CESIA

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

BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE

ÉDITION 2023

RENDEZ-VOUS SUR NOTRE SITE

www.lecesia.com

CESIA

TABLE DES MATIÈRES

4 Éditorial
5 A propos du CESIA
6 Mot du président
7 Les objectifs du Baromètre de la cybersécurité en Afrique
8 Notre Méthodologie
9 Nos partenaires
10 Les messages clés

Les cyberattaquants maintiennent leur cadence
La cybersécurité, une priorité en Afrique
Le facteur humain

12 Les actions prioritaires à court/moyen terme

Organisation de la gouvernance sécurité
Une sensibilisation efficace des collaborateurs
Se préparer à répondre à une cyberattaque de grande ampleur

13 Résultats
14 Analyse des résultats

Le profil des participants
Le dispositif de sécurité technique des entreprises
Les organisations africaines face aux cyberattaques
Le salarie au cœur de la sécurité
Gouvernance de la sécurité

33 Les besoins à moyen / long terme en Afrique

Le CLOUD en Afrique
Start Up

35 Ouverture

Le CESIA est propriétaire du présent document.

On ne peut reproduire ni diffuser aucune partie du présent ouvrage, sous quelques formes ou par quelque procédé que ce soit, sans nommer le CESIA – CLUB D'EXPERTS DE LA SECURITE DE L'INFORMATION EN AFRIQUE comme étant la source.

Aucune reprise de cette étude ne pourra être dissocié de cet intitulé

Pour plus d'information : contact@lecesia.com

Éditorial

Comme chaque année, le CESIA – CLUB D'EXPERTS DE LA SECURITE DE L'INFORMATION EN AFRIQUE publie son étude annuelle sur l'état et la perception de la maturité cyber dans les entreprises en Afrique.

Le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE 2023 se veut être une étude qualitative, réalisée directement auprès des professionnels et des décideurs de la sécurité numérique dans les entreprises en Afrique. Cette étude réalisée du 1er décembre 2022 au 15 janvier 2023 rend compte de l'état et la perception de la cybersécurité sur l'année écoulée.

Il est de plus en plus difficile de faire le tri dans les « buzz words » qui peuplent l'univers de la cybersécurité. Face à la croissance, la sophistication et la diversité des cibles des cyberattaques, les entreprises africaines croulent sous les offres de solutions technologiques. Derrière ce foisonnement se dégagent plusieurs tendances, qui répondent aux évolutions des entreprises comme des stratégies des cyberattaquants.

Dans ce contexte, les entreprises africaines redoutent de subir une cyberattaque de grande ampleur, seulement 20% d'entre elles disposent d'un programme de cyber-résilience. Si les professionnels de la cybersécurité en Afrique jugent avoir un meilleur positionnement dans leurs entreprises et un budget qui augmente depuis 2020, ils notent tout de même un manque de formation et de sensibilisation, un manque de ressources et des compétences dédiées à la cybersécurité et une absence de visibilité sur les solutions du marché.

A propos du CESIA

Depuis 2019, le CESIA - CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE est un espace d'échange et de partage d'expérience réservé aux décideurs et aux professionnels de la sécurité numérique exerçant en Afrique ou ayant un intérêt pour le développement du secteur sur le continent.

Cette année, le CESIA compte 170 membres présents dans 18 pays en Afrique avec pour objectif :

- Promouvoir et valoriser les métiers de la sécurité de l'information à travers un code d'éthique adopté par les membres de l'Association ;
- Participe aux démarches nationales et être force de proposition sur des textes règlementaires, guides et autres référentiels ;
- Permet la coopération entre experts de la sécurité de l'information et entre ces experts et les pouvoirs publics en favorisant le partage de connaissances et d'expériences ;
- Sensibiliser les dirigeants d'entreprises, les organismes publics et l'opinion publique nationale et internationale à l'importance de la sécurité de l'information ;
- Contribuer aux programmes d'éducation et de formation dans le domaine de la sécurité de l'information ;
- Réaliser des ouvrages, des synthèses sur l'état de l'art et des techniques en la matière, de créer et formaliser des recommandations, des méthodologies ;
- Communiquer auprès du grand public par des partenariats d'évènements, des conférences, des salons et tous autres évènements publics.

Les membres du CESIA occupent les fonctions de fonction de DSI, Directeur Technique, Directeur cybersécurité, DSSI, RI, RSI, RSSI, Responsable SOC/CERT, CSSI ou réfèrent sécurité.

60 rue François 1er
75008 Paris

contact@lecesia.com

Réseaux sociaux

Mot du président

Didier SIMBA
Président et Fondateur du CESIA

Plusieurs pays en Afrique font preuve d'une grande volonté d'accéder à la 4e révolution industrielle, celle des usages numériques et mobiles, dans le but de moderniser les conditions de vies des utilisateurs en facilitant les démarches grâce au numérique. De nombreux projets numériques ont été lancés en Afrique. D'ailleurs, le continent est déjà très à la pointe au niveau des usages mobiles, des micropaiements et l'usage des applications mobiles.

Cela dit, si la crise sanitaire a permis d'accélérer la transformation digitale sur le continent, elle a tout aussi révélé au grand jour la dépendance des entreprises à l'outil informatique. Elle a confirmé l'essor inexorable des infrastructures numériques et la nécessité vitale de les sécuriser.

En 2022, les cybercriminelles ont poursuivi l'amélioration de leur capacité et le gain financier ou l'espionnage restent les menaces majeures de l'année.

Les entreprises africaines de toute taille et de tout secteur sont les cibles des cyberattaques de plus en plus sophistiquées. Dans ce contexte la prochaine étape dans un délai très court, est de construire un numérique de confiance nationale dans les différents États, afin de protéger leurs infrastructures critiques, ainsi que les États et leurs populations. Un travail collectivement avec l'ensemble des acteurs, publics et privés devient indispensable.

Plus que jamais, les professionnels de la cybersécurité ont besoin de partager des pratiques et des expériences. La compréhension des risques et le partages d'information sur les menaces et les pratiques sont essentiels dans l'exercice de notre fonction : le **CESIA – CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE s'impose donc comme étant l'espace d'échange d'idée pour répondre à ce besoin et le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE s'impose quant à lui comme un outil efficace pour suivre l'évolution des menaces et des enjeux de cybersécurité pour les entreprises et les États africains.** Il constitue un réel atout stratégique pour appréhender le niveau de maturité du continent en la matière.

Les objectifs du Baromètre de la cybersécurité en Afrique

Initié en 2019, avec une publication pilote sur 4 pays en Afrique, le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE est désormais l'enquête annuelle du CESIA. Il se veut être une étude qualitative réalisée directement auprès des professionnels et des décideurs de la sécurité numérique en général et des membres du CESIA en particulier. Notre étude indépendante vise un triple objectif :

- Faire un état de lieu sur les enjeux de la cybersécurité en Afrique et sa perception au sein des entreprise en Afrique,
- Apprécier la maturité cyber dans les entreprises et,
- Identifier les besoins en cybersécurité pour les professionnels du secteur.

Par notre étude, nous contribuons à publier les chiffres dont manque cruellement le continent en matière de cybersécurité. Ces indicateurs sont un outil qui permet aux professionnels du secteur de défendre des positions ou étayer une démonstration à leur COMEX et aide les entreprises fournisseurs de service ou de solution à identifier les besoins des entreprises.

Enfin, chaque année le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE apporte des précisions sur l'impact des projets de transformation numérique au sein des entreprises ou des États en Afrique.

Notre Méthodologie

Notre échantillon représente plus de 350 participants dans 21 pays d'Afrique qui sont membres du CESIA ou professionnel de la sécurité numérique, membre du réseau de nos partenaires.

80% des participants sont des décideurs (DSI, Directeur Technique, Directeur cybersécurité, DSSI, RI, RSI, RSSI, CISO, Responsable SOC/CERT, CSSI ou réfèrent sécurité).

20% des participants sont consultants séniors en SSI.

Notre enquête s'est déroulée du **1er décembre 2022 au 15 janvier 2023.**

Les participants ont été interviewés via un **formulaire anonyme en ligne.**

Nos partenaires

La transformation digitale, parfois appelée transformation numérique, désigne le processus qui consiste, pour une organisation, à intégrer pleinement les technologies numériques dans l'ensemble de ses activités : Son offre produits et services, ses relations client, ses process internes, ses relations fournisseurs, etc.

La ligne de service conseil en transformation digitale de ST DIGITAL a pour objectif d'accompagner les entreprises dans leur processus de transformation digitale. - www.st.digital

AFRICA CYBERSECURITY MAG est un magazine spécialisé sur la Cybersécurité, la Cyberdéfense, la Cyber Juridiction 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). - www.cybersecuritymag.africa

FORMIND est un leader Français indépendant expert en cybersécurité.

Nous accompagnons plus de 500 clients (dont de nombreux grands comptes) issus de multiples secteurs d'activités : Banques, Assurances, Utilities, Industrie, Transport, Santé, Retail....

Nos interlocuteurs, essentiellement DSI, RSSI, Risk Managers et Directions de l'audit et du contrôle, Direction Conformité, apprécient notre double compétence technique et métier. – www.formind.fr

La société d'incubation numérique du Gabon est une société de service d'innovation numérique. La raison d'être de la SING SA est de renforcer la compétitivité des économies africaines en étant un catalyseur de la transformation digitale et de l'innovation numérique.

Nous réalisons cette mission grâce à :

Une approche pragmatique de l'innovation au plus près de la réalité des consommateurs africains ;

Une veille constante des meilleurs outils, pratiques et méthodologies en matière d'innovation numérique ;

L'adaptabilité de nos équipes et de nos méthodes face aux défis changeants et à l'incertitude. - www.sing.ga

Les messages clés

Les cyberattaquants maintiennent leur cadence

Plus d'une organisation sur 2 (56% en 2022 contre 64% en 2021) en Afrique déclare avoir subi au moins une cyberattaque en 2022. Cette légère baisse démontre la prise de conscience des enjeux liés à la cybersécurité par les organisations africaines mais surtout les efforts consentis qui portent leur fruit.

Cet indicateur reste à la baisse en comparaison aux années précédentes (82% en 2020 et 64% en 2021). Il n'en demeure pas moins vrai que les conséquences sont considérables sur les activités de l'entreprise : Dans 48% (43% en 2021) des cas on constate une perturbation de la production pendant une durée significative ou indisponibilité du site Web.

Cette année encore, pour un peu plus d'une entreprise sur 2, l'impact reste négligeable.

Dans 1 cas sur 2, le Phishing reste le vecteur d'attaque privilégié (51% en 2022 contre 69% en 2021). Les tentatives de connexion non autorisées restent à la 2e place du podium (44% en 2022 contre 34% en 2021) suivi de l'ingénierie sociale (30% en 2022 contre 28% en 2021). Toutefois, 45% des entreprises pensent ne pas être prêtes à gérer une cyber-crise (52% en 2021).

La cybersécurité, une priorité en Afrique

Les entreprises et organisation africaines prennent la mesure des enjeux cyber et cela se dénote par le sponsoring du top management dans les projets de sécurité.

La gestion de la cybersécurité est de plus en plus faite en interne (69% en 2022 contre 63% en 2021). Pour se prémunir d'une crise cyber, les entreprises mettent en place des sauvegardes sécurisées dans la majorité des cas. En plus des antivirus et les pares-feux, les entreprises se protègent en sécurisant les accès distants (74% en 2022. Contre 55% en 2021) et en activant le MFA dès que possible (57%), suivi de très près par filtrage URL (56% contre 33% en 2021).

Comme chaque année, très peu d'entreprise disposent d'un programme de cyber-résilience (17% en 2022 contre 15% en 2021).

Enfin, les entreprises n'ont toujours pas recours aux solutions innovantes issues des strat-up et dans la très grande majorité des cas (46%) pointent le manque de maturité, la pérennité des offres et le manque de budget.

Le facteur humain

Si moins d'entreprises disposent d'un plan annuel de sensibilisation (47% en 2022 contre 61% en 2021), 71% (80% en 2021) d'entre elles considèrent que les salariés sont bien sensibilisés aux risques cyber. 26% (20% en 2021) des collaborateurs respectent les recommandations de sécurité numérique.

Une fois sensibilisées, 25% des entreprises ont mis en place un dispositif pour tester l'application des recommandations par les collaborateurs.

Au nombre des usages numériques des salaries présentant les risques, on note : le BYOD (43% en 2022 contre 40% en 2021), l'usage des ressources professionnelles pour des raisons personnelles (33%) et le Shadow IT (22% en 2022 contre 21% en 2021).

