-région. Cet événement a fourni une plateforme unique pour des confrontations stimulantes et des collaborations exceptionnelles entre de jeunes talents en cybersécurité.

L'objectif principal du Hackathon va au-delà de la simple compétition car il vise à favoriser l'échange de connaissances, le partage d'expertise et le renforcement des capacités dans le domaine de la cybersécurité. Les participants ont eu l'occasion de travailler sur des défis complexes, de mettre en pratique leurs compétences en matière de défense numérique, et d'explorer des solutions novatrices pour contrer les menaces émergentes dans le cyberespace.

Des membres du comité d'organisation

Les membres de la team Togo au hackathon

Les participants au hackathon de la CEDEAO

En favorisant un esprit de collaboration et d'innovation, le Hackathon de la CEDEAO contribue à la création d'une communauté régionale solide de professionnels de la cybersécurité. Ces jeunes talents, issus de divers horizons culturels, ont pu échanger des idées, partager des bonnes pratiques et tisser des liens qui transcendent les frontières nationales.

La collaboration entre les différents partenaires, notamment la commission de la CEDEAO, OCWAR-C et Expertise France, témoigne de l'importance accordée à la sécurité numérique dans la sous-région. En soutenant activement de telles initiatives, ces partenaires contribuent à renforcer la résilience des systèmes informatiques et à promouvoir un environnement numérique sûr et fiable au sein de la CEDEAO. Le Hackathon demeure ainsi un catalyseur essentiel pour l'émergence de talents en cybersécurité et la consolidation des efforts régionaux dans la lutte contre les menaces cybernétiques.

4.1.4. Les activités de sensibilisation et de formation

4.1.4.1. Atelier de sensibilisation des institutions financières aux enjeux de la cybersécurité

Le vendredi 27 janvier 2023, en collaboration avec Cyber Defense Africa, l'Agence Nationale de la Cybersécurité (ANCy) a organisé l'atelier de sensibilisation et de formation à l'endroit des banques et autres établissements financiers sur les enjeux de la cybersécurité.

Cet atelier qui s'est tenu à Lomé, est parti du constat que les institutions financières sont devenues des cibles privilégiées pour les pirates informatiques. L'objectif majeur de cet événement était d'informer ces institutions sur les procédures et les moyens leur permettant de renforcer leur résilience contre les attaques de leurs systèmes d'information, tout en respectant les lois en vigueur au Togo.

Les participants ont bénéficié de l'expertise de spécialistes en cybersécurité qui ont abordé deux thèmes fondamentaux. Le premier thème, «l'écosystème de la cybersécurité au Togo», a fourni aux participants une compréhension approfondie de la situation actuelle de la cybersécurité dans le pays, en mettant en lumière les cadres réglementaires et institutionnels.

Le deuxième thème, «les institutions financières africaines au cœur des cyberattaques», a mis l'accent sur les défis spécifiques auxquels les institutions financières du continent sont confrontées en termes de cybersécurité. En examinant des cas concrets et en fournissant des analyses approfondies, les experts ont pu sensibiliser les participants aux tactiques sophistiquées utilisées par les cybercriminels et aux conséquences potentielles de ces attaques sur la stabilité financière et la réputation des institutions.

Une attention particulière a été accordée à la nécessité de se conformer aux lois en vigueur au Togo en matière de cybersécurité. Aussi, des conseils sur la mise en place de mesures de sécurité respectant les réglementations nationales ont été prodigués.

Le Directeur Général de l'ANCy avec à sa gauche le Directeur de la Réglementation et du Contrôle de Conformité de l'ANCy et à droite du Directeur Technique de CDA

Vue partielle de l'assistance

En fournissant aux institutions financières des informations précieuses et des outils pratiques, cet atelier visait à les doter des moyens nécessaires pour renforcer la protection des données clients, éviter les pertes financières et sauvegarder leur réputation. En fin de compte, cette initiative contribue à renforcer la résilience du secteur financier togolais face aux menaces croissantes de la cybercriminalité.

4.1.4.2. Ateliers de sensibilisation aux enjeux de la cybersécurité, à l'endroit des professionnels de l'hôtellerie et de la restauration

L'atelier organisé le 18 avril 2023 à Lomé a constitué une initiative louable visant à sensibiliser les professionnels de l'hôtellerie et de la restauration aux risques inhérents aux cyberattaques, qui pourraient compromettre la pérennité de leur secteur d'activité. La conscientisation des acteurs de l'industrie hôtelière sur ces menaces de plus en plus sophistiquées revêt une importance capitale, compte tenu de la dépendance croissante du secteur envers les technologies de l'information et la fréquentation de plus en plus grande de ces endroits par le public.

L'objectif premier de cet atelier était d'éduquer les professionnels sur les diverses formes de cyberattaques susceptibles de viser les établissements hôteliers et de restauration. Des exemples concrets et des scénarios réalistes ont été présentés pour illustrer les méthodes utilisées par les cybercriminels dans ce contexte spécifique. Cela a permis aux participants de mieux comprendre les risques auxquels ils sont exposés.

Un autre aspect de cet atelier était de fournir des conseils pratiques et des directives sur la mise en place de mesures de sécurité, notamment des recommandations sur la sécurisation des systèmes informatiques, la gestion des accès, la sensibilisation des employés aux bonnes pratiques en matière de cybersécurité, et la mise en œuvre de politiques de protection des données à caractère personnel. L'objectif ultime était d'autonomiser les professionnels pour qu'ils puissent prendre des mesures concrètes afin de protéger leurs clients, leurs employés et leur entreprise contre les cybermenaces.

Les hôteliers et restaurateurs sensibilisés à Lomé

Les hôteliers et restaurateurs sensibilisés à Kpalimé

Un aspect important de l'atelier a été la sensibilisation aux réflexes à adopter en cas d'incident de cybersécurité. Les participants ont été informés sur la manière de réagir rapidement et efficacement pour minimiser les dommages en cas de violation de la sécurité informatique notamment en recourant aux services du CERT.tg

Cet atelier a été une étape essentielle dans la sensibilisation et la préparation des professionnels de l'hôtellerie et de la restauration face aux défis croissants de la cybersécurité. En les dotant des connaissances et des outils nécessaires, il a contribué à renforcer la résilience du secteur face aux menaces numériques et à assurer la sécurité des données sensibles et des activités commerciales.

Il est à noter que la même formation a été délivrée à Kpalimé le 21 juillet 2023, où l'ANCy a rencontré les acteurs du secteur de l'hôtellerie et de la restauration de la zone.

4.1.4.3. Sensibilisation des étudiants de l'École Polytechnique de Lomé (EPL) à l'importance de la cybersécurité

La rencontre du 11 août 2023 au siège de l'ANCy à Lomé avec une délégation d'étudiants de l'École Polytechnique de Lomé (EPL) de l'université de Lomé a été une opportunité importante pour sensibiliser ces futurs professionnels aux enjeux de la cybersécurité. L'objectif était de susciter un intérêt accru parmi les étudiants pour les métiers dans le domaine en pleine expansion de la cybersécurité.

Au cours de cette rencontre, les étudiants ont bénéficié d'une présentation des réalités et défis du monde de la cybersécurité,. Des discussions ont couvert un large éventail de sujets, y compris les tendances actuelles en matière de cybermenaces, les technologies émergentes en cybersécurité et les rôles variés qu'ils pourraient jouer dans ce domaine.

Les étudiants ont pu prendre conscience de la complexité et de la gravité des menaces présentes dans le monde numérique. Les discussions ont mis en avant l'importance de la cybersécurité dans la protection des systèmes d'information, des données sensibles et de la société dans son ensemble. L'engagement exprimé par les étudiants à poursuivre leurs carrières dans le domaine de la cybersécurité témoigne du succès de cette rencontre. Le fait que ces jeunes talents se montrent intéressés à contribuer à la protection de la société contre les menaces numériques représente une avancée positive dans la formation de la prochaine génération d'experts en cybersécurité au Togo.

Vue partielle des étudiants de l'EPL en visite à l'ANCy

4.1.4.4. Formations intensives pour les magistrats et les forces de l'ordre sur la lutte contre la cybercriminalité et la collecte des preuves électroniques

Dans le cadre de ses relations de coopération, l'ANCy a organisé en collaboration avec OCWAR-C, deux sessions de foration pour les magistrats sur le thème : « Cybercriminalité et technique de collecte des preuves numériques ».

La participation des magistrats togolais à cette session de formation à Lomé s'est avérée

indispensable car les défis liés à la cybercriminalité sont en constante évolution, nécessitant une mise à jour régulière des compétences des professionnels impliqués dans la justice. La familiarisation avec les techniques d'investigation numérique, les lois nationales et internationales sur la cybersécurité, ainsi que les bonnes pratiques en matière de collecte et de préservation des preuves numériques, sont des éléments clés qui ont été présentés pour renforcer l'efficacité des autorités judiciaires face à ces nouvelles formes de criminalité.

Photo de famille des organisateurs et des bénéficiaires de la formation

De plus, le lien direct avec la politique nationale de cybersécurité du Togo, adoptée en 2018, souligne l'importance de cette formation dans la mise en œuvre concrète des mesures prévues pour faire face aux menaces de cybersécurité.

