Deloitte.

Etude de la maturité Cybersécurité 2021 Afrique Francophone

MAKING AN IMPACT THAT MATTERS since 1845

Juin 2021

Sommaire

03
Avant-propos

08
Contexte
Impact COVID et principales préoccupations des entreprises en matière de cyberattaques

11
Investissement
Allocation et répartition des budgets sur la cybersécurité

14
Stratégie
Existence d'une stratégie cybersécurité et implication du top management

17
Organisation
Rattachement hiérarchique du RSSI et répartition du temps alloué à la cybersécurité

21
Sensibilisation
Sensibilisation des collaborateurs face aux risques cybersécurité

23
Outsourcing
Activités cybersécurité externalisées à des tiers

25
Technologies
Outils déployés pour la protection et la sécurisation du système d'information

27
Détection & Réponse
Dispositifs de détection et de réponse mis en place

29
Résilience
Dispositif de résilience face aux incidents cybersécurité

31
Méthodologie et Remerciements

© 2021 Deloitte Afrique SAS

Avant-propos

© 2021 Deloitte Afrique SAS

Avant-propos

Au fur et à mesure que le monde se transforme et se consolide, que les modes de travail évoluent, notamment dans le contexte marqué par la pandémie de COVID-19, les frontières de la cybersécurité s'étendent. Avec chaque nouvel appareil connecté, découverte numérique ou processus automatisé, de nouvelles vulnérabilités et des préoccupations en cybersécurité émergent.

Dans le contexte du « Cyber Everywhere », Deloitte a mené une enquête auprès de deux cent cinquante entreprises africaines à travers une vingtaine de questions qui permettent de dresser un panorama de leur niveau de maturité cybersécurité ainsi que ses perspectives, les organisations se positionnent-elles pour saisir les opportunités naissantes de la cybersécurité ? Ou y a-t-il un écart entre leurs objectifs de transformation et leurs limitations en termes de temps et de ressources ?

Cette étude permet d'apporter des éléments de réponse chiffrés sur les défis auxquels se confrontent les organisations africaines. Parmi ces défis, nous avons souhaité adresser les sujets de gouvernance, incluant le rôle du responsable de la sécurité des systèmes d'information au sein de l'organisation, ainsi que l'implication et la sensibilisation des décideurs au risque cyber dans les opérations qui permettraient de définir une stratégie de cybersécurité adéquate.

Au-delà des aspects organisationnels, l'étude tend à présenter la situation des organisations africaines s'agissant des moyens mis en disposition dans la mise œuvre de leur stratégie de cybersécurité. Ainsi, dans un contexte de pénurie de compétences spécialisées et de cadres règlementaires en évolution, nous nous sommes intéressés au recours à l'externalisation et aux technologies permettant d'assurer la protection, la détection et la résilience face aux cybermenaces.

Les résultats de cette étude, dédiée au marché africain, ont également été mis en perspective avec le baromètre de l'enquête mondiale Deloitte « Cyber everywhere. Succeed anywhere ». En multipliant les points de vue d'experts, cette étude donne aux Directions Générales et aux Responsables de la Sécurité des Systèmes d'Information des grandes entreprises africaines, des éléments d'information et des sources d'inspiration. Nous souhaitons, à travers cette étude, apporter notre contribution au renforcement de la cybersécurité des entreprises africaines.

Aristide Ouattara
Risk Advisory Lead Partner
Deloitte Afrique Francophone

Sofiane El Abdi
Cyber Risk Lead Partner
Deloitte Afrique Francophone

© 2021 Deloitte Afrique SAS

Avant-propos

Large couverture des entreprises d'Afrique Francophone

Près de 210 entreprises de 11 pays en Afrique Francophone ont participé à ce baromètre. Ces entreprises sondées couvrent un échantillon représentatif des secteurs d'activité des entreprises africaines : Services Financiers, Télécoms, Média & Technologie, Industrie et service, Secteur public, autres

210
Entreprises Africaines

11
Pays de l'Afrique Francophone

22%
Des groupes internationaux

51%
Des entreprises avec plus de 1 000 employés

20%
Télécoms, Média & Technologie

31%
Services Financiers (Finance, Banque, Assurance & Investissement)

24%
Industrie et service

© 2021 Deloitte Afrique SAS

Avant-propos

Points clés

Contexte et risques cybersécurité

- Durant la pandémie de la COVID-19, la majorité des entreprises sondées ont eu recours au télétravail total ou partiel, et estiment y être suffisamment outillées.
- La principale préoccupation des entreprises africaines en matière de cyberattaques concerne les logiciels malveillants suivis par les attaques de phishing. En effet, la moitié des entreprises ont constaté une augmentation du nombre d'incidents depuis 2020.

Investissements, gouvernance, stratégie et organisation

- Les budgets alloués à la cybersécurité restent insuffisants, 66% des entreprises investissent moins de 200k € par an. Contrairement aux tendances mondiales, les budgets alloués à la cybersécurité ne sont pas équitablement répartis entre les différents domaines ; 35% des investissements cybersécurité sont dédiés à la sécurité des infrastructures IT et seulement 5% sont dédiés à la sécurité des données, la détection des incidents, le suivi des menaces ou encore la gestion des identités et des accès.
- Uniquement la moitié des entreprises africaines déclarent disposer d'une stratégie et d'une feuille de route cybersécurité en adéquation avec la stratégie globale de leurs entreprises.
- La majorité des entreprises ont désigné un responsable de la sécurité SI. Toutefois, et contrairement aux tendances mondiales, uniquement 7% du temps des responsables sécurité SI est dédié à la détection et la réponse aux cybermenaces.

Technologie, externalisation et résilience

- Le manque des compétences qualifiées en cybersécurité, les faibles budgets et le manque d'appui du management représentent les principales contraintes limitant les entreprises africaines dans l'atteinte de leurs objectifs tant cyber que métiers.
- Le dispositif de résilience dans les entreprises africaines reste insuffisant. En effet, uniquement 22% des entreprises sondées disposent d'un SOC, 42% disposent d'un plan de continuité d'activité et 11% uniquement ont souscrit à une police d'assurance pour couvrir le risque en matière de cybersécurité.

© 2021 Deloitte Afrique SAS

Baromètre de maturité Cyber Afrique- 2021

© 2021 Deloitte Afrique SAS

Contexte

- Impact COVID: Adoption de la solution du télétravail face à la pandémie
- La principale préoccupation des entreprises en matière de cyberattaques

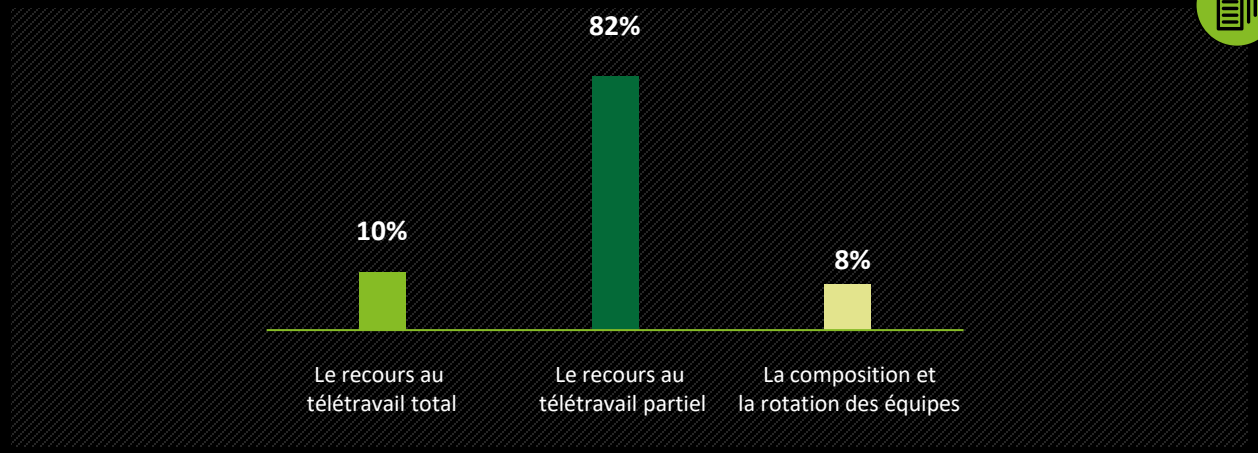
© 2021 Deloitte Afrique SAS

Contexte

Impact COVID: Adoption de la solution du télétravail face à la pandémie

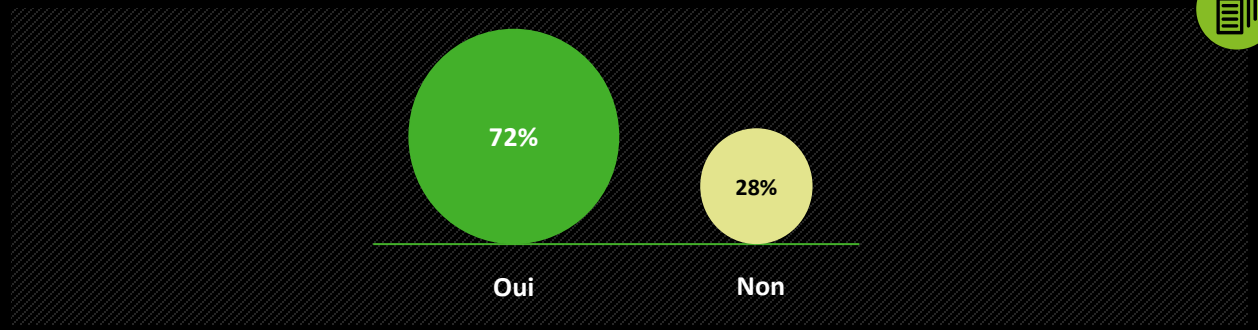
1 92% des entreprises sondées ont eu recours au télétravail total ou partiel

Face à l'impact du COVID-19, la solution adoptée est



2 72% des entreprises sondées estiment qu'elles sont suffisamment outillées en matière de télétravail

Face à l'impact du COVID-19, la solution adoptée est



- La crise mondiale générée par l'épidémie du Coronavirus (COVID19) met à rude épreuve la capacité de résilience des entreprises africaines. La majorité d'entre elles ont invité leurs collaborateurs à adopter le télétravail, afin de pouvoir conserver leurs liens contractuels et continuer à assurer efficacement ses activités. C'est le cas de 92% des entreprises. Toutefois, 8% d'entre elles ont opté pour un modèle hybride, consistant à instaurer des rotations d'équipes. Cela pourrait se comprendre car si de nombreuses entreprises se sont laissées surprendre par la pandémie, celle-ci fut pour d'autres une opportunité de croissance des affaires, d'où une nécessité d'adaptation. C'est le cas des services financiers numériques, des industries évoluant dans la fabrication de produits d'entretien, des institutions de santé, etc.

