CYBERFORCES
Protect your business

WAVESTONE

Enjeux & perspectives d'une résilience numérique au Maroc

Retours du **Cybersecurity day**
du 21 novembre 2023

Février 2024

Sommaire

Executive Summary

Executive Summary

Les entreprises marocaines sont aujourd'hui confrontées à des défis croissants en matière de cybersécurité en raison de systèmes d'information de plus en plus complexes et exposés et d'une augmentation conséquente de la quantité de données au sein des SI. Elles sont de ce fait , devenues la cible privilégiée d'une cybercriminalité croissante.

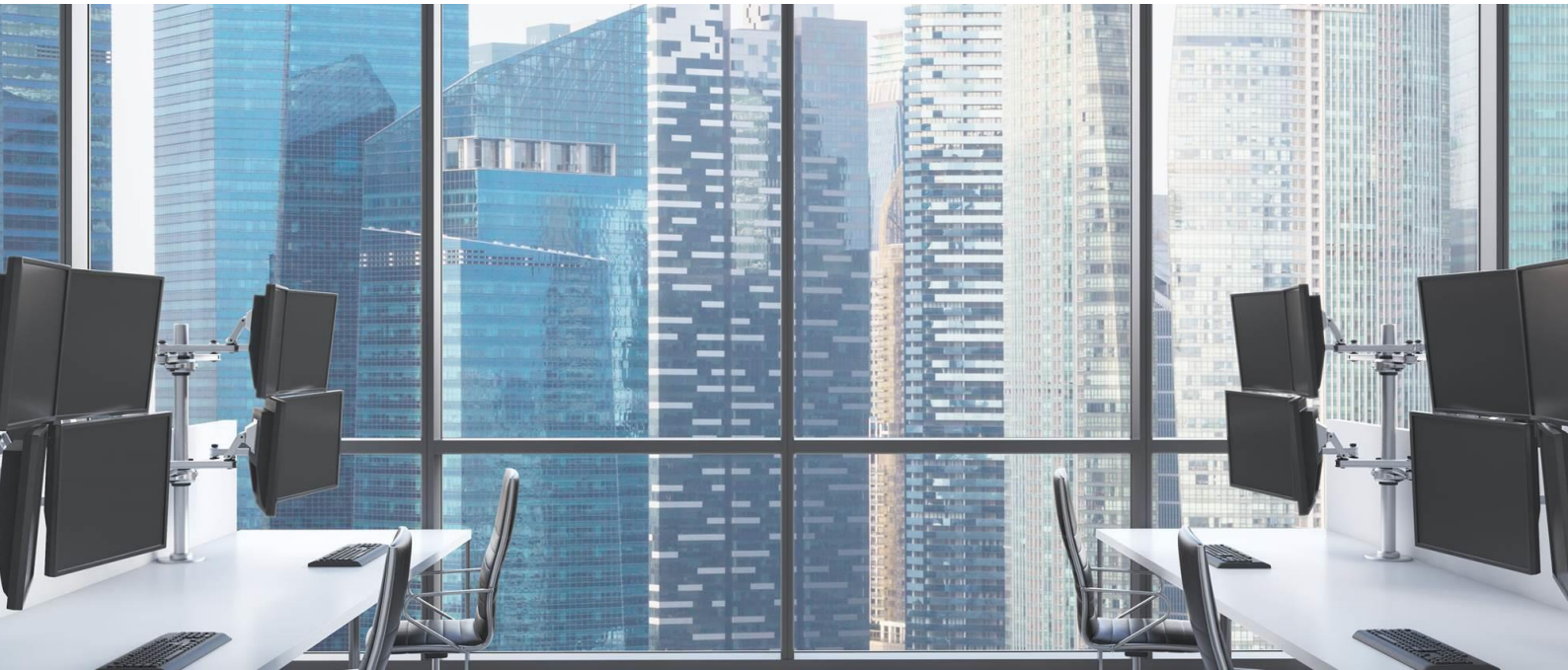
En réponse à cette menace, la législation a évolué avec la mise en place de la stratégie nationale de cybersécurité et l'instauration de lois et de réglementations par la DGSSI (Direction Générale de la Sécurité des Systèmes d'Information) en tant que législateur et régulateur national en matière de Cybersécurité telles que la loi 05-20. Cette évolution réglementaire s'est accompagnée par la définition d'une Directive Nationale de Sécurité des Systèmes d'Information (DNSSI) imposée à toutes les entités disposant d'Infrastructures d'Importance Vitale pour le pays.

Dans ce contexte, le Maroc a vu son classement au "Global Cybersecurity Index" s'élever à la 32e place, témoignant des efforts déployés.

Cependant, le pays demeure confronté à des enjeux de maturité en matière de cybersécurité. Pour discuter de ces enjeux, Cyberforces et Wavestone ont organisé le Cybersecurity Day le 21 novembre 2023, un événement marqué par la présence d'experts nationaux et internationaux pour discuter de ces enjeux et présenter leurs recommandations.

Les derniers résultats du Cyber Benchmark Wavestone montrent que le niveau de maturité des organisations au niveau international a progressé (49%, +3 points depuis 2022). Cependant des disparités sectorielles persistent. Le secteur financier affiche un score élevé de 59,2%, tandis que d'autres secteurs, tels que le secteur des services (44%) et le secteur public (36,1%), présentent des scores plus modestes, en raison de difficultés à identifier les financements nécessaires.

Malgré une augmentation des effectifs dédiés à la cybersécurité qui témoigne des efforts menés, de nombreux challenges subsistent. Les organisations cherchent à renforcer leurs équipes à travers diverses stratégies, notamment des programmes de gestion des talents, voire d'externalisation.



Le Cloud fait également l'objet d'un traitement particulier dans cette dynamique d'évolution. En effet, des cibles Cloud existent dans plusieurs organisations marocaines. Toutefois, la réglementation marocaine stipule que les données personnelles doivent être stockées sur des serveurs locaux pour garantir la sécurité et la confidentialité des données. La notion de Cloud souverain prend ainsi toute son importance et permet de garantir la souveraineté numérique du pays et de protéger les données sensibles contre les cyberattaques et les violations de la vie privée, les offres de Cloud souverain restent cependant à date assez limitées et plus onéreuses.

En réponse à ces défis, les experts recommandent plusieurs stratégies de protection, notamment l'accent mis sur la sensibilisation à la cybersécurité, l'application rigoureuse de bonnes pratiques d'hygiène informatique, et l'adoption d'une stratégie Zero Trust.

En parallèle, le paysage Cyber continue d'évoluer, avec des tendances à surveiller telles que l'adoption croissante du modèle Zero Trust, la nécessité de sécuriser les données traitées, la sécurité des IoTs, l'exploitation de l'IA par les cybercriminels, et la nécessité d'une gestion efficace des talents en cybersécurité.

Pour répondre aux nouveaux attendus liés à leurs fonctions émanant des enjeux et tendances explicités plus haut, les CISOs voient leur rôle évoluer vers une posture plus large de Chief Security Officer (CSO), englobant des responsabilités étendues, comme la sécurité physique, la résilience, et la sécurité industrielle. Ces transformations reflètent une prise de conscience croissante de l'importance stratégique de la cybersécurité au sein des organisations.

En conclusion, la cybersécurité à l'international et plus particulièrement au Maroc est confrontée à des défis complexes nécessitant des stratégies holistiques, des investissements continus et une collaboration étroite entre les entreprises, les gouvernements et les experts en cybersécurité.