La Secrétaire Générale du Centre de formation des professions de justice (CFPJ) à droite, remettant une attestation de formation à une magistrate récipiendaire

Les magistrats formés en début septembre 2023, se sont retrouvés du 13 au 17 novembre 2023 pour une restitution. Ceci a fait de ces magistrats, des acteurs clés dans la transmission continue des connaissances sur la cybersécurité au sein de la communauté judiciaire togolaise, contribuant ainsi à une justice numérique robuste et adaptée aux défis du XXIe siècle.

Les élèves greffiers ont également été sensibilisés par la même occasion, sur les enjeux de la cybersécurité.

4.1.4.5. Tournée nationale de sensibilisation

La première phase de la tournée nationale de sensibilisation, s'est déroulée du 10 au 20 septembre 2023 respectivement à Cinkassé, Mango, Pagouda, Bassar, Tchamba et Sotouboua, et la deuxième phase du 4 au 8 décembre 2023, dans les villes de Badou, Tohoun, Tabligbo et Kévé. Ces sessions visaient à former, informer et sensibiliser les acteurs locaux sur l'écosystème de la cybersécurité, ainsi que sur les bonnes pratiques à adopter pour se protéger et protéger leurs organisations.

Les entités locales, de plus en plus connectées aux technologies numériques, bénéficient simultanément d'opportunités et font face à des risques accrus. La cybersécurité devient ainsi une préoccupation majeure, car les informations sensibles et les services publics peuvent être vulnérables aux cyberattaques. L'initiative de sensibilisation de l'ANCy visait donc à renforcer la résilience de ces entités locales face aux défis croissants de la cybersécurité.

Au total, près de 2000 participants, représentant les administrations publiques, les collectivités territoriales, le secteur privé et la société civile, ont bénéficié de ces sensibilisations. Les sessions ont couvert les enjeux stratégiques, juridiques, techniques et opérationnels de la cybersécurité, ainsi que les moyens de prévention, de détection et de réaction face aux incidents de cybersécurité. Cela incluait notamment la présentation de bonnes pratiques adaptées aux réalités de ces entités locales.

La diversité des participants reflète la nécessité de sensibiliser un large éventail d'acteurs, car la cybersécurité concerne non seulement les entités gouvernementales, mais aussi les organisations du

secteur privé, la société civile et les personnes physiques. Au total, près de 800 participants ont bénéficié de ces sensibilisations aidant à accroître la compréhension et la préparation face aux défis croissants liés à la cybersécurité.

Les thèmes abordés lors des sessions, tels que les enjeux stratégiques, juridiques, techniques et opérationnels de la cybersécurité, ainsi que les moyens de prévention, de détection et de réaction face aux incidents de cybersécurité, couvrent de manière complète les aspects les plus importants de ce domaine. Il est à noter également que ces initiatives contribuent à renforcer la culture de la cybersécurité au niveau local, favorisant une meilleure protection des infrastructures et des données sensibles. Elles témoignent de l'engagement continu des autorités togolaises à renforcer la sécurité numérique dans le pays.

Sensibilisation à Badou

Sensibilisation à Tohoun

Sensibilisation à Mango

Sensibilisation à Tabligbo

Sensibilisation à Kévé

4.1.4.6. Sensibilisation des élèves du primaire et du secondaire de la Fondation Makafui

Le 23 novembre 2023, une activité de sensibilisation a été organisée à Lomé dans le cadre de la mobilisation des couches sociales vulnérables visant à renforcer leur empreinte numérique et à sécuriser leur présence sur Internet et les réseaux sociaux.

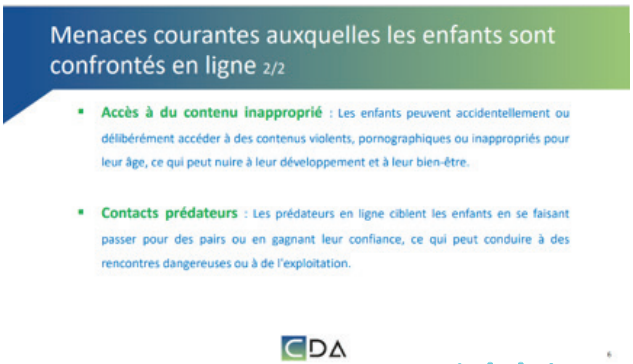
Cette initiative s'est particulièrement concentrée sur les enfants, en raison de leur vulnérabilité et de leur manque d'expérience, les exposant à divers risques lors de l'utilisation d'Internet. En effet, les enfants peuvent être confrontés à des contenus inappropriés, voire violents, au cyberharcèlement, à des contacts indésirables, à des liens malveillants et à des fichiers infectés.

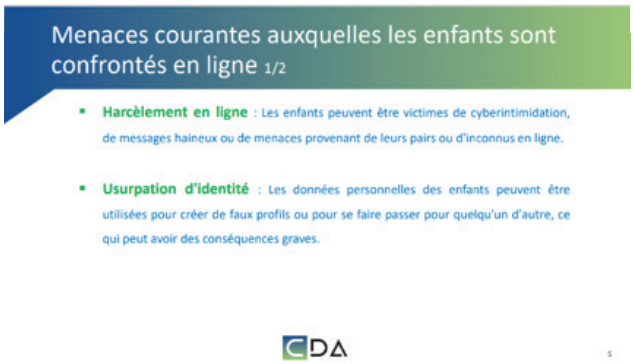
L'événement a réuni 180 enfants en présence de leurs enseignants, offrant une opportunité d'explorer les tenants et les aboutissants de la sécurité en ligne à travers une méthodologie adaptée à leur niveau. L'objectif était de leur fournir les connaissances nécessaires pour prendre des décisions éclairées et protéger la sécurité des dispositifs familiaux face aux risques liés à l'utilisation d'Internet.

Des élèves du primaire et du collège à une séance de sensibilisation

4.1.4.7. Sensibilisation des personnes du troisième âge sur la cybersécurité et la vigilance numérique des personnes vulnérables

Le 27 novembre 2023, l'ANCy a organisé à Lomé une sensibilisation spécifique pour les personnes du troisième âge, qui sont de plus en plus connectées en ligne pour divers besoins tels que la communication, la gestion financière et les achats en ligne. Cette démarche visait à les informer sur les risques significatifs liés à la cybersécurité, notamment en ce qui concerne la protection des informations personnelles et financières, ainsi que de la vie privée.





Des veuves du 3è âge sensibilisées

Au cours de cet événement, l'ANCy a rassemblé plus d'une centaine de personnes du troisième âge pour les sensibiliser sur l'écosystème de la cybersécurité et leur fournir des conseils pratiques adaptés à leur génération. L'objectif était de les aider à adopter les bonnes pratiques en matière de sécurité en ligne, afin de minimiser les risques et de profiter en toute sécurité des avantages de la connectivité numérique.

D'anciens combattants et anciens militaires sensibilisés

4.1.4.8. La campagne digitale contre les menaces de cybersécurité en période des fêtes de fin d'année

Pour sensibiliser le public sur les risques de cyberattaques pendant les fêtes de fin d'année et promouvoir de bonnes pratiques, l'ANCy a lancé une campagne digitale d'information sur les menaces existantes pendant cette période. Des éléments visuels ont été créés par l'Agence et partagés sur ses canaux digitaux au cours de la seconde moitié du mois de décembre.

Afin d'assurer une diffusion maximale de ces visuels, l'ANCy a collaboré avec les médias. Reconnaissant le rôle des médias dans l'information, l'éducation et le divertissement, une collaboration étroite a été encouragée pour informer et éduquer le public, renforçant ainsi la sécurité en ligne de toute la communauté pendant les fêtes de fin d'année.

À cet effet, l'ANCy, conjointement avec Cyber Defense Africa (CDA), a réuni les acteurs des médias le mardi 19 décembre 2023 à Lomé. Lors de cette rencontre, un appel à l'action a été lancé, incitant les médias à jouer un rôle essentiel dans la diffusion intensive des éléments visuels contenant des messages conçus par l'ANCy et publiés sur ses canaux de communication.

4.1.5. La participation aux évènements internationaux sur la cybersécurité

Vue partielle du parterre de journalistes présents

Un des visuels de sensibilisation partagés sur les réseaux sociaux

4.1.5.1. Le Cyber Africa Forum (CAF)

La troisième édition de ce forum, placée sous le thème «Enjeux, acteurs et partenariats : quelles solutions pour sécuriser la transformation digitale de l'Afrique ?», s'est déroulée du 24 au 25 avril 2023 à Abidjan. Cette édition a été consacrée à la nécessité de renforcer les partenariats multisectoriels et transnationaux en matière de sécurité numérique.

4.1.5.2. La formation sur le droit international des cyber opérations

Elle s'est déroulée du 12 au 14 juin 2023 au siège de l'Union Africaine à Addis-Abeba et a réuni 15 pays autour du droit international des cyber opérations.

