Baromètre 2023 de la Cybersécurité et du Cloud en Tunisie

Bilan et perspectives

EY
Building a better working world

SOMMAIRE

ÉDITO

Le Cloud et la Cybersécurité constituent certainement deux enjeux stratégiques majeurs pour nos décideurs, et notamment nos Directeurs des Systèmes d'Information et Responsables de la Sécurité des Systèmes d'Information.

Là où le Cloud est sur l'agenda des décideurs depuis un peu plus de dix ans déjà, l'adoption des entreprises s'est faite avec des approches et un engouement assez disparates. Bien qu'ayant convaincu de nombreuses entreprises, les promesses attendues ne se sont pas matérialisées de façon égale par chacune d'entre elles.

Quant à la Cybersécurité, la prolifération et la multitude des cybermenaces auxquelles nos entreprises doivent faire face les amènent à repenser leur dispositif de gouvernance et de gestion de la Cybersécurité. Elles ne le font probablement pas à un rythme satisfaisant et adapté au niveau des risques, mais elles gagnent progressivement en maturité.

Pour la première fois, EY établit un Baromètre couvrant à la fois le Cloud et la Cybersécurité et visant à comprendre le positionnement de nos entreprises par rapport à ces deux sujets, leurs pratiques ainsi que leurs perspectives.

Le Cloud a-t-il tenu ses promesses? Quelles sont les entreprises qui réussissent à en tirer un véritable avantage métier ? L'approche de la Cybersécurité est-elle réellement en évolution vers les standards et les bonnes pratiques ? Quelles préoccupations freinent une plus grande maturité de nos entreprises sur ces thématiques ?

En parcourant le Baromètre EY Cloud et Cybersécurité, vous trouverez des réponses à ces interrogations légitimes. Les résultats de l'enquête EY vous permettront de prendre connaissance des pratiques en la matière et de situer par déduction les pratiques de votre entreprise par rapport à celles des autres organisations. Ainsi, votre feuille de route de transformation digitale Cloud et Cybersécurité gagnera en clarté, ouvrant la voie à une maturité renforcée.

SAMI ZAOUI

Associé, EY Technology Consulting Leader & FSSA Technology Leader

SENDA BOUKEF

Directrice, EY Technology Transformation

EXECUTIVE SUMMARY

Nous avons interrogé un ensemble d'entreprises privées et administrations publiques tunisiennes à travers un questionnaire en vue d'évaluer les tendances et perspectives du Cloud et de la Cybersécurité pour cette année. Les réponses obtenues nous ont permis de nous centrer sur un échantillon représentatif de 49 organisations privées et publiques, pour la plupart des acteurs majeurs de l'économie tunisienne et couvrant de manière plutôt équilibrée différents secteurs d'activités.

Les retours des Directeurs des Systèmes d'information (DSI) et des Responsables de la Sécurité des Systèmes d'Information (RSSI) qui ont répondu au questionnaire ont fourni un éclairage intéressant sur l'adoption du Cloud et sur les pratiques en matière de Cybersécurité.

Contrairement à nos attentes, les coûts semblent être un facteur mineur dans la décision sur l'approche face au Cloud. Si les entreprises décident d'amorcer leur adoption c'est surtout pour gagner en agilité et pour supporter leur transformation digitale, plutôt que pour réduire leurs coûts informatiques. Les entreprises qui n'ont pas entamé leur migration vers le Cloud sont essentiellement freinées par leur perception de l'offre locale, considérée comme limitée et peu flexible, et par le manque d'expertise pour la gestion du Cloud, plutôt que par ses coûts supposément plus élevés.

Pour la majorité des répondants, aussi bien ceux qui ont adopté le Cloud que ceux qui n'y sont pas, le sujet est dans l'agenda des initiatives pour 2023. Toutefois, les entreprises semblent vouloir prendre du recul et avancer sur un périmètre Cloud avec une approche réfléchie, probablement en vue de faire les bons choix pour un Cloud qui apporte vraiment de la valeur à l'organisation.

Nous notons également que les préoccupations relatives à la sécurité sont rarement absentes de l'approche au Cloud. Les entreprises qui ne sont pas adeptes du Cloud y voient même un avantage potentiel pour une meilleure gestion des risques et une meilleure qualité de service.

En nous intéressant aux aspects liés à la Cybersécurité, notre étude a mis en lumière des budgets relativement limités et des difficultés dans la sensibilisation interne, aussi bien pour assurer l'applicabilité de la politique de sécurité que pour limiter les menaces dues à des défauts de vigilance des collaborateurs.

Sans surprise, les entreprises qui semblent avoir une bonne maturité en Cybersécurité et qui allouent les budgets appropriés pour sa gestion sont mieux positionnées pour détecter rapidement et adresser efficacement les cybermenaces.

Au final, il apparaît que la mise en place des contrôles et des procédures de sécurité appropriées au niveau d'une organisation permet non seulement de mieux maîtriser les risques liés à la Cybersécurité, de faire face plus efficacement aux cybermenaces mais aussi de pouvoir adopter le Cloud plus sereinement et de tirer pleinement profit de ses avantages métier. Les entreprises qui font l'économie des investissements nécessaires à une gestion adaptée de la Cybersécurité risquent non seulement l'impact des cybermenaces qu'elles ne maîtrisent pas, mais aussi de perdre une longueur d'avance en agilité et en compétitivité face à leurs concurrents.

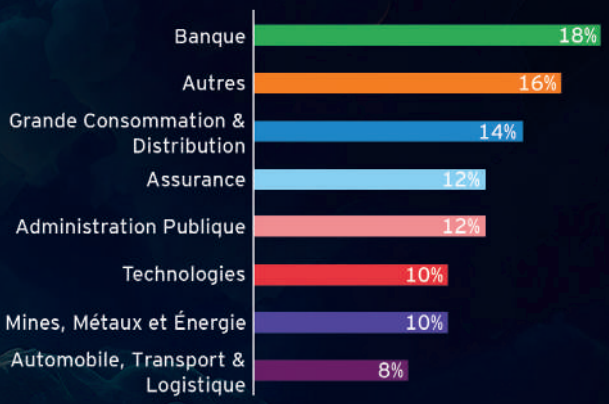
RÉSUMÉ DE L'ÉCHANTILLON

1 Nombre d'entreprises

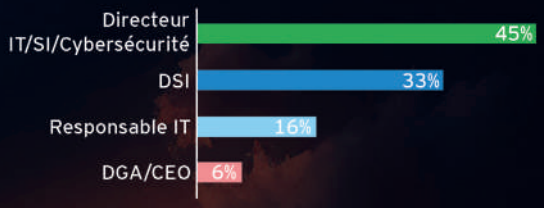
49

2 Type de société

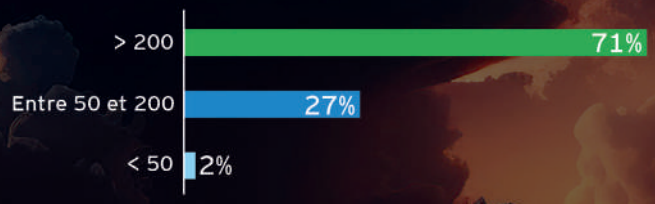
3 Secteur d'activité



4 Profil des répondants



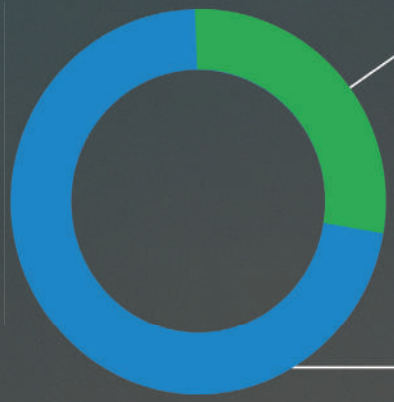
5 Nombre total d'employé



Volet Cloud

1. Perception de l'offre Cloud locale

▸ Une offre Cloud locale le plus souvent considérée comme limitée et peu flexible.

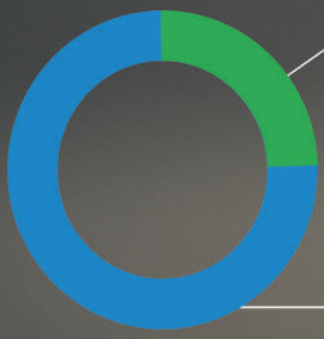


28%
Considèrent que l'offre Cloud locale est complète et adaptée

72%
Considèrent que l'offre Cloud locale est soit limitée et peu flexible soit orientée hébergement et non alignée avec le modèle Cloud

2. Adoption

▸ L'utilisation du Cloud est désormais bien répandue au sein des entreprises



24%
des répondants n'utilisent aucun service Cloud

76%
des répondants déclarent utiliser des services Cloud et non alignée avec le modèle Cloud

▸ Les entreprises qui «résistent» au Cloud sont conscientes de ses avantages potentiels mais préfèrent garder le contrôle

Une perception positive :

62% des répondants y voient une meilleure gestion des risques et un meilleur niveau de service

54% des répondants y voient une plus grande agilité et un accès aux technologies avancées

Les principaux défis et freins au changement

54% des répondants ont cité une absence d'une offre de service appropriée

100% des répondants du secteur bancaire ont mentionné des limitations règlementaires sur l'usage du Cloud

Les initiatives Cloud prévues pour les entreprises qui «résistent»

75% ont prévu de commencer à identifier le périmètre pertinent pour le Cloud

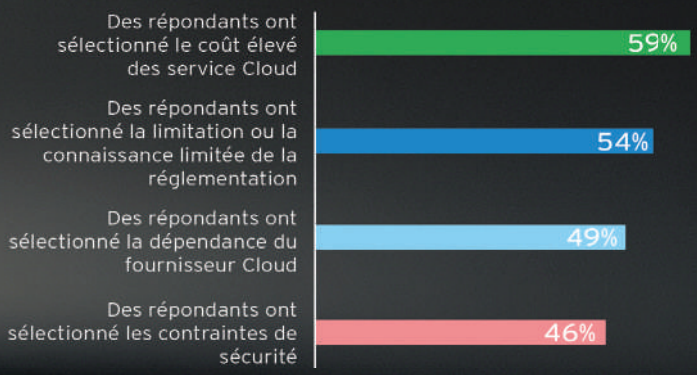
25% projettent de migrer vers le Cloud

▸ Une adoption du Cloud faite à différentes vitesses et pour diverses motivations

Le principal moteur de l'adoption du Cloud

75% des répondants trouvent l'agilité comme principal moteur d'adoption du Cloud

Même lorsque le Cloud a été adopté, les entreprises voient des freins à une adoption plus forte ou plus généralisée au sein de l'organisation



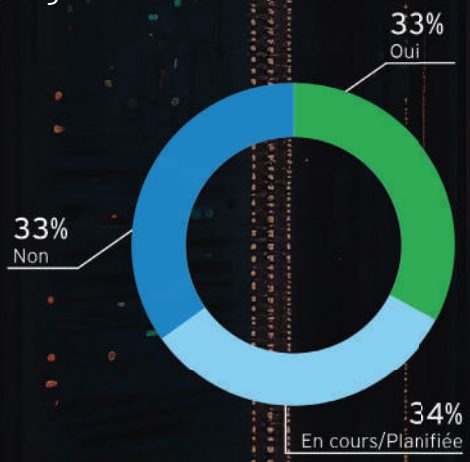
Volet Cybersécurité

1 *Des difficultés pour faire appliquer la politique de sécurité*

74% des répondants déclarent avoir une politique de sécurité documentée

47% ont déclaré que la politique de sécurité documentée est partiellement ou peu appliquée

2 *La mise en place de Centre Opérationnel de Sécurité (SOC) est en progression*



3 *Des budgets limités dédiés à la Cybersécurité dans la majorité des secteurs d'activité*

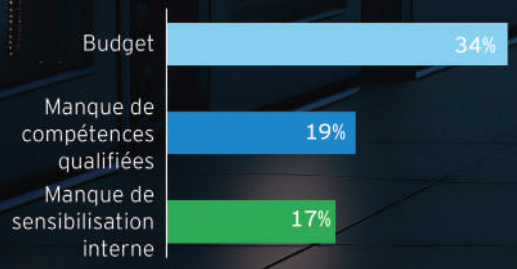
38% des répondants déclarent disposer d'un budget inférieur à 100 mille dinars

Les secteurs d'activité qui investissent le plus dans la Cybersécurité sont les Banques, les Assurances et les Télécommunications

4 *Des priorités d'investissement en Cybersécurité alignées avec les préoccupations, mais probablement en manque de budget*

58% des répondants déclarent la protection des données comme la priorité numéro 1 en matière d'investissements en Cybersécurité

5 *Le manque de budget est le principal obstacle à une gestion efficace et satisfaisante de la Cybersécurité*



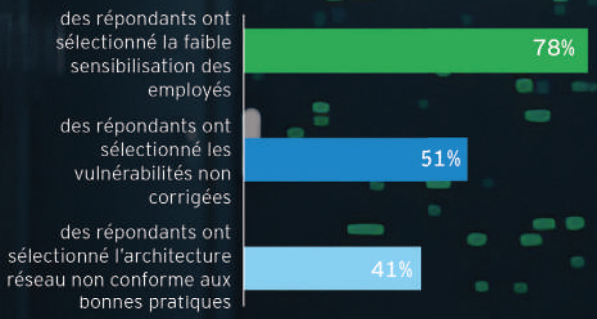
6

Le défaut de vigilance des collaborateurs constitue une part significative des sources potentielles de menaces

41% Hackers (externe)

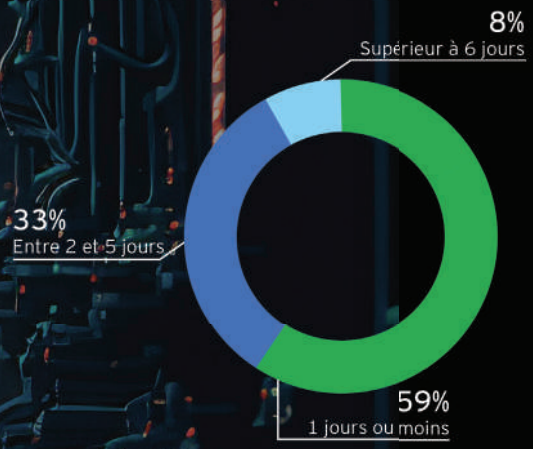
37% Défaut de vigilance des employés (interne)

Les principales faiblesses



7

Les entreprises qui ont mis en place un SOC ont généralement une capacité accrue à détecter et à adresser rapidement les incidents de sécurité.