Contexte général

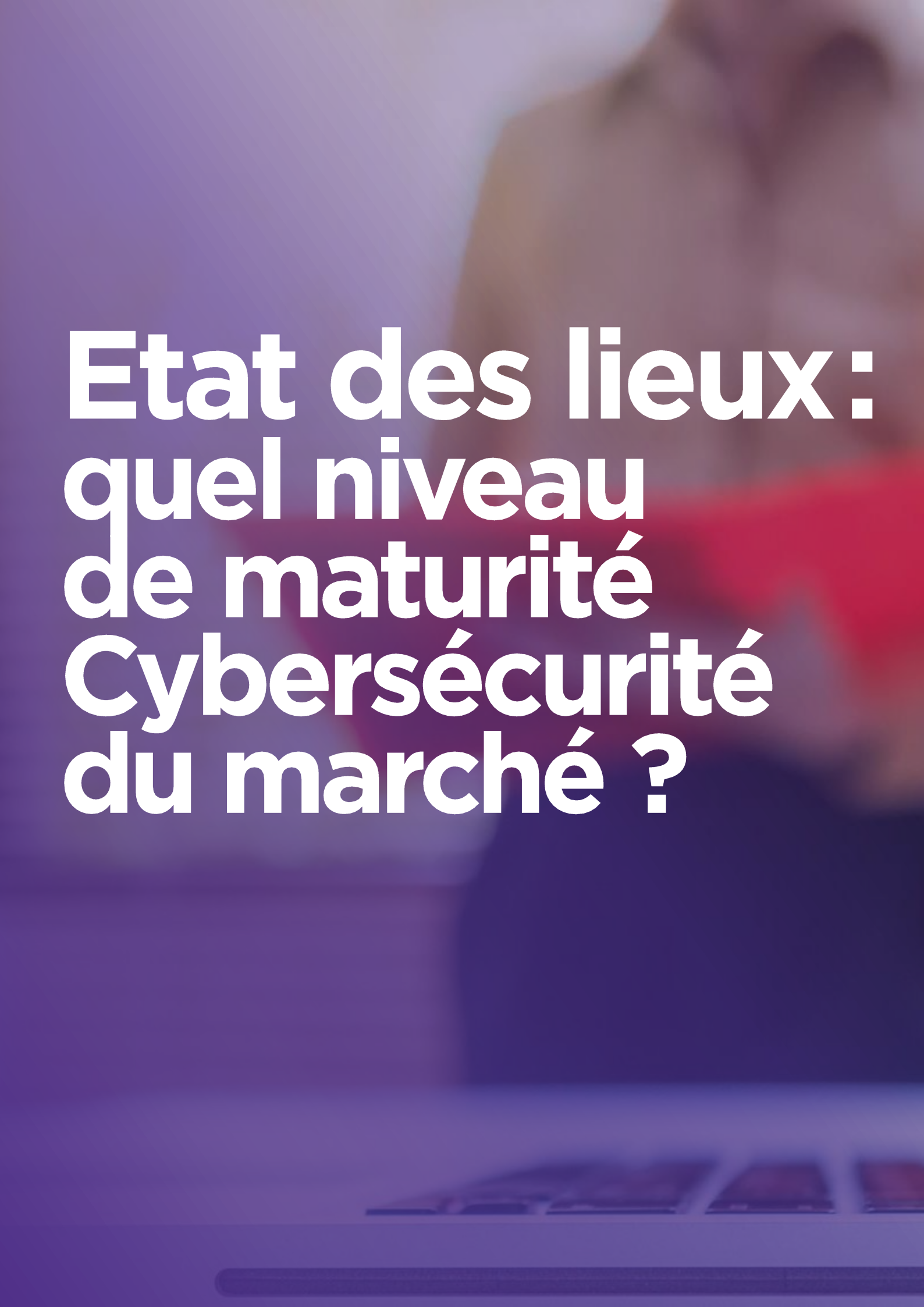
Contexte général

L'ensemble des entreprises marocaines fait face depuis quelques années à des enjeux de cybersécurité de plus en plus importants. Cela est dû à des systèmes d'information de plus en plus complexes et exposés, ainsi qu'à une explosion des données informationnelles de l'entreprise concomitamment à une cybercriminalité croissante sur le territoire marocain, avec plusieurs secteurs touchés, banques, industries, secteurs privés comme publiques.

Face à cette menace, la législation s'est également renforcée et cela depuis les années 2010 avec la définition d'une stratégie nationale de cybersécurité, la mise en place du cadre légal (lois 05-20, 09-08, 43-20, etc.) et la définition d'une Directive Nationale de Sécurité des Systèmes d'Information imposée à l'ensemble des entités ayant des infrastructures d'importance vitale pour le pays.

C'est dans ce contexte que Cyberforces et Wavestone ont organisé un symposium dédié aux enjeux et perspectives de la cybersécurité au Maroc: le Cybersecurity Day.

Cet événement d'une journée, non ouvert au public, a rassemblé plus de 150 décideurs et responsables de la sécurité des SI des secteurs public et privé marocains. Il a pour vocation de créer un écosystème homogène et qualitatif, où les experts, les chercheurs et les professionnels sont rassemblés autour d'une plateforme d'échange pour partager des idées novatrices, des recherches pointues et des solutions pratiques autour des enjeux de la cybersécurité au Maroc, à l'aune des aspects réglementaires et normatifs du Royaume.

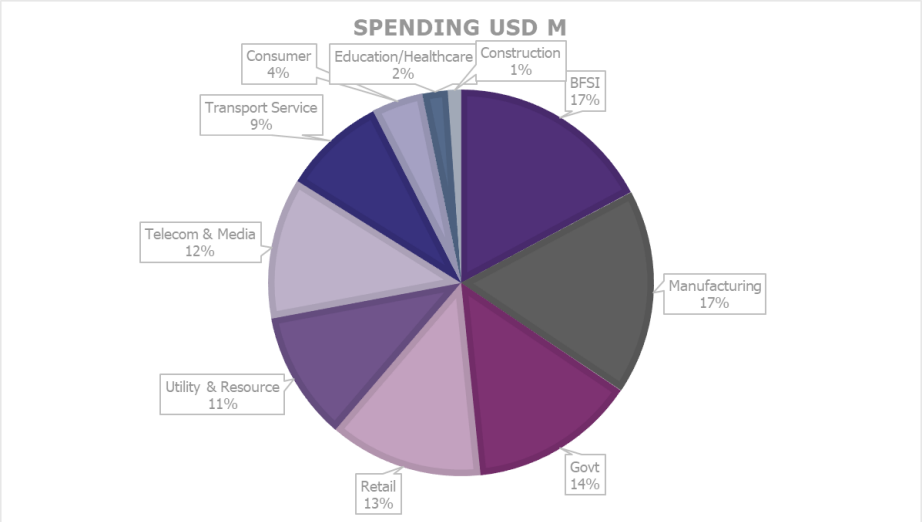


Etat des lieux : quel niveau de maturité Cybersécurité du marché ?

Le Maroc et la maturité Cyber

Le Maroc progresse dans les classements internationaux de maturité Cyber…

Le royaume est désormais classé 32ème [1] au dernier classement du « National Cybersecurity Index » qui classe les pays selon leur niveau d'engagement en matière de Cybersécurité. Le Maroc est également classé 50ème [2] au dernier classement du « Global Cybersecurity Index », autre index mesurant l'engagement des pays en matière de Cybersécurité au niveau global.



… avec un engagement d'ampleur des décideurs africains en matière de Cybersécurité observé

En 2022, le secteur financier et le secteur industriel occupaient tous deux la 1ère place en Afrique[3] avec le plus d'engagements d'investissement en matière de Cybersécurité observée avec 16% du total d'investissements Cyber, en 2ème et 3ème place se positionnaient respectivement le secteur public et le secteur du Retail.

Les décideurs et membres des conseils d'administration en Afrique accordent aujourd'hui une importance primordiale à la cybersécurité et considèrent la protection des données de leurs clients et de leurs collaborateurs comme l'une des principales priorités à traiter.

La majorité des décideurs sont également conscients de l'importance d'avoir des systèmes d'information et des processus résilients et en font une priorité à mesure similaire. Toutefois, l'instauration d'une culture de la résilience et d'une infrastructure et des processus résilients dans l'ensemble de l'organisation est une entreprise de grande envergure nécessitant une attention soutenue et des budgets dédiés.

[1] NCSI
[2] GCI
[3] IDC Security spending tracker, July 2023

Évolution et Disparités dans la Maturité en Cybersécurité

Une évolution qui se recoupe avec la hausse du niveau de maturité cybersécurité globale ...

Avec un score global de maturité de 49%[4] (+3 points depuis 2022), les entreprises au niveau international ressentent les effets positifs de leurs investissements cyber des dernières années. C'est ce que révèle la quatrième édition du Cyber Benchmark, outil Wavestone basé sur une évaluation terrain de plus de 100 entreprises, parmi les plus importantes en France, en Europe et récemment au Maroc sur près de 200 points de contrôles organisationnels et techniques inspirés des standards internationaux NIST CSF et ISO 27001/2.