Panel d'ouverture du CAF Abidjan 2023

En effet, l'augmentation récente des activités malveillantes en ligne et l'évolution rapide des capacités cybernétiques ont conduit les États à s'interroger sur la manière dont le droit international s'applique aux activités des États dans le cyberespace

ECOWAS
CEDEAO

Logo de la CEDEAO

4.1.5.3. Le Cyber Week 2023 à l'Université Tel-Aviv

Cet évènement de grande envergure s'est tenu à Tel-Aviv en Israël du 26 au 29 juin 2023. Il portait sur des sujets tels que les dernières tendances en matière de cybersécurité, les stratégies de transformation numérique, la numérisation du secteur financier et des administrations publiques, la sécurité des données et l'utilisation responsable et éthique des données, l'intelligence artificielle et les défis de la cyber diplomatie.

Les panélistes de la CyberWeek

4.1.5.4. La semaine des CSIRT de la CEDEAO 2023 à Abidjan

Elle s'est tenue du 31 juillet au 4 août 2023 et a regroupé 13 pays pour cette troisième édition. L'objectif principal de cette rencontre sous régionale était de définir les modalités de fonctionnement du centre régional de coordination de la cybersécurité, qui aura pour mission de faciliter la coopération et le partage d'informations entre les CSIRT nationaux, ainsi que de renforcer leurs capacités techniques et opérationnelles. L'atelier visait également à élaborer un document de projet qui sera soumis à la commission de la CEDEAO pour obtenir son aval et son financement.

Le CSIRT est le Computer Security Incident Response Team. Il est un élément clé dans la défense contre les attaques et les intrusions informatiques. En détectant, en analysant et en répondant aux incidents de sécurité, il contribue à maintenir la cybersphère sécurisée et résiliente. Au Togo, il s'agit du CERT.tg.

4.1.5.5. Le symposium pour l'avancement de la cybersécurité en Afrique de l'Ouest

Le symposium pour l'avancement de la cybersécurité en Afrique de l'Ouest, organisé par la CEDEAO en collaboration avec le projet OCWAR-C, qui s'est tenu à Abuja au Nigeria les 19 et 20 octobre 2023, a été une étape significative dans le renforcement des efforts régionaux en matière de cybersécurité. La réunion des experts des États membres de la CEDEAO lors de ce symposium a permis de dresser un bilan des activités menées par le projet OCWAR-C dans ces pays, offrant ainsi une vision globale des progrès réalisés et des défis rencontrés.

La centralisation des réflexions autour de la mise en place du Centre Régional de Coordination de la Cybersécurité a permis aussi de réfléchir à la coordination des efforts régionaux, favorisant l'échange d'informations, la mise en commun des ressources et la définition de stratégies communes pour renforcer la cybersécurité dans la région de l'Afrique de l'Ouest. En effet, la mise en place d'un Centre Régional de Coordination de la Cybersécurité pourrait être un élément clé pour assurer une réponse cohérente et efficace aux défis de la cybersécurité dans la région.

Photo de famille des participants

4.1.5.6. La Conférence mondiale sur le renforcement des capacités en matière de cybersécurité (GC3B)

Cette grande rencontre mondiale de la cybersécurité tenue à Accra au Ghana du 29 au 30 novembre 2023, revêt une grande importance dans le contexte mondial de la cybersécurité. En réunissant des décideurs, des praticiens et des experts, l'objectif de la conférence était de catalyser l'action mondiale en faveur de la cyber-résilience et du renforcement des capacités dans le cadre des programmes de développement international.

Les panélistes du GC3B

Les thèmes tels que la cyber-résilience et le renforcement des capacités qui y ont été développés s'inscrivent parfaitement dans le contexte du développement international, reconnaissant que la cybersécurité est devenue une composante essentielle de la stabilité et de la prospérité mondiale. Les discussions et les échanges lors de cette conférence ont permis de partager les meilleures pratiques, d'identifier les lacunes et de formuler des recommandations pour renforcer la sécurité numérique à l'échelle internationale.

4.1.6. Lutte contre la cybercriminalité au Togo

Les données statistiques de la lutte contre la cybercriminalité au titre de l'année 2023 révèlent que les cybercriminels ont ciblé une large palette de victimes, impactant aussi bien les particuliers que les entreprises et l'administration publique, avec des pertes financières considérables.

Selon les statistiques du Ministère de la Sécurité et de la Protection Civile, ces incidents surviennent presque quotidiennement et engendrent des pertes financières considérables. Pour l'année 2023, les pertes financières individuelles varient de 48 500 FCFA à plus de 900 millions FCFA. Le montant total de ces pertes financières attribuées à la cybercriminalité s'élève à plus de 1,5 milliards de francs CFA.

Au regard de l'ampleur du phénomène et de ses conséquences tant humaines que financières, il est essentiel de bien comprendre les différents types d'attaques menées et les méthodes employées par les cybercriminels, afin de mieux les contrer.

4.1.6.1. L'hameçonnage

L'hameçonnage ou phishing est une forme de cyberattaque qui consiste, pour des individus malveillants, à voler des informations sensibles telles que les noms d'utilisateur, les mots de passe et les coordonnées bancaires appartenant à des victimes non averties. Les hameçonneurs utilisent généralement de faux comptes de messagerie ou sites Internet d'apparence authentique pour inciter les victimes à communiquer des informations personnelles telles que des identifiants de connexion ou des informations bancaires. Ils peuvent également avoir recours à l'ingénierie sociale sous forme d'usurpation d'identité et d'attaques par logiciel malveillant pour accéder à des données confidentielles. Ce type d'attaque est une menace courante au Togo.

4.1.6.2. Les escroqueries en ligne et extorsion

Les arnaques en ligne, y compris les fausses boutiques en ligne et les escroqueries sentimentales, sont courantes et peuvent entraînent des pertes énormes pour les citoyens togolais. Les cybercriminels usent de l'ingénierie sociale pour atteindre leur but. Cette menace est exacerbée par le peu de maîtrise numérique des victimes, ce qui en fait des cibles faciles pour les cybercriminels qui les mettent en confiance avec de fausses promesses pour leur soutirer de l'argent.

4.1.6.3. Escroqueries aux faux ordres de virement

Les institutions togolaises, tant publiques que privées, sont vulnérables aux attaques. Les cybercriminels exploitent des failles dans les processus financiers pour détourner des fonds, causant des pertes financières significatives.

4.1.6.4. Les attaques par rançongiciels

Les attaques par rançongiciel qui consistent à cibler les personnes, les commerces et des organismes publics comme privés, se multiplient. Les rançongiciels sont une forme malveillante de logiciels qui bloquent l'accès des utilisateurs à leurs propres données, systèmes et appareils en cryptant leurs fichiers. Une fois le cryptage terminé, les victimes reçoivent un message les informant qu'elles doivent s'acquitter d'une certaine somme (souvent en bitcoin ou dans une autre cybermonnaie) pour que leurs fichiers soient décryptés et qu'elles puissent à nouveau y accéder. Elles paralysent des services et perturbent les opérations.

4.1.6.5. La cyber extorsion

La cyber extorsion consiste, pour un criminel, à utiliser des techniques numériques pour menacer des victimes ou leur extorquer de l'argent et/ou d'autres actifs. En règle générale, le cybercriminel menace de révéler des informations personnelles gênantes, de supprimer des données importantes, de saboter des systèmes et réseaux, ou encore de lancer une attaque par déni de service distribué (DDoS). La cyber extorsion progresse aussi avec la prolifération d'Internet et des technologies mobiles. Un nombre croissant de personnes reçoivent des demandes de rançon et se font extorquer.

4.1.6.6. Les chevaux de Troie bancaires et voleurs d'informations

Il s'agit de logiciels malveillants qui visent les informations financières des utilisateurs, entraînant des pertes directes pour les particuliers et les institutions financières togolaises. Ces attaques représentent une nouvelle menace imminente pour les acheteurs sur Internet et sapent la confiance dans les moyens de paiement en ligne.

Ces méthodes variées et sophistiquées, mettent en évidence l'ampleur de la cybercriminalité au Togo, nécessitent une réponse coordonnée et efficace, d'où notre engagement à redoubler d'efforts afin de renforcer les mesures de sécurité nationales visant à protéger la vie économique et sociétale.

C'est dans cette dynamique que l'Agence nationale de la cybersécurité (ANCy) conformément à ses missions, joue un rôle central dans la coordination des efforts de lutte contre la cybercriminalité au Togo. Elle offre des formations spécialisées et des campagnes de sensibilisation grand public, partage des renseignements et collabore avec la Justice, la Police et la Gendarmerie pour le démantèlement des réseaux et les poursuites contre les cybercriminels.

4.2. Les missions de l'ANCy opérées par CDA

4.2.1. Les missions principales de CDA

CDA en tant que bras opérationnel de l'ANCy, est chargé :

1. D'opérer le CERT national (CERT.tg) 24h/24 et 7j/7.

2. D'opérer le SOC national 24h/24 et 7j/7.

3. De la sensibilisation des usagers des équipements, des services et installations informatiques, de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information.

4. De la coordination de la riposte aux attaques informatiques.
5. Du support technique pour le compte de l'ANCy.

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

4.2.2. Les chiffres clés de 2023

4.2.2.1. Incidents traités sur l'année 2023

Figure 1 : Incidents traités

Sur l'année 2023, CDA a surveillé via son service SOC, des actifs du Gouvernement et de ses clients privés. Au total l**es systèmes ont analysé plusieurs Téraoctets de données** provenant des équipements réseaux, des systèmes et aussi des applications surveillées.

