CESIN : Les instantanés 2022

Le CESIN a mis en place depuis l'automne 2019, un dispositif d'enquête régulier, appelé « la question de la semaine ». Ces enquêtes flash permettent, en 2 à 3 clics de recueillir la position des membres sur un point précis, qu'il concerne leurs démarches de cybersécurité, un point d'actualité, une tendance ou un sujet de fond. Fort de ses plus de 900 membres, de leur diversité (et donc représentativité de la réalité de la cybersécurité en France[1]) et du nombre de répondants à chaque mini-sondage, le CESIN peut proposer une vision transverse, représentative de la réalité des entreprises. Comme le club le fait chaque année depuis maintenant 4 ans, il semblait naturel de partager ces enseignements, au-delà des membres, à l'ensemble de la « communauté cybersécurité ».

Cette synthèse de l'année 2022 s'appuie sur les 27 questions qui ont été proposées aux membres du CESIN. Les panels sont représentatifs, s'étendant de 114 à 255 répondants, si on exclut une question spécifique aux 88 RSSI ayant, dans leur périmètre de responsabilités, une entité en Chine. La moyenne se situe à 172 répondants.

Comme nous avions commencé à le dessiner lors de la synthèse des instantanés 2021, les sujets, très variés, peuvent néanmoins se regrouper selon 4 catégories : les sujets d'actualité, les mesures de sécurité, l'organisation et la gouvernance et les sujets innovants.

Enfin, tout au long de cette quatrième année, nous voyons revenir certaines questions qui ont déjà été traitées lors des exercices précédents, permettant de dessiner des tendances.

Points d'actualité

L'actualité de début 2022 a bien sûr, et malheureusement, été marquée par le début de la guerre Russie-Ukraine. Le cyber espace étant devenu une zone de conflit à part entière, les inquiétudes de la communauté cyber étaient fortes, en premier lieu pour les RSSI en charge d'entités en Ukraine ou en Russie. L'inquiétude s'étendait néanmoins à l'ensemble de la communauté en raison de potentiels dommages collatéraux du conflit ou d'actions de représailles contre les intérêts des pays occidentaux soutenant l'Ukraine et/ou prenant des sanctions à l'encontre de la Russie. Le groupe du veille du CESIN a été très actif afin de partager les informations pertinentes avec les membres du club à cette période. C'est cependant via un sujet très précis que le conflit a été pris en compte dans une question hebdomadaire. L'ANSSI, dans son rapport de la menace cyber consacré au conflit publié en mars mettait en garde contre **l'utilisation de logiciels de sécurité russes**, au premier rang desquels, ceux édités par la société Kaspersky **[Q73]**. Ces solutions étaient utilisées par 25% des 201 répondants dont 44% envisageaient un changement de solution à court/moyen

1 Afin de mieux prendre cette diversité de ces membres, le CESIN, à introduit, à partir de Novembre 2022, pour les questions hebdomadaires posées à ses membres, la répartition des répondants par taille d'entreprise et secteur d'activité.

terme et 40% avaient déjà initié les travaux (donc potentiellement avant le début du conflit armé).

La dimension géopolitique de la cybersécurité ayant été un sujet traité lors du congrès annuel de décembre 2022, une question similaire a été proposée aux membres à l'issue de celui-ci **[Q93]**. Le panel de répondants était légèrement différent, composé de 138 RSSI dont 32% étaient utilisateurs des solutions Kaspersky. Parmi ceux-ci 53% en avaient achevé le décommissionnement alors que celui-ci était en cours pour 20%. Néanmoins, 27% de répondants prévoyaient de conserver cette solution, contre 16% en Mars. Une différence assez nette qui peut s'expliquer par un retour à la raison, quelques mois après la phase de sidération vis-à-vis de ce conflit armé en Europe. L'ampleur du projet de remplacement de sa solution anti-malware ainsi que son intégration à des roadmaps sécurité déjà difficiles à prioriser (et à financer) est potentiellement une autre explication.

Les situations de crise induites plus ou moins directement par la guerre en Ukraine furent nombreuses tout au long de l'année, jusqu'à l'annonce gouvernementale, de fin d'année, de **potentielles coupures de fourniture d'électricité pendant l'hiver**. La question sur le sujet **[Q92]** a permis d'identifier que ce risque était pris en compte par 73% des entreprises, sans grande disparité selon leur taille. Le pourcentage assez important d'entreprises n'ayant pas pris en compte ce risque envisageait probablement de s'appuyer sur leurs dispositifs de continuité existants. La question a aussi permis d'identifier que le PCA est dans le périmètre de responsabilités de 47% des RSSI, avec de fortes disparités entre les grandes entreprises (33%), les ETI (45%) et les PME/TPE (77%).

Deux autres sujets d'actualité traités lors de l'année 2022 concernaient l'évolution réglementaire. Le premier s'intéressait au projet d'un **Cyber Resilience Act** de la commission européenne **[Q86]**. Celui-ci vise à responsabiliser les éditeurs de logiciels et de matériels sur la sécurité de leurs solutions, couvrant un spectre très large. Face à la croissance continue du nombre de vulnérabilités auxquelles les RSSI ont à faire face, c'est donc sans surprise que 62% d'entre eux considèrent que cette évolution réglementaire est importante et doit être surveillée, seuls 2% considèrent qu'elle peut constituer un frein à l'innovation. A date de l'enquête, fin octobre, 36% des répondants n'avaient pas suffisamment pris connaissance du projet pour se prononcer.

La seconde évolution réglementaire pour laquelle le CESIN a consulté ses membres concerne la position prise par le Ministère de l'Économie quant à sa validation du **principe d'indemnisation des rançons** payées par les entreprises victimes de rançongiciels, sous réserve d'un dépôt de plainte **[Q81]**. Les réactions à cette annonce furent vives au sein de la communauté, craignant avant tout le risque d'encourager le cyber crime et celui que le cyber assureur ne rembourse « que » la rançon et non plus l'ensemble des frais nécessaires au retour à un fonctionnement nominal. C'est donc sans surprise que plus de 82% des 249 répondants ont manifesté leur opposition à la position de Bercy. Les 9% de répondants favorables à la mesure et les 9% qui ne se prononcent pas prennent potentiellement en compte que dans certaines organisations, hors de notre communauté (c'est-à-dire sans RSSI, voire sans DSI), le paiement de la rançon est parfois la seule option possible pour assurer la survie de l'entreprise.

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, mais plutôt en suivant le cycle Identify, Protect, Detect, Respond & Recover, recommandé par le framework du NIST.

S'il est partagé par les membres du CESIN « qu'on protège bien ce qu'on connait bien », l'étape d'identification de l'ensemble des assets à protéger et, parmi ceux-ci, des plus sensibles devient prépondérante dans le contexte de dématérialisation massive des processus de nos entreprises, d'ouverture et d'interconnexion des SI, de recours aux services Cloud…. Une part importante du challenge est de maitriser son exposition sur Internet, potentielle porte d'entrée sur l'ensemble du SI si un actif vulnérable ou mal configuré s'y trouve. Etant donné que cette exposition s'étend inexorablement, la thématique méritait bien deux questions hebdomadaires. La première permettait aux membres **d'évaluer l'exhaustivité et la précision de la connaissance de leurs actifs exposés sur Internet** **[Q76]**. Si, sans surprise, une large majorité (68%) ont une vision réaliste d'une bonne connaissance mais avec certains doutes concernant l'exhaustivité, 23% disposent d'un inventaire exhaustif, précis et régulièrement suivi de leurs assets exposés. Seuls 9% considèrent que cette connaissance est défaillante. La fréquence du contrôle de l'exposition Internet permet certainement d'expliquer ce taux de confiance important. Il est, en effet, réalisé mensuellement par 42% des répondants et par le même pourcentage trimestriellement. Moins de 5% des organisations ne réalisent ce contrôle qu'annuellement et 11% chaque semestre. Des chiffres qui sont cohérents avec ceux des réponses à la question **[Q57]**, posée en 2021 sur la même thématique.

La seconde question sur cette thématique portait elle sur l'outillage de ces contrôles et, plus largement sur **l'outillage permettant de maitriser son exposition sur Internet** **[Q77]**. Cet outillage apparait peu développé ou peu aligné sur les besoins des RSSI. En effet uniquement 20% s'appuient sur une solution du marché, alors 29% gèrent cet inventaire entièrement manuellement et que 29% des répondants ont fait le choix hybrides nécessitant une réconciliation manuelle de données issues d'outils. Un déficit d'outillage spécifique que les solutions se réclamant du néo-concept de CAASM (Cyber Asset Attack Surface Management) ont pour ambition de combler.

Un autre volet fondamental de maitrise de son environnement technique est la **gestion de l'obsolescence** **[Q87]**. En effet, les DSI font des choix stratégiques dans leur processus de gestion des assets, notamment leur maintien en condition opérationnelle et de sécurité. De ces choix peut résulter un certain taux d'obsolescence, que ce soit en termes d'OS, de middlewares, d'applications, de matériels ou de tout autre composant du SI. Les assets obsolètes deviennent une zone de forte exposition aux risques car sans support éditeur et confrontés à une vulnérabilité non patchable, Ils deviennent exploitables par des attaquants. Un risque qui se situe donc aux frontières des risques IT et des risques de cybersécurité avec néanmoins une tendance à leur prise en compte dans la cartographie des risques de sécurité pour 49% des entreprises. 26% des entreprises positionnent le risque d'obsolescence comme un risque IT et, pour

26% d'entre elles, l'obsolescence reste peu gérée et mal maitrisée. La gestion de l'obsolescence doit aussi désormais intégrer le prisme du green IT.

La réduction du risque d'obsolescence, passant potentiellement sous la responsabilité du fournisseur, peut-être perçue comme un des avantages des projets **Move-to-Cloud** **[Q91]** de plus en plus présents au sein de nos entreprises. Cependant, la migration d'une infrastructure interne vers des services IaaS ou PaaS amène son lot de risques propres et nécessite une évolution de la démarche de cybersécurité ainsi que de l'outillage associé. C'est le choix qu'on fait 30% d'entreprises en s'équipant d'outils de sécurité complémentaires et spécifiques. Celui-ci était (Décembre 2022) déployé pour 13% d'entre elles et en projet pour les 17% autres. 48% des entreprises s'appuient exclusivement sur les outils et interfaces mis à disposition par leur Cloud Provider, que 23% d'entre elles utilisent pour un suivi régulier. Pour 11% des entreprises, la prise en compte de la sécurité n'a pas encore accompagné la migration vers des solutions Cloud, probablement parce que celle-ci est récente, ou porte sur des composants peu sensibles. Enfin 11% des entreprises ne sont pas encore inscrites dans une trajectoire de migration vers des services Cloud et s'appuient sur des infrastructures internes. Il est à noter que ces pourcentages sont relativement cohérents, quelle que soit la taille des entreprises. Les différences notables portent sur le plus fort taux de pénétration des solutions Cloud dans les grands groupes et leur recours plus important à un outillage spécialisé.

