CESIA

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

4ÈME ÉDITION

BAROMÈTRE
DE LA CYBERSÉCURITÉ
EN AFRIQUE

2024

www.lecesia.com

Table des **MATIÈRES**

Éditorial 04

A propos du CESIA 05

Mot du président 06

Les objectifs du Baromètre de la cybersécurité en Afrique 07

Notre méthodologie 08

Nos partenaires 09

Les messages clés 11

- L'activité cybercriminelle spectaculairement à la hausse 11
- La cybersécurité, une priorité en Afrique 11
- Le facteur humain 11

Les actions prioritaires à court/moyen terme 13

- Organisation de la riposte 13
- Une sensibilisation efficace des collaborateurs et des formations efficientes 13
- Connaître et comprendre son environnement 13

Analyse des résultats 15

- Chapitre 1 : Le profil des participants 15
- Chapitre 2 : Exposition des entreprises africaines aux cyberattaques 17
- Chapitre 3 : Le dispositif de sécurité technique des entreprises 19
- Chapitre 4 : L'humain au cœur de la cybersécurité 22
- Chapitre 5 : Gouvernance de la sécurité 24
- Chapitre 6 : IA – Intelligence Artificielle & Ouverture 26

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 2024** 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 au 31 janvier 2024 rend compte de l'état et de 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 en cybersécurité, 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. Cependant, plus d'une entreprise sur deux ne dispose d'un programme de cyber-résilience. Si les professionnels de la cybersécurité en Afrique jugent avoir un meilleur positionnement dans leurs entreprises grâce au sponsoring du top management et une bonne visibilité du Responsable de Sécurité des Systèmes d'Information (RSSI) quand il existe, ils notent tout de même un manque de formation, de sensibilisation, de ressources, de 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 et/ou ayant un intérêt pour le développement du secteur sur le continent.

Cette année, **le CESIA** compte 180 membres présents dans 21 pays en Afrique avec pour objectif de :

- **Promouvoir et valoriser les métiers de la sécurité de l'information à travers un code d'éthique adopté par les membres de l'Association ;**
- **Participer aux démarches nationales et être force de proposition sur des textes règlementaires, guides et autres référentiels ;**
- **Permettre 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 tout autres évènements publics.**

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

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, plusieurs événements marquants dans les pays ont permis d'accélérer leur transformation digitale. En particulier, dans certains pays, des cyberattaques abouties sur des infrastructures critiques ont permis de confirmer la nécessité vitale de les sécuriser.

En 2023, les cybercriminels ont poursuivi l'amélioration de leur capacité facilitée entre autres par l'Intelligence Artificielle (IA). Le gain financier ou l'espionnage reste les menaces majeures de l'année.

Les entreprises africaines de toute taille et de tous 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. Cela passe par un travail collectif avec l'ensemble des acteurs, publics et privés qui 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 partage 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 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.

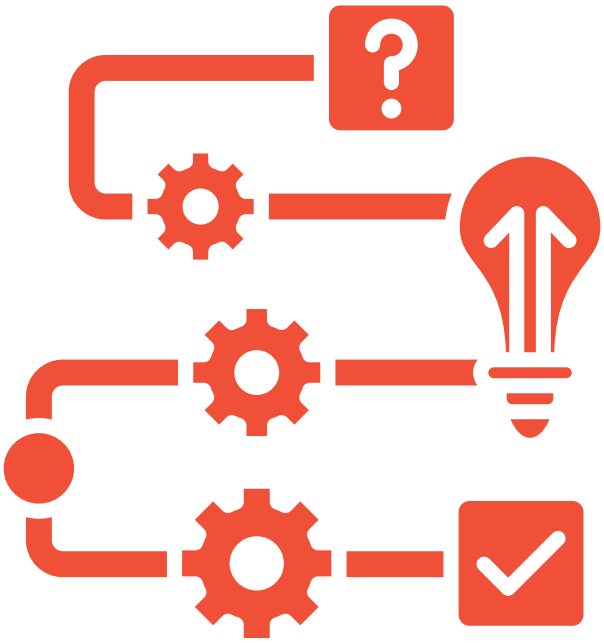
LES OBJECTIFS DU BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE

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 des lieux sur les enjeux de la cybersécurité en Afrique et sa perception au sein des entreprises 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 **450 participants** dans 15 pays d'Afrique qui sont membres du CESIA ou professionnels de la sécurité numérique, membre du réseau de nos partenaires.

87% des participants sont des décideurs (DSI, Directeur Technique, Directeur cybersécurité, DSSI, RI, RSI, RSSI, CISO, Responsable SOC/CERT, CSSI ou référent sécurité).

13% des participants sont consultants séniors en SSI ou Administrateur Sécurité.

Notre enquête s'est déroulée du **1er** au **27 janvier 2024.**

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

NOS PARTENAIRES

DSTrust est le 1er cabinet de conseil basé au Gabon, spécialisé en sécurité numérique, cybersécurité et continuité d'activité.

Nous sommes à la pointe de la cybersécurité avec un rayonnement international sur trois (3) piliers : **Le conseil, la prévention / formation / sensibilisation et la sécurité offensive.** Notre démarche est basée sur la culture de la rigueur et le pragmatisme avec un engagement sur le résultat. Nos collaborateurs sont expérimentés et formés aux standards internationaux et, nos clients sont des entreprises de toutes tailles : les grandes entreprises mais aussi les TPE et les PME.

Visitez notre site Internet : **www.dstrust.ga**

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, dans le monde et organise plusieurs activités spécifiques (conférences, Webinaires, Journée d'études et de réflexions). - www.cybersecuritymag.africa

CyberSpector SAS est une entreprise innovante dans le domaine de la cybersécurité, la cyber-intelligence et de l'ingénierie des systèmes, des projets et avant-projet numérique qui a été créée en mars 2021.
CyberSpector est spécialisé en cybersécurité ainsi que dans le développement et l'intégration des systèmes d'information, précisément en ingénierie système, en cyber-intelligence, cyber-résilience, à la protection des données et l'accompagnement à la mise en place de stratégie et gouvernance de la cybersécurité aux bénéfices des grandes entreprises, mais aussi des PME et TPE.
Visitez notre site Internet : **www.cyberspector.com**

TECHSO GROUP est un acteur de la cybersécurité en Afrique et en Europe. La résilience cybersécurité de nos clients est notre raison d'être !
Son offre est articulée autour des thématiques suivantes : Conseil en sécurité, Développement et mise en œuvre des architectures sécurisées, Mise en place de solutions cybersécurité, Accompagnement à la conformité par rapport aux projets réglementaires (PCI-DSS, CSP SWIFT, ISO 27001, DNSSI et loi 05-20, GDPR ... etc).
Se faire accompagner par TECHSO GROUP, c'est à la fois capitaliser sur les expériences des collaborateurs, leur réactivité, leur créativité et une forte capacité à se réinventer à chaque mission.
www.techsogroup.com

LES MESSAGES CLÉS

L'activité cybercriminelle spectaculairement à la hausse

74% des organisations en Afrique déclarent avoir subi au moins une cyberattaque en 2023 contre 56% en 2022. Cette augmentation spectaculaire en seulement douze (12) mois serait due aux déclarations qui sont de plus en plus nombreuses et à plus de participation des déclarants.
Après le pic connu en 2020, cet indicateur est le deuxième plus élevé sur les quatre (4) dernières années (82% et 2020, 64% en 2021, 56% en 2022 et désormais 74% en 2023). Les conséquences sont considérables sur les activités de l'entreprise : Interruption des activités de l'organisation, vol d'information stratégique, fraude financière, atteinte à la confidentialité et/ou à l'image de marque.

Pour la quatrième année consécutive, le phishing reste le vecteur d'attaque privilégié et à la hausse soit 57% des cas (contre 51% en 2022 et 69% en 2021). L'ingénierie sociale monte à la deuxième place 35% en 2023 (contre 30% en 2022 et 28% en 2021).

Comme chaque année, les experts de la sécurité numérique en Afrique indiquent que leurs organisations ne sont pas prêtes à gérer une cyberattaque de grande ampleur dans 57% des cas contre 52% en 2021.

La cybersécurité, une priorité en Afrique

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

Pour les organisations ayant subi une cyberattaque, les causes pointées sont le manque de sensibilisation à la sécurité numérique, les erreurs de configuration et l'insuffisance des mesures de sécurité. Pour se prémunir des cyberattaques, les entreprises déploient en moyenne onze solutions techniques de sécurité : EDR, sécurisation d'accès à distance (VPN et/ou équivalent), MFA, proxy et filtrage d'URL, SIEM, SOC, Anti-DDoS, supervision de base de données, NAC et CASB ; en plus des antivirus.

Cela dit, 56% des entreprises ne disposent pas de programme de cyber-résilience et 46% ne disposent pas de SOC.

Enfin, les entreprises n'ont toujours pas recours aux solutions innovantes issues des strat-up et dans la très grande majorité des cas 53%, contre 46% l'année dernière pointent le manque d'opportunité, le manque de connaissance des offres, le manque de maturité ou pérennité des offres.