- Le télétravail rime toutefois avec une ouverture vers l'extérieur et une augmentation de la fenêtre d'exposition aux attaques cyber. Notre étude a démontré que 28% des organisations estiment n'avoir pas été suffisamment outillées afin de faire face à ces risques, autant sur le plan technique que sur le plus humain.

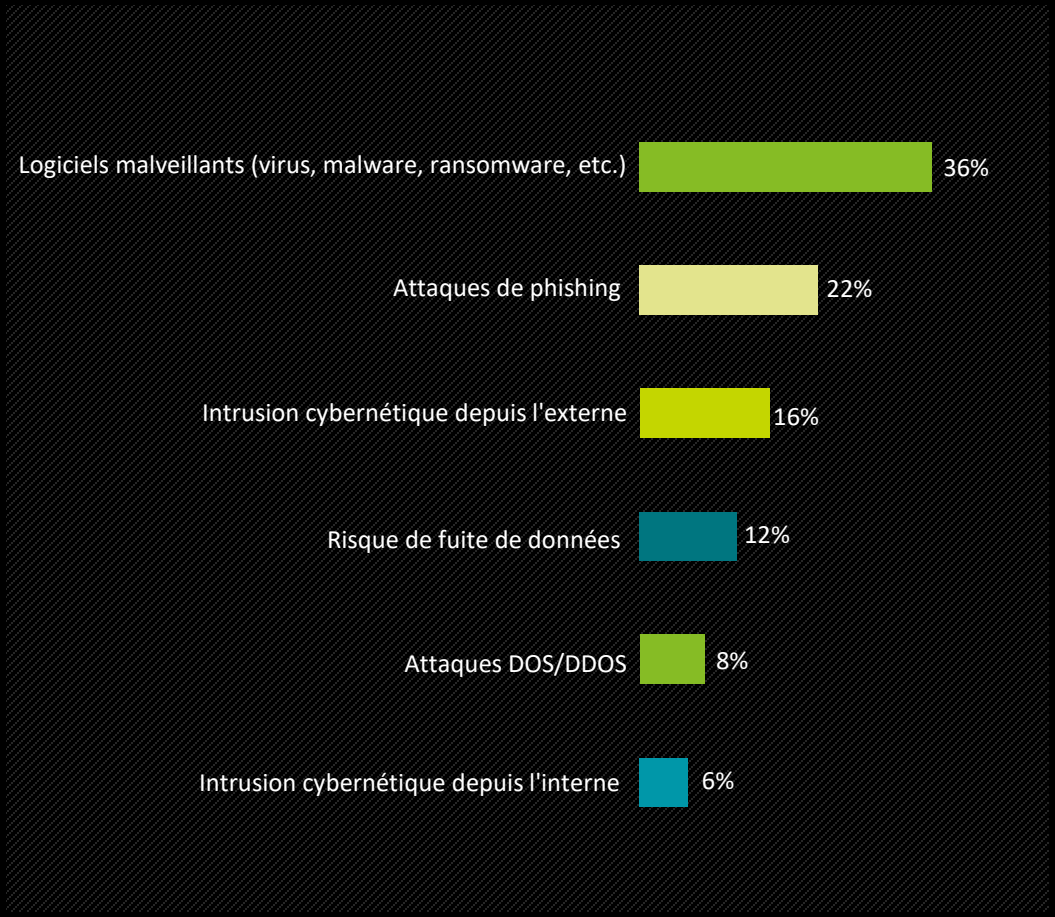
© 2021 Deloitte Afrique SAS

Contexte

La principale préoccupation des entreprises en matière de cyberattaques

3 **La principale préoccupation des entreprises africaines en matière de cyberattaques concerne les logiciels malveillants suivis par les attaques de phishing**

Quelle est votre principale préoccupation en matière de cyberattaques?



- Parmi les incidents les plus importants, nous pouvons citer ceux provenant de logiciels malveillants et des attaques par hameçonnage. Ils constituent à eux seuls des préjudices subis par 78% des entreprises. En effet, l'apparition de la pandémie a été l'occasion pour certains de profiter de l'anxiété et de la sensibilité limitée des utilisateurs aux règles d'identification de courriels ou fichiers malveillants. Nombreux sont ceux qui, souhaitant recueillir des informations liées à la pandémie, se sont vus proposer de télécharger des fichiers ou des applications les exposant à des pertes de données ou à une confiscation de leurs données moyennant le paiement d'une rançon.

- Ce qui nous amène à la seconde catégorie de préoccupations révélées par les organisations : les attaques cybernétiques provenant de l'extérieur, et les fuites de données. Elles ont pour cause racine le manque de préparation et de mesures de sécurité adéquates déployées avant ouverture du réseau à l'extérieur. Dans certains cas, les employés des organisations ont eux-mêmes été vecteurs de la réalisation de ces incidents, ce qui nous ramène encore une fois au manque de sensibilisation en cybersécurité d'une bonne partie d'entre eux.

Avec la crise qu'a engendrée la COVID et la transition vers le télétravail, nous avons constaté une augmentation des risques liés aux cyberattaques. Les attaques de Phishing et de Ransomware sont celles qui préoccupent notre organisation.

Fahd Chaouch, Directeur Exécutif, Société Magasin Général, Tunisie

© 2021 Deloitte Afrique SAS

Investissement

- Allocation des budgets à la cybersécurité
- Répartition des budgets sur les différents domaines de la cybersécurité

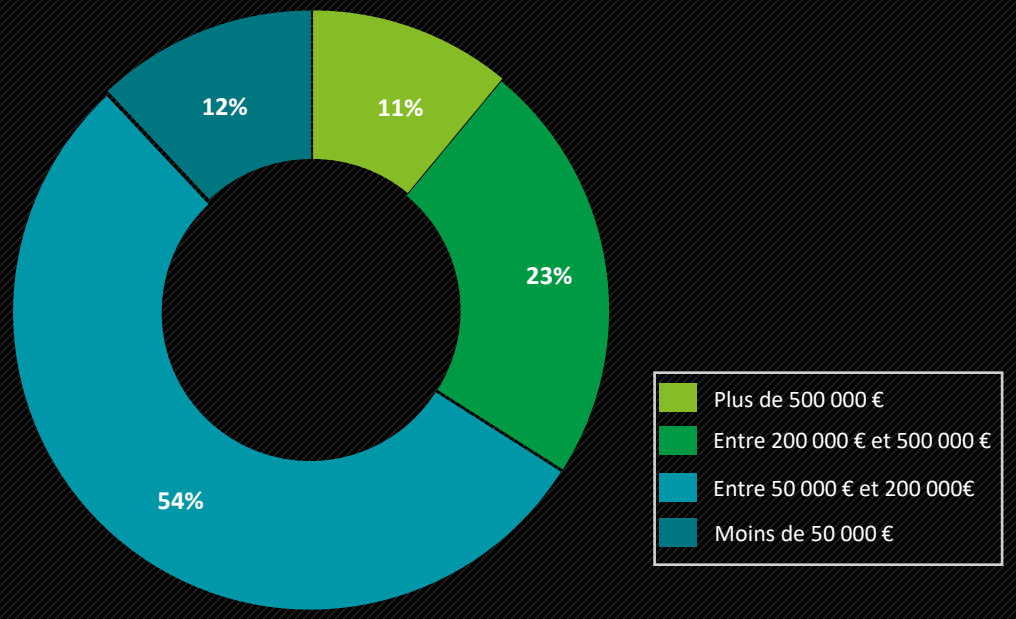
© 2021 Deloitte Afrique SAS

Investissements

Allocation des budgets à la cybersécurité

1 Les budgets dédiés à la cybersécurité restent insuffisants, 66% des entreprises investissent moins de 200k € par an

Quel est le montant approximatif que votre organisation investit en cybersécurité sur une base annuelle? *



* Ces chiffres portent sur les grandes entreprises (ayant + 500 employés)

- Il est à déplorer les investissements limités de près de 65% des organisations dans le renforcement de leur dispositif de cybersécurité. Les 11% d'entre elles qui prévoient des budgets conséquents à la gestion des risques liés à la cybersécurité, sont des groupes financiers panafricains, ou encore des opérateurs de télécommunications. Pour ceux-ci, la sécurité du système d'information relève d'un caractère vital, tout en constituant des exigences d'ordre réglementaire et légal.

Nous constatons un niveau d'investissement encore insuffisant des institutions financières de la zone UEMOA dans la prévention et la gestion des risques de cybersécurité.

Jean Louis Menann Kouamé, Directeur Général Orange Bank Africa

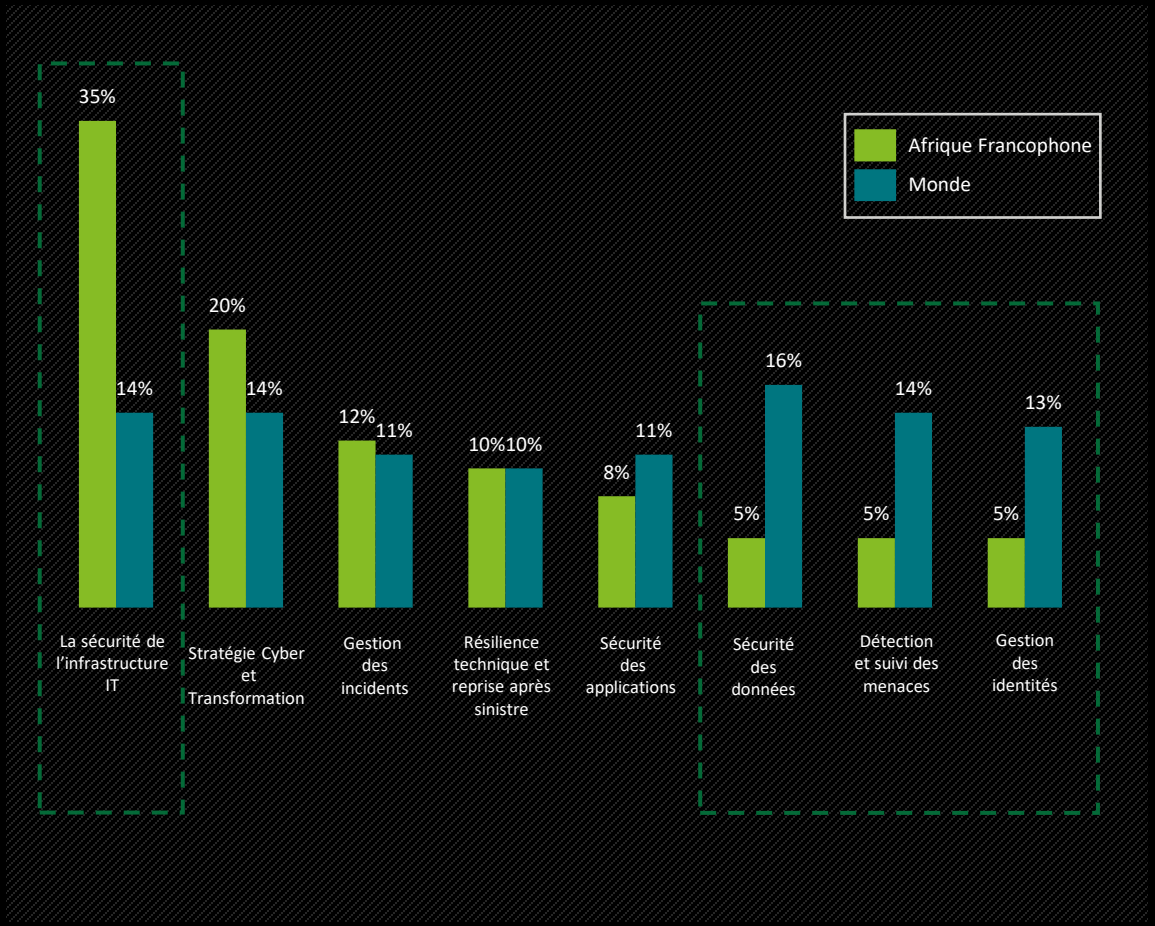
© 2021 Deloitte Afrique SAS

Investissements

Répartition des budgets sur les différents domaines de la cybersécurité

2 **Contrairement aux tendances mondiales, les budgets alloués à la cybersécurité ne sont pas équitablement répartis entre les différents domaines ; 35% des investissements cybersécurité sont dédiés à la sécurité des infrastructures IT et seulement 5% sont dédiés à la sécurité des données, la détection et le suivi des menaces et la gestion des identités**