49 / 100

score de maturité globale

... avec de fortes disparités sectorielles à l'international

Le niveau de sécurité global de 49% cache de fortes disparités en fonction des secteurs. La Finance tire son épingle du jeu avec un score de 59,2%[5] (+4,8 points depuis 2022). Ce résultat s'explique par les investissements historiques réalisés dans ce secteur, encouragés par les réglementations (DORA, NIS2, CRA).

L'Industrie est elle aussi en progrès (+4,6 points), fruit des efforts engagés pour rattraper le retard accumulé. Les Services (44%) et le Public (36,1%) ferment la marche. Bien que conscients des risques, ces derniers peinent à identifier les financements nécessaires.

Au Maroc, le Cyber Benchmark a principalement été déroulé chez des acteurs de la Finance et les premiers résultats montrent un niveau de maturité globalement en retrait par rapport au niveau mondial. Cela s'explique aisément car on est souvent sur des structures moins importantes en termes de taille et donc sur des équipes dédiées à la Cybersécurité et des budgets moins élevés qu'au niveau mondial.

Dans les organisations évaluées, les équipes continuent de grossir : on compte environ 1 personne dédiée à la cybersécurité pour 1300 employés, soit 11% de plus que l'an dernier. Pourtant, ce nombre semble resté trop faible au regard des enjeux actuels. Certains acteurs cherchent à traiter le sujet de manière dédiée, en particulier grâce aux "talent management programs".

En s'intéressant aux particularités de chaque secteur (réglementation, digitalisation, risque Cyber, ...), on constante qu'un palier a été atteint dans le secteur financier.

[4] Cyber Benchmark Wavestone, 2023 : https://ma.wavestone.com/fr/insight/cyberbenchmark-2023/

[5] Cyber Benchmark Wavestone, 2023: https://ma.wavestone.com/fr/insight/cyberbenchmark-2023/

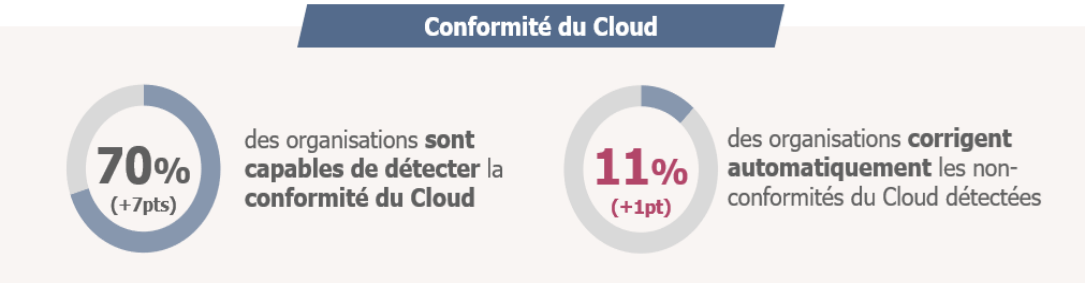
Sécurisation du Cloud

Sécurisation du Cloud : mieux administrer, superviser, détecter et remédier

Au niveau international le sujet Cloud a fait l'objet d'investissements importants, ce qui a permis d'augmenter grandement le niveau de maturité concernant la thématique de sécurité du Cloud, passant de de 36,1% à 44,5%.

La progression la plus importante se fait au niveau de l'administration Cloud : entre 2022 et 2023, 14% des organisations ont mis en place une authentification multi-facteurs (code en plus du mot de passe) ou un bastion (rebond intermédiaire) pour l'accès aux actions d'administration Cloud.

70% des organisations disent vérifier automatiquement la conformité du Cloud à l'aide d'outils ; cependant, elles ne sont que 11% à corriger automatiquement les problèmes associés.

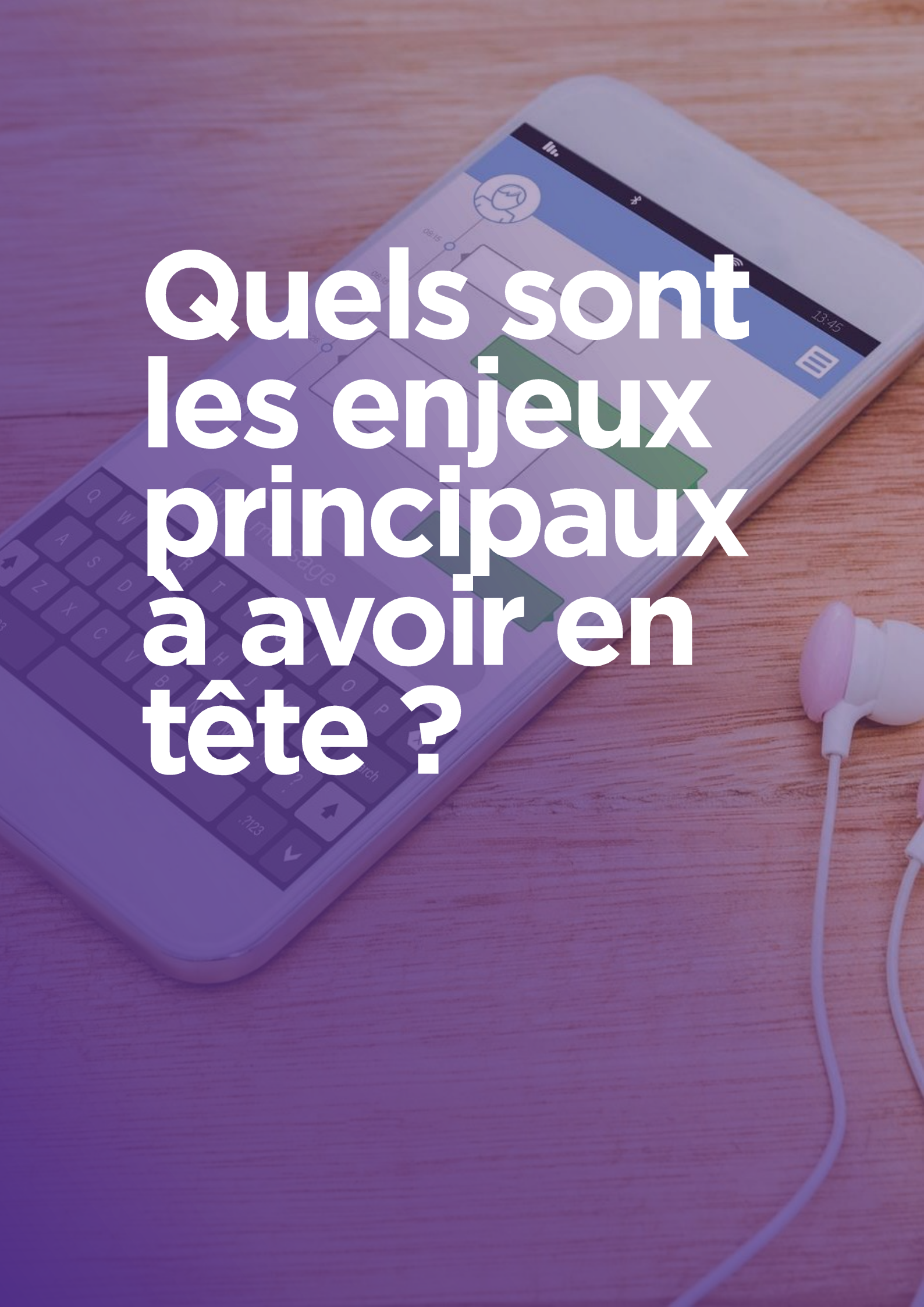


Au niveau de la région META (Middle East, Turkey, Africa), les secteurs les plus régulés tel que le secteur industriel (21%) et le secteur financier (12%) présentent les parts d'investissements les plus importants en termes de services et d'infrastructures Cloud[6] selon les derniers chiffres d'IDC. De manière globale, la région dépense 5% de son budget SI dans les sujets de cybersécurité, comparativement à 3,6% dans le reste de l'Afrique, selon le cabinet d'études.

