CESIN : Les instantanés S2 2023

Les instantanées du CESIN du deuxième semestre de 2023 s'appuient sur 11 mini-sondages hebdomadaires effectués auprès des membres du CESIN. Les panels varient entre 74 et 166 répondants avec une moyenne se situant à 121 répondants pour ce semestre.

Les questions posées chaque semaine sont hétérogènes. Elles sont regroupées selon 4 catégories : les sujets d'actualité / incidents notables de la période passée, mesures de sécurité, l'organisation / gouvernance et innovation.

Cette nouvelle synthèse apporte une vue synthétique et facilement exploitable ainsi qu'un regard éclairé sur chaque question.

Les mesures de sécurité

Les questions hebdomadaires soumises aux membres du CESIN traitent tout à la fois de processus et procédures que de mesures techniques. Elles ne sont pas ordonnées ici selon un quelconque ordre de priorité, ni par chronologie.

BYOD

À la lumière des enjeux Numérique Responsable, puisque les équipements utilisateurs représentent près de 80% de l'empreinte carbone numérique (source : ADEME/ARCEP) due en grande majorité à la fabrication de ces équipements, le débat autour du BYOD refait son apparition dans certaines organisations. Les détracteurs du BYOD font valoir que, depuis ces 3 ou 4 dernières années, les postes ne disposant pas des protections de sécurité minimum, notamment les EDR, ont été de sérieux vecteurs d'entrée pour les attaques, et que les efforts consentis pour protéger le parc des endpoints corporate sont ruinés si par ailleurs des laptops non correctement protégés peuvent se connecter sur les réseaux de l'entreprise. La propriété des terminaux (laptops et smartphones) ne fait toujours pas consensus, les stratégies combinent ou oscillent entre le BYOD (Bring Your Own Device), le COPE (Company Owned, Personally Enabled) et le COBO (Company Owned Business Only). Les politiques BYOD, COBO, CYOD ou BOPE sont autant d'outils de gouvernance aidant à orienter la gestion des actifs. Il est essentiel de les choisir avec soin afin de mettre en place un cadre réglementant les usages Ce cadre doit être transmis, compris et intégré à l'environnement de travail.

Pour rappel, en 2022, 40 % des PME ont été victimes de cyberattaques, dont 95 % avaient une origine humaine. Cela soulève la question de la manière de réduire le risque humain. Si la sensibilisation, les campagnes de phishing ou l'éducation sont autant d'outils à mobiliser pour atténuer ce risque, il est également efficace, voire plus, de réduire les surfaces d'attaque afin de bloquer les portes d'entrée dans son SI.

Nous vous avions questionné nos membres en 2019 sur le sujet et nous avons voulu savoir si la situation a évolué **[Q123].** Sur 149 répondants à ce sondage :

57% interdisent le BYOD dont :

- **23%** pour les laptops et smartphones mais des usages privés sur les terminaux d'entreprise sont admis ;
- **10%** pour des raisons de sécurité, en tant que matériel destiné à exécuter sa mission professionnelle, mais le smartphone personnel est admis et enrôlé uniquement au titre de la fourniture d'un second facteur d'authentification dans le cadre de la généralisation du MFA ;
- **9%** pour les laptops et smartphones, les usages privés sur les terminaux d'entreprise sont également interdits ;
- 10% mais en partie subi car il s'est développé un certain nombre d'exceptions qui sont tolérées ;
- **5%** pour les laptops et smartphones des collaborateurs, mais est admis et encadré pour certaines populations et en particulier les prestataires.

Les **37%** restant ont opté pour plusieurs cas de politiques où le BYOD :

- pour les smartphones est admis et encadré pour une partie du parc des terminaux (base de volontariat des collaborateurs) (**27%**) ;
- pour les laptops est admis et encadré pour une partie du parc des terminaux (base de volontariat des collaborateurs) (**4%**) ;
- est largement répandu dans l'entreprise et encadré aux plans RH et sécurité (**3%**) ;
- a été mis en place mais il y a un retour arrière pour des raisons RH et/ou sécurité (**2%**) ;
- est le modèle « par défaut », l'entreprise ne fournit pas d'équipement d'entreprise aux collaborateurs (sauf de manière exceptionnel) (**1%**);

Enfin **6%** d'entre vous ont répondu être dans une autre configuration.

MDM - Mobile Device Management

Dans le prolongement de notre question sur le BYOD, nous voulions étudier son impact sur le MDM. Ainsi, la question **[Q125]** consistait à savoir quelle était la stratégie cybersécurité du EMM/MDM pour les équipements BYOD ? Par ailleurs, s'agissant de l'enrôlement des terminaux BYOD à une solution EMM/MDM, des dispositions juridiques particulières ont-elles été mise en œuvre ? 120 membres ont répondu à cette question.

Le Mobile Device Management est une suite d'outils destinée à surveiller, administrer et sécuriser une flotte de terminaux mobiles en entreprise. La procédure d'enrôlement, où chaque appareil est enregistré dans la solution MDM, constitue une étape cruciale. Les politiques de sécurité et d'utilisation sont ensuite définies, garantissant que seuls les appareils enregistrés ont accès aux ressources de l'entreprise, avec des paramètres tels que le renforcement du système, l'attribution d'accès au Wi-Fi et au VPN.

50% autorisent les BYOD[1] avec :

- une politique de sécurité différente des équipements internes (**23%**) ;

1 Ce chiffre reste en cohérence avec celui de la question précédente (57%) l'échantillon de répondants n'étant pas forcément identique

- sous réserve "d'être enrôlés dans le MDM et se voir appliquer la même politique de sécurité qu'un équipement interne" (**27%**).

Pour **42%** d'entre vous, les BYOD sont interdits. Enfin, **9%** ont répondu "autres" notamment quand le BYOD est autorisé pour des utilisations bien spécifiques, avec des règles d'implémentation ou de sécurité spécifiques selon les organisations.

L'impact des politiques MDM se révèle crucial dans la gestion du BYOD, avec la possibilité d'autoriser ces dispositifs tout en appliquant des politiques de sécurité différenciées. Certains adoptent une approche stricte, interdisant les BYOD, tandis que d'autres permettent ces dispositifs sous réserve de l'enrôlement dans le MDM et l'application des mêmes normes de sécurité que pour les équipements internes.

SELF RESET

La gestion des oublis de mot de passe par les utilisateurs représente un nombre conséquent d'appels aux services desk des entreprises, pour ceux qui ont conservé un processus humain de reset. Les difficultés liées à l'authentification de l'appelant afin de vérifier si la demande est légitime restent prégnantes. Le besoin de réinitialiser un mot de passe en cas d'oubli est réel mais nous savons aussi que de nombreux nouveaux cas d'attaques utilisent ce processus de reset de mot de passe pour obtenir des comptes valides d'accès au SI. Ce processus doit donc être solide qu'il soit humain ou automatique, pour éviter des attaques soit techniques soit d'ingénierie sociale, en encore hybrides.

Nous essayons, dans tous les périmètres du SI de forcer une authentification à double facteur pour confirmer des identités. Il ne serait pas cohérent de permettre des self-reset de mots de passe sur la base de la fourniture d'un seul facteur.

La solution de la question secrète reste perfectible. Parfois les réponses sont aisément devinables par un attaquant, parfois les questions sont trop complexes et l'utilisateur lui-même ne se souvient plus de la réponse. Et la méthode se heurte souvent à des problèmes de confidentialité sur le stockage des réponses quand ce ne sont pas des sujets CNIL par rapport aux données utilisées.

Le renvoi du mot de passe sur une messagerie tierce et la plupart du temps personnelle se heurte au problème du refus potentiel de l'utilisateur de communiquer une adresse email personnelle.

114 ont répondu à cette question **[Q126]** visant à connaître la stratégie de sel-reset password mise en place dans les organisations.

47% n'ont pas de vrai "self-reset" password :

- pour **36%**, les reset passent par le support et
- pour près de **11%,** il y a un processus humain sécurisé permettant de qualifier et valider les demandes avec authentification de l'utilisateur de manière formelle (par exemple par rappel du hiérarchique, d'un collègue, etc.).

45% ont mis en place une stratégie de "self-reset" password répartis comme suit :

- **11%** ne l'autorisent que si la demande est effectuée depuis un poste corporate et qui authentifie en plus le demandeur sur la base d'un facteur (par exemple le smartphone) ;

- **8%** ne l'autorisent que si le demandeur est sur le réseau interne (pour limiter les risques d'usurpation) et qui l'authentifie sur la base d'un facteur (par exemple le smartphone), cela oblige le demandeur à venir sur site ;
- **8%** authentifient le demandeur sur la base d'un facteur (par exemple le smartphone) et en envoyant un mail de demande de validation sur l'adresse personnelle du salarié, c'est accepté chez eux ;
- **7%** authentifient le demandeur sur la base d'un facteur (par exemple le smartphone) et en envoyant un mail de demande de validation à un tiers (par exemple le manager) ;
- **4%** ont mis en place une solution de self-reset avec question secrète en ayant adressé les risques liés au stockage des réponses et les aspects juridiques potentiels (renforcement du stockage des réponses, déclaration à la CNIL, etc.) ;
- **7%** ont mis en place une solution de self-reset avec question secrète en assumant les risques liés au stockage des réponses et les aspects juridiques potentiels ;

Enfin, près de **8%** ont répondu "autre" soit parce qu'ils ont des manières hybrides de gérer cette question selon les publics ou ont une authentification passwordless (voir le rapport de la synthèse des instantanées du premier semestre 2023[2]).