Votre entreprise alloue la plus grande partie du budget cybersécurité à



- Les investissements liés à la cybersécurité des entreprises dans le monde sont répartis d'une manière équitable sur les différents domaines de la cybersécurité. Ceci démontre d'une stratégie globale axée sur la réduction du risque tandis que les entreprises africaines continuent d'investir majoritairement sur la sécurité des réseaux et des infrastructures IT.
- Les résultats en Afrique ont été révélateur: 35% des investissements des entreprises africaines en cybersécurité sont consacrés à la sécurité des infrastructures IT au détriment d'autres domaines aussi importants tels que la sécurité des données (5%), la gestion des identités et des accès (5%), la détection et la réponse aux menaces (5%). Ceci peut s'expliquer par :
  - Des budgets limités alloués à la cybersécurité
  - Une absence d'une vision holistique de la cybersécurité permettant d'identifier et de traiter toutes les zones à risques de l'entreprise
  - Une absence d'indicateurs pertinents remontés du préjudice éventuel aux décideurs, leur permettant de prendre des décisions d'investissement avisées en matière de cybersécurité
  - Des RSSI qui restent majoritairement rattachés à la Direction des Systèmes d'Informations (DSI) et qui restreignent souvent leurs champs d'activité à la technique

Les entreprises allouent la plus grande partie de leurs budgets aux activités qui leur génèrent directement des retours sur investissement. Il faudrait donc que la cybersécurité ne soit pas considérée comme un centre de coût, mais plutôt comme un centre de profit.

Mame Diop, Sous-Directrice du Système d'Information et de la Sécurité, Orange Côte d'Ivoire

© 2021 Deloitte Afrique SAS

Stratégie

- Existence d’une stratégie cybersécurité alignée avec la stratégie globale de l’entreprise
- Implication du Top management et Reporting des indicateurs cybersécurité
- Contraintes empêchant les entreprises d’atteindre leurs objectifs de cybersécurité

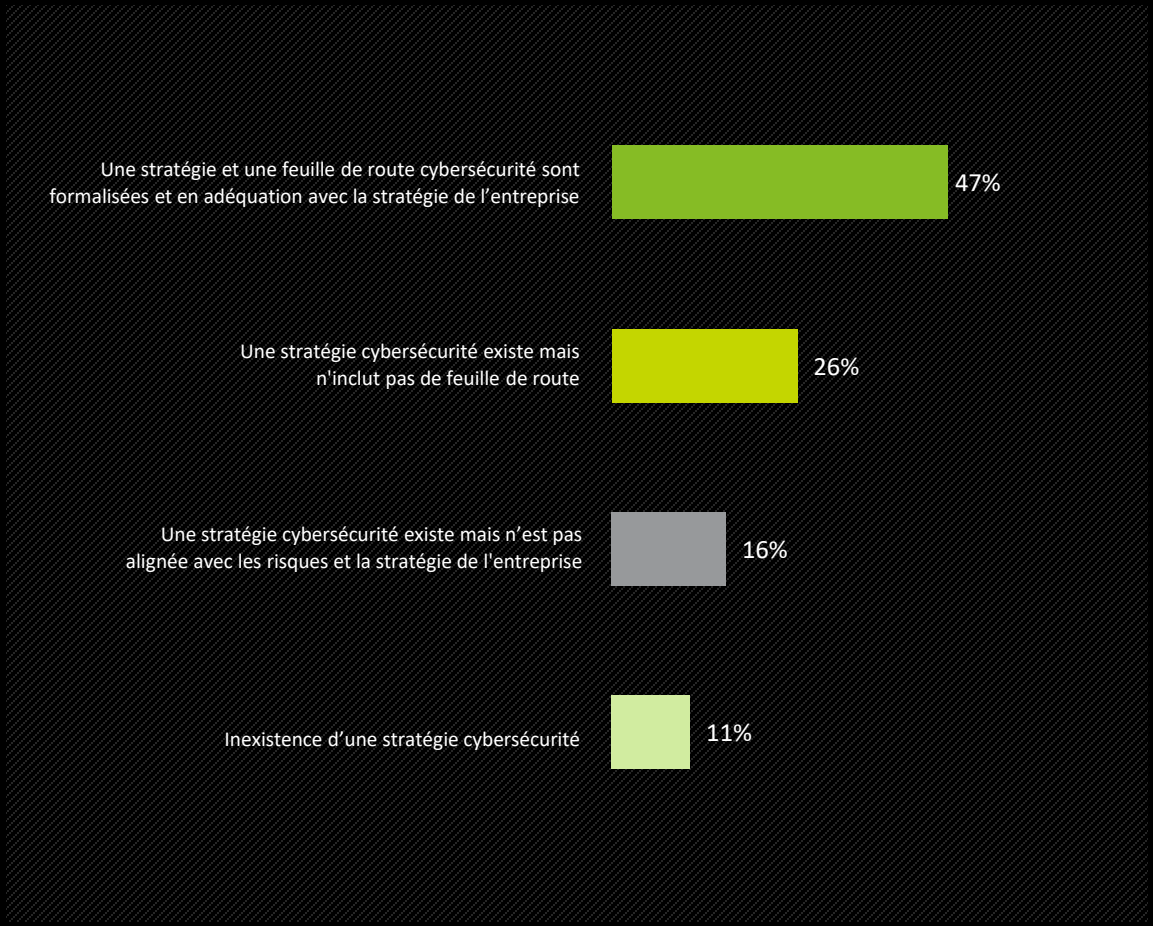
© 2021 Deloitte Afrique SAS

Stratégie

Existence d'une stratégie cybersécurité alignée avec la stratégie globale de l'entreprise

1 **47% des entreprises africaines déclarent disposer d'une stratégie et d'une feuille de route cybersécurité en adéquation avec leur stratégie globale**

Votre organisation a-t-elle définit une stratégie de sécurité de l'information ou de cybersécurité comportant une feuille de route?



- Notre étude a démontré une volonté des entreprises africaines à vouloir développer un programme de cybersécurité aligné avec les objectifs stratégiques et l'appétence aux risques de leur organisation. En effet, 47% des entreprises sondées déclarent avoir formalisé et aligné leur stratégie de cybersécurité et leur feuille de route avec leur stratégie globale.
- Cependant, 26% des organisations affirment avoir une stratégie de cybersécurité n'incluant pas de feuille de route. Cette dernière constitue un outil de pilotage permettant de déployer un dispositif de maîtrise constamment en adéquation avec le profil de risque.

La cybersécurité est un élément essentiel de la stratégie digitale des états et des entreprises. La principale responsabilité des gouvernements est d'implémenter une stratégie nationale de cybersécurité cohérente et inclusive. Et pour se faire, les gouvernements doivent allouer les budgets appropriés.

Syrine Tlili, Directrice Générale, ANCE-Tuntrust, Tunisie

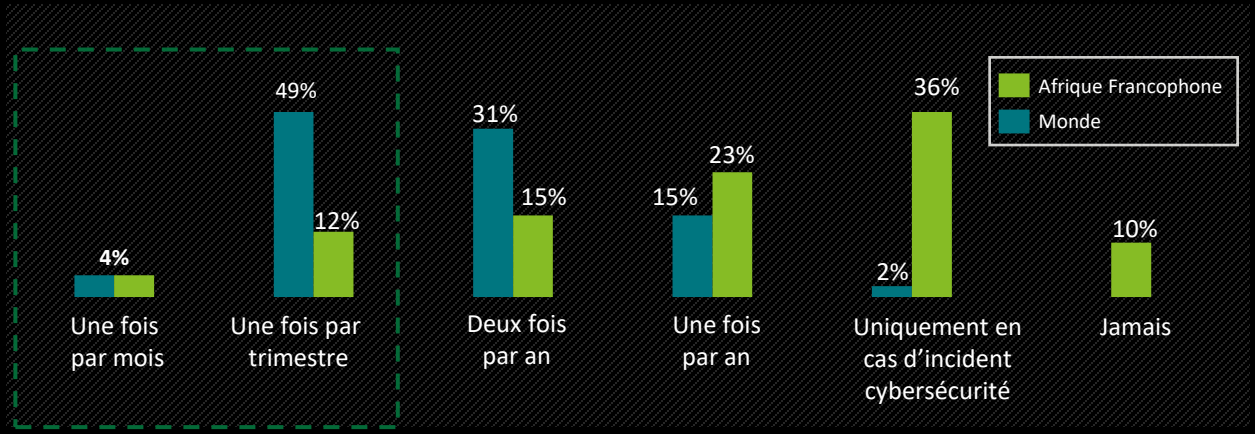
© 2021 Deloitte Afrique SAS

Stratégie

Implication du top management et reporting des indicateurs cybersécurité

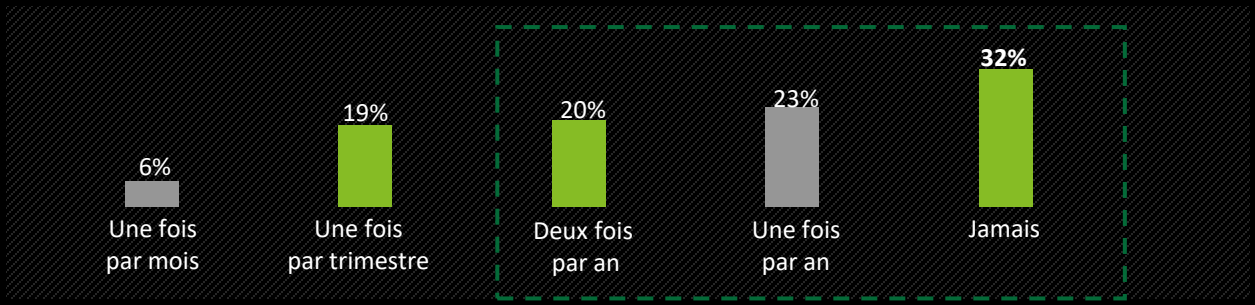
2 **49% des organisations mondiales et uniquement 12% des entreprises africaines discutent trimestriellement sur le sujet de la cybersécurité dans leurs comités exécutifs**

A quelle fréquence les sujets de la cybersécurité sont à l'ordre du jour du comité exécutif ?



