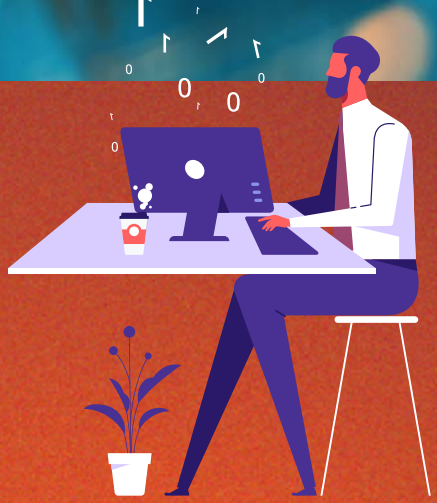
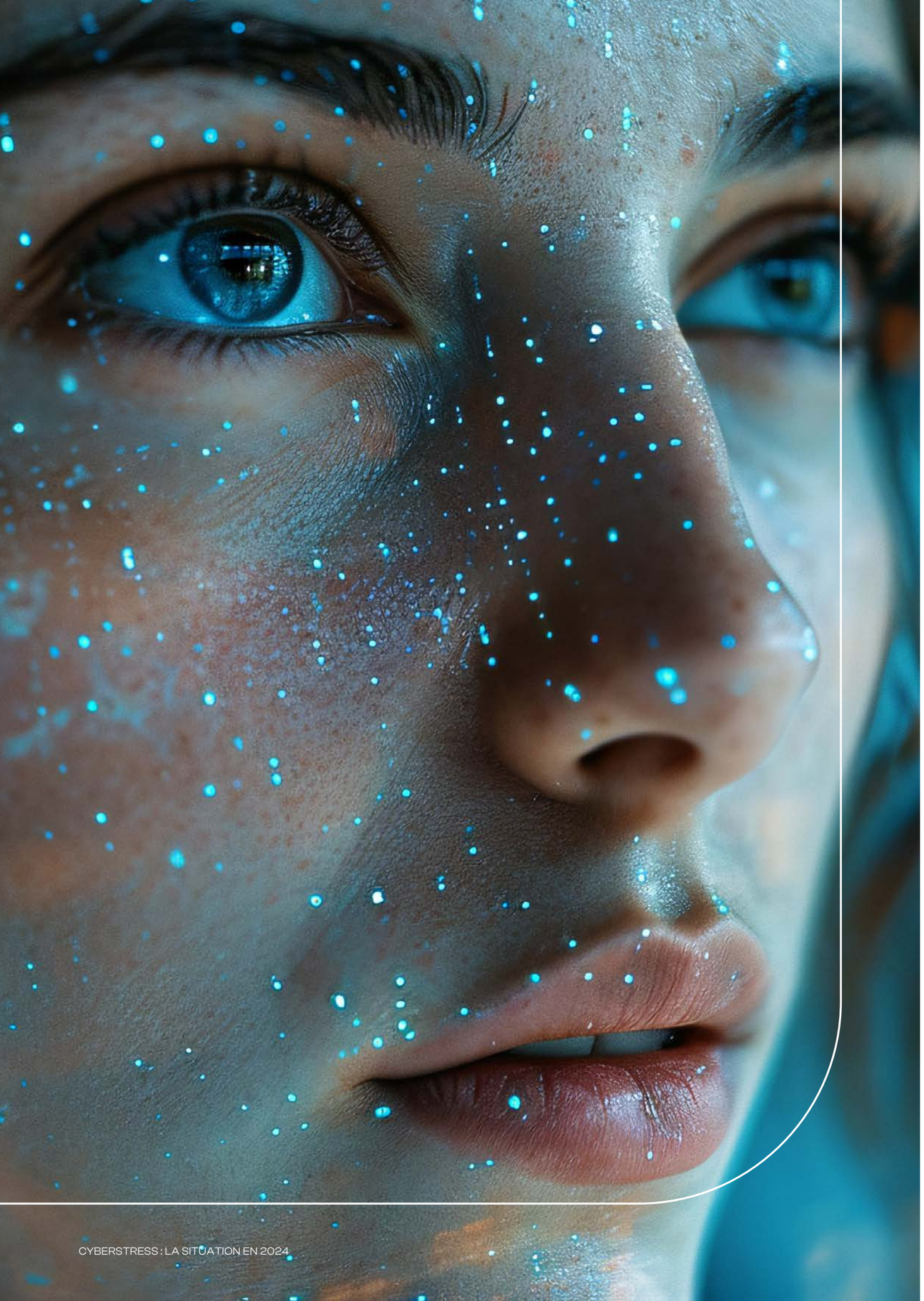
CYBERSTRESS : LA SITUATION EN 2024

Une grande étude réalisée par le CESIN et Advens



Advens
For cyber, people & planet

CESIN



En synthèse

Si, à première vue, la situation des responsables Cyber vis-à-vis du stress s'améliore, de nombreux défis persistent. Tout l'enjeu consiste à ce que le stress, inhérent au métier, soit pris en considération à son juste niveau. Le but ? Qu'il n'influe négativement ni sur le niveau de sécurité global de nos organisations ni sur la qualité du travail des responsables Cyber.

Point positif, les résultats montrent une diminution de 10 points des responsables Cyber stressés. Cela traduit une forme de maturité du rôle de responsable Cyber et de la façon dont il est perçu par l'organisation. Cette évolution est probablement due à une meilleure compréhension du risque Cyber par les entités, à une prise de conscience des directions générales et à un renforcement des moyens alloués à la Cyber.

Bonne nouvelle également, les responsables Cyber en poste depuis moins de deux ans sont moins stressés, sans doute parce qu'ils sont mieux préparés par leur formation et/ou parce qu'ils bénéficient d'un statut et de moyens qui réduisent le stress.

Mais attention, un responsable Cyber sur deux se trouve encore en situation de stress et un sur quatre en stress élevé. Bien sûr, certains facteurs de stress sont inhérents à la fonction, d'ailleurs, 85 % vivent bien l'adrénaline associée à une situation de crise Cyber. Pour autant, les responsables Cyber acceptent un peu moins de gérer des aléas en permanence (70 contre 78 en 2021) ou de faire face à une menace asymétrique (38 % l'acceptent contre 50 en 2021).

Alors finalement, est-ce si grave ?

50 % de responsables Cyber stressés, cela reste trop et surtout, cela reste impacte la sécurité ! Plus de 40 % des répondants ont par exemple fait évoluer la façon dont ils accompagnent les projets informatiques, passant d'un véritable go/no go (au pouvoir de blocage) à une simple formulation de recommandation (potentiellement non bloquantes).

À l'heure où l'augmentation de la menace, le développement de nouveaux périmètres d'attaques et la pression règlementaire viennent renforcer l'importance du rôle de responsable Cyber, il faut poursuivre les efforts pour pouvoir gérer toujours plus d'audits… sans stress démesuré !

CHIFFRES À RETENIR

85 %
des responsables Cyber vivent bien l'adrénaline du métier.

1
responsable Cyber sur 2 se dit stressé, soit une diminution de près de 10 points par rapport à 2021 (de 60 % à 50 %).

77 %
ressentent du stress lors d'un audit à l'idée d'être encore loin d'avoir fait ce qu'ils estiment nécessaire pour être au niveau de maturité souhaité.

73 %
des répondants ressentent un « décalage trop important entre la capacité à faire et les attentes de l'organisation en matière de protection contre les attaques et de gestion des risques ».

58 %
ont déjà donné un avis favorable à une posture sécurité alors qu'elle était contraire à leurs convictions par découragement ou par angoisse des négociations nécessaires à les faire valoir.

Sommaire

ÉDITORIAL

Mylène JAROSSAY, Vincent LEFRET, CESIN
Benjamin LEROUX, Advens

En 2021, la communauté des responsables Cybersécurité se penchait sur le sujet de la santé mentale au travail, grâce à une étude menée conjointement par Advens et le CESIN. Gestion du stress, résilience émotionnelle, charge mentale : quelques-uns seulement connaissaient ces termes, d'autres les vivaient sans pouvoir les nommer.

L'étude menée en 2021 se voulait la plus objective possible, basée sur une méthodologie connue et surtout sur un ensemble de données significatif et représentatif d'une bonne partie de la communauté des responsables Cyber en France.

Le constat réalisé à l'époque avait mis en avant une situation préoccupante, avec un taux élevé de responsables Cyber subissant un niveau de stress important allant pour certains jusqu'à des situations de dépression ou de burn-out. L'étude avait également mis en avant un certain nombre de facteurs générant du stress dont certains sont clairement « intrinsèques » à la profession.

Faire face à une croissance des Cyberattaques et devoir affronter des adversaires souvent invisibles

Être parfois seul à bord avec des moyens d'action limités

Être constamment en alerte et gérer des crises qui peuvent survenir à tout moment du jour ou de la nuit

Devoir convaincre sans cesse sur les risques pour faire prendre des mesures délicates et parfois impopulaires

Des états de fait évidents pour celles et ceux qui vivent ce métier au quotidien depuis des années… mais des réalités surprenantes pour les non-initiés !
Cette première étude a donc permis une mise en lumière du sujet et une prise de conscience de la part de la profession et de son écosystème. Le métier de responsable Cyber est une profession atypique en entreprise qui fait constamment face à une forme d'adversité, dans un combat asymétrique et déséquilibré sur le plan du nombre et des moyens.

Quelques années ont passé. En 2024, le sujet interpelle toujours, encore repris récemment dans les médias en se basant sur des études dont la source est potentiellement loin de nous. Ces études, souvent d'origine anglo-saxonne, ont tendance à pointer du doigt une situation très alarmante et décrivent une profession prise au dépourvu. Est-ce vraiment le cas ?

L'un des engagements pris en conclusion de l'étude de 2021 était de ré-évaluer ce niveau de stress dans le futur. Ce sujet, bien souvent abordé via un prisme individuel, se doit d'être traité de façon systémique et collective, pour apporter un éclairage à l'ensemble de la profession. Trois ans plus tard, promesse tenue, nous avons repris la démarche d'étude et nous l'avons enrichie, du fait des enseignements de la première étude et de l'évolution de la profession ces dernières années.

Voici les conclusions de l'édition 2024.

01

RAPPEL DE L'APPROCHE CHOISIE

1.1 Démarche d'étude

Cette enquête est donc une mise à jour de l'étude menée en 2021. Notre objectif est d'identifier d'éventuelles évolutions. Nous avons souhaité aussi aller plus loin, en abordant certaines nouveautés pour éclairer différemment le sujet du stress dans la Cyber. La démarche d'étude suit cette logique : elle reprend la trame méthodologique de 2021 et l'enrichit.

Cette étude est basée sur un questionnaire, transmis aux membres du CESIN, dans le but de recueillir un volume de données significatif et de refléter ainsi au mieux la situation des responsables Cyber en France en 2024.

La première section de ce questionnaire est un baromètre du niveau de stress. Mesurer ce niveau peut s'avérer délicat, car dépendant de nombreux facteurs et de tout autant de méthodes et de référentiels. Nous avons fait le choix de réutiliser l'outil retenu en 2021 : la « Perceived Stress Scale » qui permet, au travers d'un nombre de questions et d'une auto-évaluation, de donner une mesure du stress perçu par chacune des personnes interrogées, sur leur cas individuel. Ce choix permet d'une part de comparer les chiffres à 2021 et de conserver l'aspect pratique (nombre de questions réduit dans la version de la PSS choisie) et neutre (questions non liées à la situation personnelle ou à la Cyber) d'un tel outil.