En complément de l'exposition internet et de la maitrise de l'obsolescence des composants du SI, un sujet récurrent, voire un serpent de mer de la bonne connaissance de son SI est l**a classification des données** **[Q79]**. La démarche est considérée comme un des piliers de toute démarche de sécurité, permettant de proportionner les efforts de protection aux données les plus sensibles de l'entreprise et ainsi de rationaliser la démarche de cybersécurité. Mais l'exercice est également extrêmement fastidieux, long, coûteux avec de forts doutes sur son efficience. Une situation qui pourrait néanmoins évoluer avec l'apparition sur le marché d'outils de classification de plus en plus pertinents. A mi-2022, ces outils étaient effectivement utilisés par 52% des 177 répondants, mais uniquement comme une aide à une classification qui demeurait manuelle. Seuls, 5% des répondants utilisaient ces outils de façon automatique, preuve que leur efficacité opérationnelle demeure assez éloignée de la promesse marketing. Une situation qui est confirmée par les 43% de RSSI qui renoncent toujours à se lancer dans une démarche de classification. Des chiffres qui démontrent une légère évolution depuis 2020 **[Q37]**, où seulement 50% des répondants avaient lancé une démarche de classification.

Des chiffres qui sont également confirmés par une question plus large, portant sur **la gestion du patrimoine informationnel stratégique** **[Q84]**, sujet pris en compte par 60% des 148 répondants, potentiellement ceux effectivement engagés dans une démarche de classification. Néanmoins, un sujet encore assez nouveau puisqu'uniquement 6% des répondants ont formalisé une stratégie de protection du patrimoine informationnel de leur entreprise. 24% des RSSI répondants ont néanmoins mis en place une coordination avec les autres acteurs potentiels au sein de leur entreprise (gestion des risques, protection des données, gestion de crise) alors que 10% ont identifié les menaces spécifiques et mis en œuvre les mesures de sécurité ad-hoc.

A défaut de pouvoir s'appuyer sur une classification et un marquage fiable des données facilitant la mise en œuvre d'un dispositif de DLP, d'autres mesures, plus pragmatiques (mais potentiellement contraignantes) sont mises en œuvre par les entreprises pour réduire le risque de fuite de données. Parmi celles-ci la limitation ou, à minima, la supervision de l'utilisation de solutions cloud à l'initiative de l'utilisateur (Shadow-IT), au premier rang desquelles les solutions de **stockage de données en ligne** **[Q72]**. Il apparait néanmoins que le blocage totale de l'accès à ce type de solution, hors celles validées par l'entreprise, n'est en place que pour 27% des organisations. 31% ont mis en œuvre une surveillance des usages afin de détecter ceux qui sembleraient abusifs et/ou risqués. 44% des entreprises ont renoncé à prendre des mesures spécifiques et sont dans une démarche d'acceptation du risque. Il faut donc espérer que ces entreprises ne sont pas les mêmes que celles qui ont renoncé à la classification des données, au risque d'une importante perte de maitrise de leur patrimoine informationnel. Si ces chiffres démontrent effectivement une importante exposition aux risques, celle-ci serait en forte augmentation, en comparaison à une enquête similaire d'octobre 2019 **[Q5]**. Il apparaissait alors que le blocage était en place dans 41 % des entreprises (vs. 27%), la supervision pour 12% (vs. 31%) et l'acceptation du risque pour uniquement 16%. Un pourcentage qui se rapproche néanmoins des 44% de 2022 si on y ajoute les 31% d'entreprise ou l'usage était interdit par la Charte mais où cette interdiction n'était pas déclinée en mesures de blocage opérationnel.

Au chapitre de la protection des données, il est un basique de sécurité qui redevient prépondérant : la sauvegarde. Si celui-ci a pu sembler, un certain temps délaissé, la multiplication des attaques par ransomwares nous a rappelé l'absolue nécessité de disposer de sauvegardes fiables et régulièrement testées pour être en capacité à y faire face. Les attaquants ont aussi su s'adapter en développant de nouveaux malwares s'attaquant en priorité aux systèmes de sauvegardes, avant de chiffrer les données de production. Il est donc redevenu nécessaire, en complément des services performants de sauvegarde en ligne, de disposer d'un jeu de **sauvegardes off-line** **[80]**. Celui-ci étant le seul recours pour faire face à un ransomware ayant à la foi corrompu les données de production et leurs sauvegardes en ligne. Ces sauvegarde offline sont mise en œuvre par 70% des entreprises dont 32% les limitent à leurs données les plus sensibles. Pour les 30% d'entreprises qui n'utilisent que des sauvegardes en ligne, celles-ci risquent, de fait, de subir un impact élevé en cas d'attaque par ransomware.

Si la protection des données demeure un volet de la démarche de protection complexe à mettre en œuvre, la protection des endpoints est en plein essor via une tendance forte depuis quelques années : **le déploiement d'EDR** **[Q71]**. Et, effectivement , les tendances constatées via le baromètre annuel du CESIN se confirment avec 70% des 255 répondants ayant achevé leur déploiement et celui-ci étant en cours ou en projet pour 22%. Un taux d'équipement qui a donc progressé de 20% depuis la dernière question de la semaine sur le sujet, en 2019, plaçant l'EDR comme un composant quasi incontournable de notre arsenal de défense.

Mais, pour être efficace, la solution EDR, une fois déployée, nécessite une charge d'exploitation non négligeable afin de prendre en compte les alertes, de s'assurer de la pertinence de la détection, du confinement des infections et des attaques,

de réaliser les investigations complémentaires et l'ensemble des actions de remédiation. Si cette énumération de tâches semble naturellement placer **la gestion de l'EDR** **[Q82]** sous la responsabilité du SOC, ce choix d'organisation n'a été fait que par 53% des entreprises alors que pour 28%, l'EDR est géré par une autre entité dédié à la cybersécurité opérationnelle. 19% d'entreprises ont, pour leur part, confié la gestion de l'EDR à son éditeur, sous forme de service managé, solution potentiellement la plus pragmatique et efficace pour des organisations de petite taille.

Une mesure complémentaire de protection des endpoints, à la frontière des mesures de maitrise de son parc est le **déploiement de configurations standard pour le durcissement des operating systems et les logiciels** **[Q67]**. Cette bonne pratique est effectivement en place dans 80% des entreprises dont 60% définissent leurs propres règles alors que seules 20% mettent en œuvre les recommandations d'organismes tels le CIS ou le NIS. Pour aller encore plus loin, certaines organisations mettent en œuvre un contrôle d'intégrité des logiciels installés **[Q68]**. Cependant, début 2022, cette mesure demeurait marginale puisque mise en œuvre uniquement par 9% des 142 répondants.

Autre pilier du volet préventif de toute démarche de cybersécurité : l'authentification et son incontournable mot de passe. Bien que celui-ci soit aujourd'hui considéré comme insuffisant, qu'il requiert d'être complété d'un second facteur (**[Q34]** traitée en 2020) ou qu'il soit remplacé, là où cela est possible, par des mécanismes d'authentification plus modernes (**[Q64]** traitée en 2021), il n'en reste pas moins, pour chaque RSSI, l'exercice imposé de définition de **la politique de mot de passe** **[Q74]** de son organisme. Plusieurs caractéristiques des mots de passe font débat : longueur, complexité, … et surtout historique. Un sujet relancé par l'ANSSI fin 2021, qui recommande dorénavant de ne plus imposer le sacro-saint changement tous les 90 jours. Prenant en compte cette évolution de posture, début 2022, les RSSI du CESIN apparaissent relativement conservateurs puisque 53% conservent une obligation de renouvellement tous les 90 jours de mots de passe de 8 à 10 caractères. 30% ont franchi le pas d'un renouvellement semestriel ou annuel et seuls 5% n'imposent que des renouvellements moins fréquents mais pour des mots de passe (ou plutôt phrases de passe) très longs, sans être nécessairement très complexes en termes d'alphabets utilisés. Une évolution qui prendra certainement du temps tant la pédagogie et l'accompagnement au changement sont nécessaires à toute évolution des politiques de mots de passe et tant le principe des « 90 jours » est ancré dans les référentiels d'audit.

Un outil qui facilite la compréhension et l'adoption de la politique de mots de passe (entre autres) est, en amont du programme de sensibilisation, la **Charte Utilisateurs** **[Q85]**. Un outil qui, pour être efficace, doit être régulièrement maintenu à jour, bien que son élaboration et sa validation puissent être chronophages. Une révision rendue également nécessaire par les évolutions profondes et rapides des contextes dans lesquels se positionnent ces chartes : télétravail et ses conséquences (sécurité du réseau domestique, assistants personnels à la maison, usage des matériels par la famille, sécurité physique des matériels, échanges professionnels potentiellement « écoutés » par des proches…), généralisation de la visioconférence et des messageries instantanées, développement de l'usage des mobiles, de la téléphonie sur IP,

nouveaux outils collaboratifs online, développement des ransomwares et généralisation des EDR, extension des SOC et des capacités de surveillance des salariés, … Des tendances fortes qui justifient que 43% des 168 répondants ont récemment révisé leur charte et que le chantier est en projet court terme pour 31 %.

S'il est un type d'accès pour lequel l'authentification mais également la traçabilité et la supervision doivent être renforcées, ce sont les accès à risques, de type administrateur, indispensables aux actions de configuration, paramétrage, … des composants du SI. Des besoins de sécurité renforcés et spécifiques auxquels les solutions de **Privileged Access Management** **[Q89]** peuvent apporter une réponse. Une solution adoptée par 54% des entreprises et en projet pour 29%. Parmi les 54% d'organisations équipés, 16% ont généralisé la solution de PAM à un grand nombre de systèmes et d'applications alors que 17% l'ont spécialisée sur l'ensemble de leurs assets critiques et 20% uniquement sur une partie de ceux-ci.

Sur le volet détection de la démarche de cybersécurité, le CESIN s'est penché, en février 2022 sur la **Politique de gestion des logs** **[Q69]**. Celle-ci a pour objectif de garantir que l'on dispose bien des traces pertinentes en termes de natures d'évènements et de rétention pour détecter des scénarios suspects et/ou pour investiguer a posteriori. Elle permet également de spécifier les logs qui seront qui stockées localement et ceux qui seront envoyées à un SIEM, et, plus globalement de formaliser une stratégie de gestion des journaux d'évènement. Un document fondateur donc de la démarche de détection qui est effectivement formalisé pour 64% des entreprises dont 23% l'appliquent à leurs actifs sensibles ainsi qu'à tout nouveau projet. Pour les 33% d'entreprises qui n'ont pas défini leur propre politique de gestion de logs, les stratégies par défaut des systèmes sont mises en œuvre.

La gouvernance et l'organisation

Les questions hebdomadaires portants sur la gouvernance se sont intéressées à certains piliers de celles-ci, à commencer par le **Comité Sécurité** **[Q70]**, instance de gouvernance permettant d'impliquer les directions métiers et support dans la démarche de cybersécurité. Le Comité Sécurité, animé par le Responsable Cybersécurité, permet de présenter les risques cyber, la stratégie et la feuille de route associée, mais aussi de faire le bilan des projets, de la menace, de la sinistralité en général et dans l'entreprise, ainsi que de partager un reporting illustrant la maturité et la performance cyber de l'entreprise. Un organe de pilotage qui semble donc indispensable mais qui n'est mis en œuvre que par 67% des entreprises dont 26% considèrent que son rôle demeure limité. Un potentiel axe d'amélioration donc afin que la cybersécurité devienne une véritable démarche d'entreprise.

