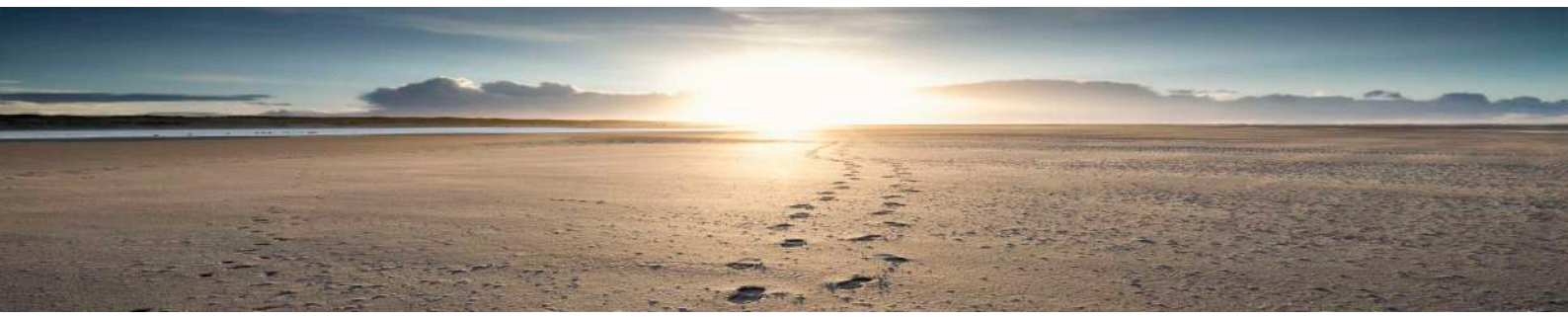
CESIA

CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE

BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE

ÉDITION 2021

Sommaire



BUREAU DU CESIA

*Créé en janvier 2020, le **CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE (CESIA)** est un espace d'échange et de partage exclusivement réservé aux Directeurs des Systèmes d'Information (**DSI**), aux Directeurs de la Sécurité des Systèmes d'Information (**DSSI**) et aux Responsables de la Sécurité des Systèmes d'Information (**RSSI**) exerçant dans les secteurs privés ou publics. Le bureau actuel est constitué des membres suivants :*

Didier SIMBA - Gabon

Fondateur et Président du CESIA.
Responsable de Sécurité des Systèmes d'Information (RSSI) au sein du Groupe BPCE.

Mame DIOP BA - Côte-d'Ivoire

Vice - Président du CESIA.
Deputy Director of IT and Information Security - ORANGE Côte-d'Ivoire

Élisée Trésor SIMA - Gabon

Trésorier du CESIA.
Consultant Senior Cybersécurité Managing - Capgemini

Eyram SEBA - Togo

Administrateur au CESIA.
Responsable de Sécurité des Systèmes d'Information (RSSI) - CEET

Yann OBELEMBIA - Gabon

Administrateur au CESIA.
Chief Information Officer - ECOBANK Gabon

Laïka MBA - Gabon

Administrateur au CESIA.
Directrice Générale - ST DIGITAL Gabon

Gilles CHOULA - Cameroun

Administrateur au CESIA.
Responsable de Sécurité des Systèmes d'Information (RSSI) - GROWTH CONTINUE Consulting

ÉDITORIAL

Cette première édition du baromètre de la cybersécurité en Afrique a été réalisée durant le mois de janvier 2021 directement auprès des membres du CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE (CESIA).