Le facteur humain

Un indicateur à la hausse, 57% des entreprises en Afrique disposent d'un plan annuel de sensibilisation, mais 60% de ces organisations n'ont pas mis en place un dispositif pour tester l'application des recommandations de sécurité (audit, campagnes de faux phishing, etc.)

63% des organisations n'ont pas recours aux prestataires externes pour sensibiliser leurs collaborateurs.

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 riposte

Compte tenu de la recrudescence des cyberattaques sur les organisations africaines et de l'absence des ressources en cybersécurité, nous recommandons de mettre en place un dispositif efficient de gestion de crise cyber.
Cela passe par la désignation d'un référent sécurité ou un Responsable de Sécurité des SI (RSSI) qui doit se généraliser à tous les secteurs d'activités.
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 :

- Mise en place des fiches reflexe,
- Plan de sensibilisation de la cellule de crise,
- Organisation des exercices de gestion de crise cyber.

Le RSSI doit être formé et disposer des moyens financiers et organisationnels pour exercer sa fonction.
Afin de renforcer le travail collectif, le texte RSSI ou le référent sécurité doit avoir la possibilité d'échanger avec ses pairs. 60% des RSSI s'appuient sur l'expertise interne de leur organisation.

Une sensibilisation efficace des collaborateurs et des formations efficientes

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.

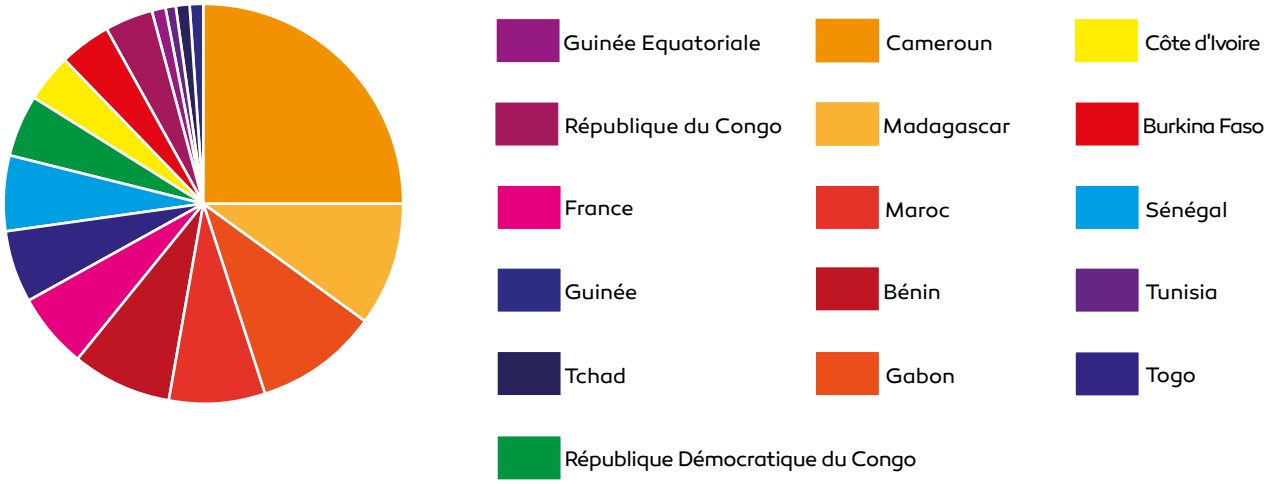
Pour une sensibilisation efficace, le programme de sensibilisation doit définir des objectifs. Ces objectifs doivent être mesurables et trouver un juste équilibre entre le niveau de compétence visé pour chaque groupe de salariés et le temps total d'apprentissage nécessaire pour les amener à ce niveau.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

Connaître et comprendre son environnement

Nous recommandons très fortement de faire un état des lieux de son organisation.
Il est possible de piloter la sécurité de son entreprise par les risques en mettant en place une cartographie des risques et en la faisant valider par le comité de direction.

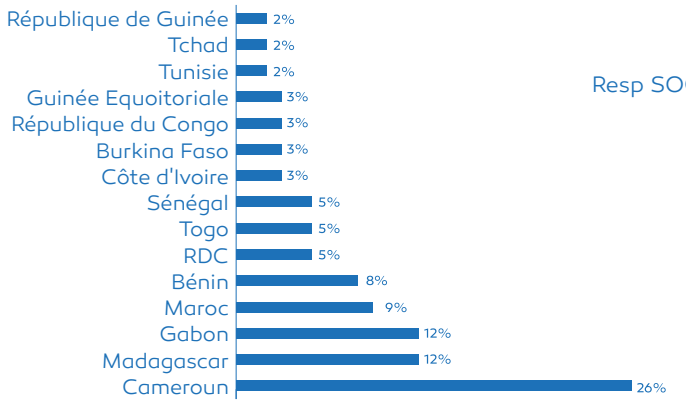
ANALYSE DES RÉSULTATS

Chapitre 1 : Le profil des participants

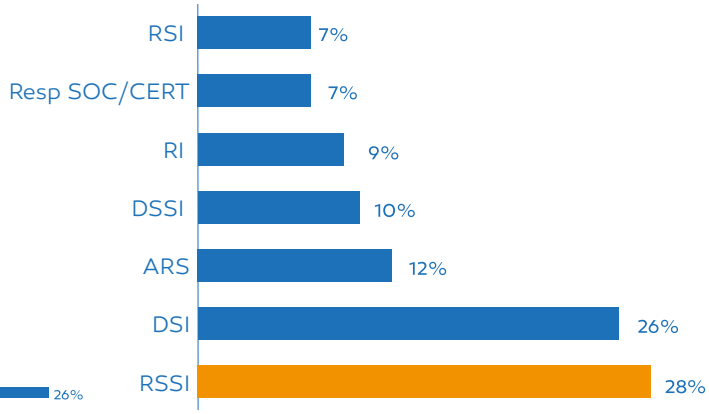


15 pays ont participé à la 4ème édition du baromètre de la cybersécurité en Afrique. Le podium est occupé par : CM **Cameroun** qui garde la 1ère place ; MG **Madagascar** qui rentre dans le top 3 et GB **Gabon** en 3ème position.