Pour que le Comité Sécurité, quand il est en place, puisse prendre des décisions appropriées, il est nécessaire de l'alimenter d'éléments de reporting, via un **Tableau de bord de sécurité** **[Q75]**. Un tableau de bord qu'il est nécessaire d'adapter à ses différents interlocuteurs et d'alimenter avec les « bons » indicateurs qui permettront de prendre les « bonnes » décisions. Des objectifs parfois complexes à combiner qui justifient la création, par le CESIN, d'un lab dédié. L'état des lieux réalisé lors de l'initialisation de ce lab confirme qu'il s'agit

d'un outil indispensable du RSSI, mis en œuvre par 98% d'entre eux (dont 33% via un projet en cours). Pour 42%, il ne s'agit pas d'un unique mais de plusieurs tableaux de bord, adaptés à leurs différents interlocuteurs. Les fréquences de publication sont majoritairement mensuelles ou trimestrielles (42% dans les deux cas) et plus rarement semestrielle (12%) voire annuelle (4%). Des fréquences assez réduite qui s'expliquent probablement par la charge de travail nécessaire à la production des tableaux de bord et leur lente évolution dans le temps. On note également une bonne capacité de synthèse puisque les tableaux de bord à destination du Comex se limitent à 2 à 4 indicateurs dans 43% des cas.

Le budget [Q83]. demeure le nerf de la guerre de toute démarche de cybersécurité. Une tendance 2023 à l'augmentation légère (38%) voire sensible (26%) confirme la plus grande prise en compte des risques de cybersécurité. D'autant plus que les budgets ne sont en régression que pour 8% des organisations et stables pour 28%. Des tendances très éloignées de celles de 2020 **[Q30]** (en préparation des budgets 2021) où la crise sanitaire avait conduit à des réductions, parfois drastiques (plus de 20% pour 16% des répondants) des budgets cybersécurité et, plus globalement, à leur stabilité (48%).

En termes d'organisation, la question hebdomadaire portait sur la **gestion des imprévus [Q90]** (les incidents de cybersécurité ayant une fâcheuse tendance à se produire en heures non ouvrées). Pour faire face à ces imprévus, si 5% des entreprises (uniquement des grands groupes) disposent d'une organisation internationale « Follow the sun », 15 % d'entre elles (sans réelle différence de taille) ont mis en place une astreinte des équipe internes de cybersécurité, combinée à des SLA 24/7 des services de sécurité externalisés. Pour 31% des entreprises (assez étonnement avec une prépondérance de grands groupes), seul le SOC fonctionne en 24/7 avec un RSSI joignable H24. Une majorité d'entreprises (49%) et, sans surprise, principalement les PME et ETI n'ont pas mis en place d'organisation spécifique à la gestion des incidents en heures non ouvrées mais se reposent sur le professionnalisme des équipes Cyber Sécurité pour se mobiliser si nécessaire.

Les sujets innovants

Bien que le terme de « Résilience » **[Q88]** apparaisse formellement dans un projet de Loi européen (cf. [Q86] ci-dessus), l'utilisation de ce terme est assez récente dans l'écosystème cybersécurité mais devient de plus en plus présent. Il était donc pertinent de faire réagir les membres du club à ce (potentiel) nouveau concept. Et, effectivement, à date de l'enquête, en Novembre 2022, 38% des 160 répondants, potentiellement déjà échaudés par d'autres « buzz words » considéraient que la cyber-résilience n'est qu'un concept marketing qui n'apporte rien de nouveau au sujet de la continuité de services. Parmi les 62% de répondants considérant le concept porteur d'innovation, une moitié considèrent néanmoins que celui n'influencera qu'à la marge leur démarche de cybersécurité. Des positions tranchées et éloignées que les récents travaux du CESIN sur le sujet (réunion de collège et Groupe de Travail) n'ont que partiellement permis de réconcilier.

ANNEXE

QUESTION DE LA SEMAINE : DETAIL DES RESULTATS

[Q5] Stockage en ligne

Des outils collaboratifs permettant à vos utilisateurs de stocker leurs documents, pour y travailler, les archiver ou les échanger sont en place dans vos entreprises. Ces espaces de stockage sont utilisées soit pour un stockage individuel, soit en partage avec d'autres utilisateurs ou avec des partenaires, fournisseurs et autres interlocuteurs externes. Des droits d'accès sont paramétrables sur ces espaces et selon les outils que vous utilisez (NAS, solutions cloud…), vous gérez ces droits en central ou bien cette gestion est plus ou moins déléguée à vos utilisateurs, avec des mauvaises surprises parfois sur les configurations.

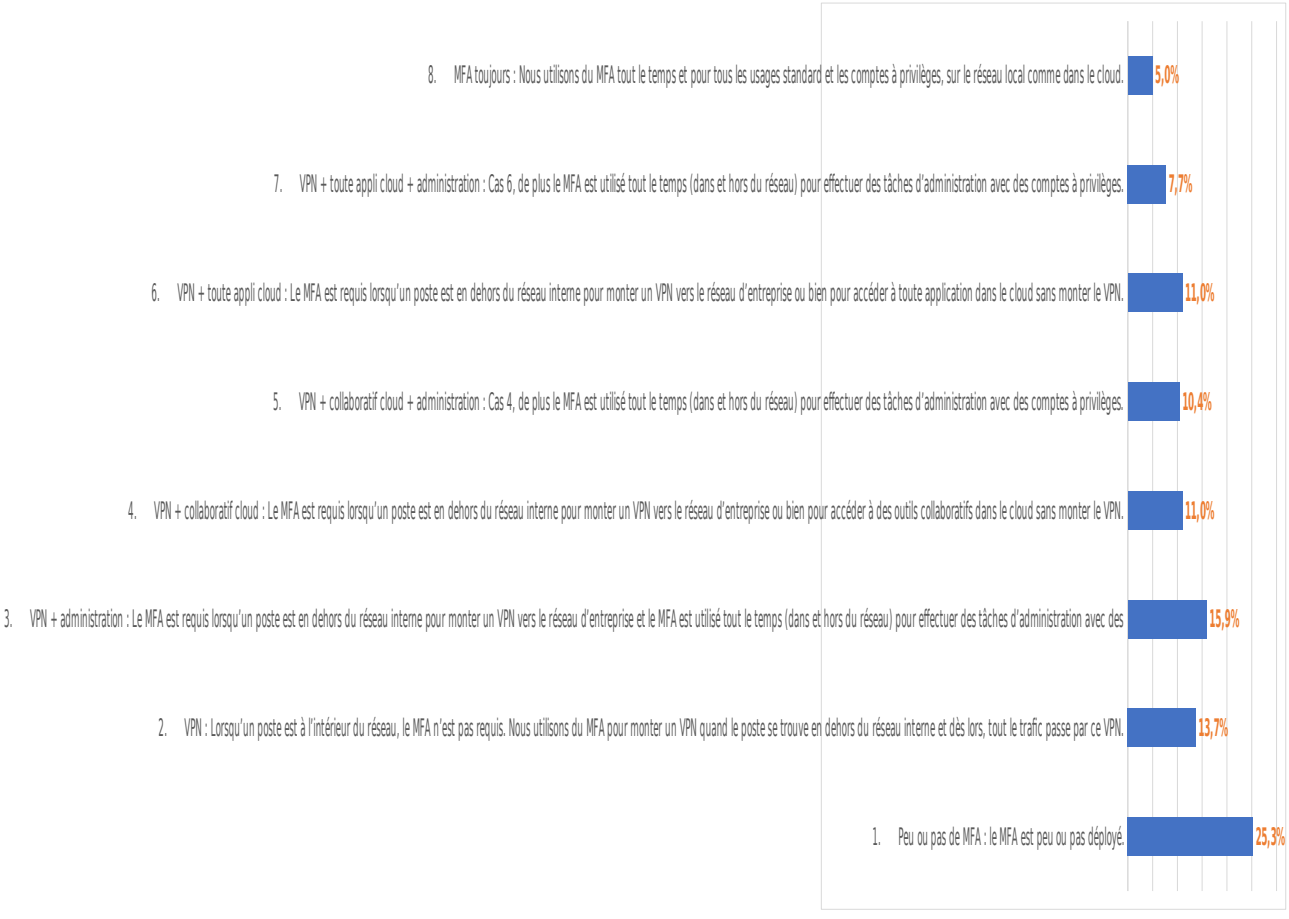
Pourtant la tentation de solutions alternatives est grande chez vos utilisateurs qui préfèrent utiliser d'autres outils, non validés par la DSI, parfois sous l'influence de leur correspondants externes qui les imposent ou parce qu'ils jugent que ces outils sont plus simples ou plus ergonomiques. Les *box et *transfer en tous genres sont alors susceptibles de fleurir et d'héberger des données de l'entreprise.

[Q30] Les budgets

L'impact économique de la crise sanitaire n'est pas encore connu au niveau des métiers de l'IT et de la cybersécurité. Une enquête internationale parue dans la presse spécialisée la semaine dernière fait apparaitre que 40% des décideurs informatique ont réduit le budget dédié à la cybersécurité pour limiter l'impact financier de la crise liée au Covid-19. Une situation qui peut surprendre dans le climat actuel de cyber "insécurité". Qu'en est-il dans vos entreprises ?

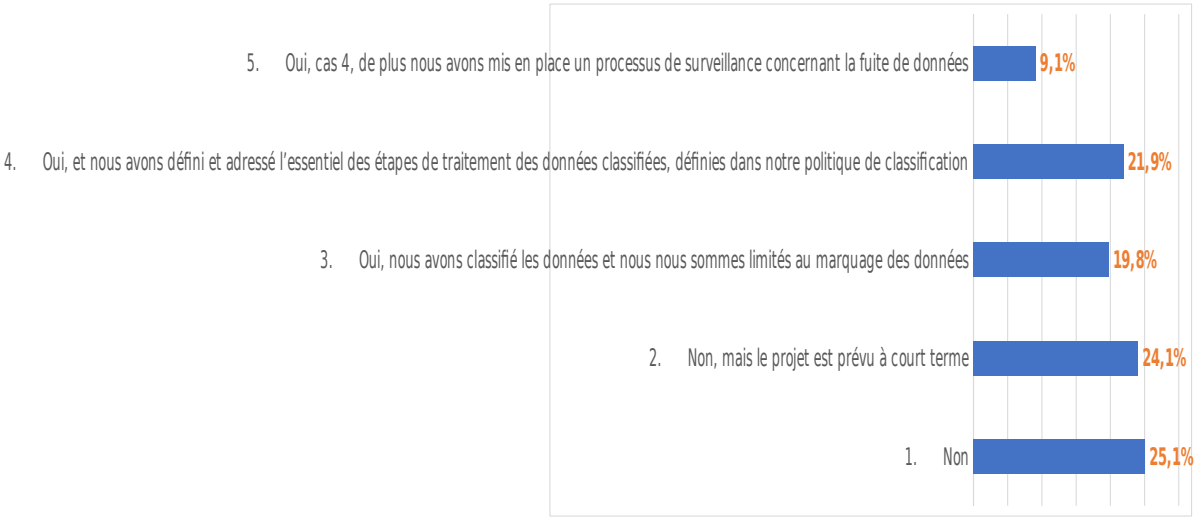
[Q34] MFA

La transition vers le cloud a conduit à un développement rapide du MFA. L'authentification simple par mot de passe n'est plus considérée comme acceptable, au regard du risque d'une usurpation d'identité. En l'absence de second facteur, les usurpations d'identité peuvent se multiplier que ce soit sur des usages collaboratifs, des applications métiers ou des tâches de développement ou d'administration. Où en êtes-vous de la mise en œuvre du MFA ?