En pleine période de crise sanitaire liée au COVID-19 entrainant la généralisation du télétravail, les experts sécurité dans les entreprises africaines doivent relever de nombreux défis. Comment être certain que le salarié en télétravail est bien celui qui est assis devant le PC de l'entreprise quand les SAS de contrôle d'accès physique de l'entreprise ne sont plus là ? Comment maintenir un niveau de sécurité satisfaisant du poste de travail quand celui-ci est en dehors des locaux et surtout lorsqu'il n'est pas connecté en permanence au réseau de l'entreprise ? Comment empêcher les utilisateurs de céder au Shadow IT en mode système D quand tous les outils collaboratifs ne sont pas encore là ou que ceux qui sont proposés ont une ergonomie perfectible ? Comment empêcher les fuites de données lorsque les utilisateurs sont livrés à eux-mêmes avec des outils collaboratifs déployés à la va-vite sans avoir pris le temps de les former à ces solutions très riches mais souvent très complexes à utiliser ? Comment trouver la parade à des milliers d'attaques via des tentatives de phishing véhiculant des messages d'aubaine sur des offres des abonnements de vidéo streaming pour les salariés confinés et en manque de distraction ? Comment maintenir le niveau de sensibilisation des collaborateurs aux risques SI à distance ?

Toutes ces questions et bien d'autres encore, font l'objet de préoccupations des experts de la sécurité et le constat est sans appel, moins de 10% des collaborateurs ont été en télétravail. Les entreprises africaines sont mal préparées en matière de cybersécurité : une gouvernance cyber perfectible, un manque de budget, un manque de ressources et des compétences dédiées à la cybersécurité, etc sont autant de points qui ralentissent la mise en place d'un réel programme cyber en entreprise.

« Il n'existe pas de sécurité absolue, mais les DSI et les RSSI des entreprises africaines doivent avoir une sécurité juste au niveau »

 # Didier SIMBA - Président du CESIA

MÉTHODOLOGIE DU SONDAGE

Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des grandes entreprises en Afrique, le Club d'Experts de la Sécurité de l'Information en Afrique (CESIA) publie la première édition de son baromètre annuel après une phase pilote l'année dernière menée sur 4 pays. Cette année, **le sondage a été réalisé sur les 18 pays Africains dans lesquels sont répartis ses 120 membres**. Les résultats de l'étude portent sur un échantillon de 76 répondants soit 63%. Ils mettent à jour la réalité concrète de la Cybersécurité sur le continent et constituent des chiffres aussi révélateurs qu'alarmants.

L'association dévoile aujourd'hui les résultats de cette enquête indépendante réalisée entre le 1er et le 24 janvier 2021 exclusive menée auprès de ses membres : Directeurs des Systèmes d'Information (**DSI**), Directeurs de la Sécurité des Systèmes d'Information (**DSSI**) ou Responsables de la Sécurité des Systèmes d'Information (**RSSI**) de grandes entreprises en Afrique.

---

*Le **CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE (CESIA)** est un espace d'échange et de partage de connaissances et d'expériences avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique en Afrique.*

LES 4 MESSAGES CLÉS

LES ENTREPRISES AFRICAINES SE PROTÈGENT

- **52%** des entreprises africaines se disent assez confiantes en leur capacité à faire face aux cyber-risques,
- **55%** d'entre elles pensent ne pas être préparées à faire face à une cyber attaque de grande ampleur. Elles se protègent donc avec en moyenne, 18 solutions dont seulement 31% de solutions innovantes issues des start-up (69% n'ont pas recours aux solutions innovantes jugées comme peu matures pour 37% des participants.)
- **70%** des entreprises conscientes des risques cyber, mettent en place un programme de cyber-résilience ou sont en cours de déploiement de ces programmes. Par ailleurs, 30% des entreprises n'ont pas mis en place des programmes de Cyber-résilience ou ne projettent même pas de le faire et elles n'auraient pas recours au cyber-assurance (67% des entreprises).
- **82%** des entreprises disent avoir subi en 2020, moins de 3 attaques avec un impact négligeable. Parmi les grands types d'attaques subies notons : Phishing/spear-phishing (69%), les tentatives de connexion (44%) et l'ingénierie sociale (29%).

LA SENSIBILISATION DES COLLABORATEURS

D'après les DSI et les RSSI, les entreprises gagneraient à mieux sensibiliser les collaborateurs.

- **72%** des entreprises disent sensibiliser leurs collaborateurs,
- **41%** d'entre elles disent avoir mis en place un processus pour tester l'application des recommandations par les salariés et 54% disposent d'un plan annuel de sensibilisation.