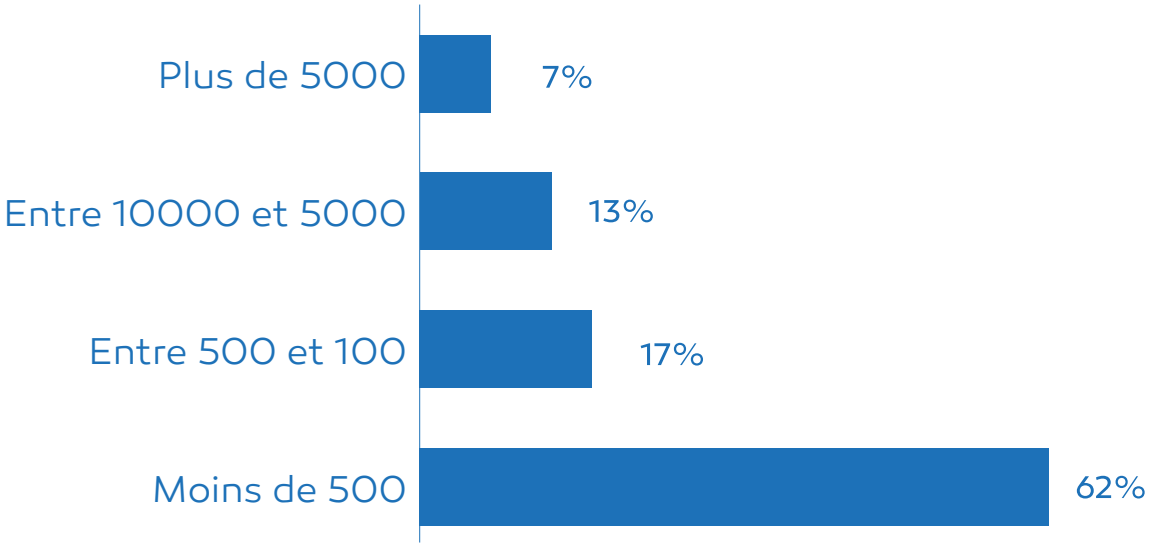
Taux de participation par pays



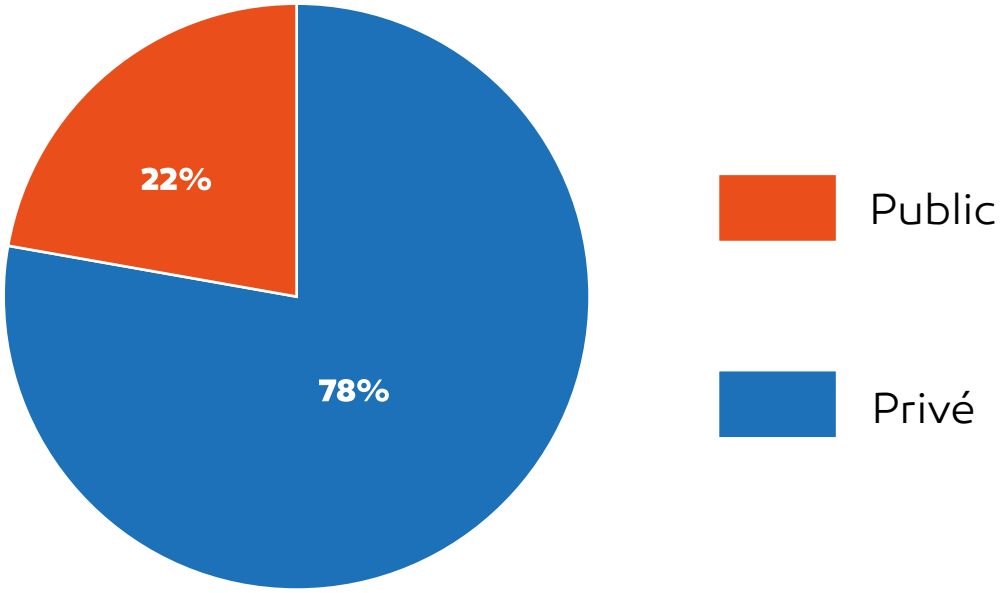
Fonction



La taille des entreprises



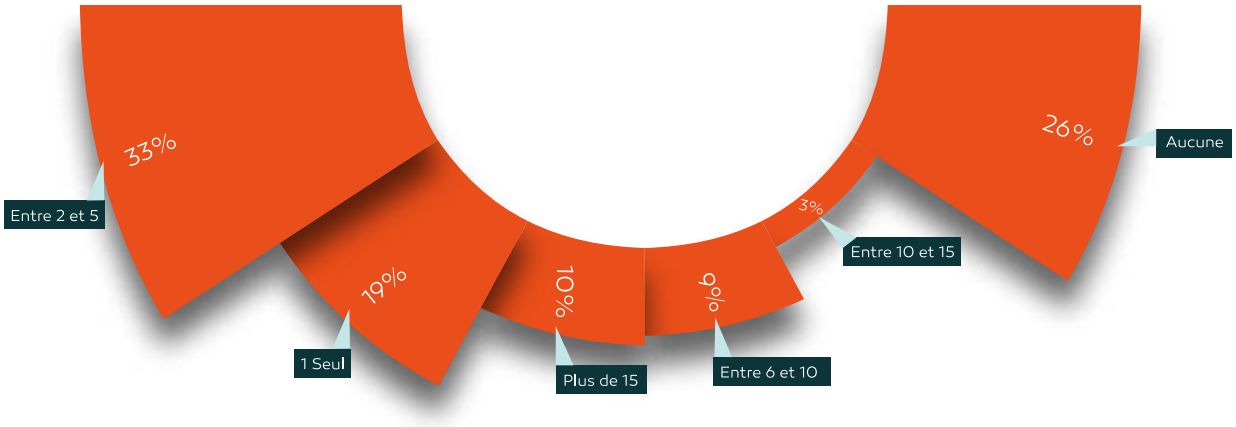
Secteur d'activité



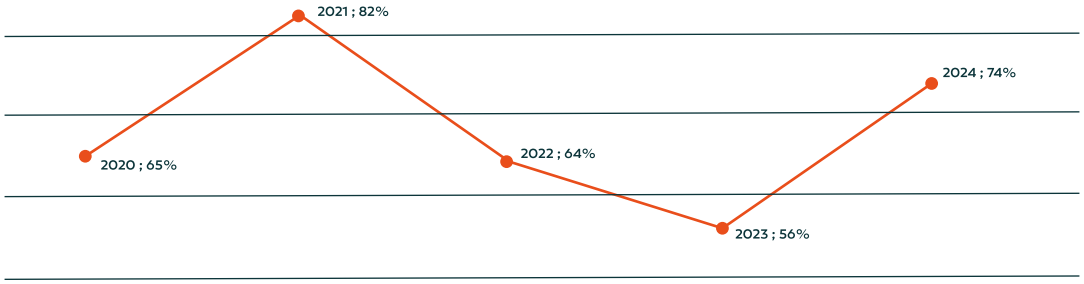
Tous les secteurs d'activités sont représentés dans cette édition 2024.
Dans le temps, les secteurs bancaires et les nouvelles technologies sont particulièrement ciblés.

Chapitre 2 : Exposition des entreprises africaines aux cyberattaques

Cette année, 74% des organisations africaines ont subi au moins une cyberattaque aboutie. Une hausse spectaculaire de 18% par rapport à l'année dernière. Les experts s'accordent à dire que cette tendance va rester haute les prochaines années.



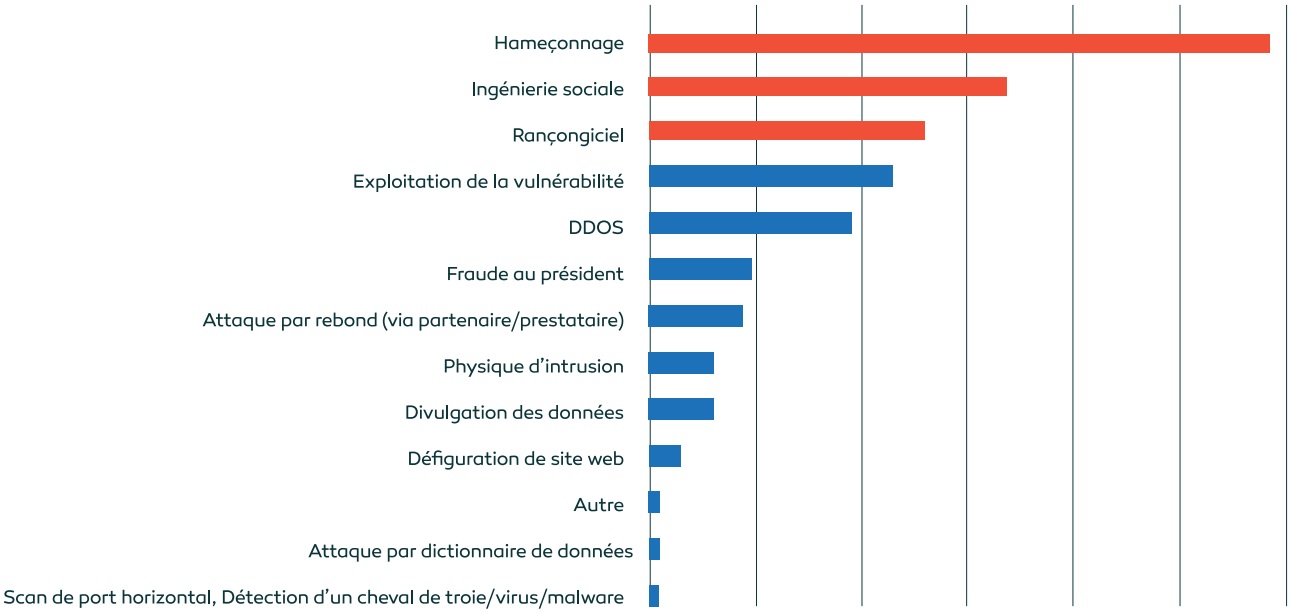
Combien de cyberattaques ont été constatées dans votre organisation au cours des 12 derniers mois ?



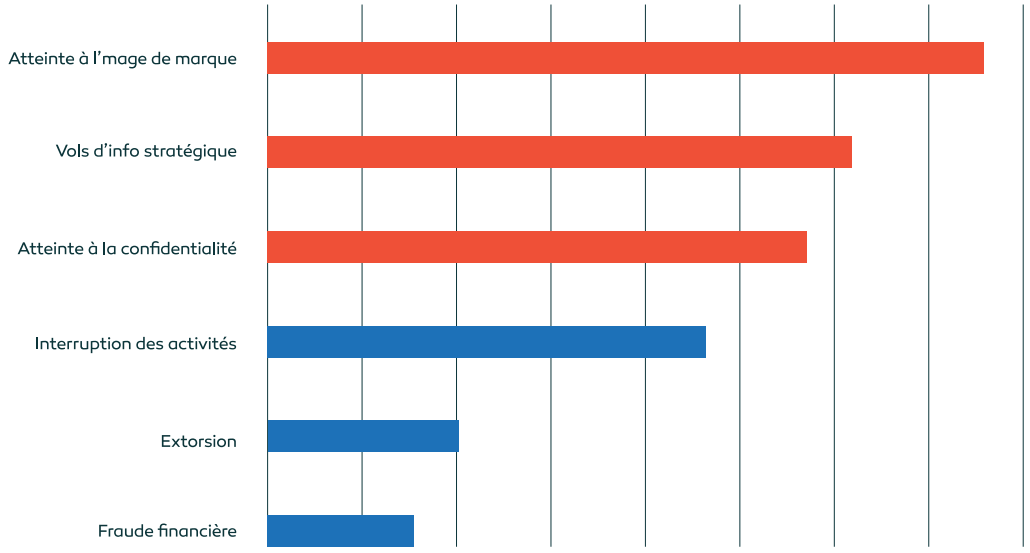
74% Des organisations ont subi une cyberattaque en 2022.

La 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.