Ces données analysées ont évolué au fil des intégrations clients pendant toute l'année 2023.

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 66 703 incidents de cybersécurité (ou anomalies) au cours de l'année 2023. Cependant, il est à noter que ce chiffre porte également sur les faux positifs.

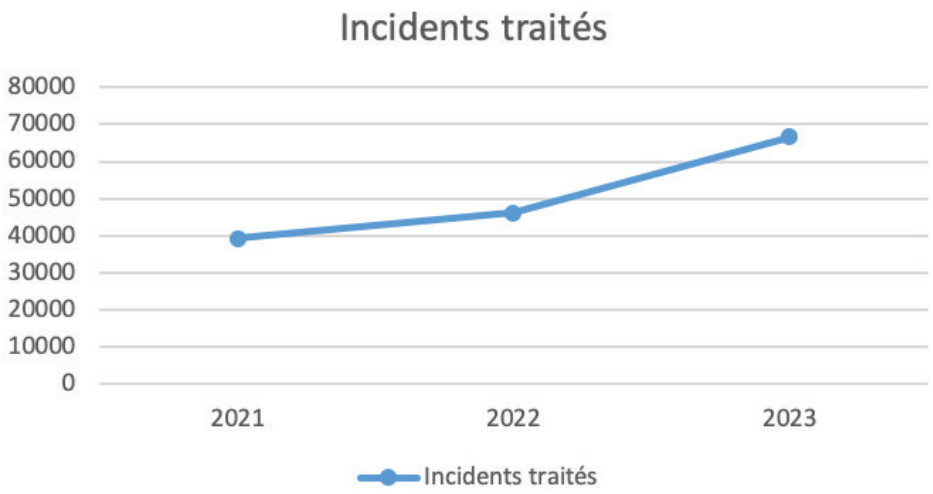
4.2.2.2. Evolution des données au cours de l'année 2023

Graphique 1 : Évolution des incidents traités en 2023

Concernant les incidents de cybersécurité, ils sont le résultat des règles de corrélations définies 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, au cours de l'année 2023, nous avons connu une augmentation des incidents en juin (du fait de la mise à jour d'une règle de corrélation) ainsi qu'une augmentation en octobre dû aux nouveaux clients SOC.

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

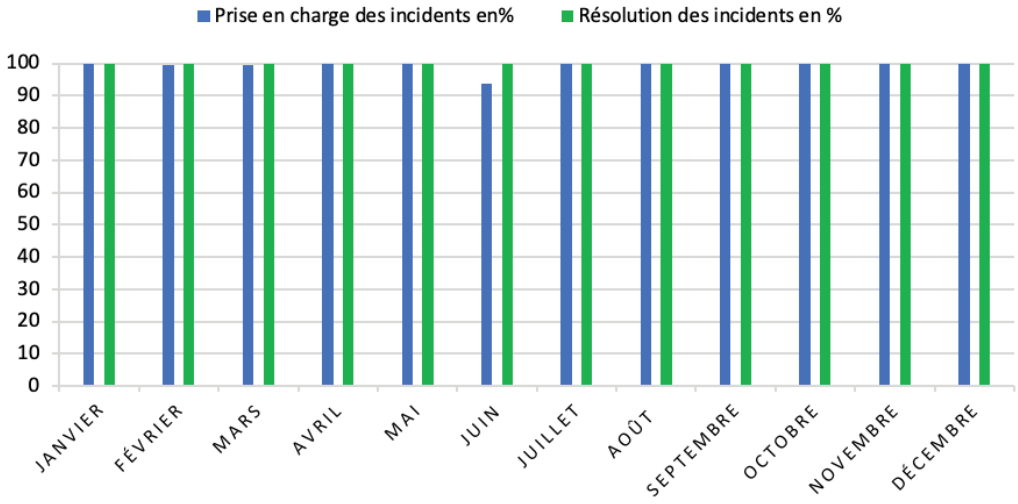
4.2.2.3.1. Incidents traités



Graphique 2 : Évolution des incidents traités depuis le démarrage du SOC

Le nombre d'incidents détectés augmente année après année du fait également du nombre croissant de clients SOC intégrés.

4.2.2.3.2. Respect des SLA



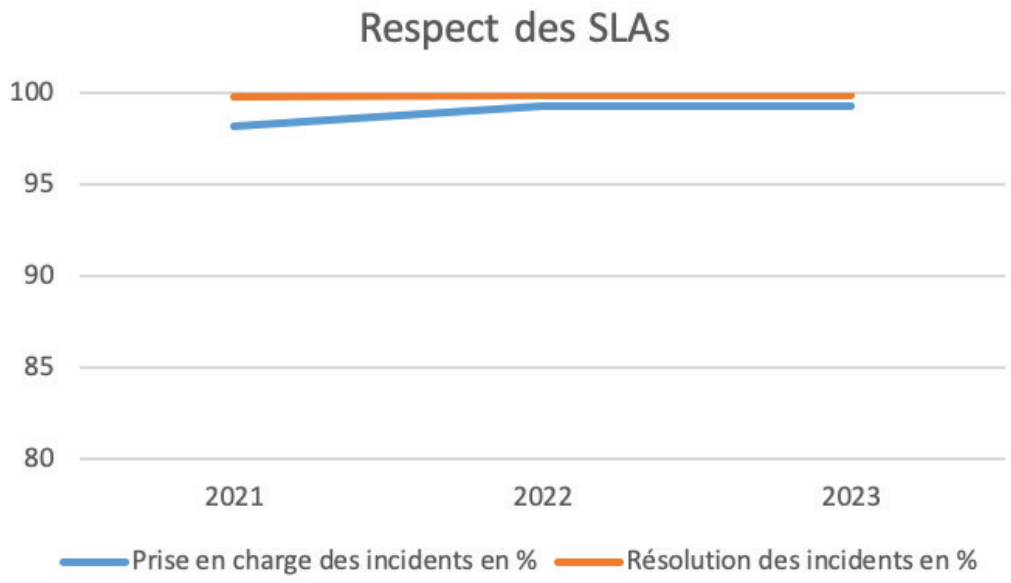
Graphique 3 : Niveau des SLA en 2023

CDA est tenu au respect des SLA 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 98,4 et 100% sauf en juin ou le pourcentage est tombé à 93.61% du fait d'une mise à jour technique.

Cependant, la moyenne de respect des SLA sur toute l'année 2023 pour **la prise en charge des incidents est de 99.3% 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 d'alertes sonores lorsqu'un incident survient et le recrutement de nouveaux analystes L1 qui se concentrent uniquement sur la gestion des incidents.



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

4.2.3. Activités SOC de 2023

4.2.3.1. Les clients SOC de CDA en 2023

Le SOC de CDA a participé à protéger les infrastructures informatiques des acteurs économiques publics et privés du Togo.

4.2.3.2. 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, l'Agence Nationale de la Cybersécurité (ANCy) a mandaté Cyber Defense Africa (CDA), en tant que prestataire qualifié, pour l'exécution des audits de conformité aux règles nationales de cybersécurité.

4.2.3.3. Partenariats SOC

4.2.3.3.1. EC-COUNCIL

EC-Council est le plus grand organisme de certification technique de cybersécurité au monde. Ses titres de certification sont reconnus dans le monde entier et valident qu'un professionnel de la sécurité de l'information possède les compétences et les connaissances requises dans un domaine spécialisé de la sécurité de l'information.

EC-Council délivre des formations qui sont devenus des références dans le domaine de la cybersécurité tels que le Certified Ethical Hacker (CEH), le Certified Network Defender (CND) ou le Computer Hacking Forensic Investigator (CHFI).

EC-Council

4.2.3.3.2. PECB

PECB est un organisme de formation qui offre des services de formation, de certification et des programmes de certificats aux personnes dans plusieurs disciplines. PECB aide les experts et les organisations à faire preuve d'engagement et de compétence en leur fournissant une formation, une évaluation, une certification et des programmes de certification conformément à des normes rigoureuses et reconnues internationalement.

PECB délivre notamment les formations ISO telles que ISO 27001.