Les experts de la cybersécurité, relèvent que les usages numériques des salariés présentent les risques suivants : l'utilisation des Devices personnels (46%), le travail à distance (23%) et Shadow IT (16%).

L'IMPACT DU COVID-19

L'année 2020 est marquée par la crise sanitaire liée au COVID-19, pour les entreprises africaines, moins de 10% de collaborateurs ont été en télétravail

- **58%** des entreprises n'étaient pas préparées à déployer un dispositif de travail à distance et ce n'est toujours pas un sujet pour 43% d'entre elles.
- **19%** des entreprises ne disposent pas de cellule de crise, celles qui en disposent l'ont déclenchée au moins une fois en 2020.

D'après les RSSI et les DSI, le télétravail présente des risques :

- Maintenir un niveau de sécurité satisfaisant du poste de travail quand celui-ci est en dehors des locaux et surtout lorsqu'il n'est pas connecté en permanence au réseau de l'entreprise (85%),
- Empêcher les fuites de données lorsque les utilisateurs sont livrés à eux-mêmes avec des outils collaboratifs riches et complexes à utiliser (66%) déployés à la va-vite sans avoir pris le temps de les former,
- Maintenir le niveau de sensibilisation des collaborateurs aux risques SI à distance (50%).

L'IA ET LE CLOUD EN AFRIQUE

- **71%** des entreprises utilisent le cloud pour stocker une partie de leurs données,
- **41%** utilisent déjà le cloud public. Cet outil de stockage pose cependant des risques, les plus forts étant l'indisponibilité du réseau Internet (64%), la confidentialité des données vis-à-vis de l'hébergeur (47%) et la difficulté de mener des audits (pentest, contrôle des configurations, visite sur site…) (39%),
- **56%** des entreprises sont disposées à utiliser des solutions qui présentent de la technologie Intelligence Artificielle.

LES 4 ACTIONS PRIORITAIRES À COURT/MOYEN TERME

CARTOGRAPHIER LES RISQUES INHÉRENTS À SON ACTIVITÉ ET SON PÉRIMÈTRE

La maitrise des risques passe par son identification, sa cotation, son impact à la fois sur les actifs métiers de l'entreprise mais aussi les actifs supports. L'analyse devrait porter sur l'impact **DICP** (Disponibilité - Intégrité - Confidentialité - Preuve) mais aussi sur l'**IFOJR** (Image - Financier - Organisationnel - Juridique - Réglementaire). Le tout centralisé dans un seul tableau de bord à destination du top management.

Pour ce faire, chaque entreprise doit désigner un Responsable de Sécurité des Systèmes d'Information (RSSI) indépendant avec une fiche de poste claire précisant ses missions et un plan de formation adéquat.

SENSIBILISER ET FORMER LES UTILISATEURS

70% des attaques sont de type phishing (hameçonnage) à destination des utilisateurs. Par ailleurs, les DSI et RSSI sont unanimes, ils considèrent le facteur humain comme étant le plus gros risque en entreprise. La maitrise de ce risque passe par la mise en place et le déploiement d'une vraie culture cyber en entreprise, pour ce faire, la sensibilisation devrait être pyramidale, le top management (Direction Générale, Conseil d'Administration) devrait en premier lieu se sentir concerné. Puis vient la formation à tous les niveaux : les utilisateurs du SI, les développeurs, les administrateurs réseaux/système, les gestionnaires des bases de données, les fonctions cadres (directeurs métiers, RSSI, RH, etc.)

METTRE EN ŒUVRE UN COMITÉ DE PILOTAGE DE LA SSI

Le top management doit être au cœur des décisions cyber. Aussi, les entreprises doivent mettre en place un comité présidé par la plus haute instance de l'entreprise qui valide les décisions et stratégies de sécurité. Ce comité doit à minima voir la participation de la plus haute instance de l'entreprise, du directeur des systèmes d'information, du responsable sécurité et de l'ensemble des directeurs métiers.

Le comité a pour mission de définir, valider et réévaluer au moins une fois dans l'année la Politique de Sécurité des Systèmes d'Information (PSSI) et de suivre sa mise en œuvre.