Cette année, nous continuons de suivre l'impact de la crise sanitaire sur la sécurité numérique dans les entreprises et organisations en Afrique.

Le continent étant très peu touché par la crise sanitaire, le télétravail et/ou le nomadisme n'a pas été généralisé. Les entreprises continuent de juger risqué le déploiement de ce dispositif. Au nombre de risques évoqués, notons :

- 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 ;
- Maintenir le niveau de sensibilisation des collaborateurs aux risques SI à distance ;
- Empêcher les fuites de données lorsque les utilisateurs sont livrés à eux-mêmes avec des outils collaboratifs déployés à la va-vite sans de la conduite de changement habituellement mise en place.

Dans tous les cas, pour environ 40% des entreprises, le budget de la cybersécurité a augmenté à la suite de cette crise sanitaire.

Les détails de l'analyse quantitative de cette étude se trouve dans la section « L'analyse des résultats »

Les actions prioritaires à court/moyen terme

Organisation de la gouvernance sécurité

La désignation d'un réfèrent sécurité ou un Responsable de Sécurité des SI (RSSI) devrait se généraliser à tous les secteurs d'activités.

Par ailleurs, si 31% des RSSI sont encore rattachés à la Direction des Systèmes d'Information (DSI), ils demeurent très opérationnels. Face à la sophistication des cyberattaques et aux conséquences de plus en plus importantes pour les entreprises, le référent sécurité devrait se focaliser sur l'organisation et l'animation de la sécurité au sein de son entreprise.

Le RSSI doit être formé et disposer des moyens financiers et organisationnels pour exercer sa fonction.

Enfin, afin de renforcer le travail collectif, le RSSI et/ou le référent sécurité des organisations doit avoir la possibilité d'échanger avec ses pairs. 29% des RSSI opèrent de manière solitaire et/ou s'appuient sur les experts internes.

Une sensibilisation efficace des collaborateurs

53% des organisations ne disposent pas de plan annuel de sensibilisation SSI. De nombreux programmes de sensibilisation à la sécurité pèchent par manque d'efficacité.

Pour une sensibilisation efficace, le programme de sensibilisation doit définir des objectifs. Ces objectifs doivent être mesurables et trouver un juste équilibre entre le niveau de compétence visé pour chaque groupe de salariés et le temps total d'apprentissage nécessaire pour les amener à ce niveau. Un programme de sensibilisation SSI doit garantir l'appréciation de la formation et, par conséquent, son efficacité.

Se préparer à répondre à une cyberattaque de grande ampleur

Nous recommandons la mise en place d'un plan de cyber résilience validé et testé régulièrement.

Le plan de résilience intègre un plan de gestion de crise, de communication et de continuité d'activité.

Résultats

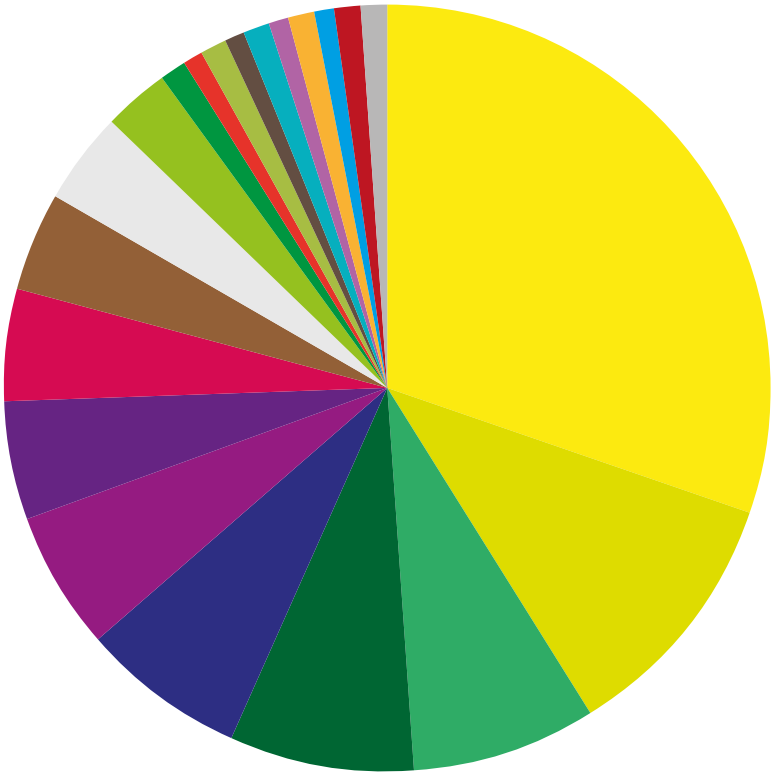
Analyse des résultats

Le profil des participants

21 pays ont participé à la 3e édition du baromètre de la cybersécurité en Afrique contre 17 pays lors de la précédente édition : un record pour cette étude.

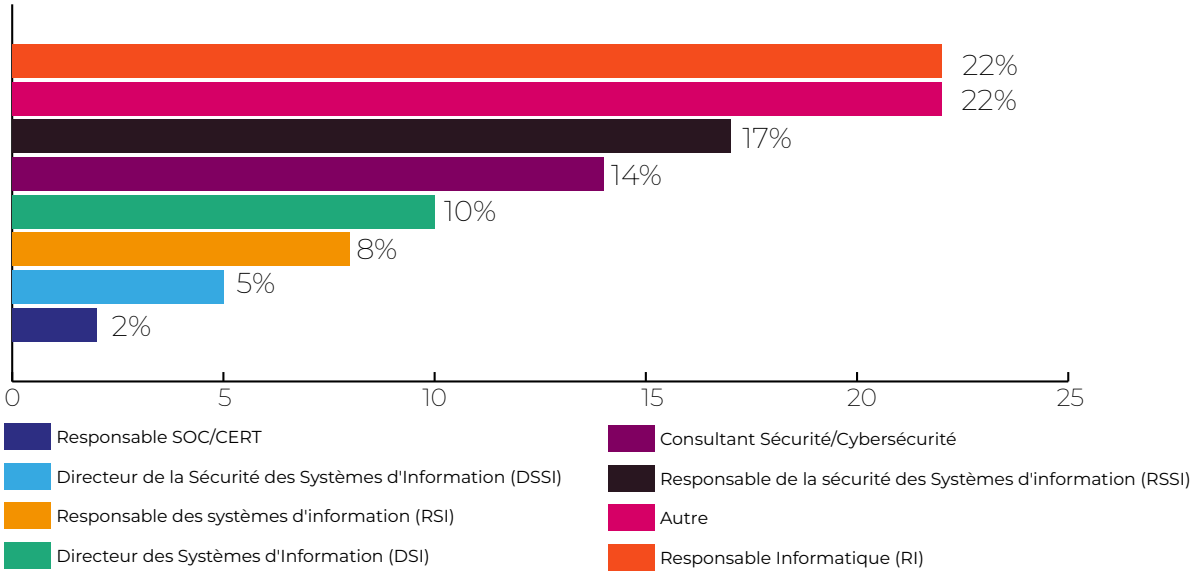
Le podium est occupé par :

- **Cameroun qui gagne 6** place par rapport à l'année dernière.
- **Côte d'Ivoire qui perd une place** par rapport à l'année dernière
- **Bénin qui gagne 13 places** par rapport à l'année dernière



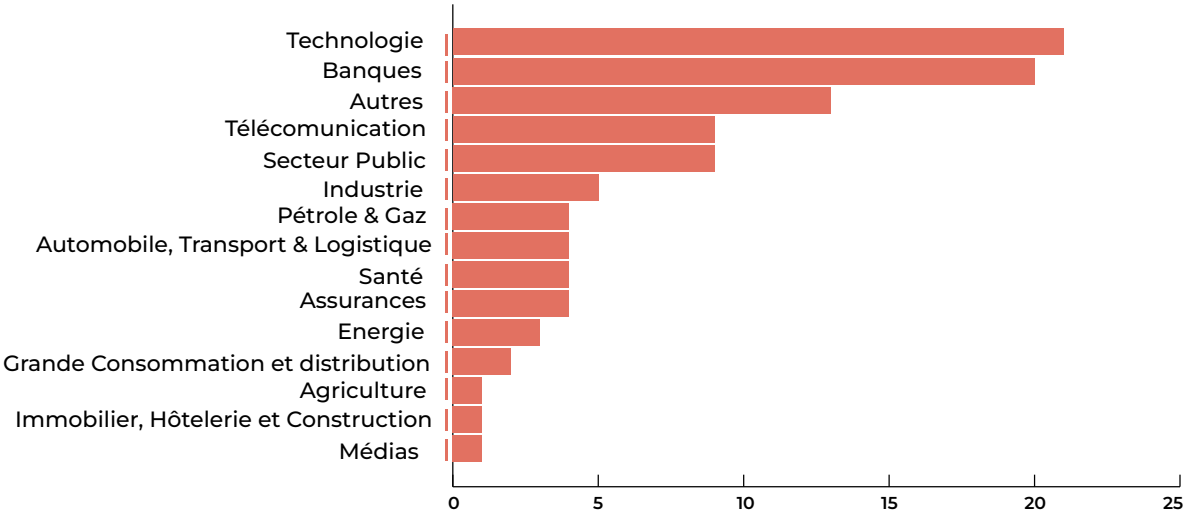
Cameroun, Côte d'ivoire, Bénin, Gabon, Togo, Guinée, Sénégal, Maroc, RDC, RC, Guinée Equatoriale, Tunisie, Tchad, Mali, Niger, Maurice, Madagascar, Érithée, Djibouti, Comore, Burkina Faso

Taux de participation par pays

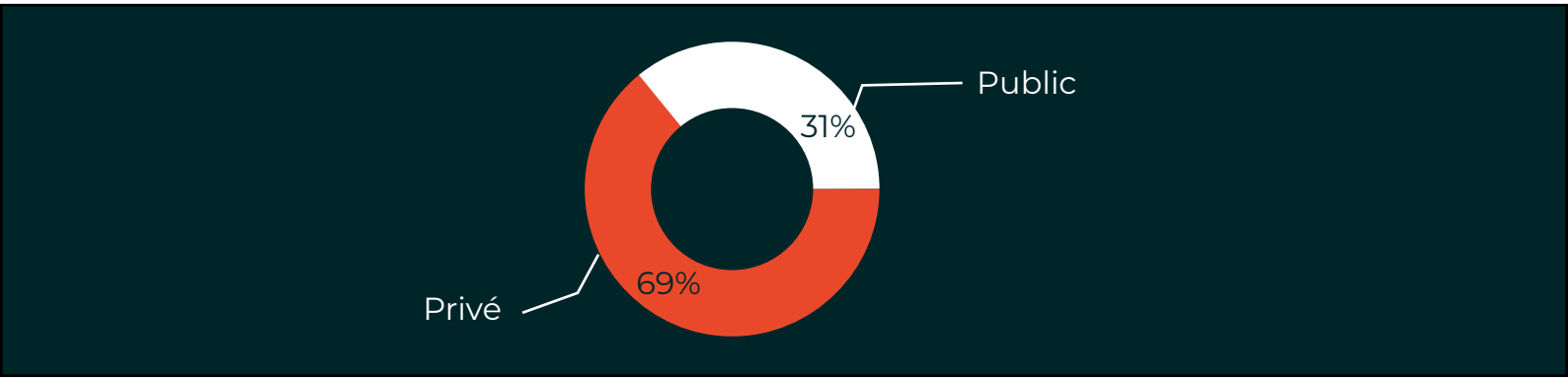


Tous les secteurs d'activités sont représentés dans cette édition 2023.

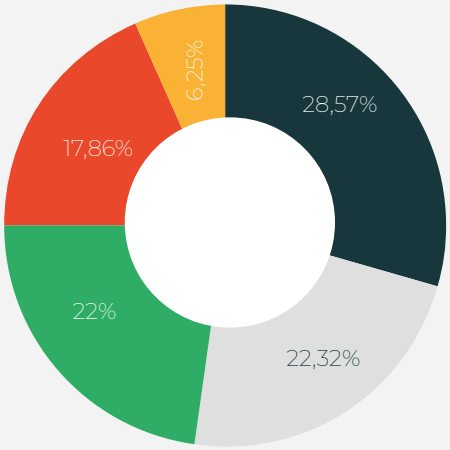
Les secteurs bancaires et les nouvelles technologies sont particulièrement ciblés.