PECB

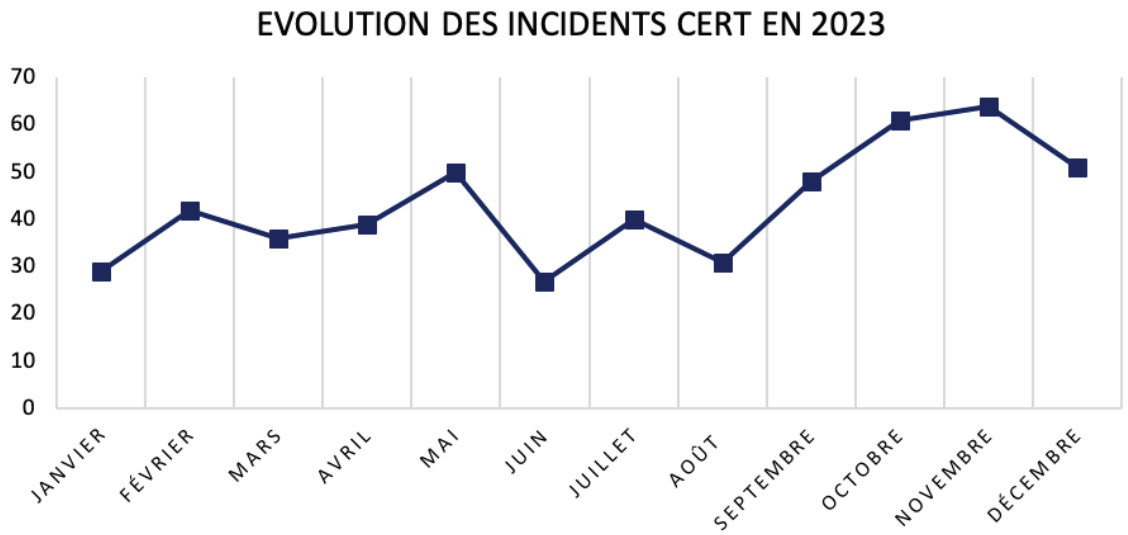
4.2.4. Activités CERT.tg en 2023

4.2.4.1. Traitement des Incidents CERT

4.2.4.1.1. Tableau des incidents traités

CDA a traité 518 incidents CERT au cours de l'année 2023 dont **218 vrais positifs.**

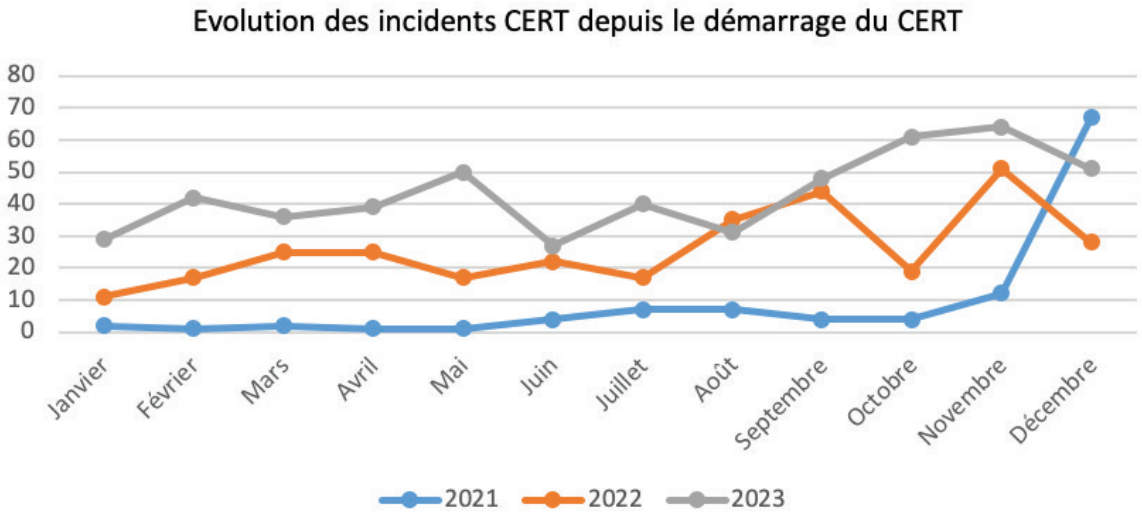
4.2.4.1.2. Évolution des incidents traités



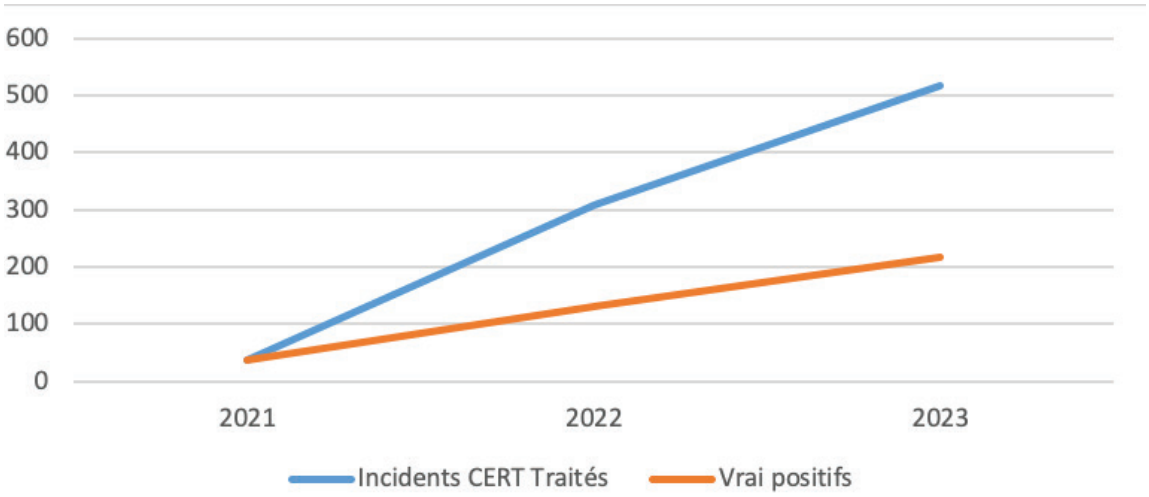
Graphique 5 : Évolution des incidents CERT

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.

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



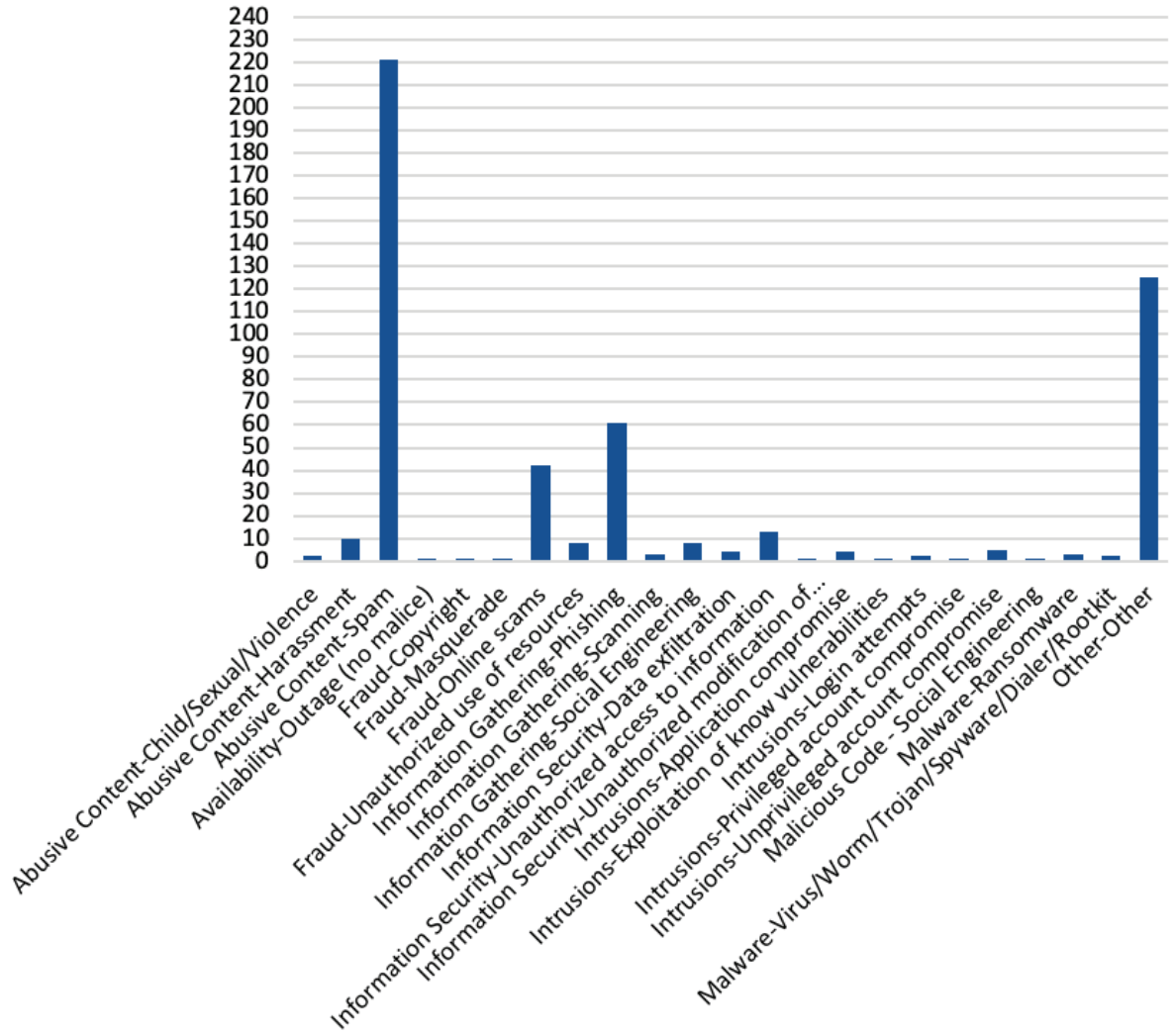
Graphique 6 : Évolution des incidents CERT par mois



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.

4.2.4.1.3. Répartition des incidents CERT traités en 2023



Graphique 8 : Répartition des incidents CERT traités

Les incidents les plus traités par le CERT.tg sont les campagnes de phishing, les fraudes en ligne et les spams tout comme en 2022 et en 2021. La tendance reste ainsi la même qu'en 2022 même si le nombre global des incidents a significativement augmenté.