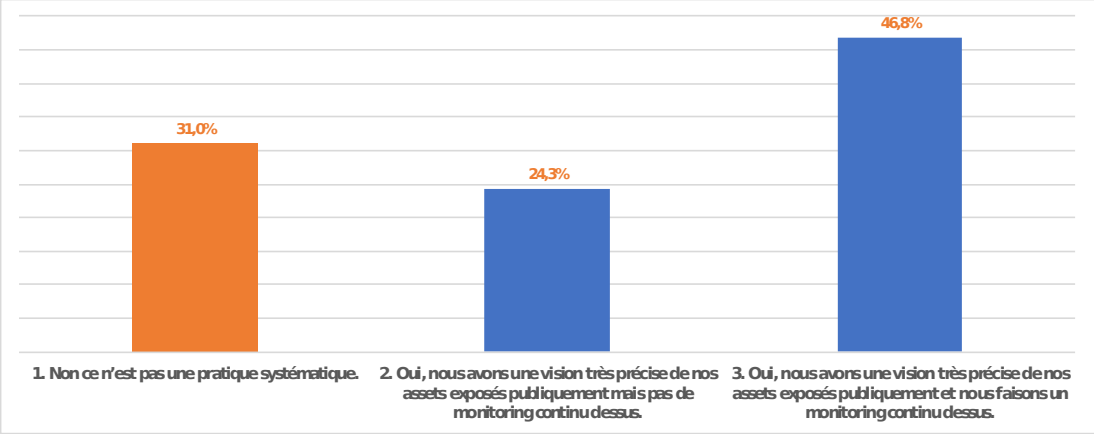
[Q37] Classification

La protection des données démarre généralement par un processus de classification des données. Différents niveaux de classification peuvent être alors mis en place et des traitements sont prévus derrière ces niveaux pour adresser les opérations réalisées tout au long du cycle de vie des données : création, marquage, utilisation (accès, lecture, modification, impression, échange, duplication), conservation (stockage, sauvegarde, archivage), destruction. Avez-vous mené un projet de classification ?



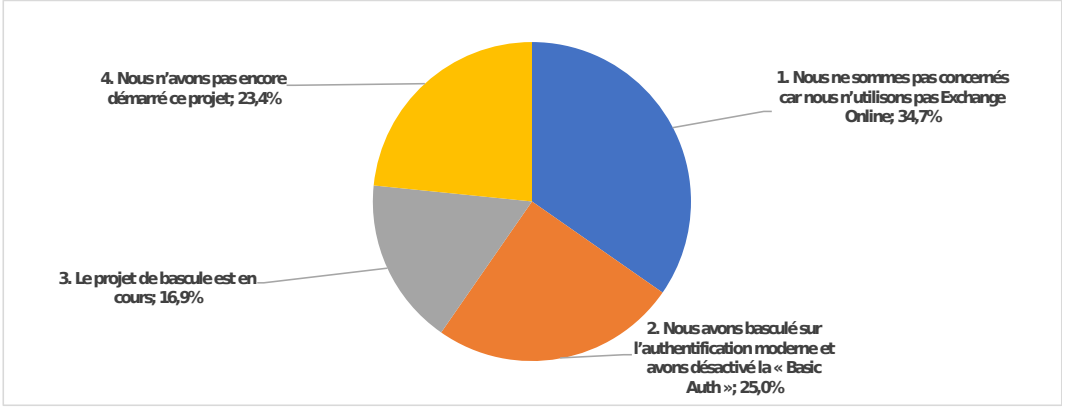
[Q57] Détection périmétrique

Un pourcentage élevé de cyberattaques arrive à entrer via du phishing, mais il y a aussi des attaques qui profitent d'IP publiques mal protégées. Pour éviter de subir une attaque via le second scénario, il faut d'une part bien connaître son exposition publique depuis des datacenters classiques ou depuis ses environnements cloud, et d'autre part il faut scanner ces assets pour vérifier qu'il n'y a pas de ports anormalement exposés. Réalisez-vous un inventaire / une découverte de votre périmètre et un monitoring de votre exposition publique ?



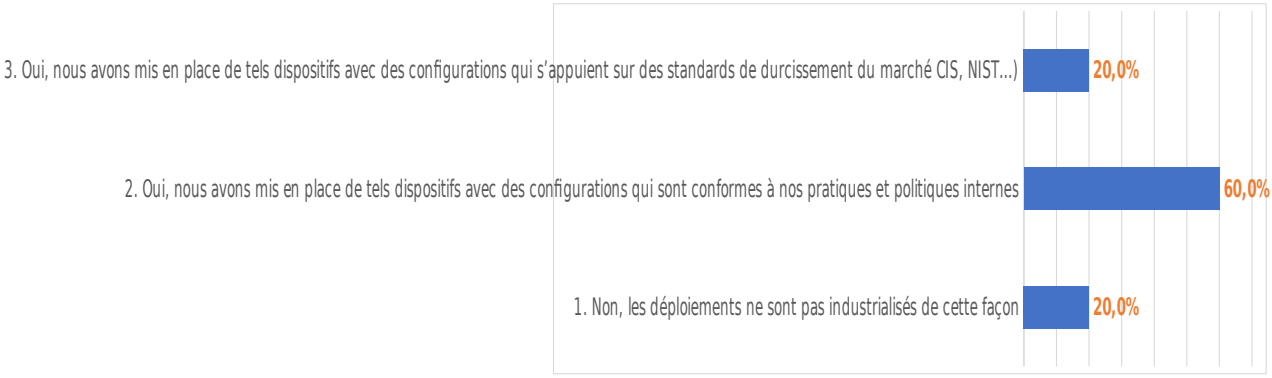
[Q64] Authentification basique Microsoft

Microsoft vient d'annoncer la date de fin de l'authentification basique (basic auth) pour le 1er Octobre 2022. Cette date limite a fluctué ces derniers mois, elle vient d'être confirmée. Cela concerne les utilisateurs d'Exchange Online. Le passage à la « Modern Auth » va améliorer sensiblement la sécurité des tenants O365. Où en êtes-vous de cette implémentation ?



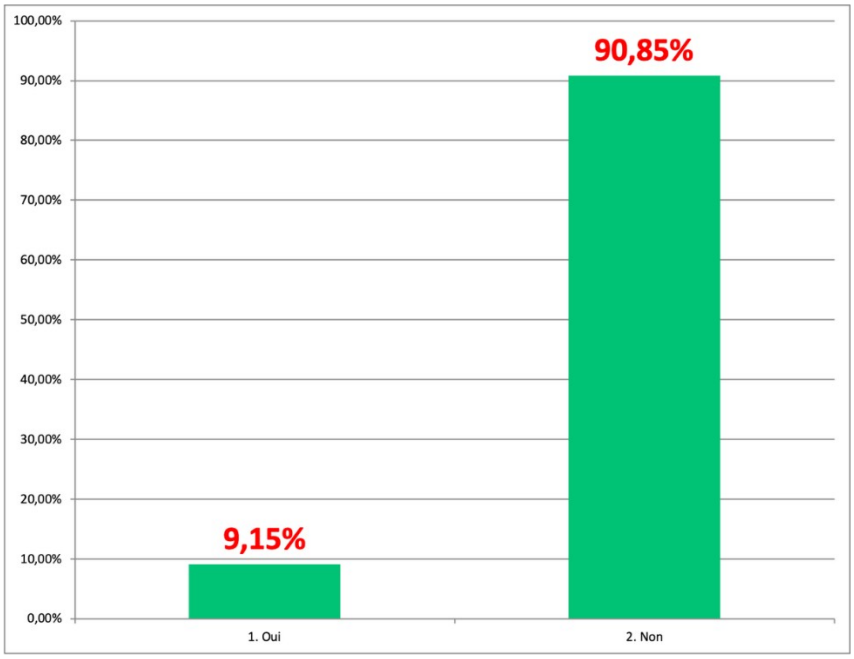
[Q67] Configurations standard

La maîtrise de la sécurité des systèmes et des applications passe par une approche industrialisée des configurations. Avez-vous mis en place des dispositifs permettant de déployer des configurations standard pour les systèmes d'exploitation et les logiciels ?



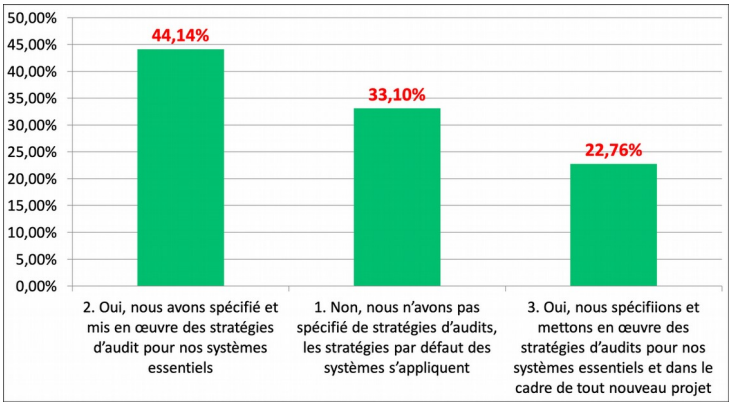
[Q68] Intégrité des logiciels

Vous gérez probablement un inventaire des logiciels autorisés sur vos endpoints (postes de travail et serveurs). En complément de ces inventaires, avez-vous mis en place des outils de contrôle d'intégrité des logiciels installés pour valider que ceux-ci n'ont pas été modifiés avant qu'ils ne puissent s'exécuter ?