Secteurs d'activité représentés



- *Q1 : Qui êtes vous ?*

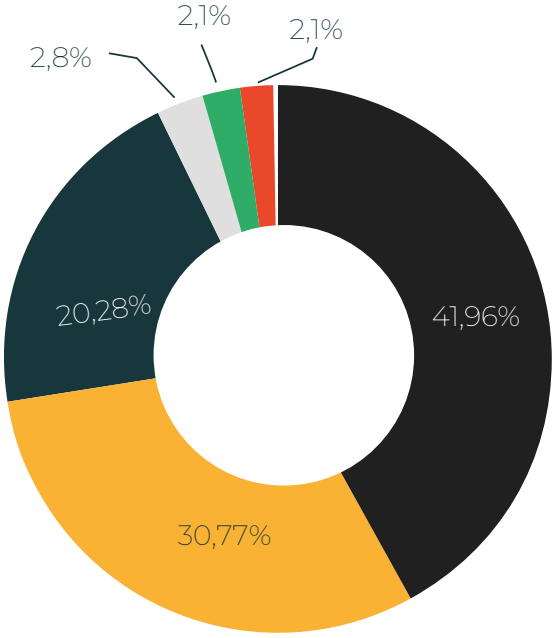


Les participants de notre étude sont majoritairement des Responsables Informatiques exerçant les activités de cybersécurité.

- Directeur de la sécurité des Systèmes d'Information (DSSI)
- Directeur des Systèmes d'information (DSI)
- Consultant Sécurité/Cybersécurité
- Responsable de la Sécurité des Systèmes d'Information
- Responsable Informatique (RI)

- **Q2 : Dans votre organisation, est ce que le DSSI/RSSI est rattaché**

Un top management de plus en plus conscient des enjeux de la cybersécurité dans les organismes en Afrique.

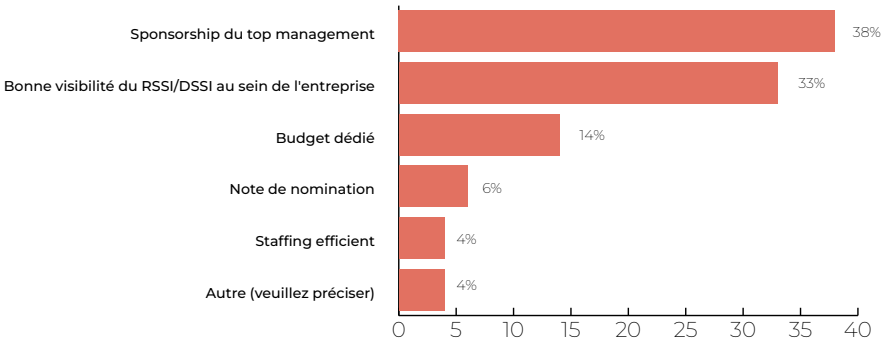


- A la Direction Générale
- A la Direction des Systèmes d'information
- A la Direction de l'Audit Interne
- A la Direction des risques
- Je ne sais pas
- Autre

Le dispositif de sécurité technique des entreprises

Le sponsorship du top management ainsi que la bonne visibilité du RSSI, deux principaux critères qui démontrent que la cybersécurité est une priorité pour l'entreprise.

- **Q9 : Parmi les critères ci-dessous, merci d'indiquer celui qui démontre le plus que la Cybersécurité est une priorité dans une entreprise ?**



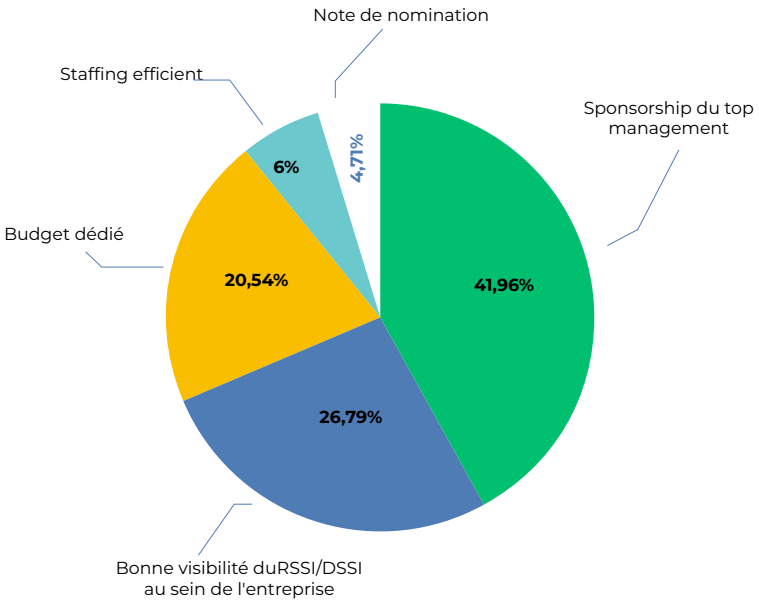
14%

des personnes interrogées estiment que le budget dédié est un critère de priorité de la cybersécurité régulièrement.

- **Q10 : Tenant compte de votre position actuelle, lequel démontre le plus l'engagement d'une entreprise en matière de cybersécurité ? (À dire d'expert)**

42%

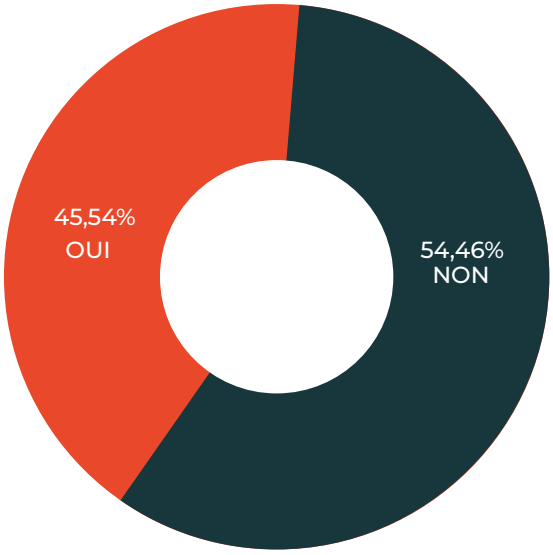
des personnes intéressées estiment que **le parrainage du top management est un critère d'engagement de l'entreprise en matière de cybersécurité**.



- **Q11 : Selon vous, votre entreprise est-elle préparée à gérer une cyberattaque ?**

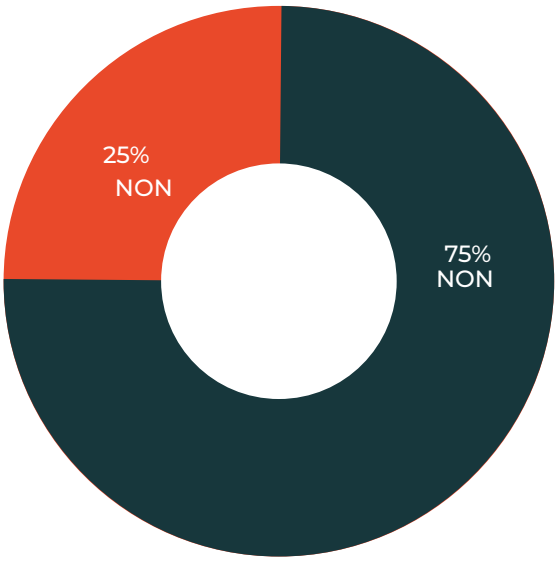
45%

Des entreprises africaines 52% en 2021, déclarent ne pas être préparées à gérer une cyberattque



Une « cyberattaque », telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information, entraînant un impact significatif d'image, financier, organisationnel, juridique et/ou réglementaire.

- *Q12 : Au sein de votre organisation, avez-vous mis en place des procédures ou un dispositif de gestion des incidents de sécurité ?*



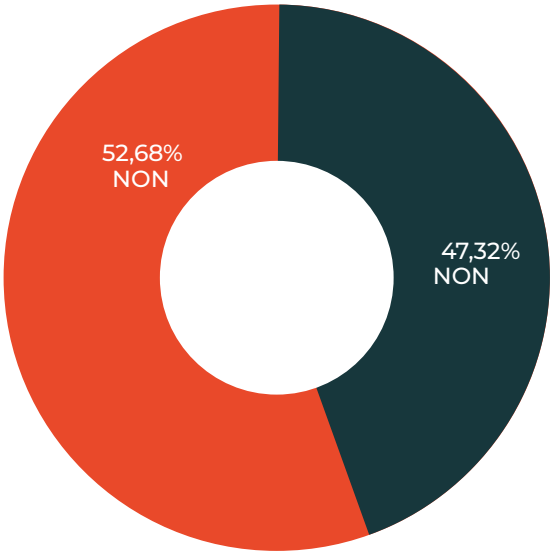
25%

des entreprises africaines interrogées n'ont pas mis en place un dispositif de gestion des incidents de sécurité

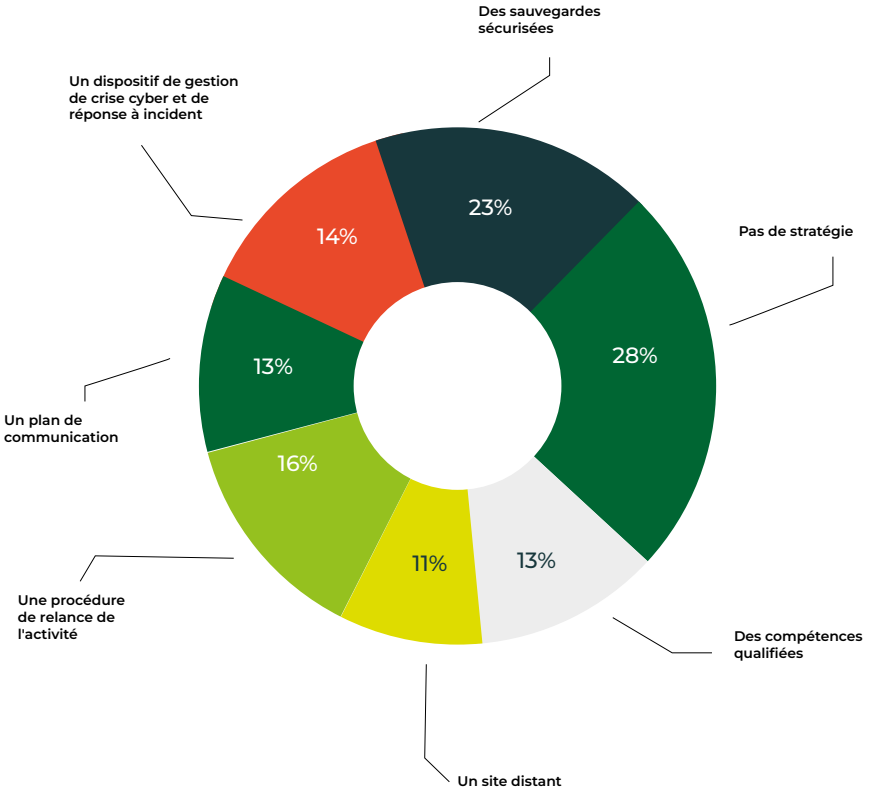
- ## Q13 : Testez-vous régulièrement cette procédure de gestion d'incident ou gestion de crise ?

53%

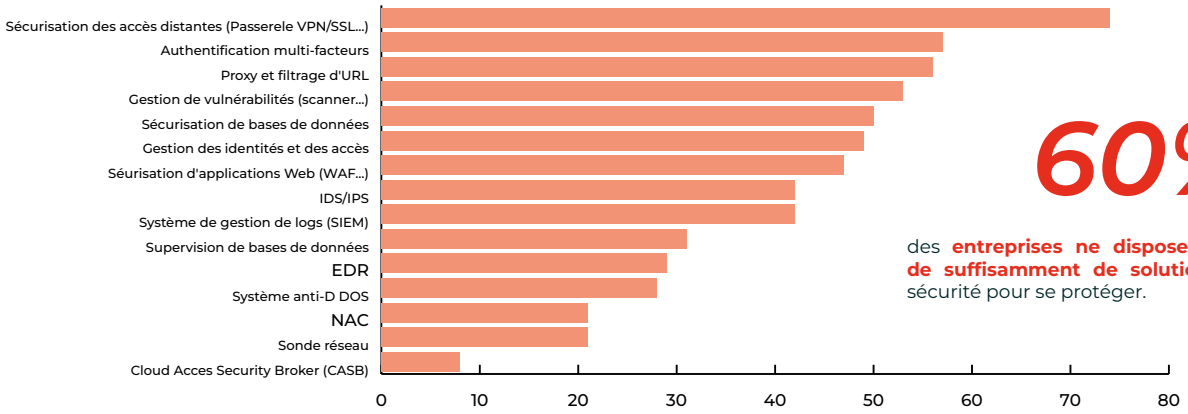
des **entreprises africaines interrogées déclarent que leur dispositif de gestion de crise cyber n'est pas testé régulièrement**.