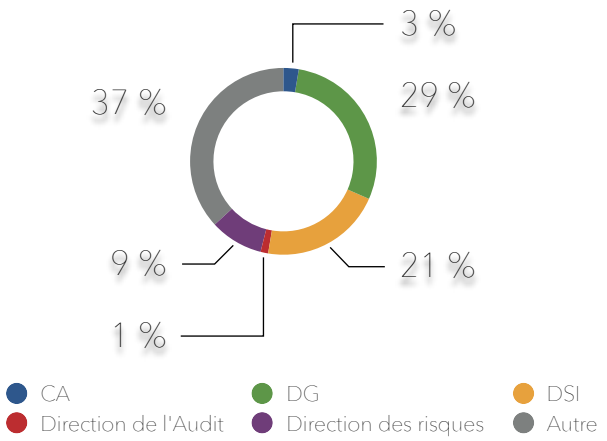
PROMOUVOIR L'AMÉLIORATION CONTINUE BASÉE SUR LA STRATÉGIE NATIONALE EN VIGUEUR DANS LE PAYS.

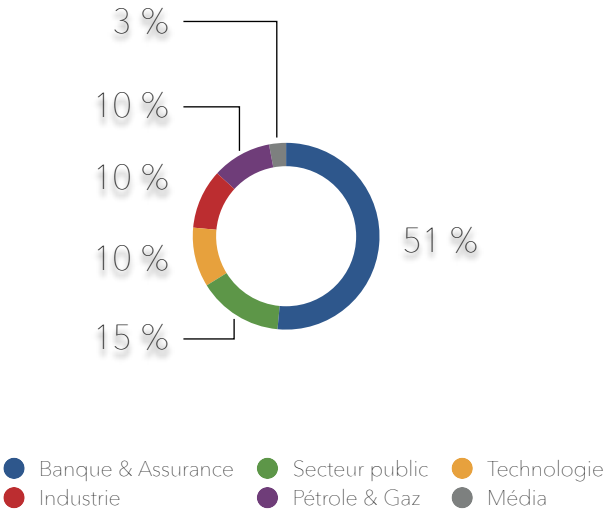
L'amélioration continue permet d'assurer un niveau de sécurité aligné sur les objectifs de l'entreprise.

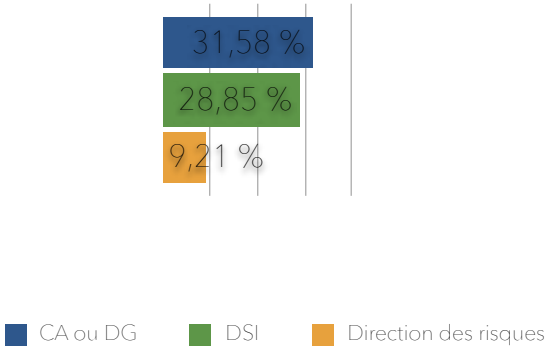
La cybersécurité étant un sujet central en Afrique, les pays africains dotés d'un cadre légal définit par le gouvernement doivent s'y conformer et assurer un maintien du niveau de conformité. Cela passe par la mise en place d'un dispositif de veille, d'alerte et de correction des vulnérabilités en temps réel.

ANALYSE DES RÉSULTATS

ORGANISATION DE LA SÉCURITÉ SI DANS LES ENTREPRISES







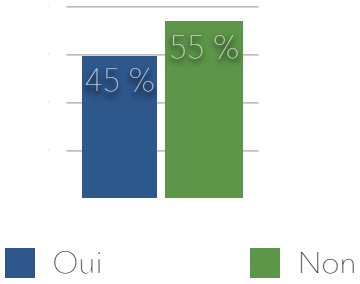
42% des RSSI sont désormais rattachés à une haute hiérarchie de l'entreprise ou à des entités de contrôles. (3% au Conseil d'Administration, 29% à la Direction Générale, 1% à la Direction de l'Audit interne et 9% à la direction des risques). Les entreprises africaines envoient de bons signaux qui tendraient de plus en plus à mettre leurs RSSI à une position organisationnelle réellement indépendante.