[Q69] Politique d'Audit

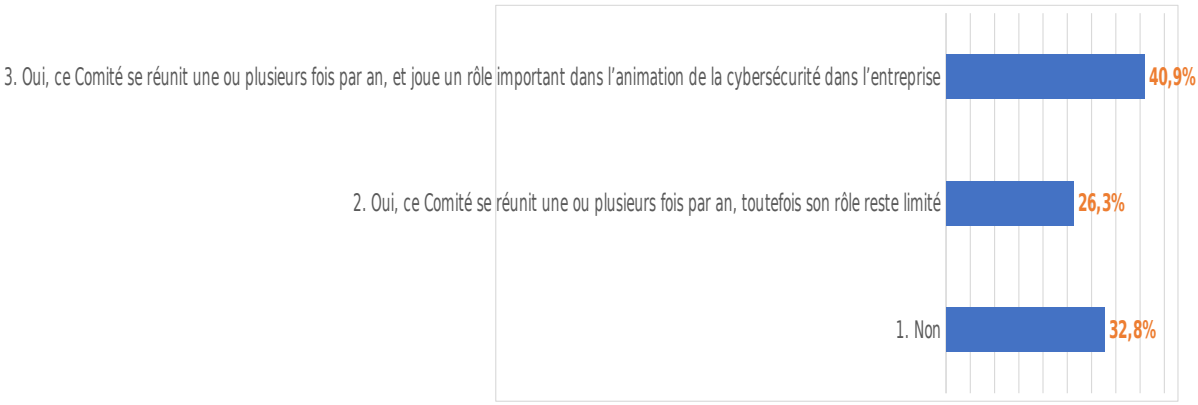
La stratégie d'audit des systèmes et des applications permet de garantir que l'on dispose bien des traces pertinentes en termes de natures d'évènements loggés et de rétention pour détecter des scénarios suspects et/ou pour investiguer a posteriori. La stratégie d'audit spécifie par ailleurs si telles ou telles natures de logs seront stockées localement et/ou envoyées à un SIEM, ces collectes de logs pouvant avoir des durées de rétentions différentes. Avez-vous défini et mis en place une telle stratégie ?



CHOIX DE RÉPONSES	RÉPONSES	
1. Non, nous n'avons pas spécifié de stratégies d'audits, les stratégies par défaut des systèmes s'appliquent	33,10 %	48
2. Oui, nous avons spécifié et mis en œuvre des stratégies d'audit pour nos systèmes essentiels	44,14 %	64
3. Oui, nous spécifiions et mettons en œuvre des stratégies d'audits pour nos systèmes essentiels et dans le cadre de tout nouveau projet	22,76 %	33
TOTAL		145

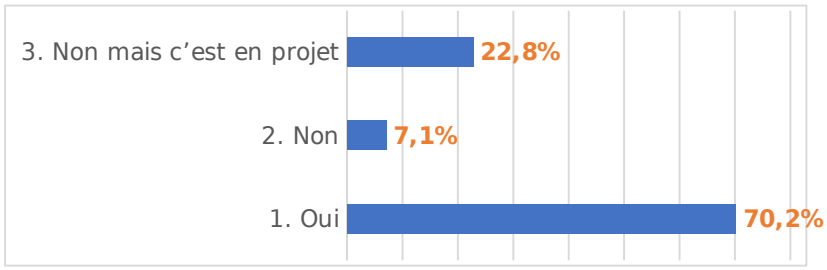
[Q70] Comité sécurité

Il est important que les directions métiers et support de l'entreprise aient une bonne connaissance et compréhension de la cybersécurité pour que celle-ci soit naturellement associée aux différentes initiatives et pour établir ainsi un réel partenariat avec ces Directions. Pour cela, un Comité Sécurité réunissant ces personnes et animé par le Responsable Cyber, permet de présenter les risques cyber, la stratégie et la feuille de route associée, mais aussi faire le bilan des projets cyber, de la menace, de la sinistralité en général et dans l'entreprise (bilan des incidents) et pour présenter un reporting illustrant la maturité et la performance cyber de l'entreprise. Avez-vous mis en place un tel Comité réunissant les directions métiers et support de l'entreprise ?



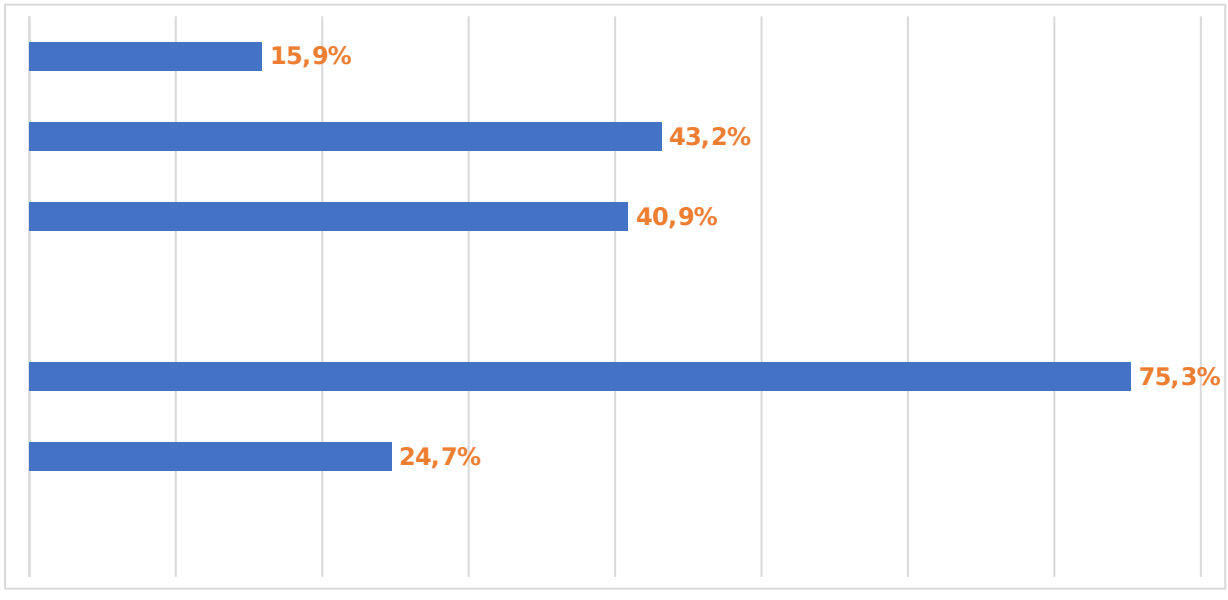
[Q71] EDR

La question de la semaine porte sur la politique de mise en place d'un EDR. Avez-vous mis en place un EDR ?



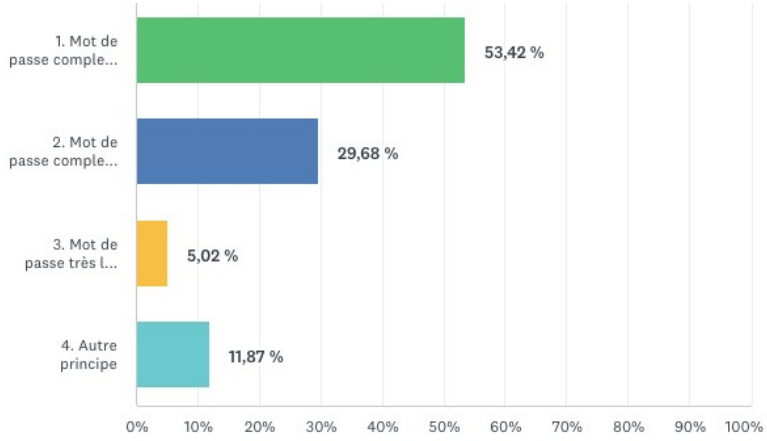
[Q73] Utilisation des outils numériques liés à la Russie

Les récentes mises en garde de l'ANSSI sur les produits cybersécurité d'origine russe, Kaspersky en premier lieu, ont-elles un impact sur votre stratégie de protection cyber ?



[Q74] La politique de gestion des mots de passe (PGMP)

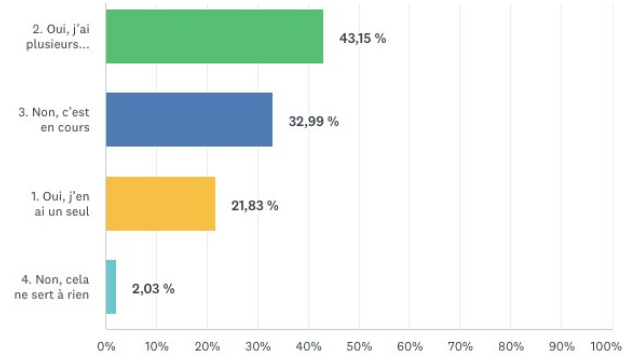
La politique de gestion des mots de passe (PGMP) fait souvent débat et est très variable d'une entreprise à l'autre. Quelle politique de mot de passe avez-vous mis en place dans votre entreprise ?



CHOIX DE RÉPONSES	RÉPONSES	
1. Mot de passe complexe (3 types de caractères a minima), 8 ou 10 caractères et renouvelé assez fréquemment, par exemple tous les 90 jours	53,42 %	117
2. Mot de passe complexe (3 types de caractères a minima), 8 ou 10 caractères et renouvellement tous les 6 mois ou annuels	29,68 %	65
3. Mot de passe très long mais pas nécessairement complexe (un long texte simple, par exemple) avec renouvellement peu fréquent	5,02 %	11
4. Autre principe	11,87 %	26
TOTAL		219

[Q75] Tableaux de Bord

Dans le cadre du Lab Tableaux de Bord, nous aimerions connaître votre avis. Avez-vous mis en œuvre un tableau de bord cyber dans vos organisations ?

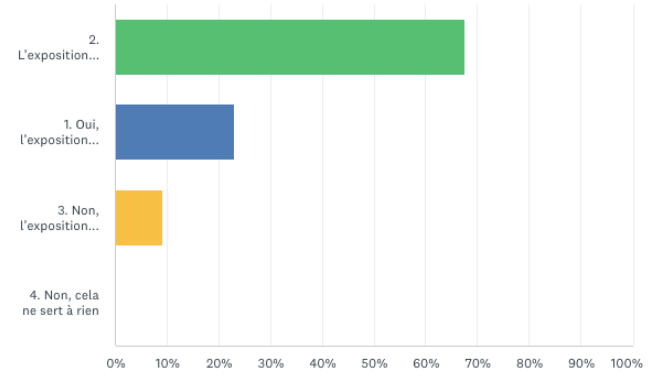


CHOIX DE RÉPONSES	RÉPONSES	
2. Oui, j'ai plusieurs tableaux de bord en fonction de mes interlocuteurs qui le reçoivent	43,15 %	85
3. Non, c'est en cours	32,99 %	65
1. Oui, j'en ai un seul	21,83 %	43
4. Non, cela ne sert à rien	2,03 %	4
TOTAL		197

[Q76] Exposition publique – Episode 1

Dans le contexte actuel des cyber menaces, il est plus que jamais nécessaire de maîtriser son exposition publique sur Internet. Un seul asset exposé et vulnérable, mal configuré et/ou pas correctement durci et c'est un point d'entrée potentiel pour un attaquant. Or la maîtrise de son exposition Internet n'est pas simple, que ce soit pour ses actifs dans ses propres datacenters, chez des hébergeurs de clouds privés et sites web ou dans

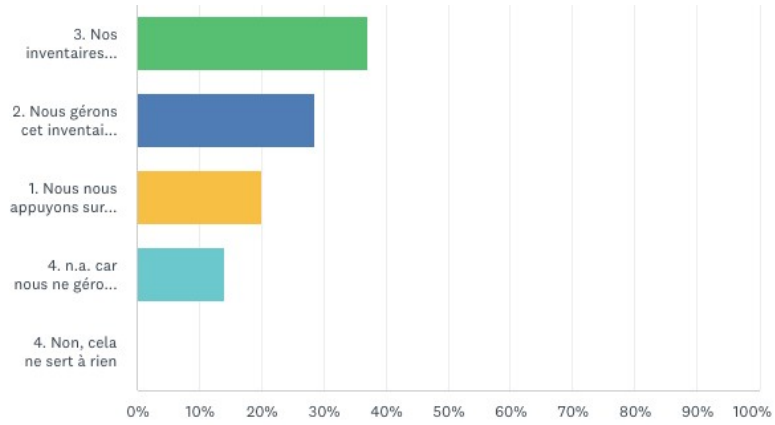
des environnements de cloud public. Dans ce premier épisode sur le sujet, on s'interroge sur le degré de connaissance de son exposition. Avez-vous une connaissance exhaustive et précise de vos assets exposés (inventaire IP publics et assets associés, nature de ces assets) ?