NOUVEAUTÉ

Cette première section a été enrichie de 10 questions visant à évaluer l'intensité du stress vécu. Nous avons identifié une série de situations dont les professionnels de la Cybersécurité font couramment l'expérience et qui peuvent témoigner d'un stress difficile à contrôler. Ces questions visent à identifier à quelle fréquence et avec quelle intensité ces situations se produisent au sein de la communauté des répondants. Un exercice de mise en situation qui complète l'évaluation fournie par la PSS*.

La seconde section s'intéresse aux facteurs du stress ressenti. Plusieurs facteurs spécifiques au métier peuvent influer sur la charge mentale portée au quotidien par les professionnels de la Cybersécurité. Il s'agit donc de comprendre quels sont les facteurs à l'œuvre et comment ils agissent.

La troisième section est également une nouveauté de l'édition 2024. En 2021, étudier le stress était relativement précurseur. Quelques années plus tard, il nous a semblé intéressant d'évaluer le niveau de prise de conscience des répondants à ce sujet. Cette section a donc pour objectif d'identifier l'existence, ou non, de plans d'action dédiés à la gestion du stress, à titre individuel ou pour les équipes Cyber concernées. Parmi ces actions, certaines concernent directement le stress. D'autres, plus larges, concernent des pratiques de Cybersécurité, dont les répondants auraient pu décider de les faire évoluer en réponse à un certain niveau de stress.

La démarche d'étude employée se nourrit directement du cadre méthodologie utilisé en 2021, mais aussi des actions menées par le CESIN depuis 2021, ainsi que des réflexions de l'équipe en charge de cette étude.

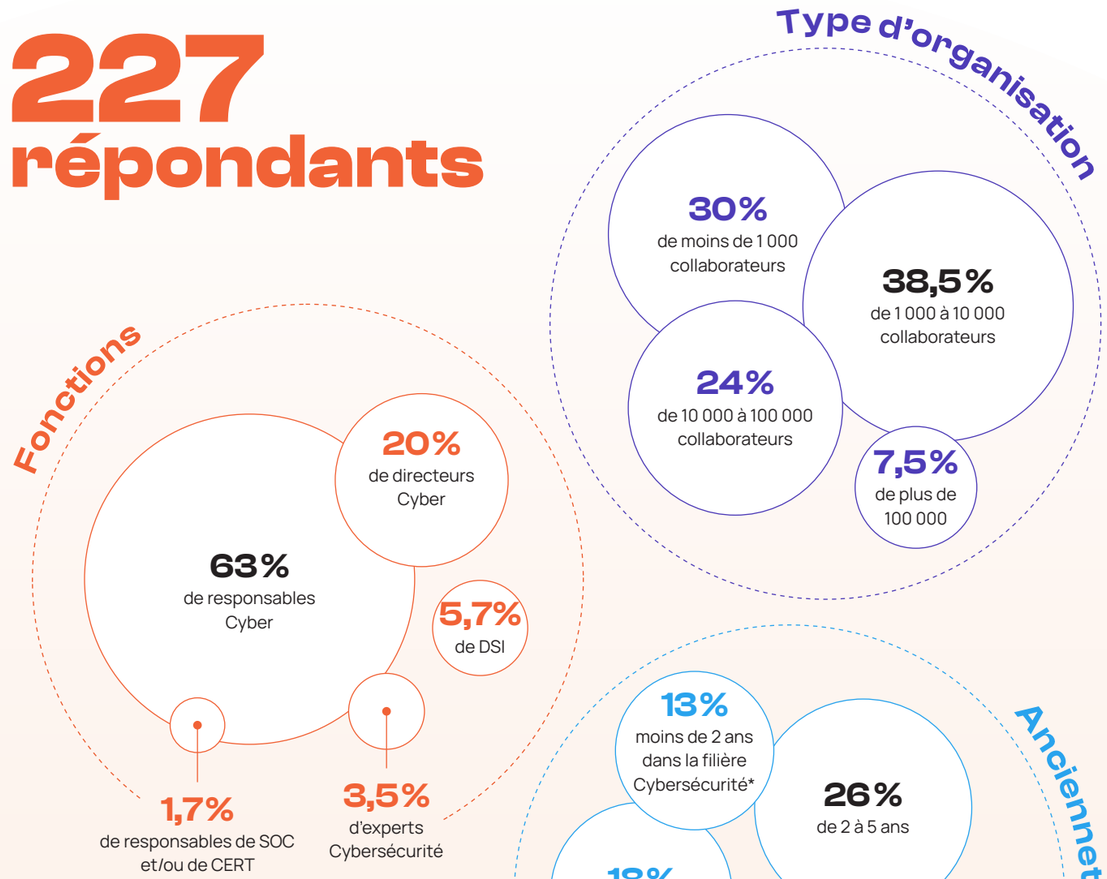
* Perceived Stress Scale

1.2 Échantillon

Le panel de répondants est issu de la communauté des membres du CESIN, qui rassemble des responsables Cyber évoluant au sein d'entreprises et d'administrations françaises.

Les réponses ont été récoltées au travers d'un questionnaire mis en ligne par le CESIN, rempli à l'été 2024.

227 répondants



2021

L'étude de 2021 avait permis de récolter les réponses de 330 répondants. La baisse d'environ un tiers peut s'expliquer par différents facteurs : un questionnaire plus long (59 questions) et donc plus chronophage, des sollicitations plus fréquentes de cette communauté (compte tenu de l'activité d'études, de sondages et baromètres menés par le CESIN) ou encore par l'actualité de l'été 2024, marqué par une intense préparation de la communauté Cyber aux Jeux Olympiques de Paris.

1.3 Recueil de témoignages

Autre nouveauté 2024 : un certain nombre de répondants ont accepté de témoigner, de façon anonyme ou non, dans le cadre de cette seconde édition.

Prendre la parole sur le sujet du stress n'est pas toujours un exercice facile. Nous remercions vivement ces volontaires pour leur apport précieux, qui permet d'une part d'illustrer ces travaux par des situations vécues, et d'avancer certaines hypothèses quant à l'analyse des résultats. Ces témoignages sont disséminés au sein du présent document.

NOTE

Cette étude vise à comprendre ce qui cause le stress ressenti, à travers le prisme du métier. Les facteurs personnels comme la situation familiale ou professionnels plus larges (les relations avec les collègues ou la hiérarchie, la trajectoire de carrière, la santé de l'entreprise, etc.) ne sont pas pris en compte, bien qu'ils puissent influer de manière générale sur le stress au travail. L'analyse porte sur une série de critères considérés comme des caractéristiques intrinsèques du métier de responsable Cyber.

VERS UN ÉTAT DE MATURITÉ OU UN ÂGE DE RAISON ?

2.1 2021-2024 : évaluation et évolution du stress perçu

Échelle PSS et résultats comparés

Déjà utilisée en 2021, l'échelle du stress perçu (Perceived Stress Scale ou PSS) est un modèle de mesure international reconnu qui permet d'évaluer de façon globale si une personne estime avoir la capacité ou non à faire face à des événements ou à des moments difficiles à vivre, sans toutefois les spécifier.

PLUS D'INFORMATIONS SUR L'ÉCHELLE EN ANNEXE

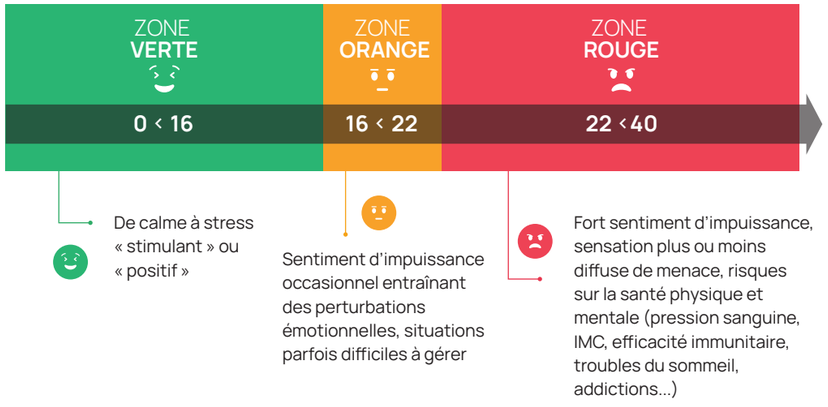
En additionnant les scores des 10 questions posées (voir détails plus loin), nous obtenons un total compris entre 0 et 40 pour chaque participant. Ces résultats permettent de situer l'individu et le collectif sur l'échelle ci-dessous.

Le score moyen du panel est de 17,56 en 2024 (contre 18,4 en 2021). Une amélioration globale de près d'un point encore plus perceptible quand on s'attarde sur la proportion de répondants en niveau de stress perçu faible : + 10 % entre 2021 et 2024.

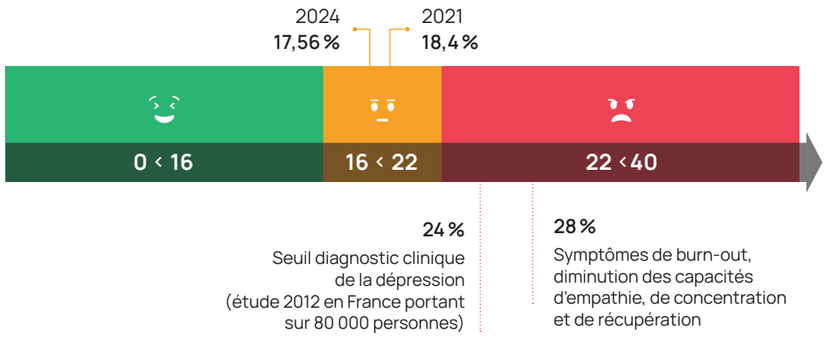
En première lecture, on constate que la moitié des responsables Cyber se positionnent en situation de stress faible, ce qui constitue un progrès de 10 points par rapport à l'étude de 2021. Il reste encore un responsable Cyber sur deux qui est en situation de stress modéré à élevé. Et près de 7 % des répondants dépassent le score de 28 sur l'échelle, indiquant un risque de dépression clinique ou de burn-out. Malgré le progrès observé entre les deux études et une tendance à l'amélioration quant au stress perçu, la situation n'est pas encore sous contrôle dans un nombre élevé de cas.

Il existe naturellement un certain biais inhérent à ce genre d'étude, les personnes en situation de stress répondant plus volontiers à ce genre d'enquête, car il s'agit sans doute pour eux d'accompagner la démarche de reconnaissance du stress dans les métiers de la Cyber… et dans le même temps, il est régulièrement dit que les populations masculines (encore en large majorité au sein des métiers de la Cybersécurité) ont tendance à sous-évaluer leur niveau de charge mentale, ce qui peut apporter un autre biais de minimisation.