La gouvernance / l'organisation

Le cycle de la maturité : retour sur l'Université d'Été du CESIN

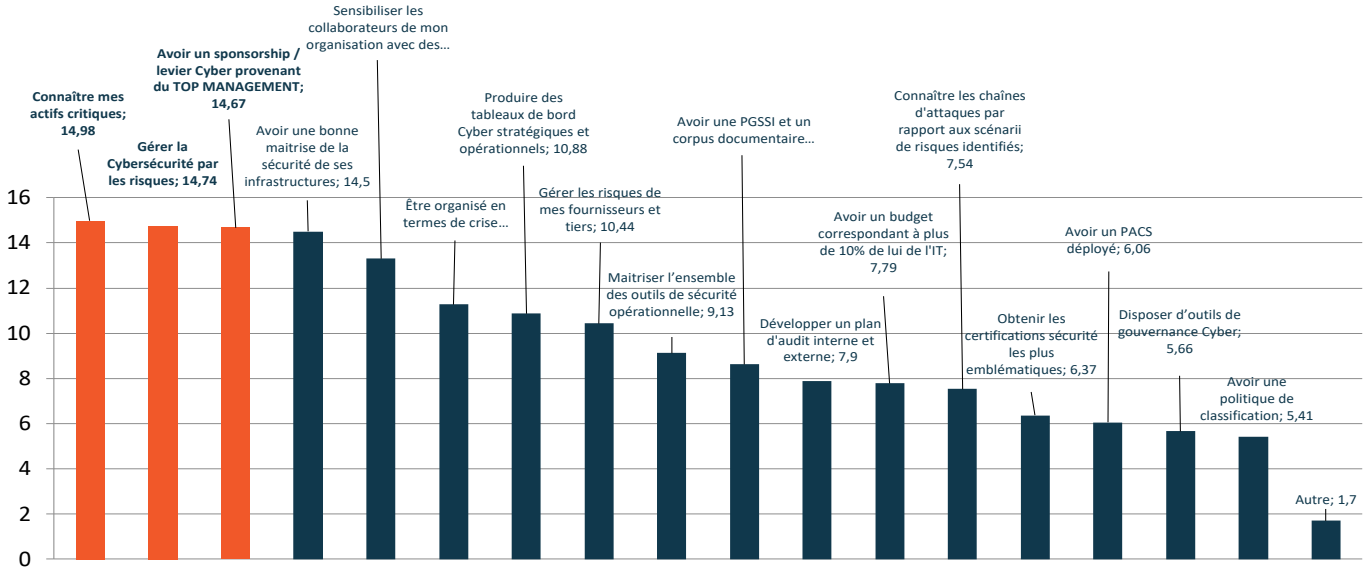
A l'été 2023, nous avons interrogé nos membres sur le sujet de la maturité cyber qui était le thème de notre Université à travers 5 questions : **[Q115]** « Évaluer la maturité, les questions essentielles », **[Q116]** « Évaluer la maturité, en contextualisant les questions », **[Q117]** « Tableau de bord de maturité », **[Q118]** « Indices de non-maturité » et la question **[Q119]** « Maturité du responsable cyber ». Ces questions ont fait l'objet d'ateliers durant l'université du CESIN. Les résultats et conclusions sont disponibles sur le site du CESIN[3].

Question **[Q115]** : les questionnaires de maturité sont nombreux, avec un certain recouvrement sur les questions posées d'un questionnaire à l'autre. Cependant, il y a encore eu peu ou pas de réflexion commune sur ce qui pourrait être un ensemble de critères permettant de contextualiser les réponses aux questions. Or les réponses à des questions sur la maturité d'une entreprise ne peuvent s'analyser de façon intrinsèque, il faut collecter un minimum d'éléments de contexte sur l'entreprise. Par exemple, sa taille, sa couverture géographique (pays, nombre de sites), la place de l'IT, la centralisation ou pas de son Système d'Information, la nature de ses métiers et des données clés à protéger (données R&D, données clients, etc.) sans compter la part de l'OT.

Qu'est ce qui tend à renforcer la maturité de son organisation ?

2 Uniquement accessible aux membres : https://cesin.fr/articles-slug/?slug=1951-Les+instantan%C3%A9s+du+CESIN+-+1er+semestre+2023
3 Uniquement accessible aux membres : https://cesin.fr/document.php?d=64f5cc5e46e86

Nous avons eu **116 répondants** à cette question :



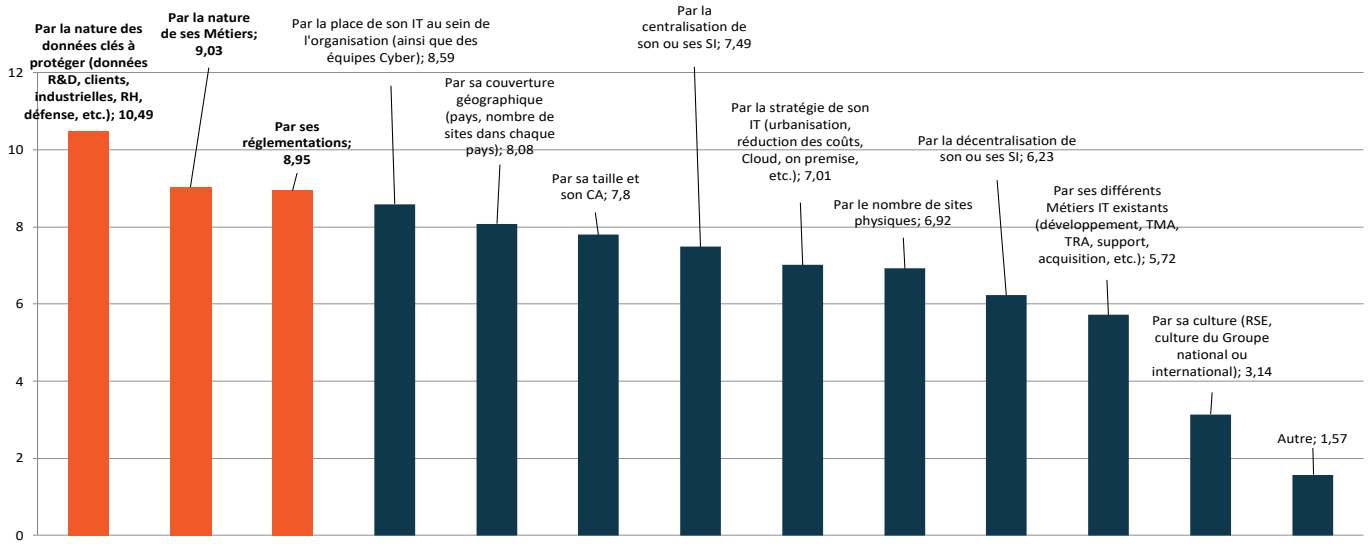
D'autres propositions parmi :

- élaborer une cartographie pour déployer de manière exhaustive mes processus Cyber ;
- assurer la sécurité de mes chaînes d'approvisionnement.

Question **[Q116]** : il existe de multiples questionnaires et référentiels pour évaluer la maturité d'une organisation. Ceux-ci rivalisent en nombre de questions, mais ces référentiels sont souvent des listes « à plat », sans qu'une pondération entre toutes ces questions permettent de discerner les éléments essentiels et de prendre du recul pour réellement estimer la maturité d'une entreprise en cybersécurité.

Quels sont les critères qui permettent de définir le contexte cyber de son organisation ?

74 membres ont répondu à ce sondage :



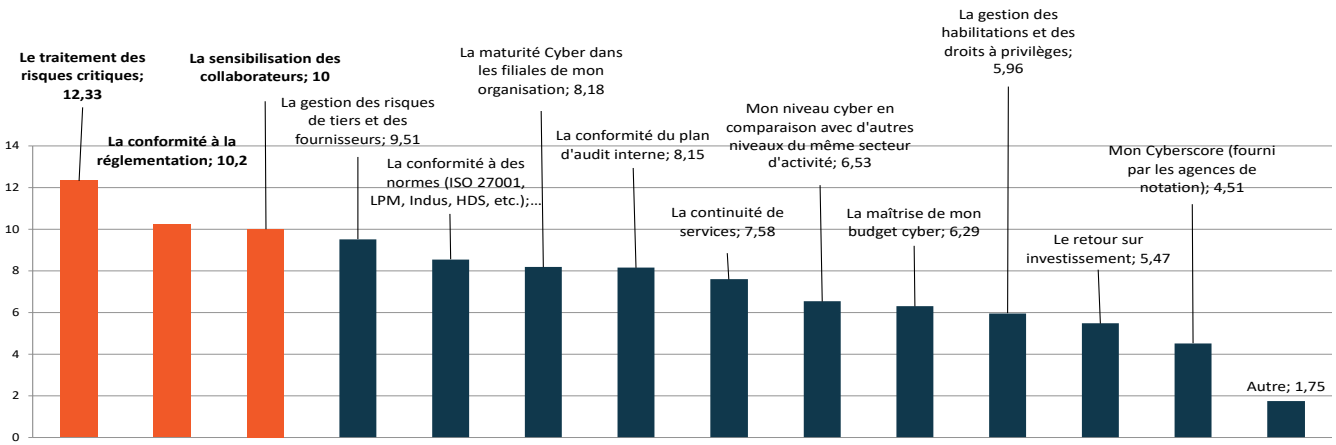
D’autres propositions parmi :

- par la dépendance de son business vis à vis de son IT/IS → Par ses différents Métiers IT existants (développement, TMA, TRA, support, acquisition, etc.) et leur place et dépendance vis à vis de l’IT ;
- par le pragmatisme de l'organisation (ITIL) → par la place de son IT au sein de l'organisation (ainsi que des équipes Cyber) et du pragmatisme de cette dernière ;
- par le fait d'avoir déjà été victime d'attaque(s) directe(s) ou indirecte(s).

Question **[Q117]** : il existe de nombreux tableaux de bord en cybersécurité, selon que l’on s’intéresse à la cybersécurité opérationnelle, la conformité, la performance, la gestion du risque cyber et la sinistralité ou encore la maturité. Ces tableaux de bord peuvent comporter, selon le cas, des données instantanées, des statistiques, des courbes de tendances, des benchmarks, des faits marquants, etc. Qu’est-ce qui constitue le tableau de bord sur la maturité d’une entreprise en cybersécurité, qu’un responsable cybersécurité devrait pouvoir présenter à son COMEX ? Ce n’est pas un tableau de bord que l’on présente fréquemment, et il faut pouvoir observer l’évolution de la maturité dans le temps avec une historisation de cette maturité.

Quelles sont les informations à fournir à présenter dans un tableau de bord stratégique à destination de son COMEX ?