CHOIX DE RÉPONSES	RÉPONSES	
2. L'exposition Internet est relativement bien connue, même si elle n'est sans doute pas exhaustive	67,63 %	117
1. Oui, l'exposition Internet est parfaitement inventoriée et suivie avec précision	23,12 %	40
3. Non, l'exposition Internet est plutôt mal identifiée	9,25 %	16
4. Non, cela ne sert à rien	0,00 %	0
TOTAL		173

[Q77] Exposition publique – Episode 2

Dans un premier épisode sur le sujet, nous vous avions interrogé sur le degré de connaissance de votre exposition publique sur Internet (inventaire IP publics et assets associés, nature de ces assets). Dans ce second épisode, nous cherchons à déterminer la méthode utilisée pour cette maîtrise de nos assets publics. Comment faites-vous pour établir et maintenir la connaissance de votre surface d'attaque publique ?

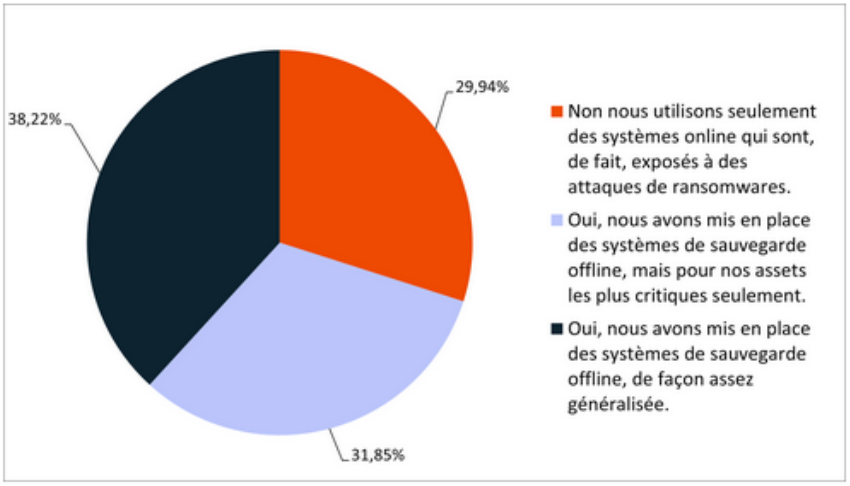


CHOIX DE RÉPONSES	RÉPONSES	
3. Nos inventaires sont gérés et maintenus de façon hybride : sur la base d'une ou plusieurs solutions du marché, avec une réconciliation par rapport à un processus de gestion manuelle de nos assets	37,20 %	61
2. Nous gérons cet inventaire manuellement. Les assets sont enregistrés et l'inventaire est mis à jour au fur et à mesure des déploiements, des updates et des décommissionnements.	28,66 %	47
1. Nous nous appuyons sur une (ou plusieurs) solutions du marché qui nous donne(nt) la liste de nos assets publics et les services exposés.	20,12 %	33
4. n.a. car nous ne gérons pas précisément cet inventaire	14,02 %	23
4. Non, cela ne sert à rien	0,00 %	0
TOTAL		164

[Q80] Sauvegardes offline

Les attaques par ransomwares ont très vite mis en évidence qu'il était important d'être assurés de disposer de sauvegardes pour rétablir ses systèmes et ses données.

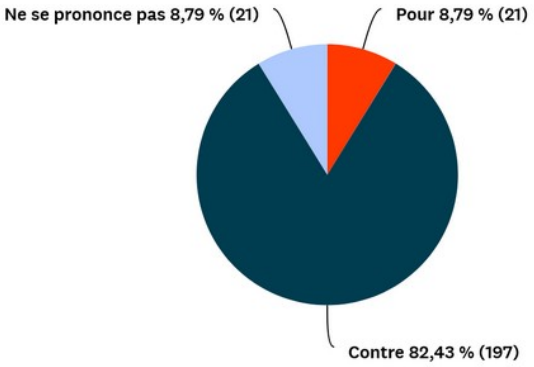
Étant donné que les attaquants ciblent en premier lieu les systèmes de sauvegarde, il est apparu un besoin de sauvegardes immuables ou « offline ». Avez-vous mis en place ce type de sauvegarde dans votre SI ?



CHOIX DE RÉPONSES	RÉPONSES	
Non nous utilisons seulement des systèmes online qui sont, de fait, exposés à des attaques de ransomwares.	29,94 %	47
Oui, nous avons mis en place des systèmes de sauvegarde offline, mais pour nos assets les plus critiques seulement.	31,85 %	50
Oui, nous avons mis en place des systèmes de sauvegarde offline, de façon assez généralisée.	38,22 %	60
TOTAL		157

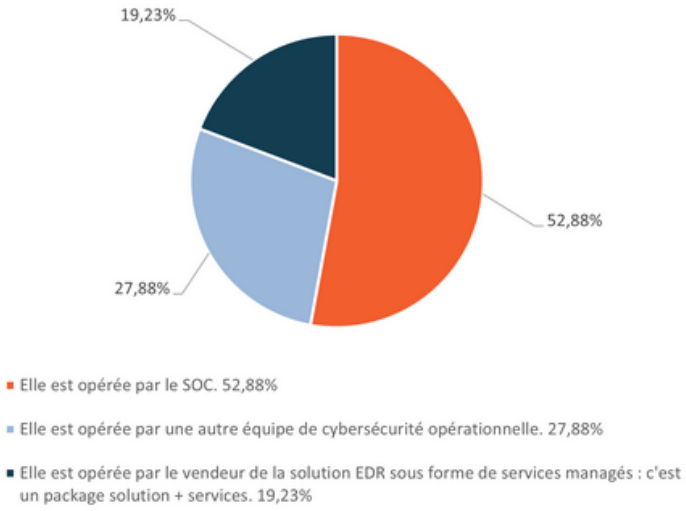
[Q81] Rançons

Vous avez sans doute lu que Bercy donne son feu vert au principe d'indemnisation des rançons payées par les entreprises victimes, sous réserve que ces entreprises portent plainte. Les réactions sont vives et nombreuses dans notre communauté, suite à cette annonce (risque d'encourager au cybercrime ? Avantage pour les assureurs qui paieront moins cher une rançon que le traitement d'un ransomware très impactant, etc.). Et vous, quel est votre avis sur cette disposition ?



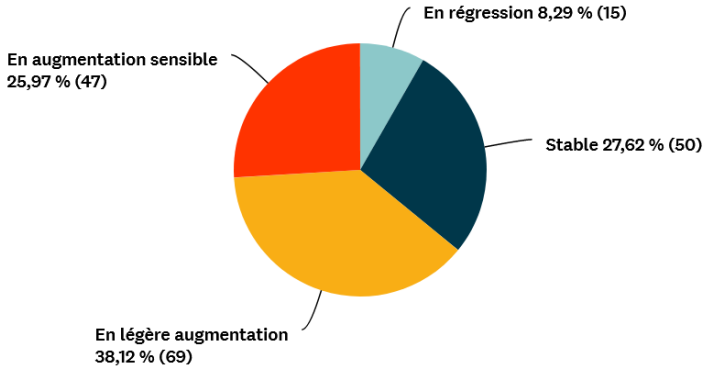
[Q82] Gestion EDR

Vous êtes nombreux à avoir déployé des EDR dans vos entreprises. Comment est opérée la plateforme EDR (gestion des alertes, détection, containment, investigation, remédiation) ?



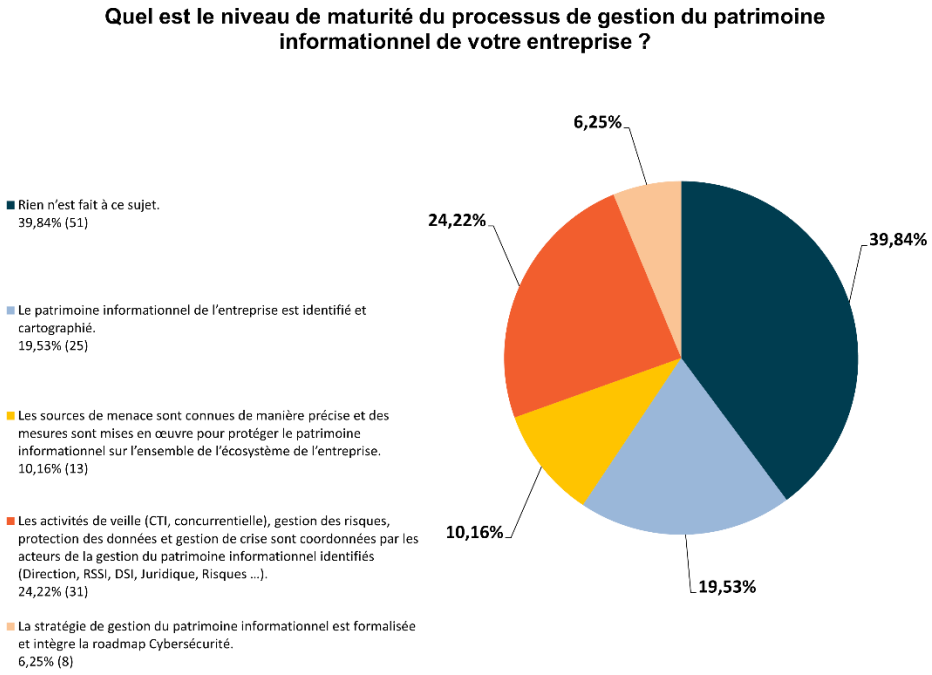
[Q83] Budget Cyber 2023

Nous sommes en pleine période de l'établissement des budgets pour 2023. Comment se situe votre budget cyber 2023 par rapport à 2022 ?



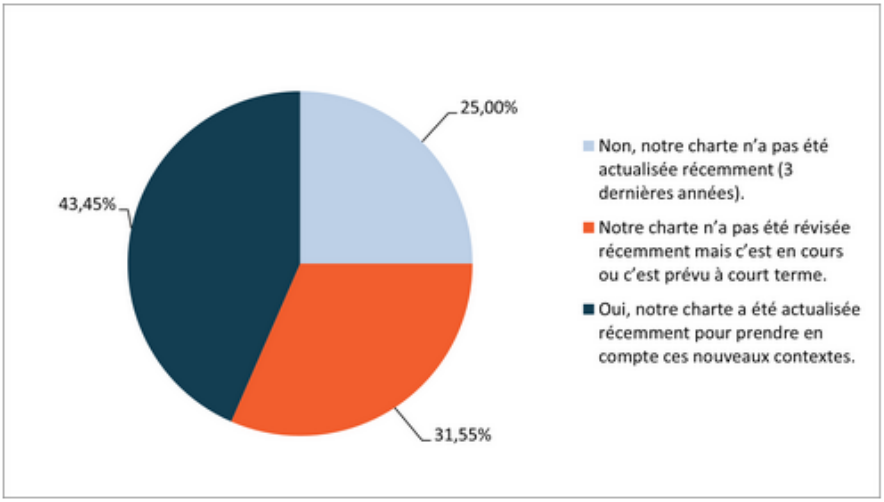
[Q84] Gestion du patrimoine informationnel stratégique

Les cyberattaques sont utilisées dans la guerre économique. Leurs objectifs : récupérer à minima des informations stratégiques et dans les cas extrêmes compromettre la survie de l'entreprise victime au profit d'un concurrent. Aujourd'hui plus que jamais, la cybersécurité et l'intelligence économique stratégique (IES) entretiennent des liens évidents. Ces deux expertises ont pour but d'augmenter la maturité et la résilience des entreprises face aux nombreux risques. Le patrimoine informationnel est constitué de l'ensemble des informations stratégiques et est la représentation de la valeur d'une entreprise. Il est donc important de l'identifier, le cartographier et le défendre de manière adéquate. Au-delà du système d'information (SI), avec la gestion du patrimoine informationnel, c'est une vision plus globale qui est proposée : celle de la protection de l'Information dans son ensemble. Quel est le niveau de maturité du processus de gestion du patrimoine informationnel de votre entreprise ?



[Q85] Charte utilisateurs

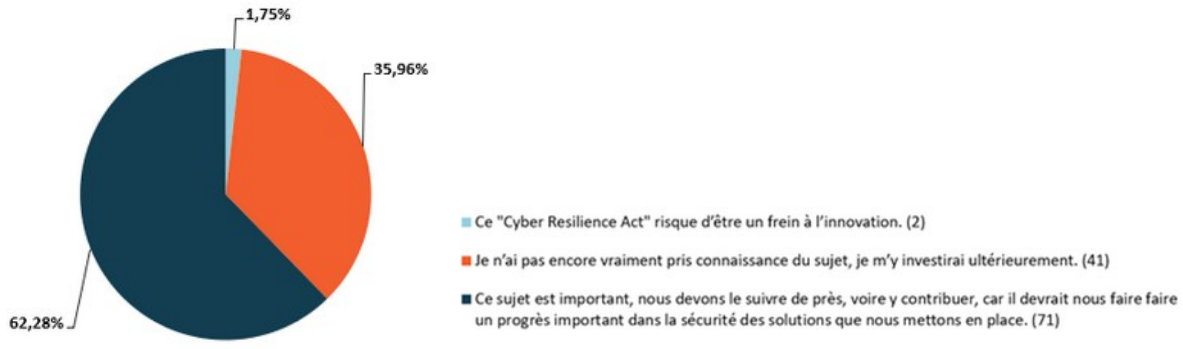
Vous disposez probablement d'une charte cybersécurité destinée à vos utilisateurs, peut-être publiée sur votre intranet et/ou intégrée à votre Règlement Intérieur. Beaucoup de bonnes pratiques ont été publiées sur ces chartes et il y a eu une longue période de stabilité quant à leur contenu. Depuis 3 ans, un certain nombre de facteurs sont de nature à nécessiter des révisions et adaptations assez profondes de ces chartes : le télétravail et la mise à l'épreuve du contexte pro/perso (sécurité du réseau domestique, assistants personnels à la maison, usage des matériels par la famille, sécurité physique des matériels, échanges professionnels potentiellement « écoutés » par des proches…), usage intensif de la visioconférence et des messageries instantanées, développement de l'usage des mobiles dans le SI, développement de la téléphonie sur IP en complément du chat, move-to-cloud incluant les outils de collaboration online, développement des ransomwares et généralisation des EDR, extension des SOC et des capacités de surveillance des salariés, etc. Avez-vous révisé votre charte utilisateurs pour prendre en compte ces différents aspects ?



[Q86] Cyber resilience act

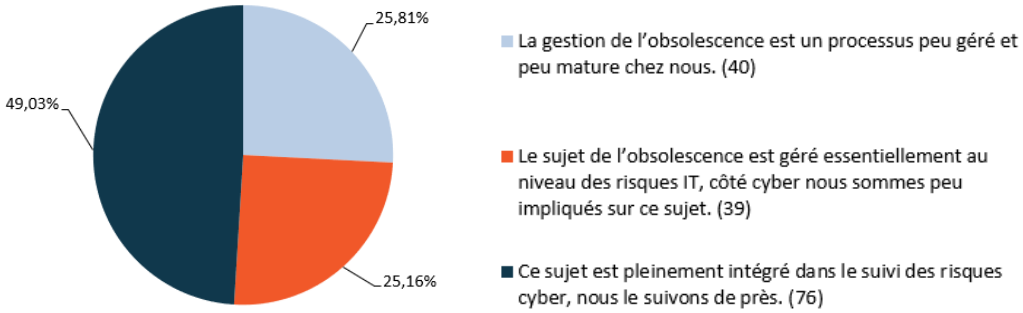
Le projet de loi intitulé « Cyber Resilience act » de la Commission Européenne vise à responsabiliser les éditeurs de logiciels et de matériels sur la sécurité de leur solution, que ce soit du logiciel classique ou sur logiciel embarqué dans des objets connectés, que ces solutions soient destinées aux entreprises ou aux particuliers. Cette approche est bienvenue, ayant tous observé une croissance importante du nombre de vulnérabilités ces

dernières années, avec une impunité totale des éditeurs, et tandis que les clients sont obligés de consacrer de plus en plus d'énergie à la gestion des patchs, avec des coûts importants et des impacts potentiels sur les activités. Est-ce que vous vous sentez pleinement concernés par ce projet de loi ?



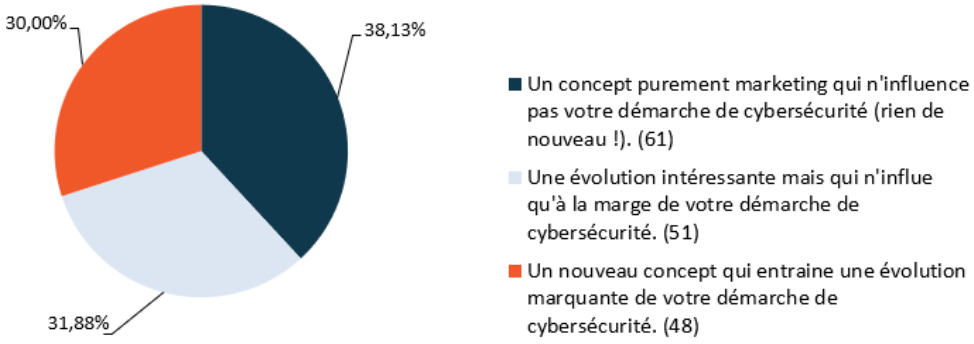
[Q87] Gestion de l'obsolescence

Votre DSI a fait des choix stratégiques dans son processus de gestion des assets, notamment sur la gestion des versions et la maintenance des assets en condition opérationnelle et de sécurité. De ces choix résulte un certain taux d'obsolescence sur vos assets, que ce soit en termes d'OS, de middlewares, d'applications, de matériels ou de tout autre composant du SI. Le sujet de l'obsolescence est généralement intégré à la gestion des risques IT et peut l'être également à la gestion des risques cyber, dans le cadre du processus de gestion des vulnérabilités. En effet, un OS obsolète ayant dépassé la date de fin de support éditeur et confronté à une vulnérabilité non patchable, devient potentiellement exploitable par des attaquants. Comment prenez-vous en compte ce sujet de l'obsolescence ?



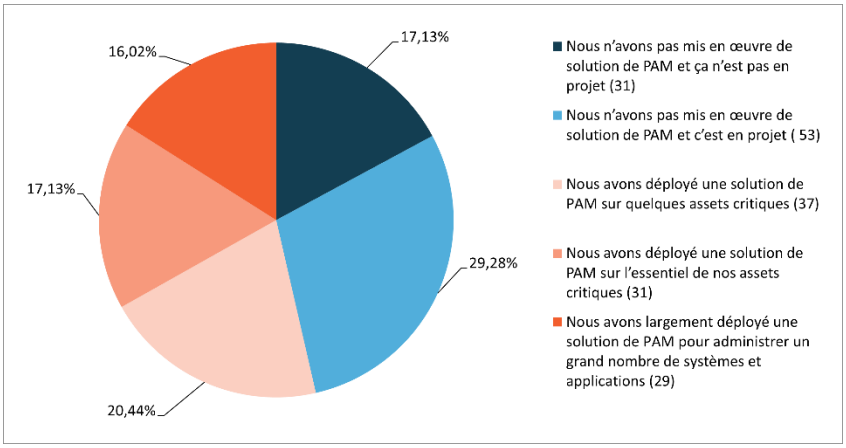
[Q88] Cyber résilience

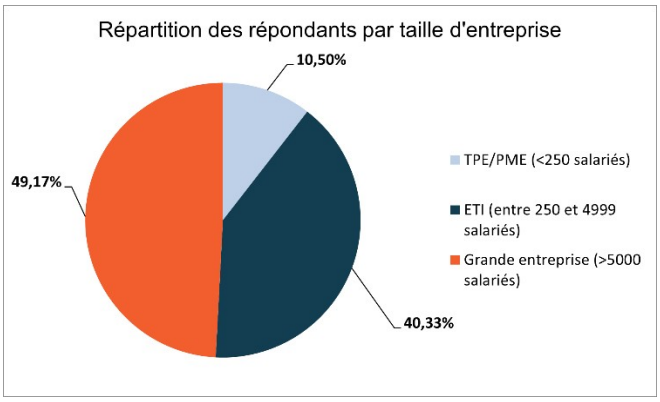
La "cyber résilience" est un terme omniprésent dans notre écosystème depuis 2 à 3 ans. Mais que se cache-t-il vraiment derrière ces deux mots ? Est-ce un énième buzz word comme nous en connaissons régulièrement dans notre environnement ? Ou, au contraire, est-ce une évolution majeure du paradigme que chaque RSSI se doit de prendre en compte ? Pour vous, dans votre contexte, que représente la "cyber résilience" ?