8

Une satisfaction des moyens de protection qui va de pair avec les dépenses en Cybersécurité

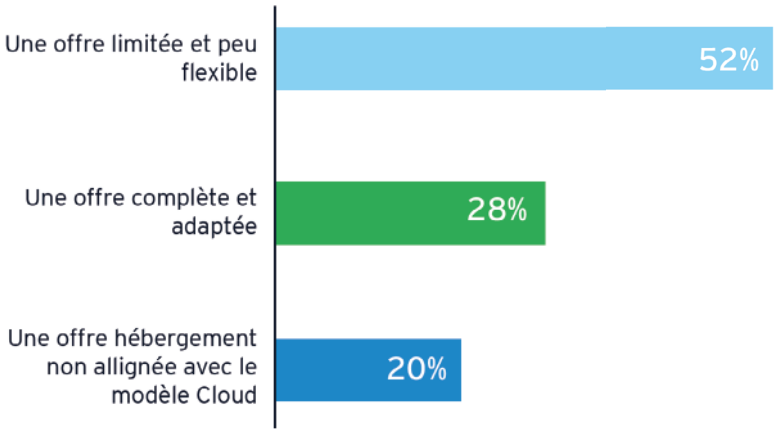
84% des répondants déclarent êtres non satisfaits ou partiellement satisfaits des moyens technologiques à leur disposition pour garantir la sécurité des actifs de l'entreprise. Toutes les entreprises dépensant plus de 250 mille dinars déclarent être satisfaites des moyens de protection.

Baromètre Cloud

1 PERCEPTION DE L'OFFRE CLOUD LOCALE

UNE OFFRE CLOUD LOCALE LE PLUS SOUVENT CONSIDÉRÉE COMME LIMITÉE ET PEU FLEXIBLE.

Quelle est votre perception de l'offre de service Cloud du marché local (49 sociétés) ?



72% des répondants considèrent que l'offre Cloud locale est soit limitée et peu flexible soit orientée hébergement et non alignée avec le modèle Cloud

Seuls 28% des répondants considèrent que l'offre Cloud locale est complète et adaptée. Le reste des répondants, qu'ils soient utilisateurs de Cloud ou non, estiment que l'offre est soit limitée et peu flexible soit orientée hébergement et non alignée avec le modèle Cloud.

Il est par ailleurs vrai que le terme «Cloud» est souvent utilisé par les décideurs, et notamment les Directeurs des Systèmes d'Information, pour désigner de manière très générale les services d'externalisation, sans que les caractéristiques typiques d'une offre Cloud, à savoir : **le self-service, l'automatisation, l'élasticité** et **la facturation à l'utilisation,** soient effectivement incluses.

Le self-service ou le **libre-service à la demande** permet à l'utilisateur d'un service Cloud de créer les ressources dont il a besoin à travers un portail. Par exemple : un développeur qui a besoin de travailler sur une base de données pourra sélectionner la base de données (Database as a Service) de son choix sur le portail de l'offre Cloud et pourra y accéder directement dès sa création, en général très rapide, plutôt que de demander au service informatique de lui en créer une, ce qui peut prendre plusieurs jours.

L'automatisation est relative à l'automatisation des différents processus nécessaires à la création d'un service Cloud. Dans l'exemple précédent, lors de la demande de création de la base de données en mode service, l'utilisateur sélectionne les options de configurations. Le service Cloud procède à la création de la base de données en automatisant les opérations nécessaires, entre autres la configuration de l'accès pour l'utilisateur ou l'affectation de l'espace de stockage. Ceci permet non seulement de minimiser les risques d'erreur mais aussi de minimiser les délais d'approvisionnement. La base de données est mise à disposition au bout de quelques minutes au lieu de plusieurs jours.

L'élasticité d'un service Cloud est sa capacité à s'adapter rapidement aux besoins des applications qu'il supporte, soit en augmentant ou en réduisant les ressources associées (mémoire, stockage, etc.). Si dans l'exemple plus haut, la base de données Cloud peut être exposée à des charges significativement plus élevées en fin de mois, l'élasticité permettra à la base de données d'avoir des capacités importantes en fin de mois et des capacités moindres en dehors de cette période.

La facturation à l'utilisation est ce qui permet à un utilisateur de service Cloud de ne payer que pour les ressources qu'il consomme effectivement, plutôt que pour un service fixe. Dans l'exemple précédent, le coût de la base de données pourra être élevé en fin de mois et moins élevé les jours où ses capacités sont moindres.

Nous comprenons par ailleurs que le potentiel du marché tunisien n'a pas permis aux fournisseurs de services Cloud locaux de développer des offres à l'image des *hyperscalers* internationaux (les fournisseurs Cloud mondiaux à très grande échelle, tels que : Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, Alibaba Cloud). Il n'est pas exclu que les répondants satisfaits de l'offre Cloud locale soient en réalité satisfaits de l'offre d'hébergement, au vu du nombre de Data Centers locaux aux normes internationales.

Nous retenons que la nature de l'offre Cloud locale a un impact certain sur les degrés d'adoption du Cloud. En effet, les entreprises ont généralement une certaine réticence à l'hébergement des données à l'extérieur du territoire, même lorsque la réglementation le permet. Cette étude a fait ressortir que 13% des entreprises semblent avoir une connaissance limitée de la règlementation liée au Cloud. Dans l'étude EY publiée en 2021 «Cloud Computing : où en est l'Afrique francophone?», 70% des entreprises déclaraient ne pas connaître suffisamment la règlementation liée au Cloud. Très souvent, le choix d'un fournisseur Cloud qui héberge les données dans le pays est motivé par une perception de la règlementation plutôt que par une compréhension approfondie de celle-ci.

Pendant longtemps, la règlementation relative à l'hébergement des données et des applications en mode Cloud s'est limitée à la règlementation sur la protection des Données Personnelles, largement inspirée de la Règlementation Générale pour la Protection des Données Personnelles (RGPD) Européenne comme c'est le cas pour de nombreuses règlementations similaires à travers le monde.

Un nouveau décret présidentiel sur la Cybersécurité a été publié dans le Jort du samedi 11 mars 2023. Le texte de loi vise à organiser davantage le domaine de la Cybersécurité en Tunisie ainsi que les missions de l'Agence Nationale de la Sécurité Informatique (ANSI) chargée de la gouvernance du cyberespace national. Sa nomination devient par ailleurs "Agence Nationale de la Sécurité Cybernétique" (ANSC).

Entre autres missions, l'ANSC sera chargée d'attribuer le label «sécurisé» à chaque logiciel ou équipement électronique sur demande du développeur ou de l'importateur.

En vertu de ce décret, les structures qui gèrent des **infrastructures numériques d'importance vitale** sont tenues d'utiliser des logiciels et équipements ayant le label « sécurisé », avoir leur propre centre d'hébergement principal et un centre de secours **auprès d'un fournisseur de services Cloud ayant obtenu le label**, respecter les mesures et les procédures nécessaires pour assurer la continuité d'activité et protéger les bases de données sensibles dont la compromission pourrait affecter la sécurité nationale en cas de crise cybernétique, et ce selon un manuel de procédure approuvé par décret, sur proposition du Ministre chargé des Technologies de la Communication.

L'ANSC sera également chargée d'attribuer, de renouveler et de retirer le label «Fournisseur de services informatiques en nuage gouvernemental (G-cloud)» et le label « Fournisseur de services informatiques en nuage national (N-cloud) » aux fournisseurs des services d'hébergement après avis des Ministres de la Défense Nationale et de l'Intérieur.

Nous nous attendons à de futurs développements fournissant plus de spécificités dans la règlementation dans les semaines ou mois à venir.

2 LES ENTREPRISES QUI «RÉSISTENT» AU CLOUD

LES ENTREPRISES QUI « RÉSISTENT » AU CLOUD SONT CONSCIENTES DE SES AVANTAGES POTENTIELS MAIS PRÉFÈRENT GARDER LE CONTRÔLE

> “En ne prenant pas le risque d’aller vers le Cloud, on risque surtout d’être dépassé par ceux qui l’auront adopté efficacement.

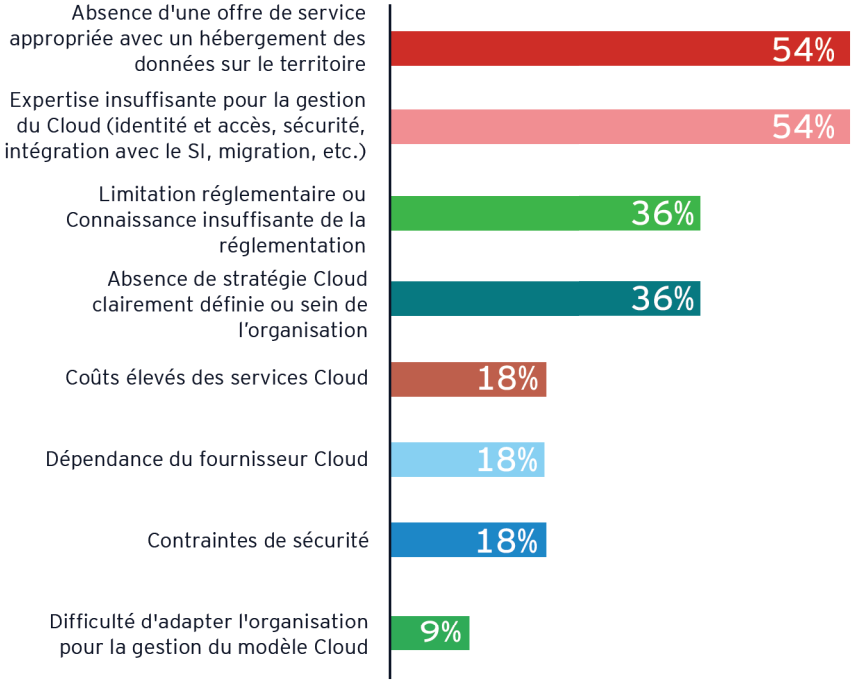
Nous parlons de « résistance » parce qu’il y a une forte orientation mondiale, notamment de la part des éditeurs logiciels, pour favoriser de plus en plus le modèle Cloud dans leurs offres. Cette tendance est de plus renforcée par le nombre croissant d’entreprises qui adoptent la stratégie de « Cloud First », consistant à adopter le modèle Cloud pour toute nouvelle infrastructure, plateforme ou application.

24% des entreprises sollicitées n’utilisent aucun service Cloud mais le sujet ne leur est pas inconnu. Elles ont leur propre vision des apports potentiels du Cloud et ont conscience de ce qui inhibe ou freine leur adoption.

Il n’est toutefois pas exclu que certaines d’entre elles soient tout de même en train d’utiliser le Cloud pour les services de messagerie et de collaboration ou encore pour certaines applications métier.

La résistance au Cloud est principalement motivée par un besoin de contrôle et par le manque d'expertise pour la gestion du Cloud

Quels sont les principaux défis ou freins à l'utilisation du Cloud dans votre organisation (Pour les entreprises qui n'ont pas encore utilisé les services Cloud) ?



La migration vers le Cloud peut être un processus difficile pour de nombreuses organisations. En fait, notre enquête a révélé que 24% des entreprises sollicitées rencontrent encore des difficultés ou des obstacles à l'adoption du Cloud. L'un des principaux obstacles cités dans l'enquête, qui concerne 54% des répondants, est l'absence d'une offre de services appropriée et flexible sur le territoire local. Cette question est particulièrement cruciale pour les entreprises soumises à des réglementations strictes en matière de protection de données. Si les fournisseurs de services Cloud ne peuvent pas répondre à ces exigences, cela peut entraver l'adoption du Cloud. Si au contraire, les fournisseurs de services Cloud continuent à développer des solutions spécialisées qui répondent aux besoins et aux exigences uniques des différents secteurs et environnements réglementaires, il est possible que l'adoption du Cloud continue à croître et finisse par convaincre les entreprises qui ont jusque-là résisté à son adoption.

Une autre raison pour laquelle certaines entreprises ont été réticentes à adopter le Cloud est le manque d'expertise pour sa gestion, y compris la gestion des identités et des accès, la sécurité et l'intégration avec les systèmes d'information existants. Ce problème se pose également à l'échelle mondiale. En effet, selon le rapport Cloud Security 2022 mené par Cybersecurity Insiders, le manque d'expertise du personnel empêche

40% des répondants d'adopter des solutions Cloud pour leur organisation.

Il est également important de noter que des entreprises du secteur bancaire ont mentionné les limitations règlementaires sur l'usage du Cloud comme un obstacle majeur.

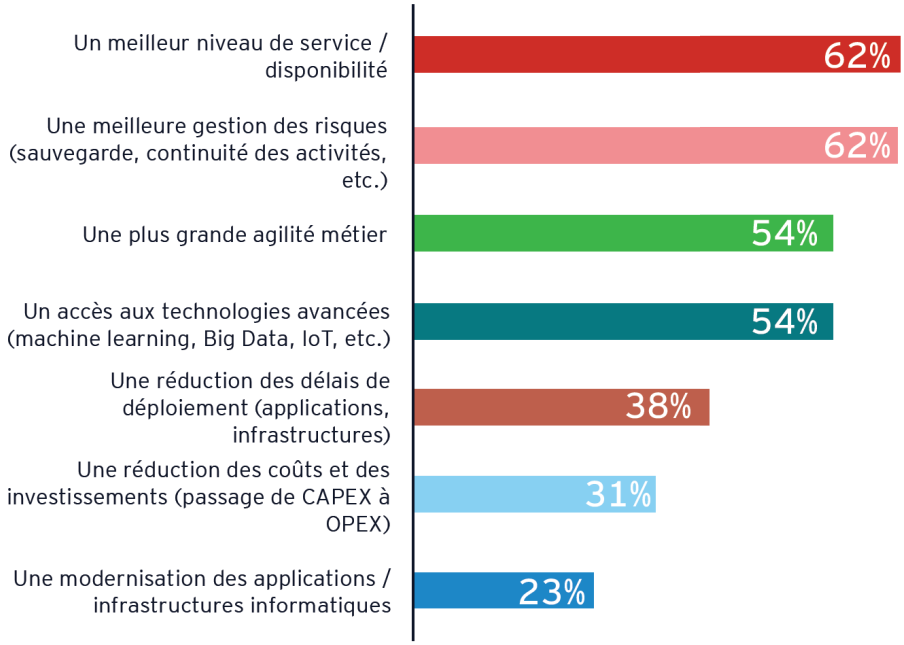
En revanche, très peu de répondants ont mentionné les coûts du Cloud comme frein à son adoption.

Le Cloud étant un modèle où l'organisation et la gouvernance IT sont impactés, la résistance au changement reste également une cause implicite de la résistance à son adoption.

Là où la stratégie de « non-Cloud » ne peut pas être contestée, ce que ces entreprises risquent réellement c'est de voir leurs compétiteurs tirer bénéfice du Cloud pour déployer rapidement de nouvelles applications en vue d'optimiser l'expérience client ou de proposer de nouveaux services.

Sur les répondants qui n'utilisent pas les services Cloud, la majorité des sélections relatives aux potentiels avantages du Cloud tournent autour d'une meilleure gestion des risques, un meilleur niveau de service ainsi que l'accès aux technologies avancées

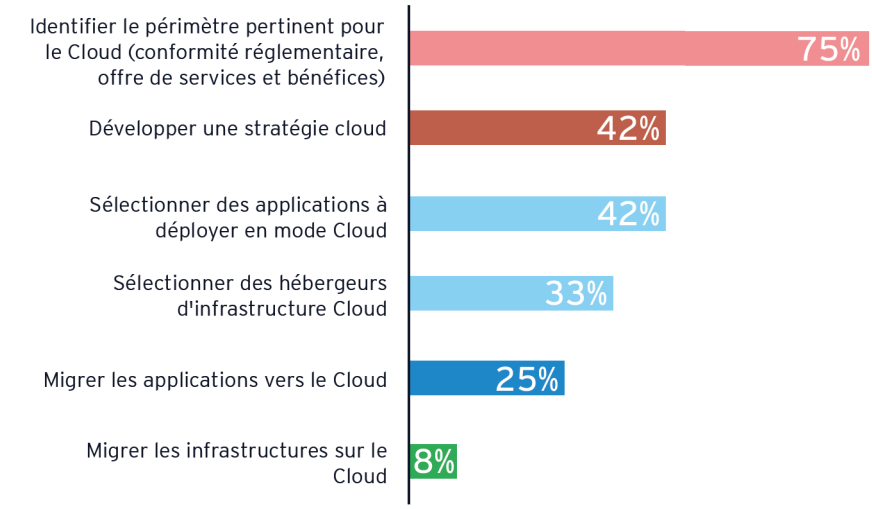
Quelle est votre perception des potentiels avantages du Cloud ? (12 sociétés celles qui n'utilisent pas les services Cloud)



Là où on pourrait penser que la sécurité et la gestion des risques constituent des freins à l'adoption du Cloud, les entreprises qui n'utilisent pas les services Cloud y trouve au contraire un avantage potentiel. Ces dernières estiment également que le Cloud sera en mesure de leur offrir un meilleur niveau de service, un accès aux technologies avancées et une plus grande agilité métier.

Si une grande partie des entreprises qui n'utilisent pas le Cloud projettent en 2023 de démarrer une réflexion sur son adoption, seules 25% projettent réellement de migrer des environnements vers le Cloud

Quelles sont vos initiatives Cloud prévues en 2023 ? (12 sociétés celles qui n'utilisent pas les services Cloud)



75% des entreprises qui n'ont pas adopté le Cloud projettent tout de même en 2023 de commencer à identifier le périmètre pertinent pour le Cloud, celui susceptible de leur apporter réellement de la valeur métier. Elles prévoient également de sélectionner les applications à déployer en mode Cloud et de développer une stratégie Cloud appropriée.

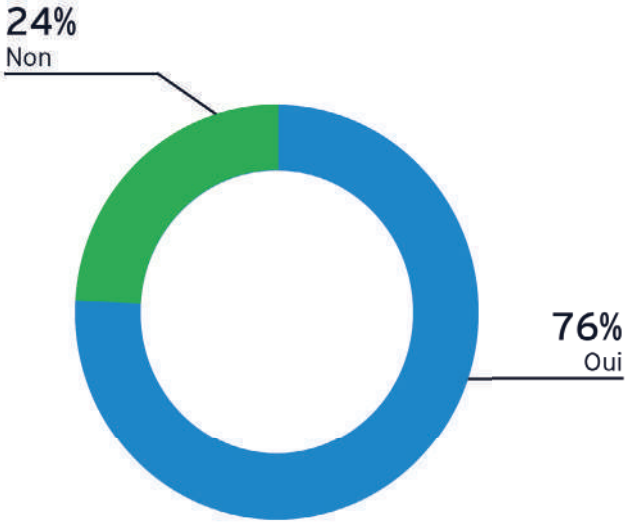
Selon Gartner, d'ici 2026, près de 80% des grandes organisations auront fait appel à des consultants externes pour élaborer leur stratégie Cloud, contre 46% en 2020.

Toutefois, seules 25% projettent effectivement d'entamer la migration vers le Cloud en 2023. Ceci sous-entend d'une part que ces entreprises n'y voient pas d'urgence et surtout qu'elles souhaitent prendre le temps d'opérer l'adoption avec une approche structurée et réfléchie.

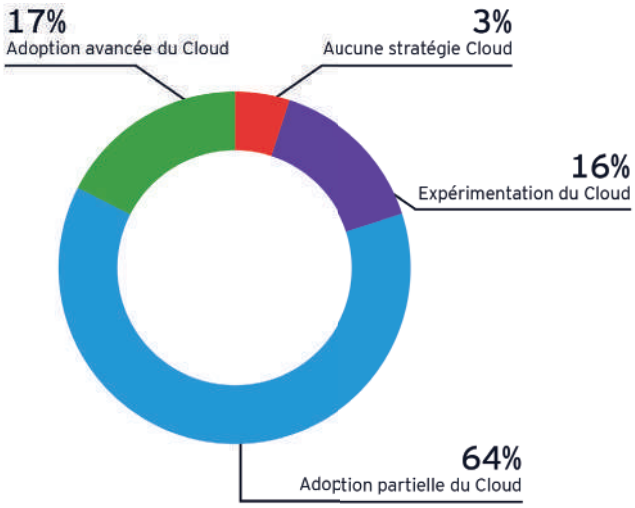
3 UNE ADOPTION DU CLOUD À DIFFÉRENTES VITESSES

76% des répondants déclarent utiliser des services Cloud. Sur cette population, seuls 18% déclarent adopter le Cloud de manière avancée.

Votre organisation utilise-t-elle des services Cloud ?



Quel est le niveau d'adoption du Cloud au sein de votre organisation ?



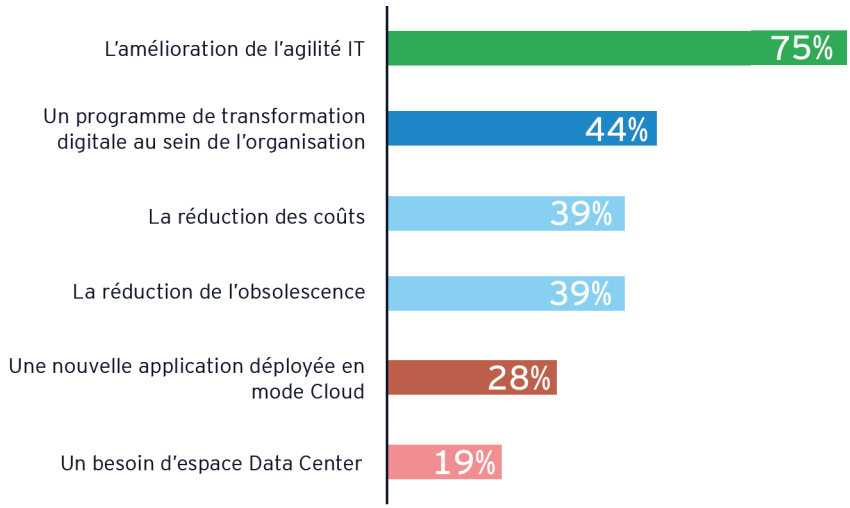
L'adoption du Cloud suit la tendance générale observée dans les autres pays Africains francophones. En effet, selon l'étude EY publiée en 2021 «Cloud Computing : où en est l'Afrique francophone ?», le niveau d'adoption est de 75%.

Sur les entreprises qui utilisent le Cloud en Tunisie, 16% sont encore au stade d'expérimentation, 17% ont une adoption avancée et la grande majorité, à hauteur de 64%, est plutôt dans une adoption partielle. Nous notons que 3% des répondants qui utilisent le Cloud assument le faire sans aucune stratégie préalable.

Nous notons également que les Banques et les Assurances constituent le secteur d'activité où l'adoption du Cloud est la plus forte.

L'agilité reste le principal moteur d'adoption du Cloud, là où le gain en coût semble avoir une importance moindre.

Quels ont été les principaux moteurs de votre adoption Cloud ?

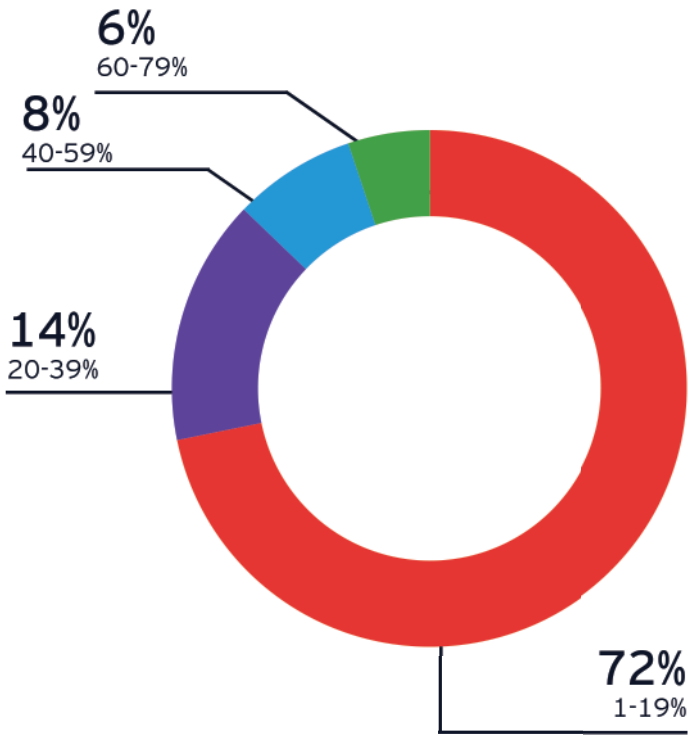


L'amélioration de l'agilité IT arrive en tête des moteurs de l'adoption du Cloud pour 75% des répondants. En deuxième position, les programmes de transformation digitale semblent avoir motivé l'adoption du Cloud avec 44% des entreprises. La réduction des coûts et la réduction des obsolescences arrivent en troisième position avec 39%.

Les résultats de cette question peuvent refléter une bonne compréhension du modèle Cloud et de ses avantages potentiels par les entreprises qui l'ont adopté.

Une part modérée des coûts opérationnels informatiques est dédiée au Cloud, naturellement en augmentation avec le niveau d'adoption

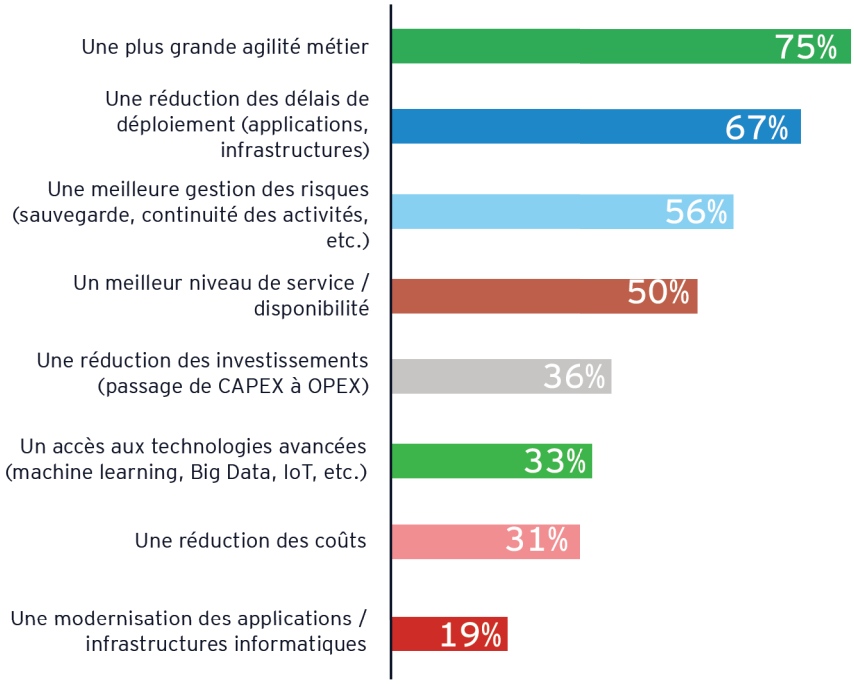
Quelle est la part de vos coûts opérationnels informatiques consacrés au Cloud ?



72% des répondants qui utilisent les services Cloud y consacrent moins de 19% de leurs coûts opérationnels et plus de 14% des répondants déclarent y consacrer plus de 40% de leurs coûts opérationnels. Ces derniers sont essentiellement ceux qui déclarent avoir une adoption avancée du Cloud.

Le Cloud a été plutôt fidèle à sa promesse pour une plus grande agilité mais a de plus démontré un apport certain pour une meilleure gestion des risques au sein de l'organisation

Quels sont les principaux bénéfices que le Cloud a apporté à votre organisation ?



L'agilité métier est reconnue comme le principal apport du Cloud, suivie de la réduction des délais de déploiement, d'une meilleure gestion des risques puis d'un meilleur niveau de disponibilité. Viennent ensuite la réduction des investissements, l'accès aux technologies avancées, la réduction des coûts et finalement la modernisation des applications et des infrastructures.

Cette question s'intéresse aux bénéfices que les entreprises ont réellement expérimenté suite à leur adoption du Cloud. Si nous comparons ces résultats avec les moteurs de l'adoption du Cloud, nous pouvons avancer que :

- Le Cloud a globalement répondu aux attentes pour un gain en agilité, IT et métier,

- Une meilleure gestion des risques a été constatée sans qu'elle ait été ciblée au départ,

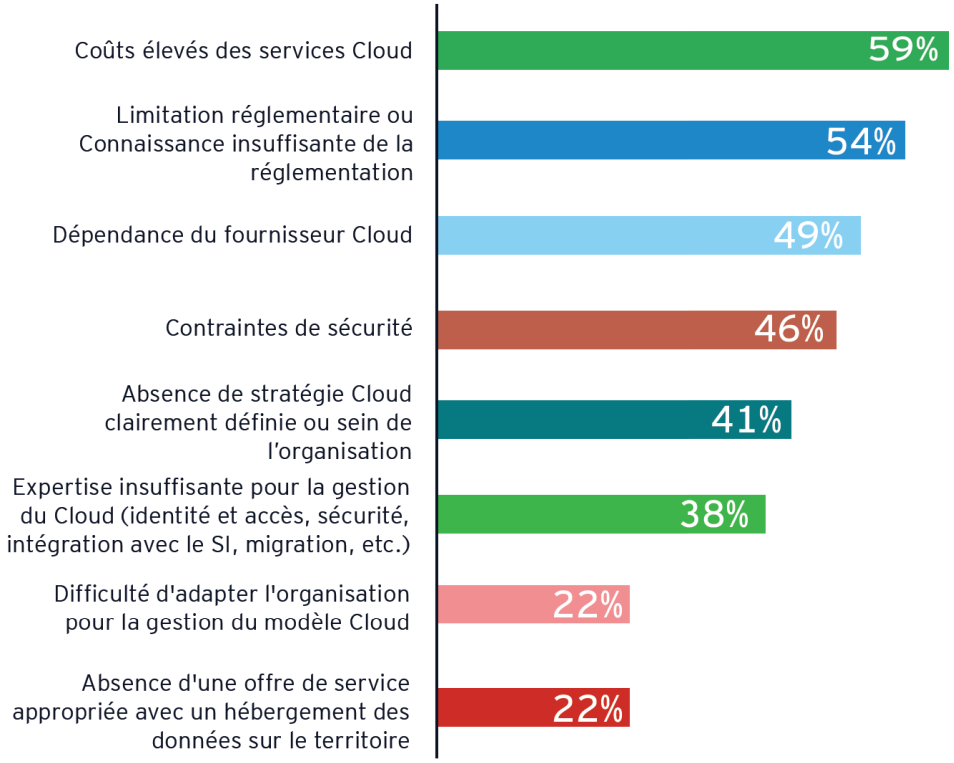
- Si le gain en coût n'a pas été un facteur important pour l'adoption, les entreprises ne le considèrent pas non plus comme un avantage significatif du modèle Cloud.

Néanmoins, la possibilité de réduire les investissements en passant à **une facturation mensuelle ou trimestrielle** pour les services Cloud reste appréciée. L'avantage financier lié aux modalités de facturation du Cloud séduit moins certaines organisations, tenues de consommer un budget alloué et préférant le « sécuriser » dans des acquisitions de matériel et de logiciel.

L'efficacité du Cloud dans la gestion des risques s'explique par l**a standardisation et l'alignement de ses offres aux standards internationaux de sécurité,** ainsi que par **sa capacité à répondre efficacement à divers cas d'usages pour la sauvegarde, la restauration et le secours informatique.**

Le business case du Cloud ne semble pas convaincre; les coûts associés, considérés comme élevés restent le principal frein à une adoption plus étendue du Cloud.

Quels sont les principaux défis ou freins à l'utilisation du Cloud dans votre organisation ?



Même lorsque le Cloud a été adopté, les entreprises voient des freins à une adoption plus forte ou plus généralisée dans l'organisation. Le coût arrive en tête des freins, suivi par la contrainte de dépendance au fournisseur Cloud, puis par la connaissance insuffisante des réglementations et la limitation réglementaire sur l'usage du Cloud pour les données sensibles. Finalement viennent l'insuffisance de l'expertise pour la gestion du Cloud, les contraintes de sécurité et l'absence de stratégie Cloud.

Si nous nous intéressons aux coûts, nous estimons que les entreprises font probablement face à deux difficultés :

D'une part, **la difficulté de comparer les coûts des services Cloud**, qui incluent toutes les composants nécessaires à la fourniture du service – hébergement, infrastructure système, réseau, sécurité, automatisation, supervision, accès réseau, services de gestion, etc. -, avec les coûts d'un service plus ou moins équivalent fourni de manière «traditionnelle» dans le Data Center de l'entreprise. En théorie, les coûts du service Cloud devraient être plus bas du fait de la mutualisation des ressources et de l'économie d'échelle mais un Directeur des Systèmes d'Information n'arrivera pas forcément à quantifier de manière précise ce que lui coûte réellement une application ou un serveur Windows.

D'autre part, **la maîtrise des coûts du Cloud est un défi en soi**. La facturation à l'usage de plusieurs services Cloud est certes attrayante mais elle pose la difficulté de pouvoir prévoir et planifier avec précision les coûts du Cloud avant le démarrage d'un projet. Il est également nécessaire de suivre rigoureusement les coûts et l'utilisation des ressources afin de ne manquer aucune opportunité d'optimisation. L'adoption du Cloud s'accompagne nécessairement par un changement organisationnel en support d'une gestion différente des coûts informatiques.

Quant à la crainte de dépendance au fournisseur Cloud, elle peut être comprise à travers deux axes : D'un côté, **la dépendance par rapport à la solution technique du fournisseur Cloud** qui pourrait être moins flexible qu'une solution classique.

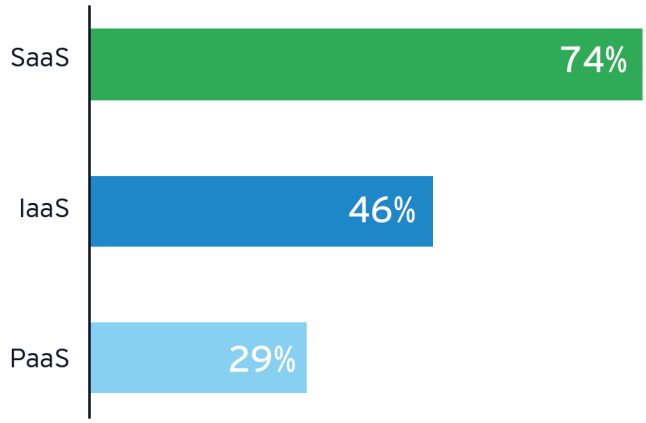
De l'autre, **la dépendance contractuelle sur le périmètre de responsabilités respectives et sur les niveaux de service.** Cette préoccupation suggère que les organisations peuvent être confrontées à des défis récurrents dans la gestion de leurs relations avec les fournisseurs de services Cloud. Cela souligne l'importance de sélectionner un fournisseur qui s'aligne sur les besoins et les objectifs de l'organisation, de prendre le temps de revoir les contrats de services Cloud et de contrôler régulièrement la relation avec le fournisseur pour s'assurer qu'elle reste efficace et bénéfique.

Paradoxalement, le Cloud peut être vu comme offrant plus de flexibilité aux entreprises (à travers l'accès à une panoplie de services extensibles, disponibles à la demande avec une facturation souple) ou comme limitant les niveaux de flexibilité auxquels un Directeur des Systèmes d'Information est habitué (du fait de la standardisation des offres en mode Cloud). **Adopter efficacement le Cloud implique de trouver la bonne balance entre acquis et compromis.**

4 CARTOGRAPHIE DES SERVICES CLOUD UTILISÉS

Les services SaaS restent les services Cloud les plus largement utilisés

Quels sont les types de services Cloud utilisés dans votre entreprise



Selon les données de l'enquête, les services logiciels en mode Cloud (SaaS) sont les plus largement utilisé au sein des organisations avec 74% des entreprises qui déclarent les utiliser. Ces taux d'utilisation sont cohérents avec les chiffres de la région Afrique, Turquie et Moyen-Orient.

Avec un service Cloud de type Infrastructure en tant que service ou ***Infrastructure as a Service (IaaS)***, le fournisseur de service Cloud fournit et gère l'infrastructure (réseau, stockage, système) et met à la disposition du client un élément d'infrastructure prêt à l'emploi, tel qu'un serveur par exemple, et où le client fournit et gère les couches middleware et applicative.

Les services Cloud de type Plateforme en tant que service ou ***Platform as a Service (PaaS)*** sont généralement destinés aux développeurs. Le fournisseur de service Cloud fournit et gère l'infrastructure (réseau, stockage, système) ainsi que les logiciels de base (système d'exploitation et middleware) et met à la disposition de l'utilisateur un élément de plateforme prêt à l'emploi, tel qu'une base de données ou un serveur d'application par exemple.

Avec un service Cloud de type Logiciel en tant que service ou ***Software as a Service (SaaS)***, le fournisseur de service Cloud fournit et gère le logiciel ainsi que l'infrastructure sous-jacente (réseau, stockage, système) et met à la disposition du client une application prête à l'emploi, tel qu'une application de gestion des ressources humaines par exemple. Le client accède directement à l'application pour l'utiliser.

Avec un service Cloud de type Processus Métier en tant que service ou ***Business Process as a Service (BPaaS)***, le fournisseur de service Cloud gère un processus métier de bout en bout pour le compte du client, y compris la solution logicielle utilisée pour ce processus métier ainsi que l'infrastructure sous-jacente. Les exemples incluent l'externalisation de la gestion des fiches de paie ou des notes de frais chez un fournisseur Cloud.

Ce résultat n'est pas surprenant. Il est tout à fait attendu que les avantages du Cloud soient plus conséquents lorsqu'on monte dans la chaîne de service Cloud.

Une entreprise qui utilise une offre Cloud de type infrastructure (IaaS) reste généralement responsable de la gestion opérationnelle de l'infrastructure (haute disponibilité, sauvegarde, correctifs de sécurité, etc.) mais aussi des couches middleware et applicative.

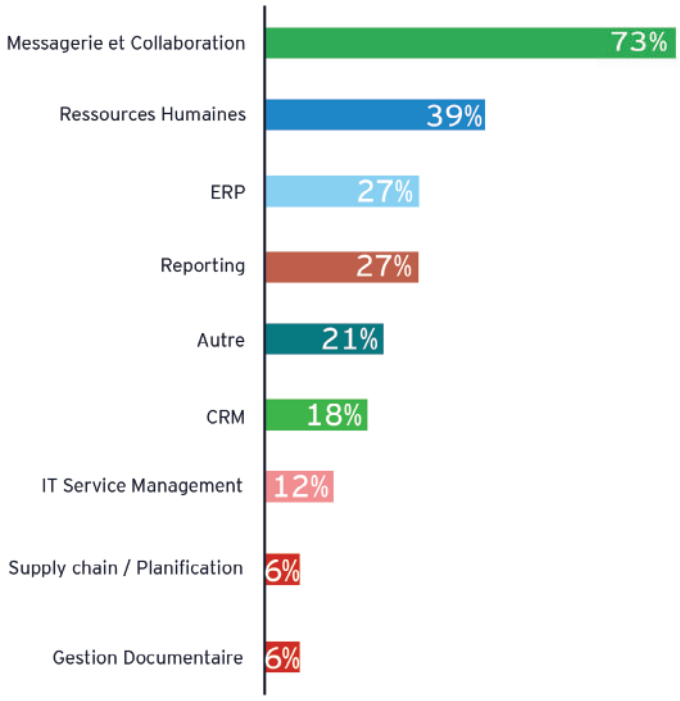
Une entreprise qui utilise la même application en mode Software comme service (SaaS) a directement accès à l'application pour l'utiliser ; le fournisseur Cloud gère l'ensemble des couches sous-jacentes.

Cependant, les prédictions de plusieurs analystes aussi bien sur la région qu'au niveau mondial s'orientent vers une croissance plus élevée et plus rapide du marché IaaS. L'étude IDC sur les prédictions du marché mondial IaaS pour la période 2022-2026 prévoit un taux de croissance annuelle du marché IaaS de 35%. Les entreprises semblent y trouver un bon compromis entre la souplesse et la scalabilité du Cloud d'un côté, et la possibilité de contrôle granulaire sur les couches supérieures de l'autre. Nous notons également le développement croissant d'offres de service, de plus en plus structurées, autour de la gestion des environnements Cloud. Selon l'enquête IDC *Industry CloudPath* de 2022, près de la moitié (49.8%) des utilisateurs Cloud font appel à des sociétés de services externes pour gérer leurs environnements Cloud.

Une entreprise qui optera pour des services IaaS pourra ainsi toujours externaliser la gestion opérationnelle des couches « supérieures » et tirer pleinement profit des avantages du Cloud.

Les outils de messagerie et de collaboration arrivent en tête des applications SaaS. Les applications métier de type RH et ERP sont tout de même significativement utilisées en mode Cloud

Quels sont les principaux domaines d'utilisation des applications Cloud (SaaS) dans votre organisation ?



73 % des entreprises ont choisi les applications SaaS Cloud pour les outils de messagerie et de collaboration tels que le courrier électronique, les réunions virtuelles ou le partage de fichiers en ligne.

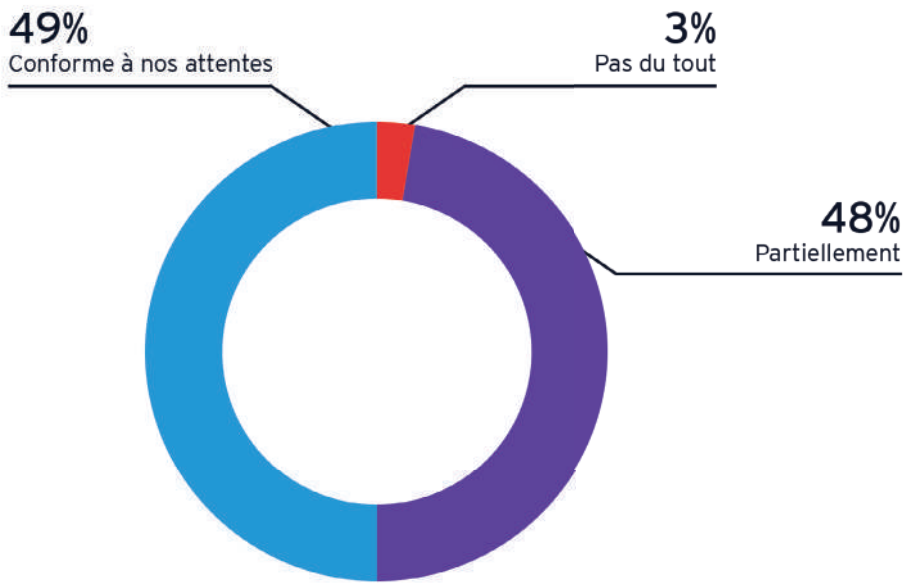
La gestion des ressources humaines est un autre domaine d'utilisation important pour 39 % des entreprises. Finalement, l'autre grand domaine d'utilisation est celui des applications ERP avec 27 % des répondants.

Ceci est en phase avec les pratiques en Afrique Francophone qui sont très concentrés sur les applications de type messagerie et applications de support informatique, mais à moindre échelle sur les applications métiers (ERP, RH) ou encore les technologies émergentes (Internet des objets ou IoT), démontrés par l'étude de EY en Afrique Francophone de 2021 « Cloud Computing: où en est l'Afrique francophone ? ».

5 RETOURS D'EXPÉRIENCE ET PERSPECTIVES

Globalement, **97%** des répondants qui utilisent les services Cloud considèrent que ces derniers ont répondu, au moins partiellement, à leurs attentes

Par rapport aux objectifs initiaux, considérez-vous que le Cloud a répondu à vos attentes ?

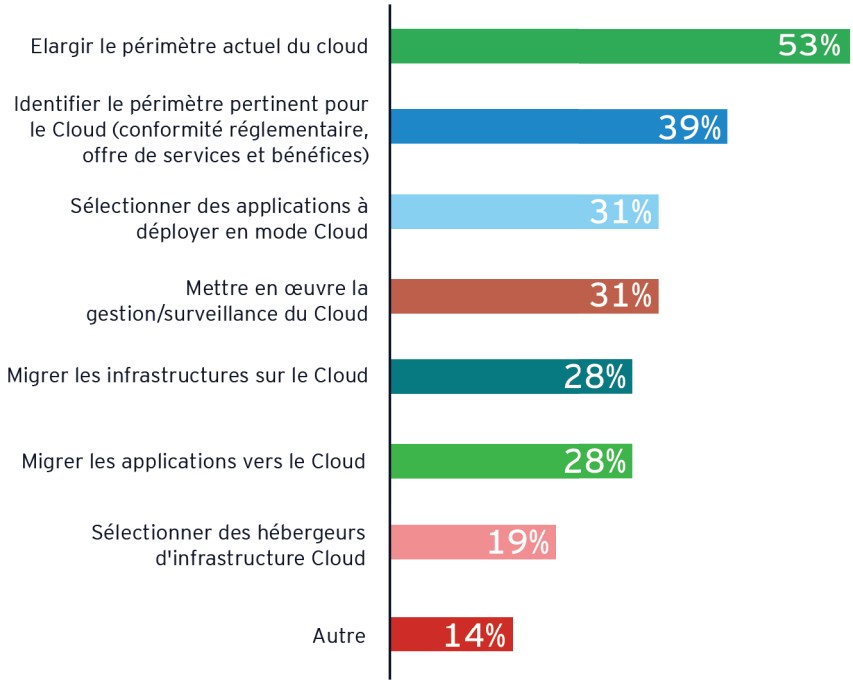


Si nous nous intéressons au secteur d'activité, nous voyons que les Banques et les Assurances, qui ont globalement la plus forte adoption du Cloud comme on l'a vu plus haut, sont plutôt partiellement satisfaites, alors que les entreprises des secteurs Grande Consommation, Distribution, Immobilier, Hôtellerie, Construction, Technologies et Télécommunications estiment une bonne conformité par rapport à leurs attentes.

Nous pouvons supposer que les Banques et les Assurances, qui disposent généralement d'équipes IT assez matures, ont des niveaux d'exigence et des besoins en flexibilité plus élevés.

Chez ceux qui l'ont adopté, le périmètre du Cloud tend plutôt à s'étendre mais les entreprises voudraient également prendre le temps de bien identifier le périmètre d'extension et de développer ou d'affiner leur stratégie Cloud

Quelles sont vos initiatives Cloud prévues en 2023 ?



Les freins au Cloud et la perception de ses apports ne semblent pas affecter l'engouement des entreprises qui l'ont déjà adopté. 53% d'entre elles prévoient d'étendre leur périmètre d'utilisation du Cloud en 2023. Les principaux chantiers qui viennent ensuite sont relatifs à l'identification du périmètre pertinent pour le Cloud et le développement d'une stratégie Cloud. **Le désir d'expansion semble vouloir s'accompagner d'une planification structurée et réfléchie.**

EXEMPLES DE CAS D'USAGE POUR L'ADOPTION DU CLOUD

L'entreprise : Un leader sur le marché local de l'agro-alimentaire. L'entreprise a été fondée en 2006 et compte environ 500 collaborateurs ; elle dessert un réseau de marchés internationaux couvrant l'Europe, le Maghreb, le Moyen-Orient et l'Afrique dans plus de 20 pays.

Pourquoi ?

Lors de son démarrage, l'entreprise manquait à la fois de budget pour l'investissement en infrastructure et de ressources techniques en informatique. Le Cloud s'est naturellement imposé comme un choix pertinent pour adresser ces deux contraintes. L'entreprise l'a ainsi adopté depuis une dizaine d'années.

Comment ?

Après un démarrage progressif, l'ensemble des environnements informatiques est aujourd'hui géré en mode Cloud, à l'exception de quelques services encore hébergés dans leurs propres locaux.

Et aujourd'hui ?

Le DSI est déchargé de toutes les problématiques liées à la gestion des infrastructures, il peut se concentrer sur des activités de stratégie et de planification, en étroite collaboration avec les autres directions métier.

L'entreprise : Une banque majeure sur le marché, fondée dans les années soixante. Forte d'un réseau d'une centaine d'agences, elle propose un catalogue de service assez riche aux clients particuliers et entreprises.

Pourquoi ?

La banque avait besoin de mettre en place un site de secours informatique afin d'assurer la continuité de ses services en cas de sinistre mais ne souhaitait pas investir dans un Data Center dédié, pour des raisons de coûts et de gestion opérationnelle

Comment ?

La banque dispose d'une équipe informatique expérimentée et compétente pour la gestion des environnements IT dans les propres Data Centers de la banque. La banque n'a souhaité externaliser, pour le moment, que la partie secours informatique. Elle a fait appel à un prestataire externe proposant une offre de type *Disaster Recovery as a Service (DRaaS)* où le secours informatique est géré de manière standardisée et industrialisée par le prestataire.

Et aujourd'hui ?

Des répétitions de bascule vers le site de secours sont organisées deux fois par an et la banque est tout à fait prête à affronter un sinistre, sans impact significatif sur ses clients ou ses opérations.

L'entreprise : Un leader sur le marché local du secteur mode et textile. Fondée dans les années quatre-vingt-dix, l'entreprise étend sa présence à l'international et est en train de diversifier ses activités.

Pourquoi ?

Suite à une expansion assez rapide de l'activité métier, le DSI a fait face à des limites d'espace dans son propre Data Center et devait décider rapidement de la solution pour ne pas entraver les activités métier. C'est ainsi que l'adoption du Cloud a été enclenchée.

Comment ?

Le DSI a entamé son adoption du Cloud en y faisant migrer une partie des services « non critiques » tout en continuant à gérer les applications critiques dans son propre Data Center.

Et aujourd'hui ?

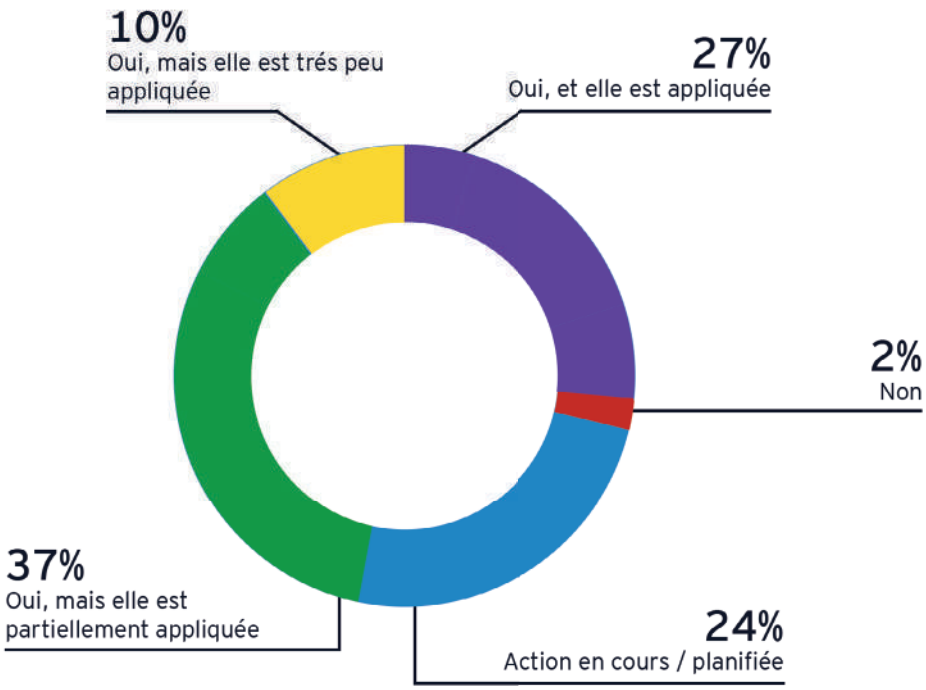
Le DSI ne souhaite pas renoncer à son Data Center local et ne trouve aucun mal à gérer un environnement hybride (une partie sur site, une partie dans le Cloud). Il a mis en place des processus pour la gestion des coûts du Cloud et assure la supervision des deux environnements. Il a gagné en agilité et arrive à répondre rapidement aux demandes des équipes métiers, notamment pour les nouveaux projets.

Baromètre Cybersécurité

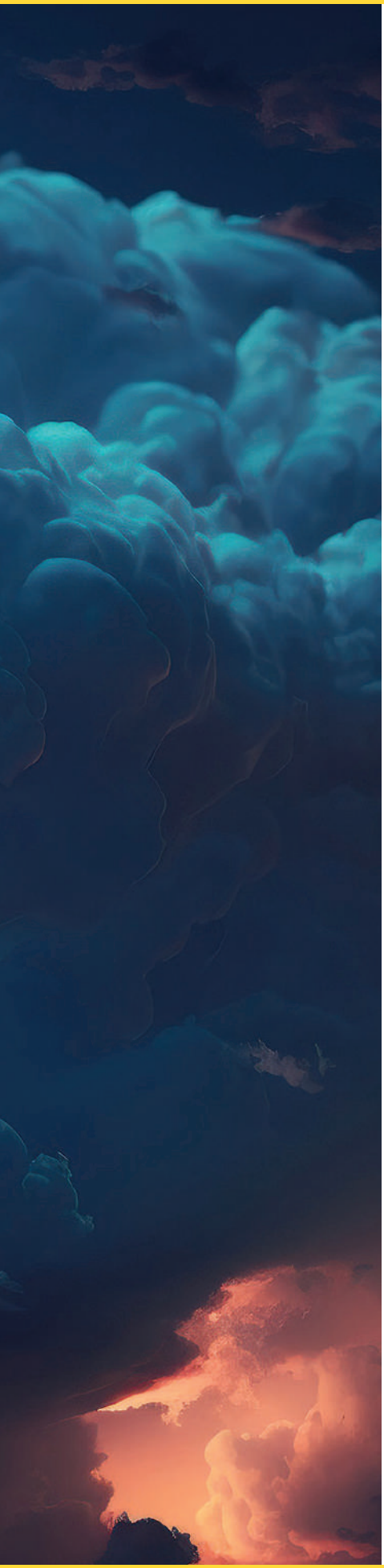
1 GOUVERNANCE DE LA CYBERSÉCURITÉ

La grande majorité des entreprises a déjà développé une politique de sécurité mais semble peiner à assurer son implémentation

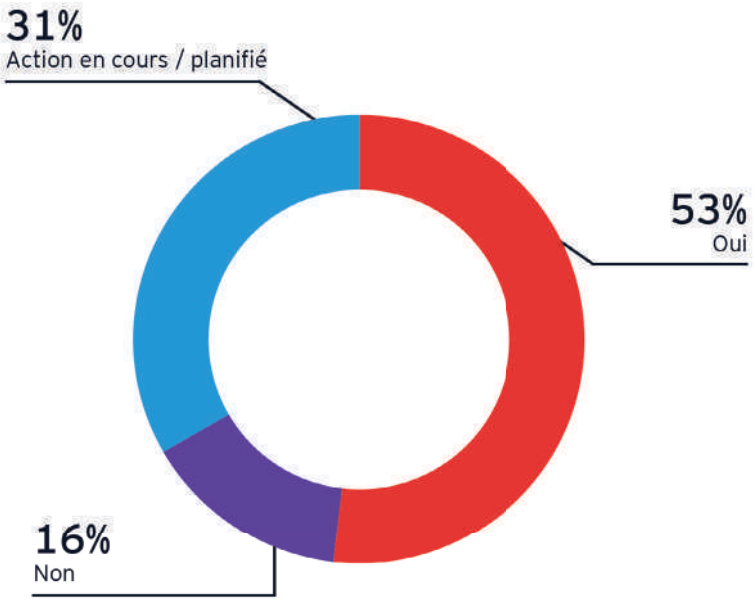
Votre organisation dispose-t-elle d'une politique de sécurité ?



74% des répondants déclarent avoir une politique de sécurité documentée leur permettant de gouverner la sécurité de leur système d'information. Cependant, la quasi-majorité des répondants (soit plus de 47%) ont déclaré que la politique de sécurité documentée est partiellement appliquée. Ceci indique que les entreprises doivent mener des actions pour s'assurer que leur politique de sécurité est pleinement mise en œuvre. Il va de soi que **la mise en œuvre efficace de la politique de sécurité est essentielle pour garantir la protection des systèmes d'information** de l'entreprise contre les cybermenaces. Il est donc crucial que les entreprises travaillent à améliorer la mise en œuvre de leur politique de sécurité pour renforcer leur posture de Cybersécurité.

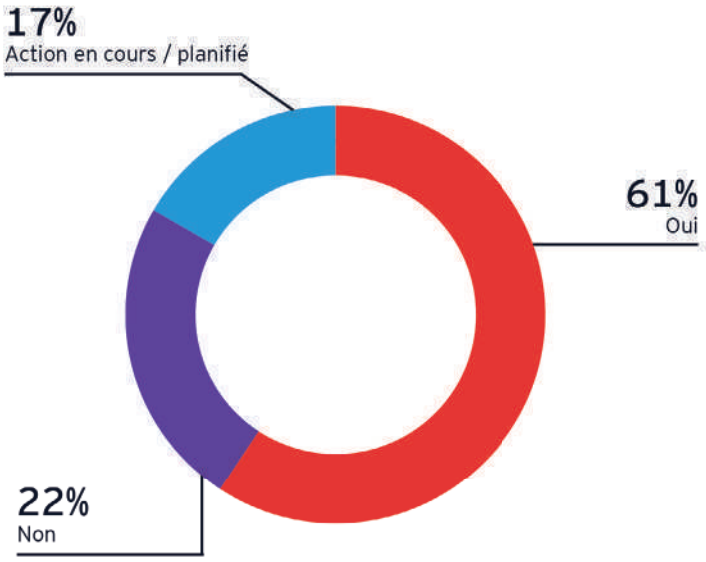


Votre organisation dispose-t-elle d'une stratégie de Cybersécurité ?



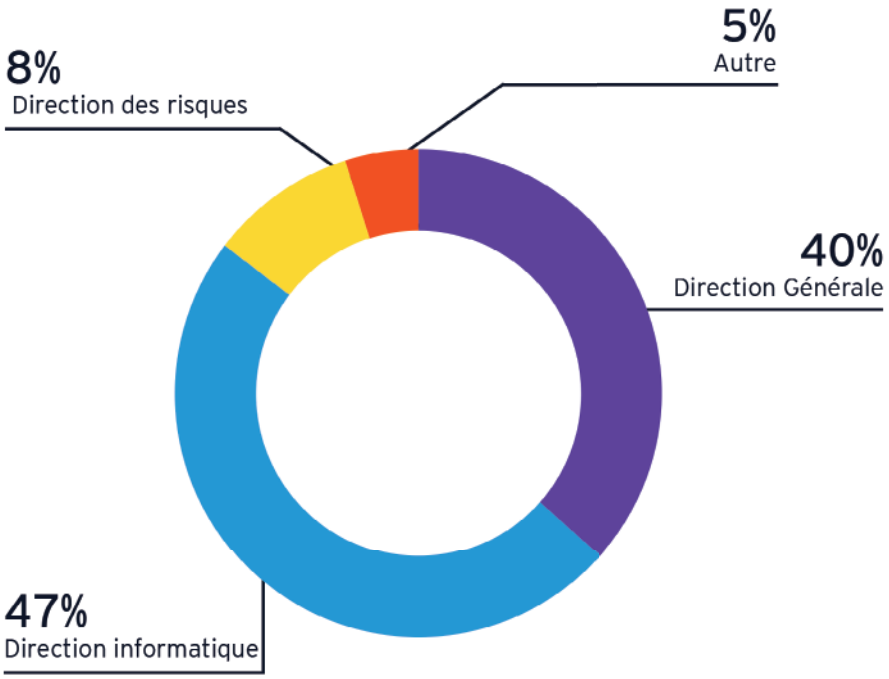
Une entreprise sur deux dispose d'une stratégie de Cybersécurité élaborée à moyen terme (1 à 3 années à venir) : Le manque de budget et de ressources dédiées à la Cybersécurité, ainsi que l'écart entre les responsabilités actuelles et les priorités des responsables de Cybersécurité sont autant de facteurs qui entravent la capacité des entreprises à élaborer et à mettre en œuvre des plans stratégiques de Cybersécurité à long terme.

Avez-vous une fonction dédiée à la Cybersécurité (RSSI, CISO, CSO, Directeur sécurité, etc.) ?



47% des responsables de Cybersécurité sont rattachés à la Direction Informatique ce qui peut indiquer que la Cybersécurité est encore souvent considérée comme un enjeu purement technologique

Quel est le rattachement du responsable de la Cybersécurité ?



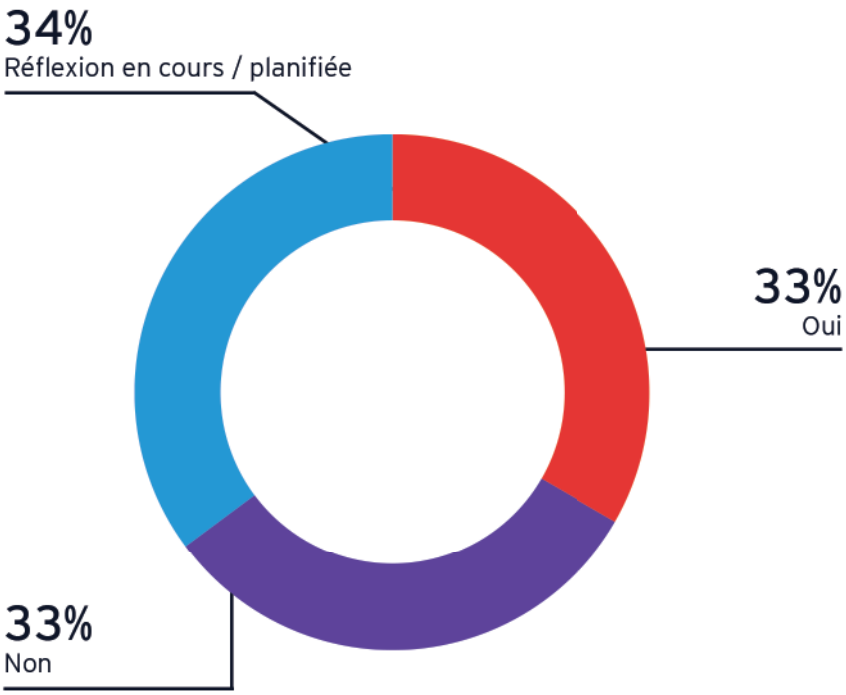
1/3 des entreprises en Tunisie n'ont pas encore de fonction dédiée à la Cybersécurité.

40% des répondants déclarent que le responsable de la Cybersécurité est rattaché à la Direction Générale et 47 % qu'il est rattaché à la Direction Informatique. Ces chiffres montrent une tendance à l'alignement de la Cybersécurité avec la stratégie globale de l'entreprise, avec un nombre croissant de responsables de la Cybersécurité rattachés à la Direction Générale. Cependant, il reste encore un pourcentage important de responsables de la Cybersécurité rattachés à la Direction des Systèmes d'Information, ce qui peut indiquer que la Cybersécurité est encore souvent considérée comme un enjeu purement technologique.

Ces résultats sont cohérents avec les résultats de l'étude EY Global Information Security Survey 2020 où 44% des responsables de Cybersécurité sont rattachés à une Direction des Systèmes d'Information ou une Direction de Transformation Digitale.

La mise en place d'un Security Operation Center ou SOC, qu'il soit interne ou externe, se généralise.

Utilisez-vous un SOC interne ou externalisé ?



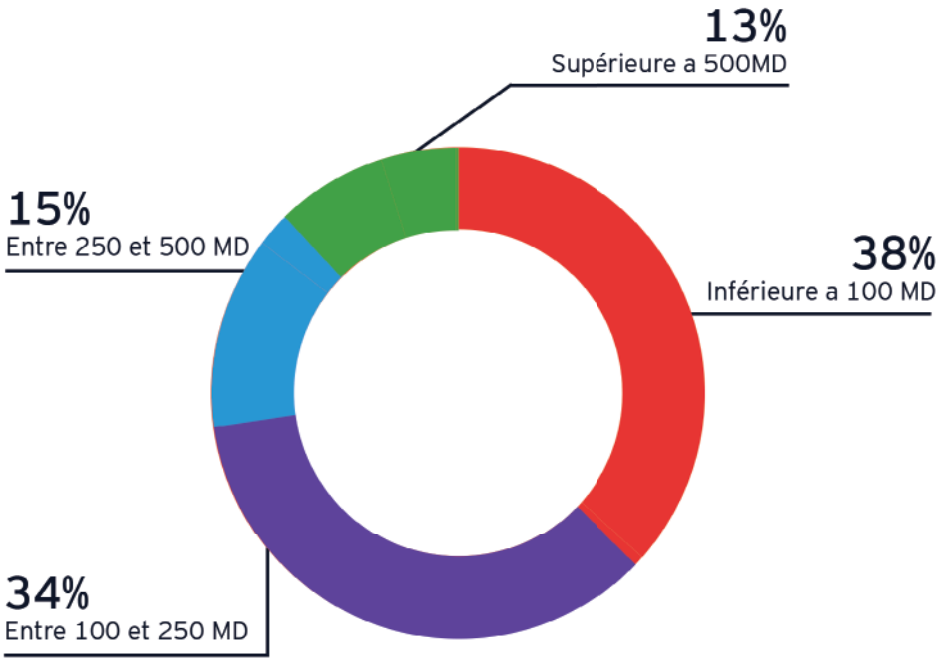
33% des entreprises ont déjà mis en place un centre opérationnel de sécurité (Security Operation Center ou SOC) interne pour gérer les incidents de Cybersécurité, tandis qu'un autre tiers a externalisé cette fonction en faisant appel à un fournisseur de services de sécurité gérée. Le reste des entreprises n'a pas encore mis en place de SOC ou est en train de réfléchir à sa mise en place. Cela montre **que les entreprises sont conscientes de l'importance d'avoir un SOC** pour assurer une surveillance continue et une **réponse rapide aux incidents de sécurité,** mais que certaines peuvent rencontrer des difficultés pour mettre en place un tel dispositif.

Il convient de souligner que les entreprises qui ne disposent pas encore d'un SOC ou qui envisagent de le mettre en place pourraient considérer d'utiliser les services d'un SOC externe. Elles profiteraient ainsi de l'expertise en cybersécurité des ressources et d'une gouvernance déjà en place, surtout si elles ne peuvent pas se permettre d'avoir un SOC interne dédié.

2 DÉPENSES

Des budgets limités dédiés à la Cybersécurité dans la majorité des secteurs d'activité

A combien s'élève votre dépense annuelle totale en Cybersécurité ?



38% des répondants déclarent disposer d'un budget inférieur à 100 milles dinars.

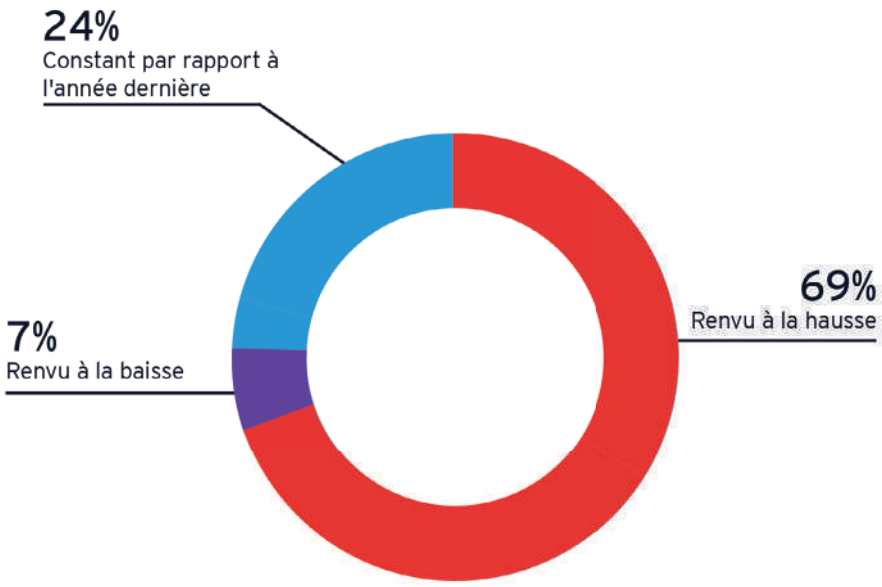
Les secteurs d'activité qui investissent le plus dans la Cybersécurité sont les Banques, les Assurances et les Télécommunications.

Rappelons qu'au niveau mondial et Selon l'enquête d'EY "Global Information Security Survey" publiée en 2020 les dépenses en Cybersécurité variaient en moyenne de 0,5% à 3,5% du chiffre d'affaires annuel, selon la taille de l'entreprise. Les grandes entreprises dépensaient en moyenne environ 1,5% de leur chiffre d'affaires en Cybersécurité, tandis que les petites entreprises dépensaient environ 3,5%.

Les entreprises interviewées semblent ne pas disposer d'un budget adéquat leur permettant de sécuriser l'entreprise de manière appropriée.

Des budgets Cybersécurité globalement revus à la hausse mais pas forcément de manière conséquente

Comment estimez-vous l'évolution de votre budget total à la Cybersécurité pour les 12 prochains mois ?



Seuls 69% des participants déclarent que leurs budgets dédiés à la Cybersécurité verront une courbe ascendante sur les 12 prochains mois. Cette tendance est alignée avec le tendances mondiales en matière de budgets consacrés à la Cybersécurité. Ceci concerne notamment toutes les banques interrogées.

Nous suspectons toutefois cette évolution de ne pas être suffisamment conséquente pour s'aligner aux tendances à l'International pour permettre aux entreprises interrogées d'améliorer leur posture de manière pleinement satisfaisante.

Les budgets Cybersécurité revus à la baisse restent exceptionnels et ne concernent pas un secteur en particulier.

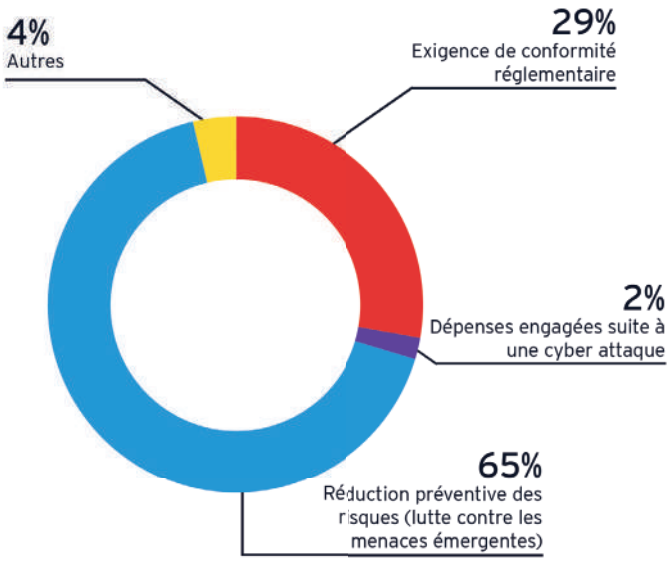
Selon une étude publiée par Gartner en septembre 2021 sur les dépenses mondiales en sécurité de l'information et de gestion des risques, ces dépenses devraient atteindre 150,4 milliards de dollars en 2021, soit une augmentation de 12,4 % par rapport à 2020.

Les dépenses mondiales en sécurité de l'information et en gestion des risques devraient continuer à augmenter au cours des prochaines années, pour atteindre 170,4 milliards de dollars en 2023.

Dans le cadre de notre Baromètre, les cas de budgets Cybersécurité revus à la baisse restent exceptionnels et pas nécessairement liés à un secteur d'activité en particulier.

La conformité réglementaire et la gestion des risques restent, pour 94% des entreprises, le principal facteur de nouvelles dépenses.

Quel est le principal facteur justifiant de nouvelles dépenses en Cybersécurité ?

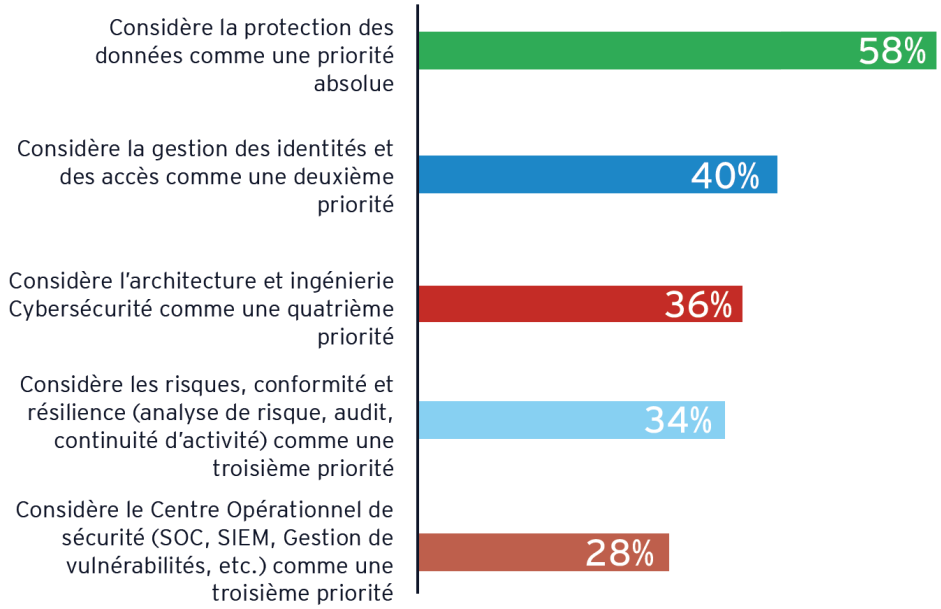


Ces dépenses sont ainsi motivées par des priorités préventives et défensives plutôt que par l'innovation ou la transformation. Ceci est en phase avec l'étude EY 2020 «Global Information Security Study» qui confirme que 77% des dépenses liées à la Cybersécurité ont un caractère défensif, axé sur la gestion des risques et la conformité plutôt que sur l'opportunité. En effet, aucune entreprise interrogée n'a déclaré budgétiser la Cybersécurité dans le cadre de nouvelles initiatives ou de programmes de digitalisation par exemple. Cela peut s'expliquer par le fait que les entreprises considèrent souvent la Cybersécurité comme une dépense incontournable pour protéger leurs activités existantes plutôt que comme un investissement dans de nouveaux projets innovants. Ceci ne devrait pas les empêcher d'intégrer la sécurité en amont dans tout projet de transformation afin de maximiser leurs chances de réussite.

3 PRIORITÉS

Des priorités d'investissement en Cybersécurité alignées avec les préoccupations, mais probablement en manque de budget

Quelles sont les priorités de votre organisation en matière de Cybersécurité ?

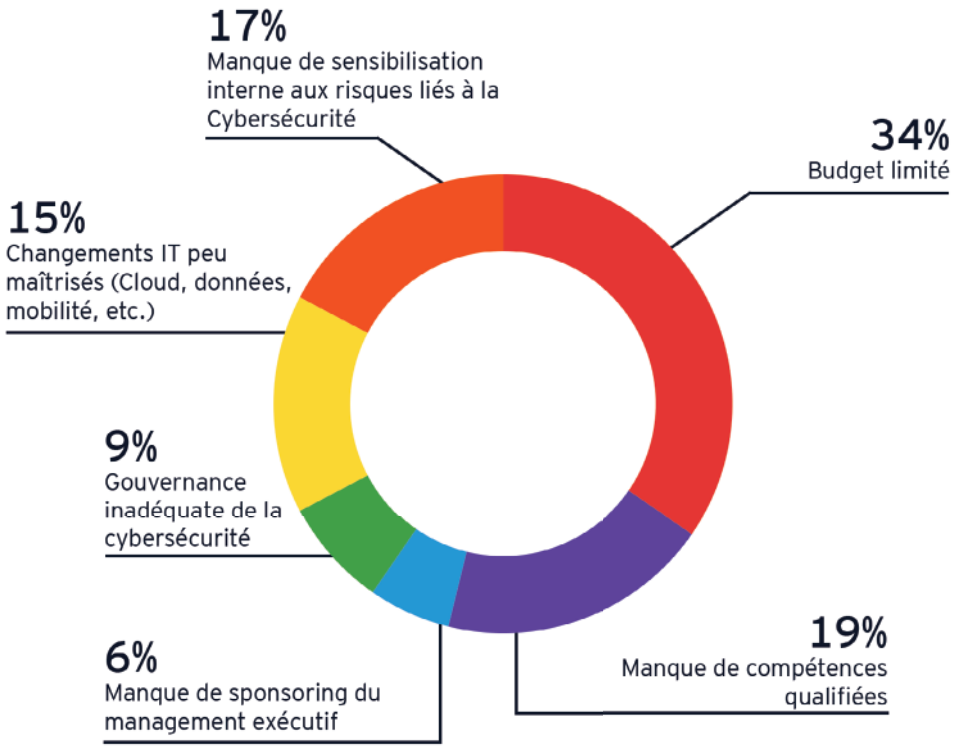


58% des répondants déclarant la protection des données comme la priorité numéro 1 en matière d'investissements en Cybersécurité, il existe clairement un écart entre les priorités déclarées par les responsables/ directeurs de sécurité et les budgets alloués par la Direction Générale.

Nous avons vu plus haut que les budgets étaient essentiellement motivés par la conformité réglementaire et la gestion des risques. Nous notons ici que les priorités d'investissements sont ainsi principalement orientées vers la protection des données, la gestion des identités et des accès et le monitoring de la sécurité.

Le manque de budget et de compétences est le principal obstacle à une gestion efficace et satisfaisante de la Cybersécurité

Quel est le facteur principal qui empêche votre organisation d'atteindre ses objectifs en matière de Cybersécurité ?



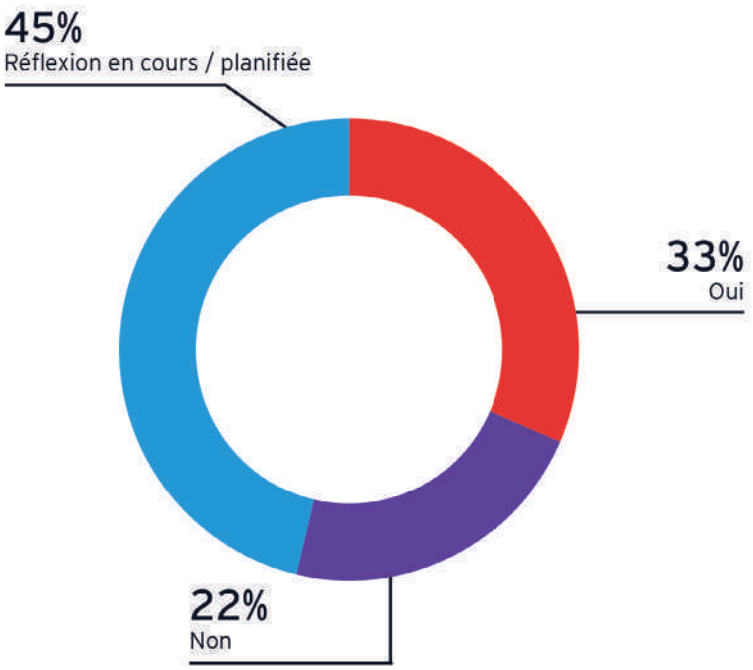
Tel qu'attendu, les limitations de budget constituent le principal frein à l'atteinte des objectifs en matière de Cybersécurité. Le manque de compétences qualifiés est également sélectionné par 19% des répondants.

Pour pallier ces limites, **les entreprises envisagent de plus en plus les service managés en Cybersécurité.** Si utilisés de manière appropriée, ces derniers peuvent en effet renforcer la maturité en Cybersécurité, à un coût compétitif et en amenant les technologies et surtout les compétences qui peuvent manquer à l'entreprise.

En troisième position, les répondants ont sélectionné le manque de sensibilisation interne aux risques liés à la Cybersécurité. Ceci peut être adressé en mettant en place un programme de sensibilisation adapté, délivré de manière obligatoire et régulière à l'ensemble des collaborateurs et dont les résultats seraient mesurés dans le temps.

L'externalisation de processus de Cybersécurité est envisageable par la majorité des répondants ; seuls 22% y sont réticents

Utilisez-vous ou comptez-vous utiliser des services managés en Cybersécurité ?



33% des entreprises externalisent la gestion d'un processus de Cybersécurité chez un prestataire de services.

De plus, 45 % des répondants déclarent qu'une action/réflexion est en cours pour externaliser une partie des processus de Cybersécurité.

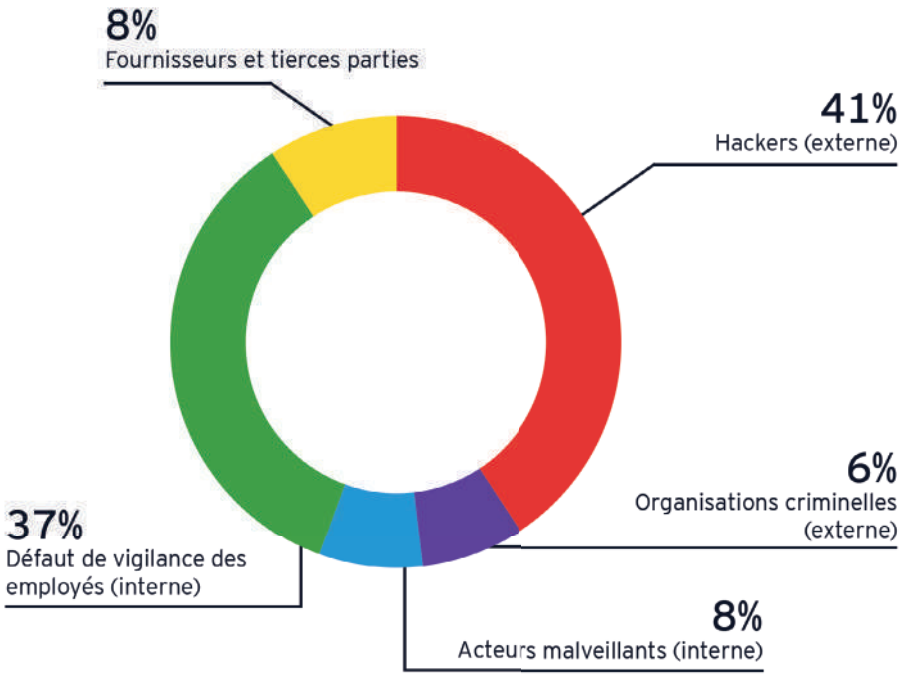
Notons que l'ouverture ou non aux services managés en Cybersécurité ne concerne pas un secteur d'activité ou une taille d'entreprise en particulier.

Au niveau mondial et selon une étude de Gartner de 2021, les dépenses mondiales en services de sécurité managés devraient augmenter de 11% en 2021 pour atteindre 67 milliards de dollars, ce qui montre une forte tendance à l'adoption de ces services.

4 CYBERATTAQUES ET PRINCIPALES FAIBLESSES

Sans surprise, les hackers externes sont la première source de menace pour les entreprises. La sensibilisation interne à la Cybersécurité reste essentielle même si les entreprises semblent avoir du mal à l'assurer

Principale source de menace en termes de fuite, intrusion ou altération des données



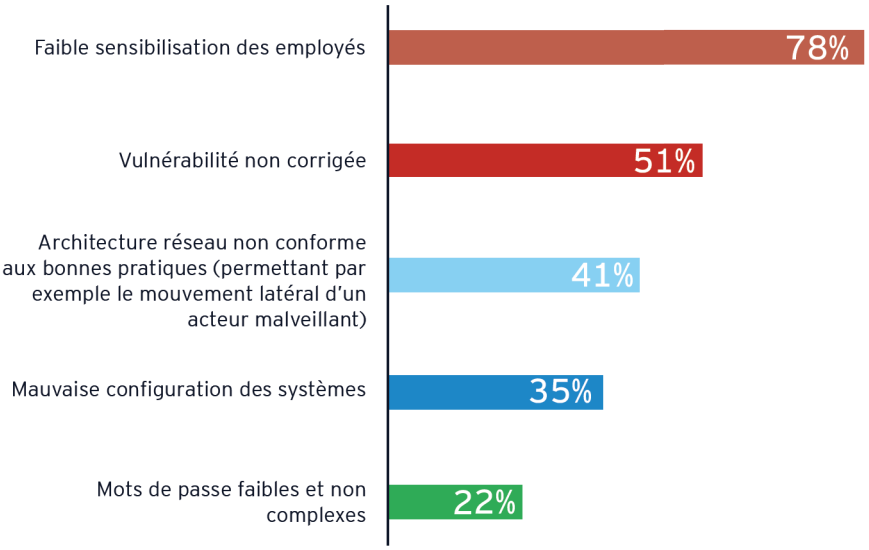
Les répondants désignent les hackers externes comme première source de menace avec 41% de réponses. Le défaut de vigilance des employés est la deuxième préoccupation des décideurs de sécurité, dont 37% déclarent que la survenance d'une intrusion ou d'une fuite pourrait provenir d'un employé de l'entreprise peu ou pas sensibilisé à la Cybersécurité.

Ceci rappelle l'importance cruciale de la sensibilisation interne des collaborateurs sur les thématiques liées à la Cybersécurité, ce qui permet de prévenir une bonne partie des menaces Cybersécurité, sans pour autant nécessiter d'investissements lourds.

Seuls 8% des répondants désignent les fournisseurs et tierces parties comme principale source de menace. Ces entreprises sont toutes consommatrices de services Cloud. Nous comprenons que l'adoption du Cloud peut être accompagnée par une extension de la surface d'attaque

aux fournisseurs du service Cloud. Il est certes crucial d'adapter les contrôles et les pratiques de sécurité aux environnements Cloud et de suivre les bonnes pratiques de sécurité associées. Une entreprise ne peut pas aller vers le Cloud sans remettre en question la manière dont elle gère la Cybersécurité.

Principales faiblesses pouvant mener à une cyberattaque



D'après les résultats de l'enquête, les principales vulnérabilités menant à une cyberattaque sont liées aux aspects humains et techniques. Les employés jouent un rôle crucial dans la prévention des cyberattaques, mais leur faible sensibilisation constitue la principale faiblesse, étant donné que 78% des réponses pointent ce facteur. Les vulnérabilités non corrigées (51%) sont également préoccupantes, suivies d'une architecture réseau ne répondant pas aux bonnes pratiques (41%) et d'une mauvaise configuration des systèmes (35%). Enfin, les mots de passe faibles et peu complexes représentent également une source de préoccupation importante, avec 22% des réponses. Pour renforcer la cybersécurité de l'entreprise, il est donc crucial de **sensibiliser les employés aux pratiques de sécurité, de maintenir les systèmes à jour, de suivre les meilleures pratiques en matière de conception de réseau, de configurer correctement les systèmes et d'utiliser des politiques de mot de passe robustes.**

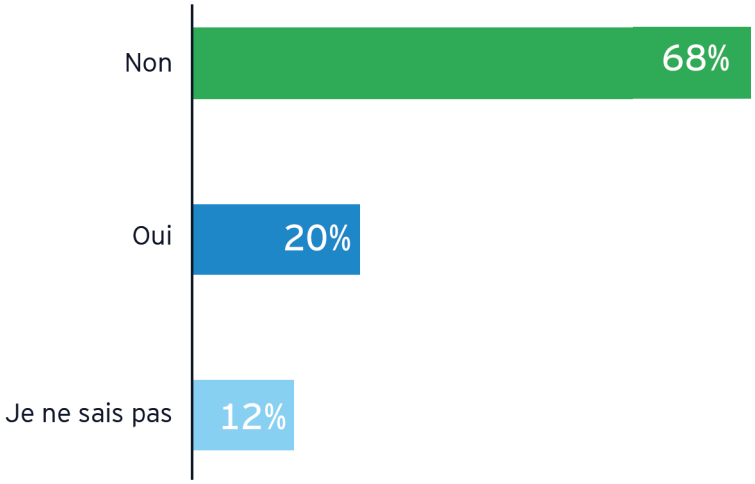
D'autres enquêtes menées ces dernières années ont également révélé des résultats similaires en ce qui concerne les principales faiblesses qui peuvent conduire à des cyberattaques.

Par exemple, une enquête de 2021 menée par le fournisseur de solutions de sécurité Check Point a révélé que les principales causes d'incident de sécurité informatique étaient la négligence des utilisateurs, les vulnérabilités logicielles et les attaques de phishing. L'enquête a également révélé que les cyberattaquants étaient de plus en plus ciblés et sophistiqués dans leurs méthodes d'attaque.

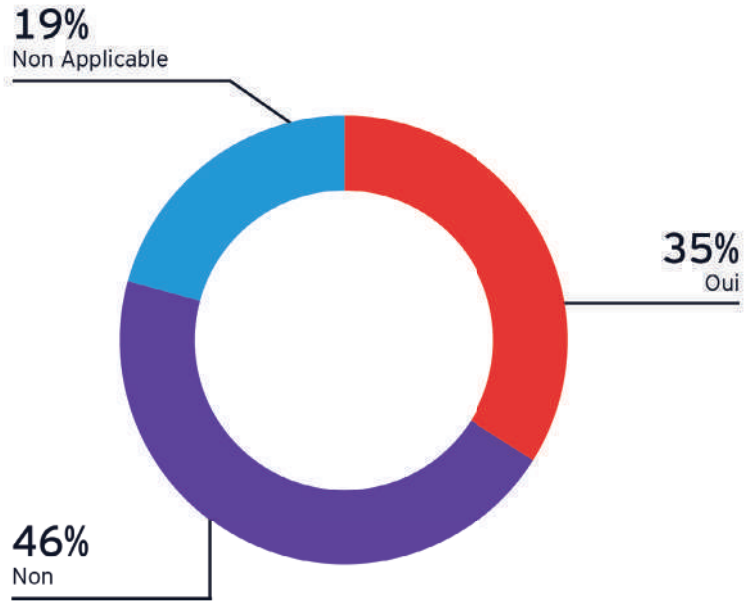
5 CAPACITÉS DE DÉTECTION ET DE RÉPONSE

Un nombre de cyberattaques qui continue d'augmenter mais des capacités qui semblent globalement limitées pour la détection des menaces

Pensez-vous avoir subi une attaque lors des 12 derniers mois ?