54% des participants à cette étude sont des RSSI et 25% des DSI. Les 25% restant sont experts cybersécurité après une très longue expérience en tant que RSSI ou DSI.

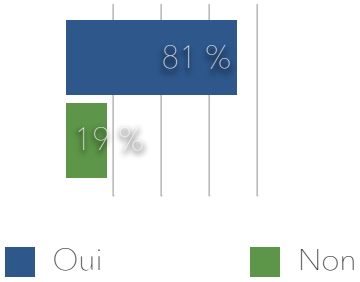
Les entreprises Africaines sont de plus en plus conscientes des enjeux de la cybersécurité et des risques auxquels elles sont exposées. Pour environ 50% des entreprises, la cybersécurité est bien une priorité. Toutefois, pour 43% des entreprises, ça reste un sujet moyennement abordé, les budgets et les compétences dans les équipes sont jugés insuffisants et même le suivi d'action est perfectible. Pour une minorité, environ 8% des entreprises, la cybersécurité n'est pas du tout un sujet.

Le positionnement hiérarchique du RSSI dépend généralement de la taille et de la maturité de l'entreprise. S'il ne devrait pas être intégré à la DSI, le RSSI doit pour autant collaborer de manière très étroite avec elle. Parce qu'elle a la main mise sur le SI, il doit régner une relation de confiance entre les 2 entités pour qu'une coordination efficiente puisse être instaurée.

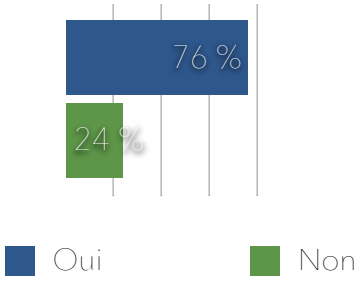
DES ENTREPRISES QUI SE PROTÈGENT DE PLUS EN PLUS



Selon vous, votre entreprises est-elle préparée à gérer une crise de grande ampleur ?



Avez-vous une PSSI dans votre entreprise et révisée au moins une fois par an ?



Afin de suivre et maitriser vos risques SI, disposez-vous d'une cartographie des risques SI dans votre entreprise ?

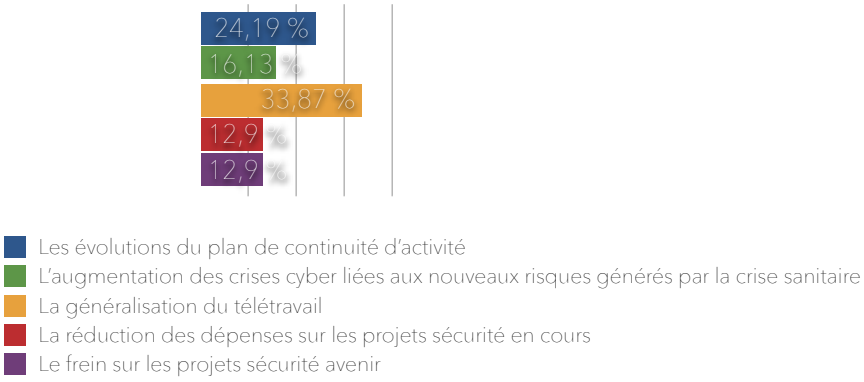
Pour se protéger, les entreprises ont recours à environ 18 solutions de sécurité. Toutefois, la majorité (55%) pensent ne pas être préparée à gérer une cyber-attaque de grande ampleur. D'ailleurs, 29% des entreprises ont mis en place un programme de cyber-résilience, la très large majorité des entreprises en Afrique (71%) n'en dispose pas ou sont en cours de mise en place.