- ## Q14 : Si vous disposez d'une stratégie de gestion de crise cyber, merci de nous indiquer quels sont les éléments que vous avez pris en compte parmi les exemples ci-dessous ?



- **Q15 : Parmi les solutions de protection suivantes (liste non exhaustive), quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ?**



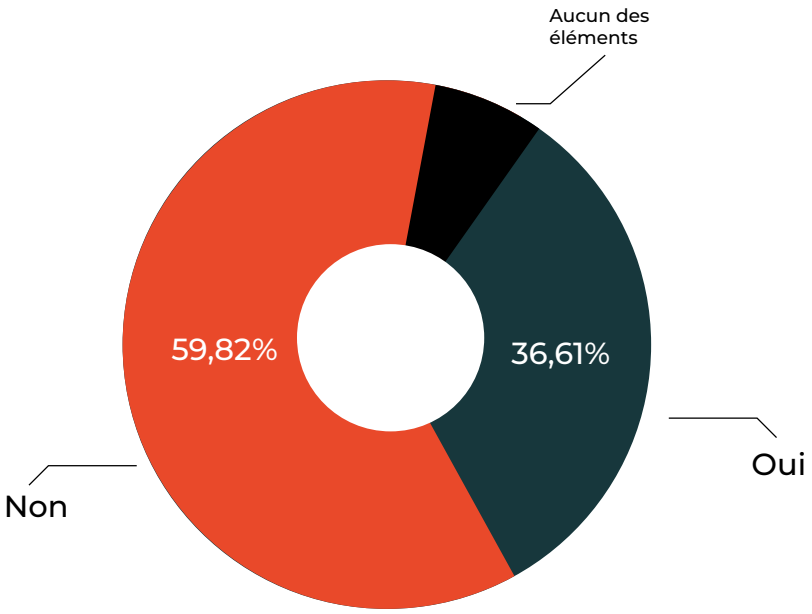
60%

des **entreprises ne disposent pas de suffisamment de solutions** de sécurité pour se protéger.

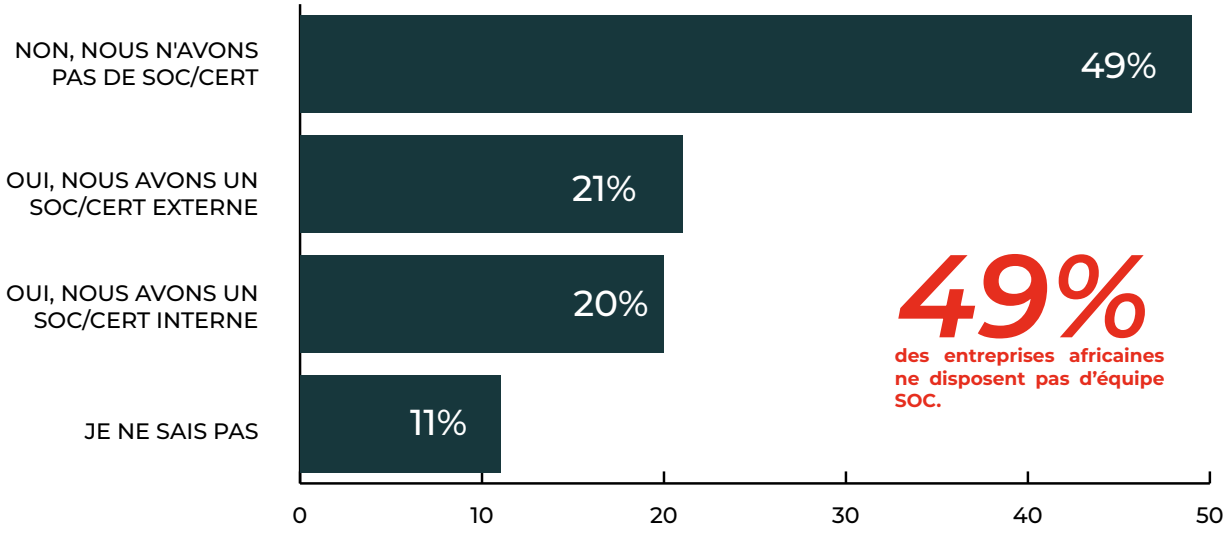
- **Q16 : Disposez-vous de suffisamment de solutions de sécurité pour vous protéger ?**

56%

des **entreprises africaines interrogées déclarent un manque de solutions** de sécurité pour mieux se protéger.



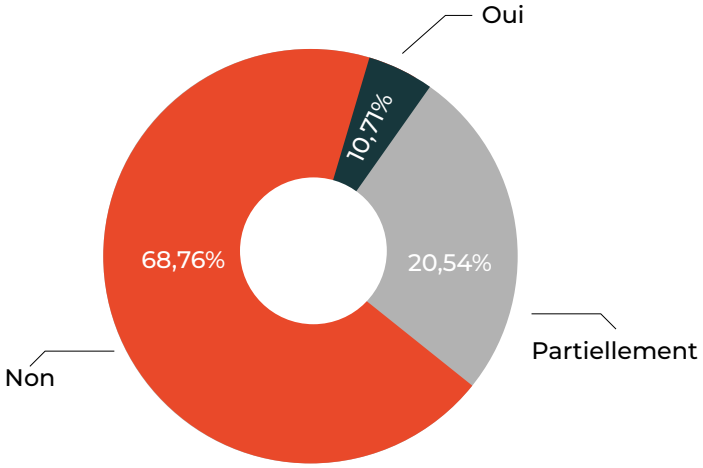
- ## Q17 : Disposez-vous d'un SOC ou CERT ?

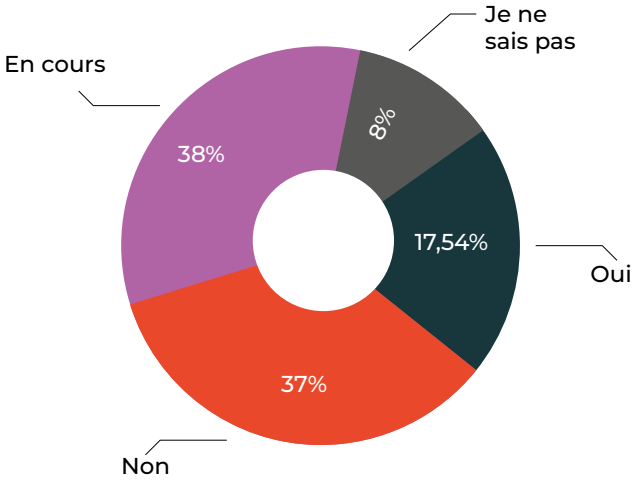


49%
des entreprises africaines ne disposent pas d'équipe SOC.

- ## Q18 : La gestion de la cyber sécurité dans votre entreprise est-elle externalisée ?

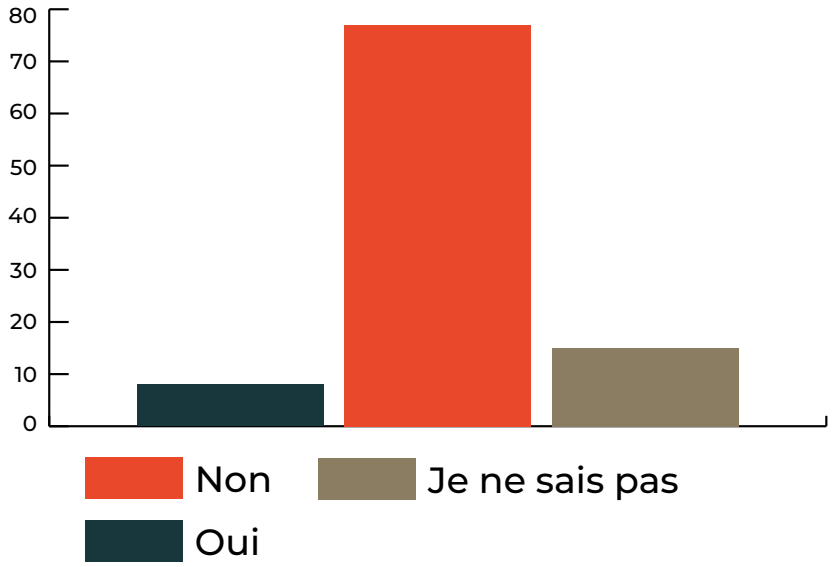
31%
des entreprises africaines externalisent leur cybersécurité





17%
des entreprises disposent d'un programme de cyber résilience

- Q20 : Votre entreprise a-t-elle souscrit à une assurance cyber ?



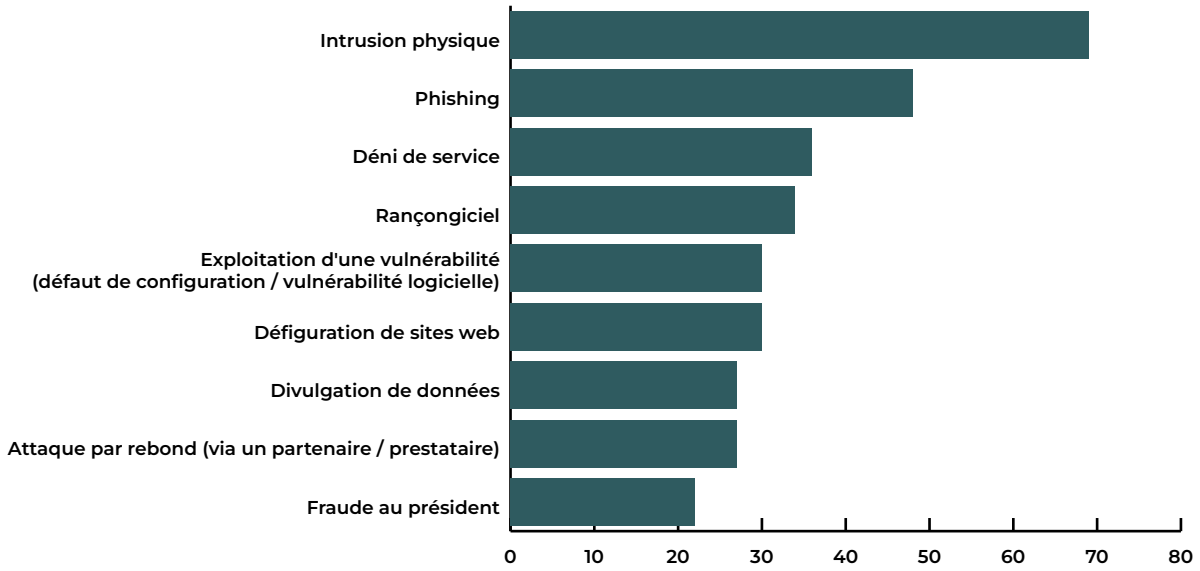
77%

contre 80% en 2022.

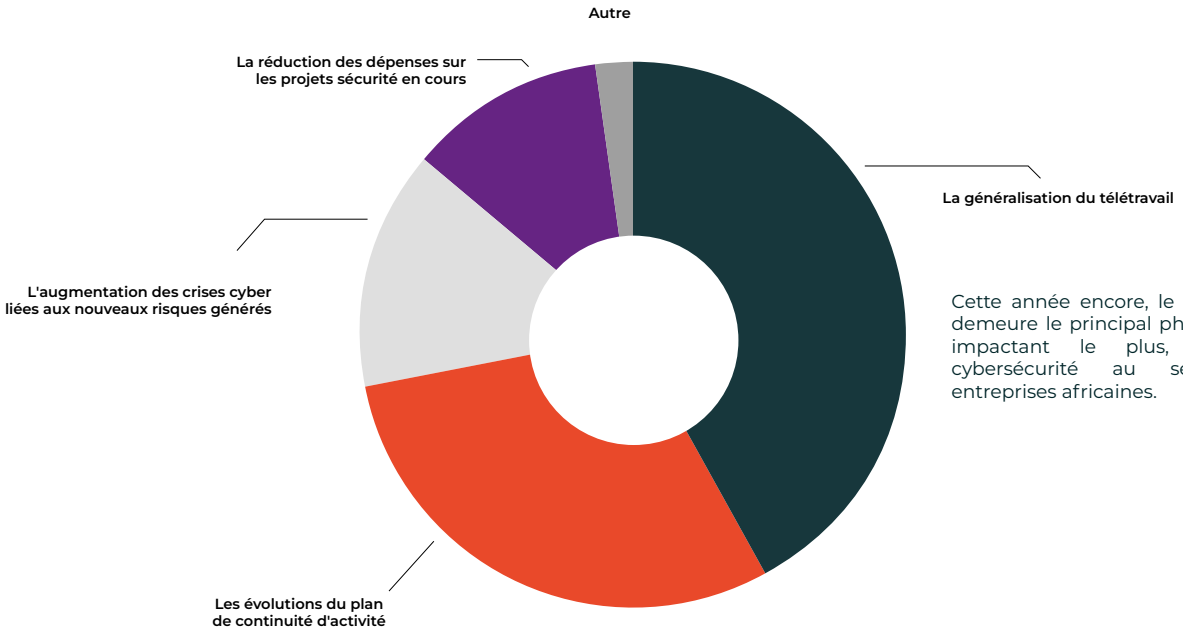
Des **organisations n'ont pas souscrit aux offres de cyber assurance**

Les organisations africaines face aux cyberattaques

- Q23 : Selon votre conviction, quelles seraient les 3 attaques pour lesquelles votre organisation semble la mieux protégée ?