3 **75% des entreprises africaines communiquent rarement voire jamais leurs indicateurs de sécurité à leurs directions générales et/ou comités exécutifs**

À quelle fréquence le reporting sur les indicateurs de sécurité est communiqué à la direction générale / aux comités exécutifs?



- La mise en place de la stratégie cybersécurité repose sur l'implication du management. Malheureusement, de nombreux dirigeants en Afrique n'abordent pas le sujet aussi souvent qu'ils devraient le faire, restant fixé sur l'atteinte des objectifs tout en omettant ce risque pouvant se manifester. Or en suivant la moyenne mondiale, 49% des organisations évoquent trimestriellement les aspects liés à la cybersécurité dans leurs comités exécutifs, contre 12% en Afrique.
- Cependant, 36% des entreprises africaines se sont vues contraintes de traiter des incidents liés à la sécurité de l'information dans leurs comités exécutifs. Les dirigeants d'entreprises gagneraient à adopter une approche plus proactive et à limiter les actions en réponse à des préjudices constatés.
- Par ailleurs, les conseils d'administration devraient exiger de la direction qu'elle fournisse un ensemble d'indicateurs de performance de la sécurité et des indicateurs de risque clés leur permettant de bien suivre l'état de la cybersécurité de leurs entreprises. Cependant, 75% des entreprises africaines communiquent rarement voire jamais leurs indicateurs de sécurité à leurs directions générales et/ou comités exécutifs.

La protection de notre système d'information a toujours été au centre de notre stratégie d'entreprise.

Mishael Kompani, Directeur Audit Interne, CITI Bank, République Démocratique du Congo

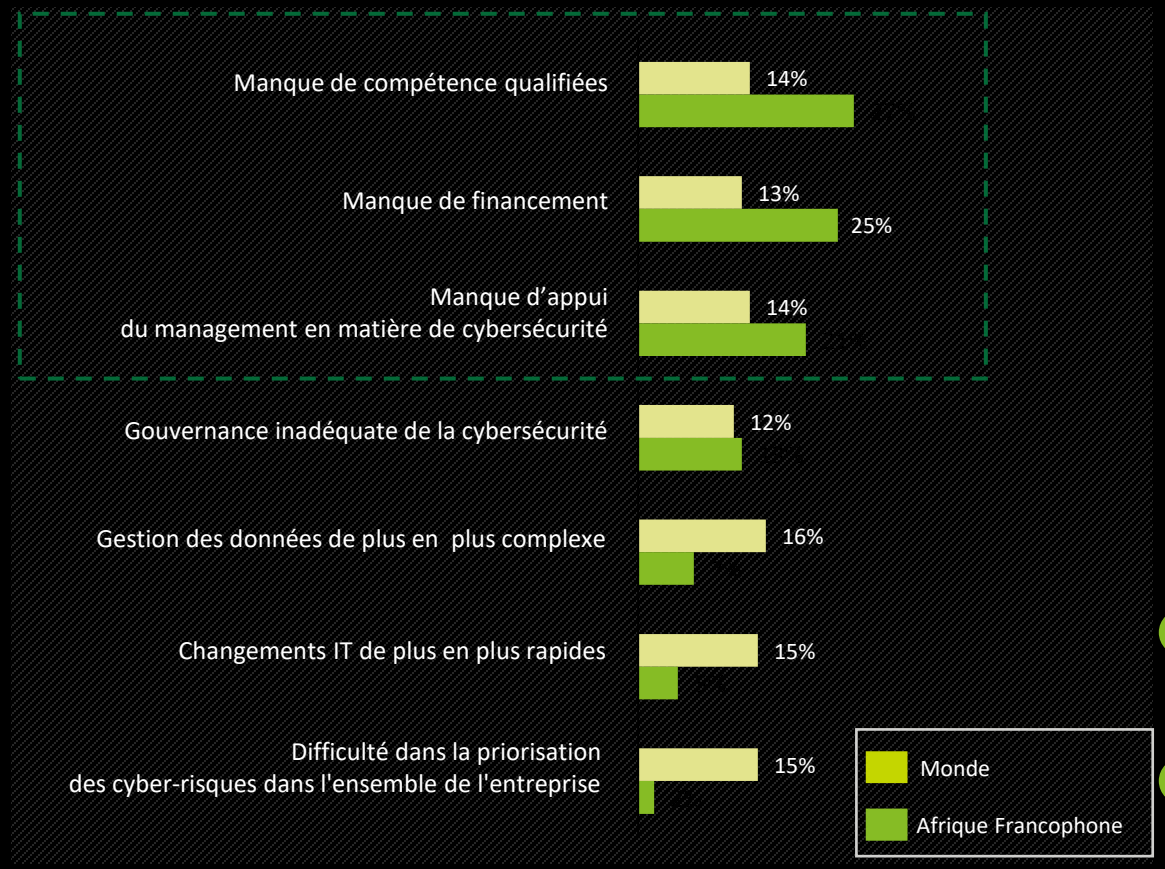
© 2021 Deloitte Afrique SAS

Stratégie

Contraintes empêchant les entreprises d'atteindre leurs objectifs de cybersécurité

4 Le manque de compétences qualifiées en cybersécurité, ainsi que les faibles budgets et le manque d'appui du management représentent les principales contraintes empêchant les entreprises africaines d'atteindre leurs objectifs de cybersécurité

Selon vous, quel est l'aspect le plus difficile dans la gestion de la cybersécurité dans votre organisation ?



- La majorité des responsables de la sécurité des SI (RSSI) interrogés avouent leurs inquiétudes sur leur capacité à garantir un niveau adéquat de sécurisation de leurs entreprises. Ceci est dû principalement à trois obstacles majeurs, affichant des proportions en Afrique bien supérieures à la moyenne mondiale :

1. Le manque de compétences qualifiées et ceci s'explique par le faible taux d'encadrement et la faible disponibilité des experts en cybersécurité au regard de la forte demande des entreprises souhaitant recruter et se renforcer massivement sur ce secteur
2. Le manque de financement et les faibles budgets alloués à la cybersécurité
3. Le faible appui du management aux initiatives de cybersécurité qui sont traitées pour beaucoup comme des problématiques IT en marge des enjeux métiers et ne sont même pas suffisamment discutés au niveau des comités de direction

La coordination cybersécurité, le partage d'informations sur les cyberattaques ainsi que la mise à disposition des ressources qualifiées représentent les enjeux cybersécurité majeurs dans le secteur public.

Syrine Tlili, Directrice Générale, ANCE-Tuntrust, Tunisie

La première ligne de défense n'est plus seulement technologique, elle est également humaine et organisationnelle.

El Hadji Malick Gueye, Directeur Risk Advisory chez Deloitte Afrique

© 2021 Deloitte Afrique SAS

Organisation

- Rattachement hiérarchique du RSSI
- Répartition du temps alloué par les responsables de sécurité de l’information

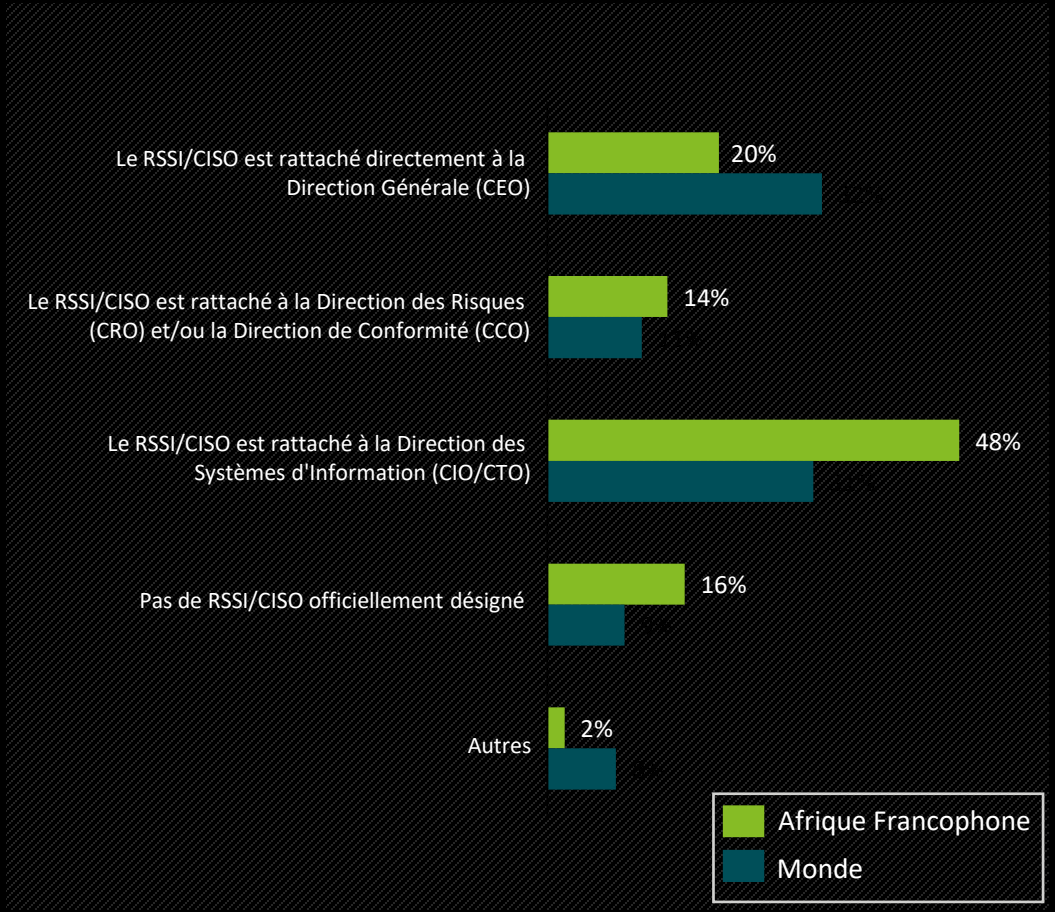
© 2021 Deloitte Afrique SAS

Organisation

Rattachement hiérarchique du responsable de la sécurité des systèmes d'information (RSSI)

1 La majorité des entreprises ont désigné un responsable de la sécurité SI, toutefois 57% des RSSI africains sont encore rattachés à la Direction Informatique

Le responsable de la sécurité des systèmes d'information (RSSI) dans votre organisation est rattaché à quelle entité ?