92 membres ont répondu à cette question :



D’autres propositions parmi :

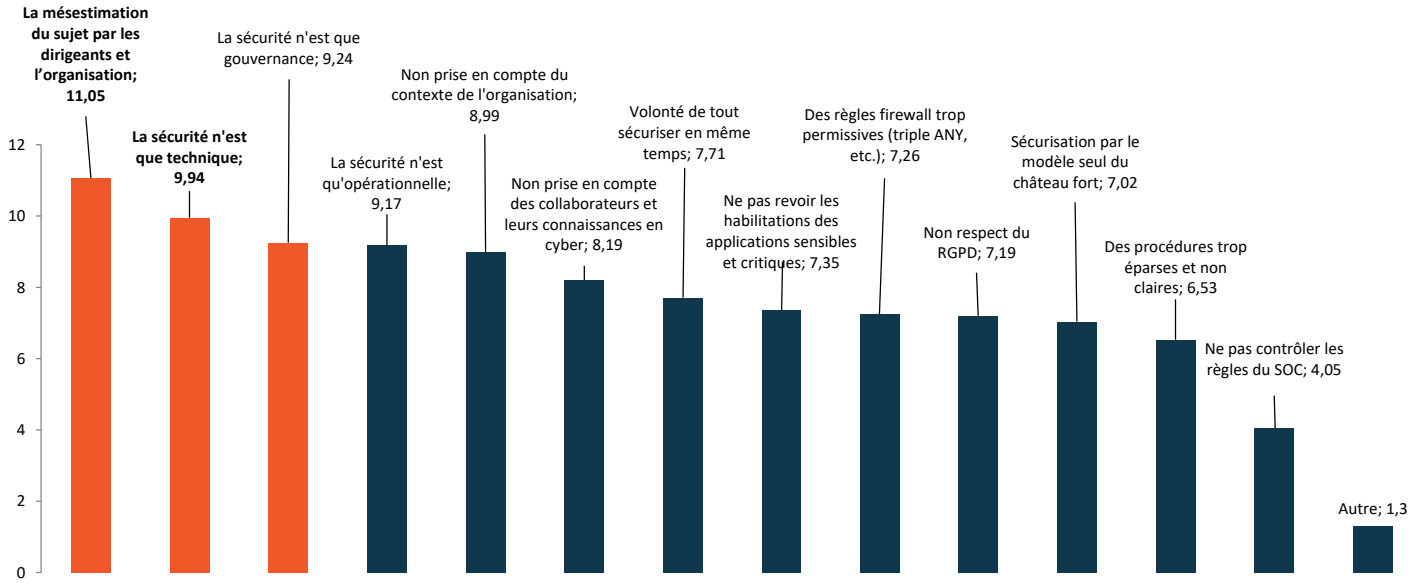
- la conformité au(x) référentiel(s) choisis par l’organisation (ISO 27001, LPM, Indus, HDS, etc.) ;
- le taux d’avancement de la feuille de route Cyber / du plan stratégique Cyber.

Question **[Q118]** : on a coutume d’évaluer la maturité en cybersécurité à travers ce que l’entreprise arrive à bien faire en matière de sécurité, les méthodes, processus et solutions déployées. Et si l’on

envisageait la question sous l'angle inverse ? Quelles sont les mauvaises pratiques encore persistantes dans l'entreprise et qui témoignent d'un défaut de maturité ?

Il s'agissait de demander l'avis de nos membres sur les mauvaises pratiques amenant à des non-conformité cyber.

93 ont répondu à cette question :



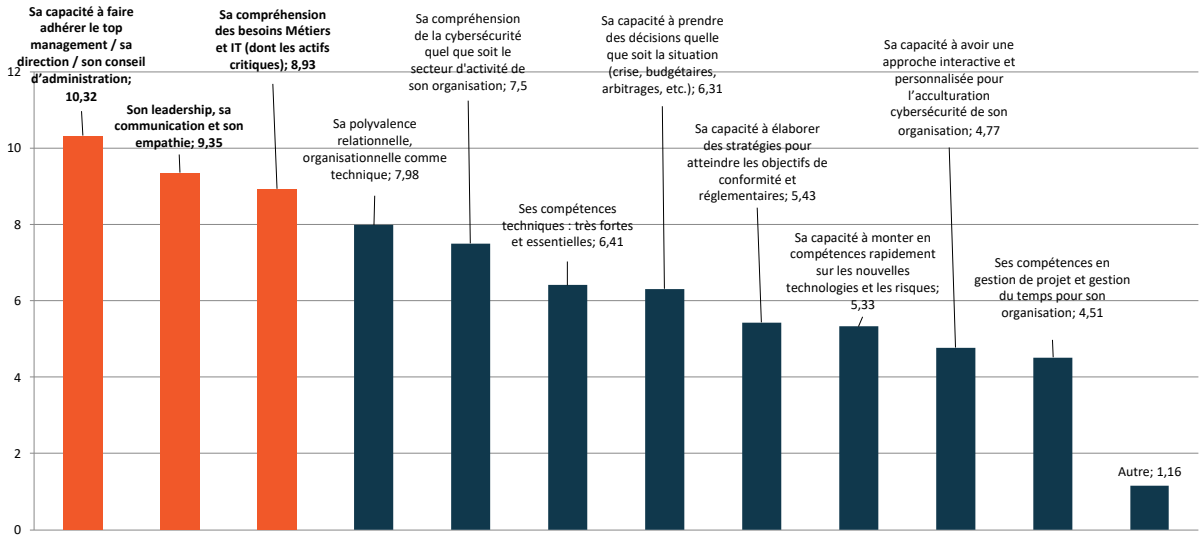
D'autres propositions parmi :

- la sous-estimation de la menace cyber et la méconnaissance / non prise en compte de nos vulnérabilités ;
- shadow IT (et la maturité d'une entreprise ne se définie pas par les solutions déployées. Les solutions déployées ne démontrent que la capacité financière d'une entreprise).

Question **[Q119]** : On peut considérer qu'une entreprise ne fait des progrès en cybersécurité que s'il y a vraiment des personnes compétentes en charge du sujet. Ce principe est vrai pour la cyber comme pour d'autres domaines, mais cette question est plus aigüe dans le domaine cyber qui est récent en termes de développement des ressources. Dans ce domaine pour lequel les besoins et le nombre de ressources sont en forte croissance, la façon de juger de la maturité du responsable cyber est encore peu discutée et encore moins formalisée. Il suffit, pour s'en convaincre, de comparer la diversité des critères attendus dans les différentes fiches de postes de responsables cyber. Comment peut-on juger de la maturité d'un responsable cyber ?

Nous vous avons demandé l'avis de nos membres sur ce qui définit un bon responsable Cyber.

123 ont répondu à cette question :



A été rajoutée la proposition de la capacité à gérer le stress, être résilient, s'adapter aux changements.

Les sujets innovants

L'intelligence artificielle

Depuis quelques années l'Intelligence Artificielle est devenue un sujet prometteur pour notre monde digitalisé. L'arrivée de ChatGPT a bousculé les agendas et beaucoup d'initiatives autour de l'IA se font jour. L'idée du sondage était de connaître le niveau de préoccupation **[Q122]** lié à ce sujet montant. **166** ont répondu à ce questionnaire.

Depuis sa sortie en novembre 2022, ChatGPT n'était alors que le dernier d'une vaste généalogie d'outils labellisés IA, capables d'aider voire de remplacer l'humain dans ses tâches. Comment ne pas penser à DeepBlue, champion d'échecs, ou à Aladdin qui gérait déjà en 2020, 21 600 000 000 de dollars ? Nous pourrions même mentionner l'idée de proto-IA déjà présente dans nos mythes et légendes. Mais ces derniers étaient jusqu'alors cantonnés à des milieux plus restreints de connaisseurs, chercheurs ou entreprises à gros budgets, etc. Il est désormais révolu le temps où le grand public ne voyait de l'IA que les expérimentations de Microsoft avec Tay (un chatbot sur Twitter qui a commencé à tenir des propos nazis en moins de 24 heures), ou celui des IA gérant notre monde depuis les coulisses (les recommandations d'achats, les réseaux sociaux, etc.).

Face à tout cela, **70%** de nos membres se sentent plutôt concernés : dont **37%** très concernés (avec de nombreuses initiatives dans les entreprises) et **33%** se sentent concernés avec quelques projets en discussion.

À l'intérieur de cette vague de fond, les entreprises qui n'étaient pas en lien avec l'IA ont commencé à muter pour devenir également des entreprises de l'IA (du moins dans une certaine mesure). Après tout, il est devenu difficile de ne pas résister à l'envie d'utiliser le chat pour effectuer toutes nos tâches rébarbatives (et ce, sans doute à raison).

Ainsi, pour près de **11%**, cette technologie n'est pas encore plébiscitée et enfin **18%** restent en mode veille, notamment sur l'IA pour la défense et pour les attaquants.

La question qui découle donc n'est pas tant de savoir si les entreprises sont prêtes, mais plutôt si elles ont commencé à inclure dans leur vision stratégique les mutations que va opérer l'IA dans les métiers. C'est du moins ce que semble corroborer une étude de Kaspersky citée par *Le Monde Numérique*, indiquant que 40% des 2 000 cadres de haut niveau interrogés prévoient d'utiliser des outils d'IA générative tels que ChatGPT afin de combler le manque de compétences critiques par l'automatisation des tâches dans les métiers de l'IT. La moitié d'entre eux prévoit également d'automatiser les tâches banales des travailleurs. Reste donc à savoir si ces mêmes interviewés possèdent l'instruction nécessaire pour comprendre les enjeux de sécurité liés aux données ; toujours selon cette même étude, seuls 22 % des cadres ont discuté de la mise en place de règles d'utilisation de ces mêmes outils.

Ce sujet innovant a fait l'objet de la thématique de fond du congrès du CESIN en décembre 2023. Les résultats d'atelier et conférences sont disponibles sur le site du CESIN pour les membres.