[Q89] Comptes à privilèges

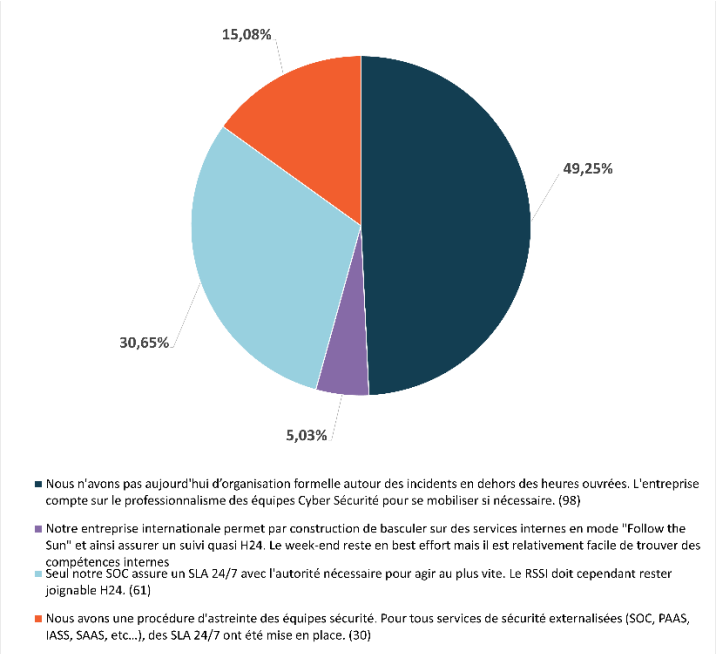
La mise en place de solutions de PAM (Privileged Access Management) permet d'améliorer la sécurité, la traçabilité et la surveillance des comptes à privilèges. Ces solutions sont en général utilisées pour protéger l'accès aux systèmes et applications critiques. Où en êtes-vous du déploiement de ce type de solution ? Où en êtes-vous du déploiement de ce type de solution ?

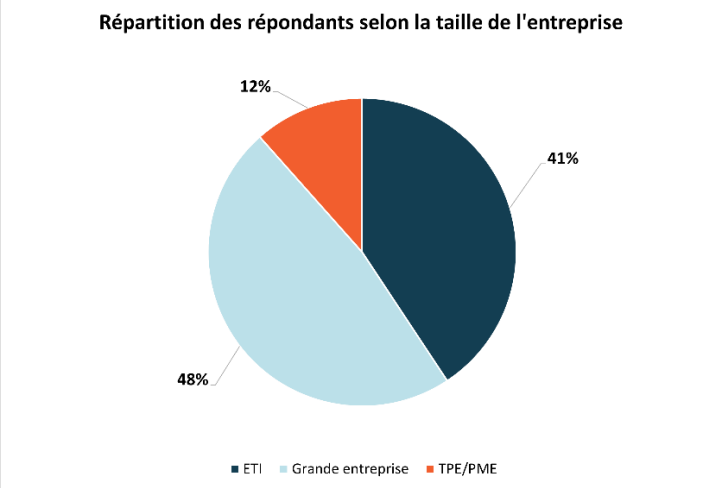


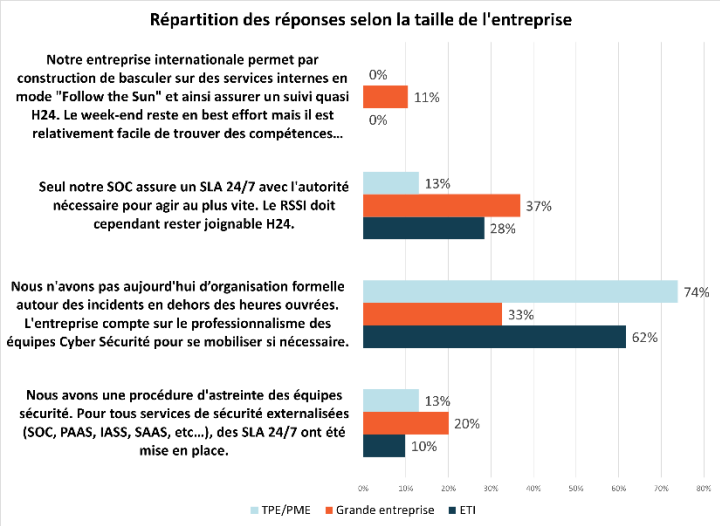


[Q90] Imprévus Cyber

Grâce à Murphy, bon nombre d'incidents arrivent en dehors des heures dites ouvrée. Dans votre organisation, comment faites-vous face à ces imprévus de nature Cyber Sécurité ?



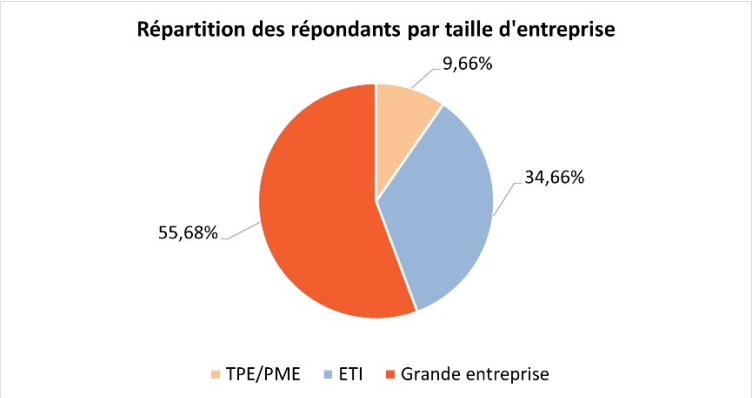


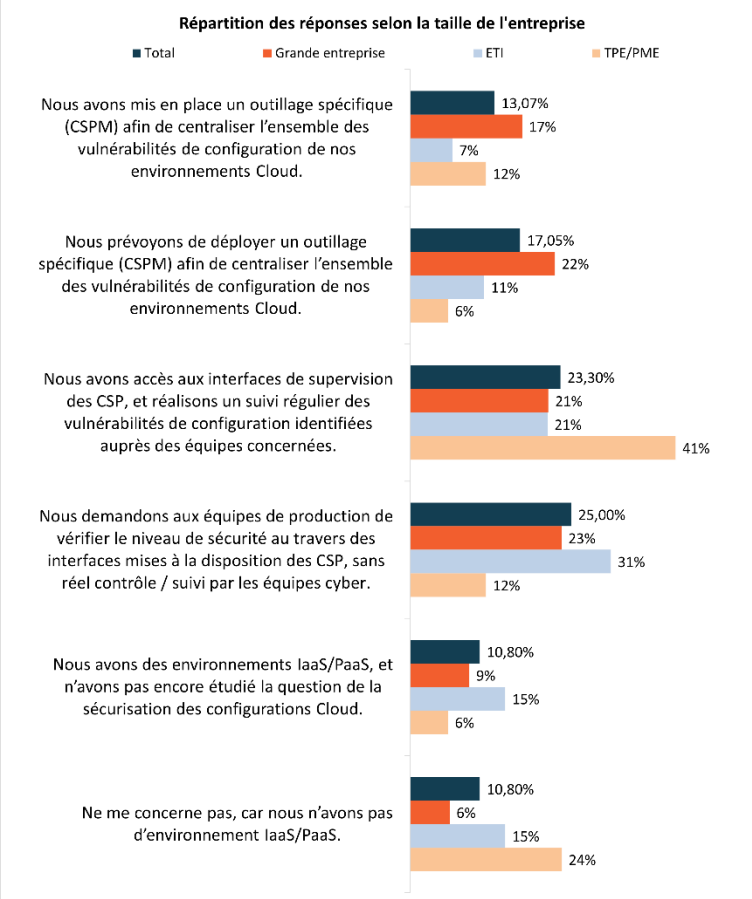


[Q91] Move-to-cloud

Le Move-to-Cloud étant à l'agenda d'un bon nombre d'organisations, avec la migration des ressources en datacenters vers du IaaS et PaaS, cela suppose de nouveaux risques au niveau de sa gestion au quotidien, et en

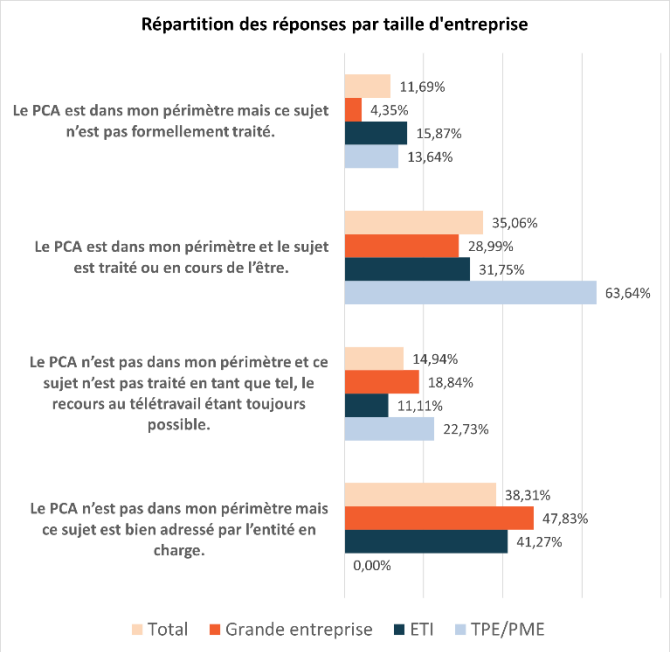
particulier de sa configuration, pour laquelle les équipes Cyber ne sont pas systématiquement sollicitées ou, lorsqu'elles le sont, ne disposent pas nécessairement des compétences Cloud requises pour accompagner les équipes de production. Comment appréhendez-vous cela ?

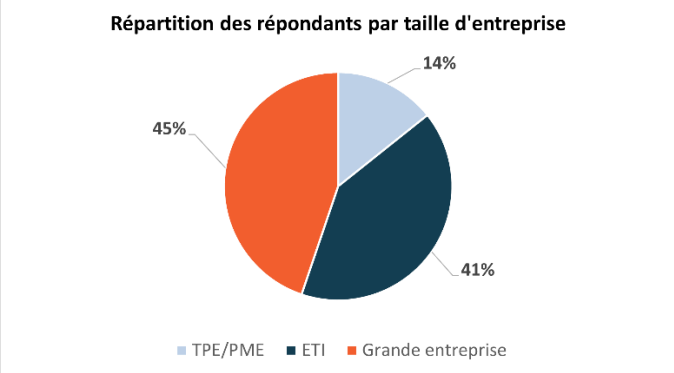




[Q92] PCA

La perspective de coupures du réseau électrique cet hiver n'est pas à exclure au regard de nos capacités réduites de production. Les entreprises encore équipées de datacenters ont toutes au moins un groupe électrogène mais concernant les sites utilisateurs, ça n'est pas toujours le cas. En ce qui concerne votre entreprise, comment ce sujet est-il traité ?





[Q93] Géopolitique et choix logiciel

Comme cela a été évoqué lors du Congrès, la géopolitique a fait son entrée dans l'agenda du RSSI dans ses choix technologiques particulièrement depuis le début du conflit Russo-Ukrainien. Cela s'est particulièrement illustré avec les recommandations de l'ANSSI à propos des risques d'utilisation des logiciels russes : Et vous comment gérez-vous ce sujet ?