- Dans la même dynamique des entreprises mondiales, celles en Afrique prennent de plus en plus conscience de l'importance de la cybersécurité. Elles sont désireuses de recruter un RSSI et de constituer une équipe spécialisée et dédiée à la sécurité de l'information de leurs entreprises. En effet, notre étude a révélé que la majorité de celles-ci disposent d'un RSSI. Il est aussi à noter que dans certains secteurs, le cadre réglementaire en fait une exigence majeure en matière de renforcement du dispositif de contrôle interne global. C'est le cas du secteur financier.
- Cependant, et en opposition aux tendances mondiales, les RSSI des entreprises établies en Afrique sont majoritairement membres de la Direction des Systèmes d'Information (DSI).
- Ce modèle d'organisation révèle un niveau de maturité encore assez faible ; ainsi qu'un écart de conformité avec les bonnes pratiques de gouvernance. Celles-ci prônent une autonomie des RSSI dans leur rôle de chef d'orchestre et d'animation du dispositif de sécurité du SI, en articulation avec les opérationnels et les différents corps de contrôle.

Le rôle principal d'un RSSI est de s'assurer de l'alignement de la stratégie de cybersécurité avec la stratégie globale de l'entreprise et de veiller à l'atteinte de ses objectifs.

Dhia Hachicha, Directeur Cyber Risk, Deloitte Afrique Francophone

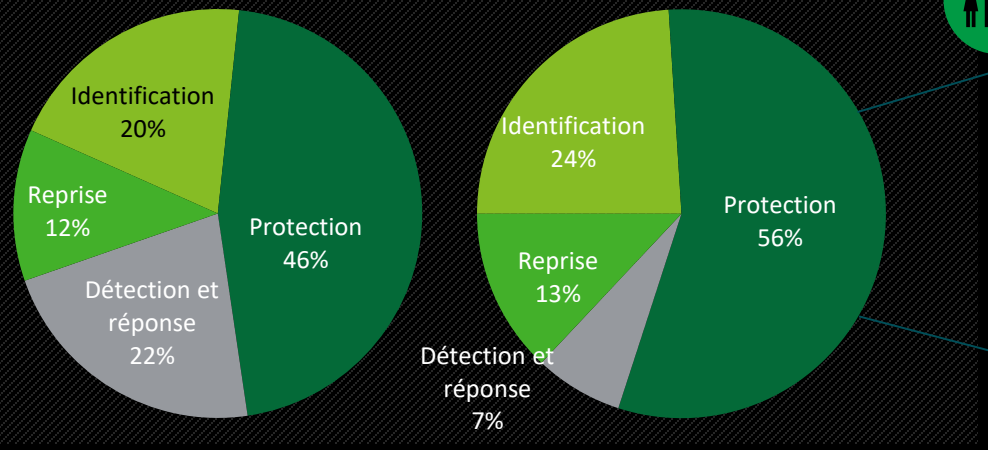
© 2021 Deloitte Afrique SAS

Organisation

Répartition du temps alloué par les responsables de sécurité de l'information

2 Contrairement aux tendances mondiales, uniquement 7% du temps des responsables sécurité SI est dédié à la détection et la réponse aux cybermenaces

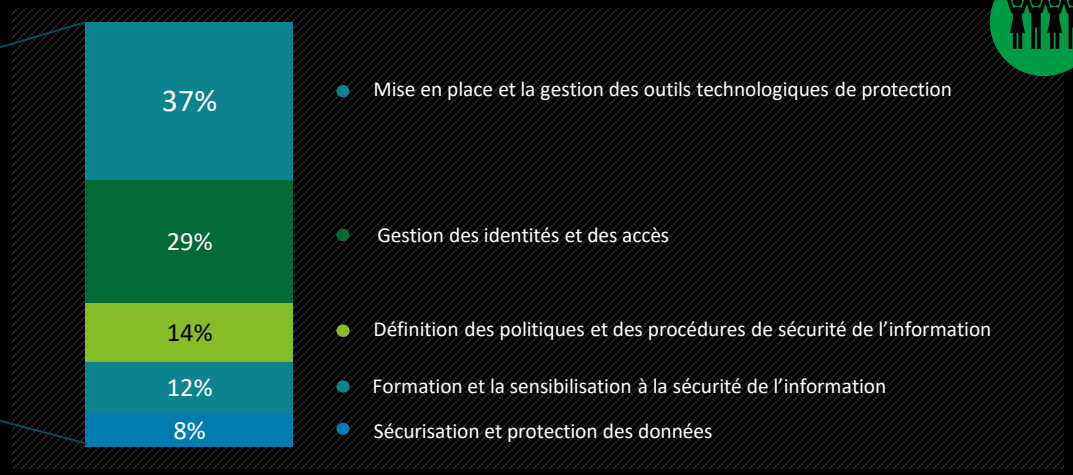
Comment les responsables de la sécurité de l'information de votre organisation répartissent leurs temps entre les fonctions ci-dessous du Framework NIST?



Monde

3 La mise en place et la gestion des outils technologiques de protection demeurent l'activité principale des responsables cybersécurité en Afrique

Comment les responsables de la sécurité de l'information de votre organisation répartissent leurs temps entre les fonctions de protection ci-dessous ?



Afrique francophone

- L'examen des données de l'enquête sur la répartition du temps par les équipes cybersécurité des organisations du continent a démontré que ces derniers consacrent une grande partie de leur temps sur une des cinq fonctions essentielles du Framework Cybersécurité de l'Institut national des normes et de la technologie (NIST) : La protection. En effet, 37% de leur temps est dédié à la mise en place et la gestion des outils technologiques de protection, 29% à la gestion des identités et des accès, et 14% à la définition des politiques et des procédures de sécurité de l'information.

>

- Vu le nombre considérable de tâches sous leurs responsabilités, les RSSI n'allouent que 12% de leur temps à la sensibilisation des membres du personnel, et 8% à la sécurisation et protection des données. Or, de plus en plus de pays en Afrique se dotent de lois de protection des données à caractère personnel, sous la supervision d'une autorité dédiée.
- Parallèlement, les résultats de l'enquête révèlent que les RSSI des entreprises africaines ne consacrent que 7% de leur temps à la détection et la réponse, sujet sur lequel leurs homologues dans le monde en sont à 22% d'occupation.

© 2021 Deloitte Afrique SAS

Sensibilisation

Sensibilisation des collaborateurs face aux risques cybersécurité

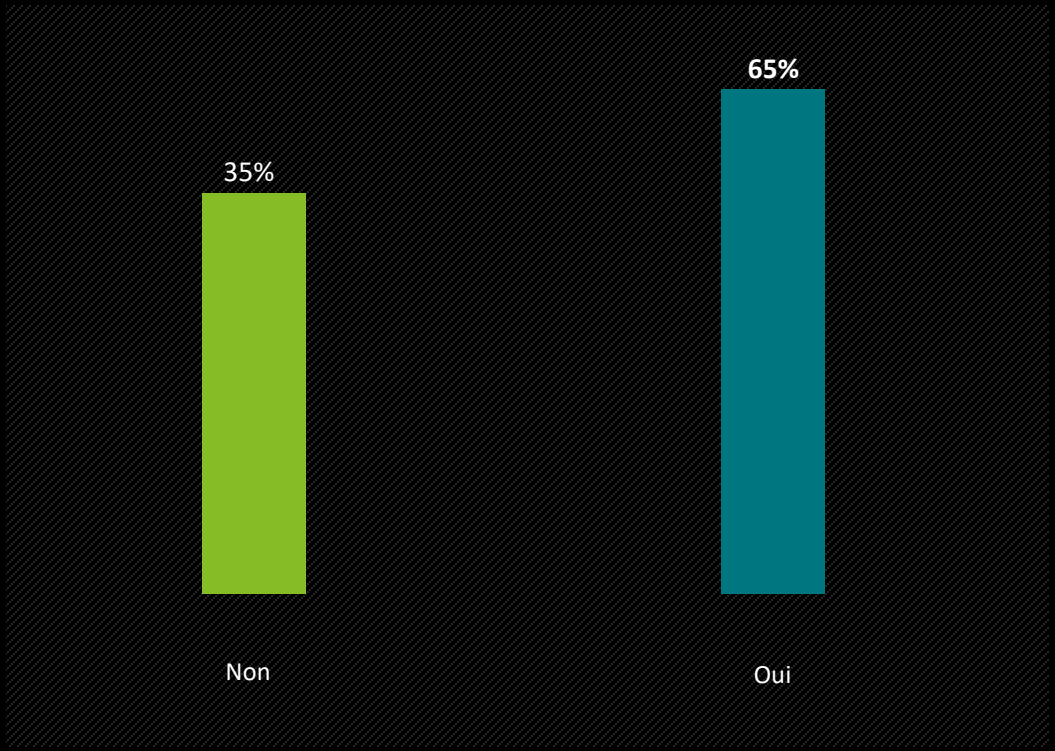
© 2021 Deloitte Afrique SAS

Sensibilisation

Sensibilisation des collaborateurs face aux risques cybersécurité

Malgré la généralisation du travail à distance à l'ère du COVID, 35% des entreprises sondées estiment que leurs collaborateurs ne sont pas sensibilisés aux risques cybersécurité du télétravail

Les collaborateurs de votre entreprise sont-ils sensibilisés aux risques du télétravail ?



Il ressort de l'enquête que 35% des entreprises estiment que leurs collaborateurs ne sont pas sensibilisés aux risques cybersécurité liés au télétravail. Ce taux assez élevé explique les préjudices exposés plus haut et pour lesquels les vecteurs se trouvent être les employés eux-mêmes.

Les alertes de sécurité d'ouverture de sessions, et les campagnes d'attaques à blanc permettent d'anticiper les cyberattaques, et de mieux sensibiliser les collaborateurs.

Jean Luc Diatta, Directeur du Système d'Information, Banque Régionale de Marchés(BRM), Sénégal

Les opérations de simulation d'attaques permettent de tester la capacité de l'équipe IT à gérer des cyberattaques et de mieux sensibiliser les utilisateurs finaux.