Le secteur public et le secteur de la santé présentent quant à eux le taux de croissance annuel moyen le plus important sur 2021-2026 en région META avec respectivement 30,2% et 29,8% selon les mêmes chiffres.

Au niveau du Royaume, la situation est sensiblement différente. En effet, des cibles Cloud existent dans plusieurs organisations. Toutefois, ces cibles Cloud devront systématiquement être sur des Cloud souverains compte tenu de la réglementation en place, à date ces offres Cloud restent souvent limitées et plus onéreuses.

[6] IDC Public Cloud Infrastructure Spending, Jan 2023



Quels sont les enjeux principaux à avoir en tête ?

Risques liés à la cybersécurité

Les risques liés à la cybersécurité figurent sur la carte mondiale des risques identifiés par le World Economic Forum (WEF) depuis plusieurs années. Les risques Cyber ont évolués d'un niveau de risque bas en 2020 à un niveau moyen en 2023 et se classent désormais au 7ème rang parmi les risques les plus susceptibles de devenir une menace critique pour le monde, selon le classement Global Risks Horizon du World Economic Forum.

En 2023, le CERT-Wavestone (équipe de réponse à incident) a traité près de 40 incidents majeurs de cybersécurité pour des grandes entreprises ou des organismes publics, majoritairement français. Et pour 16 d'entre eux, une équipe dédiée a été mise en place pour accompagner le pilotage et la gestion de crise.

De manière générale, l'année a été riche en matière de cyber attaques, les groupes de cyber criminels étant toujours plus actifs. Face au contexte géopolitique tendu en Europe, si certains groupes d'attaquants se sont radicalisés pour effectuer des actions de déstabilisation en soutien à la Russie, la menace a peu évolué : la majorité des groupes d'attaquants reste motivée par des gains financiers, et continue de se développer à cette fin

Types d'attaques observées en 2023

Anatomie de la surface d'une attaque moderne

Microsoft met en lumière des éléments cruciaux sur les surfaces d'attaque les plus ciblées en 2023 avec des chiffres révélateurs[7] :

- Le temps médian nécessaire pour qu'un attaquant puisse se déplacer latéralement dans un réseau d'entreprise une fois qu'un appareil est compromis est d'1 heure 42 minutes.
- Une hygiène de sécurité de base pourrait prévenir 98% des cyberattaques.
- En se concentrant sur les e-mails, il est noté qu'une attaque de phishing peut permettre à un attaquant d'accéder à des données sensibles en 72 minutes, les attaques de phishing ne cessent également de croître avec évolution de 61% du nombre d'attaques observées de 2021 à 2022.
- L'évolution du paysage de l'identité offre de nouvelles opportunités aux acteurs malveillants, avec une augmentation de 74% des attaques de mots de passe observées en 2022. De plus, 93% des investigations faisant suite à des attaques de ransomware ont révélé un contrôle d'accès à privilèges insuffisant et des lacunes au niveau des contrôles de mouvement latéral.
- La sécurisation des surfaces d'attaque externes se révèle être un défi à l'échelle d'Internet, avec 1613 compromissions de données via Internet observées en 2021, dépassant l'intégralité des compromissions de données identifiées en 2020, et 53% des organisations ayant connu au moins une violation de données causée par un tiers entre 2018 et 2020.

Réponse à incident : les leçons de 2023

- La motivation principale des attaques reste le gain financier, avec 46% des incidents gérés. Le moyen d'extorsion le plus utilisé est toujours le ransomware.
- La porte d'entrée principale des attaquants demeure l'utilisation frauduleuse de comptes valides. Parmi les compromissions, les comptes Office 365 sont fortement représentés.
- Les attaques opportunistes dominent l'échantillon à 77%. En complément des ransomwares, elles ciblent aussi les données sensibles des organisations victimes, avec la menace d'une publication comme moyen de pression privilégié.
- Nous commençons dès aujourd'hui à voir les enjeux de demain : capacité de découplage de SI en urgence et influence de l'Intelligence Artificielle.

[7] *Anatomy of a modern attack surface | Security Insider (microsoft.com)*

Cibles : les attaques restent de nature opportuniste

Si tous les secteurs et toutes les tailles d'entreprises sont ciblés, quatre tendances se confirment :

1. Des structures touchées de plus en plus petites

Les grandes entreprises ont amélioré leurs capacités de détection et de réponse sur les dernières années, et sont donc moins sensibles aux attaques avérées.

En réponse, les cybercriminels s'orientent vers des cibles plus simples et moins matures en cybersécurité. A ce titre, nous remarquons une forte croissance des attaques sur le continent africain et le Maroc apparaît comme l'une des deux cibles privilégiées sur le continent, avec l'Afrique du Sud. Le Royaume est en effet, selon Interpol, le 2nd pays africain[8] dont les institutions financières ont subi le plus de cyberattaques en 2022.

« Cyberattaques au Maroc : menaces croissantes, vigilance impérative » Mohamed Halloum

Le constat est alarmant, avec des systèmes d'information au Maroc qui demeurent structurellement défaillants, exposant ainsi les organisations marocaines à des vulnérabilités sérieuses. Les attaques opportunistes prennent de l'ampleur, ciblant spécifiquement les pays émergents et les entreprises insuffisamment protégées, réduisant ainsi les efforts nécessaires pour atteindre leurs objectifs. Il est clair que la menace évolue, avec la barre de maturité Cybersécurité de plus en plus élevée, surtout pour les pays avancés, nécessitant une vigilance accrue face à ces nouvelles réalités. La nécessité de renforcer les infrastructures de sécurité est urgente pour faire face à cette tendance croissante d'attaques ciblées

2. Les données des entreprises de plus en plus visées

La menace de publication des données volées est devenue le moyen de pression le plus efficace auprès des entreprises qui en sont victimes. En 2023, 77% des cas de ransomwares observés[9] dans le cadre d'incidents de sécurité traités par le CERT-Wavestone pour le compte de clients internationaux combinaient un vol de données direct et des exfiltrations en amont du chiffrement ; la note de rançon faisait quasi-systématiquement mention du vol de données.

[8] *Interpol African Cyberthreat Assessment Report, 2023*
[9] *Rapport CERT-Wavestone, 2023*

3. L'effet de levier des plateformes de virtualisation

Les attaquants ont trouvé dans les environnements ou plateformes de virtualisation une façon de toucher plusieurs centaines voire milliers de serveurs virtuels en une seule attaque. Ces infrastructures sont ainsi devenues l'une de leurs cibles préférées.

4. La rapidité accrue des attaques

L'exécution d'un ransomware est passée de plusieurs semaines à quelques jours. Cette réduction du temps d'attaque a permis l'apparition d'attaques impliquant de multiples ransomwares, où des groupes d'attaquant différents peuvent s'en prendre à une même victime à moins de 2 jours d'écart.

Vecteur d'attaque 1 : l'utilisation de comptes valides volés reste toujours la porte d'entrée principale des attaquants

Cette année encore, les comptes utilisateurs valides restent une cible de choix[10] (42%), devant les sites web vulnérables (23%) et les systèmes d'accès distants (17%). Les accès à ces comptes sont obtenus par l'achat de base de données sur le darknet, l'exploitation de mots de passe faibles, ou encore très largement par des techniques de phishing.

En 2023, les compromissions de compte Office 365 sont fréquentes. Parmi les facteurs d'explications :

- la très forte utilisation de cette solution bureautique dans les entreprises ;
- le manque de sécurisation de ces comptes lors de leur mise en place.

En ce sens, nous avons pu observer durant le Cybersecurity Day une démonstration d''implantation d'un ransomware ciblant un OIV américain réalisée par Professeur Haitham Rashwan de Dell Cybersecurity Services. Dans la majorité des cas observés, la mise en place d'authentification multi-facteurs (MFA) aurait permis d'empêcher la compromission des comptes valides en question dans le cas d'infection ransomware ou autre vecteur d'attaque similaire.

[10] Rapport CERT-Wavestone, 2023

Vecteur d'attaque 2 : vol de données bancaires et extorsion via une évolution et une croissance des attaques de phishing et de la fraude digitale

En effet, l'année 2023 a vu la prolifération d'attaques visant autant les clients de grandes banques marocaines que les institutions bancaires avec comme objectif le vol de coordonnées et d'identifiants bancaires soit pour des usages d'extorsion ou de vente sur le darknet.