4.2.4.2. Audit de sécurité pour les entités gouvernementales

En 2023, CDA a réalisé 18 audits d'applications web portées par le gouvernement, des audits de salles de serveurs et des audits complets de sécurité des entités gouvernementales.

4.2.4.3. Analyses de vulnérabilités des actifs du Gouvernement

Dans le cadre de ses activités CERT, CDA effectue des analyses mensuelles de vulnérabilités sur les noms de domaines actifs dans le domaine gouv.tg et sur toutes les adresses IP publiques gouvernementales. Il s'agit d'une initiative visant à anticiper la découverte d'éventuelles failles et vulnérabilités et surtout à les corriger.

Le rapport des résultats de l'analyse de vulnérabilités et des tests d'intrusion a été partagé avec les responsables concernés et l'ANCy. Des actions correctives indiquées dans les rapports doivent être menées par les propriétaires des domaines concernés pour corriger ces vulnérabilités détectées.

4.2.4.4. Analyses de vulnérabilités sur le .tg

CDA effectue régulièrement des analyses de vulnérabilités sur les noms de domaines actifs sur l'ensemble du .tg.

4.2.4.5. Alertes sur les vols d'identifiants (stealers)

CDA analyse quotidiennement les sites web, blogs, groupes, et autres plateformes à la recherche d'informations pouvant nuire à la sécurité du système d'information du gouvernement togolais ou des OSE.

CDA analyse quotidiennement les sites web, blogs, groupes, et autres plateformes à la recherche d'informations pouvant nuire à la sécurité des systèmes d'information au Togo.

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.

4.2.4.6. Surveillance des sites web

CDA a mis en place dans le cadre des activités CERT une surveillance de 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.

4.2.4.7. Participation à l'exercice régional de coopération inter-agences

La CEDEAO, en collaboration avec le Bureau du programme de lutte contre la cybercriminalité du Conseil de l'Europe, a organisé une rencontre régionale de coopération inter-agences entre les équipes de réponse aux incidents informatiques (CSIRT) et les services répressifs (LEA) en Ile Maurice, du 26 au 29 septembre 2023. L'exercice a mis l'accent sur la promotion de la synergie et de la coordination entre CSIRT et les services d'application de la loi de la région de la CEDEAO et d'Afrique, car les cybercrimes sont sans frontières. **Site web CERT.tg**

4.2.4.7.1. Site Internet CERT.tg en bref

Cette année, 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 des bulletins de sécurité, ainsi que par l'intégration d'un formulaire de signalement de domaines malveillants.