Fahd Chaouch, Directeur Exécutif, Société Magasin Général, Tunisie

© 2021 Deloitte Afrique SAS

Outsourcing

Activités cybersécurité externalisées ou sous-traitées à des tiers

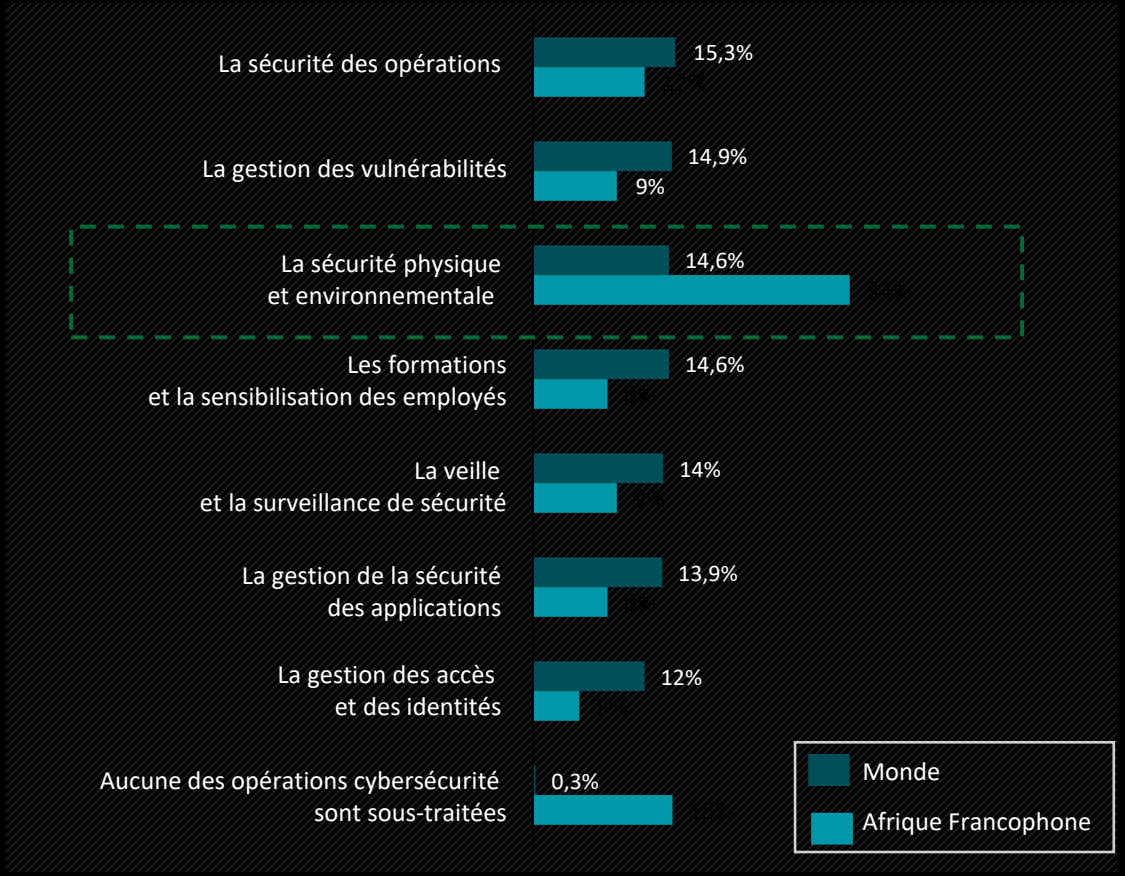
© 2021 Deloitte Afrique SAS

Outsourcing

Activités cybersécurité externalisées ou sous-traitées à des tiers

Les entreprises africaines suivent les tendances mondiales en matière d'externalisation de leurs activités de cybersécurité. Toutefois, la gestion de leur sécurité physique et environnementale demeure la fonction la plus sous-traitée

Parmi la liste ci-dessous, quelle est la fonction de votre entreprise la plus sous-traitée à des tiers/partenaires ?



- Devant l'accélération du nombre d'attaques informatiques et le niveau de complexité des systèmes de protection, de plus en plus d'entreprises africaines se tournent vers l'externalisation de leurs sécurités.
- Le recours des entreprises africaines à la sous-traitance dans le domaine de la sécurité porte essentiellement sur la sécurité physique et environnementale. Plus précisément elle consiste à se doter des services de sociétés de gardiennage. Ces organisations comptent pour 34%, pour une moyenne mondiale de 14.6%.
- Il est aussi important de relever que 15% des entreprises ne disposent d'aucune opération de cybersécurité externalisée. Elle dénote dans certains cas un sentiment d'excès de confiance, et dans la majorité des cas une contrainte liée aux budgets alloués à la cybersécurité.

La prévention de la cybercriminalité dans les établissements financiers nécessite un renforcement de la coopération entre les autorités de régulation et de contrôle ainsi que le recours à l'expertise des cabinets spécialisés.

Chokri Neji, Directeur Sécurité, Arab Tunisian Bank, Tunisie

© 2021 Deloitte Afrique SAS

Technologies

Outils déployés pour la protection et la sécurisation du système d’information

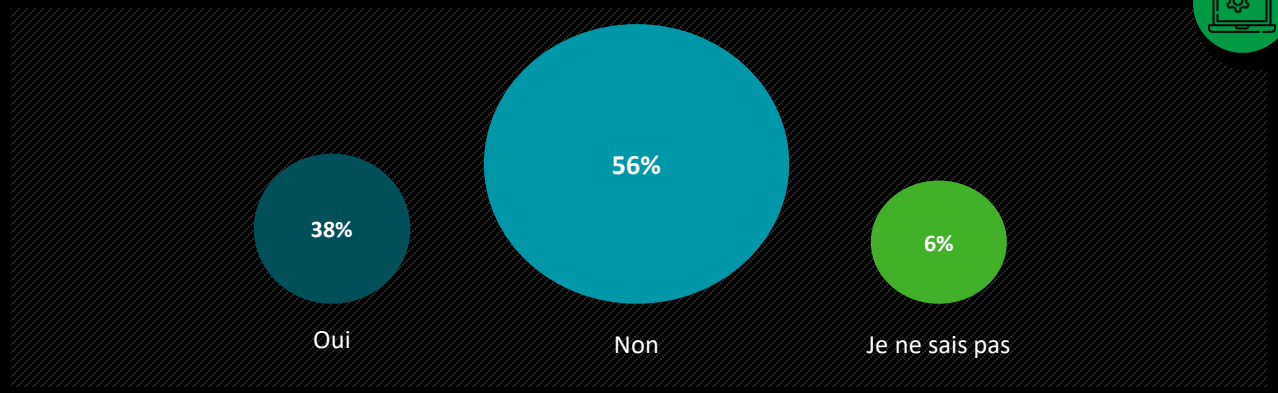
© 2021 Deloitte Afrique SAS

Technologies

Outils déployés pour la protection et la sécurisation du système d'information

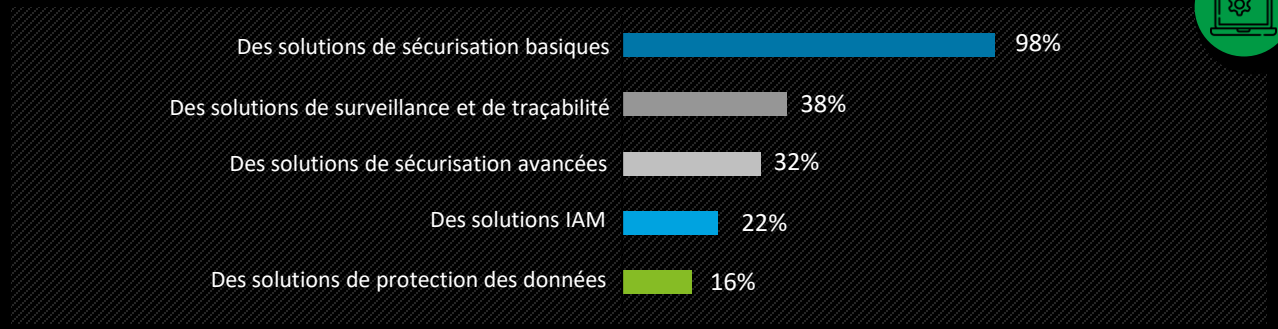
1 56% des RSSI sondés jugent que leurs entreprises ne sont pas suffisamment outillées en matière de cybersécurité

D'une façon générale, estimez-vous que votre organisation est suffisamment outillée en matière de cybersécurité ?



2 Uniquement 32% des entreprises africaines utilisent des solutions de sécurisation avancées

Quels systèmes de sécurité utilisez-vous dans votre organisation ?



- La cybersécurité a souvent été assimilée à la capacité défensive que pourrait avoir une entreprise aux cybermenaces. Seulement 38% des entreprises africaines estiment être préparées efficacement contre celles-ci, mais sans pour autant avoir réellement mis à l'épreuve leurs mesures de sécurité.
- Néanmoins, plus de la moitié des entreprises consultées sont conscientes qu'elles ne sont suffisamment pas outillées en matière de cybersécurité. Pour la majorité d'entre elles les raisons sont d'ordre budgétaire. Elles se limitent donc à des solutions de sécurisation assez basiques telles que : les Antivirus, les Antispam et les Firewalls, sans investir sur des solutions avancées telles que : DLP, NAC, AntiDDOS, IDS/IPS, SIEM, IAM, etc.

La cybersécurité dans le secteur financier est un enjeu de sécurité nationale, les banques doivent adapter leurs dispositifs de protection et déployer une activité de veille cybersécurité et mettre en place des systèmes de cyberdéfense avancés.

Chokri Neji, Directeur Sécurité, Arab Tunisian Bank, Tunisie

© 2021 Deloitte Afrique SAS

Détection & Réponse aux cybermenaces

Dispositifs de détection et de réponse mis en place pour faire face aux cybermenaces

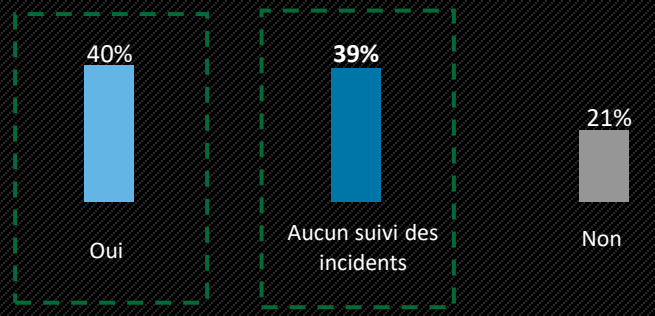
© 2021 Deloitte Afrique SAS

Détection & Réponse aux cybermenaces

Dispositifs de détection et de réponse mis en place pour faire face aux cybermenaces

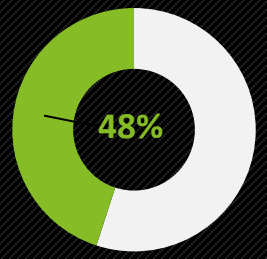
1 40% des entreprises ont constaté une augmentation du nombre d'incidents depuis l'année dernière et 39% ne réalisent pas le suivi de leurs incidents cybersécurité

Le nombre d'incidents de cybersécurité vécus par votre organisation a-t-il augmenté depuis l'année dernière ?