Les attaquants utilisent principalement des techniques de phishing qui ne cessent d'évoluer avec les avancées de l'IA pour cibler les clients des banques. Ces derniers envoient des SMS aux clients de la banque identifiés via des bases de données issues d'attaques antérieures ou via social engineering en se faisant passer pour leur banque légitime, les incitant ainsi à fournir leurs informations personnelles via des liens frauduleux.

Les nouveaux chiffres publiés par Interpol sur l'écosystème des menaces en Afrique sont alarmants et classent le Maroc en 2023 devant l'Egypte et l'Afrique du Sud comme pays le plus ciblé par les attaques de phishing[11] qui représentent 91 % des cyberattaques visant la population marocaine. Cette situation confirme la nécessité de renforcer la cybersécurité des institutions bancaires via des investissements et des moyens techniques et de sensibiliser les clients pour protéger les institutions financières et les individus contre ces menaces croissantes.

Vecteur d'attaque 3 : propagation de Malware via l'installation et le téléchargement de softwares non vérifiés

L'accélération de la digitalisation observée au Maroc dans les secteurs à régulation moins contraignante que le secteur bancaire tel que le secteur industriel, notamment au niveau des PME, engendre des risques Cybersécurité spécifiques liés à l'utilisation non autorisée de softwares et d'outils vulnérables ou infectés par le personnel.

Ce type de pratique informelle relève principalement d'une maturité Cybersécurité encore balbutiante dans ces secteurs où les fondations du socle de sécurité SI sont encore en cours de construction pour palier à :

[11] Interpol African Cyberthreat Assessment Report, 2023

La mise en place d'un processus standard pour évaluer les risques est un premier point d'attention à avoir en tête pour mieux anticiper les menaces potentielles et mettre en place les mesures de protection.

Capitaliser sur les possibilités d'outsourcing en faisant appel à des prestataires experts pour compléter l'équipe interne est un deuxième point clé à prendre en compte pour renforcer les compétences et la réactivité face aux cybermenaces.

Comment mieux se protéger face à ces menaces ?

Les réponses proposées par notre panel d'experts sont diverses et pourront être combinées pour assurer une protection optimale des entreprises.

Il faut tout d'abord noter que l'ensemble du panel s'accorde sur une prise de conscience des cadres dirigeants d'entreprises sur l'importance du sujet, pouvant légitimer la mise à disposition de capacités humaines et financières plus importantes.

Par ailleurs, la législation marocaine en place est continuellement renforcée par la DGSSI (Direction Générale de la Sécurité des Systèmes d'Information) qui joue un rôle central dans la régulation et le contrôle des activités cybernétiques avec la mise en place de lois, normes et directives (Loi 05-20, DNSSI ...) visant à assurer la sécurité des systèmes d'information à l'échelle nationale. La DGSSI exerce également une mission de prévention des risques cyber en élaborant des stratégies de sensibilisation, de formation et de surveillance, visant à renforcer la résilience du pays face aux menaces numériques.

ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Protection face aux menaces

En ce sens, le renforcement des réglementations en matière de cybersécurité a été classé comme l'enjeu destiné à avoir le plus d'impact sur les investissements et la stratégie des entreprises en Afrique[12], dans l'enquête IDC DX CIO de cette année.

« Évaluer les risques, externaliser, équilibrer les budgets et parler aux métiers pour une sécurité proactive »
Shilpi Handa[13]

La mise en place d'un processus standard pour évaluer les risques est un premier point d'attention à avoir en tête pour mieux anticiper les menaces potentielles et mettre en place les mesures de protection. Capitaliser sur les possibilités d'outsourcing en faisant appel à des prestataires experts pour compléter l'équipe interne est un deuxième point clé à prendre en compte pour renforcer les compétences et la réactivité face aux cybermenaces.

De plus, une répartition des budgets sécurité de manière équilibrée, ne se limitant pas uniquement à l'infrastructure, mais englobant tous les aspects critiques est primordiale.

Il est également nécessaire de viser la continuité opérationnelle en toute circonstance en soulignant l'importance de la surveillance constante et de l'adaptation aux évolutions des attaques, grâce à une politique de résilience parallèle à celle de la cyberdéfense. Enfin, l'usage d'un langage métier dans la gestion budgétaire est fortement préconisé, favorisant une meilleure compréhension et communication entre les parties prenantes.

« Une hygiène irréprochable dans la gestion des comptes : 10 actions cruciales pour le CISO »
Hicham FAIK

Il est impératif d'adopter une solide hygiène de sécurité, en particulier dans la gestion des comptes, pour garantir la robustesse du système. Parmi les actions prioritaires qu'un CISO devrait entreprendre immédiatement pour assurer une gestion optimale des comptes, il est crucial d'éliminer les comptes inactifs, qui sont des cibles attrayantes pour les hackers, en les fermant et en les rouvrant uniquement au besoin. Le contrôle des développeurs et des processus de développement est également essentiel.

[12] *https://cyberpolicyportal.org/states/morocco*
[13] *Associate Director, Analyse cybersécurité chez IDC, et intervenante lors de la Keynote d'introduction du Cybersecurity Day*

Une approche ciblée consiste à définir et suivre les activités sensibles, automatiser les processus de création et de suppression d'utilisateurs, éliminer les utilisateurs à privilèges aux capacités étendues, et documenter chaque action pour répondre aux attentes des auditeurs. La mise en place d'un processus d'autorisation efficace, incluant des chemins liés aux risques, des vérifications de séparation des tâches et des tests de vraisemblance, est essentielle. En restant vigilant au niveau des alertes sur les activités irrégulières, en révisant régulièrement les autorisations, et en adoptant une approche proactive, on renforce la sécurité de l'information dans sa globalité au sein du SI.

« Sensibiliser et partager son vécu » Driss Bennouna

Un premier moyen de se prémunir contre les attaques est d'accroître la culture Cybersécurité des organisations. Cela passe par des programmes de sensibilisation des effectifs internes (avec différents formats, capsules vidéo, exercices de phishing, événements dédiés ...) mais aussi des clients, en particulier pour les banques, car leur manque de sensibilisation peut être de plus en plus une source d'attaque.

De plus, il est important d'avoir des cercles de confiances (ex. : cercles de RSSI) pour partager des dernières attaques vécues par chaque organisation pour pouvoir mieux gérer les menaces et éviter leur généralisation chez plusieurs comptes marocains.

Wavestone et Cyberforce ont d'ailleurs à cœur de faire du **Cybersecurity Day** un espace d'échange et de réseautage permettant par exemple aux parties prenantes de partager les retours d'expérience à ce sujet, de manière formelle ou informelle.

« La sécurité, pas qu'une affaire de solutions mais surtout d'hygiène » Younes Felahi

Plusieurs organisations ont consenti à des investissements relativement importants ces dernières années dans l'acquisition et le déploiement de solutions sécurité ainsi que la définition d'un cadre de gouvernance de la sécurité SI.

Toutefois, cela peut s'avérer insuffisant.

En effet, il est nécessaire de faire preuve de rigueur au sein des équipes opérationnelles pour appliquer au quotidien les directives sécurités et réduire au strict minimum les exceptions au sein des organisations (ouverture de ports USB, attribution des droits étendus sur un périmètre SI, installation d'un logiciel non validé au niveau sécurité, ...).

Autant de vecteurs de diffusion d'un malware au sein de l'entreprise. Par ailleurs, on peut retrouver cette rigueur dans l'application sur le terrain de règles simples permettant de se prémunir contre les attaques (simplification des architectures SI, définition de patterns de développements, ...)
Qu'en est-il des aspects de gouvernance ? de procédures ? de législation ?

« La détection et la remédiation automatisées comme recours à la sophistication des menaces »
Kamel Bouleimen

Les menaces actuelles sont caractérisées par leur sophistication croissante, leur rapidité d'exécution et leur ampleur significative. Face à ces défis, la solution préconisée est d'adopter des approches de détection et de remédiation intelligentes et automatisées, en mettant particulièrement l'accent sur une analyse comportementale avancée. Cette approche permet une anticipation maximale des attaques, offrant ainsi une réponse proactive aux menaces émergentes. En outre, l'importance de penser en termes de résilience globale est soulignée, suggérant une stratégie intégrée qui aborde les aspects préventifs, réactifs et adaptatifs de la cybersécurité pour assurer une protection complète et durable.