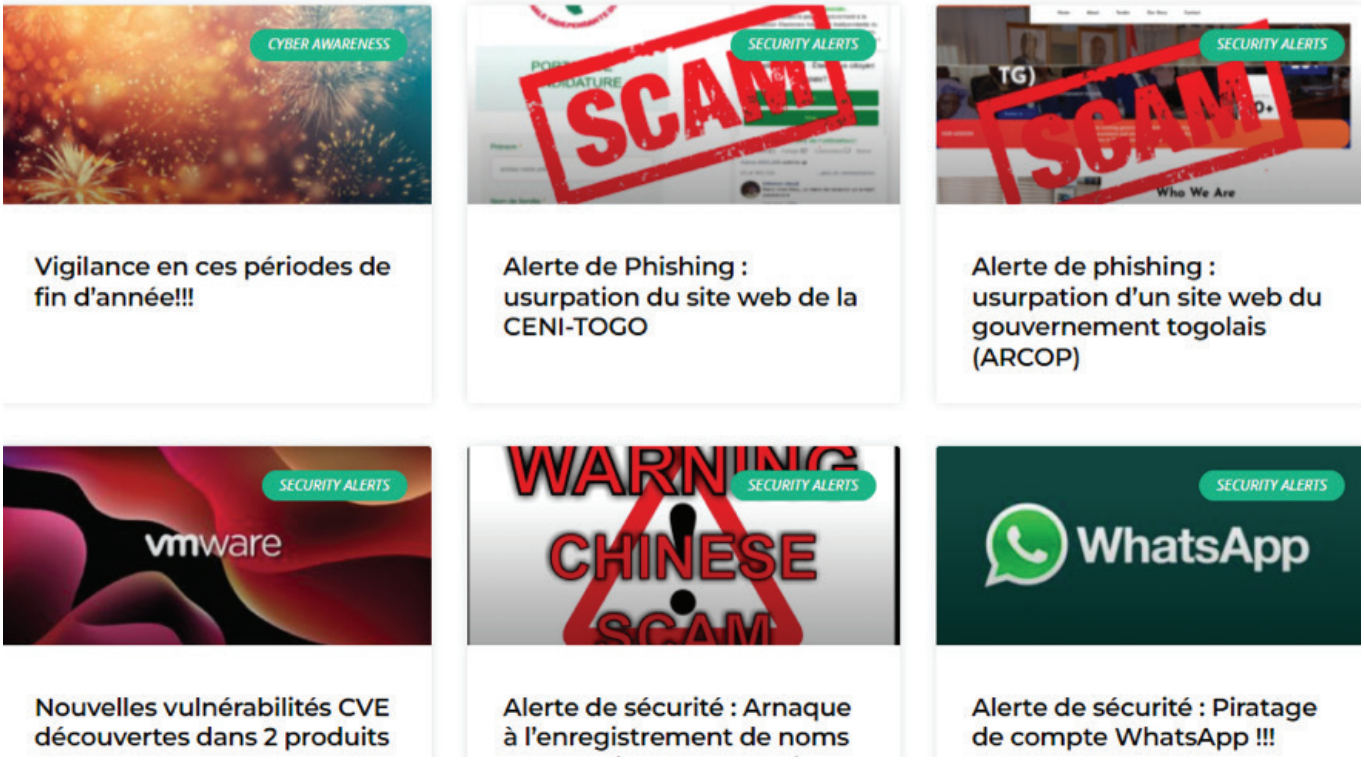


Figure 2 : Exemple de publication des bulletins de sécurité et de vulnérabilités

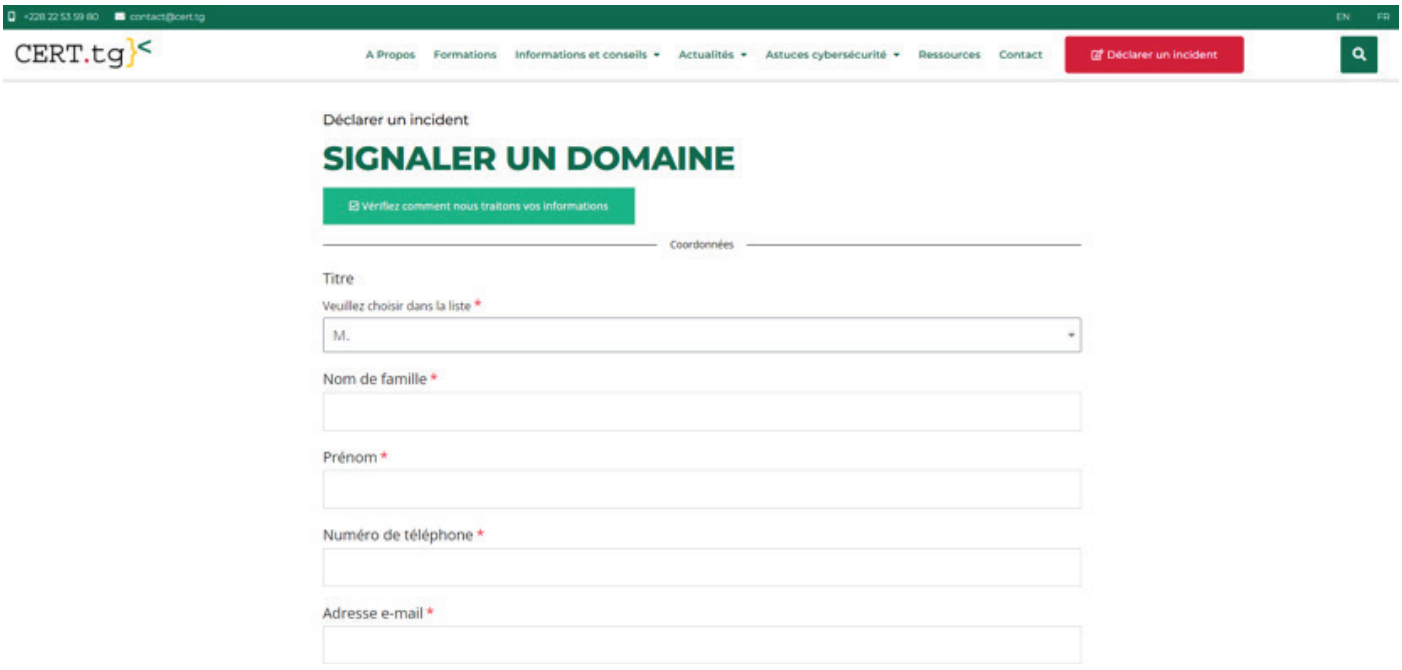
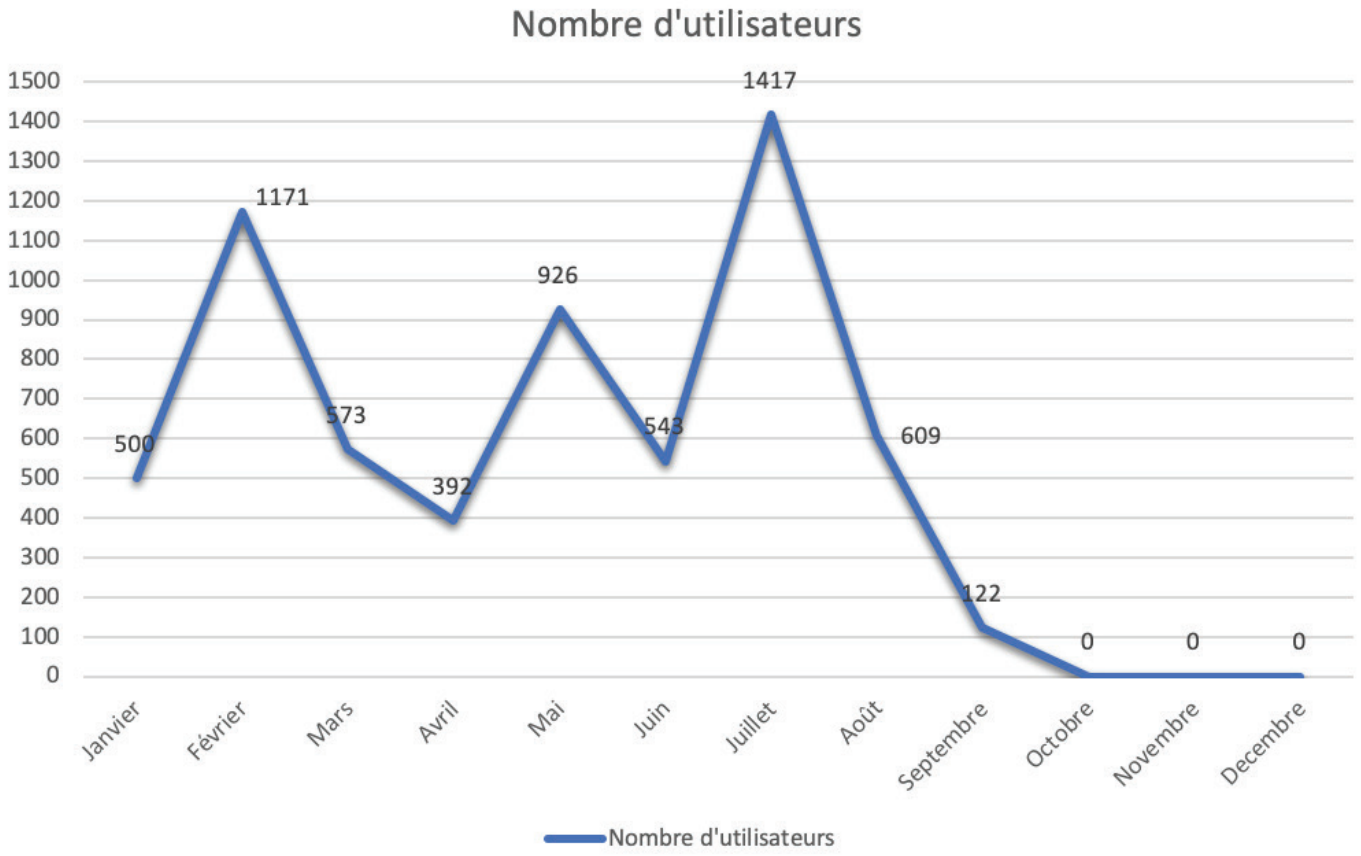


Figure 3 : Formulaire de signalement de domaine malveillants

4.2.4.7.2. Statistiques du site Internet CERT.tg en 2023



Graphique 9 : Statistiques du site Internet CERT.tg

Conformément au graphique présentant l'évolution des incidents traités par le CERT.tg, les données collectées grâce au plugin Google Analytics configuré sur le site montrent une fluctuation du nombre de visites au cours de l'année avec une augmentation en février, mai, juillet. La fréquence des visites sur la fin de l'année n'a pas pu être collectée à cause d'une panne sur la plateforme google Analytics (GA4).

4.2.4.8. Sensibilisations à la cybersécurité

Outre les sensibilisations faites conjointement avec l'ANCy, CDA a également tenu seul plusieurs séances multiformes de sensibilisation.

4.2.4.8.1. Sensibilisations en présentiel

L'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site web suspect, activation de virus ou autres menaces persistantes avancées).

Dans le but de réduire les incidents de sécurité et protéger les administrations, il est indispensable que les fonctionnaires, principaux acteurs de l'administration togolaise, soient sensibilisés et outillés pour faire face aux enjeux croissants 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, 20 sessions de sensibilisation pour un total de 1 821 participants ont été organisées** en 2023. Ce qui augmente le nombre total de ministères et administrations sensibilisés à 45 pour un total de 7377 participants à ce jour.

4.2.4.8.2. Sensibilisation sur les médias

CDA, dans le cadre de ses activités CERT et soucieux d'atteindre le plus grand nombre de la population pour une sensibilisation accrue à la cybersécurité, a animé des débats sur différents sujets de cybersécurité dans les émissions sur les radios Pyramide FM et Nana FM et la Télévision Togolaise.

Les principaux thèmes ci-dessous ont fait l'objet de sensibilisation dans ces émissions en 2023 :

- Débat sur le thème « **Vacances et usage du numérique : Avantages et risques pour les enfants** » dans l'émission Web Academy de GTT sur la radio Pyramide FM ;

- Débat sur le thème « **10 Règles de la cybersécurité** » dans l'émission Web Academy de GTT sur la radio Pyramide FM ;

- **Débat sur le thème « Vie Privée et Sécurité sur les réseaux sociaux : comment se protéger contre l'ingénierie sociale et les menaces** » dans l'émission Web Academy de GTT sur la radio Pyramide FM ;

- 1h de sensibilisation à la cybersécurité aux enfants et **aux jeunes avec SOS village Enfant** sur Pyramide Fm ;

- Débat sur le thème « **Accès sécurisé des enfants et jeunes aux numériques** » sur Nana FM ;

- Débat sur le thème « **Les wifi constituent-ils des vecteurs favorisant le cyber attaque ?** » sur Nana FM ;

- Débat sur le thème « **Sensibilisation sur l'hameçonnage (Phishing)** » dans l'émission Nektar sur la TVT.

https://actusalade.com/cybersecurite-sujet-coeur-discussion-sigma-corporation/

https://www.youtube.com/watch?v=8owc5zwDsDc

https://youtu.be/ve_M-1XG0IM

https://youtu.be/PhZryNITo1k

4.2.4.9. Formation des professionnels de justice

Le Centre International de Formation en Afrique des Avocats Francophones (CIFAF) a organisé en collaboration avec le Barreau du Togo et l'Organisation Internationale de la Francophonie (OIF), une session de formation sur le droit numérique et la protection des données à caractère personnel.

Le 11 et le 12 octobre 2023, CDA a ainsi eu l'opportunité de former les avocats présents sur les thèmes suivants :

- La cybersécurité (rôle de l'avocat)
- La cybercriminalité (rôle de l'avocat).

4.2.4.10. Participation à des événements et ateliers

4.2.4.10.1. Workshop on Cybersecurity Assurance Practices (ITU)

Le 23 mai 2023, le Directeur Technique de CDA a présenté le modèle togolais de partenariat public privé pour la cybersécurité nationale à l'atelier de travail sur les pratiques d'assurances de la cybersécurité (Workshop on Cybersecurity Assurance Practices) organisé par l'ITU.

Cet atelier visait à explorer le paysage mondial de l'assurance de la cybersécurité en présentant un éventail de pratiques et de voix en cours à travers le monde. À travers quatre tables rondes, l'atelier a approfondi la signification et la portée des pratiques d'assurance de la cybersécurité, leur mise en œuvre et la manière dont elles peuvent être adoptées et reconnues à l'échelle mondiale.

L'atelier a exploré la définition des pratiques d'assurance de la cybersécurité, fournissant un aperçu du paysage actuel de ces pratiques dans divers domaines, et présenté des études de cas de différents pays, mettant en évidence les défis rencontrés, l'impact réalisé et les leçons apprises, avant de poser la question cruciale de savoir comment ces pratiques peuvent être partagées à l'échelle internationale.

Au cours de ce panel, le Directeur technique de CDA était entouré de Mr Majed A. Alresaini, (National Cybersecurity Authority, Saudi Arabia), Ms Amy Mahn (National Institute of Standards and Technology, United States), Mr Thiago Barcante Teixeira (Anatel, Brazil).

https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/meetings/session-Q3-2-may23.aspx

4.2.4.10.2. Première édition du grand atelier du digital

CDA a participé au Grand Atelier du Digital qui s'est tenu à l'Hôtel Sarakawa du 10 au 12 Mai 2023 en présentant à l'écosystème digital togolaise, la partie opérationnelle de la cybersécurité nationale. En effet cet atelier avait pour objectif de présenter aux acteurs du digital les grands principes du gouvernement en matière de digital et d'établir un cadre d'échange avec les administrations, le secteur privé, la société civile, les partenaires techniques et financiers du Togo.

Thème de la présentation de CDA

4.2.4.10.3. Her CyberTracks

Her CyberTracks est un programme financé par le ministère fédéral allemand des Affaires étrangères et mis en œuvre conjointement par l'UIT et la GIZ. Ce programme a pour objectif de promouvoir la participation égale, pleine et significative des femmes à la cybersécurité pour un cyberespace plus résilient pour tous. Her CyberTracks propose des activités ciblées de renforcement des capacités en matière de cybersécurité pour les femmes impliquées dans les processus et négociations politiques nationaux et internationaux en matière de cybersécurité en Afrique de l'Ouest, dans les Balkans occidentaux et en Europe de l'Est.

Visuel de promotion du Her CyberTracks

Les participants du Her CyberTracks

4.2.4.10.4. CyberTech Africa

Cybertech Global Events, en collaboration avec l'Autorité nationale rwandaise de cybersécurité, le Rwanda Convention Bureau et le Secrétariat Smart Africa, ont coorganisé le tout premier Cybertech Africa le 1er et 2 août 2023, au centre des congrès de Kigali (Rwanda).

A cette occasion, le Directeur Technique de CDA a eu l'opportunité de présenter en plénière le modèle togolais pour une cybersécurité effective aux côtés du Dr Albert Antwi-Boasiaki (Directeur Général de l'autorité de cybersécurité du Ghana, Emmanuel Rosenblit (Directeur du centre d'engagement professionnel au CERT-IL, Israël), et Atine John Bosco (Directeur des systèmes d'information à l'OACPS, Belgique). Le panel était modéré par David Kanamugire (Directeur Général de l'autorité de cybersécurité, Rwanda).

Les panélistes du CyberTech Africa

4.2.4.10.5. Workshop sur la cyberdiplomatie

La CEDAO a organisé à Lomé une formation sur la cyberdiplomatie les 14 et 15 novembre 2023. Cette formation visait à développer une compréhension initiale de la cybersécurité et de la cyberdiplomatie au sein d'un groupe de diplomates, créant ainsi un pool de base de fonctionnaires pouvant aider les pays à poursuivre les efforts de la CEDEAO pour résoudre les problèmes cybernétiques et numériques. La formation a rassemblé une trentaine de représentants des ministères des Affaires étrangères des États membres de la CEDEAO, ainsi que plusieurs responsables de la CEDEAO.

Le Directeur Technique de CDA a ainsi pu présenter aux diplomates les mécanismes possibles pour la mise en œuvre d'un Framework national de cybersécurité.

4.2.4.11. Partenariats CERT

CDA a également continué cette année à entretenir ses partenariats avec des entités africaines et internationales, notamment AfricaCERT, Trusted Introducer (TF-CSIRT), Shadowserver Foundation, Computer Incident Response Center Luxembourg (CIRCL), FIRST, TrustedBorker Africa et NatCSIRT.

En 2023, le CERT national a participé au programme Cyber For Good de l'UIT.

Cyber for Good est un projet de l'UIT qui vise à combler le déficit de capacités en matière de cybersécurité dans les pays les moins avancés (PMA) en facilitant le soutien et l'accès à l'expérience, à l'expertise, aux services, aux outils et aux produits des membres de l'UIT.

Dans ce cadre, le CERT National a bénéficié de la solution BITSIGHT et IMMUNIWEB pour une utilisation gratuite pendant une année.

4.2.4.12. 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 l'ANCy et CDA depuis octobre 2022, font 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.

4.2.5. 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 2 : Liste des références de CDA

5_ LES DIFFICULTÉS RENCONTRÉES

Dans la mise en œuvre de ses activités, l'ANCy a été confrontée à certaines difficultés au nombre desquelles on peut citer principalement :

5.1. Les difficultés des administrations à financer la mise en place des dispositifs de cybersécurité nécessaires à leur protection

La question de la cybersécurité étant nouvelle pour nombre d'administrations, il n'existe pas souvent de ligne budgétaire qui y est consacrée. Cependant, les difficultés de financement des dispositifs de cybersécurité augmentent la vulnérabilité de ces administrations publiques comme privées. Sans les infrastructures nécessaires, ces administrations deviennent des cibles plus faciles pour les cyberattaques, ce qui peut entraîner des pertes de données sensibles et des perturbations importantes dans leurs services. De plus, il est à noter que l'absence de financement adéquat freine l'innovation technologique.

5.2. Le faible engagement de certains Opérateurs de Services Essentiels (OSE) à répondre promptement aux obligations issues de leur statut

Le statut des OSE les oblige à respecter des normes de cybersécurité strictes pour protéger leurs infrastructures contre les cyberattaques. En retardant la mise en œuvre des mesures de cybersécurité requises, ces OSE exposent leurs systèmes à un risque élevé de cyberattaques.

6– LES PERSPECTIVES POUR 2024

6.1. Démarrage de l'opérationnalisation de la Stratégie nationale de cybersécurité

L'année 2024 coïncide avec le démarrage de l'opérationnalisation de la Stratégie nationale de cybersécurité. Plusieurs activités sont prévues, notamment :

- L'élaboration et la révision des manuels de formation relatifs à la promotion de la cybersécurité dans les enseignements primaire et secondaire ;

- L'élaboration et la révision des modules de sensibilisation et de formation relatifs à la promotion de la cybersécurité dans l'enseignement supérieur ;

- L'organisation des séances de sensibilisation sur la cybersécurité ;

- L'organisation des compétitions de cybersécurité (hackathon, CTF) pour la détection de talents ;

- La qualification des prestataires de service de confiance élaborés par l'ANCy ;

- La participation à des échanges internationaux d'expériences en matière de cybersécurité.

6.2. Sensibilisation et formation en cybersécurité

- Sensibilisation et formation relatives à la promotion de la cybersécurité dans l'enseignement supérieur.
- Réalisation d'une étude annuelle sur l'état de la cybersécurité et de la lutte contre la cybercriminalité au Togo.
- Tournée nationale de sensibilisation aux enjeux de la cybersécurité 2024.
- Fournir une plateforme informative, éducative et interactive visant à sensibiliser les enfants aux risques numériques.

6.3. Renforcement des capacités

- Organisation de compétitions de cybersécurité pour la détection de talents.
- Renforcement des capacités techniques des personnels essentiels des administrations.
- Renforcement des capacités du personnel.

6.4. Gestion et opérationnalisation

- Opérationnalisation des services de qualification des prestataires de services de confiance, des produits en sécurité et d'agrément des centres d'évaluation.
- Élaboration d'un plan de suivi-évaluation de la stratégie.
- Poursuite des audits de conformité des OSE.

6.5. Collaboration et coordination

- Élaboration et mise en œuvre d'un programme incitatif pour l'attraction des Togolais de la diaspora, experts dans la cybersécurité.
-
- Organisation des exercices nationaux d'alerte et de gestion des incidents d'envergure nationale de cybersécurité.
- Renforcement de la collaboration avec les forces de sécurité et la justice pour une lutte efficace contre les crimes et délits de cybersécurité.
- Réunir une fois par trimestre les OSE pour faire l'état des lieux et les informer sur l'actualité de la cybersécurité.

6.6. Stratégie et analyse

- Mise en place au Togo des activités OSINT (Open Source Intelligence).
- Cafés de la cybersécurité avec les OSE.

6.7. Mise en place d'un environnement de recherche approprié

- Mise en place au Togo des activités OSINT (Open Source Intelligence).
- Cafés de la cybersécurité avec les OSE.

CONCLUSION

Dans le contexte togolais, la cybersécurité revêt une importance capitale pour les entreprises, les organismes gouvernementaux et les citoyens. Les cybermenaces sont mieux élaborées, nécessitant des mesures de sécurité toujours plus promptes, rigoureuses et systématiques. C'est dans ce cadre que l'Agence nationale de la cybersécurité (ANCy) inscrit son rôle.

Afin de faire face à ces défis croissants, l'ANCy s'engage non seulement à mettre en place des stratégies de défense robustes et à jour, mais aussi à sensibiliser et à former les différents acteurs du cyberespace togolais.

L'ANCy continuera à travailler en étroite collaboration avec les autorités nationales et les partenaires locaux et internationaux pour renforcer la sécurité du cyberespace togolais. Son engagement indéfectible à garantir la protection des citoyens et des infrastructures numériques constitue un pilier essentiel dans la préservation de l'héritage commun et dans l'assurance d'un avenir numérique sûr pour tous.

TABLES DES MATIERES

RÉPUBLIQUE TOGOLAISE

Ministère de l'Économie Numérique
et de la Transformation Digitale

ANCy
Agence Nationale
de la Cybersécurité

RAPPORT D'ACTIVITES **2023**

RÉPUBLIQUE TOGOLAISE

ANCy
Agence Nationale de la Cybersécurité

Rapport d'Activités 2023

Agence Nationale de la Cybersécurité (ANCy)

Adresse : 63 Bd du 13 Janvier,
Nyékonakpoè, Lomé-TOGO
07 BP 7878
+228 97 52 58 58
+228 70 60 60 83

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