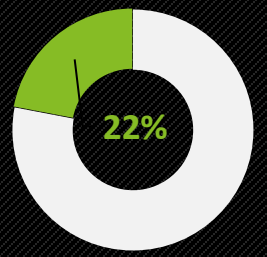


2 Uniquement 32% des entreprises africaines utilisent des solutions de sécurisation avancées

Quels systèmes de sécurité utilisez-vous dans votre organisation ?



Des entreprises disposent des outils de gestion des événements et des logs cybersécurité (SIEM)



Des entreprises disposent d'un SOC

- Une forte croissance des incidents de cybersécurité a été relevée depuis 2020. 40% des entreprises l'ont confirmée, alors que 39% d'entre elles ne disposent pas d'outils de monitoring et de suivi des incidents de cybersécurité. Il y a lieu de faire encore une fois référence à l'adoption impromptue du télétravail durant les périodes de confinement, et à l'anxiété et les compétences souvent limitées de certains administrateurs systèmes et réseaux. Elles ont été à l'origine des lacunes massives dans la cybersécurité des entreprises.
- Malgré cette augmentation des incidents et des risques cyber, près de 48% des entreprises disposent d'outils de type SIEM (Security Information and Event Management) pour la gestion des événements et des logs cybersécurité. Bien moins d'entre elles (22%) disposent d'un SOC (Security Operations Center). L'absence de déploiement de ces systèmes de surveillance, limite les capacités de prévention et d'intervention des entreprises face aux incidents de cybersécurité.

Mettre en place des outils et une organisation SOC permet d'anticiper et de réagir plus vite, de limiter les impacts d'une attaque, voire même la stopper.

Mame Diop, Sous-Directrice du Système d'Information et de la Sécurité, Orange Côte d'Ivoire

© 2021 Deloitte Afrique SAS

Résilience

Dispositif de résilience face aux incidents cybersécurité

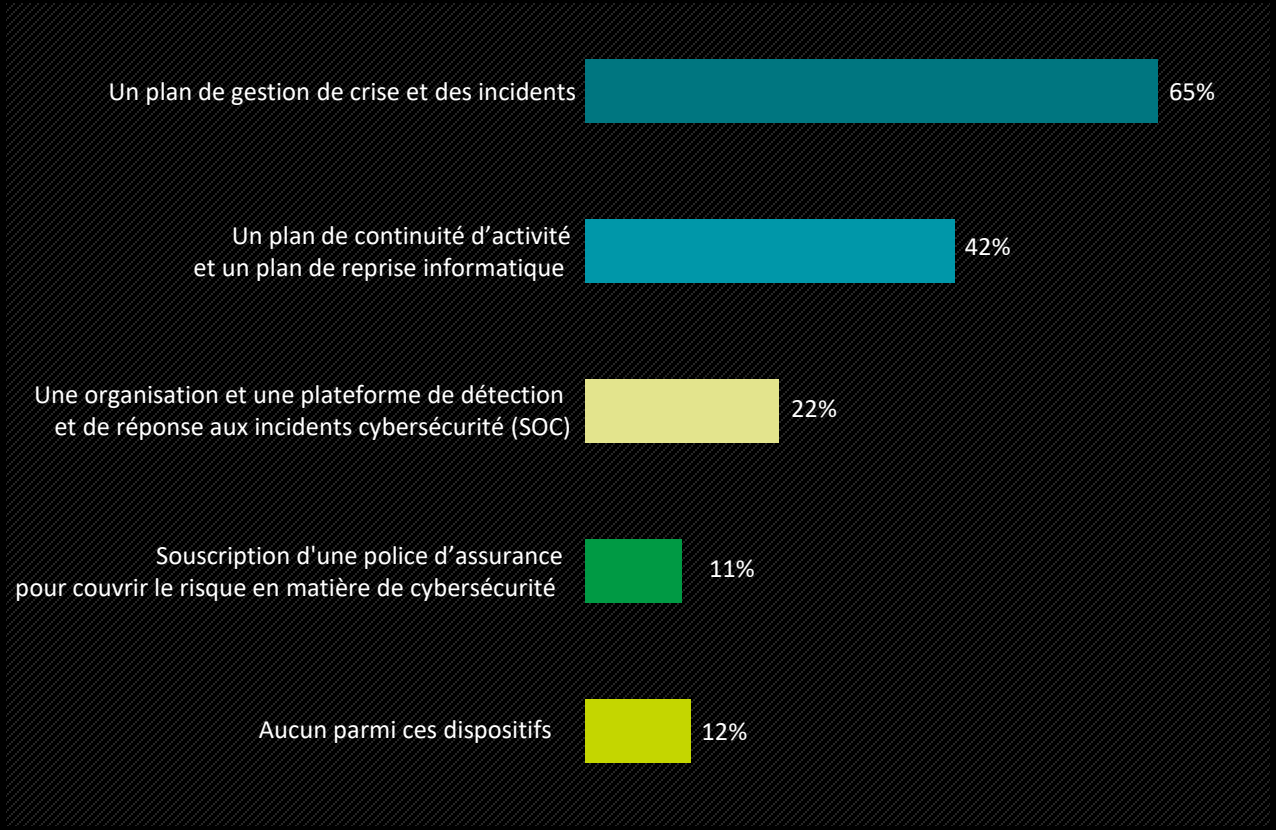
© 2021 Deloitte Afrique SAS

Résilience

Dispositif de résilience face aux incidents cybersécurité

Le dispositif de résilience dans les entreprises africaines reste insuffisant. En effet, uniquement 42% des entreprises sondées disposent d'un plan de continuité d'activité et 11% uniquement ont souscrit à une police d'assurance pour couvrir le risque en matière de cybersécurité

Quels dispositifs avez vous mis en place pour faire face aux incidents cybersécurité?



- Aucune organisation ne peut prédire ou empêcher une attaque. En revanche, elle peut renforcer sa résilience face aux menaces et limiter les dommages causés par une attaque. Elle doit rester constamment en alerte et se tenir prête. C'est pourquoi elles doivent s'efforcer de mettre à jour les différents scénarios de menaces, leurs plans de continuité d'activité et leurs plans de reprise.
- Une majorité des entreprises africaines (65%) a mis en place un cadre opérationnel pour le pilotage et la gestion de crise et des incidents. Cependant, 42% d'entre elles ont défini des plans de continuité d'activité globaux qui détaillent tous les volets techniques et organisationnels nécessaires pour assurer la continuité des opérations suite à un sinistre.
- La cyber assurance restant encore peu répandue dans la région, seules 11% des entreprises en ont souscrit.

Le nombre de cybermenaces ne cesse d'augmenter depuis le début de la pandémie. Disposer d'un plan de continuité d'activité et d'un SOC opérationnel est indispensable pour faire face à ces menaces.

Mohamed YOUSRI, Directeur de la Sécurité du Système d'Information, Sonatrach, Algérie

© 2021 Deloitte Afrique SAS

Méthodologie & Remerciements

© 2021 Deloitte Afrique SAS

Méthodologie

Notre approche

- Le baromètre Deloitte de la maturité Cyber des entreprises en Afrique a été conduit auprès de 210 entreprises africaines, présentes dans 11 pays, répartis dans 3 régions : Afrique du Nord, Afrique de l'Ouest et Afrique Centrale.
- L'objectif était de collecter et analyser des données sur le niveau d'appétence aux risques cyber de nos principaux clients et de pouvoir réaliser ainsi un comparatif de maturité entre industries, pays et régions.

Elaboration de l'étude

L'étude est organisée autour de 9 thématiques d'importance majeure pour les entreprises africaines :

- Contexte
- Investissements
- Stratégie
- Organisation
- Sensibilisation
- Outsourcing
- Technologies
- Détection & Réponse
- Résilience

Communication du questionnaire

- 20 questions ont été envoyées à un échantillon de décideurs et de responsables de sécurité africains, soigneusement identifiés sur la base de critères tels que leur pays d'origine, leur secteur d'activité, leur chiffre d'affaires, leur taille, la structure de leur capital, etc.
- Le but était de mettre à disposition des décideurs un état des lieux sur la maturité des entreprises en cybersécurité en Afrique.

Analyse des résultats

- Les 20 résultats recueillis pour chaque question ont été traités et analysés pour identifier les principales tendances des dirigeants africains et les mettre en perspective avec le contexte commercial, économique, politique et social actuel de l'Afrique.
- Des graphiques ont été réalisés pour illustrer les enseignements tirés.

Entretiens individuels

Ce baromètre a été complété par une série d'entretiens individuels avec des dirigeants d'entreprises africaines afin d'approfondir et enrichir l'étude :

Mme Syrine Tlili, Directrice Générale, ANCE-Tuntrust, Tunisie

M. Fahd Chaouch, Directeur Exécutif, Société Magasin Général, Tunisie

M. Mohamed YOUSRI, Directeur de la Sécurité du Système d'Information, Sonatrach, Algérie

Mme Mame Diop, Sous-Directrice du Système d'Information et de la Sécurité, Orange Côte d'Ivoire

M. Jean Luc Diatta, Directeur du Système d'Information, Banque Régionale de Marchés, Sénégal

M. Mishael Kompani, Directeur Audit Interne, CITI Bank, République Démocratique du Congo

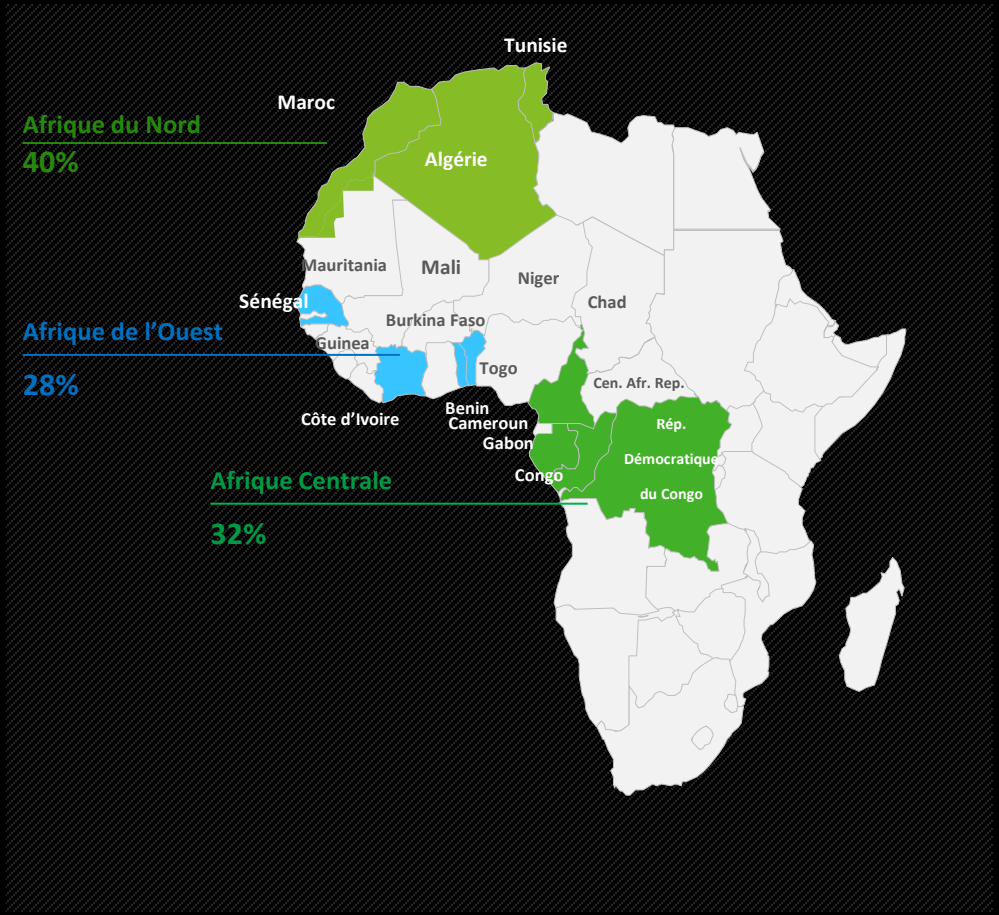
M. Chokri Neji, Directeur Sécurité, Arab Tunisian Bank, Tunisie