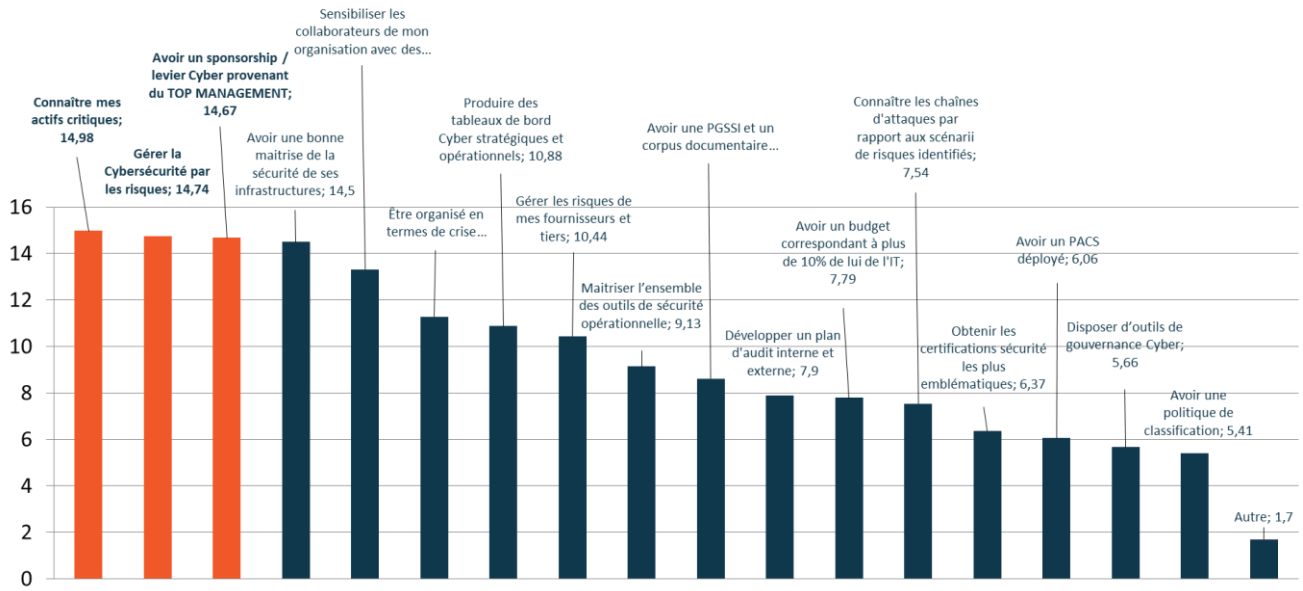
ANNEXES

QUESTION DE LA SEMAINE : DETAIL DES RESULTATS

[Q115] Évaluer la maturité, les questions essentielles

Les questionnaires de maturité sont nombreux, avec un certain recouvrement sur les questions posées d'un questionnaire à l'autre. Par contre, il y a encore eu peu ou pas de réflexion commune sur ce qui pourrait être un ensemble de critères permettant de contextualiser les réponses aux questions. Or les réponses à des questions sur la maturité d'une entreprise ne peuvent s'analyser de façon intrinsèque, il faut collecter un minimum d'éléments de contexte sur l'entreprise. Par exemple, sa taille, sa couverture géographique (pays, nombre de sites), la place de l'IT, la centralisation ou pas de son Système d'Information, la nature de ses métiers et des données clés à protéger (données R&D, données clients…), la part de l'OT, etc. Quels sont les 10 critères essentiels à mettre en parallèle des questions relatives à la maturité pour pouvoir réellement être en mesure de comprendre et de juger de la maturité d'une entreprise ?

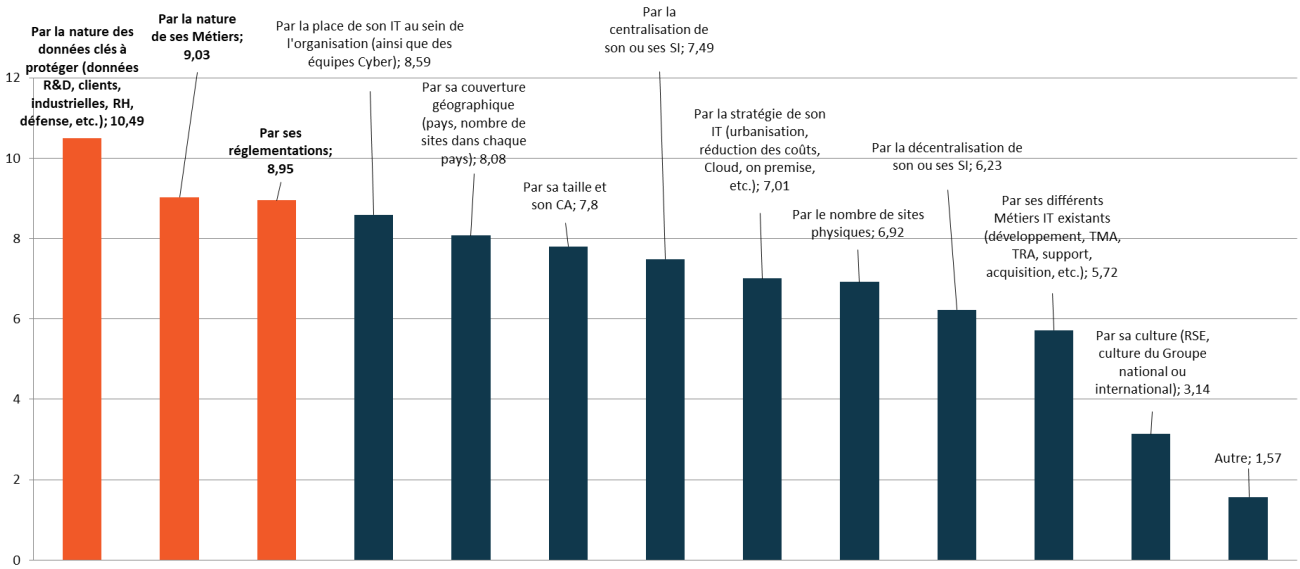
Qu'est ce qui tend à renforcer la maturité Cyber de mon organisation ? *(Classer les propositions par ordre de priorité pour vous)*



[Q116] Évaluer la maturité, en contextualisant les questions

Il existe de multiples questionnaires et référentiels pour évaluer la maturité d'une organisation. Ceux-ci rivalisent en nombre de questions, mais ces référentiels sont souvent des listes « à plat », sans qu'une pondération entre toutes ces questions permettent de discerner les éléments essentiels et de prendre du recul pour réellement estimer la maturité d'une entreprise en cybersécurité. Quelles seraient les 10 questions essentielles que vous jugez pertinentes et prioritaires de poser, pour pouvoir vous faire une bonne idée générale de la maturité d'une entreprise ?

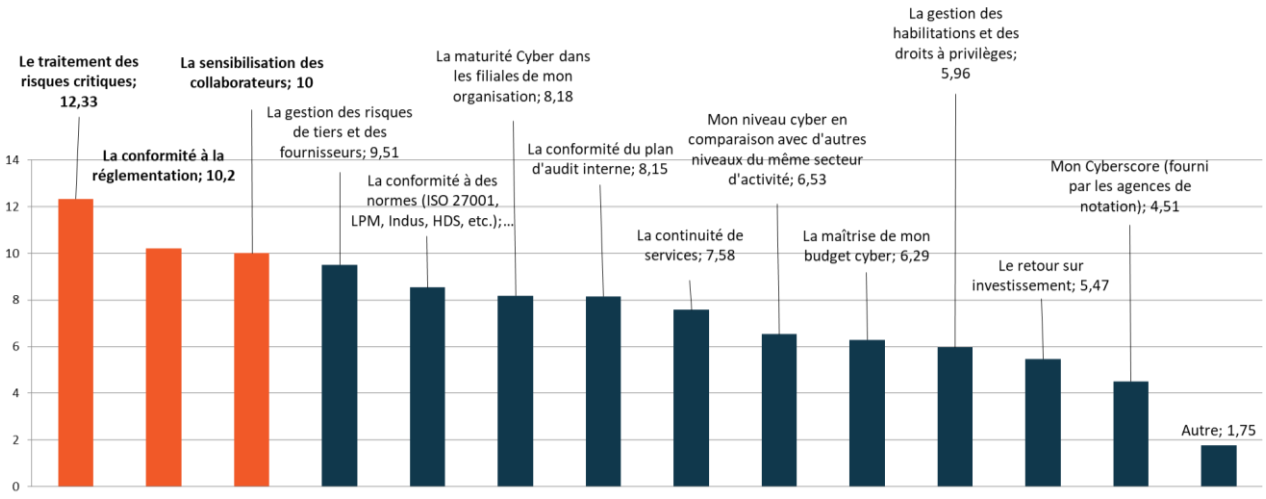
Quels sont les critères qui me permettront de définir le contexte Cyber au sein de mon organisation ? *(Classer les propositions par ordre de priorité pour vous)*



[Q117] Tableau de bord de maturité

Il existe de nombreux tableaux de bord en cybersécurité, selon que l'on s'intéresse à la cybersécurité opérationnelle, la conformité, la performance, la gestion du risque cyber et la sinistralité ou encore la maturité. Ces tableaux de bord peuvent comporter, selon le cas, des données instantanées, des statistiques, des courbes de tendances, des benchmarks, des faits marquants, etc. Qu'est-ce qui constitue pour vous le tableau de bord sur la maturité d'une entreprise en cybersécurité, qu'un responsable cybersécurité devrait pouvoir présenter à son COMEX ? Ce n'est pas un tableau de bord que l'on présente fréquemment, et il faut pouvoir observer l'évolution de la maturité dans le temps avec une historisation de cette maturité. Quels sont les 10 indicateurs ou informations à présenter au COMEX pour un tableau de bord de maturité ?

Quelles sont les informations à présenter dans un tableau de bord stratégique à son COMEX ? ***(Classer les propositions par ordre de priorité pour vous)***

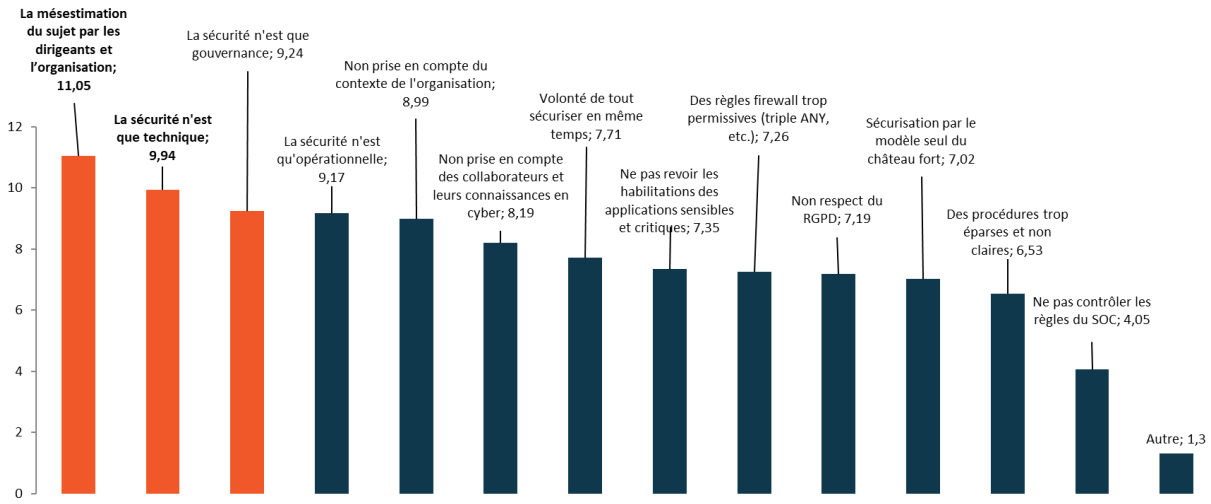


[Q118] Indices de non maturité

On a coutume d'évaluer la maturité en cybersécurité à travers ce que l'entreprise arrive à bien faire en matière de sécurité, les méthodes, processus et solutions déployées. Et si l'on envisageait la question sous l'angle inverse ? Quelles sont les mauvaises pratiques encore persistantes dans l'entreprise et qui témoignent d'un défaut de maturité ? Comment les identifier et les traquer ? Quels sont les pires cailloux dans la chaussure qui freinent la montée en maturité ?

Quelles sont les 10 indices techniques à chercher dans les pratiques effectives, montrant un non-respect de certains fondamentaux de sécurité, et qui permettaient d'observer et de mesurer le niveau de maturité sous un autre angle ?

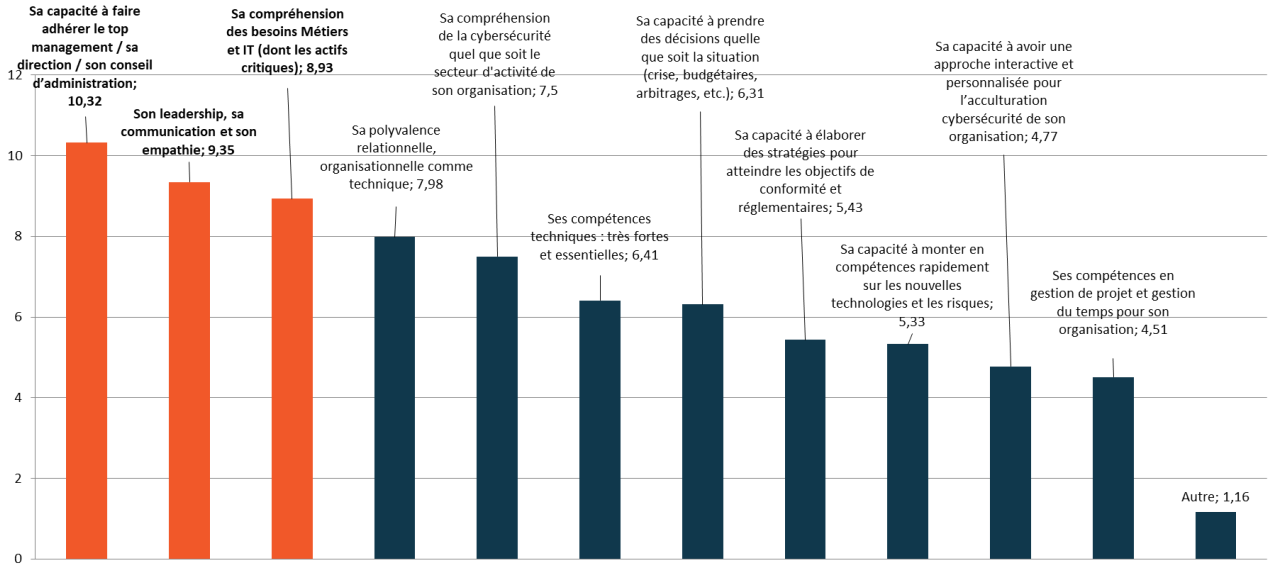
Quelles sont les mauvaises pratiques amenant à des non-conformité cyber ? *(Classer les propositions par ordre de priorité pour vous)*



[Q119] Maturité du responsable cyber

On peut considérer qu'une entreprise ne fait des progrès en cybersécurité que s'il y a vraiment des personnes compétentes en charge du sujet. Ce principe est vrai pour la cyber comme pour d'autres domaines, mais cette question est plus aigüe dans le domaine cyber qui est récent en termes de développement des ressources. Dans ce domaine pour lequel les besoins et le nombre de ressources sont en forte croissance, la façon de juger de la maturité du responsable cyber est encore peu discutée et encore moins formalisée. Il suffit, pour s'en convaincre, de comparer la diversité des critères attendus dans les différentes fiches de postes de responsables cyber. Comment peut-on juger de la maturité d'un responsable cyber ? Quels sont les 10 critères relatifs à la fois aux softs skills mais aussi à la posture et à l'action du responsable cybersécurité, qui permettraient d'estimer le niveau de maturité de ce responsable cyber dans l'exercice de sa mission ?

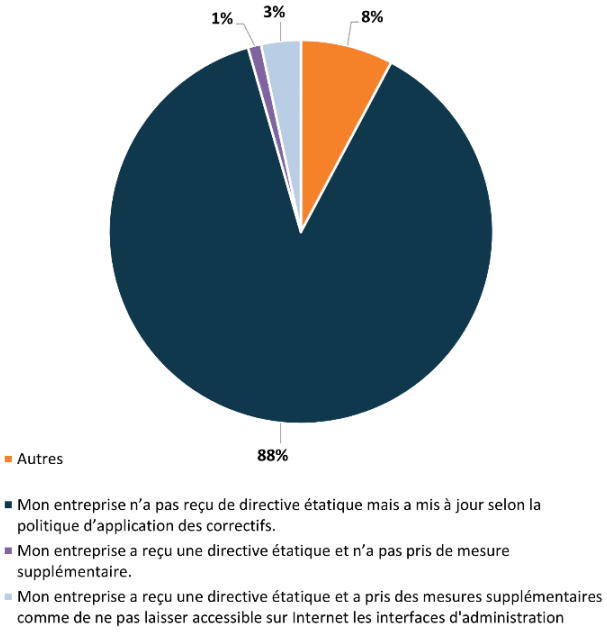
Qu'est ce qui définit un bon responsable cyber ? *(Classer les propositions par ordre de priorité pour vous)*

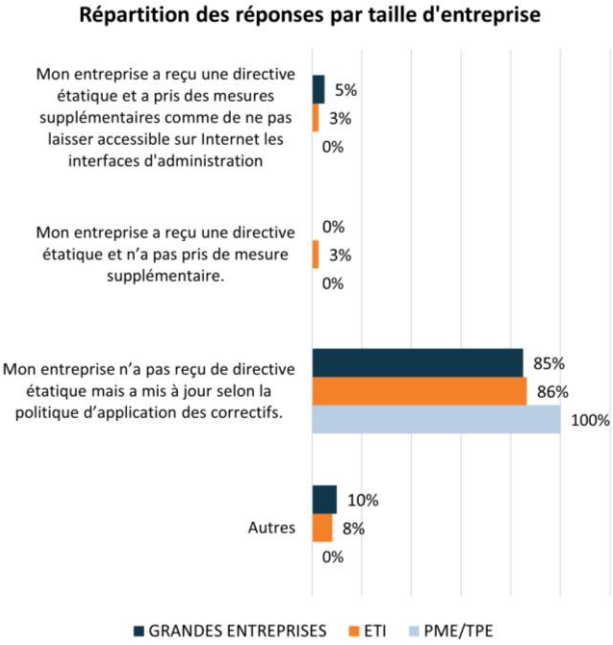


[Q121] Firewalls Fortinet

Les services de sécurité de l'État néerlandais ont émis des alertes du plus haut niveau vers leurs opérateurs essentiels concernant le danger que représentent les vulnérabilités très fréquentes sur Fortinet fort iOS forti VPN… L'origine de la menace serait géopolitique.

Pour celles et ceux qui utilisent des firewalls Fortinet avez-vous pris des mesures particulières suite à des alertes similaires reçues ?

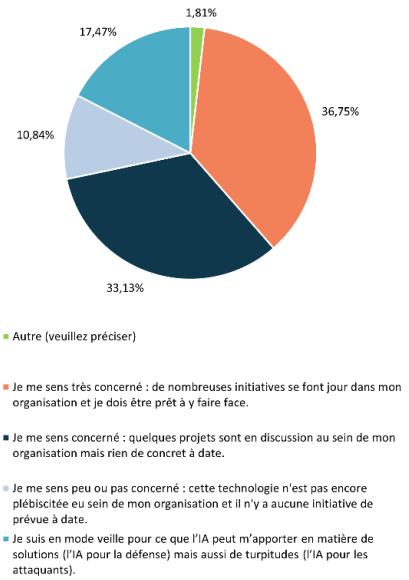


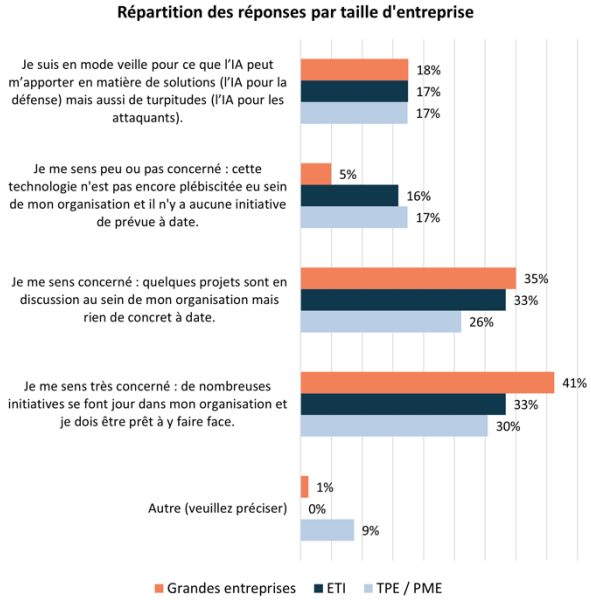


[Q122] Intelligence artificielle

Depuis maintenant quelques années l'Intelligence Artificielle est redevenue un sujet prometteur pour notre monde de plus en plus digitalisé. L'arrivée de ChatGPT a bousculé nos agendas et beaucoup d'initiatives autour de l'IA se font jour.

Quelle est votre niveau de préoccupation Cybersécurité du moment à ce sujet ?





[Q123] BYOD

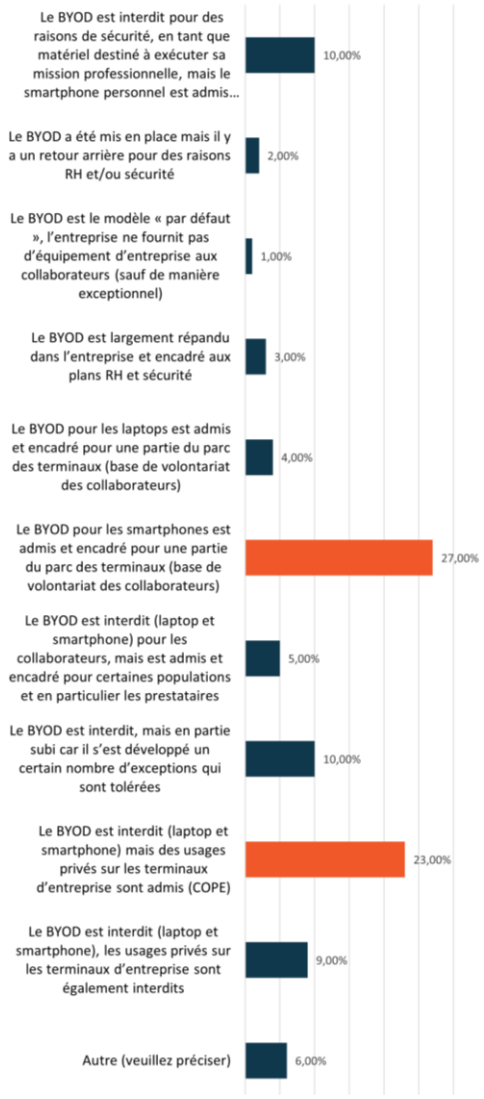
À la lumière des enjeux Numérique Responsable, puisque les équipements utilisateurs représentent près de 80% de l'empreinte carbone numérique (source : ADEME/ARCEP) due en grande majorité à la fabrication de ces équipements, le débat éternel autour du BYOD refait son apparition dans certaines organisations.

Les détracteurs du BYOD font valoir que, depuis ces 3 ou 4 dernières années, les postes ne disposant pas des protections de sécurité minimum, notamment les EDR, ont été des sérieux vecteurs d'entrée des attaques et que les efforts consentis pour protéger le parc des endpoints corporate sont ruinés si par ailleurs des laptops non correctement protégés peuvent se connecter sur les réseaux de l'entreprise.

La propriété des terminaux (laptops et smartphones) ne fait donc toujours pas consensus, les stratégies combinent ou oscillent entre le BYOD (Bring Your Own Device), le COPE (Company Owned, Personally Enabled) et le COBO (Company Owned Business Only).

Nous vous avions questionné en 2019 sur le sujet, mais depuis ce sondage, la situation a probablement évolué.

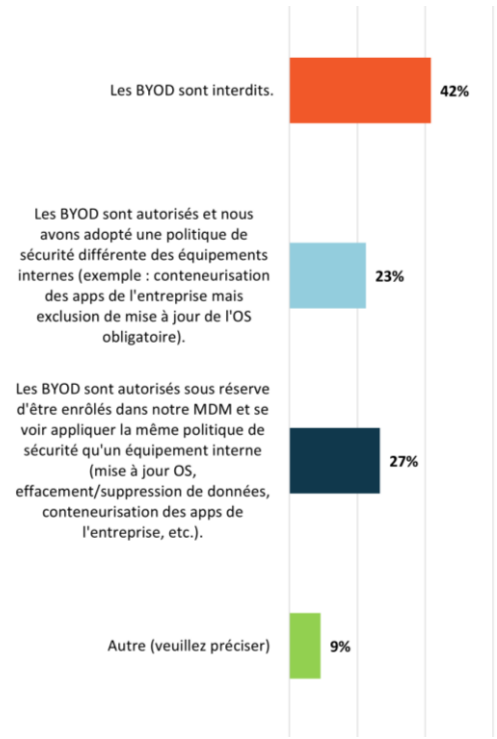
Actuellement, quelle est la stratégie adoptée dans votre organisation ?

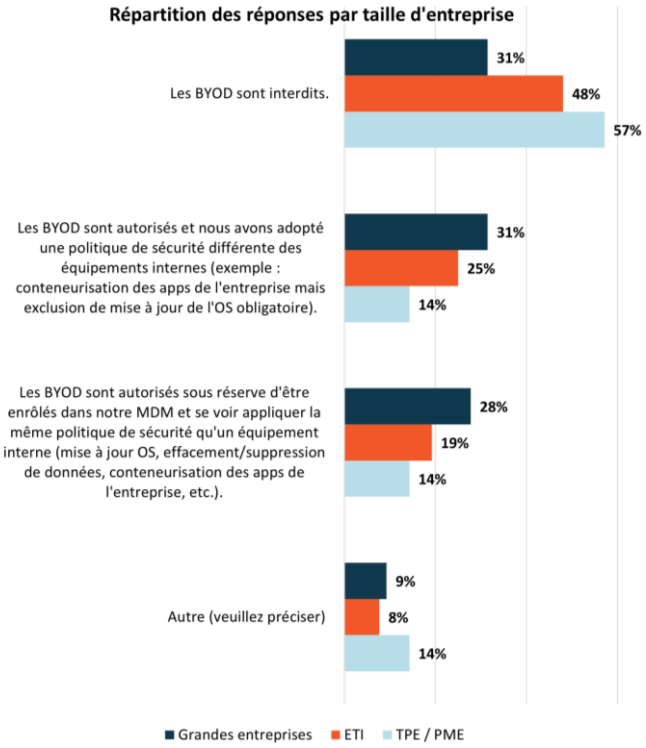


[Q125] MDM

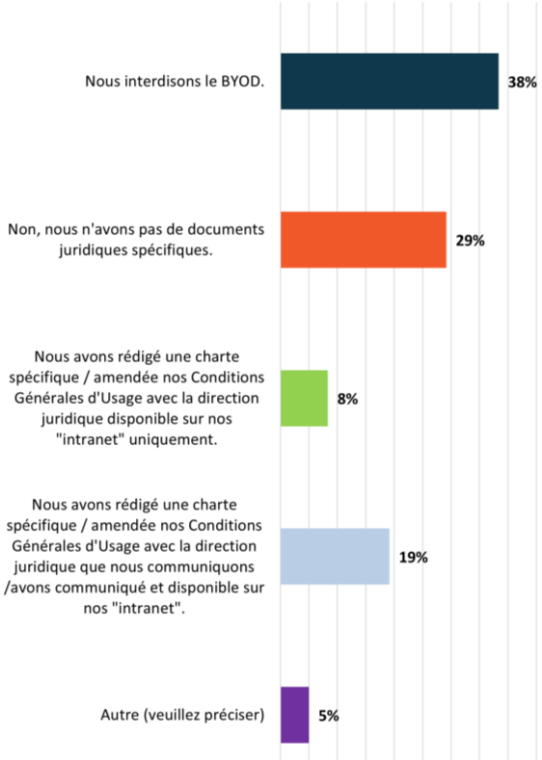
Dans le prolongement de notre question n°123 sur le BYOD, nous voulions vous interroger aujourd'hui sur son impact sur le MDM.

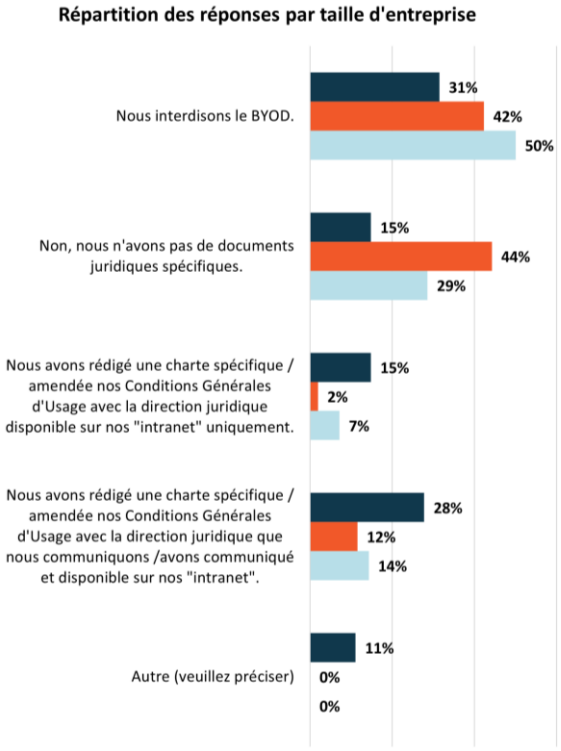
Quelle stratégie cybersécurité de votre EMM/MDM avez-vous mis en œuvre pour les équipements BYOD ?





S'agissant de l'enrôlement des terminaux BYOD à votre solution EMM/MDM, avez-vous mis en œuvre des dispositions juridiques particulières ?





[Q126] Self-Reset

La gestion des oublis de mot de passe par les utilisateurs représente un nombre conséquent d'appels aux services desk de vos entreprises, pour ceux qui ont conservé un processus humain de reset. Les difficultés liées à l'authentification de l'appelant afin de vérifier si la demande est légitime restent prégnantes. Le besoin de réinitialiser un mot de passe en cas d'oubli est réel mais nous savons aussi que de nombreux nouveaux cas d'attaques utilisent ce processus de reset de mot de passe pour obtenir des comptes valides d'accès au SI. Ce processus doit donc être solide qu'il soit humain ou automatique, pour éviter des attaques soit techniques soit d'ingénierie sociale, en encore hybrides.

Nous essayons, dans tous les périmètres du SI de forcer une authentification à double facteur pour confirmer des identités. Il ne serait pas cohérent de permettre des self-reset de mots de passe sur la base de la fourniture d'un seul facteur.

La solution de la question secrète reste perfectible. Parfois les réponses sont aisément devinables par un attaquant, parfois les questions sont trop complexes et l'utilisateur lui-même ne se souvient plus de la réponse. Et la méthode se heurte souvent à des problèmes de confidentialité sur le stockage des réponses quand ce ne sont pas des sujets CNIL par rapport aux données utilisées.

Le renvoi du mot de passe sur une messagerie personnelle se heurte au problème du refus potentiel de l'utilisateur de communiquer une adresse mail perso.

Donc quelques embûches techniques, organisationnelles ou légales sur ce sujet.

Et vous, quelle stratégie de sel-reset password avez-vous mis en place dans vos entreprises ?

Plus aller plus loin…

Question 122 : « Intelligence Artificielle »

L'Intelligence Artificielle est au cœur de l'actualité et pas seulement sur le plan cyber. Le comité programme du congrès du CESIN ne pouvait pas passer à côté d'un sujet aussi vaste et riche dont les enjeux de sécurité restent toujours un défi de taille.

Les deux journées du Congrès ont été rythmées par des temps d'échanges, de réflexion, de partage et de travail autour de la thématique "La cyberdéfense à la vitesse de l'IA".

La conférence d'ouverture par Françoise SOULIE, Conseiller scientifique (Hub France IA) a donné le la à l'événement annuel du CESIN. Après avoir introduit et définit l'IA, elle a livré sa vision sur un sujet qui va au-delà de la technologie elle-même, mettant ainsi en relief la croissance exponentielle des données et la sécurité à appliquer.

L'IA générative introduit ainsi de nouveaux risques pour les organisations - car elle est aussi au service des attaquants - mais est une vraie opportunité pour nous, professionnels de la Cybersécurité en matière de détection, de protection des actifs numériques, de réaction face aux incidents et de connaissance sur les schémas d'attaques. C'est autour de ces constats qu'ont suivi les autres conférences animées par des intervenants de haut niveau : de la protection des données personnelles et l'IA en passant par les compétences humaines au service de l'IA, ses impacts sur les RH et enfin notre propre place en tant que RSSI pour la gouverner.

Pour compléter les conférences, huit ateliers ont été co-animés par des duos RSSI et partenaires : nous avons pu collectivement réfléchir et restituer autour d'une thématique centrale basée sur l'automatisation grâce à l'IA. Les ateliers ont donc permis d'aborder des sujets de filière RH avec l'IA, des nouvelles démarches possibles en matière d'analyse de risques (et les risques !) avec l'IA, de l'utilisation de l'IA dans les stratégies de détection et de réponse, de la conformité et de la confiance que nous pourrions avoir envers l'IA ainsi que l'encadrement nécessaire à ce sujet au sein de nos organisations.

La Cybersécurité ne devrait pas être le domaine le plus touché par « le grand remplacement » des experts par des IA. Les recours à l'IA par les Métiers sont déjà là et vont se multiplier. Il va falloir se doter de compétences pour sécuriser le recours à l'IA mais aussi pour aider les autres équipes (juridique, achat, etc.) à saisir les subtilités l'IA. Cela va donc mettre en avant le rôle crucial des ressources humaines au sein des organisations.

Les membres du CESIN se sont interrogés sur les données nécessaires à fournir dans le cadre des analyses de risques avec l'IA, ce qui amène à une réflexion sur les données partageables à une IA et la fiabilité des résultats d'analyse.

Toujours dans les risques, il est difficile à ce stade d'avoir des avis définitifs dans un contexte de faible maturité des technologies, des utilisateurs et de l'écosystème Cyber. A cet effet, les premiers risques

envisagés sont : la fuite de données (nouveau canal pour un risque déjà connu) et la déviation/perte de contrôle des modèles (plus spécifique à l'IA).

Les participants ont souligné la capacité de l'IA à transformer la détection des incidents, la réponse aux menaces cyber en contribuant à réduire les faux positifs, à améliorer la détection comportementale, à prioriser sur les actions de remédiation et contextualisation le SI de l'organisation vis-à-vis de la menace.

Cependant, les membres ont également mis en avant la capacité des données à être (bien) exploitées par l'IA et des inquiétudes subsistent d'un point de vue de la consolidation des alertes et des coûts associés à certaines approches :

- coût de la mise en place de d'une solution (humain et machine) ;
- coût supplémentaire en infrastructure (datalake)
- accès aux compétences disponibles dans (et en dehors) de l'organisation ;
- structure des données impossible à qualifier et/ou quantifier ;
- qualité et confidentialité des données.

Ces problématiques nécessitent donc le développement de datalake dédiés à la cybersécurité et l'implication de champions associés à divers experts pour favoriser l'exploitation efficace des données.

La confiance dans l'IA, en particulier dans le contexte des IA génératives, est au centre des préoccupation et la montée en compétences sur ces domaines est nécessaire. Il est recommandé de monitorer et de s'approprier les outils qui permettent de challenger les algorithmes des IA.

Au-delà de la confiance, les membres recommandent la mise en œuvre des actions suivantes :

- d'un point de vue organisationnel, la création d'un guide de bonnes pratiques liées à l'usage le l'IA et la veille continue ;
- d'un point de vue juridique, établir une charte structurée, une PSSI incluant l'IA, intégrer des clauses contractuelles basées sur des normes et règlementations locales et définir les rôles et responsabilités de chaque utilisateur ;
- d'un point de vue technique, établir une liste de fournisseurs d'IA voire une labélisation, établir une liste de prompts « éthiques » et sécuriser son code applicatif.

Malgré les perspectives prometteuses plusieurs challenges sont identifiés :

- mettre en œuvre de vision stratégique de l'IA (gouvernance) appliquée à la cyber en accompagnant l'usage en le mesurant et sensibilisant les acteurs ;
- cibler les processus métiers maitrisés pour commencer par la zone de confiance, décliner sur la capacité de détection / triage
- changer de posture (*a priori*) en adoptant l'IA plutôt que la bloquer : accepter la prise de risque des usages de l'IA en les évaluant et les traitant ;
- se prémunir des dérives en positionnant des responsables concernant les usages / mé-usages de l'IA en s'appuyant sur les retours d'expérience de la "cloudification" des SI.

L'IA est un bénéfice qui induit des risques sous-jacents, il faut surfer sur la vague plutôt que la subir.

Les conclusions de ces ateliers ouvrent à de nombreuses réflexions qui vont s'articuler autour de nos prochaines paroles d'experts, sessions plénières, lab et abordées en communautés du CESIN.

Il est encore sans doute trop tôt pour savoir comment les entreprises vont réagir face à une technologie qui cumule tous les signes d'une disruption. Pour *strategie.gouv*, la technologie risque bien de se substituer au travail humain pour le faire disparaître, ou tout du moins le raréfier. Avec moins de fatalisme, *ITS IBELEM* souligne que le moment est sans doute à la prospection, un travail devant être fait pour anticiper et accompagner les organisations à prévoir leurs besoins futurs dans le domaine. Concrètement, en réfléchissant à la complexité des tâches, le risque d'erreur acceptable par l'IA et le degré d'interdépendance des tâches ou métiers au sein d'une organisation, on pourrait prédire, jusqu'à une certaine mesure, les tâches pouvant être automatisées par l'IA. Il semblerait donc qu'il n'y ait pas à avoir de fatalisme, mais des choix et des orientations stratégiques portés par les dirigeants d'organisations, avec des contextes spécifiques (économiques, sociaux, technologiques, démographiques, etc.).

Il est à noter que les entreprises utilisant l'IA constatent une amélioration des performances des salariés, une réduction des risques d'erreurs, mais seulement 40 % ont vu une diminution des coûts de main-d'œuvre. L'IA a également amélioré la relation client, surtout dans la finance et le commerce. Le coût d'investissement reste le principal frein à son déploiement, suivi du manque d'expertise en interne et des problèmes de compatibilité avec les outils existants.

Pour les établissements non-utilisateurs, près de 80 % estiment que leur activité n'est pas compatible avec cette technologie, et les freins incluent le manque de connaissance et de compétences, ainsi que le manque de temps pour s'y intéresser.

Question 124 : « BYOD »

Comment déterminer sa politique d'actifs ?

Si l'on évoque le cas extrême du laissez-faire, l'organisation laisse ses employés gérer eux-mêmes leurs outils. On part alors du postulat que l'individu va de manière autonome s'assurer de mettre en place tous les moyens à sa disposition pour se prémunir des risques cyber, une hypothèse peu probable au vu de la proportion élevée d'attaques exploitant le facteur humain. Soit l'on décide que la sécurité est secondaire à l'activité professionnelle, un paradigme difficile à assumer.

Si l'on met de côté le cas détaillé plus haut, il reste à faire un choix éclairé quant à la méthode de gestion des actifs à adopter au sein de l'organisation. Considérons d'abord la Bring Your Own Device (BYOD), qui semble initialement offrir plusieurs avantages : permettre à l'utilisateur de choisir son outil de travail sans contrainte imposée par l'employeur. En laissant l'utilisateur utiliser l'outil de son choix, on espère obtenir un travail plus productif, tout en déportant sur lui le coût et le temps de la maintenance et de la gestion. Cette méthode n'exclut toutefois pas l'employeur d'utiliser des outils de gestion (par exemple, MDM, séparation logique des profils, etc.) pour réguler certains usages de l'outil dans le cadre professionnel. Au contraire, elle assouplit la charge de travail du côté du business.

Si nous devions faire une analogie, ce serait comme si l'utilisateur était laissé dans un vaste jardin clos par un mur. Cependant, ce jardin est si étendu et son entretien si important qu'il accumule de nombreuses problématiques :

- une non-uniformité entre les Systèmes Opérateurs (SO), avec leurs lots de complications que cela entraîne ;
- des outils essentiels, voir critiques qui ne fonctionnerait pas sur telle ou telle machine ;

- un entretien plus difficile car étant fait au cas par cas ;
- une protection des données plus complexe ;
- des mises à jour plus inégales ;
- l'intégration à l'écosystème de l'organisation plus ardue ;
- un manque potentiel de dissociation des données professionnelles et personnelles.