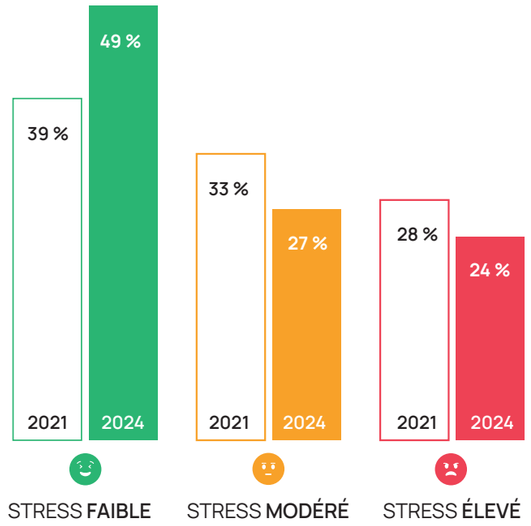
L'ÉCHELLE DE MESURE DU STRESS (PSS) →



LES RÉSULTATS EN 2024 →



↓ NIVEAUX MOYENS PERÇUS 2021 vs 2024



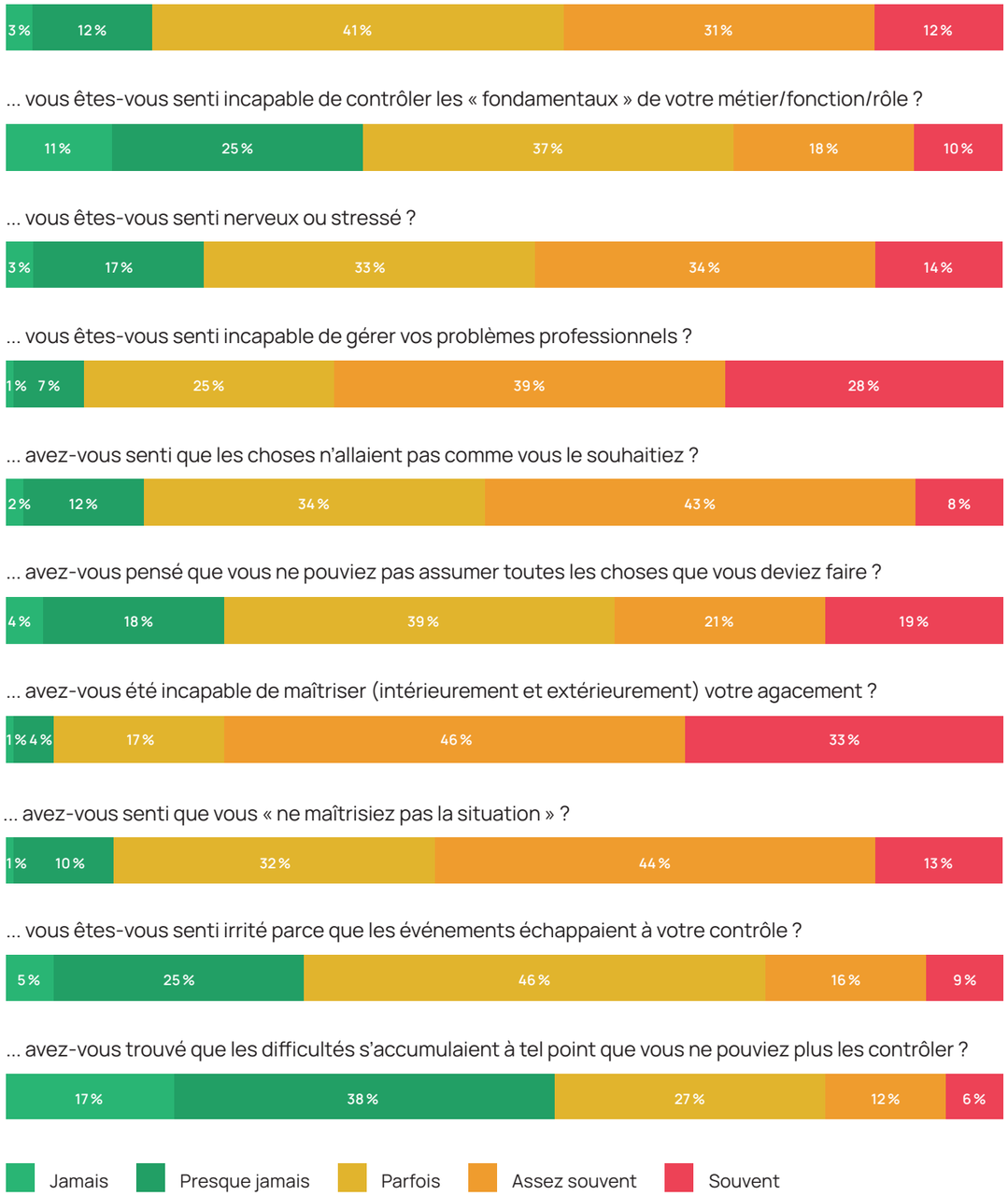
Néanmoins, il est à noter que l'échantillon des répondants est similaire à celui de 2021 en ce qui concerne la fonction exercée et les effectifs de leur entreprise. Par contre, dans l'étude 2024, un tiers des répondants sont récents dans la fonction Cyber, et n'avaient pas pu répondre à l'enquête de 2021.

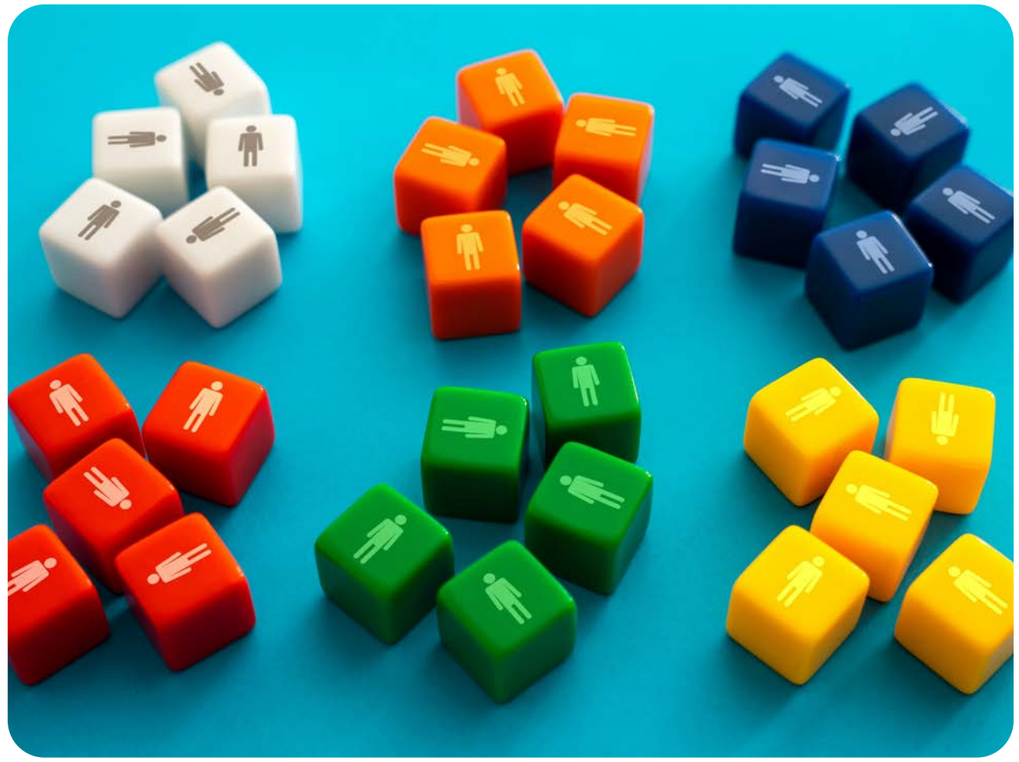
Nous pouvons ainsi remarquer que le score moyen des responsables Cyber récents dans cette filière est le plus bas.

ANCIENNETÉ DANS LA FONCTION	SCORE MOYEN
Moins de 2 ans	15
2 à 5 ans	19
de 11 ans à 15 ans	18
de 6 à 10 ans	18
Plus de 15 ans	17

Dans le détail, l'échelle de stress sur les 10 questions posées donne les résultats suivants :

Au cours du dernier mois...

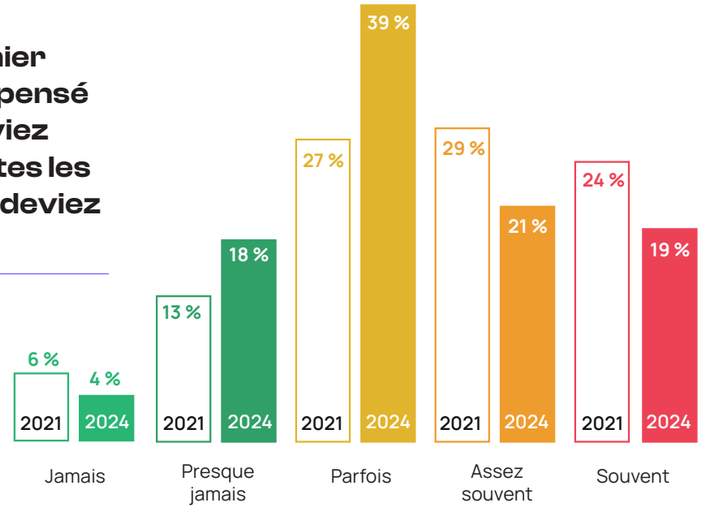




Il est assez encourageant par exemple de constater que la part de sondés qui pensent souvent ou assez souvent ne pas pouvoir assumer toutes les choses qu'ils doivent faire a reculé de 13 points.

RETROUVEZ LES RÉSULTATS COMPARÉS DES DEUX ÉDITIONS EN ANNEXE

Au cours du dernier mois, avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?



2.2 Nouveauté 2024 : en situation

BINGO DU STRESS CYBER

Je suis pris d'une crise de panique ou je me paralyse en pleine cellule de crise.	Mon N+1 m'interroge sur un incident non-envisagé : je ne sais pas répondre ou j'angoisse.	Je dois présenter un tableau de board avec des indicateurs au rouge.
Je perds mes moyens lors d'une présentation en COMEX de mon bilan et de mon plan d'actions.		Je me sens désorienté, sans réelle vision ni capacité à déterminer les directions à prendre dans ma stratégie Cyber.
Je donne un avis favorable sur une posture sécurité que je n'approuve pas par découragement ou par angoisse de négocier avec les parties prenantes.	J'angoisse lors d'un audit ou de la réponse à un questionnaire Client car je me sens encore loin du compte.	Je me sens en total décalage entre ma capacité à faire et les attentes de mon organisation en matière de gestion des risques Cyber.
	J'ai autorisé une dérogation ou un contournement d'une règle de la PSSI par peur du conflit ou par crainte d'être challengé par un collègue.	J'ai rêvé à des cyberattaques et/ou crises cyber.