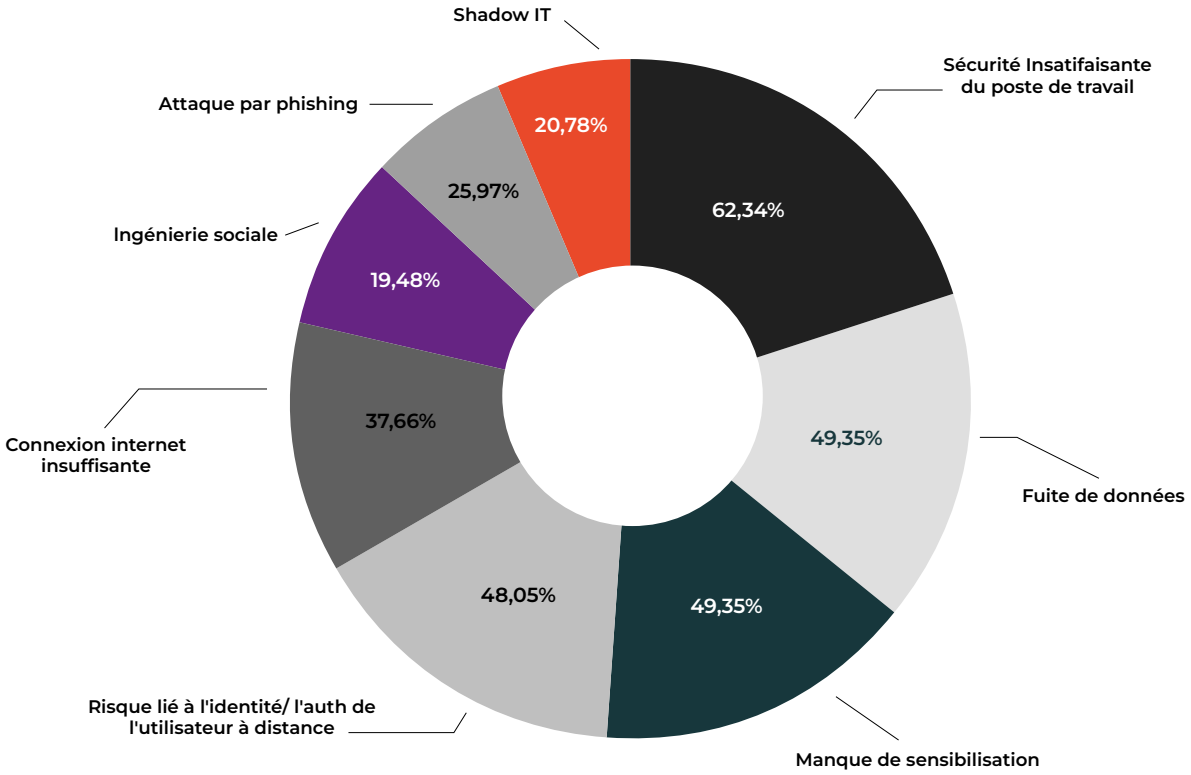


- ## Q24 : À la suite de la crise sanitaire qui est désormais derrière nous, quel phénomène a impacté le plus, l'activité cybersécurité de votre entreprise ?

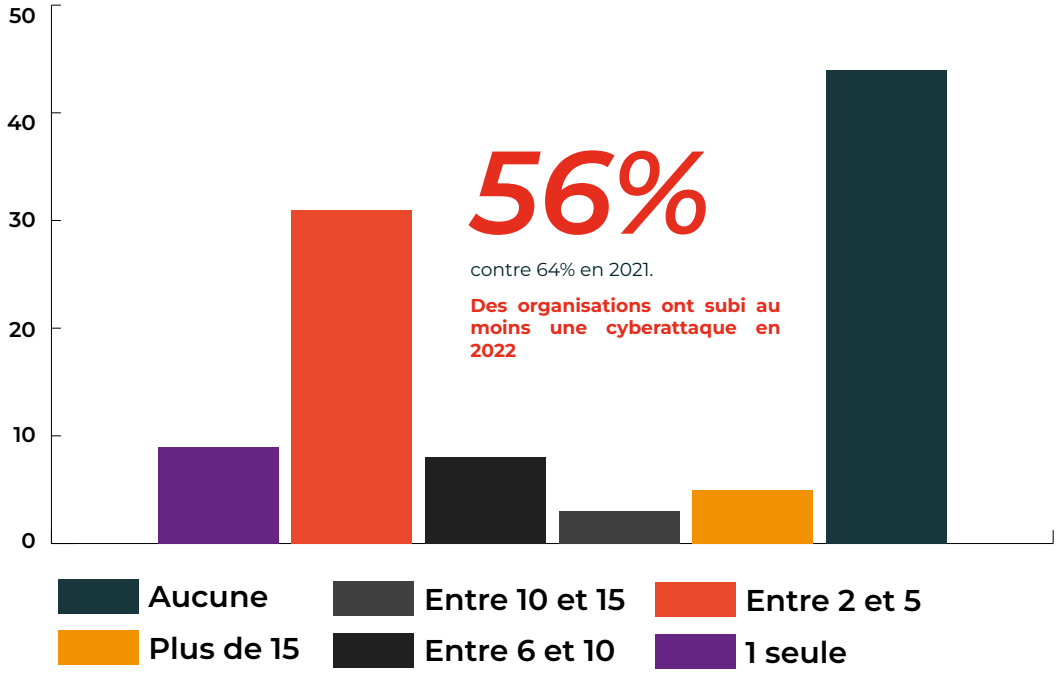


Cette année encore, le télétravail demeure le principal phénomène impactant le plus, l'activité cybersécurité au sein des entreprises africaines.

- ## Q26 : Selon vous, quels sont les 3 principaux risques liés au Télétravail / nomadisme ?

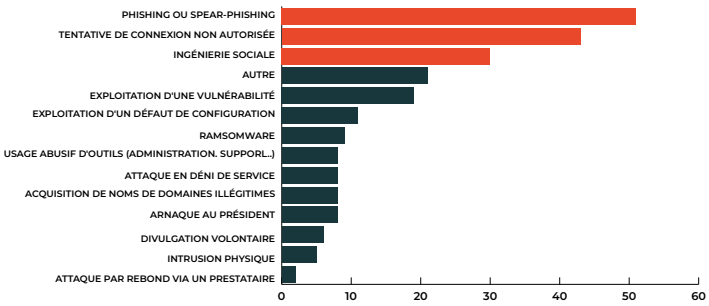


- ## Q27 : Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?



Une « cyberattaque », telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information, entraînant un impact significatif d'image, financier, organisationnel, juridique et/ou réglementaire.

- ## Q28 : Parmi les techniques d'attaques suivantes, lesquelles ont ciblé votre entreprise au cours des 12 derniers mois ?



TOP 3 DES VECTEURS

- Cette année encore, le **Phishing** garde la 1ere place dans les vecteurs d'attaques.
- Les **tentatives de connexion non autorisées** s'est installées solidement à la 2e place.
- **L'ingénierie sociale monte sur le podium par rapport à l'année dernière comme étant le 3e vecteur d'attaque privilégié.**

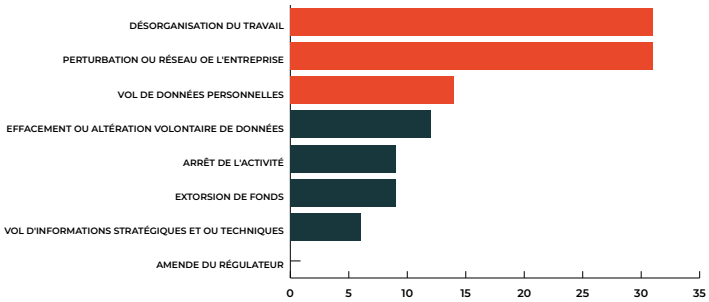
-

- ## Q29 : Quel a été l'impact des cyber-attaques sur votre business ?

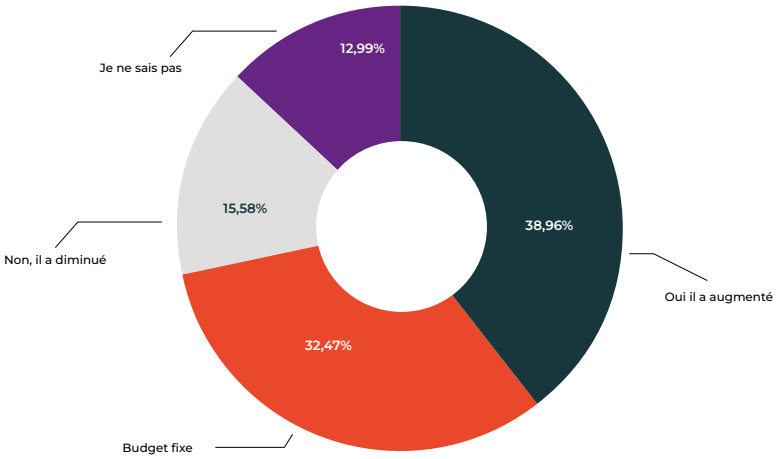
TOP 3 DES CONSEQUENCES

En cas de cyberattaque aboutie,

- Les entreprises sont désorganisées.
- Le réseau de l'entreprise est perturbé.
- **Les experts indiquent avoir subi des vols de données personnelles.**



- ## Q32 : À la suite de cette crise sanitaire, votre budget sécurité SI a-t-il évolué ?



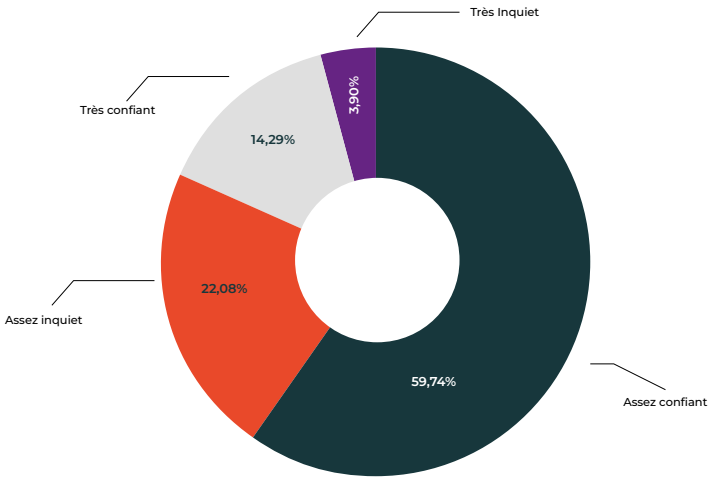
39%

des entreprises ont augmenté leur budget dédié à la sécurité SI contre 15% de revue à la baisse.