Et demain ?

Les tendances cyber à surveiller en priorité

Des tendances cybersécurité qui se démarquent sur le continent africain

Les derniers chiffres présentés par IDC reflètent une adoption croissante des technologies de détection et de réponse telles que l'EDR/NDR comme tendance numéro 1 en Afrique[14] , cet intérêt est motivé par la pénurie de compétences et le besoin de réduire le temps de résolution des incidents. Une mouvance vers les services MDR est aussi observée compte tenu du besoin croissant d'automatisation des opérations de sécurité de détection et de réponse.

Par ailleurs, d'importants investissements ont été observés dans le lancement de chantiers IAM (Identity Access Management), motivés par un engouement toujours d'actualité pour les initiatives Zero Trust comme deuxième tendance observée en Afrique[15]

La gestion des surfaces d'attaque est également l'une des trois principales tendances en matière de cybersécurité en Afrique[16] avec un intérêt croissant pressenti pour la visibilité des actifs et la gestion continue des vulnérabilités.

Zero Trust, une stratégie majeure en déploiement

Outre les problématiques organisationnelles, le marché s'adapte autour de nouvelles solutions de sécurisation pour accompagner la transformation digitale.
Cette transformation est portée par des réflexions "move to cloud" présentes dans plusieurs comptes marocains même si ralenties par des restrictions réglementaires auxquelles sont soumises les OIVs et des réticences observées chez les entreprises marocaines à transitionner vers un modèle full Cloud voire hybride.

Cette digitalisation accrue est également portée un rapprochement entre l'OT et l'IT dans le monde industriel, et encore et toujours l'ouverture du système d'information à de nombreux partenaires, acquisitions ou clients.

Ce mouvement entraîne des réponses tactiques en cybersécurité, avec l'apparition d'un outillage permettant de mieux maîtriser les projets en cours (voir encadré sur le Cloud).

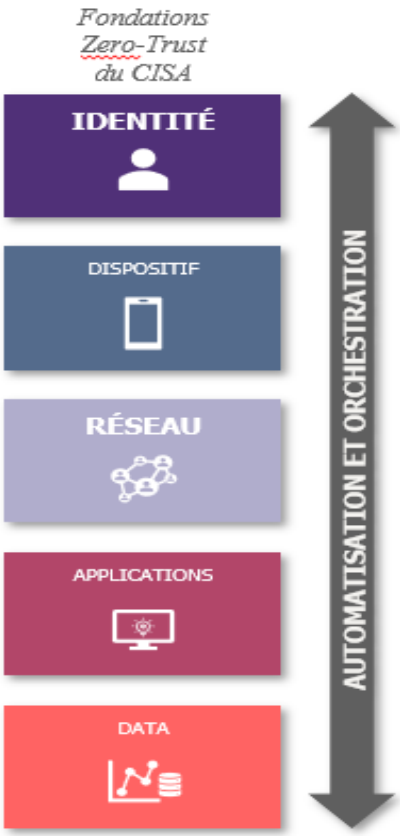
[14] *IDC's Security Survey, 2023 (January); Africa (n = 182)*
[15] *IDC's Security Survey, 2023 (January); Africa (n = 182)*
[16] *IDC's Security Survey, 2023 (January); Africa (n = 182)*

A moyen terme, l'atomisation du système d'information se poursuit et nécessite de repenser son modèle de sécurité – évidemment vers une logique Zero Trust.

Le Zero Trust est l'un des enjeux majeurs de ces prochaines années en cybersécurité. Quelques chiffres[17] illustrent son implémentation actuelle auprès de comptes internationaux et de quelques comptes marocains :

- 28% prennent en compte la sensibilité des ressources et le contexte de connexion et appliquent une authentification multi-facteurs (MFA) avec accès conditionnel – déployée à hauteur de 73% en moyenne
- 24% des entreprises ont mis en place une micro-segmentation automatique en fonction de l'exposition, de la sensibilité, de l'environnement, etc. – déployée à hauteur de 32% en moyenne.
- 14% ont intégré du Zero Trust Network Access basé sur l'identité à leurs environnements Cloud – déployé à hauteur de 46% en moyenne.
- 13% ont commencé à déployer un Security Orchestration, Automation and Response (permettant d'isoler les ressources lors de la détection d'une alerte – déployé à hauteur de 48% en moyenne.

.



[17] Cyber Benchmark Wavestone, 2023

Longtemps perçue comme une simple philosophie, le Zero Trust prend aujourd'hui de l'ampleur et les initiatives en ce sens gagnent en maturité, les investissements continuent ainsi de croître avec 60% des organisations au Moyen-Orient qui auront démarré des initiatives Zero Trust d'ici fin 2023[18]. Les principes se déclinent en mesures concrètes et de nouvelles solutions apparaissent : citons par exemple la publication des premiers frameworks, comme celui du DoD (Department of Defense) aux États-Unis. Les retours d'expérience s'avèrent plutôt positifs, en particulier sur les logiques d'accès distant ou de micro-segmentation. Pour les défis à venir, on pense forcément à la gestion de l'identité et des accès des collaborateurs, des partenaires, des clients, mais aussi de plus en plus des machines ou des données, avec les fameux IdP (Identity Provider). Cependant, le chemin vers une migration complète du système d'information semble long, n'aura sans doute pas d'intérêt pour les systèmes les plus anciens qui devront être protégés autrement.

Prévoir l'exploitation de l'IA par les cybers criminels

L'autre menace à anticiper pour 2024 et pour le futur est celle de l'intelligence artificielle.

D'une part, car les cybers criminels détournent aujourd'hui des applications de l'Intelligence Artificielle générative pour améliorer leurs capacités d'attaques, plus nombreuses et plus performantes. Par exemple avec des textes de meilleure qualité, des codes malveillants rénovés ou encore en utilisant des fausses vidéos/photos générées par l'IA (deepfake).

D'autre part, car les cybers criminels attaquent les IA directement en utilisant des méthodes d'attaques innovantes. Cela leur permet d'empoisonner des systèmes pour les faire dysfonctionner et, par exemple, contourner les mécanismes de lutte contre la fraude ou encore de voler des données en faisant parler à outrance les Chatbots.

[18] *IDC Security Survey 2022, Middle East. Base: 424*

Ne pas négliger la sécurité des objets connectés (OT/IOT)

La objets connectés (OT/IOT) peuvent représenter le maillon faible des réseaux interconnectés et leur sécurisation reste un enjeu critique pour les organisations avec 45% des CISOs en Afrique[19] ayant déclaré la sécurisation de la convergence IT-OT leur principale priorité en 2023.

Se prémunir contre le risque de Data Breach

En 2023, le coût moyen d'une Data Breach causée par un acteur interne malveillant s'élève à 4,90 millions de dollars américains. Les attaques de phishing représentent 16% des vecteurs d'attaque initiales observées dans le cadre de Data Breachs[20] . Le cycle de vie d'une Data Breach requiert en moyenne 277 jours aux organisations cibles pour être identifié et maîtrisé. Les organisations qui tirent parti de l'IA et de l'automatisation des opérations de sécurité sont en mesure de réduire ce délai de 108 jours par rapport à celles qui n'en font pas usage. Les activités de Threat Intelligence permettent également une identification précoce des violations, raccourcissant le délai de 28 jours. De plus, les entreprises dotées à la fois d'une équipe et d'un plan de réponse à incident réussissent à identifier les violations 54 jours plus rapidement que celles qui n'avaient ni l'un ni l'autre.

[19] *IDC Security Survey, January 2023, META. 100+ employees, Base: 182*
[20] *IBM Security, Cost of a Data Breach Report, 2023*

Talent Management : recrutement et fidélisation des cyber-experts via une stratégie RH efficace

Dans un marché de l'emploi tendu avec un sous-effectif de profils Cyber (déficit observé de 4 millions de talents dans le monde[21] alors que les effectifs dans ce domaine ont augmenté de près de 10% au cours de l'année écoulée), suivre les évolutions techniques et la prolifération des menaces et des risques Cyber impose une stratégie RH efficace reposant sur deux piliers : le recrutement et la formation, et la rétention des talents.

Le premier nécessite parfois de la créativité! Par exemple, en recrutant des profils non spécialistes à former, en s'appuyant sur la mobilité interne ou en visant à augmenter la diversité des profils, en particulier vers les femmes. Une fois l'équipe constituée, il devient crucial de fidéliser les collaborateurs :

- Les salaires peuvent être des leviers d'attractivité... comme de départ. La filière cybersécurité révèle des disparités salariales croissantes entre les secteurs, et, à plus large échelle, entre les pays.
- La connaissance des profils et compétences clés permet d'arbitrer entre expertise et management, tout en donnant des objectifs clairs, un chemin de carrière et des enjeux adaptés à chacun.
- La formation continue de chaque type de profil est aussi un facteur de rétention ; stratégie que les organisations devraient développer davantage, avec une formation initiale pour les profils non-cyber et la construction d'un cursus d'expertise pour les profils avancés.

[21] *Etude ISC Square, 2023*

MSSP (Managed Security Service Provider) : choisir la bonne stratégie de Sourcing selon le service, le besoin et les ressources à disposition

Les stratégies cyber ne peuvent plus faire l'économie du facteur humain pour maintenir leur niveau de sécurité. La première question que devraient se poser les RSSI : "make or buy"? Autrement dit, faut-il internaliser les compétences, ou bien externaliser les activités auprès de tiers plus ou moins proches? Historiquement, le réflexe était de se tourner vers l'extérieur dans le cadre d'un besoin temporaire ; la sécurité était vue comme un mal nécessaire. Aujourd'hui, elle devient une problématique métier à part entière, avec l'augmentation des enjeux de résilience, du niveau de sécurité des produits, des exigences dans les appels d'offre, de la multiplicité des solutions et technologies sur le marché, ou encore de l'intérêt des clients. Dès lors, il paraît indispensable de réfléchir en profondeur à sa stratégie et d'adopter une approche de Smart Sourcing.

De récents chiffres[22] donnent une idée sur les tendances de Sourcing au Maroc à travers les préférences des organisations marocaines en termes de modèle opérationnel SOC comme exemple, les tendances observées estimant que 58% des organisations marocaines optent pour un modèle opérationnel hybride combinant des ressources in-house et MSSP pour la gestion de leur SOC.

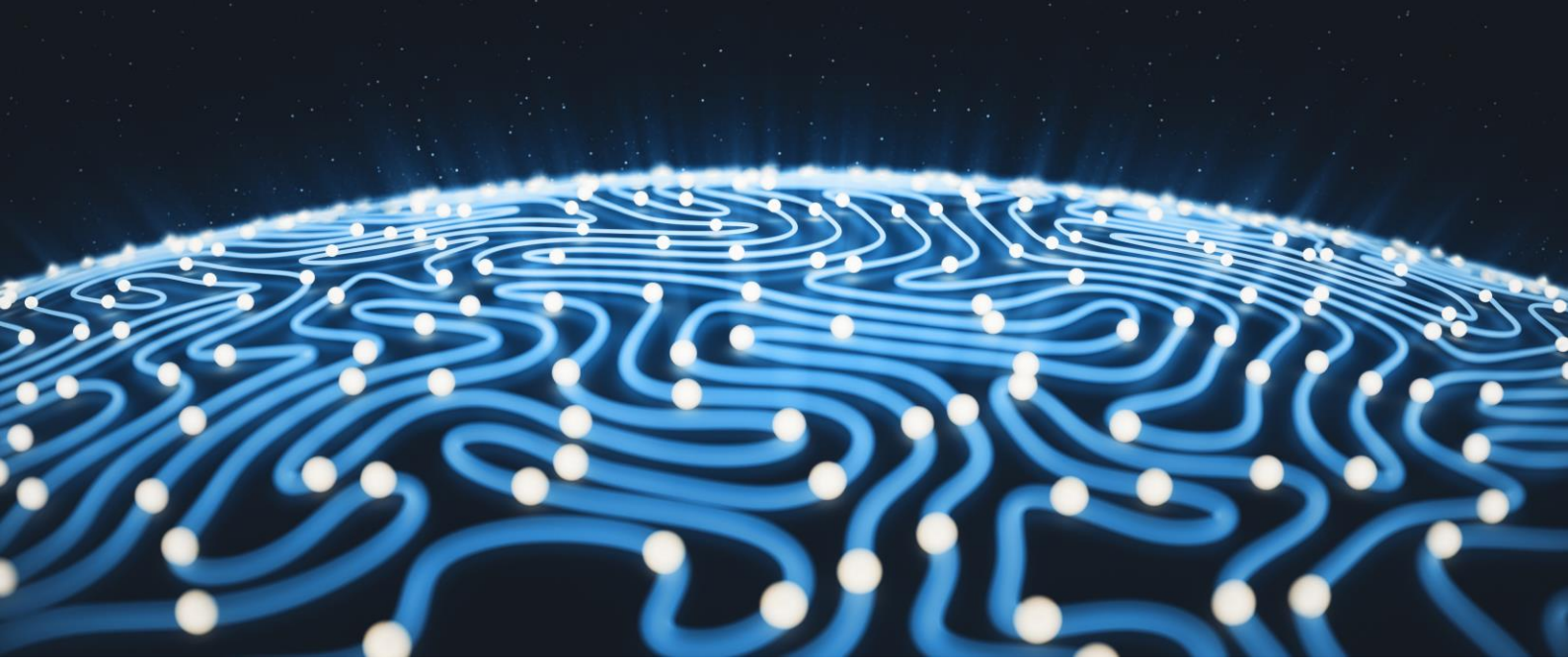
[22] *IDC Security Survey Feb 2023, Morocco n= 300C*

La sécurité des tiers face au défi d'une interconnexion croissante

De nombreux attaquants profitent des failles de sécurité dans les systèmes des tierces parties pour atteindre une organisation. Première étape pour limiter ce type d'intrusion : identifier les partenaires et prestataires à encadrer en priorité. Usuellement, les départements achats identifient les niveaux de risques en fonction du chiffre d'affaires réalisé par les tiers. Mais ce classement n'est pas toujours pertinent pour évaluer un risque de fuite de données ou d'interruption de services, dans la mesure où des prestataires de petites tailles peuvent détenir des informations critiques ou fournir un maillon d'un service essentiel.

Pour les plus critiques, il est nécessaire d'envisager un renforcement des engagements contractuels en matière de sécurité et de résilience. Pour aller plus loin, ce risque doit être pris en compte dans les processus, qu'il s'agisse de la gestion d'incidents touchant les tiers, la capacité à les intégrer dans ses systèmes de gestion d'accès, voire de leur propre niveau de résilience cyber.

Les plateformes de gestion de tiers sont une piste pour centraliser les résultats et les moyens d'agir. Celles-ci seront autant utiles en prévention, pour les analyses de résilience, que pour la définition et le suivi de la mise en œuvre des exigences, ou encore en réaction en cas d'incident.



Changement de posture : de CISO à CSO (Chief Security Officer), une transformation en cours

Le métier de CISO, principalement dans le secteur financier, opère un mouvement profond qui en fait beaucoup plus qu'une expertise technique. Les dirigeants attendent aujourd'hui des RSSI une posture de managers pour optimiser l'efficacité des projets (gestion du budget, des équipes…), et une vision large du risque et de la résilience.

Ce changement de dimension est d'ailleurs en train de s'étendre dans les autres secteurs tel que le secteur industriel au fil des années.

Le CISO doit ainsi s'inscrire dans une perspective à plus grande échelle pour répondre aux nouveaux attendus en termes de pilotage, organisation et compétences liés à son rôle :

- Extension du périmètre de responsabilité du CISO avec le passage de plusieurs activités historiquement indépendantes tel que l'anti-fraude, la sécurité physique, la résilience, la sécurité industrielle dans le scope du RSSI.
- Responsabilité accrue du CISO vis-à-vis de la direction générale : le RSSI répond directement à un membre du COMEX et se soustrait de son ancien rattachement au DSI avec un reporting régulier sur l'activité Cyber à un niveau stratégique
- Vision Métier et capacité de gestion du CISO : nécessité de disposer d'une bonne vision et compréhension des enjeux et risques métier et de compétences managériales pour optimiser l'efficacité des projets (gestion du budget, des équipes…), en complément à de solides compétences techniques

Conclusion

La cybersécurité au Maroc est confrontée à des défis complexes qui exigent des stratégies intégrées et des efforts soutenus de la part des entreprises, des gouvernements et des experts du secteur.