À l'opposé de la politique Company Owned Business Only (COBO) où l'organisation fournit l'outil à l'employé qu'elle aura elle-même choisi, et dont l'utilisation est exclusivement professionnelle, la COBO permet au décideur de résoudre les points de friction détaillés précédemment. Cela contraste avec la politique BYOD qui semble être en adéquation avec notre époque.

Reprenons l'analogie du jardin : c'est comme si l'on avait réduit la taille des plantes pour renforcer le mur. Cette méthode nécessiterait en effet un investissement initial plus important, représentant un coût significatif pour l'entreprise. Elle nécessiterait également une décision concernant une politique de gestion des actifs. De plus, les employés pourraient être réticents à l'idée que leur employeur contrôle leurs machines ou se sentir lésés si leurs outils ne répondent pas à leurs besoins.

Mais l'on pourrait également argumenter que passé l'effort initial, la politique se traduise en un gain de temps et d'argent car :

- les procédures et documentations sont uniques et ne souffrent plus d'un ou plusieurs régimes d'exception ;
- si elles sont appliquées correctement, l'uniformité permet l'application de correctifs valables pour tous ;
- le contrôle granulaire est renforcé ;
- l'exécution devient plus facile, car elle est plus aisément prédictible ;
- la transmission du savoir s'en trouve largement facilitée.

Nous nous retrouvons donc avec un système plus lourd et une inertie plus forte, mais dont la robustesse est renforcée, car il permet de pallier plus aisément les défectuosités énumérées précédemment.

On pourrait mentionner d'autres politiques telles que le Corporate Owned Personally Enabled. Cette fois, l'outil est fourni par l'organisation et les utilisateurs sont autorisés à l'utiliser pour des activités personnelles. Ou encore le Choose Your Own Device. Cette fois, l'organisation propose une sélection d'outils parmi laquelle l'employé peut choisir son outil. On comprend très vite que ces dernières déclinent les principes des deux premières politiques et les réadaptent avec plus ou moins de fidélité.

En somme, la question de la gestion des actifs résume l'éternel débat entre la sécurité et l'usage. Soit on laisse libre cours en misant sur des gains de temps, d'argent et de productivité (bien que ce soit à modérer, car la frontière entre vie professionnelle et personnelle devenant plus floue, une nouvelle forme de stress apparaît), ce qui va inévitablement impacter la sécurité. Soit la sécurité devient un point de stress pour l'organisation, troquant la flexibilité contre une sécurité renforcée, mais nécessitant un effort initial plus conséquent.

Conclusion

Il est dès lors compliqué de privilégier telle ou telle solution. Un cadre trop contraignant peut avoir des répercussions sur le business, tandis qu'un laxisme trop important peut entraîner son lot de déconvenues. Il convient de noter que si les politiques de gestion des actifs abordent généralement les ordinateurs de manière globale, peu d'attention est portée sur les outils personnels tels que les téléphones et les tablettes, qui représentent autant de vecteurs d'attaques potentiels. On peut

toujours utiliser un VPN ou une connexion chiffrée lorsqu'ils se connectent au Wifi de l'organisation, mettre en place des solutions d'EDR avancé, de container professionnels ou interdire toute information professionnelle sur ces appareils, mais ce ne sont que des palliatifs. Tout comme pour les ordinateurs, il est essentiel de se pencher également sur ces équipements.

Question 125 : « Politiques MDM »

La difficulté de l'implémentation du BYOD

L'introduction du BYOD soulève des questions complexes, et l'utilisation d'outils personnels au travail dépend souvent des politiques spécifiques de chaque entreprise. Les avantages financiers et stratégiques du BYOD, tels que l'amélioration potentielle de l'efficacité des collaborateurs, sont contrebalancés par les risques liés à la sécurité des données. L'employeur demeure responsable de la protection des données, même sur des appareils qu'il ne contrôle pas physiquement. Une tendance émerge clairement : la nécessité croissante de mettre en place des solutions de MDM pour équilibrer productivité et sécurité dans sa gestion de son parc informatique. Les entreprises doivent faire face à des défis tels que la résistance des employés à l'adoption de politiques plus strictes, tout en cherchant un équilibre entre la liberté des utilisateurs et la sécurité des données.

Les risques et les solutions

Les risques associés au BYOD, tels que les atteintes à la disponibilité, à l'intégrité et à la confidentialité des données, nécessitent une identification minutieuse et des mesures spécifiques formalisées dans une politique de sécurité. La mise en place de politiques MDM permet d'atténuer ces risques en imposant des standards de sécurité équivalents à ceux des équipements internes.

Les avantages d'un MDM

L'implémentation d'un Mobile Device Management (MDM) au sein d'une entreprise offre plusieurs avantages, notamment :

- une sécurité renforcée : le MDM permet de mettre en place des politiques de sécurité strictes pour diverses appareils mobiles, garantissant la protection des données de l'entreprise ;
- le contrôle des politiques : les administrateurs peuvent définir et appliquer des politiques de sécurité, d'utilisation et de conformité sur différents appareils, assurant une gestion centralisée ;
- la gestion des applications : les administrateurs peuvent gérer et distribuer des applications de manière centralisée, facilitant les mises à jour, les installations et les suppressions d'applications sur les appareils mobiles ;
- le contrôle d'accès aux ressources : le MDM permet de restreindre l'accès aux ressources de l'entreprise, garantissant que seuls les appareils enregistrés et conformes aux politiques de sécurité y ont accès ;
- la sécurité des données en cas de perte ou de vol : les fonctionnalités de verrouillage à distance, de localisation et d'effacement des données aident à protéger les informations sensibles en cas de perte ou de vol d'un appareil ;
- la gestion des configurations : les administrateurs peuvent gérer les configurations des appareils, y compris les paramètres Wi-Fi, VPN et autres, assurant une uniformité et une conformité au sein de la flotte mobile ;

- l’économie de temps et d'efforts : la gestion centralisée des appareils mobiles via le MDM réduit la charge administrative, permettant aux équipes informatiques de consacrer moins de temps à la résolution de problèmes individuels ;
- le support à distance : les fonctionnalités de support à distance facilitent le dépannage et la résolution des problèmes techniques sur les appareils mobiles sans nécessiter une présence physique ;
- l’optimisation des coûts : en gérant efficacement la flotte mobile, le MDM contribue à optimiser les coûts liés à l'achat d'équipements, à la gestion des licences logicielles et à la maintenance des appareils.

Question 126 : « Self reset »

Risques associés au self-reset

Les attaques exploitant les processus de reset de mot de passe pour accéder illicitement aux systèmes d'information sont en augmentation. Les failles techniques dans les systèmes de self-reset peuvent compromettre la sécurité, mettant en danger la confidentialité des données.

Les attaques basées sur l'ingénierie sociale constituent une menace croissante. Les informations nécessaires au self-reset peuvent souvent être obtenues via des manipulations habiles, soulignant la nécessité d'une validation rigoureuse de l'identité.

Les solutions actuelles et leurs limitations

Le MFA est une mesure efficace pour renforcer la sécurité. Cependant, autoriser le self-reset basé sur un seul facteur contredirait cette approche, créant une incohérence dans la politique de sécurité.

Bien que largement utilisée, la méthode des questions secrètes présente des failles. Les réponses peuvent être devinées par des attaquants, et la complexité des questions peut entraîner des oublis de la part des utilisateurs. De plus, des problèmes de confidentialité et de conformité CNIL peuvent survenir.

L'envoi du mot de passe sur une messagerie personnelle peut être refusé par les utilisateurs, introduisant un obstacle supplémentaire. De plus, cela soulève des préoccupations quant à la sécurité de la communication et du stockage des mots de passe.

Perspectives d'amélioration

L'intégration de méthodes d'authentification biométrique et multifacteur renforce la sécurité du self-reset. Ces technologies offrent une validation plus robuste de l'identité de l'utilisateur, réduisant ainsi les risques liés aux attaques.

Les logiciels de réinitialisation des mots de passe (SSPR) simplifient la gestion des mots de passe des utilisateurs finaux en leur offrant un outil en libre-service. Les solutions SSPR d'entreprise aident également à mettre en œuvre des politiques de sécurité des informations d'identification solides au sein d’une organisation afin de réduire les brèches résultant de mauvaises pratiques en matière de mots de passe.

Le développement de politiques de confidentialité strictes pour le stockage et la gestion des réponses aux questions secrètes est essentiel. Cela garantit la protection des données personnelles et la conformité aux réglementations, y compris celles de la CNIL.

Informer les utilisateurs sur les risques associés aux oublis de mots de passe et sur les mesures de sécurité mises en place peut contribuer à une meilleure compréhension et à une utilisation responsable des processus de self-reset.

Réduire l'usage des mots de passes

L'adoption de solutions telles que le Single Sign-On (SSO) et le Passwordless représente une avancée significative dans la gestion des identités et des accès.

Le SSO permet aux utilisateurs de se connecter une seule fois pour accéder à l'ensemble des applications et services. En intégrant le SSO, les entreprises simplifient l'expérience utilisateur tout en renforçant la sécurité. Les employés bénéficient d'un accès transparent, réduisant ainsi le besoin fréquent d'usage variés de mots de passe. Cette approche contribue à une gestion centralisée et sécurisée des identités.

Le Passwordless Authentication élimine la dépendance aux mots de passe traditionnels, réduisant ainsi les risques associés aux self-resets. Que ce soit par le biais de méthodes biométriques, d'authentification par code ou d'autres technologies innovantes, le Passwordless offre une alternative sûre et efficace. Cette approche, en plus de renforcer la sécurité, améliore l'expérience utilisateur en éliminant la nécessité de mémoriser des mots de passe complexes.

Conclusion

La gestion des self-resets de mots de passe représente un équilibre délicat entre la nécessité d'assurer la sécurité et de fournir une expérience utilisateur sans friction. En abordant les défis techniques, organisationnels et légaux, les entreprises peuvent mettre en place des solutions robustes qui protègent les systèmes d'information tout en préservant la confidentialité des utilisateurs.