- ## Q33 : Pour l'avenir, en ce qui concerne la capacité de votre entreprise à faire face aux cyber-risques, diriez-vous que vous êtes

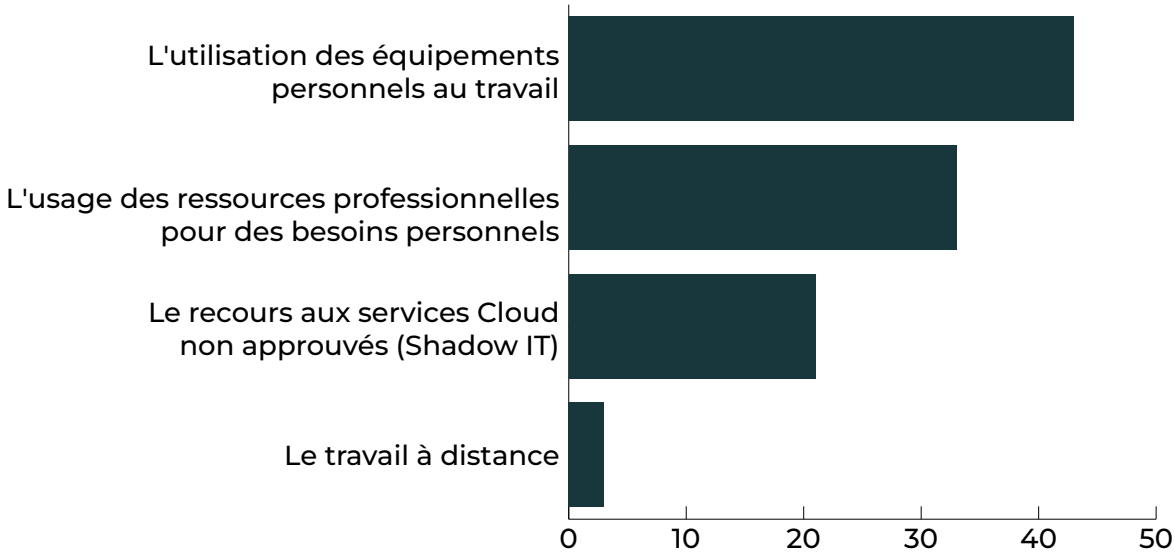
26%

des **entreprises interrogées se déclarent assez ou très inquiet en ce qui concerne leur capacité à faire face aux cyber-attaques.**

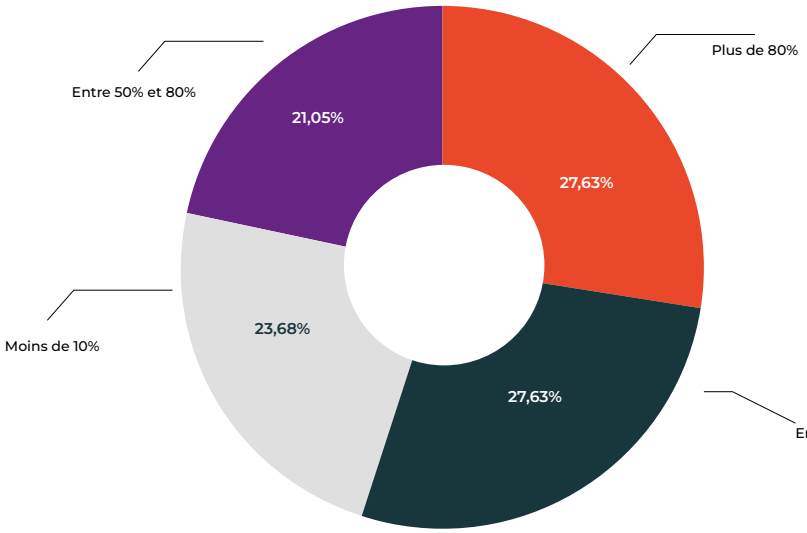


Le salarie au cœur de la sécurité

- **Q35 : Compte tenu de votre position actuelle, veuillez sélectionner l'usage présentant un risque cyber élevé pour votre organisation**



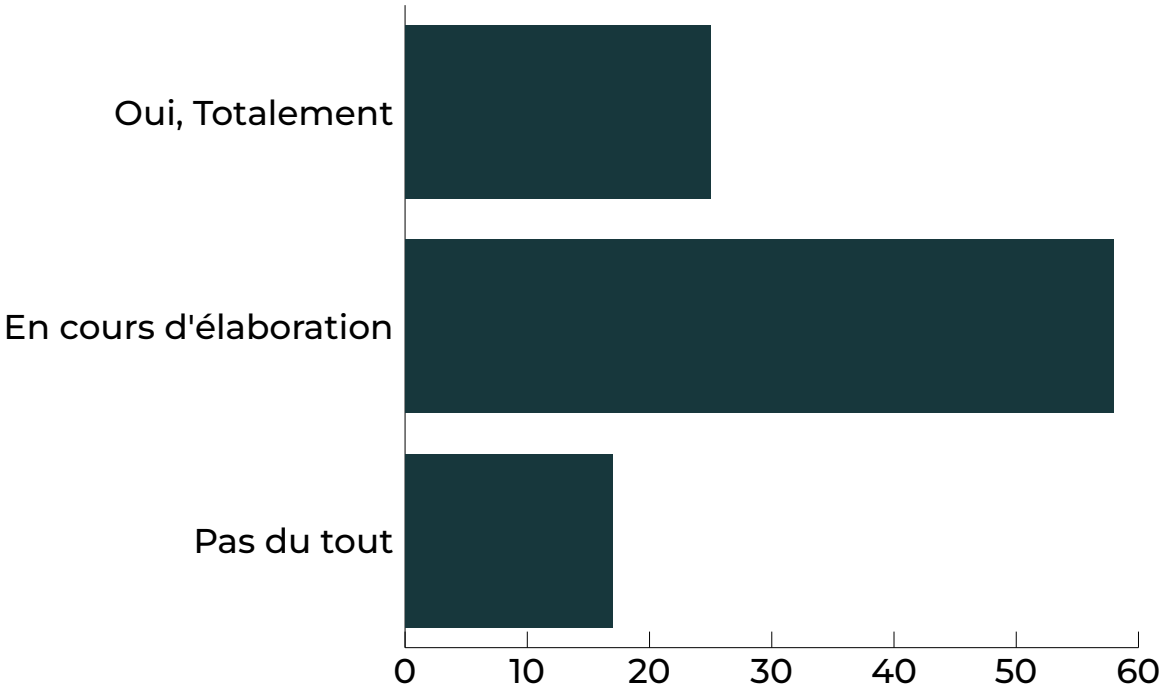
- **Q36 : Durant les 12 derniers mois, quel est le pourcentage des collaborateurs sensibilisés aux risques cyber ?**



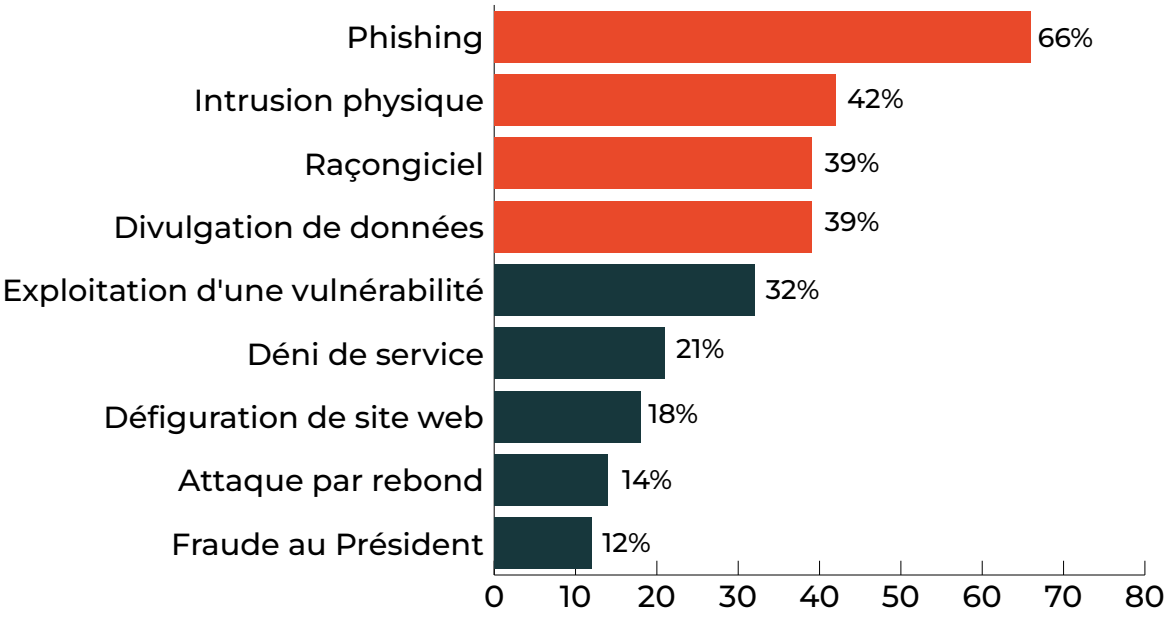
28%

des **entreprises interrogées estiment que plus de 80% de leurs collaborateurs sont sensibilisés aux risques cyber**

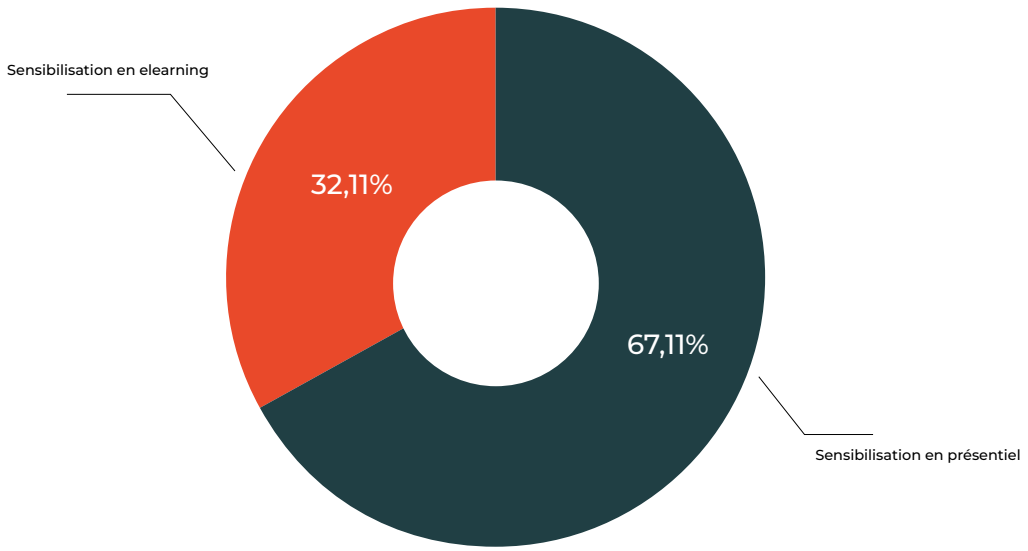
- **Q38 : Avez-vous mis en place des procédures pour tester l'application des recommandations par les salariés dans les situations concrètes comme des audits, campagnes de faux phishing, contrôles internes, etc ?**



- **Q41 : Pour quelle attaque avez-vous une fiche réflexe rédigée ou en cours de rédaction ?**