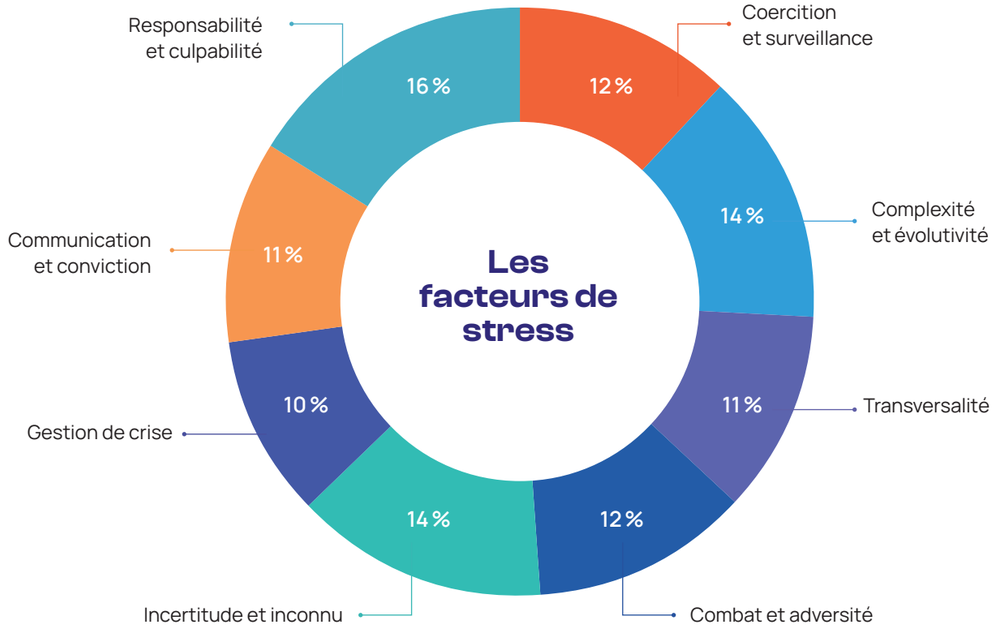
Les points saillants

- Si l'on examine les nouvelles questions relatives aux sources de stress dans l'édition 2024, on note que 38 % des responsables Cyber se sentent encore loin d'être en confiance et d'avoir atteint leurs objectifs de maturité en termes de gestion des risques et de protection.
- Cette inquiétude est renforcée lors des constats faits à l'occasion d'audits de sécurité. Le nombre de Cyber attaques réussies dans le monde forcent l'humilité. La mission Cyber est forcément complexe et difficile, et le sentiment d'être toujours éloigné de l'objectif à atteindre, peu importe nos actions, est un facteur de stress qui s'exprime clairement.
- Pour autant, les responsables Cybersécurité, même s'ils sont conscients du chemin qu'il reste à parcourir, sont plutôt confiants face à leur direction lorsqu'il s'agit de présenter leurs tableaux de bord, leur bilan et leur plan d'action. Plus de 2 responsables Cyber sur 3 ont pu ressentir néanmoins un décalage entre les attentes de leur employeur et leur capacité à faire.
- Le métier nécessite d'expliquer et de convaincre. 59 % des responsables ont pu donner un avis favorable souvent (11 %) ou de temps en temps (48 %) sur une posture sécurité qu'ils n'approuvaient pas, pour s'éviter une discussion et une « négociation » difficile ou angoissante avec les parties prenantes. On observe là un décalage, sans doute source de stress, entre la perception du risque par le responsable Cyber et ce qu'il parvient à entreprendre en actions de remédiation, pour traiter ce risque.
- Le responsable Cyber est le coordinateur des crises Cyber. Pourtant, 30 % d'entre eux ont ressenti à plusieurs reprises (2 %) ou occasionnellement (28 %) un sentiment de panique ou de paralysie lors d'une réponse à incident, dans une cellule de crise ou en dehors de la cellule. Ce résultat est plutôt surprenant.
- Le fait que 38 % des responsables Cyber rêvent occasionnellement (25 %) ou régulièrement (13 %) de Cyberattaques ou de crise Cyber montre bien l'influence des Cyber menaces sur leur vie. Cela confirme que l'on est et on reste responsable Cyber jour et nuit, devant son bureau et parfois dans son lit.

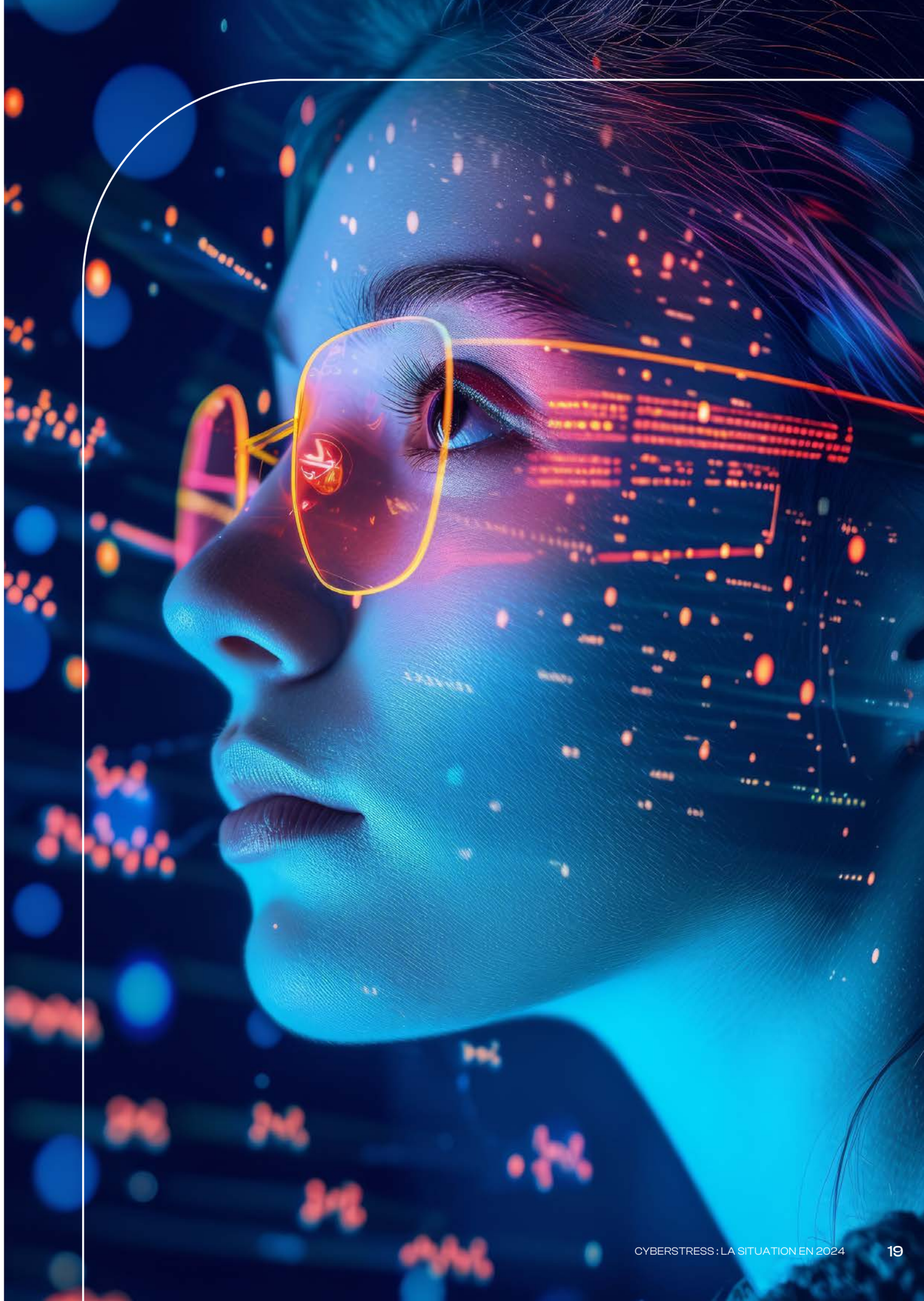
2.3 Focus sur les facteurs de stress

Pour tenter d'expliquer le niveau de stress ressenti évalué via la PSS, notre étude s'est également intéressée, comme en 2021, aux facteurs contributifs à ce stress qui seraient spécifiques au milieu de la Cybersécurité.

Les 22 questions relatives à ces facteurs peuvent être classées en 8 familles. Le poids de ces familles est calculé par rapport aux poids des facteurs de stress dans l'évaluation du ressenti des répondants : plus un facteur est considéré comme augmentant le stress, plus il a de poids dans la répartition suivante.



La répartition est assez équilibrée entre les différentes familles de facteurs de stress. La thématique de la responsabilité et de la culpabilité arrive cependant en tête : elle regroupe les questions liées au sentiment de devoir se justifier en permanence de ses actes mais aussi au regard des autres (en contexte professionnel comme personnel) face à une attaque non évitée. Ces sentiments peuvent avoir des répercussions très personnelles et un impact direct sur le niveau de stress voire de mal-être professionnel. Les thèmes relatifs à un éventuel manque d'expertise et à la nécessité de faire face à un contexte en mutation permanente sont aussi des facteurs de poids, qui peuvent d'une certaine manière engendrer un sentiment d'usure.



Analyse des facteurs de stress : principaux enseignements

LES GRANDS OUI

86 % des répondants vivent bien l'adrénaline, la pression et le sentiment d'urgence généralement associés à une crise Cyber.

81 % arrivent à s'exprimer vraiment, à se sentir en empathie, à convaincre leurs interlocuteurs.

80 % se sentent compris ou a minima soutenu par leurs proches pendant les périodes où ils gèrent des crises.

80 % trouvent leur métier singulier, dans la mesure où il fait face à des adversaires, souvent « invisibles » et malveillants, ce qui est peu usuel, car peu de professions connaissent ce contexte d'adversité.

79 % apprécient l'exercice périlleux, la balance permanente entre les décisions à prendre et les informations disponibles pour pouvoir les prendre, tout au long d'une crise.

75 % sont à l'aise avec l'étendue fonctionnelle et technique que doit couvrir le métier Cyber, qui doit assurer partout une défense efficace à tous les niveaux et sur tous les terrains.

70 % apprécient les imprévus et les aléas, nombreux dans le métier.

60 % ont le sentiment de devoir se justifier auprès des autres, voire auprès d'eux-mêmes de l'utilité de leurs actions.

57 % conçoivent la gestion du risque Cyber comme un exercice intellectuellement difficile.

LES MITIGÉS

55 % considèrent que leur situation professionnelle est incertaine, et qu'une crise majeure pourrait leur coûter leur poste.

53 % ont le sentiment d'être incompris ou d'être jugé « excessif » lorsqu'ils font des recommandations.

46 % sont sur le qui-vive en permanence, sans pouvoir déconnecter leurs pensées de leur travail, dans la crainte de la survenue d'une Cyberattaque ou d'une situation à risque.

LES GRANDS NON

86 % disent ne pas se sentir personnellement en danger, devant cette adversité et la même proportion déclare ne pas être perturbée de ne pas connaître a priori, voire ne jamais connaître, ceux qui les attaquent ou commettent une action malveillante.

83 % ne redoutant pas les situations où leur métier les amène à connaître des secrets et/ou les place dans des contextes humainement délicats ou embarrassants.

81 % indiquent ne pas se sentir découragés devant l'augmentation de la fréquence et de la puissance des Cyberattaques.

79 % ne sont pas frustrés d'être uniquement du côté de la défense et de ne jamais pouvoir riposter ou contre-attaquer.

63 % ne ressentent pas d'impuissance devant le caractère asymétrique du combat, l'attaquant ayant un net avantage sur le défenseur.

58 % ne ressentent pas de manque d'expertise technique ou méthodologique.

57 % n'éprouvent pas de sentiment de culpabilité, lié (ou pas) au regard de leur entourage et/ou leur hiérarchie, lorsqu'un incident survient, et qu'ils n'ont pu l'empêcher, le détecter et/ou en limiter l'impact.

56 % n'estiment pas difficile de devoir adapter en permanence leurs analyses et stratégies devant un contexte de menace complexe et très évolutif, de devoir apprendre et se réinventer sans cesse.

Mise en perspective

Comme en 2021, un tiers des responsables Cyber souffrent d'une image ou d'a priori parfois négatifs sur leur fonction, et un sur deux a le sentiment d'être incompris. Par ailleurs, nous observons toujours que 60 % des responsables Cyber ont le sentiment de devoir justifier l'utilité de leur action. On pourrait penser que le nombre des Cyberattaques et leur large médiatisation finissent par atténuer ce sentiment qui reste encore significatif. Il faut sans doute encore quelques années pour gommer l'image que peut renvoyer cette profession. D'autant que les façons d'aborder le métier de la Cyber ont réellement changé dans les faits et dans les pratiques.

L'expertise technique nécessaire à l'exercice du métier reste acquise pour 60 % des répondants, comme en 2021. Autant les trois-quarts des responsables Cyber font avec l'étendue des hard skills nécessaires, autant ils se sentent challengés (44 %) quant à la forte évolutivité des Cybermenaces.

La singularité du métier de la Cyber, sans cesse confronté à l'adversité, est toujours confirmée par 80 % des répondants. La « frustration » du défenseur qui subit les Cyberagressions a quant à elle diminué de 28 % en 2021 à 20 % dans cette édition.

En 2024, 70 % des responsables Cyber déclarent accepter les aléas et imprévus du métier contre 78 % en 2021. Et pourtant, le sentiment d'impuissance devant le caractère asymétrique du combat est passé de 50 % à 38 %. La capacité à mieux se défendre apparait par ailleurs dans les résultats du baromètre CESIN Opinion Way de janvier 2024, ce qui confirme la tendance. Ils étaient 28 % à se sentir découragés en 2021, devant l'augmentation de la fréquence et de la puissance des Cyberattaques. Ils sont désormais 20 % en 2024.

Un responsable Cyber sur deux se sent sur toujours le qui-vive et sans droit à la déconnexion, cependant la tendance est à l'amélioration en passant de 53 % à 46 %. Cela correspond sans doute à l'augmentation progressive de la taille des équipes Cyber. Mais finalement lorsque la crise survient, à toute heure, et qu'il faut la gérer, 85 % des responsables Cyber vivent bien l'adrénaline, la pression et le sentiment d'urgence, inhérents à la majorité des crises Cyber.

Il est intéressant d'observer que le sentiment de culpabilité en cas de survenue d'un incident que l'on n'a pas empêché, détecté et/ou limité en impact, a plutôt diminué passant de 48 % à 43 %, même si ce chiffre reste relativement élevé.

Globalement, les facteurs de stress analysés en 2021, restent toujours présents dans l'étude de 2024, les responsables Cyber sont en attente de reconnaissance et pourtant assument un peu mieux les secousses propres au métier.

REGARDS
sur les résultats

« La maturité aide à une meilleure prise de recul »

Vincent Lefret

On remarque que le niveau de stress pour les personnes ayant moins de 2 ans d'expérience dans la fonction est faible et qu'ensuite il y a un pic sur l'ancienneté entre 2 ans et 5 ans pour ensuite descendre lentement avec le temps.
La maturité dans la fonction Cyber semble permettre de mieux appréhender les différents facteurs liés au stress. Cela peut aller d'une meilleure connaissance de soi à une meilleure maîtrise des missions notamment de la gestion de crise qui est mieux appréhendée avec l'expérience que ce soit grâce à des exercices ou la mise en situation forcée.

Enfin, la maturité permet accepter d'être dans une obligation de moyen et non de résultat.

« Vers le mieux »

Benjamin Leroux

Mon sentiment général est celui d'une forme d'apaisement. On observe une réduction de 10 points du pourcentage de personnes en stress "préoccupant". Quand je relie cette information à cette étude sur le métier/la position/le salaire du responsable Cyber (en savoir plus), j'ai l'impression que bon nombre d'entre eux ont atteint une sorte de palier, une forme de maturité ou « d'âge de raison. »
J'aurais donc tendance à avoir une première lecture optimiste de ces données.

Cette impression encourageante est renforcée par l'analyse des facteurs de stress, pour lesquels la situation a assez peu évolué, voire s'est améliorée : moins de frustration par rapport à la nature combattive du métier, face à un attaquant invisible et pernicieux ou face à un contexte qui évolue tous les jours.
Enfin, la nouvelle section sur les situations vécues montre aussi que les responsables Cyber ne rêvent pas tous de crise Cyber ni ne perdent leurs moyens face à la crise ou devant le COMEX.

Cependant, il reste encore du chemin à accomplir, notamment pour que cette situation d'apaisement soit une réalité partout. C'est surtout nécessaire dans les structures les plus modestes, au sein de certaines desquelles les conditions ne sont pas réunies pour permette au responsable Cyber d'être serein..

« Des solutions existent »

Mylène Jarossay

Les chiffres montrent une amélioration pour la profession, qui est davantage dans la lumière, davantage connue et reconnue ces dernières années. A travers les deux études et l'évolution constatée, nous commençons à percevoir les contextes qui sont les plus grandes sources de stress. Et le fait de comprendre ces situations permet de réfléchir aux pistes d'amélioration.

Pour le moment, en matière d'actions de remédiation face au stress, les mesures sont encore balbutiantes. A cela deux exceptions :

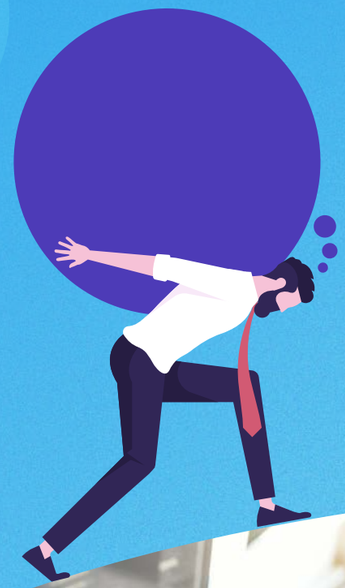
- Le fameux GO/NO transformé en recommandations entre dans les mœurs (44%) et c'est très bien car c'est une posture plus constructive sur les projets, et cela positionne le responsable Cyber en contributeur actif plutôt qu'en juge.
- Les astreintes, qui sont un moyen de ne pas être tout le temps sur le qui-vive, commencent à se déployer (44%). Il faudrait militer pour que ça devienne une évidence dans toutes les organisations.

Ces efforts d'atténuation du stress sont sans doute plus profonds qui n'y parait. Ces deux approches, d'une part transforment le responsable Cyber en facilitateur pour faire face au risque, d'autre part lui accordent un temps de respiration.

Il y a clairement une place pour construire un programme plus ambitieux afin de revisiter et d'améliorer d'autres situations de stress mais c'est un indice, très concret, d'une posture au travail qui évolue.

03

DES DIFFICULTÉS ENCORE BIEN PRÉSENTES



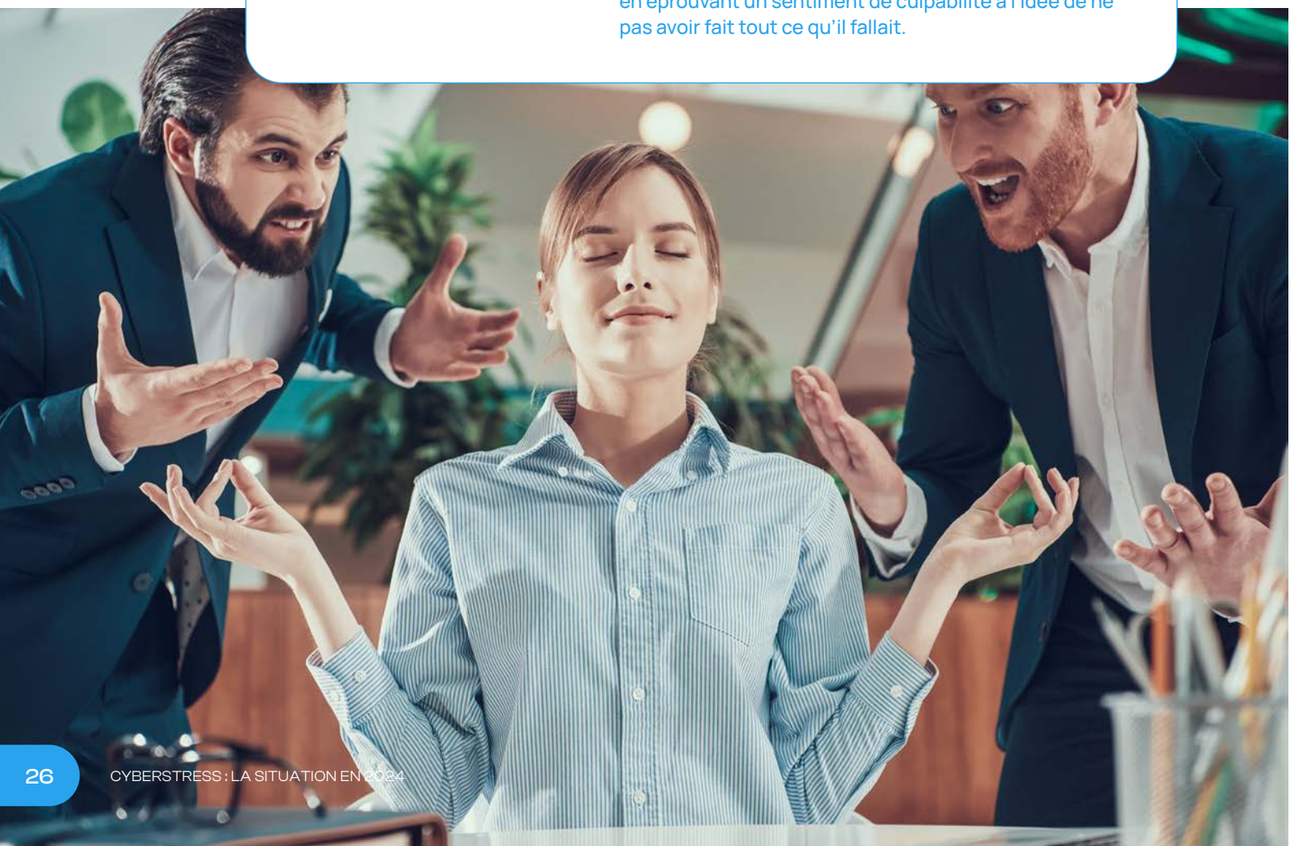
3.1 Un métier qui interroge le rapport à la crise

Même si en majorité, la gestion de crise semble maîtrisée, 30 % des responsables Cyber se sont déjà sentis en situation de panique pendant une crise. C'est bien souvent le responsable Cyber qui est le pilote des crises. A ce titre il doit donc «rassurer» tout le monde et imprimer le tempo de la gestion de crise dans l'efficacité et la sérénité. Il y a donc sur ce critère à travailler avec certains responsables Cyber pour garantir la « bonne » réaction en situation de crise.

Jérôme POGGI

Responsable de la sécurité des systèmes d'information (RSSI), Ville de Marseille

> Le RSSI est mis sous pression car il faut sécuriser le système d'information (SI), sans parfois en avoir vraiment des moyens. Il est vu comme un empêcheur de tourner en rond alors qu'il vit avec l'épée de Damoclès de la compromission du SI au-dessus de la tête. J'en ai fait la malheureuse expérience en avril 2020.
>
> L'incident provoque un stress particulier, très important. Psychologiquement, c'est très dur, notamment l'étape où il nous revient de déclarer que le SI est compromis. La situation est d'autant plus compliquée que l'on redoute d'être traité comme un fusible et débarqué tout en éprouvant un sentiment de culpabilité à l'idée de ne pas avoir fait tout ce qu'il fallait.



3.2 Une tâche d'ampleur

Le sentiment d'être loin du compte, courant dans notre métier, se confirme. Les audits sont des révélateurs du chemin qu'il reste à parcourir, tout comme le suivi des roadmaps.

2 responsables Cyber sur 3 ressentent occasionnellement ou souvent un décalage entre ce qu'ils sont en mesure de faire et les attentes de leur organisation. Le responsable Cyber serait ainsi un Sisyphe qui ne verrait jamais l'aboutissement de sa mission et devrait s'en faire une raison.

Jean-François LOUAPRE

RSSI, AGRIAL

> **Et si on stressait à tort ?**
> Au fil de mes expériences à différents postes de RSSI, dans des entreprises de taille, d'activités et de maturité variées, il m'est régulièrement arrivé de me demander si certains collègues ne s'inquiétaient pas pour de mauvaises raisons. J'en vois trois principales.
>
> Tout d'abord, un certain nombre de responsables Cyber ont peur pour leur poste. La crainte d'être remercié après une attaque est présente dans certains esprits pourtant, ce cas de figure est extrêmement rare. En cas de gestion d'une crise Cyber, le RSSI est plutôt vu comme celui qui a la capacité de sauver l'entreprise victime.
>
> Cette posture de sauveur peut parfois se muer en **posture de héros**... Un héros déraisonnable qui pense être en mesure de sauver le monde seul, toujours sur le pont, disponible toute l'année, 7 jours sur 7. Ce n'est tout bonnement pas viable. Le RSSI peut jouer un rôle clé pour répondre à un incident. C'est indéniable. Il peut insuffler une dynamique positive pour faire avancer la Cyber dans l'entreprise. Mais il ne peut pas tout faire seul.
>
> Enfin, il faut éviter de vouloir être sur tous les fronts. Rappelons un concept de base qui a tendance à être oublié : on ne peut pas tout sécuriser ! Il faut donc essayer, ce qui n'est pas toujours facile, j'en conviens, de concentrer son énergie sur les risques majeurs. Cela suppose d'accepter de laisser de côté une multitude de sujets qui conduisent à l'éparpillement puis à l'épuisement, voire au découragement.

3.3 La tentation de réduire le niveau d'exigence

L'étude révèle que les responsables Cyber concèdent parfois des dérogations (35%) ou acceptent des postures sécurité qu'ils n'approuvent pas (58%), par crainte du conflit ou de la négociation. Il faut faire la part des choses sur ce résultat. Ce n'est pas une anomalie de devoir accorder des exceptions par rapport à une politique. Ces exceptions peuvent être fondées.

Mais si cela est fait pour des raisons d'évitement psychologique, c'est plus ennuyeux car l'évaluation du bénéfice-risque de chaque posture fait partie du métier donc cela ne devrait pas coûter d'avoir à convaincre. Un médecin prescrirait-il de guerre lasse des antibiotiques à un patient qui n'en démordrait pas, alors qu'il est convaincu que les antibiotiques ne sont pas indiqués pour le cas en question ?

PARTIE 4

LES PERSPECTIVES MÉTIER

4.1 Vigilance

Le niveau moyen de stress perçu par les responsables Cyber s'améliore. Faut-il pour autant crier victoire et considérer que le problème est réglé ? Cela serait trop simple. La profession doit rester vigilante et cela tombe bien, c'est l'une de ses caractéristiques !

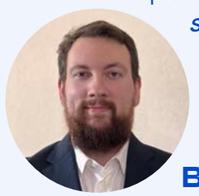
La pression entourant les métiers de la Cybersécurité ne retombera pas subitement. Et les exigences associées ne se simplifieront pas non plus.

D'une part, les attaquants ne faibliront pas : la cybercriminalité est lucrative ou stratégique quand elle est mise en œuvre à des fins géopolitiques. La menace plane sur des périmètres de plus en plus larges, grâce notamment à la démocratisation des moyens d'attaques et aux innovations liées à l'intelligence artificielle.

D'autre part, le cadre règlementaire s'étoffe considérablement avec la directive NIS 2, sans oublier DORA, son pendant pour certains métiers, le règlement européen sur la cyberrésilience (Cyber Resilience Act) ou encore celui sur l'IA (AI Act). Ces textes insistent sur l'importance des audits et du contrôle de la sécurité des fournisseurs et multiplient le nombre de structures concernées par des exigences Cyber. Ils augmentent donc mécaniquement le besoin de profils en Cybersécurité, notamment de responsable Cyber.

Le quotidien dans une PME

Le quotidien d'un RSSI dans une PME ressemble souvent à celui d'un homme-orchestre. Jonglant entre la mise en place de systèmes de sécurité et de conformité, la gestion des incidents, la formation des employés et la veille technologique, ce professionnel se retrouve fréquemment seul face à une multitude de responsabilités, façon « one man army ». Contrairement aux grandes entreprises, les PME disposent rarement d'une équipe dédiée à la cybersécurité. Le rôle de RSSI dans les PME, parce qu'essentiel, s'accompagne d'un niveau de stress et de responsabilités considérables. Ce stress est d'abord un symptôme, comme décrit par Yann Ofanowski, le coach qui avait travaillé sur l'étude de 2021 : ***« C'est le symptôme d'un système organisationnel sous pression où l'entreprise dans son ensemble va, de façon plus ou moins consciente, repousser la responsabilité du danger et de l'incertitude cyber vers les gardiens du temple, représentés par la fonction cyber. »***



Baptiste Leterrier
RSSI, United Heroes

4.2 Valorisation de la filière

38 % des sondés souffrent de l'image et des a priori parfois négatifs autour de leur fonction, qui peuvent leur compliquer la tâche voire provoquer un sentiment d'isolement. À la vigilance des responsables Cyber, doivent donc s'ajouter des travaux de valorisation de la filière et des métiers de la Cybersécurité. Parmi ces travaux, on peut noter les initiatives intéressantes visant à faire connaitre toutes les facettes des professions proposées par la filière Cybersécurité, comme celle de l'ANSSI[1] ou de l'école Guardia Cybersecurity School[2]. Cette dernière est d'ailleurs un bon exemple des écoles et formations dédiées à la filière qui ont émergé récemment. Malgré tout, le sujet des « soft skills » et celui de la gestion du stress sont encore absents des programmes de ces formations.

À cette mise en avant académique s'ajoute l'intérêt croissant des médias pour la Cyber au sens large. De plus en plus d'interviews ou d'articles sont consacrés à ses professionnels.

On peut cependant regretter que certaines thématiques soient plus mises en lumière que d'autres. Le hacker éthique, qui simule les agissements des attaquants à grand renfort de techniques sensationnelles, a ainsi plus de chance d'attirer l'attention des journalistes que le responsable Cyber qui déplace des montagnes en interne pour obtenir davantage de ressources !

Les objectifs importants de recrutement et de renforcement de la filière Cybersécurité nécessitent d'aller plus loin dans l'attractivité de la filière pour l'étendre à d'autres directions ou entités dans les organisations. Dans le cas des entreprises ayant des systèmes industriels (OT), la guerre des talents porte désormais sur les « RSSI OT ». S'il faut aller puiser cette expertise dans les rangs des équipes industrielles, il vaudrait mieux que le métier ne véhicule pas l'idée d'un stress insoutenable.

4.3 Sensibilisation

Seule une petite moitié (43 %) de la profession se dit sensibilisée au sujet du stress. Et seulement un quart des répondants a sensibilisé sa hiérarchie. En revanche, 51 % des sondés indiquent avoir sensibilisé leur équipe à cette thématique. Ces chiffres sont plutôt encourageants si on les compare avec ceux de 2021. Cependant, la proportion de stress ayant des conséquences délétères sur les plans personnel et professionnel reste trop importante pour se réjouir complètement.

Dès lors, les travaux de sensibilisation doivent se poursuivre. Ils peuvent être faits de façon unitaire, locale, dans chaque organisation mais une démarche collective et globale, grâce à une association comme le CESIN par exemple, aurait davantage d'impact. La formation est également un levier à actionner, via les circuits classiques de formation (école, organisme de formation), ou via des parcours pensés pour des populations dédiées, comme dans l'exemple du CERT-Aviation.

Marion Buchet
Responsable, CERT Aviation

La gestion des émotions et plus particulièrement du stress est une notion mésestimée dans l'éducation, ce qui en fait un problème pour beaucoup à l'âge adulte. Cependant, même si on observe évidemment une variabilité interindividuelle, c'est comme beaucoup de choses : une histoire de motivation, d'apprentissage et d'entraînement. C'est pour cette raison qu'au CERT Aviation, nous proposons une formation à la gestion du stress pour nos membres.

(1) **ANSSI :** https://cyber.gouv.fr/publications/panorama-des-metiers-de-la-cybersecurite
(2) **Guardia Cybersecurity School :** https://guardia.school/metiers

4.4 Outils

En complément de la sensibilisation, il faut parfois recourir à des outils ou des actions qui permettent une réponse plus rapide face à une situation de détresse. Sur ce point, les travaux sont encore à mener, car plus de la moitié (53 %) des responsables Cyber n'ont pas prévu de plan d'action particulier pour gérer le stress des membres de leur équipe. Certes, un tel plan d'action n'est pas toujours nécessaire, cependant, l'ensemble des chiffres de cette étude permet d'affirmer qu'il existe des situations nécessitant des réponses adaptées. Il faut qu'elles puissent être identifiées et mises en place.

La profession semble donc à première vue mal dotée en matière d'outils pour faire face au stress. Mais elle a su s'adapter et adapter d'autres outils en réponse à ce phénomène.

Le premier d'entre eux est l'astreinte. Trop souvent, le responsable Cyber doit, par manque de moyens financiers ou humains, être disponible en permanence pour réagir en cas d'alerte notamment. Face à cette situation, plus de 43 % des répondants ont mis en place un dispositif d'astreinte partagée entre plusieurs personnes. C'est un outil répandu dans de nombreuses professions dont les effets sur le niveau de stress vécu peuvent être tout à fait positifs et immédiats.

Des pistes pour faire face au stress ?

Au chapitre des solutions, il est donc important de rappeler l'intérêt de certains outils classiques. Les tableaux de bord en sont aussi un bon exemple. Pour certains, s'ils sont « mal » utilisés, ils deviennent source d'angoisse car ils peuvent être synonymes d'incapacité à faire avancer un plan d'action, d'impossibilité à remédier à des failles, etc. Un retravail des indicateurs ou de leur méthode de calcul, pourrait convertir ses tableaux de bord en de véritables guides, pour aider le responsable Cyber, sa hiérarchie et son équipe, à avancer en sérénité.

Autre outil à réinventer pour contribuer à dompter le stress : l'exercice de crise. 30 % des responsables Cyber se sont sentis angoissés et démunis face à leur chef en présence d'un incident qu'ils n'avaient pas imaginé. Évidemment, il est illusoire de penser prévoir tous les scénarios d'incidents, et de se tester face à chacun d'entre eux. Néanmoins, l'exercice de crise peut aider à se rassurer :

- si on fait preuve de suffisamment d'imagination dans la conception du scénario de l'exercice de crise ;
- si on intègre à l'exercice en lui-même une réflexion voire une formation à la pression et au stress induits par la crise.

> Nous avions construit au sein des équipes Cyber la description d'une série de biais qui interviennent pendant les crises et qui contribuent à rendre la situation angoissante. C'est une bonne piste pour déminer le sujet. Connaître les biais, c'est arriver à prendre du recul face à la crise et cela désamorce les sentiments de panique ou d'égarement. On travaille encore peu sur ces aspects-là lorsqu'on fait des exercices de crise.
>
> **Mylène Jarossay**

Le stress, une affaire de management ?

Le stress est un sujet récurrent au sein de la communauté des professionnels de la Cybersécurité. Cette étude montre que de nombreux responsables Cyber font encore l'expérience d'un stress aux effets négatifs. D'autres métiers de la Cyber, comme ceux du CERT et de la réponse aux incidents, sont également concernés au premier chef. Les exemples ne manquent pas dans une filière régulièrement exposée à l'urgence, à la crise et à l'incertitude.

Cette étude, comme la précédente édition, n'a pas pour objectif premier de remonter à une cause première mais plutôt de **mesurer l'intensité du stress** et d'en évaluer les conséquences sur le métier.

Pourtant, les travaux complémentaires menés par le CESIN lors de groupes de parole pilotés par Vincent Lefret et Yann Ofanowski après la mesure de 2021 et/ou par Advens lors de missions d'accompagnement client dédié au sujet, ont permis de formuler une hypothèse. **Le stress serait l'arbre qui cache la forêt de deux sujets clés : le management et le leadership.**

On peut considérer le stress en contexte professionnel comme le fruit d'un décalage entre la vision que nous avons de notre propre valeur et les attentes que notre direction et nos collègues vis-à-vis de cette valeur.

→ Ainsi, la figure du responsable Cyber est perçue comme un super héros capable de tout protéger, alors que ce professionnel de la Cyber a conscience que la tâche est trop vaste pour un seul individu.

→ On attend du responsable Cyber une posture stratégique mais souvent, pris dans l'opérationnel, il peine à prendre de la hauteur en voulant être sur tous les fronts.

→ Enfin le responsable Cyber, comme d'autres cadres, doit faire face à un continuum de complexité, fruit d'organisations complexes, dans une société complexe, dans un contexte géopolitique complexe…

Ce décalage contribue au stress, comme il le ferait dans n'importe quelle autre filière professionnelle. Cependant, cette étude a souligné l'exposition du secteur de la Cyber à des facteurs augmentant le niveau de stress. Il est donc d'autant plus important dans ce contexte de travailler sur les causes de ce décalage, car les facteurs intrinsèques au métier de responsable Cyber ne changeront pas : les attaquants resteront toujours des attaquants !

Les causes du stress ne sont pas à chercher dans la technique de la Cyber. Il faut plutôt se pencher sur les bonnes pratiques en matière de management et de leadership.

Choisir ses priorités, ne pas se disperser, ménager les attentes des clients internes et des clients externes, aider les membres de son équipe à faire face à une charge de travail importante, inclure les autres directeurs dans la trajectoire Cyber que l'on estime être la bonne, convaincre le top management… Autant de défis qui, relevés, peuvent avoir un impact extrêmement positif sur le niveau de stress des responsables Cyber. Et pour y arriver, nul besoin de nouvelles compétences en méthodes d'attaque, de cryptographie post-quantique ou de sécurisation de l'IA ! La boite à outils est à puiser ailleurs, dans les soft skills nécessaires à un poste de responsable, de manager ou de dirigeant. C'est peut-être une suite logique de l'évolution et de la montée en maturité de la fonction Cyber dans les organisations.

PARTIE 5

CONCLUSION

Un mot de CONCLUSION

Comme pour la première édition en 2021, nous avons eu plaisir à travailler sur la question si riche du stress dans la Cybersécurité. Ce sujet, intimement lié à notre quotidien, nous rappelle l'importance de l'Humain dans le domaine de la Cybersécurité. Plus globalement il nous rappelle que chacun d'entre nous n'est qu'un humain au travail. Nous espérons que ces travaux aideront le plus grand nombre à prendre conscience de ces problématiques, qu'il s'agisse de résilience émotionnelle, de pratiques de management ou de postures de leadership.

Pour Advens,travailler sur la dimension humaine de la cybersécurité et sur les façons de surmonter les difficultés que l'on rencontre dans une carrière dans la Cyber est pleinement en phase avec la raison d'être de la société. **La vulnérabilité est notre métier et notre cause : nous protégeons de ses risques, nous combattons ceux qui tentent de l'exploiter et nous la valorisons comme un potentiel individuel et collectif de création de valeur.**

Comment agir ?

Si cette lecture a éveillé votre intérêt pour la question du stress ou mis en lumière des difficultés au niveau de votre stress, celui de certains membres de votre équipe, de vos collègues, etc., voici quelques actions à lancer sans plus attendre. Elles peuvent être réalisées à titre individuelle ou de façon collective :

- **Mesure du stress :** utiliser l'échelle PSS et le questionnaire en 10 questions pour refaire le point sur le niveau de stress perçu ;
- **Retour d'expérience :** revenir sur les situations récemment vécues où le niveau de stress n'a pas été contrôlable ;
- **Plan d'action :** essayer d'identifier le point commun à ces situations (gestion de crise, encadrement et management, posture de leader, surcharge de travail, etc.) et construire un plan d'action dédié, en se faisant aider si besoin (direction RH, CESIN, Advens, professionnels du sujet, etc.) ;
- **Réagir à temps :** Il ne faut pas attendre qu'il y ait urgence (RPS) et savoir se tourner rapidement vers la sphère médicale et/ou les services RH de son entreprise.

ANNEXES

Échelle de mesure du stress

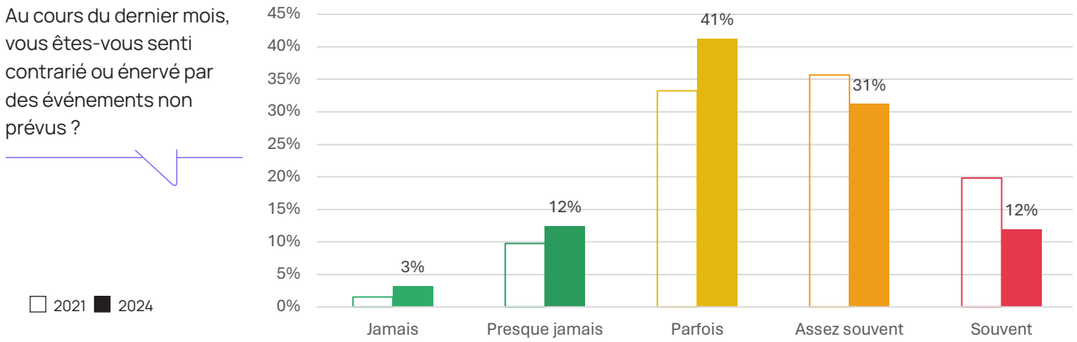
Depuis que les chercheurs se sont intéressés à l'évaluation du stress, les méthodes ont évolué car la conception même du stress s'est modifiée. Dans les années 80, les chercheurs se sont aperçus que l'impact d'une situation supposée stressante n'était pas le même selon les personnes et surtout que « l'évaluation que l'individu portait sur cette situation était déterminante sur son vécu » (Lindsay & Norman, 1980).

En 1983, Cohen, Kamarck, et Mermelstein proposent un questionnaire de stress perçu basé sur le modèle théorique transactionnel : la Perceived Stress Scale (PSS) a pour objectif « d'évaluer le degré selon lequel les personnes interrogées estiment que leur vie est imprévisible, incontrôlable et surchargée. » La PSS permet d'évaluer d'une façon globale si une personne estime avoir la capacité à faire face ou non à des événements ou à des moments difficiles à vivre, sans toutefois les spécifier. Cohen, Kamarck, et Mermelstein (1983) présentent trois versions, en 14, 10 et 4 items sous les appellations de PSS14, PSS10 et PSS4.

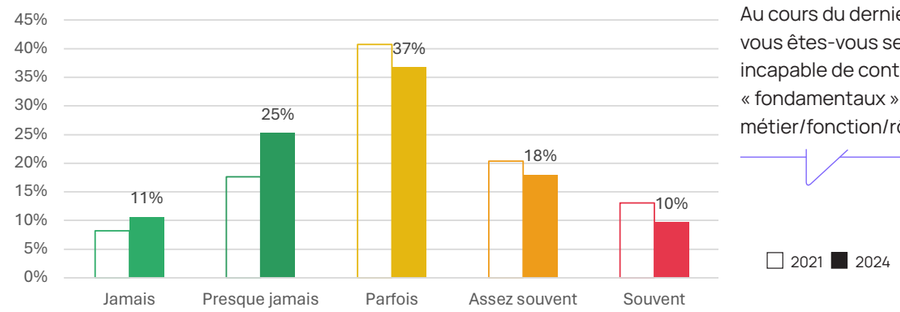
Ces modèles ont été utilisés dans de nombreux pays et déclinés dans le monde professionnel. La version française du PSS10 a fait l'objet de plusieurs études et sa fiabilité/corrélation avec d'autres modèles de référence a été démontrée.

Mesure du niveau de stress : comparaison entre 2021 et 2024

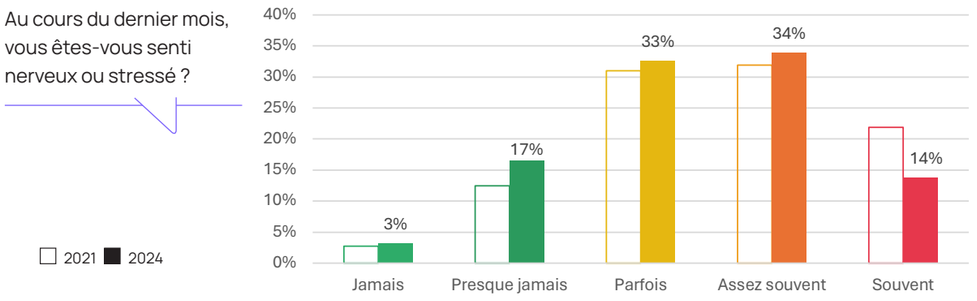
Au cours du dernier mois, vous êtes-vous senti contrarié ou énervé par des événements non prévus ?

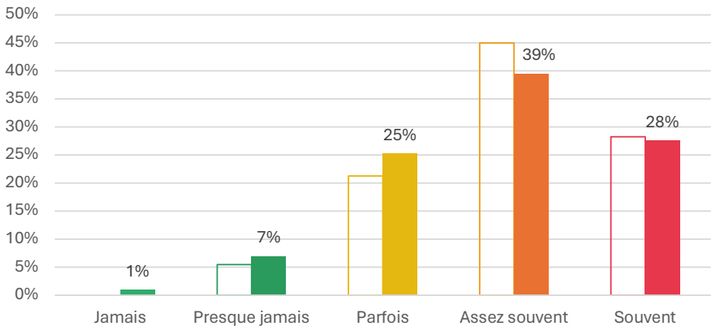


Au cours du dernier mois, vous êtes-vous senti incapable de contrôler les « fondamentaux » de votre métier/fonction/rôle ?



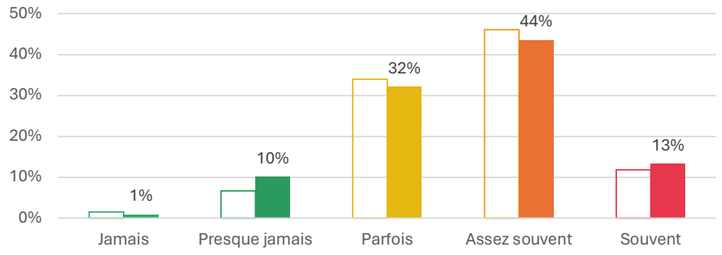
Au cours du dernier mois, vous êtes-vous senti nerveux ou stressé ?