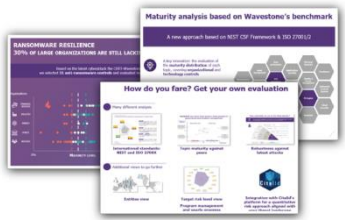
Malgré les progrès réalisés dans le renforcement de la législation et l'organisation d'événements de sensibilisation comme le Cybersecurity Day, des disparités sectorielles persistent, mettant en évidence la nécessité d'une approche globale et de ressources financières adéquates.

Les recommandations des experts, notamment en matière de sensibilisation, d'adoption de bonnes pratiques et de mise en œuvre de stratégies Zero Trust, soulignent l'importance cruciale de la préparation face aux menaces émergentes.
La transformation des rôles des CISOs en Chief Security Officers reflète une prise de conscience croissante de l'importance stratégique de la cybersécurité au sein des organisations.

En conclusion, la collaboration étroite entre les parties prenantes reste essentielle pour faire face efficacement aux défis de la cybersécurité tant au niveau national qu'international.

Annexe

Evaluez votre maturité Cyber et définissez votre stratégie avec l'outil Wavestone Cyber Benchmark



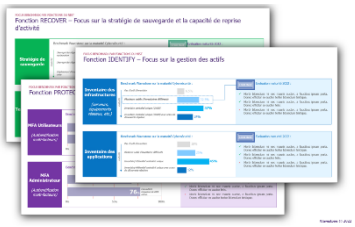
Le Cyber Benchmark est un outil grâce auquel Wavestone vous permet d'évaluer votre niveau de maturité cybersécurité selon une approche exhaustive :

- 200 questions traitant de l'ensemble des thématiques cybersécurité et reprises des référentiels internationaux NIST CSF et ISO 27001/2
- Des points de contrôles organisationnels et techniques

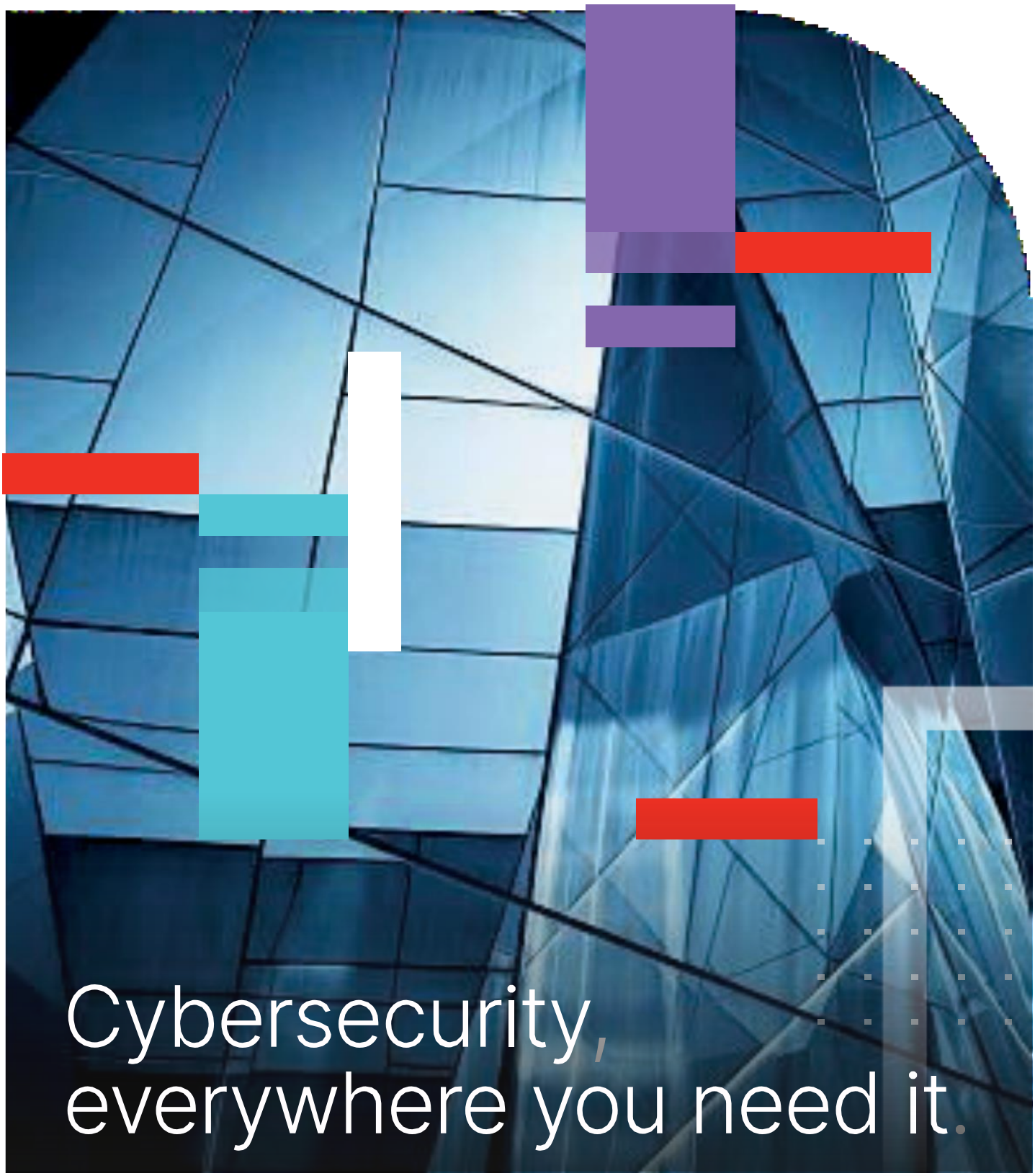
Cet outil permet à une organisation de se comparer avec ses principaux compétiteurs au niveau de son secteur et du marché :

- Plus de 100 entreprises, parmi les plus importantes en France, en Europe et désormais au Maroc
- Une analyse détaillée de votre secteur (Finance, Industrie, Energie, Services, Secteur public)

Assurant la possibilité d'approfondir l'analyse avec des modules spécifiques :



- L'outil offre la possibilité de ressortir clairement les domaines d'amélioration et analyser en détail les sujets pour lesquels l'organisation est à risque
- 3 modules disponibles dès aujourd'hui pour une analyse approfondie
- Alimentés par une expertise interne Wavestone



The Fortinet Security Fabric is the industry's highest-performing cybersecurity mesh platform. Delivering broad, integrated, and automated cybersecurity capabilities supported by a large, open ecosystem makes cybersecurity mesh architectures a reality. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities. **Learn more at fortinet.com**

FORTINET®

CYBERFORCES

Protect your business

WE PROTECT YOUR BUSINESS

CYBERFORCES, VOTRE CYBERSÉCURITÉ À 360°.

ANALYSER ET STRUCTURER

Mesurer votre exposition actuelle aux risques et établir votre stratégie en termes de cybersécurité.

PROTÉGER

Implémenter les solutions techniques sécurisant votre SI, avec un haut nouveau de contextualisation.

MAINTENIR ET DÉTECTER

Assurer le maintien en conditions opérationnelles et de sécurité de vos organes de sécurité et surveiller vos environnements.

CONTACT US

+212 522 78 79 75

sales@cyberforces.net

www.cyberforces.net

4ème Etage, Rue Zoulikha Naciri, Lotissement Florida
Centre Parc Lot 2, Casablanca 20270, Maroc

WAVESTONE

Nous accompagnons les grandes entreprises et organisations dans leurs transformations les plus critiques

Business & technologie

17 pays

4 terrains d'excellence

CA 835,2 M€

5500 collaborateurs

Tel +(212)5 22 36 32 92

Businessmonitoring@wavestone.com

https://ma.wavestone.com/fr/

Tour Capital Tower Casablanca, Maroc


CYBERFORCES
Protect your business
WAVESTONE