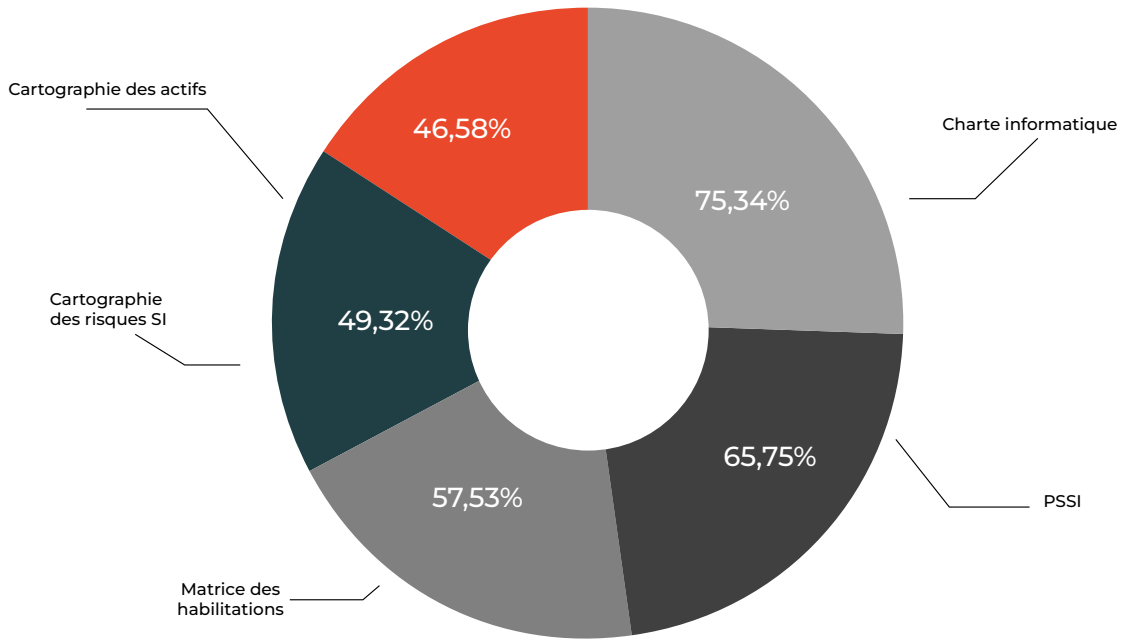


- **Q42 : Quel mode de sensibilisation utilisez-vous**

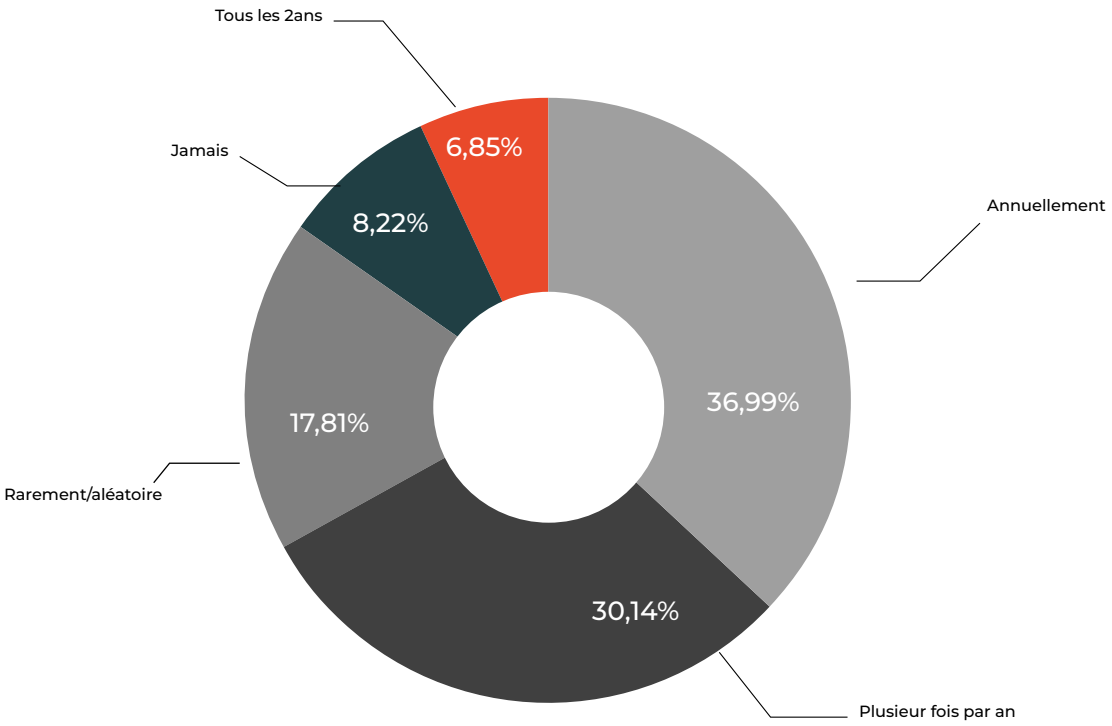


Gouvernance de la sécurité

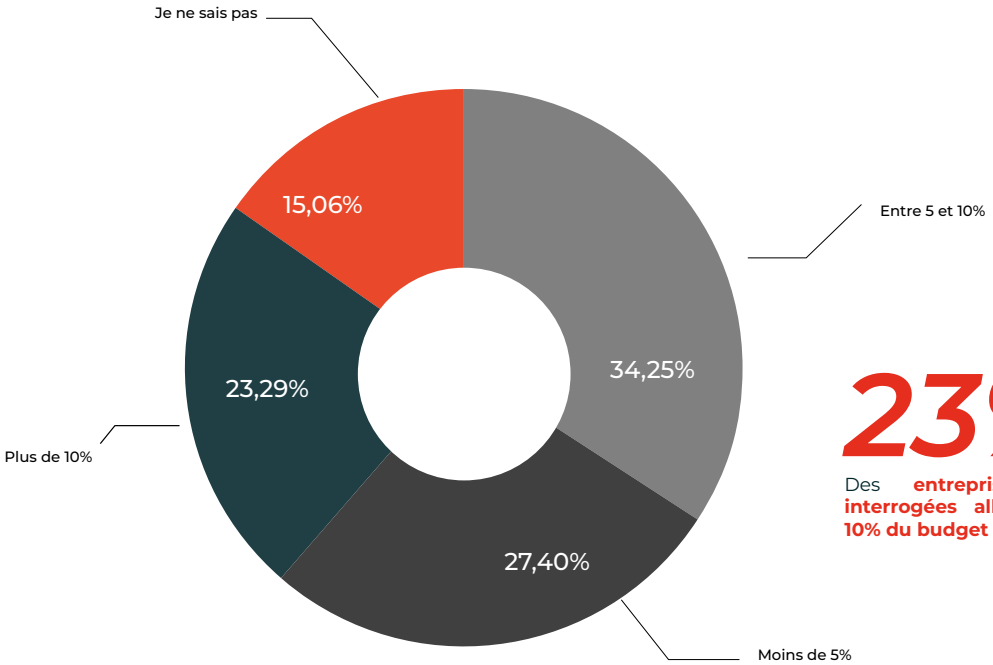
- **Q43 : En matière de gouvernance de la sécurité dans votre entreprise, les documents suivants sont-ils rédigés, validés et publiés ?**



- ## Q44 : A quelle fréquence les risques cyber de votre organisation sont-ils réévalués ?



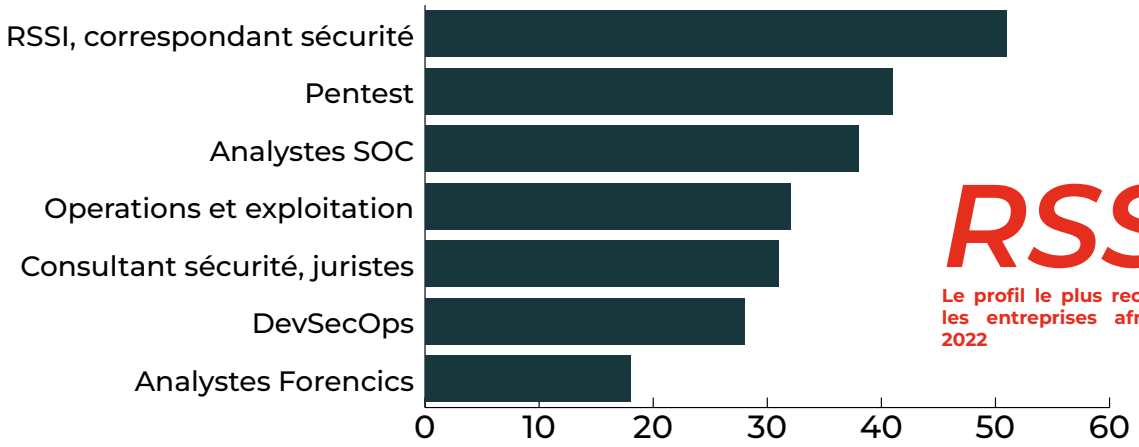
- ## Q45 : Dans votre entreprise, quelle part du budget SI est consacrée à la sécurité ?



23%

Des **entreprises africaines interrogées allouent plus de 10% du budget à la sécurité SI**

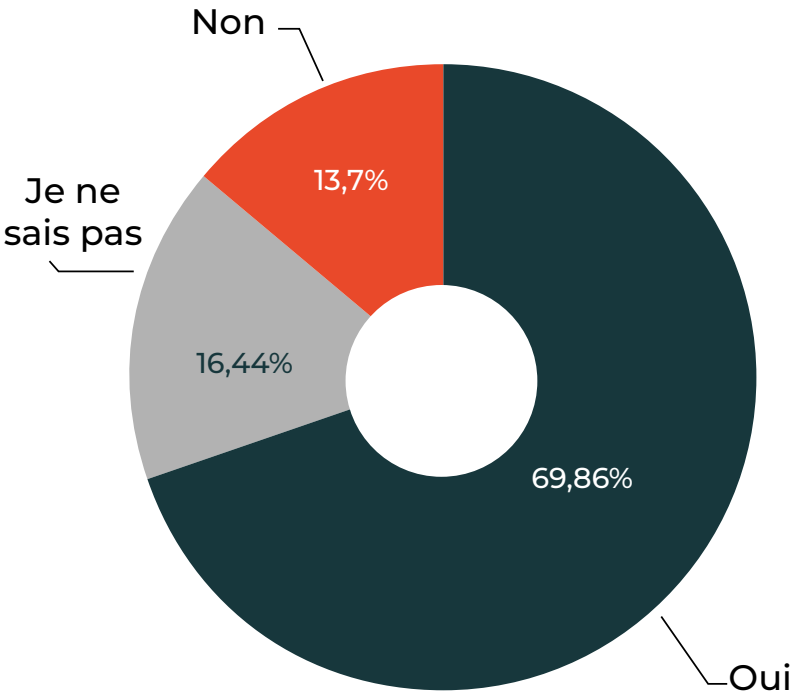
- **Q48 : Selon votre position actuelle, quel est le métier de la SSI dont a besoin votre entreprise ?**



RSSI

Le profil le plus recherché par les entreprises africaines en 2022

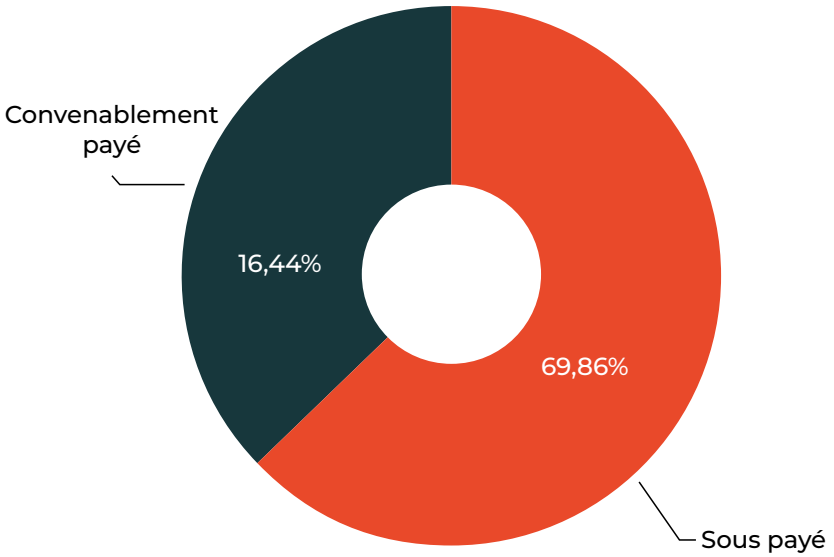
- **Q49 : Constatez-vous une pénurie de profils en SSI entrainant des difficultés de recrutement ?**



70%

Des entreprises africaines interrogées confirment une pénurie des profils en SSI.

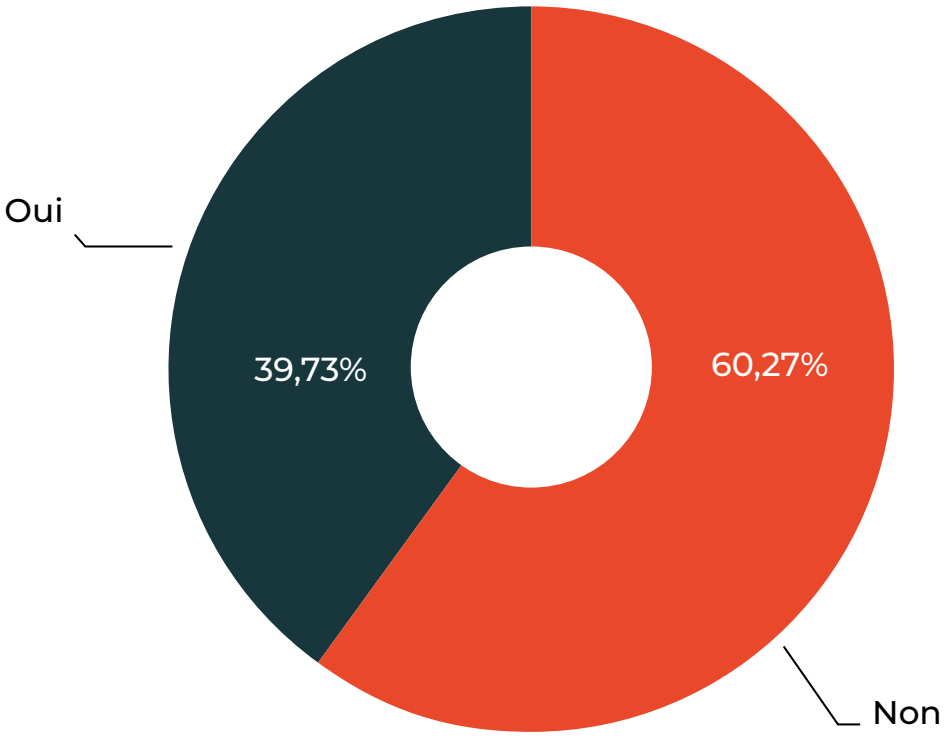
- Q51 : D'après vous, en matière de rémunération dans votre entreprise, le RSSI est...



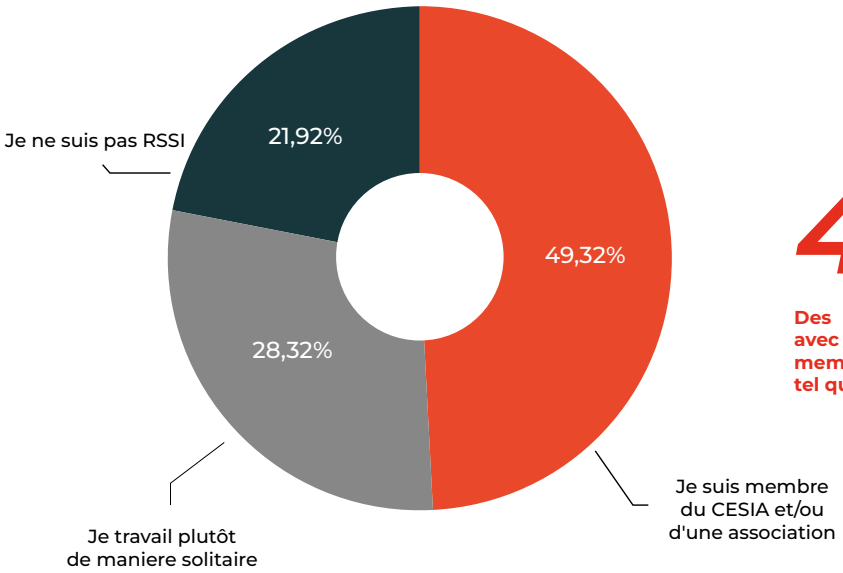
63%

Des répondants estiment que le poste de RSSI est sous rémunéré en Afrique.

- Q53 : Disposez-vous d'un plan de contrôle formalisé ?



- **Q54 : Dans votre organisation et en tant que RSSI, avez-vous la possibilité d'échanger avec d'autres RSSI ? (En dehors de votre entreprise)**



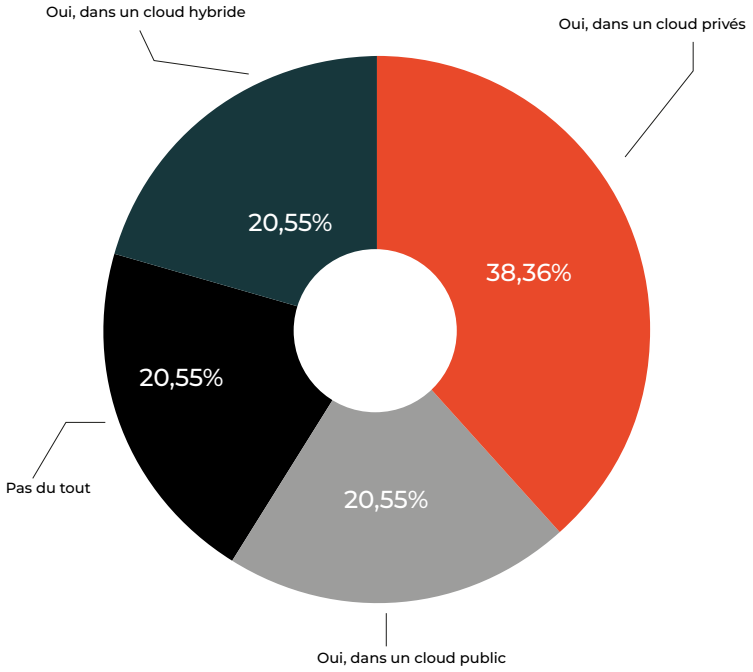
49%

Des RSSI favorisent l'échangent avec la communauté en étant membre des réseaux professionnels tel que le CESIA

Les besoins à moyen / long terme en Afrique

Le CLOUD en Afrique

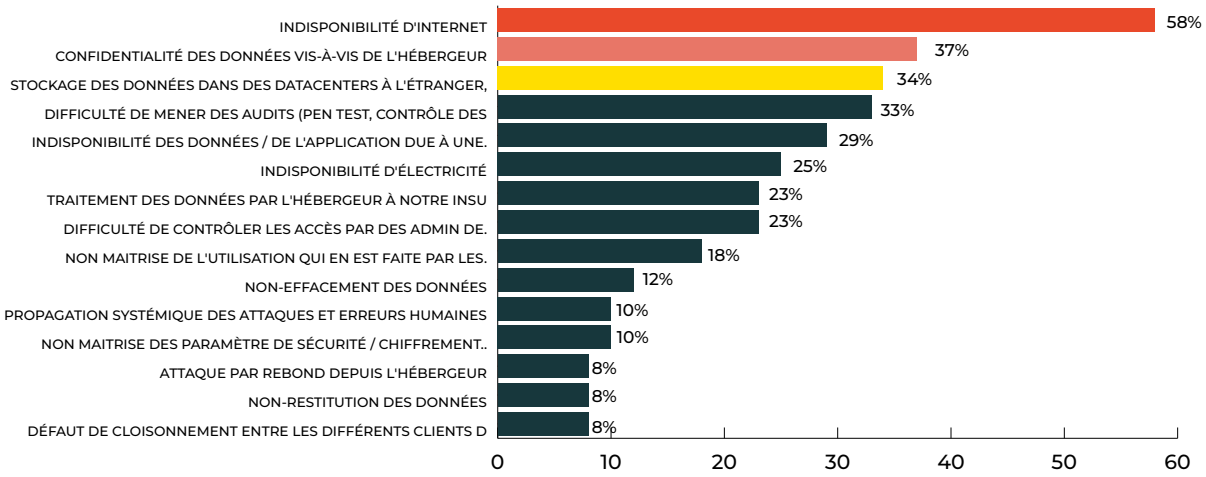
- **Q55 : Certaines données de votre entreprise sont-elles stockées dans le Cloud ?**



42%

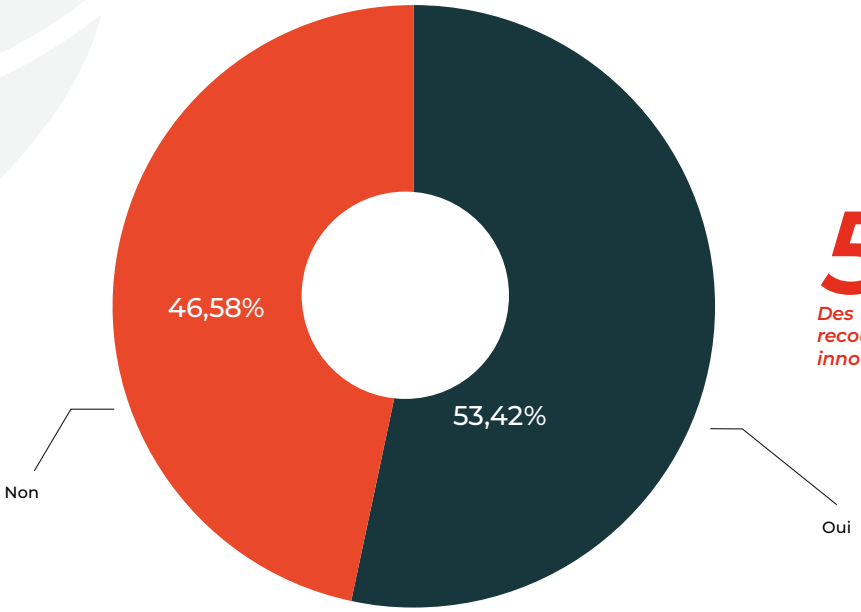
des entreprises africaines stockent certaines **données dans les Cloud publics ou hybride** mais restent très sceptiques face au Cloud et redoutent en **majorité (58%) une indisponibilité d'Internet.**

- **Q56 : Veuillez choisir les 3 principaux risques en ce qui concerne l'utilisation du Cloud ?**



Start Up

- **Q58 : Avez-vous recours aux solutions innovantes des start up ?**

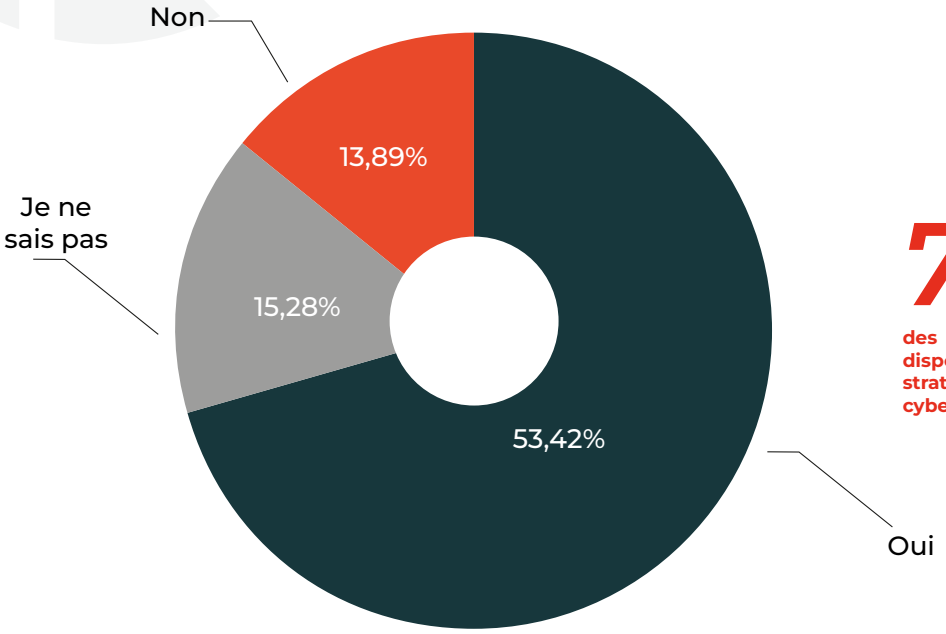


53%

Des organisations ont recours aux solutions innovantes des starts-up

Ouverture

- **Q59 : Existe-t-il une stratégie nationale de cybersécurité dans votre pays ?**



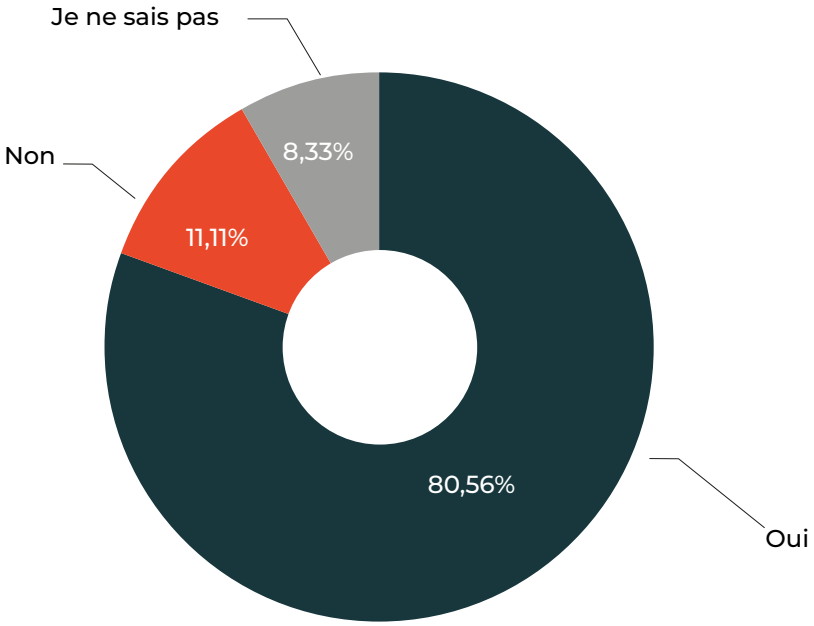
70%

des pays en Afrique disposent d'une stratégie nationale de cybersécurité.

- **Q60 : Existe-t-il une régulation ou un cadre légal relatif à la cybersécurité dans votre pays ?**

80%

des pays en Afrique ont un cadre légal relatif à la cybersécurité.



Rendez vous sur notre site

www.lecesia.com