© 2021 Deloitte Afrique SAS

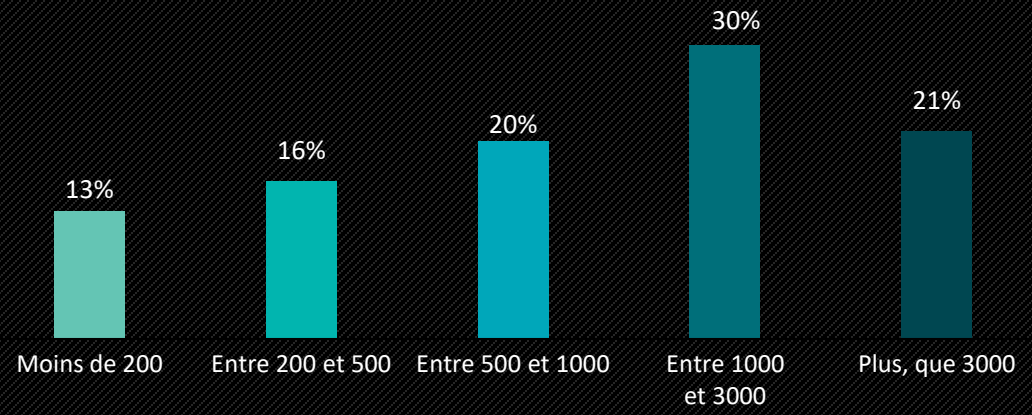
Méthodologie

Aperçu de l'échantillon de répondants

Répondants par région d'Afrique



Répondants par nombre d'employés en Afrique



11 pays représentés :

- **Algérie**
- **Bénin**
- **Cameroun**
- **Congo**
- **Côte d'Ivoire**
- **Gabon**
- **Maroc**
- **République Démocratique du Congo**
- **Togo**
- **Tunisie**
- **Sénégal**

© 2021 Deloitte Afrique SAS

Méthodologie

Aperçu de l'échantillon de répondants

Répondants par secteur d'activité

Services Financiers (Finance, Banque, Assurance & Investissement)

31%

Télécoms, Média & Technologie

20%

Industrie et service

24%

Secteur Public

20%

Autre

5%

© 2021 Deloitte Afrique SAS

Remerciements

Nous souhaitons dans un premier temps remercier tous les dirigeants d’entreprises, responsables de sécurité SI et directeurs des systèmes d’information ayant répondu au questionnaire en ligne et celles et ceux qui ont accepté de rencontrer les Associés et experts de Deloitte à travers le continent pour répondre à nos questions et partager leur point de vue.

Nous tenons également à remercier individuellement les personnalités qui nous ont permis d’illustrer chaque thème à travers des témoignages qualitatifs. Il s’agit de: Mme Syrine Tlili, Directrice Générale, ANCE-Tuntrust, Tunisie; M. Fahd Chaouch, Directeur Exécutif, Société Magasin Général, Tunisie; M. Mohamed YOUSRI, Directeur de la Sécurité du Système d'Information, Sonatrach, Algérie; Mme Mame Diop, Sous-Directrice du Système d'Information et de la Sécurité, Orange Côte d'Ivoire; M. Jean Luc Diatta, Directeur du Système d'Information, Banque Régionale de Marchés (BRM), Sénégal; M. Mishael Kompani, Directeur Audit Interne, CITI Bank, République Démocratique du Congo; M. Chokri Neji, Directeur Sécurité, Arab Tunisian Bank, Tunisie.

Leurs contributions ont permis de compléter ce baromètre par des retours d'expérience pertinents. Chacun d'entre eux s'engage à agir et à impacter positivement le continent africain avec passion et optimisme.

© 2021 Deloitte Afrique SAS

Contacts

© 2021 Deloitte Afrique SAS

Contacts

Aristide Ouattara
Partner, Risk Advisory
Leader Risk Advisory
Deloitte Afrique Francophone
aouattara@deloitte.fr

Sofiane El Abdi
Partner, Cyber Risk
Leader Cyber Risk
Deloitte France et Afrique Francophone
selabdi@deloitte.fr

Dhia Hachicha
Directeur Cyber Risk
Deloitte Afrique Francophone
dhachicha@deloitte.fr

El Hadji Malick Gueye
Directeur Risk Advisory
Deloitte Afrique Francophone
egueye@deloitte.fr

© 2021 Deloitte Afrique SAS

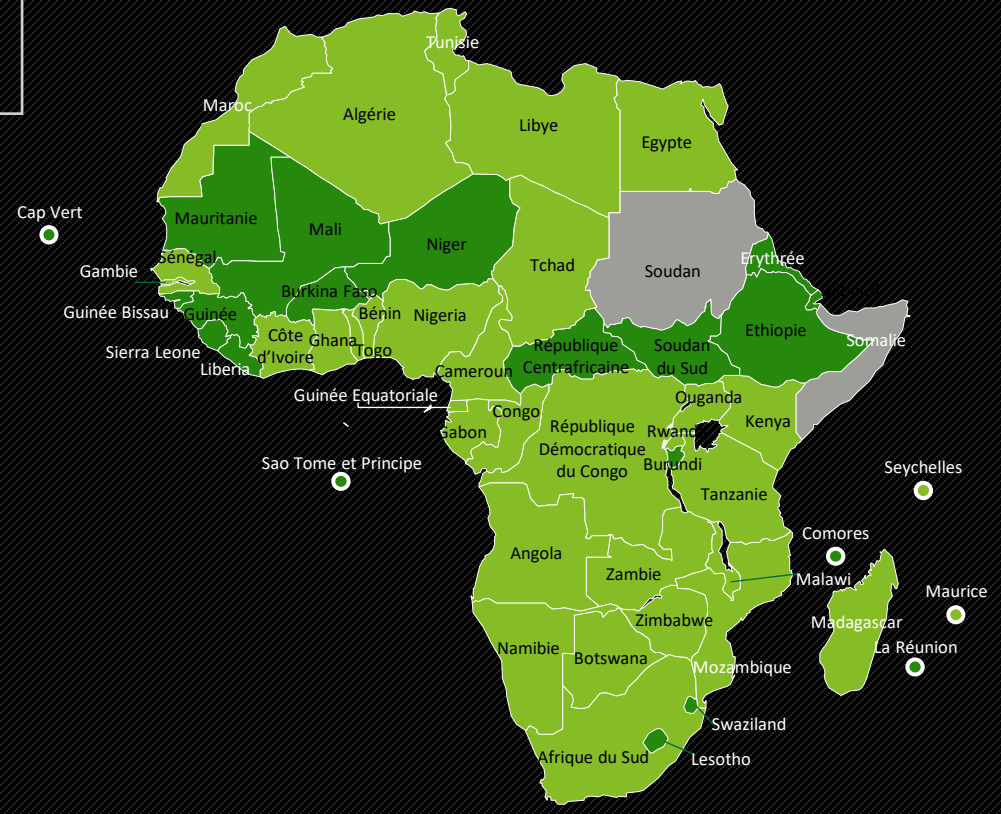
Deloitte en Afrique & Contacts

Make an impact that matters

Présence de Deloitte en Afrique

Présence de Deloitte

- Bureaux Deloitte
- Capacité d'intervention Deloitte
- Pas de présence



9000 professionnels

46 bureaux

52 pays africains servis

Contact

Emmanuel Gadret

Managing Partner

Deloitte Afrique

EGadret@deloitte.fr

© 2021 Deloitte Afrique SAS

Deloitte.

A propos de Deloitte

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited (« DTTL »), à son réseau mondial de cabinets membres et à leurs entités liées (collectivement dénommés « l'organisation Deloitte »). DTTL (également désigné « Deloitte Global ») et chacun de ses cabinets membres et entités liées sont constitués en entités indépendantes et juridiquement distinctes, qui ne peuvent pas s'engager ou se lier les uns aux autres à l'égard des tiers. DTTL et chacun de ses cabinets membres et entités liées sont uniquement responsables de leurs propres actes et manquements, et aucunement de ceux des autres. DTTL ne fournit aucun service aux clients. Pour en savoir plus, consulter www.deloitte.com/about. En France et en Afrique Francophone, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

Deloitte est l'un des principaux cabinets mondiaux de services en audit et assurance, consulting, financial advisory, risk advisory et tax, et services connexes. Nous collaborons avec quatre entreprises sur cinq du Fortune Global 500® grâce à notre réseau mondial de cabinets membres et d'entités liées (collectivement dénommés « l'organisation Deloitte ») dans plus de 150 pays et territoires. Pour en savoir plus sur la manière dont nos 330 000 professionnels make an impact that matters (agissent pour ce qui compte), consultez www.deloitte.com.

En France et en Afrique Francophone, Deloitte regroupe un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs. Fort des expertises de ses 7 000 associés et collaborateurs et d'une offre multidisciplinaire, Deloitte en France et en Afrique Francophone est un acteur de référence. Soucieux d'avoir un impact positif sur notre société, Deloitte a mis en place un plan d'actions ambitieux en matière de développement durable et d'engagement citoyen.

Cette communication ne contient que des informations à caractère général. Cette étude ne constitue ni un avis ni un service professionnel délivré par Deloitte Touche Tohmatsu Limited ou ses firmes membres ou entités liées (ensemble le Réseau Deloitte).

Avant toute décision ou action susceptible d'affecter vos finances ou votre activité commerciale, il vous revient de consulter un professionnel avisé. Aucune entité du réseau Deloitte ne sera tenue responsable d'un quelconque dommage de quelque nature que ce soit fondé directement ou indirectement sur cette communication .

© 2021 Deloitte Afrique SAS. Une entité du réseau Deloitte