Au cours du dernier mois, vous êtes-vous senti incapable de gérer vos problèmes professionnels ?

2021 2024

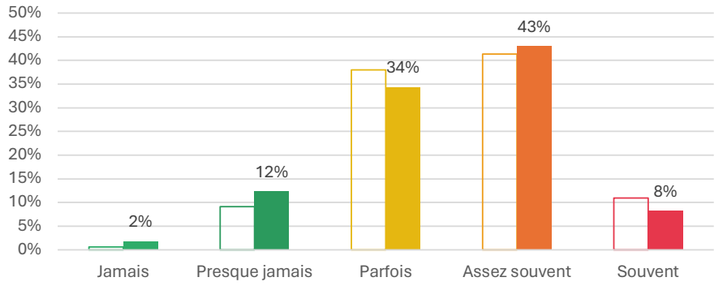


Au cours du dernier mois, avez-vous senti que vous « ne maîtrisiez pas la situation » ?

2021 2024

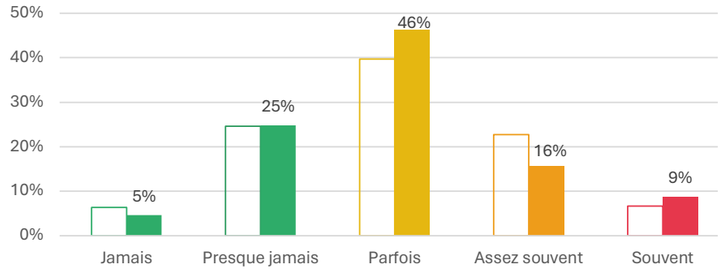
Au cours du dernier mois, avez-vous senti que les choses n'allaient pas comme vous le souhaitiez ?

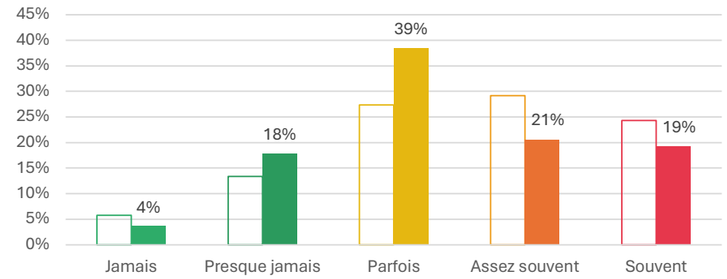
2021 2024



Au cours du dernier mois, vous êtes-vous senti irrité parce que les événements échappaient à votre contrôle ?

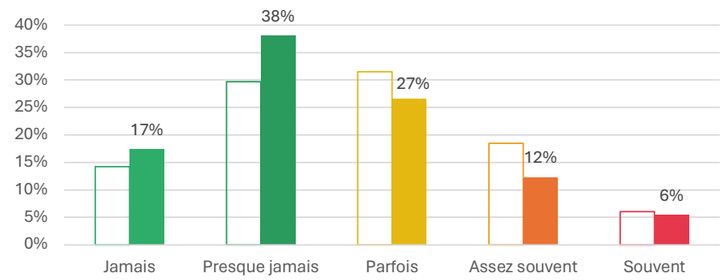
2021 2024





Au cours du dernier mois, avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?

2021 2024

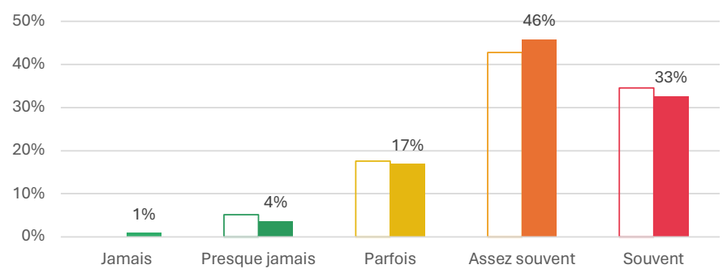


Au cours du dernier mois, avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?

2021 2024

Au cours du dernier mois, avez-vous été incapable de maîtriser (intérieurement et extérieurement) votre agacement ?

2021 2024



Résultats détaillés concernant les facteurs de stress

Quels sont les facteurs propres à la Cybersécurité et pouvant générer du stress ?

Est-ce que vous éprouvez un sentiment de culpabilité, lié (ou pas) au regard de votre entourage et/ou votre hiérarchie, lorsqu'un incident survient, et que vous n'avez pu l'empêcher, le détecter et/ou en limiter l'impact ?

Avez-vous le sentiment de devoir vous justifier auprès des autres, voire auprès de vous-même de l'utilité de vos actions ?

Comment ressentez-vous l'exercice de la communication, arrivez-vous à vous exprimer vraiment, à vous sentir en empathie, à convaincre vos interlocuteurs ?

Vous sentez-vous compris ou a minima soutenu par vos proches pendant les périodes où vous gérez des crises ?

Appréciez-vous l'exercice périlleux, la balance permanente entre les décisions à prendre et les informations disponibles pour pouvoir les prendre, tout au long d'une crise ?

Est-ce que vous vivez bien l'adrénaline, la pression et le sentiment d'urgence généralement associés à une crise cyber ?

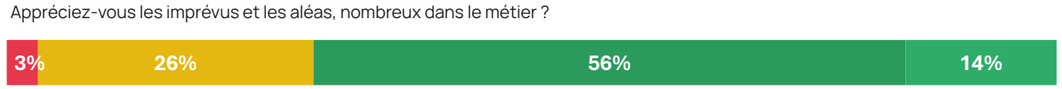
Est-ce que la gestion du risque cyber vous parait un exercice intellectuellement difficile ?

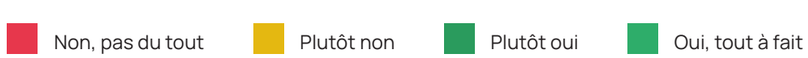
Considérez-vous que votre situation professionnelle est incertaine et qu'une crise majeure pourrait vous coûter votre poste ?

Etes-vous sur le qui-vive en permanence, sans pouvoir déconnecter vos pensées de votre travail, dans la crainte de la survenue d'une cyberattaque ou d'une situation à risque ?

Etes-vous perturbé de ne pas connaître a priori, voire ne jamais connaître ceux qui vous attaquent ou commettent une action malveillante ?

Appréciez-vous les imprévus et les aléas, nombreux dans le métier ?





Vous arrive-t-il de vous sentir personnellement en danger, devant cette adversité ?

Avez-vous un sentiment d'impuissance devant le caractère asymétrique du combat, l'attaquant ayant un net avantage sur le défenseur ?

Vous sentez-vous découragé devant l'augmentation de la fréquence et de la puissance des cyberattaques ?

Êtes-vous frustré d'être uniquement du côté de la défense et de ne jamais pouvoir riposter ou contre-attaquer ?

Trouvez-vous votre métier singulier, dans la mesure où il fait face à des adversaires, souvent « invisibles » et malveillants, ce qui est peu usuel, car peu de professions connaissent ce contexte d'adversité ?

Êtes-vous à l'aise avec l'étendue fonctionnelle et technique que doit couvrir le métier cyber, qui doit assurer partout une défense efficace à tous les niveaux et sur tous les terrains ?

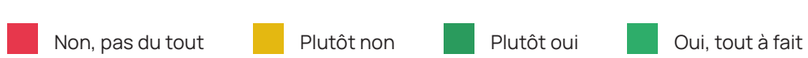
Estimez-vous difficile de devoir adapter en permanence vos analyses et stratégies devant un contexte de menace complexe et très évolutif, de devoir apprendre et vous réinventer sans cesse ?

Ressentez-vous un manque d'expertise technique ou méthodologique ?

Redoutez-vous les situations où votre métier vous amène à connaître des secrets et/ou vous place dans des contextes humainement délicats ou embarrassants ?

Avez-vous le sentiment d'être incompris(e) ou d'être jugé « excessif » lorsque vous faites des recommandations ?

Souffrez-vous de l'image et des a priori parfois négatifs autour de votre fonction, qui peuvent vous compliquer votre tâche voire provoquer un sentiment d'isolement ?



Résultats détaillés concernant les situations vécues

Comment les Responsables Cyber ont-ils vécu ces situations de leur quotidien ?

Vous avez rêvé à des cyberattaques et/ou crises cyber.

Vous avez autorisé une dérogation ou un contournement d'une règle de votre PSSI par peur du conflit ou par crainte d'être challengé par un collègue.

Vous avez ressenti un décalage trop important entre votre capacité à faire et les attentes de votre organisation en matière de protection contre les attaques et de gestion des risques.

Lors d'audits de sécurité, ou de réponses à des questionnaires sécurité divers, vous avez ressenti une angoisse à l'idée d'être encore loin d'avoir fait tout ce que vous estimez devoir faire pour être au niveau de maturité souhaité.

Vous avez donné un avis favorable sur une posture sécurité que vous n'approuviez pas intérieurement mais vous étiez découragé(e) voire angoissé(e) à la perspective d'une discussion et d'une « négociation » avec les parties prenantes.

Vous vous êtes senti désorienté, sans réelle vision ni capacité à déterminer les directions à prendre dans votre stratégie cyber.

Vous avez perdu vos moyens devant la présentation au board de votre bilan et votre plan d'actions.

Vous avez été très inquiet à l'idée de présenter votre tableau de bord cyber avec un certain nombre d'indicateurs au rouge.

Vous avez ressenti une angoisse ou n'avez pas su répondre à votre N+1 suite à la survenue d'un incident que vous n'aviez pas du tout envisagé.

Vous avez ressenti un sentiment de panique ou de paralysie lors d'une réponse à incident, dans une cellule de crise ou en dehors de la cellule.

Jamais | Oui, mais de façon très occasionelle | Oui, à plusieurs reprises

Résultats détaillés

Quelles actions ont été mises en place pour faire face au stress ?

Vous avez transformé le radical « GO/NO GO » Cyber sur les projets en une « simple » formulation de recommandations.

Vous avez fait sortir du dispositif de gestion de crise, une personne (ou vous-même) qui était en situation de panique ou de paralysie.

Vous avez revu votre feuille de route Cyber pour que les travaux à mener vous semblent moins angoissants, sans nécessairement tenir compte de l'impact sur le niveau de risque de votre organisation.

Vous avez simplifié et adapté votre tableau de bord cyber pour qu'il soit moins anxiogène à vos yeux.

Vous avez sollicité une formation ou une assistance externe pour vous aider à gérer votre charge mentale professionnelle ou celle de votre équipe.

Vous avez mis en place un dispositif d'astreinte partagée entre plusieurs personnes, qui vous permet de ne plus être jouagnable en 24/7 tous les jours de l'année.

Avez-vous envisagé un plan d'action particulier pour mieux gérer le stress des membres de votre équipe ?

Avez-vous envisagé un plan d'action particulier pour mieux gérer votre stress ?

Non | Oui

Intervenants

Mylène Jarossay	Mylène Jarossay est Directrice Cybersécurité du Groupe LVMH et Présidente du CESIN. Elle a participé à la fondation du CESIN en 2012.
Vincent Lefret	Vincent Lefret est RSSI chez U Tech et administrateur du CESIN.
Benjamin Leroux	Benjamin Leroux est Directeur Marketing chez Advens, dont il a été le RSSI. Il évolue dans le milieu de la Cybersécurité depuis plus de 20 ans.

Crédits : Adobe Stock, Shutterstock, Freepik, Flaticon
Conception-rédaction : Loreleï Fritsch I Design graphique : Agence La nageuse