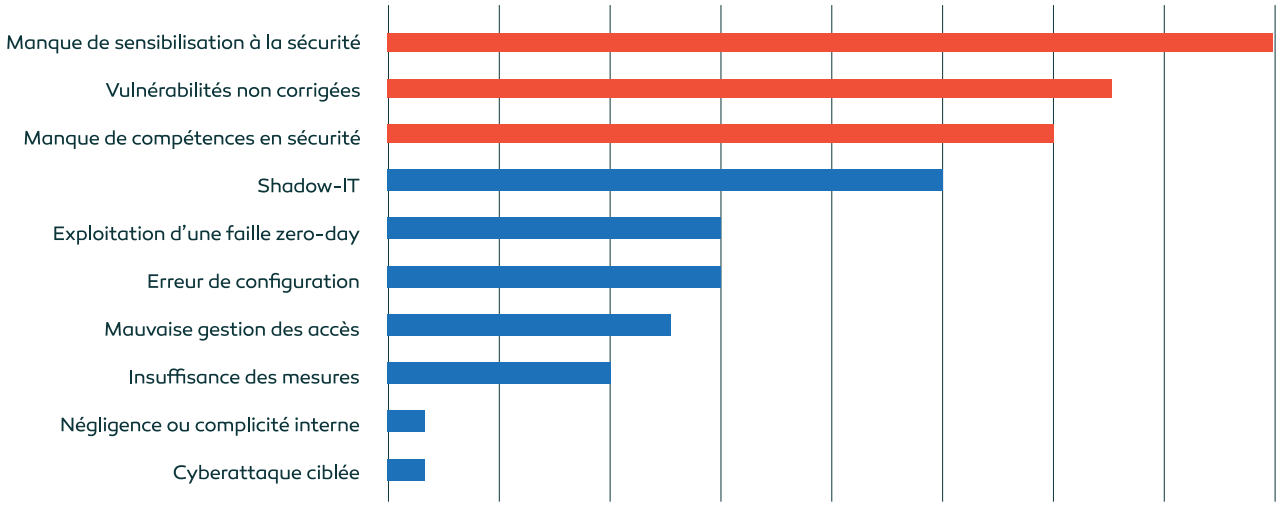
Il s'agit de quel type d'attaque ?



Quelles ont été les conséquences de cette/ces attaque(s) ?

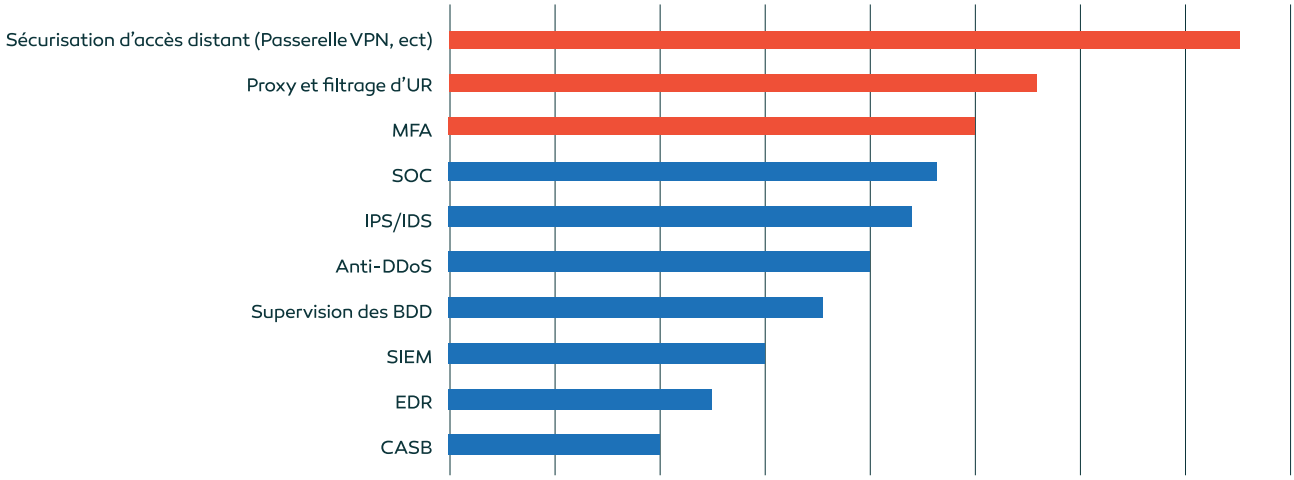


Classement des causes de cette/ces attaques



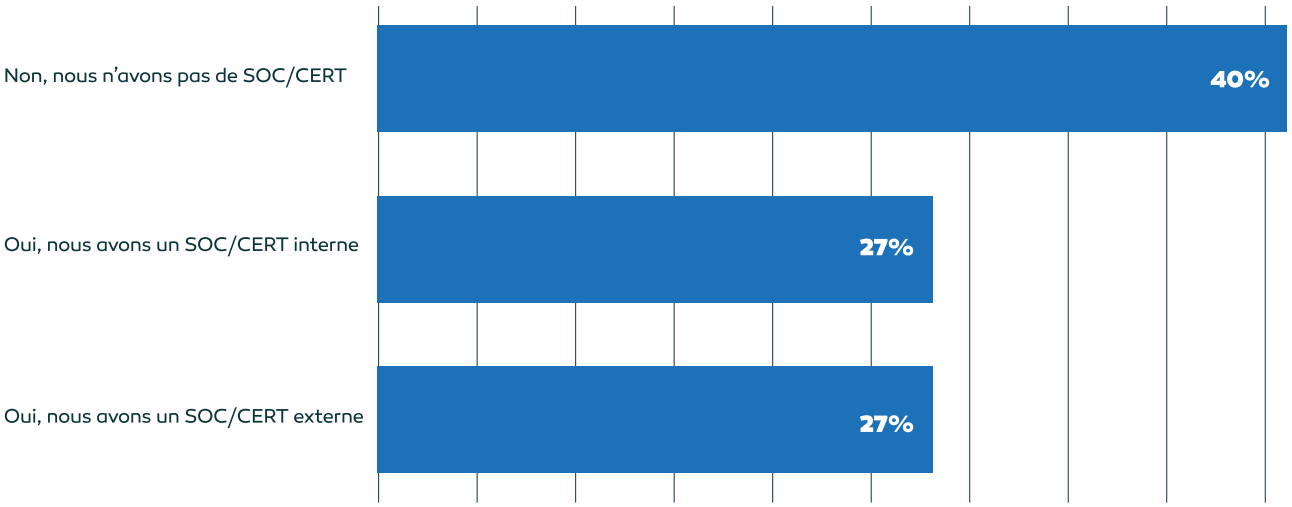
Chapitre 3 : Le dispositif de sécurité technique des entreprises

Les éléments pris en compte dans la stratégie de cybercrise



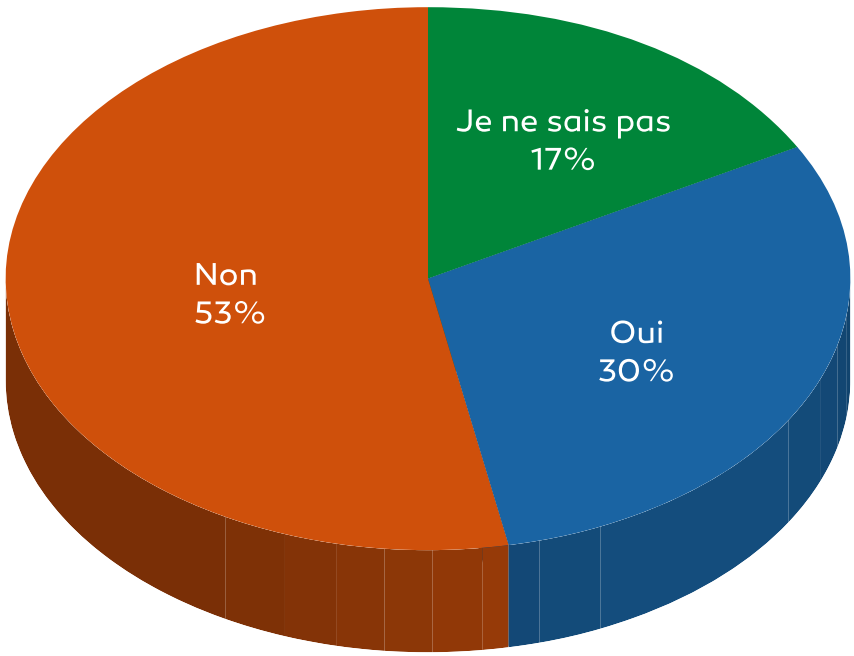
12 **Solutions techniques en moyenne pour construire la sécurité dans les organismes en Afrique**

Entreprises disposant d'un SOC/CERT ou non



Une entreprise sur deux ne dispose pas de SOC.