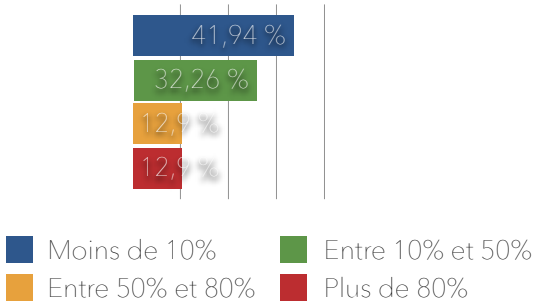
La majorité des entreprises ne souscrivent pas aux cyber assurances (67% des entreprises n'en ont pas souscrit).

Le manque de maturité ou de pérennité des offres conduit les RSSI à ne pas faire recours aux solutions innovantes (69% des entreprises n'ont pas recours aux solutions innovantes). Ils considèrent la prise de risque trop importante.

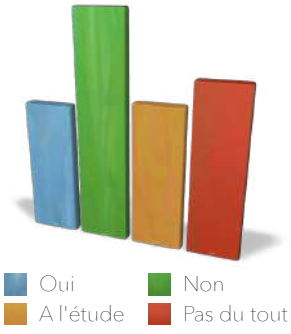
Pour se protéger, le RSSI disposent des outils clés 76% d'entre eux disposent bien d'une cartographie des risques SI et 81% ont mis en place une Politique de Sécurité des Systèmes d'Information (PSSI).

COVID-19 : UNE CRISE CYBER DANS LA CRISE SANITAIRE





Quel % de vos collaborateurs ont été en télétravail ?



Le télétravail est-il désormais une norme dans votre entreprise ?

La crise sanitaire liée au COVID-19 a marquée l'année 2020 en Afrique, elle a permis de tester la cellule de crise qui a été déclenchée au moins une fois.

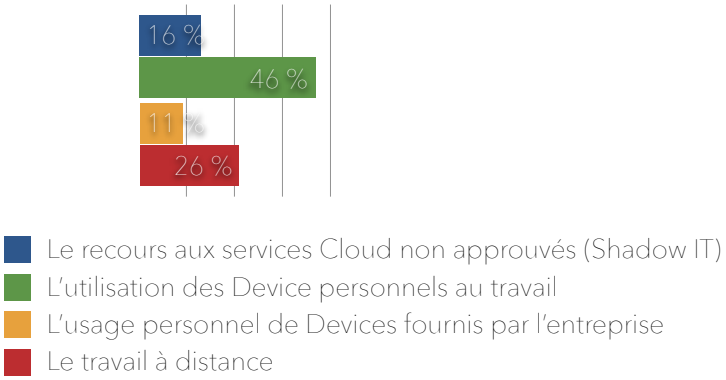
Cette crise a aussi comme impact la généralisation du télétravail (34%), les évolutions du plan de continuité d'activité (24%) et une augmentation des crises cyber liées aux nouveaux risques générés par la crise sanitaire (16%).

Environ 60% des entreprises n'étaient pas préparées au télétravail et ce n'est pas toujours une norme dans les entreprises.

82% des entreprises disent avoir subi au moins 3 cyber attaques, avec un impact négligeable dans la grande majorité, sinon une perturbation de l'activité de l'entreprise et une atteinte à leur réputation.

En 2020, le vecteur d'attaque le plus répandu reste le Phishing mais on note en deuxième position les tentatives de connexion suivi de l'ingénierie sociale.

L'UTILISATEUR EN PREMIÈRE LIGNE DE DÉFENSE



Compte tenu des usages suivants des salariés, cochez 1 risque fort selon vous pour la cyber-sécurité

Concrètement, en 2020, les entreprises ont été majoritairement confrontées à la « négligence ou erreur de manipulation ou de configuration d'un salarié » (34%).

Les RSSI et DSI des entreprises en Afrique sont unanimes : la sensibilisation et la formation des salariés reste la première ligne de défense pour lutter contre la cyber-criminalité. En effet, compte tenu de l'utilisation du SI par les salariés, les experts identifient « L'utilisation des Device personnels au travail (BYOD) » comme étant un risque fort pour la cyber-sécurité des entreprises.

Si les collaborateurs sont bien sensibilisés aux risques SI (72%), seulement 21% respectent les recommandations. Par ailleurs, 60% des RSSI disent n'avoir pas mis en place des procédures pour tester l'application des recommandations par les salariés.