Avez-vous constaté une augmentation du nombre d'attaques ?



35% des entreprises interrogées déclarent que le nombre d'attaques visant ses systèmes et ses infrastructures ont augmenté durant l'année 2022.

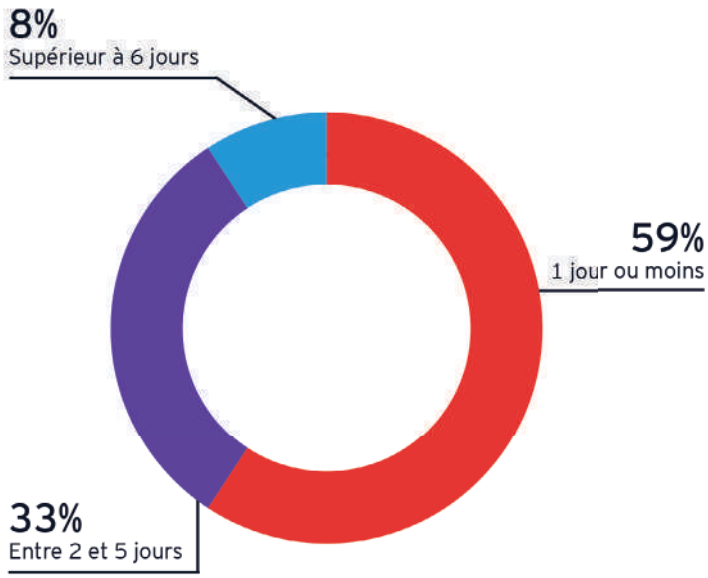
20% des répondants déclarent avoir subi une cyber-attaque durant les 12 derniers mois, et 12% des entreprises n'ont pas les éléments pour statuer ou non sur l'occurrence d'une cyberattaque réussie qui l'aurait visée.

Selon les résultats mondiaux de l'enquête EY Global Information Security Survey de 2020, une entreprise sur deux a déclaré avoir subi une attaque d'impact important durant l'année 2019.

Le manque d'outils de détection et le manque de ressources permettant de monitorer la sécurité des systèmes d'information de l'entreprise sont autant d'éléments qui nous poussent à croire que le pourcentage d'entreprises tunisiennes ayant subi une cyberattaque pourrait être bien plus important. En effet, selon le Rapport de Sécurité Cloud 2022 réalisé par Cybersecurity Insiders, 93% des personnes interrogées sont modérément à extrêmement préoccupées par la pénurie massive de professionnels de la Cybersécurité qualifiés.

Les entreprises ayant mis en place un SOC démontrent une rapidité accrue pour détecter les menaces Cybersécurité

Combien de temps en moyenne mettez-vous pour détecter les incidents de sécurité ?



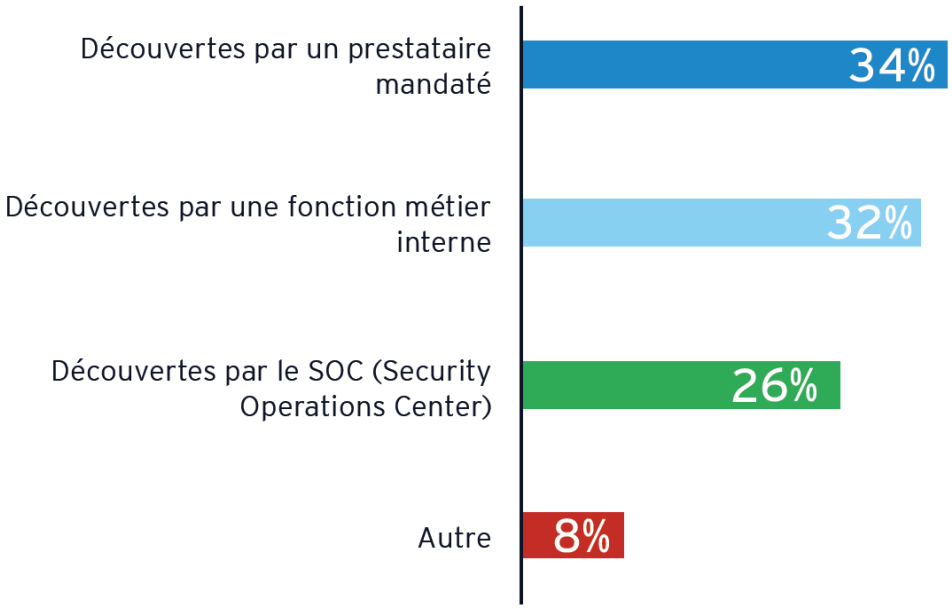
La majorité des entreprises ont une bonne capacité à détecter rapidement les incidents de sécurité, avec 59% des répondants déclarant pouvoir détecter les incidents en 1 jour ou moins. Cela est grandement facilité par la présence d'un SOC ainsi que par des procédures bien établies pour signaler les incidents de sécurité.

Cependant, il est crucial de souligner que la proportion de répondants ayant signalé une durée supérieure à un jour pour détecter les incidents de sécurité est d'environ 41%. Cela met en évidence la nécessité pour ces organisations de renforcer leurs capacités de détection et de réponse pour réduire les dommages potentiels résultant d'attaques.

La réduction du temps de détection est en effet un enjeu clé de la Cybersécurité, car **cela permet de limiter les dommages causés par l'attaque et de prendre des mesures rapidement pour éviter sa propagation.**

Des capacités de détection transverses, combinant le SOC interne, les prestataires externes et les fonctions métier internes

Comment avez-vous découvert les principales failles ?



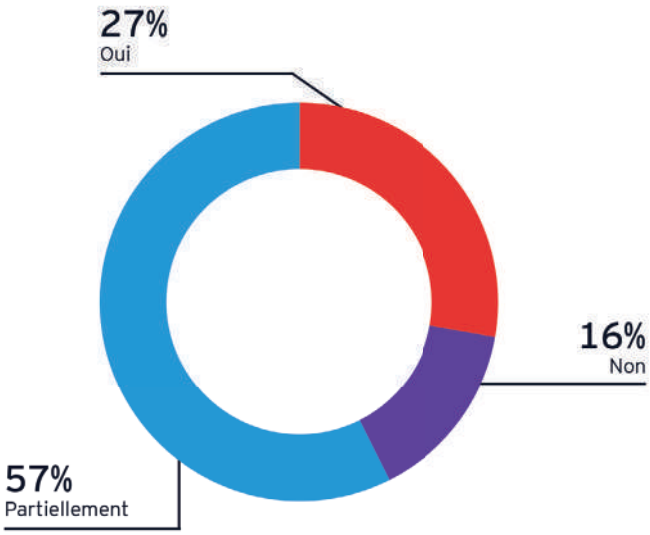
Selon les résultats de l'enquête, environ 26% des répondants ont rapporté que les failles de sécurité ont été découvertes grâce à leur SOC interne, soulignant ainsi leur efficacité dans la détection des vulnérabilités. Toutefois, plus de 34% des répondants ont signalé que les failles ont été découvertes grâce à un prestataire externe mandaté, soulignant ainsi l'importance de travailler avec des partenaires de confiance en matière de Cybersécurité pour renforcer la détection des failles. De plus, près d'un tiers des répondants ont déclaré que les failles ont été détectées grâce à une fonction métier interne, ce qui suggère que les employés de l'entreprise peuvent jouer un rôle clé dans la détection des failles de sécurité.

Ces résultats soulignent l'importance de mettre en place une approche globale de détection de failles de sécurité, en utilisant à la fois les ressources internes et externes disponibles.

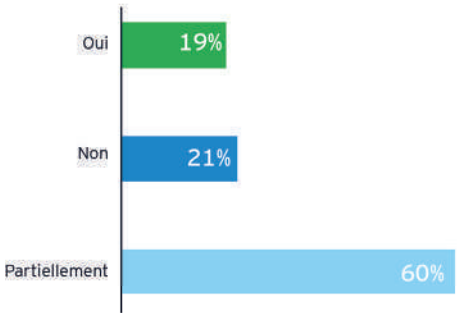
6 Satisfaction des moyens de Cyberprotection

Une grande majorité des répondants partiellement ou non satisfaits des moyens technologiques mis en place par leur organisation pour faire face aux menaces de Cybersécurité

Etes-vous satisfait des moyens de protection mis en place dans votre organisation pour garantir la sécurité de vos actifs critiques ?pour garantir la sécurité de vos actifs critiques ?



Etes-vous satisfait des capacités actuelles en termes de détection et de réponse aux incidents de sécurité ?



73% des répondants déclarent être partiellement ou non satisfaits des moyens technologiques à leur disposition pour garantir la sécurité des actifs de l'entreprise.

Cette non-satisfaction provient naturellement des budgets limités alloués (une entreprise sur trois avec un budget inférieur à 100 milles dinars).

De plus, la plupart des responsables de sécurité ont des prérogatives limitées à la gouvernance de la Cybersécurité, là où la sécurité opérationnelle reste majoritairement gérée par les directions des systèmes d'information dans l'entreprise.

Les entreprises dépensant moins de 250 mille dinars sont majoritairement peu satisfaites des moyens de protection de leurs organisations. De manière intéressante, bien que attendues, **toutes les entreprises dépensant plus de 250 mille dinars déclarent être satisfaites des moyen de protection.**

Conclusion

Le marché tunisien connait certes un nouveau rythme ascendant en matière d'adoption du Cloud ; l'agilité promise, supposée fournir un avantage compétitif et accélérer les programmes de transformation digitale, est également en train de convaincre de plus en plus les décideurs tunisiens.

Lorsqu'elles ont adopté le Cloud, les entreprises sont tout de même parfois freinées par une perception de coûts plutôt élevés et par une connaissance limitée de la règlementation. Là où les contraintes de sécurité et la dépendance au fournisseur de service Cloud constituent également des freins à une adoption plus large du Cloud, il est important de souligner que le Cloud est en mesure de supporter une meilleure gestion des risques. En effet, les fournisseurs Cloud proposent en général des services standardisés, alignés avec les normes et bonnes pratiques du marché et intégrant de nombreuses fonctions de sécurité facilement accessibles.

En nous intéressant justement à la gestion de la Cybersécurité par les entreprises sollicitées, ce Baromètre a mis en lumière plusieurs défis, entre autres : un manque de sensibilisation interne aux enjeux liés à la sécurité, des budgets Cybersécurité globalement insuffisants, et le manque de ressources qualifiées.

Ce manque d'expertise a notamment été pointé comme un autre frein pour l'adoption du Cloud. Cette préoccupation n'étant pas exclusivement locale mais assez générale au niveau mondial, elle a favorisé le développement d'offres de services autour de la gestion de la Cybersécurité et du Cloud ainsi que le conseil et l'accompagnement en vue d'outiller les entreprises pour mieux affronter ces deux sujets.

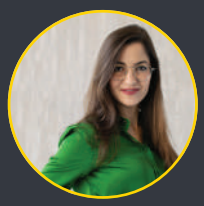
Contacts

SAMI ZAOUI

Associé, EY Technology Consulting Leader & FSSA Technology Leader

WISSEM GHAZAOUI

Associé, EY Technology Transformation



MYRIAM KHELIFI

Associée, EY Technology Risk

SENDA BOUKEF

Directrice, EY Technology Transformation

WASSIM KAMMOUN

Manager et SOC Leader, EY Cyber Security

Remerciements

Nous remercions tous les répondants pour le temps et le soin consacrés à l'enquête et pour l'éclairage apporté sur leurs pratiques et perspectives.

Nous remercions également l'ensemble de l'équipe EY qui a contribué à l'élaboration de ce Baromètre, en particulier :

- Mahdi Amri – Associé, Data & Analytics
- Myriam Bahri - Market & Business Development Director - Certifiée PNL et PCM
- Anis Sahnoun – Consultant en Transformation Technologique, certifié Amazon Web Services et Microsoft Azure
- Aya Benna – Business Analyst et consultante
- Ines Ben Sik Salem – Consultante Senior en Transformation Technologique, certifiée Prince2 et PSPO
- Souha Ben Amara – Chef de projet Marketing, certifiée PSPO
- Abderrazak El Euch – Content Manager
- Rim Abdelmoula – Chef de projet et Manager en Transformation Technologique
- Mohamed Achraf Maazoun – Manager en Transformation Technologique, certifié TOGAF, Redhat RHCSA, OpenStack et VMWare VCP
- Oussama Chibani – Consultant Senior en Transformation Technologique, certifié Microsoft Azure, ITIL et Dell Boomi

Méthodologie

Les réponses des entreprises qui ont répondu au questionnaire ont été analysées comme suit :

1. Revue de la cohérence globale des réponses pour chaque répondant

2. Elimination des doublons ; une seule réponse a été retenue pour chaque entreprise en favorisant le répondant le plus pertinent pour le contexte du Baromètre, un Directeur des Systèmes d'Information (DSI) ou un Responsable de la Sécurité des Systèmes d'Information (RSSI). Les 49 réponses analysées sont les réponses valides et uniques pour chaque entreprise interrogée.

3. Elimination des questions qui n'ont pas semblé avoir été bien comprises par une partie conséquente des répondants afin de ne pas fausser les résultats

4. Analyse des résultats pour chaque question

5. Formulation d'hypothèses sur les corrélations possibles entre différentes questions (Cloud, Cybersécurité et à travers les deux volets)

6. Validation des hypothèses de corrélations; seules les corrélations qui ont pu être solidement validées ont été retenues comme pertinentes

7. Analyse des données à la lumière des résultats de chaque question et des corrélations observées.

8. Comparaison des résultats avec ceux d'études précédentes, notamment dans d'autres géographies (Afrique, Europe, monde)

EY | Building a better working world

EY est un des leaders mondiaux de l'audit, du conseil, de la fiscalité et du droit, des transactions. Partout dans le monde, notre expertise et la qualité de nos services contribuent à créer les conditions de la confiance dans l'économie et les marchés financiers.

Nous faisons grandir les talents afin qu'ensemble, ils accompagnent les organisations vers une croissance pérenne.

C'est ainsi que nous jouons un rôle actif dans la construction d'un monde plus juste et plus équilibré pour nos équipes, nos clients et la société dans son ensemble.

EY désigne l'organisation mondiale et peut faire référence à l'un ou plusieurs des membres d'Ernst & Young Global Limited, dont chacun est une entité juridique distincte.

Ernst & Young Global Limited, société britannique à responsabilité limitée par garantie, ne fournit pas de prestations aux clients. Retrouvez plus d'informations sur notre organisation sur www.ey.com.

EY | Assurance | Tax | Transactions | Consulting

AMC Ernst & Young est une société à responsabilité limitée de droit tunisien