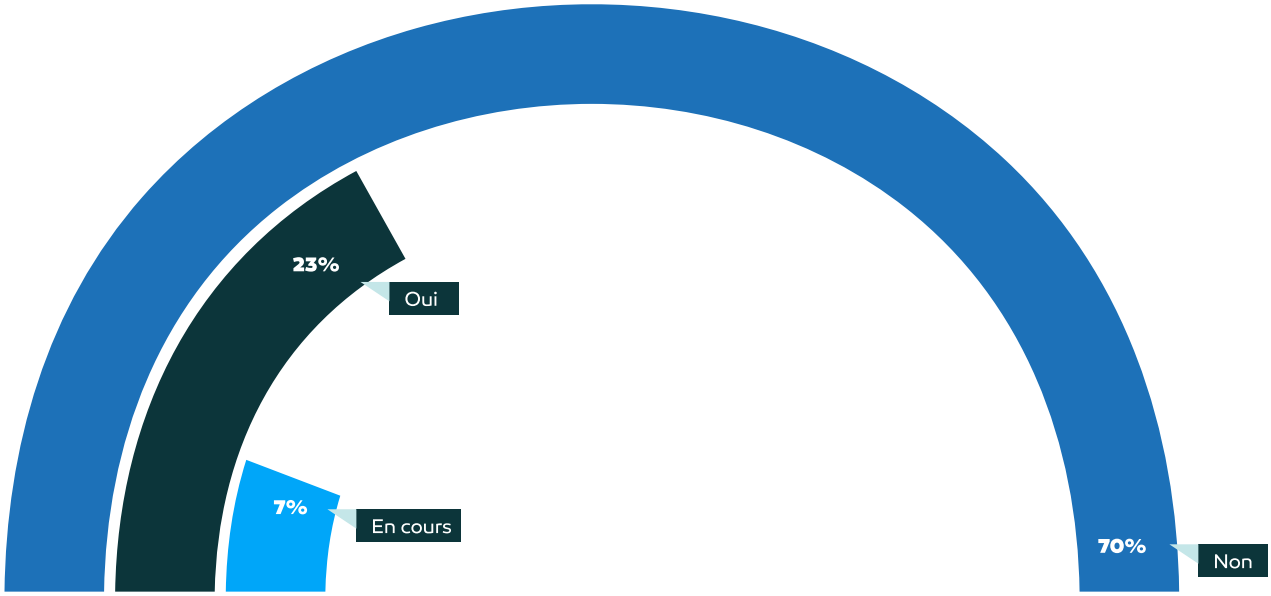
Niveau de confiance du dispositif technique de sécurité



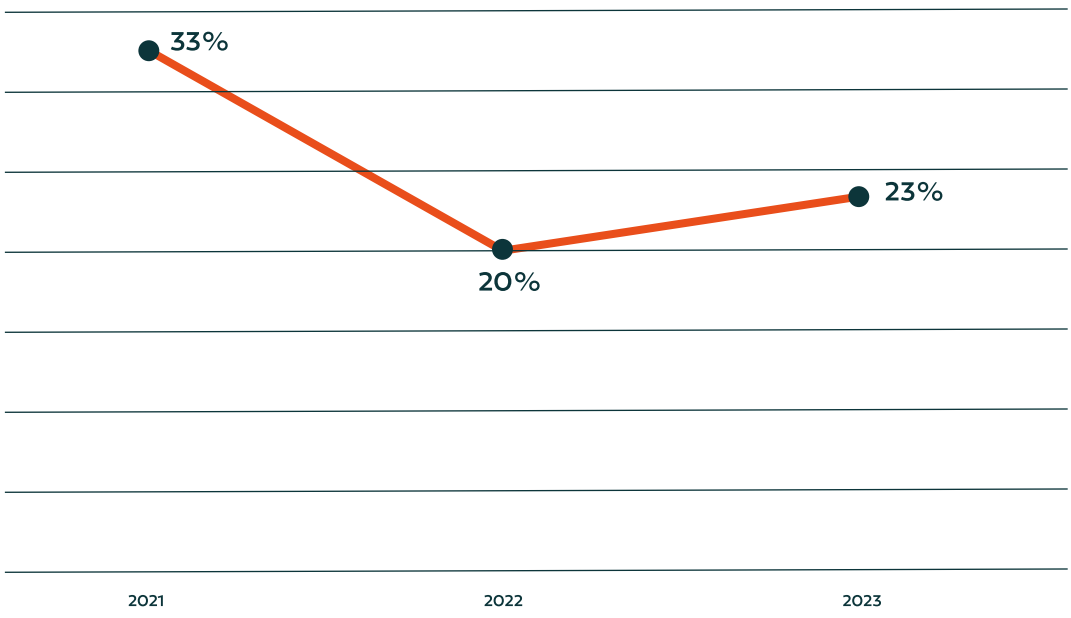
70% des référents de sécurité en Afrique n'ont pas confiance en leur dispositif de sécurité.

La cyber assurance reste un sujet très peu développé en Afrique, 77% des organismes n'ont pas souscrit à une cyber assurance.

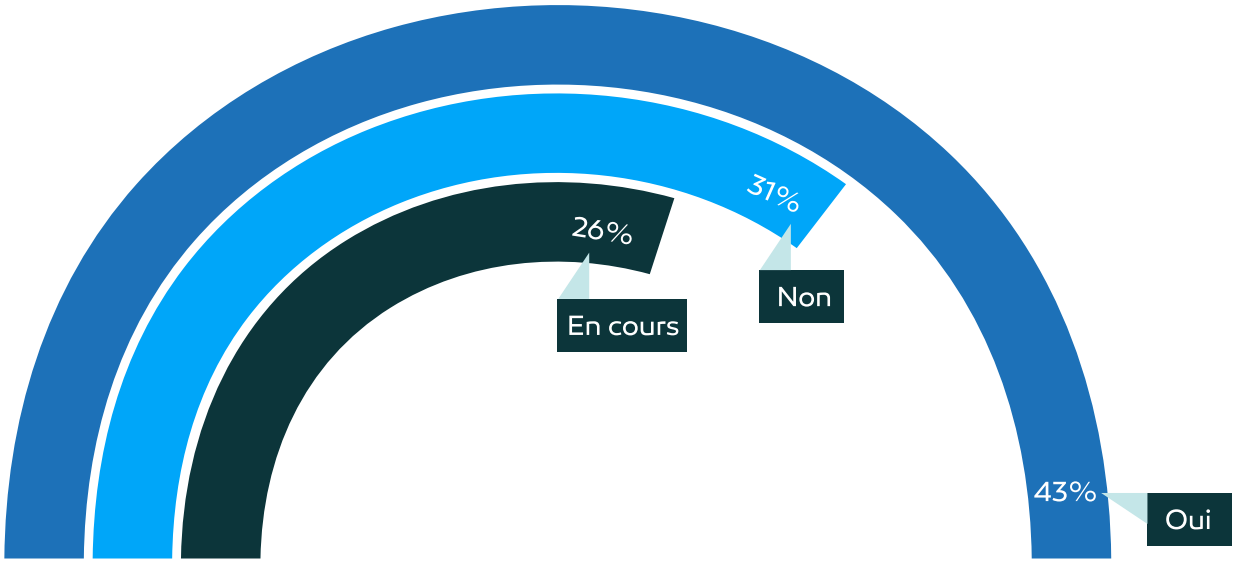
Entreprises ayant souscrit à une cyber-assurance ou non



Evolution des souscriptions aux cyber assurance dans le temps

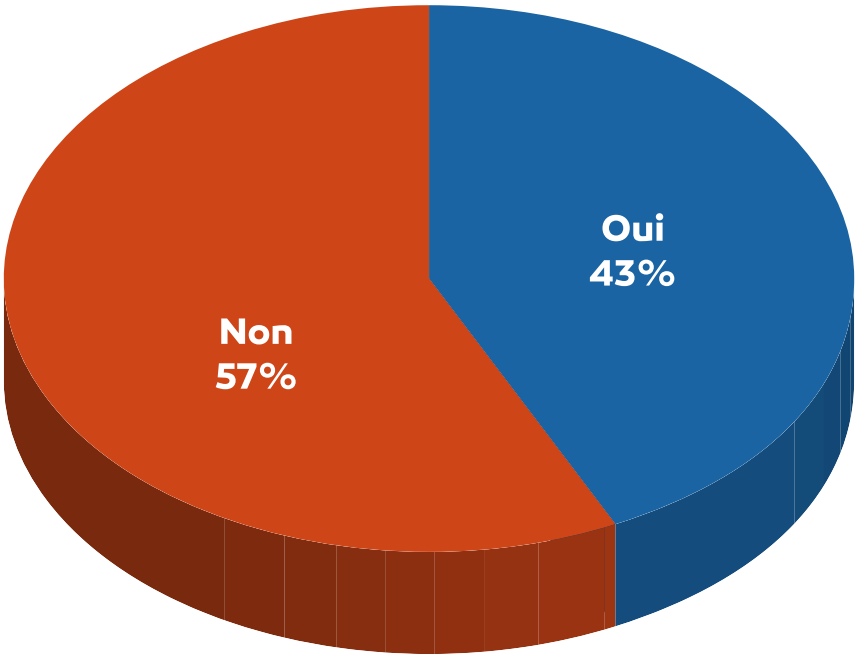


Entreprises ayant un programme de cyber résilience

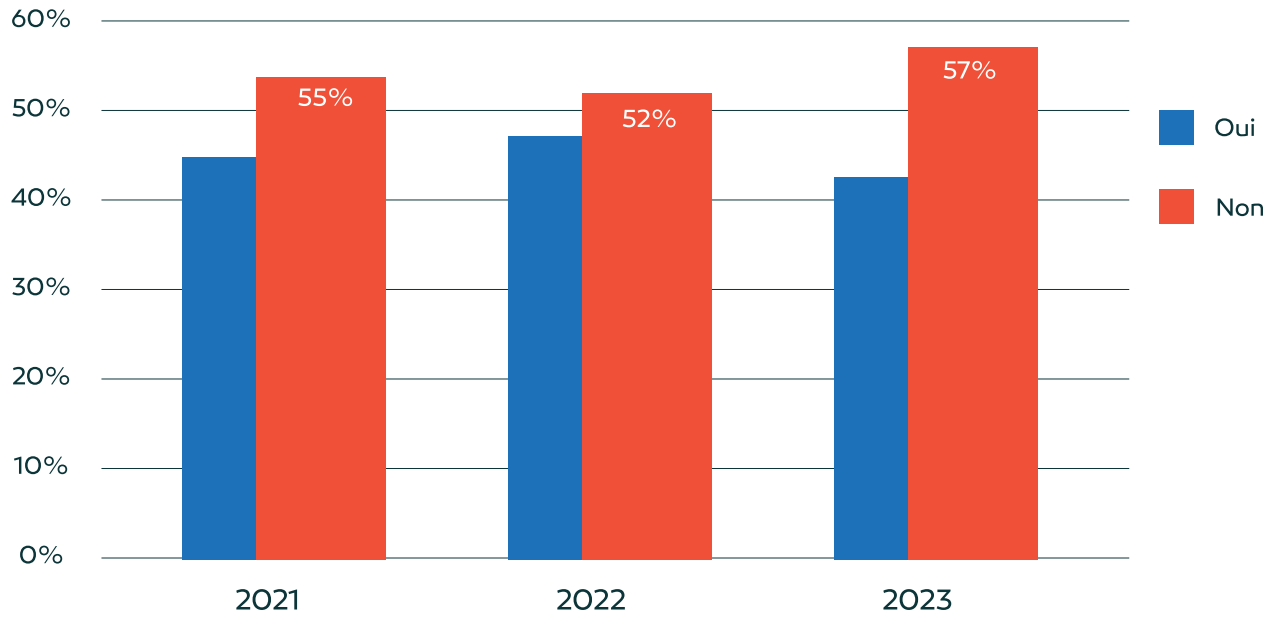


57% d'organismes ne disposent pas d'un programme de cyber résilience

Niveau de préparation des entreprises à gérer une cyberattaque de grande ampleur

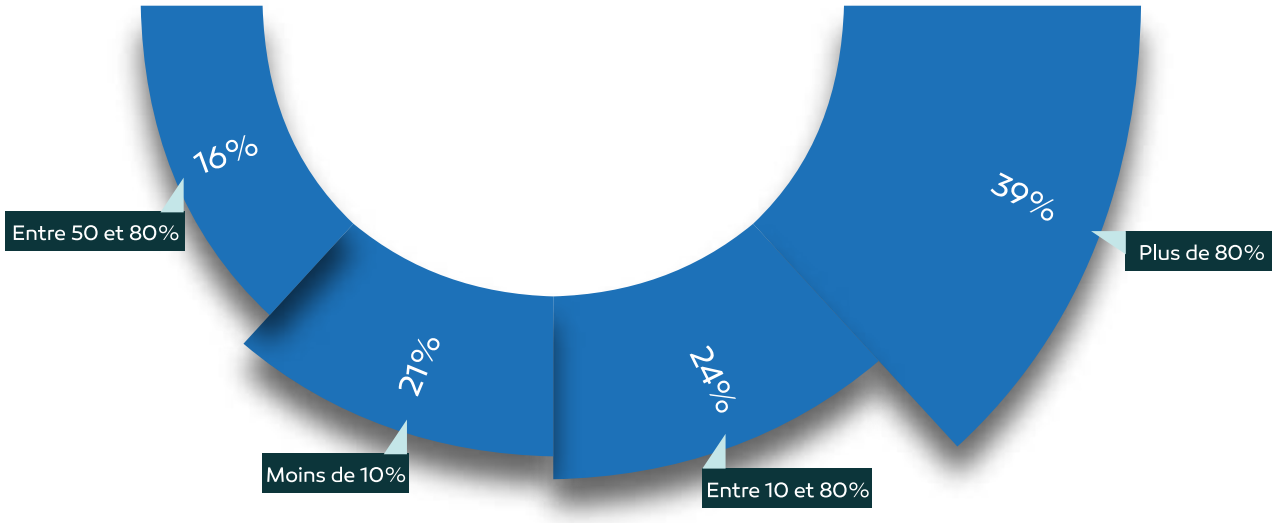


Evolution de la capacité des entreprises à gérer une cyberattaque de grande ampleur dans le temps

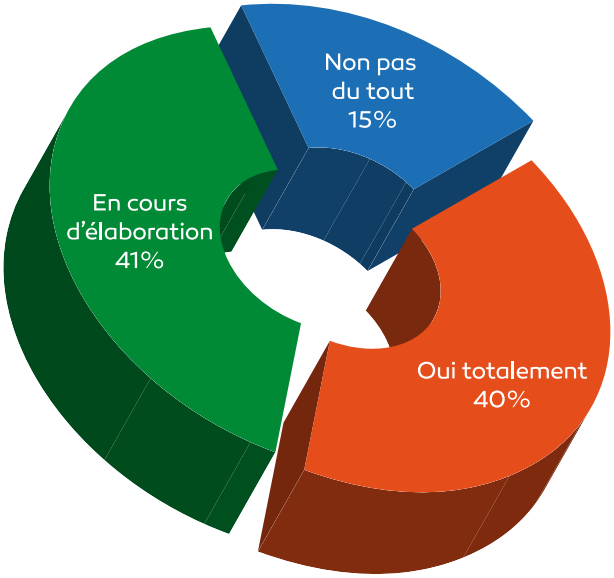


Chapitre 4 : L'humain au cœur de la cybersécurité

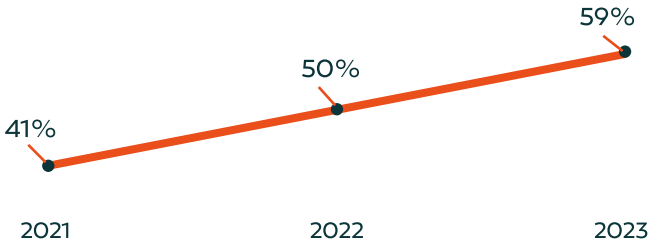
Le % des collaborateurs sensibilisés aux risques cyber durant les 12 dernier derniers mois



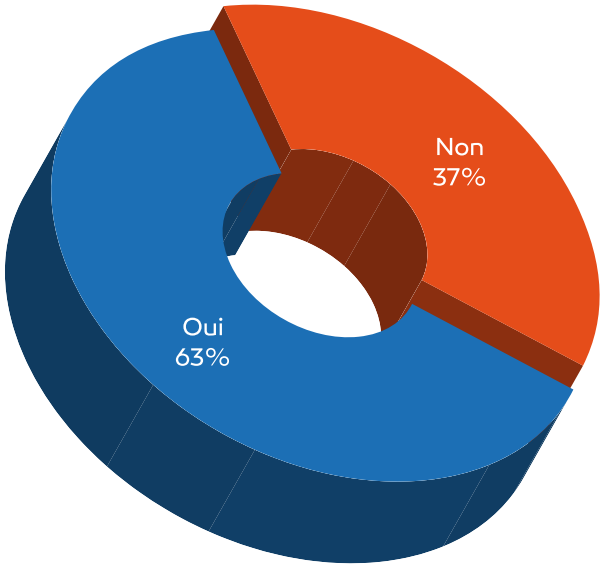
Mise en place d'un dispositif pour tester l'application des recommandations de sécurité par les salariés (audits, campagnes de faux phishing, etc.)