D'ailleurs, concernant les enjeux à venir de la cybersécurité dans les entreprises africaines, les RSSI et DSI notent :

1. Mieux former et sensibiliser les usagers aux question de cybersécurité,
2. Placer la gouvernance de la cyber-sécurité au bon niveau,
3. Allouer davantage de budget et de ressources à la cyber-sécurité.

PRÉSENTATION DU CESIA

Créé en janvier 2020, d'une volonté de se réunir entre experts de la sécurité des systèmes d'information, le **CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE (CESIA)** compte à ce jour plus de 120 membres repartis dans 18 pays d'Afrique.

Le CESIA propose un cadre d'échange et de partage d'expérience exclusivement réservé aux Directeurs des Systèmes d'Information (**DSI**), aux Directeurs de la Sécurité des Systèmes d'Information (**DSSI**) et aux Responsables de la Sécurité des Systèmes d'Information (**RSSI**) des secteurs privés ou publics.

Pour être partenaire ou nous rejoindre contactez nous via :

- Notre site Internet : www.lecesia.com
- Notre adresse mail : contact@lecesia.com
- Notre page LinkedIn :@cesia
- Notre numéro de téléphone : +33 7 54 43 78 84

REMERCIEMENTS

Avant tout, nous tenons à remercier chaleureusement l'ensemble des DSI, DSSI et RSSI ayant participé à ce sondage et contribué à la production de ce baromètre.

Le Bureau

Créée en 2019, AFRICA SECURITY PARTNERS est une association internationale consacrée à la promotion de la sécurité de l'information en Afrique.

Elle a pour ambition de contribuer à la réflexion, à la recherche, au développement économique, à la promotion et à l'intégration des initiatives dans les domaines de la cybersécurité et du numérique. - https://africasecuritypartners.org

Créée en 2019, CIBEROBS est une association ayant pour ambition d'être d'une part, un relai d'informations sur les questions liées au risque cyber en Afrique et d'autre part, de produire des analyses pointues et pertinentes sur tous les sujets liés au cyber et à la sécurité des systèmes numériques et d'informations.
https://ciberobs.com

Créée en 2019, APAC se veut l'association de référence pour la promotion de la cybersécurité en Afrique et dans le Monde, a travers le partage de connaissances, d'échanges d'expériences, le développement des bonnes pratiques. Mais également la sensibilisation des citoyens, entreprises, organisations et pouvoirs publics sur le continent.
https://apac.digital

FONTECSYS est un cabinet de conseils TIC basé à Libreville au Gabon qui propose des solutions numériques.
Notre mission est simple et belle : accompagner nos clients dans leur processus de digitalisation.

Nous sommes des passionnés, animés par des valeurs de rigueur, d'exigence, de partage et d'écoute. https://www.fontecsys.com