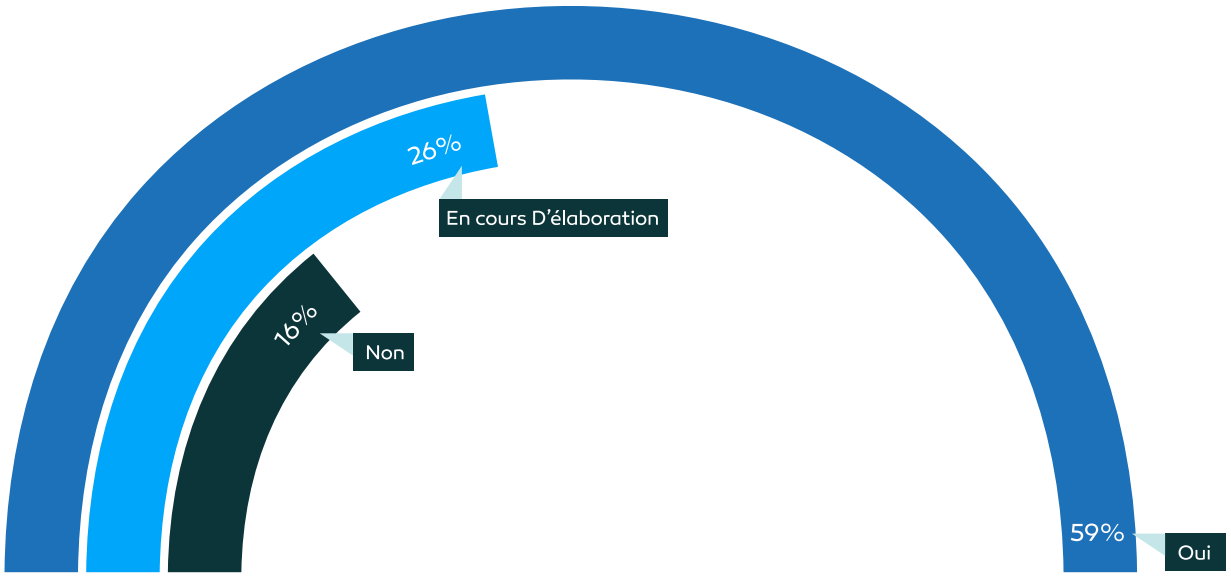
Evolution des mises en place d'un dispositif pour tester le niveau de sensibilisation des collaborateurs



Niveau de recours à des prestations externes pour sensibliser les collaborateurs

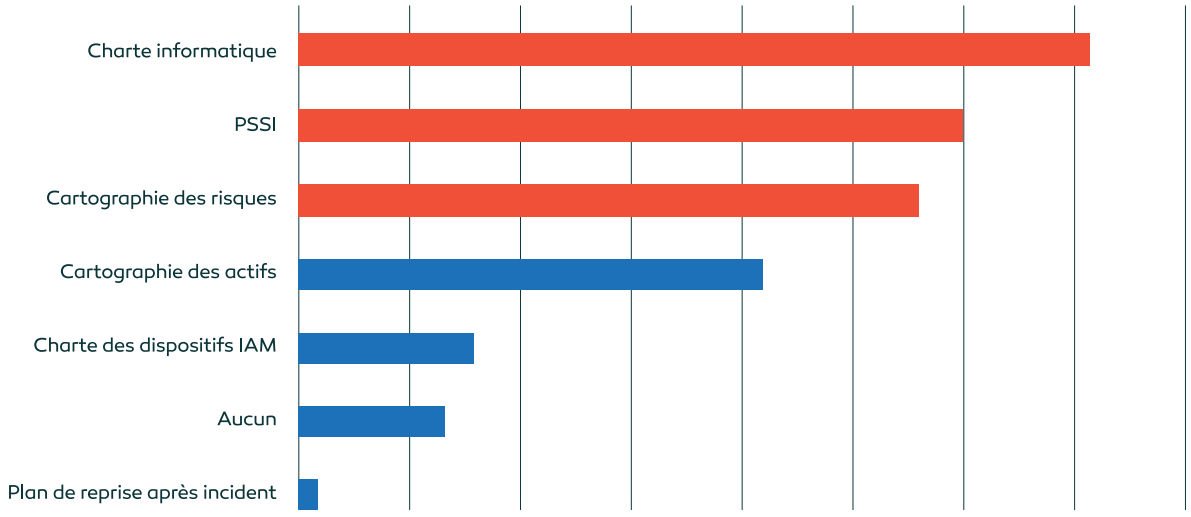


Niveau de mise en place d'un plan annuel de sensibilisation



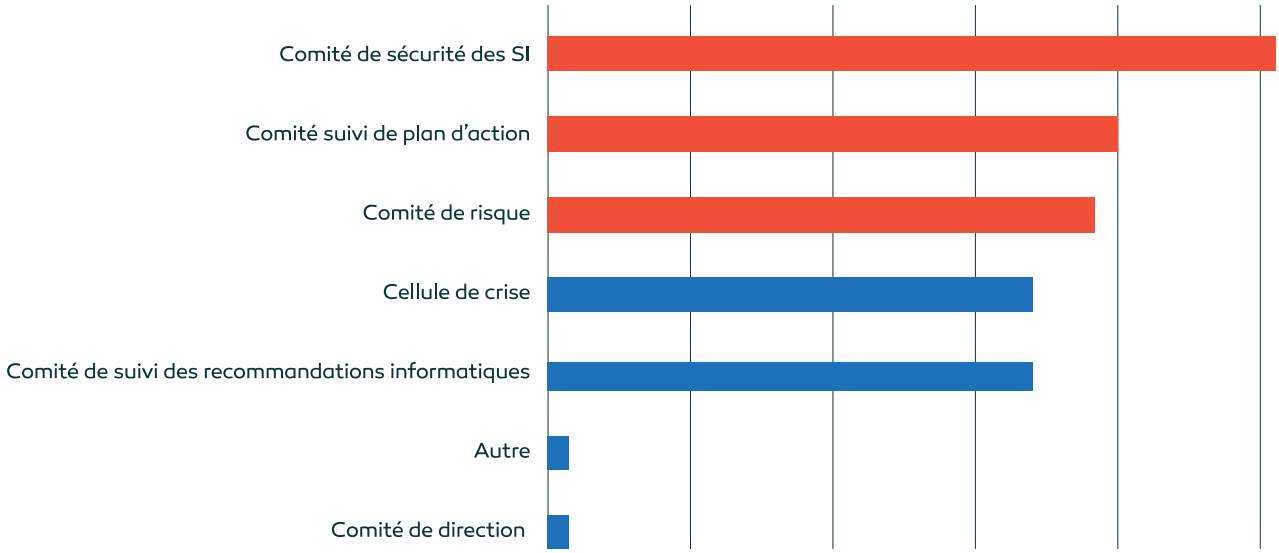
Chapitre 5 : Gouvernance de la sécurité

En matière de gouvernance de la sécurité numérique, avez-vous rédigé, validé et publié les documents suivants ?



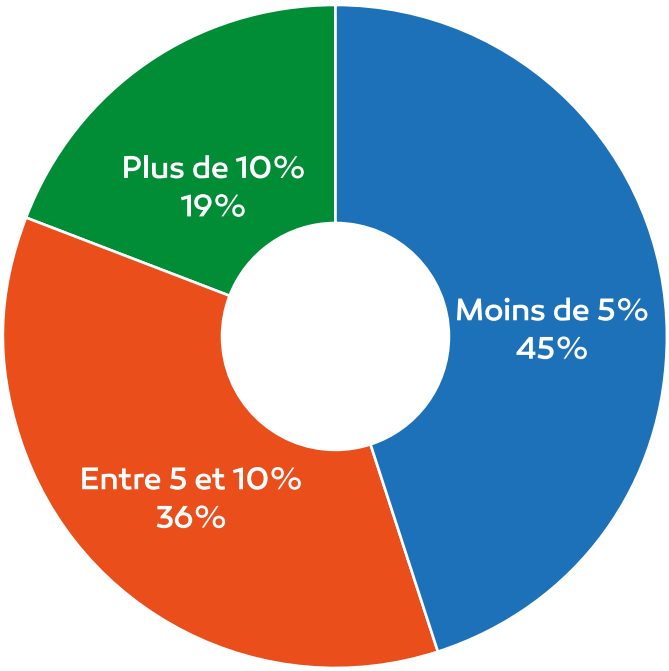
En matière de gouvernance de la sécurité numérique, les responsables de sécurité se dotent à minima d'une PSSI, d'une charte informatique et d'une cartographie des risques SI.

En matière de comitologie, votre entreprise dispose d'un ...

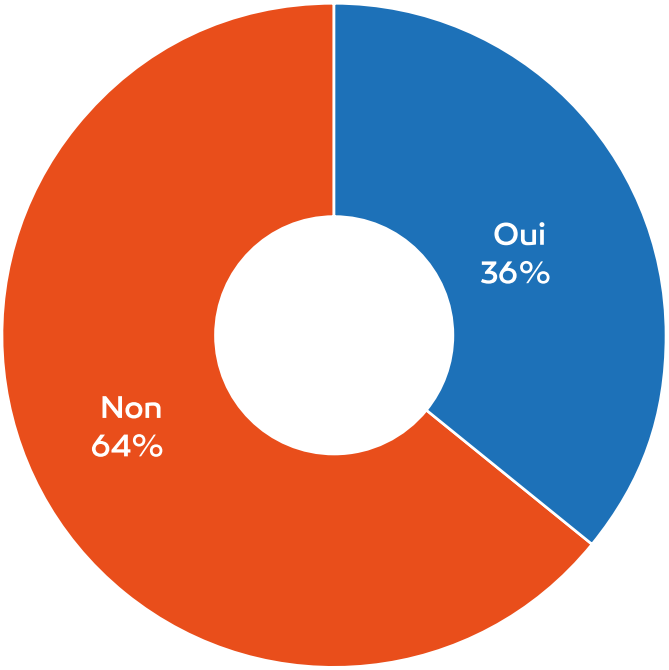


3 **C'est le nombre de comité en moyenne pour gouverner la sécurité dans les organismes.**

Part du budget SI consacrée à la sécurité dans l'entreprise

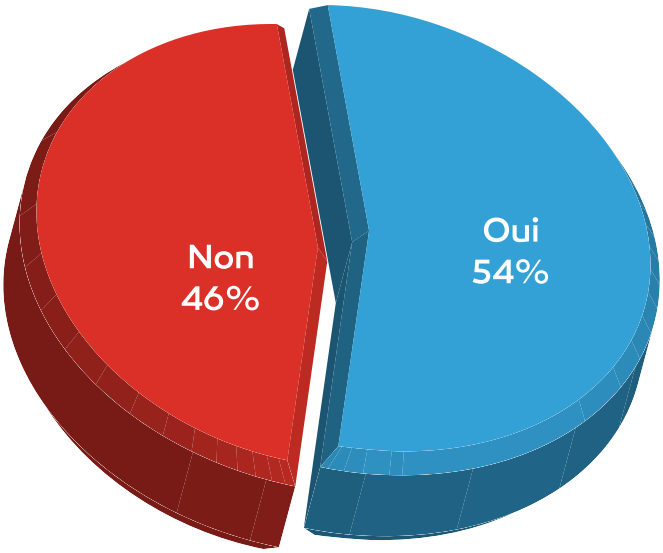


Disponibilité d'un plan de contrôle formalisé

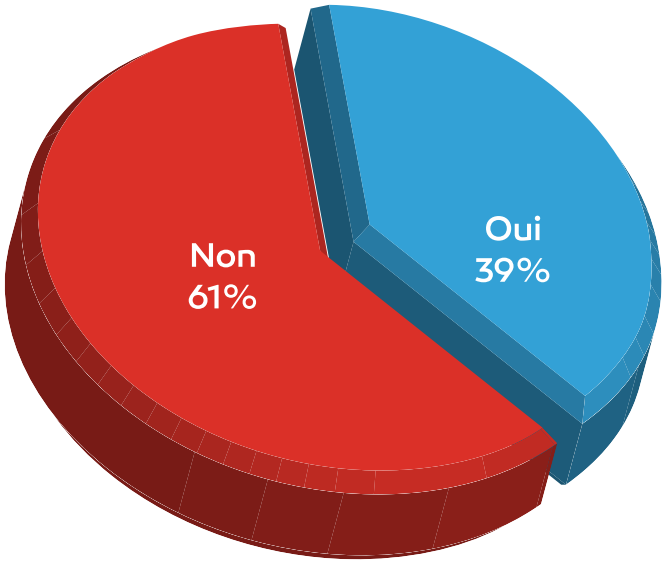


Chapitre 6 : IA – Intelligence Artificielle & Ouverture

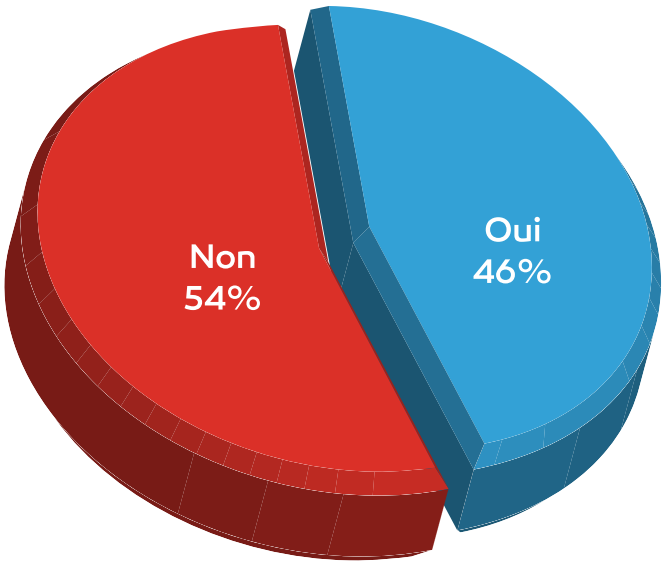
Seriez-vous prêt à laisser une solution d'IA prendre des décisions en matière de sécurité pour ce qui concerne la détection et/ou la remédiation ?



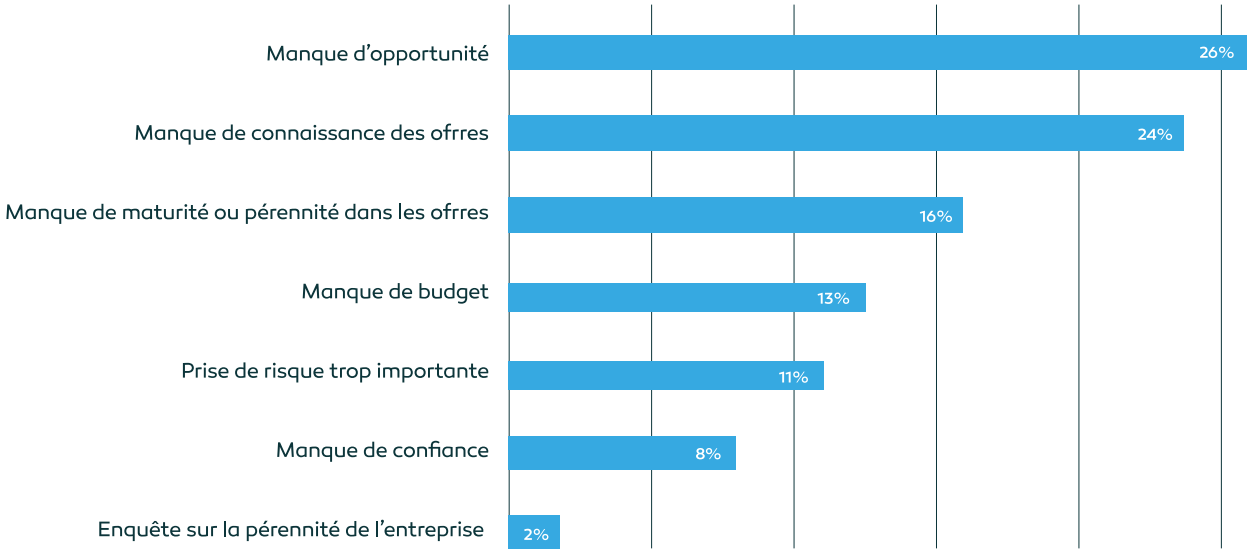
Utlisez-vous une ou plusieurs solutions de cybersécurité basées sur l'intelligence artificielle ?



Avez-vous recours aux solutions innovantes des start--up ?

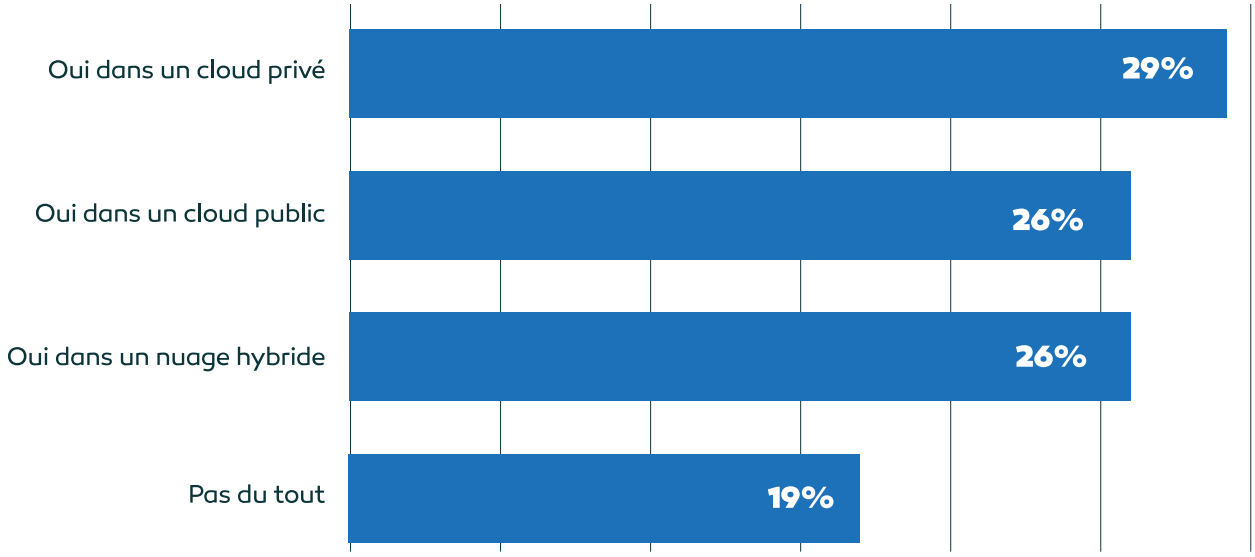


Si non pour quelle raison ?



Le coud et le cloud souverain reste un défi majeur pour les organismes en Afrique.
26% des entreprises stockent leurs données dans des clouds publics

Certaines données de votre entreprise sont enrégistrées dans le cloud ?



Pour rejoindre **le CESIA**,
Contactez-nous via notre site internet

www.lecesia.com

Suivez-nous sur nos réseaux sociaux