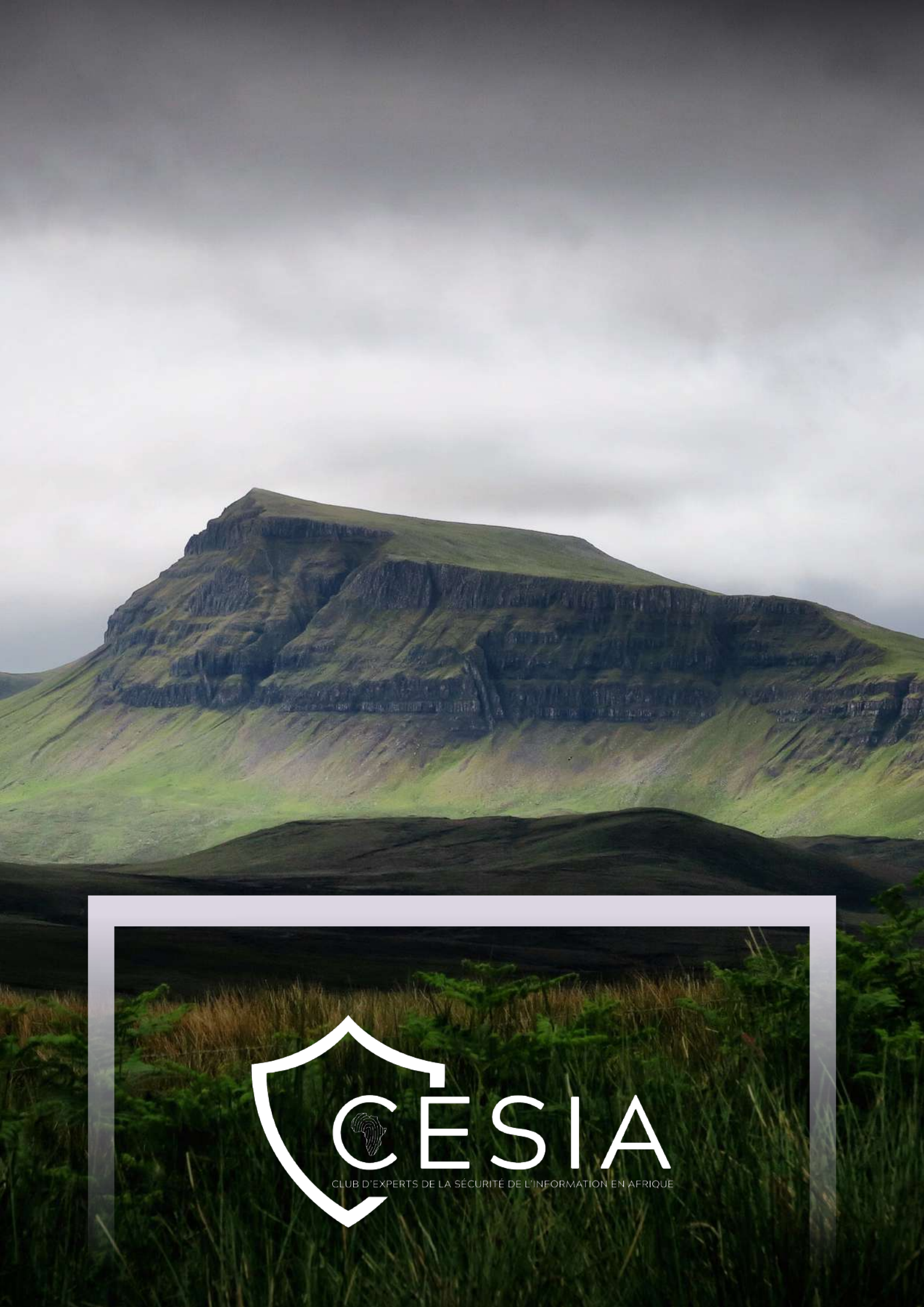
Africa CyberSecurity Mag est un magazine spécialisé sur la Cybersécurité, la CyberDéfense, la CyberJuridiction et la Protection Numérique édité par la société CyberSpector.

Le magazine fait un focus sur l'actualité de la CyberSécurité en Afrique et dans le monde et organise plusieurs activités spécifiques (conférences, Webinaires, Journée d'études et de réflexions). - https://cybersecuritymag.africa

Fondée en 2010, Polaris Secure Technologies est une société de conseil spécialisée dans la sécurité des systèmes d'information. Présente en France et en Afrique. Polaris accompagne ses clients dans tous leurs projets de sécurité informatique avec une approche globale à travers ses trois offres de services : Audit, Conseil et Formation, avec pour but de leur garantir une très bonne maîtrise de la sécurité de leurs systèmes d'information. https://www.polaris-st.com

GROWTH CONTINUE CONSULTING Group est une société de FORMATION professionnelle, d'ASSISTANCE et de CONSEIL qui a pour vocation de former et accompagner des managers africains responsables et opérationnels immédiatement.

Depuis plus de dix (10) ans, notre société se positionne comme leader de la formation professionnelle en Afrique Subsaharienne et ambitionne développer ses activités dans toute l'Afrique Francophone d'ici 2023. - https://growthcontinue.com/


CESIA
CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE